El anillo de polinomios $D[Z]$ con coeficientes en los números duales

Haydee Jiménez Tafur
Grupo de Álgebra
Universidad Pedagógica Nacional
Bogotá D.C, Colombia
jimenezhaydee@gmail.com

Carlos Luque Arias
Profesor Universidad Pedagógica Nacional
Grupo de Álgebra
Bogotá D.C, Colombia
caluque@pedagogica.edu.co

Resumen

Se presenta el anillo de las series formales con coeficientes en D y con éste el anillo de los polinomios donde se estudian sus unidades, donde resultan polinomios no constantes que tienen inverso multiplicativo; asociados y divisibilidad; mostrando que se cumple el algoritmo de la división, los teoremas del residuo y del factor, que existen polinomios con infinitas raíces diferentes; luego se realiza una presentación de los ideales en $D[Z]$ y se finaliza con afirmaciones que se muestran a nivel de conjetura, sobre polinomios irreducibles en $D[Z]$.

1. El anillo de los números duales

1.1. Operaciones en los números duales[1]

Definición 1.1. Sea D el plano cartesiano $\mathbb{R}^2$, con la adición de (a, b) y (c, d) definida componente a componente,

$$(a, b) + (c, d) = (a + c, b + d)$$

y la multiplicación definida por

$$(a, b)(c, d) = (ac, ad + bc).$$

Definición 1.2. Dos elementos $z = (a, b)$ y $w = (c, d)$ en D son iguales si y sólo si $a = c$ y $b = d$.

Teorema 1.1. Con las dos operaciones anteriores D es un anillo conmutativo, con elemento idéntico $(1, 0)$. A esta estructura se le conoce como *Números Duales* o *Números de Study*[2].

El conjunto de los números duales con la adición y la multiplicación *no forman un dominio de integridad*, debido a la existencia de elementos divisores de cero, es decir elementos diferentes de $(0, 0)$ tales que su producto es $(0, 0)$. En D los divisores de cero corresponden a elementos de la forma $(0, b)$ para cualquier número real b.

Teorema 1.2. La propiedad cancelativa se cumple en elementos de la forma $z = (a, b)$ con $a \neq 0$.

[1] La demostración de los teoremas que aparecen en esta sección puede ser consultada en: Jiménez, H., Luque, C. (2007). *El anillo de los números duales*. En: Memorias del XVII Encuentro de Geometría y V Encuentro de Aritmética. Tomo I. Bogotá: Universidad Pedagógica Nacional. p.p. 159 - 194.

[2] YAGLOM, I. (1979). *A simple non Euclidean geometry and its physical basis*, Springer Verlag, New York, p. 265.

Teorema 1.3. El anillo de los números duales es de característica 0.

Teorema 1.4. El conjunto de los números duales de la forma $(a, 0)$ es isomorfo con los números reales.

Teorema 1.5. D tiene estructura usual de espacio vectorial real de dimensión 2.

Si $n = (0, 1)$ y se nota $x(1, 0) = (x, 0)$ con el número real x, se escribe $(x, y) = x + yn$ con $n^2 = 0$.

Teorema 1.6. D es un álgebra asociativa.

Definición 1.3. El conjugado de un número dual $z = (a, b)$ es $\overline{z} = (a, -b)$.

Teorema 1.7. El álgebra asociativa D con la función definida por

$$^- : D \longrightarrow D$$

que a cada $z = (a, b)$ le asigna su conjugado dual $\overline{z} = (a, -b)$, es una $\star$-Álgebra[3].

Teorema 1.8. Para todo z en D, se cumple que $\overline{(\overline{z})} = z$.

Teorema 1.9. Para todo z, w en D, se tiene que $\overline{(zw)} = \overline{z}\,\overline{w}$.

Teorema 1.10. Para todo z, w en D y a en $\mathbb{R}$, se tiene que $\overline{(az + w)} = a\overline{z} + \overline{w}$.

Teorema 1.11. $z = \overline{z}$ si y sólo si z es un número real.

Teorema 1.12. Para todo número natural $m \geq 2$ y todo número dual z, $\overline{z^m} = (\overline{z})^m$.

Definición 1.4. Un elemento (x, y) en D es una *unidad* o es *invertible* si existe un (w, t) en D tal que $(x, y)(w, t) = (1, 0)$, éste elemento (w, t) es único y es el inverso de (x, y) denotado también por $(x, y)^{-1}$.

Teorema 1.13. Las unidades en D son de la forma (a, b) con $a \neq 0$ y

$$(a, b)^{-1} = \frac{1}{a^2}(a, -b) = (a^{-1}, -ba^{-2}).$$

Teorema 1.14 ($*$[4]). El conjunto de las unidades $U(D)$, es un grupo abeliano con la operación de multiplicación de D.

Teorema 1.15. $U(D)$ con la multiplicación tiene estructura de cuasigrupo[5] .

Definición 1.5. La división entre dos números duales $z = (a, b)$ y $w = (c, d)$ en $U(D)$, es:

$$\frac{z}{w} = zw^{-1}$$

y en términos de sus componentes:

$$zw^{-1} = (a, b)\frac{1}{c^2}(c, -d)$$

que se puede escribir como

$$zw^{-1} = \frac{(a, b)}{(c, d)}\frac{(c, -d)}{(c, -d)}.$$

[3] D no es una $C^\star$-Álgebra porque su seminorma no es una norma.

[4] Este teorema se cumple en cualquier anillo conmutativo con identidad. De aquí en adelante este tipo de teoremas estarán marcados con $*$.

[5] La definición de cuasigrupo se debe a B.A. HAUSMANN y O. ORE (HAUSMANN, B., ORE, O., *Theory of quasigroups*, Amer. J. Math. 59 (1937), 983 - 1004.), basados en el estudio de las estructuras no asociativas de R. MOUFANG (1905 - 1977) quién descubrió en 1937 la relación entre los planos proyectivos no-desarguesianos y esta estructura.

2. El anillo de polinomios $D[Z]$ con coeficientes en los números duales

2.1. El anillo de las series formales de potencias $Suc(D)$

Definición 2.1. Sea $Suc(D)$ el conjunto de todas las sucesiones infinitas que se pueden formar con elementos de D, luego un elemento de $Suc(D)$ es de la forma:

$$q = (a_1, a_1, a_2, \ldots, a_k, \ldots)$$

con a_k en D.

Definición 2.2. Dos elementos $p = (a_0, a_1, a_2, \ldots, a_k, \ldots)$ y $q = (b_0, b_1, b_2, \ldots, b_k, \ldots)$ de $Suc(D)$ son iguales si y sólo si $a_k = b_k$ para todo $k \geq 0$.

Definición 2.3. En $Suc(D)$ se definen dos operaciones, adición y multiplicación[6] , como:

$$p + q = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k, \ldots)$$
$$pq = (c_0, c_1, c_2, \ldots, c_k, \ldots)$$

para todo $k \geq 0$, en el cual cada c_k está dado por:

$$c_k = \sum_{i+j=k} a_i b_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0 \quad \text{donde } i, j \geq 0.$$

Teorema 2.1 ($*$[7]). Con estas dos operaciones $Suc(D)$ es un anillo conmutativo con unidad.

La sucesión con todos sus elementos iguales a 0, $(0, 0, 0, \ldots)$, es el elemento idéntico para la adición, la sucesión $(1, 0, 0, 0, \ldots)$ es el elemento idéntico para la multiplicación y el inverso aditivo de un elemento $p = (a_0, a_1, a_2, \ldots, a_k, \ldots)$ de $Suc(D)$ es $-p = (-a_0, -a_1, -a_2, \ldots, -a_k, \ldots)$.

Teorema 2.2 ($*$). En el anillo $Suc(D)$ de las sucesiones con coeficientes en D, el conjunto

$$F = \{(a, 0, 0, \ldots) : a \in D\}$$

con la suma y multiplicación de las sucesiones es un subanillo de $Suc(D)$.

Teorema 2.3. F es isomorfo con D.

Demostración:
La función $$f : D \longrightarrow F$$
tal que a cada elemento a de D se le asigna $f(a) = (a, 0, 0, 0, \ldots)$, es biyectiva y se cumple que:

$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b).$$

□

[6]No significa lo mismo que en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.
[7]Todos los teoremas que se enuncian sin demostración son consecuencia directa de las definiciones.

Los elementos de D considerados como sucesiones se llaman *constantes*.

