El anillo de los números duales

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

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

Resumen

Se inicia con una presentación de la estructura de $\star$-Álgebra de los números duales; se muestran diferentes representaciones que permiten la definición de potencias racionales de números duales, lo que exige una extensión de su estructura a un anillo de números duales con coeficientes complejos. Seguidamente se estudian la función exponencial dual y la función logaritmo dual que permiten la definición de potencias duales de un número dual; luego se estudian ecuaciones en los números duales haciendo un estudio particular de la ecuación de segundo grado. Finalmente se define una relación de preorden para los números duales que es monótona para la adición y multiplicación y se estudian los subanillos e ideales de los números duales.

1. Operaciones en los números duales

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. [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.

[1] Todos los teoremas que se enuncian sin demostración son consecuencia directa de las definiciones.

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

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

Demostración. Si $z_1, z_2, z_3 \in D$ y $z_2 = (a, b)$, $z_1 = (x, y)$, $z_3 = (u, v)$ con $a \neq 0$:

$$\begin{aligned} z_1 z_2 &= z_3 z_2 \\ (z_1 - z_3) z_2 &= (0, 0) \end{aligned}$$

Donde $(z_1 - z_3) = w = (c, d)$, entonces

$$z_2 w = (ac, ad + bc) = (0, 0)$$

y por definición de igualdad entre números duales se tiene que:

$$ac = 0 \qquad \text{y} \qquad ad + bc = 0$$

como $a \neq 0$ y a, b, c, d son números reales, se obtiene que $c = 0$ y $d = 0$. Entonces

$$z_1 - z_3 = (x - u, y - v) = (0, 0)$$

luego $x = u$, $y = v$ y

$$z_1 = z_3.$$

Si $z_2 = (0, b)$, $z_1 = (x, y)$, $z_3 = (u, v)$, $b \neq 0$, se tiene que:

$$\begin{aligned} z_1 z_2 &= z_3 z_2 \\ (x, y)(0, b) &= (u, v)(0, b) \\ (0, xb) &= (0, ub) \end{aligned}$$

Luego

$$\begin{aligned} xb &= ub \\ x &= u. \end{aligned}$$

Entonces si $z_1 z_2 = z_3 z_2$ y z_2 es nilpotente, sólo se puede asegurar que la primera componente de z_1 es igual a la de z_3.

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

Demostración. Dado un entero positivo m tal que $m(1, 0) = (0, 0)$ implica que $m = 0$.

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

Demostración. La función

$$\begin{aligned} \theta : \mathbb{R} &\longrightarrow D \\ a &\longmapsto (a, 0) \end{aligned}$$

es un homomorfismo inyectivo entre $\mathbb{R}$ y D, ya que

$$\begin{aligned} \theta(a + b) &= (a + b, 0) = (a, 0) + (b, 0) = \theta(a) + \theta(b) \\ \theta(ab) &= (ab, 0) = (a, 0)(b, 0) = \theta(a)\theta(b) \end{aligned}$$

y el núcleo de θ es igual al conjunto cuyo único elemento es 0. Así, $\mathbb{R} \simeq \mathrm{Im}(\theta)$.

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.

Demostración. D es un anillo conmutativo con unidad y la multiplicación por escalar y el producto son compatibles, es decir:

$$a(zw) = (az)w = z(aw) \qquad a \in \mathbb{R}; \qquad z, w \in D.$$

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

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

$$\bar{\ } : D \longrightarrow D$$

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

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

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

Demostración. Dado $z = (a,b)$ y $w = (c,d)$ en D, el producto es

$$zw = (ac, ad + bc),$$

su conjugado es

$$\begin{aligned} \overline{zw} &= (ac, -(ad+bc)) \\ &= (ac, -ad - bc) \end{aligned}$$

y por definición de multiplicación en D y definición de conjugado

$$\begin{aligned} \overline{zw} &= (a,-b)(c,-d) \\ &= \bar{z}\bar{w}. \end{aligned}$$

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

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

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

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

Demostración. Por inducción sobre m. Se verifica para $m = 2$. Si $z = (a, b)$, como consecuencia inmediata del teorema 1.9, se tiene que $\overline{z^2} = (\bar{z})^2$.

Ahora se supone que se cumple para algún $m = k$; es decir que,

$$\overline{z^k} = (\bar{z})^k$$

Se debe probar que

$$\overline{z^{k+1}} = (\bar{z})^{k+1}$$

Pero,

$$\overline{z^{k+1}} = (\overline{z^k \cdot z})$$

por el teorema 1.9

$$= (\overline{z^k} \cdot \bar{z})$$

por la hipótesis de inducción

$$= (\bar{z}^k \cdot \bar{z})$$

y de acuerdo con la definición de potenciación con k un número natural.

$$= (\bar{z})^{k+1}$$

Por lo tanto, la fórmula es válida para todo número natural 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 ($\star$). [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].

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

[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.

Demostración. Las funciones

$$\begin{aligned} L_a : U(D) &\longrightarrow U(D) \\ z &\longmapsto az \end{aligned}$$

y

$$\begin{aligned} R_a : U(D) &\longrightarrow U(D) \\ z &\longmapsto za \end{aligned}$$

son funciones biyectivas en $U(D)$; dicho de otra forma si para todo a y b en $U(D)$, las ecuaciones

$$az = b \qquad\qquad wa = b$$

tienen soluciones únicas[6].

2. División entre números duales

Definición 2.1. 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:

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

que se puede escribir como

$$\frac{z}{w} = \frac{a, b}{(c, d)}\frac{c, -d}{(c, -d)}$$

Teorema 2.1. $U(D)$ tiene estructura de cuasigrupo con la división.

3. Los números duales como espacio seminormado

Teorema 3.1. La función

$$\begin{aligned} \|\ \| : D &\longrightarrow \mathbb{R} \\ z = (a, b) &\longmapsto \|z\| = |a| \end{aligned}$$

define una seminorma[7] en D.

[6]Esta propiedad forma parte de los axiomas de Hilbert para los números reales en HILBERT, D. Fundamentos de la Geometría. Madrid, Publicaciones del Instituto Jorge Juan de Matemáticas. 1953. p.p. 244 - 249.

[7]Rowland, Todd. “Seminorm.” From MathWorld - A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/Seminorm.html

Demostración. Se desprende de las propiedades del valor absoluto de los números reales que para todo z, w en D y c en $\mathbb{R}$, se cumple que:

1. $\|z\| \geq 0$
2. $\|z\| = \|\bar{z}\|$
3. $\|z\bar{z}\| = \|z\|^2$
4. $\|zw\| = \|z\|\|w\|$
5. $\|z + w\| \leq \|z\| + \|w\|$
6. $\|cz\| = |c|\|z\|$

Para todo z un número dual nilpotente, se tiene que $\|z\| = 0$ aunque $z \neq 0$.

Teorema 3.2. La función

$$\begin{aligned} d : D \times D &\longrightarrow \mathbb{R}^+ \cup \{0\} \\ (z, w) &\longmapsto d(z, w) = \|w - z\| = |c - a| \end{aligned}$$

donde $z = (a, b)$, $w = (c, d)$, define una seudométrica[8] en D.

Demostración. Se desprende de las propiedades del valor absoluto de los números reales que para todo z, w en D se cumple que:

1. $d(z, w) \geq 0$
2. $d(z, w) = d(w, z)$
3. $d(z, t) + d(t, w) \geq d(z, w)$.

Si dos números duales z y w tienen igual la primera componente, entonces $d(z, w) = 0$ aunque $z \neq w$.

4. Otras representaciones de los números duales

4.1. Representación matricial

Un número dual puede representarse con una matriz 2×2 con entradas en $\mathbb{R}$, mediante el homomorfismo inyectivo definido por

$$\begin{aligned} \varphi : D &\longrightarrow M_{2\times 2} \\ (a, b) &\longmapsto \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \end{aligned}$$

[8]Barile, Margherita. "Pseudometric." From MathWorld - A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/Pseudometric.html

puesto que

$$\begin{aligned}
\varphi[(a,b)+(c,d)] &= \varphi[(a+c,b+d)] \\
&= \begin{pmatrix} a+c & 0 \\ b+d & a+c \end{pmatrix} \\
&= \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} + \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} \\
&= \varphi[(a,b)] + \varphi[(c,d)]
\end{aligned}$$

y

$$\begin{aligned}
\varphi[(a,b)(c,d)] &= \varphi[(ac, ad+bc)] \\
&= \begin{pmatrix} ac & 0 \\ ad+bc & ac \end{pmatrix} \\
&= \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \begin{pmatrix} c & 0 \\ d & c \end{pmatrix} \\
&= \varphi[(a,b)]\varphi[(c,d)].
\end{aligned}$$

Además es inyectiva ya que el núcleo de φ es igual al conjunto cuyo único elemento es 0.