En $Suc(D)$ se utiliza el símbolo Z para distinguir el elemento

$$Z = (0, 1, 0, 0, 0, \ldots)$$

que tiene un comportamiento particular: si se multiplica por él mismo, se obtiene:

$$Z^2 = Z \cdot Z = (0, 0, 1, 0, 0, \ldots)$$

si se insiste, resulta

$$Z^3 = Z \cdot Z \cdot Z = (0, 0, 0, 1, 0, 0, \ldots)$$

y así sucesivamente

$$Z^n = \underbrace{Z \cdot Z \cdots Z}_{\text{n-veces}} = (0, 0, 0, \ldots, 0, 1, 0, 0, \ldots)$$

donde 1 está en la posición $n + 1$.

Con este resultado se puede escribir una sucesión cualquiera

$$t = (a_0, a_1, a_2, \ldots, a_i, \ldots)$$

como

$$t = (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + (0, 0, a_2, 0, 0, \ldots) + \cdots + (0, 0, \ldots, a_i, 0, 0, \ldots) + \cdots$$

o lo que es igual

$$\begin{aligned} t = {} & a_0(1, 0, 0, \ldots) + a_1(0, 1, 0, 0, \ldots) + a_2(0, 0, 1, 0, 0, \ldots) + \cdots \\ & + a_i(0, 0, \ldots, 1, 0, 0, \ldots) + \cdots \end{aligned}$$

o sea que cualquier elemento del anillo $Suc(D)$ se puede escribir como

$$t = a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots + a_i Z^i + \cdots$$

expresión que se denomina *serie formal de potencias sobre* D y a los elementos $a_0, a_1, \ldots, a_i$ coeficientes de t. Otra forma de escribir la serie es:

$$t = t(Z) = \sum a_j Z^j$$

El elemento Z es usualmente llamado *indeterminada*. El anillo $Suc(D)$ también recibe el nombre de $D[[Z]]$.

2.2. El anillo de polinomios $D[Z]$

Definición 2.4. El conjunto de todas las series formales de $D[[Z]]$ para las que existe un número natural n, con $n \geq 0$ tal que para todo número natural k, $k > n$, se tiene que $a_k = 0$ se denota como $D[Z]$. Entonces

$$D[Z] = \{a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots + a_n Z^n : a_i \in D, n \geq 0\}$$

Un elemento de $D[Z]$ se llama polinomio con coeficientes en D.

Definición 2.5. Los polinomios $q(Z) = a_0 + a_1 Z + a_2 Z^2 + a_3 Z^3 + \cdots + a_n Z^n$ y $g(Z) = b_0 + b_1 Z + b_2 Z^2 + b_3 Z^3 + \cdots + b_k Z^k$ en $D[Z]$, son iguales si y sólo si $a_i = bi$ para todo valor de $i \geq 0$.

El mayor valor de i para el cual a_i no es cero, es llamado grado del polinomio.

2.2.1. Adición de polinomios

Definición 2.6. La suma de dos polinomios en $D[Z]$, se define componente a componente. Si

$$q(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_nZ^n \quad \text{y} \quad g(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_kZ^k$$

Entonces

$$q(Z) + g(Z) = c_0 + c_1Z + c_2Z^2 + \cdots + c_mZ^m$$

donde

$$c_i = a_i + b_i \text{ para todo valor de } i \geq 0.$$

O sea que

$$q(Z) + g(Z) = (a_0 + b_0) + (a_1 + b_1)Z + (a_2 + b_2)Z^2 + \cdots + (a_m + b_m)Z^m$$

donde $m \leq \text{máx}\{n, k\}$.

El elemento idéntico[8] para la suma es

$$\mathbf{0} = (0,0) + (0,0)Z + (0,0)Z^2 + \cdots + (0,0)Z^j + (0,0)Z^{j+1} + \cdots$$

El inverso aditivo de

$$q(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_nZ^n$$

en $D[Z]$, es

$$q(Z) = -a_0 - a_1Z - a_2Z^2 - \cdots - a_nZ^n.$$

2.2.2. Multiplicación de polinomios

Definición 2.7. La multiplicación de

$$q(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_nZ^n \quad \text{y} \quad g(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_kZ^k$$

en $D[Z]$, es

$$q(Z)g(Z) = c_0 + c_1Z + c_2Z^2 + \cdots + c_qZ^q$$

en el que cada

$$c_p = \sum_{k=0}^{p} a_k b_{p-k}$$

y $q \leq n + k$, donde q es el grado de $p(Z)q(Z)$, n es el grado del polinomio $q(Z)$ y k es el grado de $g(Z)$.

A diferencia de lo que ocurre en los dominios de integridad, en $D[Z]$ no se tiene la igualdad debido a la existencia de elementos nilpotentes en D, pues si dados dos polinomios cada uno con coeficientes principales nilpotentes, el grado del producto será menor que la suma de los grados de cada uno.

[8] Como de costumbre, se usa el símbolo 0, con significados análogos pero diferentes.

Ejemplo 2.1. Al multiplicar $p(Z) = (2,1) + (0,1)Z$ y $q(Z) = (1,2) + (0,2)$ se tiene que

$$\begin{aligned} p(Z)q(Z) &= (2,5) + (0,4)Z + (0,1)Z + (0,0)Z^2 \\ &= (2,5) + (0,5)Z \end{aligned}$$

Donde el grado(p(Z) q(Z))¡grado(p(Z)) + grado(q(Z)).

La igualdad se da cuando alguno de los dos polinomios tiene el coeficiente principal no nilpotente.

Ejemplo 2.2. Si se multiplica $p(Z) = (0,3) + (0,2)Z + (2,1)Z^2$ y $q(Z) = (1,4) + (0,1)Z$ se obtiene que

$$p(Z)q(Z) = (0,3) + (0,2)Z + (2,9)Z^2 + (0,2)Z^3.$$

Teorema 2.4. Con las dos operaciones anteriores $D[Z]$ es un anillo conmutativo con unidad.

EL elemento idéntico para la multiplicación es

$$\mathbf{1} = (1,0) + (0,0)Z + (0,0)Z^2 + \cdots + (0,0)Z^j + (0,0)Z^j + 1 + \cdots$$

El conjunto de los polinomios con la adición y la multiplicación *no forman un dominio de integridad*, debido a la existencia de elementos divisores de cero, es decir, elementos diferentes de $0 = (0,0) + (0,0)Z + (0,0)Z^2 + \cdots + (0,0)Z^j + (0,0)Z^{j+1} + \cdots$ tales que su producto es 0. En $D[Z]$ los *divisores* de cero corresponden a polinomios de la forma

$$g(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_kZ^k$$

con b_i en D nilpotente, para todo $i \geq 0$.

2.3. Unidades en $D[Z]$

Teorema 2.5. Las unidades en $D[Z]$ son de la forma

$$u(Z) = u_0 + u_1Z + u_2Z^2 + \cdots + u_nZ^n$$

donde u_0 es un número dual no nilpotente y u_i es un número dual nilpotente para todo $i > 0$.

Demostración:

El polinomio $u(Z)^{-1}$ con u_0 un número dual no nilpotente y u_i un número dual nilpotente para todo $i > 0$, definido por:

$$\begin{aligned} u(Z)^{-1} &= \frac{1}{u_0} - \frac{u_1}{u_0^2}Z - \frac{u_2}{u_0^2}Z^2 - \cdots - \frac{u_n}{u_0^2}Z^n \\ &= \frac{1}{u_0^2}\left(u_0 - u_1z - u_2Z^2 - \cdots - u_nZ^n\right) \end{aligned}$$

está en $D[Z]$ y es el inverso de $u(Z)$, puesto que

$$u(Z)u(Z)^{-1} = c_0 + c_1Z + c_2Z^2 + \cdots + c_rZ^r$$

donde

$$c_0 = u_0\frac{1}{u_0} = 1$$

los c_i con $i > 1$ son 0 pues en cada uno el primer término es el inverso aditivo del último y en los demás se presenta un producto de dos números nilpotentes que siempre es 0:

$$\begin{aligned} c_1 &= u_0\left(-\frac{u_1}{u_0^2}\right) + \frac{u_1}{u_0} \\ c_2 &= u_0\left(-\frac{u_2}{u_0^2}\right) + u_1\left(-\frac{u_1}{u_0^2}\right) + \frac{u_2}{u_0} \\ &\vdots \\ c_p &= u_0\left(-\frac{u_2}{u_0^2}\right) + u_1\left(-\frac{u_1}{u_0^2}\right) + \cdots + \frac{u_p}{u_0} \end{aligned}$$

Por tanto

$$u(Z)u(Z)^{-1} = 1 + 0Z + 0Z^2 + \cdots + 0Z^r.$$

□

Ejemplo 2.3. 1. En $D[Z]$ el polinomio

$$p(Z) = 5 + (0,3)Z + (0,4)Z^2 + (0,2)Z^3$$

tiene como inverso

$$p(Z)^{-1} = \frac{1}{5} - \frac{(0,3)}{5^2}Z - \frac{(0,4)}{5^2}Z^2 - \frac{(0,2)}{5^2}Z^3.$$

2. En $D[Z]$ el polinomio

$$p(Z) = (1,2) + (0,2)Z^2 + (0,1)Z^3$$

tiene como inverso

$$p(Z)^{-1} = (1,-2) - (0,2)Z^2 - (0,1)Z^3.$$

Teorema 2.6 (∗). El conjunto de unidades $U(D[Z])$ de $D[Z]$, es un grupo abeliano para la operación de multiplicación en $D[Z]$.

2.4. Divisibilidad en $D[Z]$

Definición 2.8. Dados dos polinomios $p(Z)$ y $q(Z)$ en $D[Z]$, se dice que $p(Z)$ divide a $q(Z)$, o que $p(Z)$ es un divisor de $q(Z)$, o que $q(Z)$ es un múltiplo de $p(Z)$ (representado como $p(Z) \mid q(Z)$) si existe un polinomio $t(Z)$ en $D[Z]$ tal que $q(Z) = p(Z)t(Z)$.

Teorema 2.7 (∗). La relación de divisibilidad es reflexiva y transitiva.

Teorema 2.8 (∗). Dados $p(Z)$, $q(Z)$, $s(Z)$ y $t(Z)$ en $D[Z]$, si $p(Z) \mid q(Z)$ y $t(Z) \mid s(Z)$ entonces $p(Z)t(Z) \mid q(Z)s(Z)$.

Teorema 2.9 (∗). Para todo $p(Z)$, $q(Z)$ y $s(Z)$ en $D[Z]$, si $p(Z) \mid q(Z)$ y $p(Z) \mid s(Z)$, entonces $p(Z) \mid (q(Z) + s(Z))$.

Teorema 2.10 (∗). Para todo $p(Z)$, $q(Z)$ y $s(Z)$ en $D[Z]$, si $p(Z) \mid q(Z)$, entonces $p(Z) \mid q(Z)s(Z)$.

Teorema 2.11 (∗). Las unidades dividen a todo elemento de $D[Z]$.

Demostración:
Si $u(Z)$ es una unidad, cualquier elemento $p(Z)$ de $D[Z]$ se expresa como

$$p(Z) = u(Z)(u(Z)^{-1}p(Z)),$$

luego $u(Z) \mid p(Z)$. □

Teorema 2.12 (∗). Los divisores de las unidades son las unidades.

Demostración:
Si $u(Z)$ es una unidad y $p(Z) \mid u(Z)$, entonces existe un $q(Z)$ en $D[Z]$ tal que $u(Z) = p(Z)q(Z)$, luego $1 = p(Z)q(Z)u(Z)^{-1}$, es decir, $p(Z)$ es una unidad. □

2.5. Asociados en $D[Z]$

Definición 2.9. Un elemento $p(Z)$ en $D[Z]$ es un asociado de un elemento $s(Z)$ en $D[Z]$ si existe una unidad $u(Z)$ en $D[Z]$ tal que $p(Z) = u(Z)s(Z)$, en otras palabras, $p(Z)$ y $s(Z)$ son asociados si $p(Z) \mid s(Z)$ y $s(Z) \mid p(Z)$.

Teorema 2.13 (∗). La relación de asociación es una relación de equivalencia sobre $D[Z]$.

Teorema 2.14. Los polinomios asociados a un polinomio nilpotente $n(Z) = c_0 + c_1Z + c_2Z^2 + \cdots + c_nZ^n$ en $D[Z]$ son polinomios nilpotentes de la forma $u_0n(Z)$ donde u_0 es un elemento en D no nilpotente.
Demostración:
Como toda unidad en $D[Z]$ es de la forma $u(Z) = u_0 + u_1Z + u_2Z^2 + \cdots + u_kZ^k$ donde u_0 es no nilpotente y u_i es nilpotente para todo número natural $i \neq 0$,

$$u(Z)n(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_rZ^r$$

donde

$$\begin{aligned}
b_0 &= c_0u_0\\
b_1 &= c_0u_1 + c_1u_0\\
b_2 &= c_0u_2 + c_1u_1 + c_2u_0\\
b_3 &= c_0u_3 + c_1u_2 + c_2u_1 + c_3u_0\\
&\vdots\\
b_p &= c_0u_p + c_1u_{p-1} + c_2u_{p-2} + \cdots + c_pu_0
\end{aligned}$$

y como el producto de dos nilpotentes es igual a 0,

$$\begin{aligned}
b_0 &= c_0u_0\\
b_1 &= c_1u_0\\
b_2 &= c_2u_0\\
b_3 &= c_3u_0\\
&\vdots\\
b_p &= c_pu_0
\end{aligned}$$

luego
$$u(Z)n(Z) = u_0 n(Z).$$

□

Teorema 2.15. Los polinomios asociados a un polinomio $h(Z) = c_0 + c_1 Z + c_2 Z^2 + \cdots + c_n Z^n$ en $D[Z]$ de grado $n > 0$ donde existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente, son polinomios de la forma

$$u_0 h(Z) + c_i Z^i (u(Z) - u_0)$$

donde $u(Z) = u_0 + u_1 Z + u_2 Z^2 + \cdots + u_k Z^k$ es una unidad.

Demostración:
El producto
$$u(Z)h(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_r Z^r$$

donde $r = k + i$ tiene como coeficientes a

$$\begin{aligned}
b_0 &= c_0 u_0 \\
b_1 &= c_0 u_1 + c_1 u_0 \\
b_2 &= c_0 u_2 + c_1 u_1 + c_2 u_0 \\
b_3 &= c_0 u_3 + c_1 u_2 + c_2 u_1 + c_3 u_0 \\
&\vdots \\
b_i &= c_0 u_i + c_1 u_{i-1} + c_2 u_{i-2} + \cdots + c_i u_0 \\
b_{i+1} &= c_0 u_{i+1} + c_1 u_i + c_2 u_{i-1} + \cdots + c_i u_1 + c_{i+1} u0 \\
b_{i+2} &= c_0 u_{i+2} + c_1 u_{i+1} + c_2 u_i + \cdots + c_i u_2 + c_{i+1} u_1 + c_{i+2} u_0 \\
&\vdots \\
b_n &= c_0 u_n + c_1 u_{n-1} + c_2 u_{n-2} + \cdots + c_i u_{n-i} + \cdots + c_n u_0 \\
b_{n+1} &= c_0 u_{n+1} + c_1 u_n + c_2 u_{n-1} + \cdots + c_i u_{(n+1)-i} + \cdots + c_n u_1 + c_{n+1} u_0 \\
&\vdots \\
b_r &= c_0 u_{k+i} + c_1 u_{(k+i)-1} + c_2 u_{(k+i)-2} + \cdots + c_i u_k + \cdots + c_{(k+i)} u_0
\end{aligned}$$

Como u_0, c_i son no nilpotentes, los c_j con $0 \leq j \leq n$ y $i \neq j$ son nilpotentes, los u_l con $1 \leq l \leq n$ son nilpotentes y el producto de dos nilpotentes es igual a 0, entonces

$$\begin{aligned}
b_0 &= c_0 u_0 \\
b_1 &= c_1 u_0 \\
b_2 &= c_2 u_0 \\
b_3 &= c_3 u_0 \\
&\vdots
\end{aligned}$$

$$\begin{aligned} b_i &= c_i u_0 \\ b_{i+1} &= c_i u_1 + c_{i+1} u_0 \\ b_{i+2} &= c_i u_2 + c_{i+2} u_0 \\ &\vdots \\ b_n &= c_i u_{n-i} + c_n u_0 \\ b_{n+1} &= c_i u_{(n+1)-i} \\ &\vdots \\ b_r &= c_i u_k \end{aligned}$$

Luego

$$u(Z)h(Z) = u_0(c_0 + c_1 Z + c_2 Z^2 + \cdots + c_n Z^n) + c_i Z^i (u_1 Z + u_2 Z^2 + \cdots + u_k Z^k)$$

o sea

$$u(Z)h(Z) = u_0 h(Z) + c_i Z^i (u(Z) - u0).$$

□

2.6. Algoritmo de división en $D[Z]$

Teorema 2.16. Dados $p(Z)$ y $q(Z)$ polinomios en $D[Z]$ con $q(Z) \neq 0$ y su coeficiente principal invertible, es decir no nilpotente, existen polinomios $t(Z)$ y $r(Z)$ en $D[Z]$ que son únicos, de manera que se cumple:

$$p(Z) = q(Z)t(Z) + r(Z)$$

donde $r(Z) = 0$ ó grado $(r(Z)) <$ grado $(q(Z))$.