4.2. Representación polar

También es posible representar un número dual utilizando un análogo a las coordenadas polares del plano complejo, definiendo la noción de circunferencia, ángulo y funciones trigonométricas duales.

Definición 4.1. Una circunferencia dual con centro en $z_0 = (a_0, b_0)$ y radio un número real r es el conjunto de puntos $z = (a, b)$, tales que

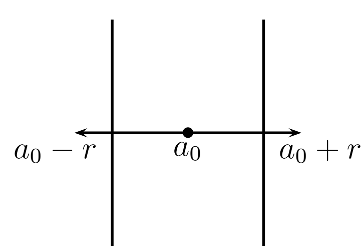
$$\|z - z_0\| = r$$

o sea

$$|a - a_0| = r$$

cuya representación gráfica está dada por dos líneas verticales

$$a = a_0 + r \qquad \text{y} \qquad a = a_0 - r$$



Nótese que toda circunferencia tiene infinitos centros, porque todos los puntos sobre la vertical que contiene a z_0 están a la misma distancia r de los puntos sobre la circunferencia.

Si se piensa en un número dual $z = (a, b)$, no nilpotente, como un *segmento rectilíneo dirigido* o *vector*, desde el origen $(0, 0)$ al punto (a, b), la magnitud dual[9] del vector es su seminorma $\|z\| = |a|$.

Definición 4.2. El *ángulo dual* θ entre el vector y la parte positiva del eje real, que se llamará también *argumento dual* del número es

$$\theta = \frac{b}{|a|}$$

A diferencia de los números complejos, el argumento dual de un número dual $z = (a, b)$ con $a \neq 0$, es único.

Definición 4.3. El *coseno dual* del *ángulo dual* θ es:

$$\text{cosd}\ \theta = \frac{a}{|a|} = \begin{cases} 1 & \text{si } a > 0 \\ -1 & \text{si } a < 0 \end{cases}$$

Definición 4.4. El *seno dual* del *ángulo dual* θ es:

$$\text{send}\ \theta = \frac{b}{|a|} = \theta$$

Definición 4.5. La representación polar de un número dual $z = (a, b)$ no nilpotente es:

$$z = r(\text{cosd}\ \theta + n\text{send}\ \theta)$$

donde $r = |a|$ y

$$\begin{aligned} a &= r\text{cosd}\ \theta \\ b &= r\text{send}\ \theta \end{aligned}$$

z también puede escribirse como:

$$z = re^{n\theta}$$

siempre que

$$e^{n\theta} = \text{cosd}\ \theta + n\text{send}\ \theta$$

esto es equivalente a:

$$\begin{aligned} e^{n\theta} &= 1 + n\theta && \text{si } a > 0 \\ e^{n\theta} &= -1 + n\theta && \text{si } a < 0 \end{aligned}$$

[9] La palabra *magnitud* no significa lo mismo que en geometría euclidiana, se usa por analogía.

Y finalmente, cualquier número dual no nilpotente se representa en forma polar como

$$z = r(\text{cosd}\,\theta + n\text{send}\,\theta)$$

o

$$\begin{aligned} z &= (a,b) = r(1+n\theta) \qquad \text{si } a>0 \\ z &= (a,b) = r(-1+n\theta) \qquad \text{si } a<0. \end{aligned}$$

El significado geométrico de la multiplicación se obtiene de multiplicar

$$z = a + nb \qquad \text{y} \qquad w = c + nd$$

en forma polar, con los siguientes resultados

$$zw = r_1 r_2(1 + n(\theta_1 + \theta_2)) \qquad \text{si } (a > 0 \text{ y } c > 0)$$

o

$$zw = r_1 r_2(1 - n(\theta_1 + \theta_2)) \qquad \text{si } (a < 0 \text{ y } c < 0)$$

o

$$zw = r_1 r_2(-1 - n(\theta_1 - \theta_2)) \qquad \text{si } (a > 0 \text{ y } c < 0)$$

o

$$zw = r_1 r_2(-1 + n(\theta_1 - \theta_2)) \qquad \text{si } (a < 0 \text{ y } c > 0).$$

Un resultado análogo al resultado en los números complejos.

Como la magnitud dual del elemento idéntico de la multiplicación es 1 y su argumento es 0, entonces el inverso multiplicativo de un número dual no nilpotente

$$\begin{aligned} z &= a + nb = r(1+n\theta) \qquad \text{si } a>0 \\ z &= a + nb = r(-1+n\theta) \qquad \text{si } a<0 \end{aligned}$$

es

$$\begin{aligned} z^{-1} &= \frac{1}{r}(1-n\theta) \qquad \text{si } a>0 \\ z^{-1} &= \frac{1}{r}(-1-n\theta) \qquad \text{si } a<0. \end{aligned}$$

Y como el cociente, cuando existe, entre dos números duales $z = a + bn$ y $w = c + dn$ es el producto entre el primero y el inverso multiplicativo del segundo, entonces, si

$$\begin{aligned} z &= r_1(1+n\theta_1) \qquad \text{cuando } a>0 \\ z &= r_1(-1+n\theta_1) \qquad \text{cuando } a<0 \end{aligned}$$

y

$$\begin{aligned} w &= r_2(1 + n\theta_2) && \text{cuando } c > 0 \\ w &= r_2(-1 + n\theta_2) && \text{cuando } c < 0 \end{aligned}$$

se tiene que

$$\frac{z}{w} = \frac{r_1}{r_2}(1 + n(\theta_1 - \theta_2)) \qquad \text{si } (a > 0 \text{ y } c > 0)$$

o

$$\frac{z}{w} = \frac{r_1}{r_2}(1 - n(\theta_1 - \theta_2)) \qquad \text{si } (a < 0 \text{ y } c < 0)$$

o

$$\frac{z}{w} = \frac{r_1}{r_2}(-1 - n(\theta_1 + \theta_2)) \qquad \text{si } (a > 0 \text{ y } c < 0)$$

o

$$\frac{z}{w} = \frac{r_1}{r_2}(-1 + n(\theta_1 + \theta_2)) \qquad \text{si } (a < 0 \text{ y } c > 0)$$

En el caso en que z sea nilpotente no se le asigna una representación polar que tenga la misma forma que en el caso anterior pues tiene magnitud dual igual a 0.

5. Potencias racionales de un número dual

Definición 5.1. Sea z un elemento de D y n un número natural, el elemento nz es:
Si $n = 0$

$$nz = (0, 0)$$

Si $n > 0$

$$(n + 1)z = nz + z$$

Definición 5.2. Sea z un elemento de D y n un número natural, el elemento z^n es:
Si $n = 0$

$$z^n = (1, 0)$$

Si $n > 0$

$$z^{n+1} = z^n z$$

Teorema 5.1 ($\star$). Sea z, w elementos en D y m, n números naturales, se cumple que:

1. $m(z + w) = mz + mw$.
2. $(m + n)z = mz + nz$.
3. $m(nz) = (mn)z$.
4. $(zw)^m = z^m w^m$.
5. $z^{m+n} = z^m z^n$.

6. $(z^m)^n = z^{mn}$.

Teorema 5.2. Las potencias naturales de un número dual cualquiera $z = (a, b)$ están dadas por la fórmula[10]

$$z^k = (a, b)^k = (a^k, ka^{k-1}b).$$

donde $k > 0$ es un número natural.

Demostración. Se recurre a la inducción sobre k. Para iniciar se observa cuando $k = 1$:

$$z^1 = (a, b)^1 = (a, b)$$

y cuando $k = 2$:

$$z^2 = (a, b)^2 = (a, b)(a, b) = (a^2, 2ab).$$

Se supone que la afirmación se cumple para k:

$$z^k = (a, b)^k = (a^k, ka^{k-1}b)$$

y se debe demostrar que se cumple para $k + 1$:

$$z^{k+1} = (a, b)^{k+1}$$

por la definición 5.2

$$z^{k+1} = (a, b)^k(a, b)^1$$

aplicando la hipótesis de inducción y la definición 5.2 se tiene que

$$z^{k+1} = (a^k, ka^{k-1}b)(a, b)$$

por la definición de multiplicación en los números duales y la propiedad distributiva de los números reales

$$\begin{aligned} z^{k+1} &= (a^{k+1}, a^kb + ka^kb) \\ &= (a^{k+1}, (k+1)a^kb). \end{aligned}$$

En representación polar,

$$z = r(1 + n\theta) \qquad \text{con } a > 0$$

o

$$z = r(-1 + n\theta) \qquad \text{con } a < 0$$

entonces

$$z^k = r^k(1 + nk\theta) \qquad \text{cuando } a > 0$$

o

$$zk = rk((-1)^k + n(-1)^{k-1}k\theta) \qquad \text{cuando } a < 0.$$

[10]Un detalle curioso es que la primera componente sólo depende de a y en la segunda componente aparece la derivada de la primera componente, multiplicada por b. Para más información véase LUQUE, C. *El cálculo una versión sin el concepto de límite.* En: Memorias VIII Coloquio Distrital de Matemáticas y Estadística. Bogotá, Universidad Pedagógica Nacional. 1991.