Demostración:
Se recurre a la inducción sobre el grado de $p(Z)$. Para iniciar se observan varios casos:

Cuando $p(Z) = 0$ se tiene la condición haciendo que $t(Z) = 0 = r(Z)$; cuando el grado $(p(Z)) <$ grado $(q(Z))$ se llega a la condición tomando $t(Z) = 0$ y $r(Z) = p(Z)$; y cuando el grado $(p(Z))$ = grado $(q(Z)) = 0$ los dos son elementos del anillo D, la proposición se demuestra escogiendo a $t(Z) = p(Z)q(Z)^{-1}$ y a $r(Z) = 0$.

Falta demostrar el caso donde el grado $(p(Z)) >$ grado $(q(Z))$, entonces se inicia la inducción sobre el grado de $p(Z)$, suponiendo que el teorema se cumple para todo polinomio de grado menor que el de $p(Z)$, donde el grado $(p(Z)) >$ grado $(q(Z)) > 1$, luego

$$\begin{aligned} p(Z) &= a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n, \quad a_n \neq 0 \\ q(Z) &= b_0 + b_1 Z + b_2 Z^2 + \cdots + b_m Z^m, \quad b_m \neq 0 \end{aligned}$$

Si se divide el termino n-ésimo de $p(Z)$ entre el término m-ésimo de $q(Z)$ se obtiene $(a_n b_m^{-1}) Z^{n-m}$.

Al multiplicar $(a_n b_m^{-1}) Z_{n-m}$ por $q(Z)$ y el resultado restárselo a $p(Z)$, obtenemos un polinomio $p_1(Z)$ de $D[Z]$, que se expresa como

$$p_1(Z) = p(Z) - (a_n b_m^{-1}) Z^{n-m} q(Z)$$

y como el coeficiente de Z^n en $p_1(Z)$ es $a_n - (a_n b_m^{-1})b_m = 0$, entonces el

$$\text{grado } (p_1(Z)) < \text{grado } (p(Z))$$

y por la hipótesis de inducción, el teorema se cumple para el polinomio $p_1(Z)$, luego existen $t_1(Z)$, $r(Z)$ en $D[Z]$ tales que

$$p_1(Z) = t_1(Z)q(Z) + r(Z)$$

donde $r(Z) = 0$ ó grado $(r(Z)) <$ grado $(q(Z))$. Entonces se obtiene que

$$\begin{aligned} p(Z) &= p_1(Z) + (a_n b_m^{-1})Z^{n-m}q(Z) \\ p(Z) &= (t_1(Z)q(Z) + r(Z)) + (a_n b_m^{-1})Z^{n-m}q(Z) \\ p(Z) &= (t_1(Z) + (a_n b_m^{-1})Z^{n-m})q(Z) + r(Z) \end{aligned}$$

Por tanto queda demostrado que el teorema se cumple para cualquier polinomio $p(Z)$.

Para mostrar la unicidad de los polinomios $t(Z)$ y $r(Z)$, se supone que existen otros polinomios $t_0(Z)$ y $r_0(Z)$ tales que

$$p(Z) = q(Z)t(Z) + r(Z) = q(Z)t_0(Z) + r_0(Z)$$

donde $r(Z) = 0 = r_0(Z)$ ó grado $(r(Z)) <$ grado $(q(Z))$ y grado $(r_0(Z))$ ¡grado $(q(Z))$.

Entonces:

$$r(Z) - r_0(Z) = (t_0(Z) - t(Z))q(Z)$$

Si se supone que $t_0(Z) - t(Z) \neq 0$ y como el coeficiente principal de $q(Z)$ es invertible, es decir no nilpotente, entonces

$$\text{grado } ((t_0(Z) - t(Z))q(Z)) = \text{grado } (t_0(Z) - t(Z)) + \text{grado } (q(Z)),$$

y como

$$\text{grado } (t_0(Z) - t(Z)) + \text{grado } (q(Z)) \geq \text{grado } (q(Z))$$

entonces

$$\text{grado } ((t_0(Z) - t(Z))q(Z)) \geq \text{grado } (q(Z))$$

pero como

$$\text{grado } (r(Z) - r_0(Z)) < \text{grado } (q(Z)),$$

se llega a una contradicción. Por lo tanto $t_0(Z) = t(Z)$ y en consecuencia $r(Z) = r_0(Z)$. □

2.7. Homomorfismo de evaluación

Teorema 2.17 (∗). La función $e_z : D[Z] \longrightarrow D$ que a todo polinomio $p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$ con $a_n \neq 0$, le asigna $a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n$ con z en D, es un homomorfismo de anillos, puesto que D es conmutativo. Este homomorfismo es llamado *homomorfismo de evaluación.*

Es importante recalcar que D sea conmutativo, pues si no lo fuera, entonces:

$$\begin{aligned} e_z[(a_0 + a_1Z)(b_0 + b_1Z)] &= e_z[a_0b_0 + (a_0b_1 + a_1b_0)Z + (a_1b_1)Z^2] \\ &= a_0b_0 + (a_0b_1 + a_1b_0)z + (a_1b_1)z^2 \end{aligned}$$

y

$$e_z(a_0 + a_1Z)ez(b_0 + b_1Z) = (a_0 + a_1z)(b_0 + b_1z) \qquad = a_0b_0 + a_0b_1z + a_1zb_0 + a_1zb_1z$$

no serían necesariamente iguales.

2.8. Teorema del residuo

Teorema 2.18 (Teorema del residuo $*$). Dado $p(Z)$ en $D[Z]$ y a en D, existe un único polinomio $q(Z)$ en $D[Z]$ tal que

$$p(Z) = q(Z)(Z - a) + p(a).$$

Demostración:
Aplicando el algoritmo de división a los polinomios $p(Z)$ y $(Z - a)$ se tiene que

$$p(Z) = q(Z)(Z - a) + r(Z)$$

donde el grado de $r(Z)$ es menor que 1, es decir, $r(Z)$ es una constante. Aplicando el homomorfismo de evaluación en a:

$$\begin{aligned} e_a(p(Z)) &= e_a(q(Z)(Z - a) + r) \\ p(a) &= q(a)(a - a) + r \end{aligned}$$

se tiene que $r = p(a)$. □

2.9. Teorema del factor

Definición 2.10. Si $p(Z)$ es un polinomio de $D[Z]$ entonces a en D es una raíz de $p(Z)$ si $e_a(p(Z)) = 0$.

Teorema 2.19 (Teorema del factor $*$). Si $p(Z)$ es un polinomio de $D[Z]$ entonces a en D es una raíz de $p(Z)$ si y sólo si $Z - a \mid p(Z)$.

Demostración:
Si a en D es una raíz de $p(Z)$, entonces $e_a(p(Z)) = 0$ y por el teorema del residuo se tiene que $p(Z) = q(Z)(Z - a)$, luego $Z - a|p(Z)$.
Si $Z - a \mid p(Z)$ entonces $p(Z) = q(Z)(Z - a)$ y aplicando el homomorfismo de evaluación en a se tiene que

$$\begin{aligned} e_a(p(Z)) &= e_a(q(Z)(Z - a)) \\ p(a) &= q(a)(a - a) = 0, \end{aligned}$$

luego a en D es una raíz de $p(Z)$. □

En el anillo de polinomios $K[x]$ con K un campo se cumple el teorema que dice: Si $p(x)$ es un polinomio distinto de 0 en $K[x]$ de grado n, entonces $p(x)$ tiene a lo más n raíces en K.