Definición 5.3. Para todo entero positivo m, y todo z en D,

$$-mz = m(-z)$$

Definición 5.4. Para todo entero positivo m, y todo z en D no nilpotente

$$z^{-m} = (z^{-1})^m.$$

Definición 5.5. Dado $z = (a, b)$ no nilpotente, $w = (c, d)$ en D, si $w^k = z$ para cualquier número natural $k > 1$, w se llama una *raíz k-ésima* de z.

Teorema 5.3. Una raíz *k-ésima* de $z = (a, b)$ con $a > 0$, es:

$$w = r^{\frac{1}{k}}\left(1 + n\frac{\theta}{k}\right).$$

Demostración.

$$w^k = \left(r^{\frac{1}{k}}\left(1 + n\frac{\theta}{k}\right)\right)^k$$

Por el teorema 5.1

$$w^k = \left(r^{\frac{1}{k}}\right)^k\left(1 + n\frac{\theta}{k}\right)^k$$

Por la definición de potenciación en los números reales y el teorema 5.2

$$\begin{aligned} w^k &= r\left(1^k + \frac{kn\theta}{k}\right) \\ &= r(1 + n\theta) = z. \end{aligned}$$

Por tanto w es una *raíz k-ésima* de z, que se notará como $z^{\frac{1}{k}}$.

Teorema 5.4. Una raíz *k-ésima* de $z = (a, b)$ con $a < 0$ y k impar, es:

$$z^{\frac{1}{k}} = r^{\frac{1}{k}}\left(-1 + n\frac{\theta}{k}\right)$$

Demostración.

$$\left(z^{\frac{1}{k}}\right) = \left(r^{\frac{1}{k}}\left(-1 + n\frac{\theta}{k}\right)\right)^k$$

Por el teorema 5.1

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}}\right)\left(-1 + \frac{n\theta}{k}\right)^k$$

Por la definición de potenciación en los números reales y el teorema 5.2

$$\begin{aligned}\left(z^{\frac{1}{k}}\right)^k &= r\left((-1)^k + \frac{(-1)^{k-1}kn\theta}{k}\right)\\ &= r((-1)^k + (-1)^{k-1}n\theta)\end{aligned}$$

y como k es impar, entonces

$$\left(z^{\frac{1}{k}}\right)^k = r(-1+n\theta) = z.$$

Cuando k es par, z no tiene raíces k-ésimas, pues según lo anterior:

$$\begin{aligned}\left(z^{\frac{1}{k}}\right)^k &= \left(r^{\frac{1}{k}}\left(-1+n\frac{\theta}{k}\right)\right)^k\\ &= r((-1)^k + (-1)^{k-1}n\theta)\end{aligned}$$

y como k es par

$$= r(1-n\theta) \neq z.$$

Si se quiere encontrar una estructura donde tenga solución el problema, se puede extender el anillo de los números duales de dos maneras naturales:

5.1. El anillo conmutativo con unidad de los números duales con coeficientes complejos

Definición 5.6. El conjunto

$$D[i] = \{(z,w)|z,w \in \mathbb{C}\}$$

donde $\mathbb{C}$ es el conjunto de los números complejos, con la adición definida componente a componente y la multiplicación definida por

$$(z,w)(z',w') = (zz', zw' + wz')$$

se llama el conjunto de los números duales con coeficientes complejos.

Teorema 5.5. $D[i]$ es un anillo conmutativo con unidad $((1,0),(0,0))$.

Teorema 5.6. $D[i]$ es representable como un conjunto de cuaternas ordenadas de números reales:

$$D[i] = \{(a,b,c,d)|a,b,c,d \in \mathbb{R}\}$$

con adición y multiplicación definidas por:

$$\begin{aligned}(a,b,c,d)+(a',b',c',d') &= (a+a', b+b', c+c', d+d')\\ (a,b,c,d)(a',b',c',d') &= (aa'-bb', ab'+ba', ac'-bd'+ca'-db', ad'+bc'+cb'+da')\end{aligned}$$

y con unidad $(1,0,0,0)$.

Teorema 5.7. $D[i]$ es representable como un conjunto

$$D[i] = \{(a + bi + cn + dk) | a, b, c, d \in \mathbb{R}\}$$

con la adición definida por

$$(a + bi + cn + dk) + (a' + b'i + c'n + d'k) = (a + a') + (b + b')i + (c + c')n + (d + d')k$$

y la multiplicación cumple la propiedad distributiva y las siguientes igualdades:

$$\begin{aligned} i^2 &= -1 \\ n^2 &= 0 = k^2 \\ in &= ni = k \end{aligned}$$

Demostración. Sea

$$1 = (1, 0, 0, 0) \qquad i = (0, 1, 0, 0) \qquad n = (0, 0, 1, 0) \qquad k = (0, 0, 0, 1)$$

con esto, cada cuaterna se escribe en la forma:

$$(a, b, c, d) = (a, 0, 0, 0)1 + (b, 0, 0, 0)i + (c, 0, 0, 0)n + (d, 0, 0, 0)k$$

y como el subanillo

$$\{(t, 0, 0, 0) | t \in \mathbb{R}\}$$

es isomorfo con $\mathbb{R}$, el elemento $(a, 0, 0, 0)$ se puede escribir como a.

Teorema 5.8. El conjunto de las cuaternas de la forma $(a, 0, c, 0) = a + cn$ forman un subanillo isomorfo con D.

Teorema 5.9. El conjunto de las cuaternas de la forma $(a, b, 0, 0) = a + bi$ forman un subanillo isomorfo con $\mathbb{C}$.

5.2. El anillo conmutativo con unidad de los complejos con coeficientes duales

Definición 5.7. El conjunto

$$C[n] = \{(z, w) | z, w \in D\}$$

con la adición definida componente a componente y la multiplicación definida por

$$(z, w)(z', w') = (zz' - ww', zw' + wz')$$

se llama el conjunto de los números complejos con coeficientes duales.

Teorema 5.10. $C[n]$ es un anillo conmutativo con unidad $((1, 0), (0, 0))$.

Teorema 5.11. $C[n]$ es representable como un conjunto de cuaternas ordenadas de números reales:

$$C[n] = \{(a,b,c,d)|a,b,c,d \in \mathbb{R}\}$$

con adición y multiplicación definidas por:

$$(a,b,c,d) + (a',b',c',d') = (a+a', b+b', c+c', d+d')$$
$$(a,b,c,d)(a',b',c',d') = (aa'-cc', ba'+ab'-dc'-cd', ac'+ca', ad'+bc'+cb'+da')$$

y con unidad $(1,0,0,0)$.

Teorema 5.12. $C[n]$ es representable como un conjunto

$$C[n] = \{(a+bn+ci+dk)|a,b,c,d \in \mathbb{R}\}$$

con la adición definida por

$$(a+bn+ci+dk) + (a'+b'n+c'i+d'k) = (a+a') + (b+b')n + (c+c')i + (d+d')k$$

y la multiplicación cumple la propiedad distributiva y las siguientes igualdades:

$$i^2 = -1$$
$$n^2 = 0 = k^2$$
$$in = ni = k$$

Demostración. Sea

$$1 = (1,0,0,0) \qquad n = (0,1,0,0) \qquad i = (0,0,1,0) \qquad k = (0,0,0,1)$$

con esto, cada cuaterna se escribe en la forma:

$$(a,b,c,d) = (a,0,0,0)1 + (b,0,0,0)n + (c,0,0,0)i + (d,0,0,0)k$$

y como el subanillo

$$\{(t,0,0,0)|t \in \mathbb{R}\}$$

es isomorfo con $\mathbb{R}$, el elemento $(a,0,0,0)$ se puede escribir como a.

Teorema 5.13. El conjunto de las cuaternas de la forma $(a,0,c,0) = a+ci$ forman un subanillo isomorfo con $\mathbb{C}$.

Teorema 5.14. El conjunto de las cuaternas de la forma $(a,b,0,0) = a+bn$ forman un subanillo isomorfo con D.

Teorema 5.15. Los anillos $D[i]$ y $C[n]$ son isomorfos.

Demostración. La función

$$\begin{aligned} f : D[i] &\longrightarrow C[n] \\ (a,b,c,d) &\longmapsto f(a,b,c,d) = (a,c,b,d) \end{aligned}$$

Es un homomorfismo de anillos pues

$$\begin{aligned} f[(a,b,c,d)+(x,y,u,v)] &= f(a+x,b+y,c+u,d+v) \\ &= (a+x,c+u,b+y,d+v) \\ &= (a,c,b,d)+(x,u,y,v) \\ &= f(a,b,c,d)+f(x,y,u,v). \end{aligned}$$

y

$$\begin{aligned} f[(a,b,c,d)(x,y,u,v)] &= f(ax-by, ay+bx, au-bv+cx-dy, av+bu+cy+dx) \\ &= (ax-by, au-bv+cx-dy, ay+bx, av+bu+cy+dx) \\ &= (a,c,b,d)(x,u,y,v) \\ &= f(a,b,c,d)f(x,y,u,v) \end{aligned}$$

además es inyectiva pues el núcleo de f es igual al conjunto cuyo único elemento es 0 y es sobreyectiva.

Retomando el problema de hallar las raíces k-ésimas de un número dual, se puede escoger uno de los anillos anteriores, por ejemplo $D[i]$.

Teorema 5.16. Una raíz k-ésima de $z=(a,b)$ en $D[i]$ con $a<0$ y k par de la forma $4t+2$, es:

$$z^{\frac{1}{k}} = r^{\frac{1}{k}} i \left(1 - n\frac{\theta}{k}\right).$$

Demostración.

$$\left(z^{\frac{1}{k}}\right)^k = \left(r^{\frac{1}{k}} i \left(1 - n\frac{\theta}{k}\right)\right)^k$$

Por la definición de potenciación en los números complejos y el teorema 5.2

$$\begin{aligned} \left(z^{\frac{1}{k}}\right)^k &= \left(r^{\frac{1}{k}}\right) i^k \left(1 - \frac{n\theta}{k}\right)^k \\ &= ri^k \left(1^k - \frac{kn\theta}{k}\right) \\ &= ri^k(1-n\theta) \end{aligned}$$

como k es de la forma 4t + 2, entonces

$$i^k = -1$$

y por tanto

$$\left(z^{\frac{1}{k}}\right)^k = r(-1 + n\theta) = z.$$

Si w es una raíz cuadrada de z también lo es $-w$, pues en cualquier anillo se cumple que $(-w)^2 = w^2$.

Teorema 5.17. Si w es una raíz k-ésima de z en $D[i]$, entonces αw es una raíz de z, donde α es una raíz k-ésima de la unidad en $\mathbb{C}$.

Teorema 5.18. Una raíz k-ésima de $z = (a, b)$ en $D[i]$ con $a < 0$ y k par de la forma $4t$, con t impar, es:

$$z^{\frac{1}{k}} = r^{\frac{1}{k}}\frac{\sqrt{2}}{2}(1 + i)\left(1 - n\frac{\theta}{k}\right).$$

Demostración.

$$\begin{aligned}\left(z^{\frac{1}{k}}\right)^k &= \left(r^{\frac{1}{k}}\left(\frac{\sqrt{2}}{2}\right)(1 + i)\left(1 - n\frac{\theta}{k}\right)\right)^k \\ &= r^{\frac{k}{k}}\left(\frac{\sqrt{2}}{2}\right)^k(1 + i)^k\left(1 - n\frac{\theta}{k}\right)^k\end{aligned}$$

y como

$$\begin{aligned}\left(\frac{\sqrt{2}}{2}\right)^k(1 + i)^k &= \left(\frac{\sqrt{2}}{2}\right)^k(\sqrt{2})^k\left(\cos\frac{k\pi}{4} + i\operatorname{sen}\frac{k\pi}{4}\right) \\ &= \cos\pi t + i\operatorname{sen}\pi t \\ &= -1\end{aligned}$$

entonces

$$\begin{aligned}\left(z^{\frac{1}{k}}\right)^k &= -r\left(1 - \frac{kn\theta}{k}\right) \\ &= r(-1 + n\theta) = z.\end{aligned}$$

Teorema 5.19. Si z en $D[i]$ es nilpotente[11] $w^k = z$ para todo número natural $k > 1$, no tiene solución.

Demostración. Se supone que existe w tal que $w^k = z$ con z nilpotente, entonces w debe ser nilpotente, porque si no lo fuera w^k no sería nilpotente, y esto contradice la hipótesis. Lo que significa que $w^k = 0$ para todo número natural $k > 1$ y esto también contradice la hipótesis. Por lo tanto no existe w que cumpla la condición.

[11]En D[i] los elementos nilpotentes son de la forma $(0, t)$ con 0 y t números complejos.

Definición 5.8. Para todo número natural k y m, con $m \neq 0$, y todo z en D no nilpotente

$$z^{\frac{k}{m}} = \left(z^{\frac{1}{m}}\right)^k$$

6. Potencias duales de un número dual

Definición 6.1. Para todo $z = (a, b)$ en D,

$$e^z = (ea\text{'}e^a b).$$

Teorema 6.1. Para todo $z = (a, b)$ en D, $ez \neq 0$.

Teorema 6.2. Para todo $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ en D, $e^{z_1} e^{z_2} = e^{z_1 + z_2}$.

Demostración. Por la definición 6.1 se tiene que

$$\begin{aligned} e^{z_1} e^{z_2} &= (e^{a_1}, e^{a_1} b_1)\,(e^{a_1}, e^{a_1} b_2) \\ &= (e^{a_1} e^{a_2}, e^{a_1} e^{a_2} (b_1 + b_2)) \\ &= \left(e^{a_1 + a_2}, e^{a_1 + a_2} (b_1 + b_2)\right) \\ &= e^{z_1 + z_2} \end{aligned}$$

Teorema 6.3. Para todo $z_1 = (a_1, b_1)$, $z_2 = (a_2, b_2)$ en D, $\frac{e^{z_1}}{e^{z_2}} = e^{z_1 - z_2}$.

Teorema 6.4. Para todo $z = (a, b)$ en D y todo número natural k, $(e^z)^k = e^{zk}$.

Demostración. Por la definición 6.1

$$(e^z)^k = (e^a, e^a b)^k$$

por el teorema 5.2

$$\begin{aligned} (e^z)^k &= ((e^a)^k, k(e^a)^{k-1} e^a b) \\ &= (e^{ak}, e^{ak} bk) \end{aligned}$$

y por la definición 6.1

$$(e^z)^k = e^{zk}.$$

Teorema 6.5. Para todo $z = (a, b)$ en D y todo número natural k, $(e^z)^{-k} = e^{-zk}$.

Demostración. Por la definición 5.4

$$(e^z)^{-k} = ((e^z)^{-1})^k$$

Como $(ez)^{-1} = \frac{1}{(e^a)^2}(e^a, -e^a b)$, entonces

$$(ez)^{-k} = \left(\frac{1}{(e^a)^2}(e^a, -e^a b)\right)^k$$

y por los teoremas 5.1 y 5.2

$$\begin{aligned}
(e^z)^{-k} &= \left(\frac{1}{(e^a)^2}\right)^k \big((e^a)^k, -k(e^a)^{k-1}e^a b\big) \\
&= \frac{1}{(e^{2ak}} \big((e^{ak}, -k(e^{ak}b\big) \\
&= \big((e^{-ak}, -(e^{-ak}bk\big) \\
&= e^{-zk}.
\end{aligned}$$

Teorema 6.6. Para todo $z = (a, b)$ en D y todo número natural m, con $m \neq 0$, $(e^z)^{\frac{1}{m}} = e^{\frac{z}{m}}$.

Demostración. Como $e^z = (e^a, e^a b)$

$$(e^z)^{\frac{1}{m}} = (e^a, e^a b)^{\frac{1}{m}}$$

por el teorema 5.3

$$\begin{aligned}
(e^z)^{\frac{1}{m}} &= (e^a)^{\frac{1}{m}}(1, \frac{e^a b}{m e^a}) \\
&= \left(e^{\frac{a}{m}}, e^{\frac{a}{m}}\frac{b}{m}\right) \\
&= e^{\frac{z}{m}}.
\end{aligned}$$

Teorema 6.7. Para todo $z = (a, b)$ en D, $e^{\bar{z}} = \overline{e^z}$.

Teorema 6.8. La función

$$\begin{aligned}
f : D &\longrightarrow D^+ = \{(x, y) \in D : x > 0\} \\
z &\longmapsto f(z) = e^z
\end{aligned}$$

es biyectiva.