En $D[Z]$ no se cumple este teorema pues se tiene los polinomios de grado n de la forma

$$p(Z) = a_1 Z + a_2 Z^2 + \cdots + a_n Z^n$$

con a_1 nilpotente, tienen infinitas raíces: los nilpotentes en D, es decir los números de la forma $(0, b)$ con b en los números reales.

2.10. Ideales en $D[Z]$

Teorema 2.20. En $D[Z]$ el conjunto $N[Z]$ de todos los polinomios nilpotentes es un ideal principal.

Demostración:
Los polinomios nilpotentes son los que tienen todos los coeficientes nilpotentes y si se multiplica un elemento nilpotente $c \neq 0$ en D por un polinomio cualquiera en $D[Z]$ todos los coeficientes del producto son nilpotentes, esto es, $\langle c \rangle = \{cq(Z) : q(Z) \in D[Z]\}$.

Además, todo polinomio nilpotente se puede escribir como el producto de un polinomio $p(Z)$ en $D[Z]$ por un elemento nilpotente $(0, d)$ distinto de 0 en D, pues cada uno de sus coeficientes es de la forma $(0, m)$ y la ecuación

$$(0, m) = (0, d)(x, y)$$

siempre tiene solución en D. Por lo tanto el conjunto de todos los polinomios nilpotentes es un ideal principal generado por cualquier elemento nilpotente en D. □

Teorema 2.21. En $D[Z]$ el conjunto $Z \cdot p(Z)$ de todos los polinomios sin coeficiente constante es un ideal principal.

Demostración:
Los polinomios sin coeficiente constante son de la forma $Z \cdot p(Z)$ para algún $p(Z)$ en $D[Z]$ y $\langle Z \rangle = \{Zq(Z) : q(Z) \in D[Z]\}$, luego el conjunto de todos los polinomios sin coeficiente constante es un ideal principal generado por el polinomio Z. □

Teorema 2.22 (∗). Si I, J son ideales en $D[Z]$ entonces $I \cap J$ es un ideal en $D[Z]$.

Teorema 2.23 (∗). Si I, J son ideales en $D[Z]$ entonces

$$I + J = \{i + j : i \in I, \wedge, j \in J\}$$

es un ideal en $D[Z]$.

Teorema 2.24. El subconjunto $ZN[Z] = Zp(Z) \cap N[Z]$ de $D[Z]$ es un ideal principal.

Demostración:

Los polinomios nilpotentes sin coeficiente constante son de la forma $c_1 Z \cdot p(Z)$ con c_1 nilpotente en D y $\langle cZ\rangle = \{cZq(Z) : c^2 = 0,\ \wedge,\ q(Z) \in D[Z]\}$, luego el conjunto de todos los polinomios nilpotentes sin coeficiente constante es un ideal principal generado por el polinomio cZ con c nilpotente. □

Teorema 2.25. El subconjunto $N[Z] + Z \cdot p(Z)$ de $D[Z]$ es un ideal principal.
Demostración:

Los polinomios con coeficiente constante nilpotente son de la forma $a_0 + a_1 Z + \cdots + a_n Z^n$ con a_0 nilpotente y si se multiplica el polinomio $c_0 + c_1 Z$ con c_0 nilpotente distinto de 0 y c_1 no nilpotente, por un polinomio cualquiera en $D[Z]$, el coeficiente constante del producto será nilpotente, esto es,

$$\langle c_0 + c_1 Z\rangle = \{(c_0 + c_1 Z)q(Z) : (c_0)^2 = 0,\ \wedge,\ c_0 \neq 0,\ \wedge,\ (c_1)^2 \neq 0,\ \wedge,\ q(Z) \in D[Z]\}.$$

Además, todo polinomio $q(Z) = d_0 + d_1 Z + \cdots + d_n Z^n$ con coeficiente constante nilpotente se puede escribir como el producto de un polinomio $p(Z) = b_0 + b_1 Z + \cdots + b_k Z^k$ en $D[Z]$ por el polinomio $c_0 + c_1 Z$ con c_0 nilpotente distinto de 0 y c_1 no nilpotente, pues cada uno de sus coeficientes debe ser de la forma

$$d_i = c_0 b_i + c_1 b_{i-1}$$

y como $c_0 = (0, t)$ con $t \neq 0$, $c_1 = (x, y)$ con $x \neq 0$, se debe encontrar $b_i = (a, b)$ y $b_{i-1} = (c, d)$ y esto siempre es posible puesto que la ecuación

$$d_i = (w, z) = (xc, at + xd + yc)$$

tiene siempre soluciones en D. □

Teorema 2.26. En $D[Z]$ el conjunto $Z^k p(Z)$ de todos los polinomios

$$q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$$

cuyos coeficientes $a_i = 0$ con i, k números naturales tales que $0 \leq i < k$ es un ideal principal.

Demostración:

Los polinomios $q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ cuyos coeficientes $a_i = 0$ con i, k números naturales tales que $0 \leq i < k$ son de la forma $Z^k p(Z)$ para algún $p(Z)$ en $D[Z]$ y $\langle Z^k\rangle = \{Z^k t(Z) : t(Z) \in D[Z]\}$, luego el conjunto $Z^k p(Z)$ es un ideal principal generado por el polinomio Z^k. □

Corolario 1. En $D[Z]$ el conjunto $Z^2 p(Z)$ de todos los polinomios

$$q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$$

cuyos coeficientes a_0, a_1 son iguales a 0, es un ideal principal.

Demostración:

Los polinomios $q(Z) = a_0 + a_1 Z + \cdots + a_n Z^n$ cuyos coeficientes $a_0 = 0 = a_1$ son de la forma $Z^2 p(Z)$ para algún $p(Z)$ en $D[Z]$ y $\langle Z^2\rangle = \{Z^2 t(Z) : t(Z) \in D[Z]\}$, luego el conjunto $Z^2 p(Z)$ es un ideal principal generado por el polinomio Z^2. □

Teorema 2.27. El subconjunto $Z^kN[Z] = Z^kp(Z) \cap N[Z]$ de $D[Z]$ es un ideal principal.

Demostración:
Los polinomios nilpotentes $n(Z) = a_0 + a_1Z + \cdots + a_nZ^n$ cuyos coeficientes $a_i = 0$ con i, k números naturales tales que $0 \leq i < k$ son de la forma $c_1Z^kp(Z)$ con c_1 nilpotente en D y $\langle cZ^k\rangle = \{cZ^kq(Z) : k > 0, \wedge, c^2 = 0, \wedge, q(Z) \in D[Z]\}$, luego el conjunto $Z^kN[Z]$ es un ideal principal generado por el polinomio cZ^k con c nilpotente. □

Teorema 2.28. El subconjunto $N[Z] + Z^kp(Z)$ de $D[Z]$ es un ideal principal.

Demostración:
Si se multiplica el polinomio $c_0 + c_1Z + \cdots + c_kZ^k$ con c_i nilpotente distinto de 0, $0 \leq i \leq k-1$ y c_k no nilpotente, por un polinomio cualquiera $p(Z)$ en $D[Z]$, los coeficientes d_j con $0 \leq j \leq k-1$ del producto

$$(c_0 + c_1Z + \cdots + c_kZ^k)(p(Z)) = d_0 + d_1Z + \cdots + d_mZ^m$$

son todos nilpotente, esto es,

$$\begin{aligned}&\langle c_0 + c_1Z + \cdots + c_{k+1}Z^k\rangle\\ &= \Big\{(c_0 + c_1Z + \cdots + c_kZ^k)q(Z) : 0 \leq i \leq k-1, \wedge, c_i \neq 0, \wedge,\\ &\qquad\qquad (c_i)^2 = 0, \wedge, (c_k)^2 \neq 0, \wedge, q(Z) \in D[Z]\Big\}.\end{aligned}$$