Demostración. a) Dado $z = (a, b)$ y $w = (c, d)$ en D, si $e^z = e^w$ entonces $(e^a, e^a b) = (e^c, e^c d)$, por lo tanto $e^a = e^c$ de donde $a = c$ y $b = d$. Luego $z = w$, lo que prueba que f es inyectiva.

b) Dado $z = (a, b)$ con $a > 0$ existe $w = (c, d)$ en D, tal que $e^c = a$ y $e^c d = b$ con $c = \ln a$ y $d = \frac{b}{a}$, lo que prueba que f es sobre.

La función inversa de f permite la siguiente

Definición 6.2. Dado $z = (a, b)$ en $D^+ = \{(x, y) \in D : x > 0\}$ y $w = (c, d)$ en D,

$$\log z = w \qquad \text{si y sólo si } e^w = z.$$

Teorema 6.9. Para todo $z = (a, b)$ en D^+, se cumple que

I. $e^{\log z} = z$

II. $\log(e^z) = z$

Teorema 6.10. Para todo $z = (a, b)$ en D^+,

$$\log z = \left(\ln a, \frac{b}{a}\right).$$

Demostración. Si $\log z = w = (c, d)$ entonces $c = \ln a$ y $d = \frac{b}{a}$ y por lo tanto

$$e^w = \left(e^{\ln a}, e^{\ln a}\frac{b}{a}\right) = (a, b) = z.$$

Teorema 6.11. Para todo z, w en D^+, $\log(zw) = logz + logw$.

Demostración. Dado $q = \log z$ y $r = \log w$ entonces por la definición 6.2 $e^q = z$ y $e^r = w$, luego $zw = eq + r$ y por tanto $q + r = \log(zw)$.

Teorema 6.12. Para todo z, w en D^+, $\log\left(\frac{z}{w}\right) = \log z - \log w$.

Teorema 6.13. Para todo z en D^+ y todo número natural n, $\log(zn) = n \log z$.

Demostración. Sea $z = (a, b)$ en D^+, por el teorema 5.2

$$\begin{aligned}
\log(zn) &= \log(a^n, na^{n-1}b) \\
&= \left(\ln a^n, \frac{na^{n-1}b}{a^n}\right) \\
&= n\left(\ln a, \frac{b}{a}\right) \\
&= n \log z.
\end{aligned}$$

Teorema 6.14. Para todo $z = (a, b)$ en D^+ y todo número natural n,

$$\log\left(z^{\frac{1}{n}}\right) = \frac{1}{n}\log z.$$

Demostración. Como $a>0$, el teorema 5.3 establece que

$$z^{\frac{1}{n}}=\left(a^{\frac{1}{n}},\frac{a^{\frac{1}{n}}b}{na^{n}}\right)$$

luego

$$\begin{aligned}\log\left(z^{\frac{1}{n}}\right)&=\log\left(a^{\frac{1}{n}},\frac{a^{\frac{1}{n}}b}{na}\right)\\&=\left(\ln a^{\frac{1}{n}},\frac{a^{\frac{1}{n}}b}{naa^{\frac{1}{n}}}\right)\\&=\left(\frac{1}{n}\ln a,\frac{b}{na}\right)\\&=\frac{1}{n}\log z.\end{aligned}$$

Teorema 6.15. Para todo $z=(a,b)$ en D^{+}, $\log\bar{z}=\overline{\log z}$.

Definición 6.3. Para todo z en D^{+} y w en D,

$$z^{w}=e^{w\log z}.$$

Teorema 6.16. Para todo z en D^{+} y w, s en D, $z^{w+s}=z^{w}z^{s}$.

Demostración. Por la definición 6.3

$$z^{w+s}=e^{(w+s)\log z}$$

por la propiedad distributiva en D

$$=e^{w\log z+s\log z}$$

por el teorema 6.2

$$=e^{w\log z}e^{s\log z}$$

y por la definición 6.3

$$=z^{w}z^{s}.$$

Teorema 6.17. Para todo z, v en D^{+} y w en D, $(zv)^{w}=z^{w}v^{w}$.

Demostración. Por la definición 6.3

$$(zv)^{w}=e^{w\log(zv)}$$

por el teorema 6.11

$$(zv)^{w}=e^{w(\log z+\log v)}$$

por la propiedad distributiva en D y el teorema 6.2

$$(zv)^{w}=e^{w\log z}e^{wlogv}$$

y por la definición 6.3

$$(zv)^{w}=z^{w}v^{w}.$$

7. Ecuaciones en los números duales

7.1. Ecuaciones de primer grado

Teorema 7.1. La ecuación $az + b = 0$ donde a y b están en D, $a^2 \neq 0$, tiene una única solución.

Demostración. Si se parte de

$$az + b = 0$$

y se suma $(-b)$ a ambos lados de la igualdad, (estabilidad de la igualdad), se obtiene:

$$(az + b) + (-b) = 0 + (-b)$$

al usar las propiedades asociativa de la suma y del inverso aditivo, se llega a

$$az = -b$$

Ahora, como $a^2 \neq 0$ si se multiplica a ambos lados de la igualdad por $\frac{1}{a}$, se consigue,

$$\frac{1}{a}(az) = \frac{1}{a}(-b)$$

Y al aplicar las propiedades asociativa y del elemento idéntico de la multiplicación, se tiene que

$$z = \frac{-b}{a}$$

y ésta es la *única* solución para la ecuación planteada.

7.2. Una ecuación con dos incógnitas

Teorema 7.2. La ecuación $az + bw = c$ donde a, b y c están en D, $a^2 \neq 0$, $b^2 \neq 0$, tiene infinitas soluciones dadas por

$$w = \frac{c - az}{b}.$$

El resultado que se obtiene es, que para cada valor que se elija para z en los números duales, se consigue un valor para w, también dentro de los números duales, siempre que todas las operaciones que se hagan estén definidas; además, no se puede graficar en un solo plano, se *requieren dos planos duales uno para z y otro para w*, variando z como se quiera; por ejemplo, si se tiene la ecuación

$$(-2, 1)z + w = (1, 3)$$

entonces

$$w = (2, -1)z + (1, 3)$$

si notamos $z = (x, y)$

$$\begin{aligned} w &= (2, -1)(x, y) + (1, 3) \\ &= (2x, 2y - x) + (1, 3) \\ &= (2x + 1, 2y - x + 3) \end{aligned}$$

y si se elige z a lo largo de la recta

$$y = x + 3$$

sus imágenes estarán en la recta

$$\begin{aligned} w &= (2x + 1, 2(x + 3) - x + 3) \\ &= (2x + 1, x + 9) \end{aligned}$$