De otro lado, todo polinomio $q(Z) = d_0 + d_1Z + \cdots + d_nZ^n$ con coeficientes d_j nilpotente, para $0 \leq j \leq k-1$, se puede escribir como el producto de un polinomio $p(Z) = b_0 + b_1Z + \cdots + b_mZ^m$ en $D[Z]$ por el polinomio $c_0 + c_1Z + \cdots + c_kZ^k$ con c_i nilpotente distinto de 0, $0 \leq i \leq k-1$ y c_k no nilpotente, pues cada uno de sus coeficientes debe ser de la forma

$$d_i = c_0b_i + c_1b_{i-1} + c_2b_{i-2} + \cdots + c_{k-1}b_{i-(k-1)} + c_kb_{i-k}$$

y como $c_0 = (0, t_0)$, $c_1 = (0, t_1)$, $c_2 = (0, t_2)$, …, $c_{k-1} = (0, t_{k-1})$, con $t_0, t_1, t_2, \ldots, t_{k-1}$, distintos de 0, $c_k = (x, y)$, con $x \neq 0$, se debe encontrar $b_i = (a_i, b_i)$, $b_{i-1} = (a_{i-1}, b_{i-1})$, $b_{i-2} = (a_{i-2}, b_{i-2}), \ldots, b_{i-(k-1)} = (a_{i-(k-1)}, b_{i-(k-1)}), b_{i-k} = (a_{i-k}, b_{i-k})$, y esto siempre es posible puesto que la ecuación

$$d_i = (w, z) = (xa_{i-k}, a_it_0 + a_{i-1}t_1 + \cdots + a_{i-(k-1)}t_{k-1} + xb_{i-k} + ya_{i-k})$$

tiene siempre soluciones en D. □

Teorema 2.29. Para todo número natural $k > 0$, se cumple que

$$\langle Z^k\rangle \subseteq \langle Z^{k-1}\rangle \subseteq \langle Z^{k-2}\rangle \subseteq \langle Z^{k-3}\rangle \subseteq \cdots \subseteq \langle Z^2\rangle \subseteq \langle Z\rangle.$$

Demostración:
Por inducción sobre k, el caso para $k = 1$ es evidente.

Se supone que la afirmación es cierta para todo número natural $i < k$, entonces es cierta en particular para $i = k - 1$.

Dado $p(Z) = a_0 + a_1Z + \cdots + a_nZ^n$ en Z^k por el teorema 2.26

$$\langle Z^k \rangle = \{Zkt(Z) : t(Z) \in D[Z]\},$$

luego $a_j = 0$ con $0 \leq j \leq k-1$ y como

$$\langle Z^{k-1} = \{Z^{k-1}t(Z) : t(Z) \in D[Z]\}$$

si $s(Z) = b_0 + b_1Z + \cdots + b_mZ^m$ está en $\langle Z^k - 1\rangle$, entonces $b_l = 0$ con $0 \leq l \leq k-2$, por tanto $p(Z)$ está en $\langle Z^k - 1\rangle$ de donde $\langle Z^k\rangle \subseteq \langle Z^{k-1}$, y por la hipótesis de inducción

$$\langle Z^k\rangle \subseteq \langle Z^{k-1}\rangle \subseteq \langle Z^{k-2}\rangle \subseteq \langle Z^{k-3}\rangle \subseteq \cdots \subseteq \langle Z^2\rangle \subseteq \langle Z\rangle.$$

□

Teorema 2.30. $D[Z]/\langle Z\rangle$ es isomorfo con D.

Demostración:
En el anillo

$$D[Z]/\langle Z\rangle = \{q(Z) + \langle Z\rangle : q(Z) \in D[Z]\}$$

las clases de equivalencia son los polinomios cuyo coeficiente constante es igual. Entonces la función

$$\begin{aligned} \lambda : D[Z]/\langle Z\rangle &\longrightarrow D \\ q(Z) + \langle Z\rangle &\longmapsto a_0 \end{aligned}$$

con $q(Z) = a_0 + a_1Z + \cdots + a_nZ^n$, es un homomorfismo puesto que dados

$$t(Z) = a_0 + a_1Z + \cdots + a_nZ^n \quad \text{y} \quad s(Z) = b_0 + b_1Z + \cdots + b_kZ^k$$

$$\begin{aligned} \lambda[(t(Z) + \langle Z\rangle) + (s(Z) + \langle Z\rangle)] &= \lambda[(t(Z) + s(Z)) + \langle Z\rangle] \\ &= a_0 + b_0 \\ &= \lambda[t(Z) + \langle Z\rangle)] + \lambda[(s(Z) + \langle Z\rangle)] \\ \lambda[(t(Z) + \langle Z\rangle)(s(Z) + \langle Z\rangle)] &= [(t(Z)s(Z)) + \langle Z\rangle] \\ &= a_0b_0 \\ &= \lambda[(t(Z) + \langle Z\rangle)]\lambda[(s(Z) + \langle Z\rangle)] \end{aligned}$$

Además λ es inyectiva ya que $N_\lambda = \{\langle Z\rangle\}$ y λ es sobreyectiva pues dado a en D, existe la clase de polinomios en $D[z]/\langle Z\rangle$ cuyo coeficiente constante es a. □

Teorema 2.31. En $D[Z]$ el ideal principal $Z \cdot p(Z)$ no es un ideal maximal.

Demostración:
Demostración: Por el *teorema*[9] *11.5* y el *teorema 2.30* se concluye que $Z \cdot p(Z)$ no es un ideal maximal. □

Teorema 2.32. $Z \cdot p(Z)$ no es un ideal primo.

2.11. Polinomios irreducibles en $D[Z]$

Las afirmaciones que se muestran a continuación sobre polinomios irreducibles en $D[Z]$ están a nivel de conjetura, fruto de los casos estudiados, porque al realizar intentos de demostración, éstos incluyen dos casos: uno en el que el producto de los coeficientes $a_i b_j$ de los polinomios considerados como factores sean todos iguales a 0 y el otro cuando uno de los productos $a_i b_j$ es el inverso aditivo de la suma de los demás. Este último caso no ha sido considerado en los intentos de demostración pero se sospecha que no se puede dar cuando se fijan los grados de los polinomios producto.

Afirmación 2.1. Un polinomio $h(Z) = c_0$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 es nilpotente.

Demostración:
[parcial] Si $h(Z) = c_0$ y $h(Z) = p(Z)q(Z)$ con

$$p(Z) = a_0 + a_1 Z + a_2 Z^2 + \cdots + a_r Z^r, \quad a_r \neq 0$$
$$q(Z) = b_0 + b_1 Z + b_2 Z^2 + \cdots + b_s Z^s, \quad b_s \neq 0$$

de manera que $0 \leq r + s$, entonces se deben buscar las condiciones sobre los coeficientes de $p(Z)$ y $q(Z)$ para que al realizar el producto se obtenga $h(Z)$.

Para que $c_0 = a_0 b_0$ sea nilpotente, es necesario que uno de los factores sea nilpotente y el otro no nilpotente.

Si a_0 es no nilpotente y b_0 es nilpotente, entonces dados

$$\begin{aligned} c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \\ c_3 &= a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 \\ &\vdots = \\ c_p &= a_0 b_p + a_1 b_{p-1} + a_2 b_{p-2} + \cdots + a_p b_0 \end{aligned}$$

los c_i con $1 \leq i \leq n$ deben ser iguales a 0, entonces si cada producto es cero, y como se tiene que a_0 es no nilpotente, observando la columna donde aparece a_0, resulta que los b_m con $1 \leq m \leq s$ deben ser iguales a 0. También se tiene que b_0 es nilpotente y observando la columna donde éste

[9] *Teorema 11.5. M* es ideal maximal en D si y sólo si D/M es un campo. La demostración de este teorema puede ser consultada en: Jiménez, H., Luque, C. (2007). *El anillo de los números duales.* En: Memorias del XVII Encuentro de Geometría y V Encuentro de Aritmética. Tomo I. Bogotá: Universidad Pedagógica Nacional. p.p. 192.

aparece, se obtiene que los a_j con $1 \leq j \leq r$ deben ser nilpotentes o iguales a 0. Con esas dos nuevas condiciones los otros productos que se presentan son iguales a 0.

Entonces $p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r$, debe cumplir que a_0 sea no nilpotente y los a_j con $1 \leq j \leq r$ sean nilpotentes o iguales a 0, es decir, son unidades. Y $q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s$, debe cumplir que b_0 sea nilpotente y los b_m con $1 \leq m \leq s$ sean iguales a 0, es decir, es una no unidad.

Por tanto un polinomio $h(Z) = c_0$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 es nilpotente y se cumplen las condiciones dadas. □

Afirmación 2.2. Un polinomio $h(Z) = c_0 + c_1Z$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 y c_1 son no nilpotentes.

Demostración:

[parcial] Si $h(Z) = c_0 + c_1Z$ y $h(Z) = p(Z)q(Z)$ con

$$p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r, \quad a_r \neq 0$$
$$q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s, \quad b_s \neq 0$$

de manera que $1 \leq r + s$, entonces se deben buscar las condiciones sobre los coeficientes de $p(Z)$ y $q(Z)$ para que al realizar el producto se obtenga $h(Z)$.