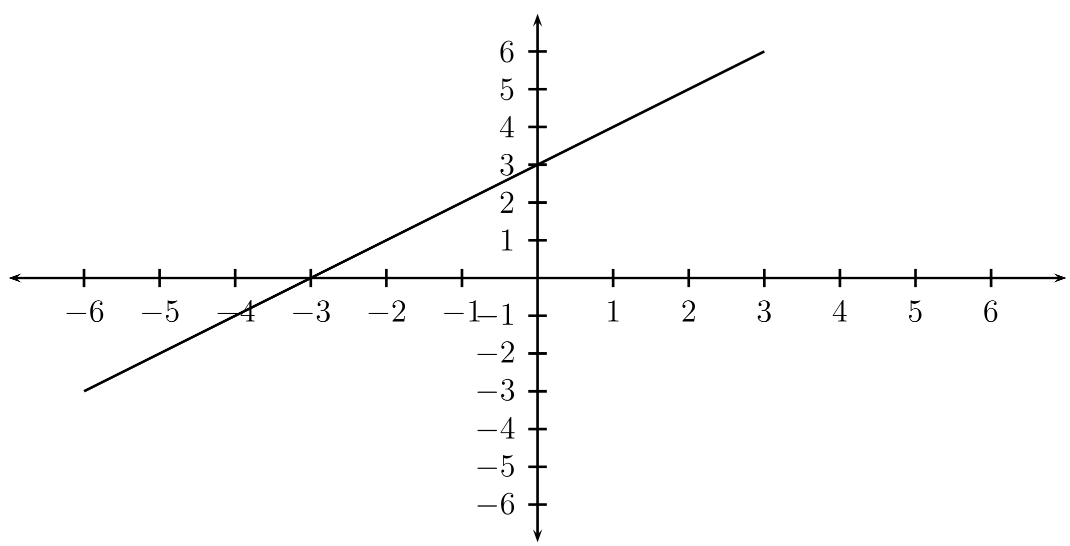
si notamos $w = (u, v)$

$$u = 2x + 1 \qquad \text{y} \qquad v = x + 9$$

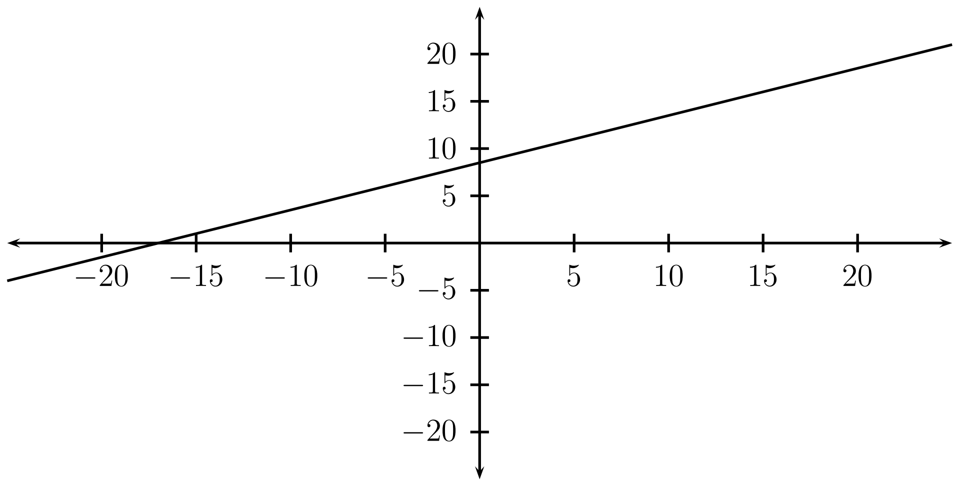
despejando x en términos de u y reemplazando en v se obtiene

$$v = \frac{u + 17}{2}$$

Entonces en el plano z se grafica la recta $y = x + 3$:



Y en el plano w se grafica la recta $v = \frac{u+17}{2}$:



7.3. Ecuaciones de segundo grado

Teorema 7.3. La ecuación $az^2 + bz + c = 0$ donde a, b y c están en $D[i]$ y si se cumple uno de los casos:

I. $a = (a_1, a_2)$, $b = (b_1, b_2)$, y $c = (c_1, c_2)$ son números no nilpotentes y $b_1^2 - 4a_1c_1 \neq 0$

II. a, c son no nilpotentes y b nilpotente

III. a, b son no nilpotentes y c nilpotente

tiene dos soluciones dadas por

$$z_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \qquad \text{y} \qquad z_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Demostración. I. Se parte de la ecuación $az^2 + bz + c = 0$ donde $a = (a_1, a_2)$, $b = (b_1, b_2)$, y $c = (c_1, c_2)$ son números no nilpotentes en $D[i]$ y $b_1^2 - 4a_1c_1 \neq 0$, luego para resolver la ecuación se suma $(-c)$ a ambos lados de la ecuación y se obtiene

$$\begin{aligned}(az^2 + bz + c) + (-c) &= 0 + (-c)\\ az^2 + bz &= (-c)\end{aligned}$$

Como $a^2 \neq 0$, tiene inverso y se multiplica por $\frac{1}{a}$ a ambos lados de la ecuación para conseguir

$$\begin{aligned}\frac{1}{a}\left(az^2 + bz\right) &= \frac{1}{a}(-c)\\ z^2 + \frac{b}{a}z &= -\frac{c}{a}\end{aligned}$$

Ahora se suma $\left(\frac{b}{2a}\right)^2$ a ambos lados de la ecuación, con el propósito de formar un cuadrado perfecto,

$$z^2 + \frac{b}{a}z + \left(\frac{b}{2a}\right)^2 = -\frac{c}{a} + \left(\frac{b}{2a}\right)^2$$

y como

$$z^2 + \frac{b}{a}z + \left(\frac{b}{2a}\right)^2 = \left(z + \frac{b}{2a}\right)^2$$

Al reemplazar en la ecuación, y al utilizar que $\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$, se obtiene que:

$$\begin{aligned}\left(z + \frac{b}{2a}\right)^2 &= -\frac{c}{a} + \left(\frac{b}{2a}\right)^2\\ &= \frac{-4ac + b^2}{4a^2}\\ &= \frac{b^2 - 4ac}{4a^2}\end{aligned}$$

Y al sumar la expresión $\left(-\frac{b^2-4ac}{4a^2}\right)$ a ambos lados de la igualdad,

$$\left(z + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2} = 0$$

Como se tiene que

$$x^2 - y^2 = (x + y)(x - y),$$

$x^2 = t$ significa que $x = \sqrt{t}$, y la definición de radicación

$$\sqrt{4a^2} = 2a$$

se consigue que,

$$\left(z + \frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a}\right)\left(z + \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a}\right) = 0.$$

Como $b_1^2 - 4a_1c_1 \neq 0$, $(b_1^2 - 4ac)^{\frac{1}{2}}$ existe y es no nilpotente, además puesto que $a_1 \neq 0$, $c_1 \neq 0$ entonces $a_1c_1 \neq 0$ y $(b_1^2 - 4ac)^{\frac{1}{2}} \neq b_1$. Luego

$$\frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a} = u \qquad \text{y} \qquad \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a} = v$$

son no nilpotentes. Entonces para que se cumpla que

$$(z + u)(z + v) = 0$$

debe darse que

$$z = -u \qquad \text{y} \qquad z = -v$$

o

$$z + u = h \qquad \text{y} \qquad z = -v$$

o

$$z = -u \qquad \text{y} \qquad z + v = j$$

o

$$z + u = l \qquad \text{y} \qquad z + v = m$$

donde h, j, l y m son elementos nilpotentes en $D[i]$.

Pero para que $-u + h$ sea una raíz de la ecuación $az^2 + bz + c = 0$ es necesario que

$$a(-u + h)^2 + b(-u + h) + c = 0$$
$$a(u^2 - 2uh + h^2) - bu + bh + c = 0$$

y como $au^2 - bu + c = 0$ y $h^2 = 0$ entonces

$$-2auh + bh = 0$$
$$h(-2au + b) = 0$$

y como u, a y b son no nilpotentes, $-2au + b$ es no nilpotente, luego $h = (0, 0)$.

Por tanto las soluciones de la ecuación $az^2 + bz + c = 0$ se reducen a

$$z_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \qquad \text{y} \qquad z_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

II. Se parte de la ecuación $az^2 + bz + c = 0$ donde $a = (a_1, a_2)$, $c = (c_1, c_2)$ son números no nilpotentes y $b = (0, b_2)$ es nilpotente en $D[i]$, luego para resolver la ecuación se realiza el procedimiento anterior hasta obtener que

$$\left(z + \frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a}\right)\left(z + \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a}\right) = 0.$$

Como $b^2 = 0$ y $a^1 \neq 0$, $c_1 \neq 0$ entonces $b^2 - 4ac \neq 0$, por tanto $(b^2 - 4ac)^{\frac{1}{2}}$ existe y es no nilpotente. Luego

$$\frac{b}{2a} - \frac{\sqrt{b^2 - 4ac}}{2a} = u \qquad \text{y} \qquad \frac{b}{2a} + \frac{\sqrt{b^2 - 4ac}}{2a} = v$$

son no nilpotentes. Entonces para que se cumpla que

$$(z + u)(z + v) = 0$$

debe darse que

$$z = -u \qquad \text{y} \qquad z = -v$$

o

$$z+u=h \qquad \text{y} \qquad z=-v$$

o

$$z=-u \qquad \text{y} \qquad z+v=j$$

o

$$z+u=l \qquad \text{y} \qquad z+v=m$$

donde h, j, l y m son elementos nilpotentes en $D[i]$.

Y por la misma razón presentada en el caso anterior, las soluciones de la ecuación $az^2+bz+c=0$ se reducen a

$$z_1 = \frac{-b-\sqrt{b^2-4ac}}{2a} \qquad \text{y} \qquad z_2 = \frac{-b+\sqrt{b^2-4ac}}{2a}.$$

III. Se parte de la ecuación $az^2+bz+c=0$ donde $a=(a_1,a_2)$, $b=(b_1,b_2)$ son números no nilpotentes y $c=(0,c_2)$ es nilpotente en $D[i]$, luego para resolver la ecuación se realiza el procedimiento anterior hasta obtener que

$$\left(z+\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}\right)\left(z+\frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}\right)=0.$$

Como $c_1=0$, entonces $b_1^2-4a_1c_1=b_1^{2\text{o}}not=0$, por tanto $(b^2-4ac)^{\frac{1}{2}}$ existe y es no nilpotente. Luego

$$\frac{b}{2a}-\frac{\sqrt{b^2-4ac}}{2a}=u$$

es nilpotente y

$$\frac{b}{2a}+\frac{\sqrt{b^2-4ac}}{2a}=v$$

es no nilpotente. Entonces para que se cumpla que

$$(z+u)(z+v)=0$$

debe darse que

$$z=-u \qquad \text{y} \qquad z=-v$$

o

$$z+u=h \qquad \text{y} \qquad z=-v$$

o

$$z=-u \qquad \text{y} \qquad z+v=j$$

o

$$z+u=l \qquad \text{y} \qquad z+v=m$$

donde h, j, l y m son elementos nilpotentes en $D[i]$.