Para que $c_0 = a_0b_0$ sea no nilpotente, es necesario que los dos factores sean no nilpotentes.

Si a_0 y b_0 son no nilpotentes, entonces para que $c_1 = a_0b_1 + a_1b_0$ sea no nilpotente se dan los siguientes casos:

a_1	b_1
No nilpotente	No nilpotente
No nilpotente	Nilpotente
No nilpotente	0
Nilpotente	No nilpotente
0	No nilpotente

Y como

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0$$
$$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$$
$$\vdots =$$
$$c_p = a_0b_p + a_1b_{p-1} + a_2b_{p-2} + \cdots + a_pb_0$$

los c_i con $2 \leq i \leq n$ deben ser iguales a 0, entonces si cada producto es cero, $a_1b_1 = 0$, implica que de las opciones mencionadas sólo son posibles aquellas donde a_1 es no nilpotente y b_1 es 0, o cuando a_1 es 0 y b_1 es no nilpotente.

Como se tiene que a_0 es no nilpotente y $a_0b_m = 0$ con $2 \leq m \leq s$ entonces los b_m deben ser iguales a 0. Análogamente como b_0 es no nilpotente, los a_j con $2 \leq j \leq r$ deben ser iguales a 0. Con esas condiciones los otros productos que se presentan son iguales a 0.

Entonces si $p(Z) = a_0+a_1Z+a_2Z^2+\cdots+a_rZ^r$, cumple que a_0 es no nilpotente, a_1 es no nilpotente y los a_j con $2 \leq j \leq r$ son iguales a 0, es decir, son no unidades; $q(Z) = b_0+b_1Z+b_2Z^2+\cdots+b_sZ^s$, debe cumplir que b_0 sea no nilpotente, b_1 sea igual a 0 y los b_m con $2 \leq m \leq s$ sean iguales a 0, es decir, es una unidad.

Y si $p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r$, cumple que a_0 es no nilpotente, a_1 es igual a 0 y los a_j con $2 \leq j \leq r$ son iguales a 0, es decir, son unidades; $q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s$, debe cumplir que b_0 sea no nilpotente, b_1 sea no nilpotente y los b_m con $2 \leq m \leq s$ sean iguales a 0, es decir, es una no unidad.

Por tanto un polinomio $h(Z) = c_0 + c_1Z$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 y c_1 son no nilpotentes y se cumplen las condiciones dadas.

Afirmación 2.3. Un polinomio $h(Z) = c_0 + c_1Z + c_2Z^2 + \cdots + c_nZ^n$ en $D[Z]$ de grado $n > 0$ es irreducible en $D[Z]$, si existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente.

Se recurre a la inducción sobre el grado de $h(Z)$. Para iniciar se observa que cuando $n = 1$ se tienen tres casos:

1. Sea $h(Z) = c_0 + c_1Z$ donde c_0 y c_1 son nilpotentes. En este caso, se puede expresar un polinomio $h(Z)$ con las condiciones dadas, por ejemplo, $h(Z) = (0, 2) + (0, 4)Z$ como un producto de dos polinomios $p(Z)$ y $q(Z)$ que no son unidades:

   Dado $p(Z) = (0, 2)$ y $q(Z) = (1, 2) + (2, 1)Z$ el producto $p(Z)q(Z)$ es $h(Z)$. Dado $p(Z) = (0, 2)$ y $q(Z) = (1, 2) + (2, 1)Z + (0, 3)Z^2$ el producto $p(Z)q(Z)$ es $h(Z)$.

   Luego es reducible.

2. Sea $h(Z) = c_0 + c_1Z$ donde c_0 y c_1 son no nilpotentes. En este caso de acuerdo a la afirmación 2.2 se tiene que los polinomios que tienen esa forma son irreducibles si cumplen las condiciones dadas.

3. Sea $h(Z) = c_0 + c_1Z$ donde c_0 es nilpotente y c_1 es no nilpotente.

Si $h(Z) = c_0 + c_1Z$ y $h(Z) = p(Z)q(Z)$ con

$$p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r, \quad a_r \neq 0$$
$$q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s, \quad b_s \neq 0$$

de manera que $1 \leq r + s$, entonces se deben buscar las condiciones sobre los coeficientes de $p(Z)$ y $q(Z)$ para que al realizar el producto se obtenga $h(Z)$.

Para que $c_0 = a_0b_0$ sea nilpotente, es necesario que uno de los factores sea nilpotente y el otro no nilpotente.

Si a_0 es nilpotente y b_0 es no nilpotente, entonces para que $c_1 = a_0b_1 + a_1b_0$ sea no nilpotente se dan los siguientes casos:

a_1	b_1
No nilpotente	No nilpotente
No nilpotente	Nilpotente
No nilpotente	0

Y como

$$\begin{aligned} c_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\ &\vdots \\ c_p &= a_0b_p + a_1b_{p-1} + a_2b_{p-2} + \cdots + a_pb_0 \end{aligned}$$

los c_i con $2 \leq i \leq n$ deben ser iguales a 0, entonces si cada producto es cero, $a_1b_1 = 0$, implica que de las opciones mencionadas sólo es posible aquella donde a_1 es no nilpotente y b_1 es 0.

Como se tiene que a_0 es nilpotente y $a_0b_m = 0$ con $2 \leq m \leq s$ entonces los b_m deben ser nilpotentes o iguales a 0. También como b_0 es no nilpotente, los a_j con $2 \leq j \leq r$ deben ser iguales a 0. Pero con esas condiciones no se puede asegurar que los otros productos que se presentan son iguales a 0, pues como a_1 es no nilpotente, para que $a_1b_m = 0$ con $2 \leq m \leq s$, los b_m sólo deben ser iguales a 0.

Entonces $p(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_rZ^r$, debe cumplir que a_0 sea nilpotente, a_1 sea no nilpotente y los a_j con $2 \leq j \leq r$ sean iguales a 0, es decir, son no unidades. Y $q(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_sZ^s$, debe cumplir que b_0 sea no nilpotente y los b_m con $1 \leq m \leq s$ sean iguales a 0, es decir, es una unidad.

Por tanto un polinomio $h(Z) = c_0 + c_1Z$ en $D[Z]$ es irreducible en $D[Z]$, si c_0 es nilpotente y c_1 es no nilpotente y se cumplen las condiciones dadas.

Si para algún número natural $n > 0$, un polinomio $h(Z) = c_0 + c_1Z + c_2Z^2 + \cdots + c_nZ^n$ en $D[Z]$, en el cual existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente, se tiene que $h(Z)$ es irreducible.

Se debe probar que todo polinomio de grado $n + 1$ que cumpla las condiciones es irreducible.

Todo polinomio $p(Z)$ de grado $n + 1$ en $D[Z]$ que satisfaga las condiciones de la afirmación 2.3 es de la forma $p(Z) = x0 + Zh(Z)$ con x_0 nilpotente o $p(Z) = h(Z) + c_{n+1}Z^{n+1}$ con c_{n+1} nilpotente,

pues si $h(Z) = c_0 + c_1Z + c_2Z^2 + \cdots + c_nZ^n$ donde existe un único $1 \leq i \leq n$ tal que c_i es no nilpotente y para todo $0 \leq j \leq n$ con $i \neq j$, c_j es nilpotente, para obtener un polinomio de grado $n + 1$ que cumpla también las condiciones se dan los siguientes casos:

1. Multiplicar $h(Z)$ por el polinomio Z y al polinomio resultante sumarle un elemento x_0 nilpotente en D.
2. Al polinomio $h(Z)$ sumarle el polinomio $c_{n+1}Z^{n+1}$ con c_{n+1} nilpotente en D.
3. Se multiplica el polinomio Z por el polinomio $c - jZ^j + c_{j+1}Z^{j+1} + c_{j+2}Z^{j+2} + \cdots + c_nZ^n$ para algún $j \leq n$ obteniéndose como resultado

$$c_jZ^{j+1} + c_{j+1}Z^{j+2} + c_{j+2}Z^{j+3} + \cdots + c_nZ_{n+1}$$

luego a este polinomio se le suma $c_0+c_1Z+c_2Z^2+\ldots+c_{j-1}Z^{j-1}$ pero hace falta el j-ésimo término por tanto el polinomio de grado $n+1$ queda de la forma:

$$c_0 + c_1Z + c_2Z^2 + \cdots + c_{j-1}Z_{j-1} + qZ^j + c_jZ^{j+1} + c_{j+1}Z^{j+2} + c_{j+2}Z^{j+3} + \cdots + c_nZ^{n+1}$$

para algún q nilpotente.