Pero para que $-u+h$ sea una raíz de la ecuación $az^2+bz+c=0$ es necesario que

$$a(-u+h)^2+b(-u+h)+c=0$$
$$a(u^2-2uh+h^2)-bu+bh+c=0$$

y como $au^2-bu+c=0$ y $h^2=0$ entonces

$$-2auh+bh=0$$
$$h(-2au+b)=0$$

y puesto que u es nilpotente, $-2au$ es nilpotente, pero como b es no nilpotente, $-2au+b$ es no nilpotente, luego $h=(0,0)$.

Por tanto las soluciones de la ecuación $az^2+bz+c=0$ se reducen a

$$z_1=\frac{-b-\sqrt{b^2-4ac}}{2a} \qquad \text{y} \qquad z_2=\frac{-b+\sqrt{b^2-4ac}}{2a}.$$

Ejemplo
La ecuación

$$(2,3)z^2+(1,2)z+(0,1)=0$$

tiene por soluciones

$$\begin{aligned} z &= \frac{(-1,-2)\pm\sqrt{(1,2)^2-4(2,3)(0,1)}}{2(2,3)} \\ &= \frac{(-1,-2)\pm\sqrt{(1,-4)}}{(4,6)} \end{aligned}$$

lo que significa que las dos raíces son:

$$\begin{aligned} z_1 &= \frac{(-1,-2)+(1,-2)}{(4,6)} = \frac{(0,-4)}{(4,6)} = (0,-4)\left(\frac{1}{4},-\frac{3}{8}\right) = (0,-1) \\ z_2 &= \frac{(-1,-2)-(1,-2)}{(4,6)} = \frac{(-2,0)}{(4,6)} = (-2,0)\left(\frac{1}{4},-\frac{3}{8}\right) = (-\frac{1}{2},\frac{3}{4}) \end{aligned}$$

8. Cuaternios duales

Definición 8.1. El conjunto

$$H_D=\{(a,b,c,d)|a,b,c,d\in\mathbb{R}\}$$

donde $\mathbb{R}$ es el conjunto de los números reales, con la adición y multiplicación definidas por:

$$(a,b,c,d)+(a',b',c',d')=(a+a',b+b',c+c',d+d')$$
$$(a,b,c,d)(a',b',c',d')=(aa',ab'+ba',ac'+ca',ad'+bc'-cb'+da')$$

se llama el conjunto de los números cuaternios duales.

Teorema 8.1. H_D es un anillo conmutativo con unidad[12] $(1,0,0,0)$.

Teorema 8.2. H_D es representable como un conjunto

$$H_D = \{(a+bn+cm+dk)|a,b,c,d \in \mathbb{R}\}$$

con la adición definida por

$$(a+bn+cm+dk)+(a'+b'n+c'm+d'k) = (a+a')+(b+b')n+(c+c')m+(d+d')k$$

Y la multiplicación cumple la propiedad distributiva y las siguientes igualdades:

$$n^2 = m^2 = k^2 = 0$$
$$k = nm = -mn$$

es definida por

$$(a+bn+cm+dk)(a'+b'n+c'm+d'k) = (aa')+(ab'+ba')n+(ac'+ca')m+(ad'+bc'-cb'+da')k.$$

Demostración. Sea

$$1 = (1,0,0,0) \qquad n = (0,1,0,0) \qquad m = (0,0,1,0) \qquad k = (0,0,0,1)$$

con esto, cada cuaterna se escribe en la forma:

$$(a,b,c,d) = (a,0,0,0)1 + (b,0,0,0)n + (c,0,0,0)m + (d,0,0,0)k$$

y como el subanillo

$$\{(t,0,0,0)|t \in \mathbb{R}\}$$

es isomorfo con $\mathbb{R}$, el elemento $(a,0,0,0)$ se puede escribir como a, luego

$$(a,b,c,d) = a+bn+cm+dk.$$

El conjunto de los números cuaternios duales con la adición y la multiplicación *no forman un dominio de integridad*, debido a la existencia de elementos divisores de cero, que corresponden a elementos de la forma $(0,b,c,d)$ para cualquier número real b, c y d.

Teorema 8.3. El elemento inverso multiplicativo de $q = a+bn+cm+dk$, con $a \neq 0$ es

$$q^{-1} = \frac{\bar{q}}{\|q\|^2} = \frac{1}{\|q\|^2}(a-bn-cm-dk)$$

donde se ha definido

$$\bar{q} = a-bn-cm-dk \qquad \text{y} \qquad \|q\|^2 = q\bar{q} = a^2.$$

[12]Realmente forma un *álgebra de Grassmann* pues, junto con su estructura de espacio vectorial, sus elementos generadores: n, m y s anticonmutan. (LUQUE, C., DUQUE, O. *Introducción a las Álgebras de Grassmann*. En las memorias del VII Encuentro de Geometría y sus Aplicaciones. 1996. pp. 227-252).

Teorema 8.4. H_D es representable como un conjunto de matrices 4×4 con entradas en $\mathbb{R}$

$$HD = \left\{ \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

con la adición y multiplicación usual de matrices.

Demostración. Se define la función

$$\begin{aligned} \varphi : H_D &\longrightarrow M_{4\times 4} \\ (a, b, c, d) &\longmapsto \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} \end{aligned}$$

que es un homomorfismo inyectivo puesto que

$$\begin{aligned} \varphi[(a, b, c, d) + (a', b', c', d')] &= \varphi[(a + a', b + b', c + c', d + d')] \\ &= \begin{pmatrix} a + a' & 0 & 0 & 0 \\ c + c' & a + a' & 0 & 0 \\ b + b' & 0 & a + a' & 0 \\ d & b & -(c + c') & a + a' \end{pmatrix} \\ &= \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} + \begin{pmatrix} a' & 0 & 0 & 0 \\ c' & a' & 0 & 0 \\ b' & 0 & a' & 0 \\ d' & b' & -c' & a' \end{pmatrix} \\ &= \varphi[(a, b, c, d)] + \varphi[(a', b', c', d')] \end{aligned}$$

$$\begin{aligned} \varphi[(a, b, c, d)(a', b', c', d')] &= \varphi[(aa', ab' + ba', ac' + ca', ad' + bc' - cb' + da')] \\ &= \begin{pmatrix} aa' & 0 & 0 & 0 \\ ac' + ca' & aa' & 0 & 0 \\ ab' + ba' & 0 & aa' & 0 \\ ad' + da' + bc' - cb' & ab' + ba' & -(ac' + ac') & aa' \end{pmatrix} \\ &= \begin{pmatrix} a & 0 & 0 & 0 \\ c & a & 0 & 0 \\ b & 0 & a & 0 \\ d & b & -c & a \end{pmatrix} \begin{pmatrix} a' & 0 & 0 & 0 \\ c' & a' & 0 & 0 \\ b' & 0 & a' & 0 \\ d' & b' & -c' & a' \end{pmatrix} \\ &= \varphi[(a, b, c, d)]\varphi[(a', b', c', d')]. \end{aligned}$$

Además es inyectiva ya que el núcleo de φ es igual al conjunto cuyo único elemento es 0.

9. Preorden en los números duales

Teorema 9.1. En los números duales no existe un conjunto de números positivos P.

Demostración. Si existiera un conjunto de números positivos P, entonces debe cumplirse que: Si $n \neq 0$, entonces $n \in P$ o $-n \in P$.

Pero, si $n \in P$ entonces $n^2 = 0$ debe pertenecer a P y $0 \notin P$. Y si $-n \in P$, entonces $(-n)^2 = 0$ debe pertenecer a P y $0 \notin P$.

Definición 9.1. Un subconjunto H de D se llamará de números D-Positivos si se cumple:

1. Si a y b pertenecen a H entonces $a + b$ y ab pertenecen a H.
2. Si a es un número dual, se cumple exactamente una de las tres situaciones:

$$a \in H, \ a^2 = 0, \ -a \in H$$

Definición 9.2. Para todo a, b en D,

$$\begin{aligned} a < b & \quad \text{si y solo si} \quad b - a \in H. \\ a > b & \quad \text{si y solo si} \quad b < a \\ ab & \quad \text{si y solo si} \quad a < b \text{ o } a = b \\ ab & \quad \text{si y solo si} \quad a > b \text{ o } a = b \end{aligned}$$

Si $a < 0$ se dice que a es D-Negativo.