El caso iii. se reduce al i. si $j = 0$ y se reduce al ii. si $1 \leq j \leq n$, por tanto dado un polinomio $h(Z)$ que cumpla las condiciones sólo existen dos formas diferentes de conseguir un polinomio de grado $n+1$ que también cumpla las condiciones.

Si $p(Z) = x_0 + Zh(Z)$ con x_0 nilpotente, se debe probar que es irreducible. Si $p(Z)$ no es irreducible existen $q(Z) = a_0 + a_1Z + a_2Z^2 + \cdots + a_uZ^u$ y $r(Z) = b_0 + b_1Z + b_2Z^2 + \cdots + b_vZ^v$ tales que $p(Z) = q(Z)r(Z)$ donde $q(Z)$ y $r(Z)$ no son unidades; entonces

$$q(Z)r(Z) = x_0 + Zh(Z)$$

y para que $x_0 = a_0b_0$ sea nilpotente, es necesario que uno de los factores sea nilpotente y el otro no nilpotente o los dos sean nilpotentes.

Si a_0 es nilpotente, b_0 es no nilpotente y existe al menos un b_g para algún número natural $1 \leq g \leq v$ que sea no nilpotente, pues $r(Z)$ no es unidad, para cumplir las condiciones es necesario que sólo uno de los coeficientes del producto sea no nilpotente, entonces puede darse que:

Si b_{i-j} con $1 \leq i-j \leq v < n+1$ es no nilpotente y se elige que $c_{i-1}Z^i$ sea el coeficiente no nilpotente en el producto,

$$\begin{aligned}
c_0 &= a_0b_1 + a_1b_0 \\
c_1 &= a_0b_2 + a_1b_1 + a_2b_0 \\
c_2 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\
&\vdots \\
c_{j-1} &= a_0b_j + a_1b_{j-1} + a_2b_{j-2} + \cdots + a_jb_0 \\
c_j &= a_0b_{j+1} + a_1b_j + a_2b_{j-1} + \cdots + a_jb_1 + a_{j+1}b_0 \\
&\vdots \\
c_{i-1} &= a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_jb_{i-j} + a_{j+1}b_{i-(j+1)} + \cdots + a_ib_0 \\
c_i &= a_0b_{i+1} + a_1b_i + a_2b_{i-1} + \cdots + a_jb_{i+1-j} + \cdots + a_ib_1 + a_{i+1}b_0 \\
&\vdots \\
c_{t-1} &= a_0b_t + a_1b_{t-1} + a_2b_{t-2} + \cdots + a_jb_{t-j} + \cdots + a_tb_0
\end{aligned}$$

entonces es necesario que por lo menos uno de los sumandos sea no nilpotente, por ejemplo a_jb_{i-j}, por tanto a_j debe también ser no nilpotente. Pero si a_j es no nilpotente el producto a_jb_0

sería no nilpotente pues b_0 es no nilpotente y el coeficiente c_{j-1} sería también no nilpotente, lo que contradice la hipótesis.

Otra opción es elegir b_{i-j} con $1\ i-j \leq v < n+1$ no nilpotente y c_{t-1} como el coeficiente no nilpotente en el producto, entonces es necesario que por lo menos uno de los sumandos sea no nilpotente, por ejemplo $a_j b_{t-j}$, por tanto a_j y b_{t-j} deben ser no nilpotentes. Pero si a_j es no nilpotente los productos $a_j b_0$, $a_j b_{i-j}$ serían no nilpotentes y los coeficientes c_{j-1}, c_{i-1} también lo serían, lo que contradice la hipótesis.

Ahora, si a_0 y b_0 son nilpotentes, para cumplir las condiciones es necesario que sólo uno de los coeficientes del producto sea no nilpotente, por ejemplo c_{i-1}:

$$\begin{aligned} c_0 &= a_0b_1 + a_1b_0 \\ c_1 &= a_0b_2 + a_1b_1 + a_2b_0 \end{aligned}$$

$$\begin{aligned} c_2 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\ &\vdots \\ c_{i-2} &= a_0b_{i-1} + a_1b_{i-2} + a_2b_{i-3} + \cdots + a_jb_{i-1-j} + \cdots + a_{i-2}b_1 + a_{i-1}b_0 \\ c_{i-1} &= a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots + a_jb_{i-j} + a_{j+1}b_{i-(j+1)} + \cdots + a_ib_0 \\ c_i &= a_0b_{i+1} + a_1b_i + a_2b_{i-1} + \cdots + a_jb_{i+1-j} + a_{j+1}b_{i-j} + \cdots + a_ib_1 + a_{i+1}b_0 \end{aligned}$$

entonces es necesario que por lo menos uno de los sumandos sea no nilpotente, por ejemplo $a_j b_{i-j}$, por tanto a_j y b_{i-j} deben ser no nilpotentes. Pero puede haber otro sumando, por ejemplo $a_{j+1}b_{i-(j+1)}$, donde a_{j+1} sea nilpotente y $b_{i-(j+1)}$ sea no nilpotente; o a_{j+1} sea no nilpotente y $b_{i-(j+1)}$ sea no nilpotente; o a_{j+1} sea no nilpotente y $b_{i-(j+1)}$ sea nilpotente, que no afecta que c_{i-1} sea no nilpotente pero que si causa que otros coeficientes lo sean, presentándose una contradicción:

Si a_{j+1} es nilpotente y $b_{i-(j+1)}$ es no nilpotente, el producto $a_j b_{i-1-j}$ sería no nilpotente y el coeficiente c_{i-2} sería no nilpotente.

Si a_{j+1} es no nilpotente y $b_{i-(j+1)}$ es no nilpotente, el producto $a_{j+1}b_{i-j}$ sería no nilpotente y el coeficiente c_i sería no nilpotente.

Si a_{j+1} es no nilpotente y $b_{i-(j+1)}$ es nilpotente, el producto $a_{j+1}b_{i-j}$ sería no nilpotente y el coeficiente c_i sería no nilpotente.

Por tanto, el polinomio $p(Z) = x_0 + Zh(Z)$ con x_0 nilpotente, es irreducible.

De manera análoga se obtiene que el polinomio $p(Z) = h(Z) + c_{n+1}Z^{n+1}$ con $c_n + 1$ nilpotente, es irreducible. □

Bibliografía

[1] ALBIS, V. *Temas de aritmética y álgebra*. Bogotá, Universidad Nacional de Colombia. 1984.

[2] BEREZIN, F. *Introduction to Superanalysis*. MPAM 9, Reidel. 1987.

[3] CASTRO, I. *Temas de teoría de cuerpos, teoría de anillos y números algebraicos*. Tomo I. Bogotá, Universidad Nacional de Colombia. 1987.

[4] DUBREIL, P.; DUBREIL - JACOTIN, M. *Lecciones de álgebra moderna*. Barcelona, Reverté. 1965.

[5] FRALEIGH, J. *A first course in abstract algebra*. Sixth edition. New York, Addison - Wesley. 1999.

[6] HERSTEIN, I. Álgebra moderna. México, F. Trillas. 1970.

[7] HILBERT, D. *Fundamentos de la Geometría*. Madrid, Publicaciones del Instituto Jorge Juan de Matemáticas. 1953.

[8] ILSE, D; LEHMANN, I.; SCHULZ, W. *Gruppoide und funktionalgleichungen*. Berlin, VEB Deutscher Verlag der Wissenschaften. 1984.

[9] LENTIN, A.; RIVAUD, J. *Álgebra moderna*. Madrid, Aguilar. 1971.

[10] LUQUE, C. El cálculo: una versión sin el concepto de límite. Bogotá, Universidad Pedagógica Nacional. 1993.

[11] LUQUE, C.; DUQUE, O. *Introducción a las álgebras de Grassmann*, en: Memorias del VII Encuentro de Geometría y sus aplicaciones. Bogotá, Universidad Pedagógica Nacional. pp. 227 - 252. 1996.

[12] PÉREZ, E. Estructuras algebraicas. Notas de Clase. Bogotá, Universidad Pedagógica Nacional. 2003.

[13] YAGLOM, I. A simple non euclidean geometry and its physical basis. New York, Springer - Verlag. 1979.

[14] Sitios Consultados en Internet *http://mathworld.wolfram.com/*