Teorema 9.2. La relación $<$ es transitiva.

Demostración. Para todo a, b en D, si $a < b$ y $b < c$ entonces $b - a \in H$ y $c - b \in H$, por tanto su suma $(b - a) + (c - b) \in H$, es decir $c - a \in H$, luego $a < c$.

Teorema 9.3. La relación $\leq$ es un preorden[13] sobre D.

Dos números sobre la misma fibra vertical; es decir, con la primera componente igual, no son comparables.

La relación de preorden $\leq$, permite definir una relación de equivalencia sobre D, cuyas clases son las fibras verticales, es decir, los elementos que no son comparables:

$$a \sim b \text{ si y sólo si } a \text{ y } b \text{ tienen la misma primera componente.}$$

[13] Clarkson, Michael. "Preorder." From MathWorld - A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/Preorder.html

Si a y b son números duales, se cumple exactamente una de las siguientes condiciones:

$$a < b, \ a \sim b, \ b < a$$

Esto se debe a que el número $b - a$ está en una sola de las situaciones:

$$b - a > 0, \text{ ó } (b - a)2 = 0, \text{ ó } b - a < 0$$

Teorema 9.4. (Monotonía de la adición): Dados números duales cualesquiera x, y, z, y w si $x < y$ y $z < w$ entonces[14]:

$$x + z < y + w.$$

Demostración. Si se supone que $x < y$ y $z < w$ entonces $(y - x) \in H$ y $(w - z) \in H$ y su suma

$$(y - x) + (w - z) \in H$$

pero esta suma puede escribirse como

$$(y + w) - (x + z) \in H$$

lo que significa que

$$x + z < y + w.$$

Teorema 9.5. (Monotonía de la multiplicación): Para todo x, y en D y z en H, si $x < y$ entonces $xz < yz$.

Demostración. Si se supone que $x < y$ entonces $(y - x) \in H$. Como z está en H, $z(y - x) \in H$, esto es $(zy - zx) \in H$, lo que significa que $xz < yz$.

Teorema 9.6. Para todo x, y en D y z es D-Negativo, si $x < y$, entonces $xz > yz$.

Teorema 9.7. Para todo x, y, z en D, si $x + z < y + z$ entonces $x < y$.

Un ejemplo de un conjunto de números D-Positivos para los números duales es el conjunto:

$$H = \{(x, y)D : x > 0\}.$$

10. Subanillos de los números duales

Teorema 10.1. Los siguientes subconjuntos de D son subanillos propios:

1. $S_1 = \{(0, b)D : b \in \mathbb{R}\}$ es un anillo conmutativo con elementos nilpotentes.
2. $S_2 = \{(a, 0)D : a \in \mathbb{R}\}$ es un dominio de integridad isomorfo con $\mathbb{R}$.

[14] A pesar de que no todo par de elementos son comparables, si x e y son comparables y z y w también, entonces $x + z$ es comparable con $y + w$.

3. $S_3 = \{(a,b)D : a,b \in \mathbb{Q}\}$ es un anillo conmutativo con unidad y con elementos nilpotentes.

4. $S_4 = \{(a,b)D : a,b \in \mathbb{Z}\}$ es un anillo conmutativo con unidad y con elementos nilpotentes.

5. $S_5 = \{(0,b)D : b \in \mathbb{Q}\}$ es un anillo conmutativo con elementos nilpotentes.

6. $S_6 = \{(0,b)D : b \in \mathbb{Z}\}$ es un anillo conmutativo con elementos nilpotentes.

7. $S_7 = \{(a,0)D : a \in \mathbb{Q}\}$ es un dominio de integridad isomorfo con $\mathbb{Q}$.

8. $S_8 = \{(a,0)D : a \in \mathbb{Z}\}$ es un dominio de integridad isomorfo con $\mathbb{Z}$.

11. Ideales de los números duales

Teorema 11.1. Sea $(0,b)$ en D, el conjunto de todos los elementos nilpotentes

$$\langle (0,b) \rangle = \{x(0,b) : x \in D\}$$

es un ideal principal en D.

Demostración. Si $(0,i)$, $(0,j) \in \langle (0,b) \rangle$ entonces

$$(0,i) - (0,j) = (0,i-j) \in \langle (0,b) \rangle.$$

Y si $(a,c) \in D$ y $(0,j) \in \langle (0,b) \rangle$ entonces

$$(a,c)(0,j) = (0,aj) \in \langle (0,b) \rangle.$$

Al ideal $(0,b)$ se le llamará N.

Teorema 11.2. El ideal anulador de N es N.

Teorema 11.3. Si (x,y) es no nilpotente en D, entonces

$$\langle (x,y) \rangle = \{(z,w)(x,y) : (z,w) \in D\} = D.$$

El anillo D tiene sólo tres ideales que son $\{0\}$, D y N.

Definición 11.1. Un ideal maximal en D es un ideal propio M que no está contenido en un ideal propio estrictamente mayor.

Teorema 11.4 ($\star$). M es un ideal maximal de D si, y sólo si $M \neq D$ e $\langle M, a \rangle = D$ para todo a que no está en M.

Demostración. Se supone que M es un ideal maximal del anillo D y a un elemento que no pertenece a M. Si $\langle M, a\rangle$ es el ideal generado por el conjunto $M \cup \{a\}$, se cumple que $M \subseteq \langle M, a\rangle \subseteq D$. Estas inclusiones implican que si M es ideal maximal, $\langle M, a\rangle = D$.

Ahora se supone que I es un ideal en D tal que $M \subseteq I \subseteq D$, y si a es un elemento de I que no está en M, entonces $M \subseteq \langle M, a\rangle \subseteq I$. Pero como $\langle M, a\rangle = D$ entonces $I = D$ y con esto se concluye que M es un ideal maximal de D.

Teorema 11.5 ($\star$). M es un ideal maximal en D si y sólo si D/M es un campo.

Demostración. Demostración: Se supone que M es un ideal maximal del anillo D, y como D/M es un anillo conmutativo con identidad, se necesita encontrar el inverso multiplicativo de un elemento $a + M$ de D/M, donde $a + M$ es distinto del elemento cero, es decir a no está en M. Como M es maximal, entonces por el teorema 11.4 se tiene que $\langle M, a\rangle = D$ para todo a que no está en M:

$$D = \langle M, a\rangle = \{m + xa | m \in M, x \in D\}.$$

Como 1 está en D, se puede escribir de la forma

$$1 = m' + x'a$$

para determinados m' en M y x' en D, luego $1 - x'a$ está en M, es decir

$$1 + M = x'a + M = (x' + M)(a + M)$$

Con lo que se demuestra que $x' + M$ es el inverso multiplicativo de $a + M$.

Ahora se supone que D/M es un campo y que I es un ideal en D tal que $M \subset I \subseteq D$. Como M es un subconjunto propio de I existe a un elemento de I que no está en M, entonces $a + M$ tiene inverso multiplicativo

$$(a + M)(x + M) = 1$$

para $x + M$ en D/M. Entonces $1 - ax$ está en $M \subset I$ y como ax está en I pues es un ideal, la suma está en I, es decir, 1 está en I, luego $I = D$. Con lo que se demuestra que M es un ideal maximal en D.

Teorema 11.6. El ideal N es un ideal maximal en D.

Teorema 11.7. es isomorfo con $\mathbb{R}$.

Demostración. Se define la función

$$\begin{array}{rcl} \varphi : D/N & \longrightarrow & \mathbb{R} \\ (a, b) + N & \longmapsto & a \end{array}$$

que es un homomorfismo puesto que

$$\begin{aligned}
\varphi[((a,b)+N)+((c,d)+N)] &= \varphi[(a+c,b+d)+N] \\
&= a+c \\
&= \varphi[((a,b)+N)]+\varphi[((c,d)+N)]
\end{aligned}$$

$$\begin{aligned}
\varphi[((a,b)+N)((c,d)+N)] &= [(ac,ad+bc)+N] \\
&= ac \\
&= \varphi[((a,b)+N)]\varphi[((c,d)+N)]
\end{aligned}$$

Además φ es inyectiva pues $N_\varphi = \{N\}$ y φ es sobreyectiva pues dado a en $\mathbb{R}$, existe $(x+y)+N$ en D/N tal que $x=a$ e y es cualesquier número real.

Definición 11.2. Un ideal primo en D es un ideal propio J tal que para todo z y w en D se tiene que si zw está en J entonces z está en J o w está en J.

Teorema 11.8 ($\star$). J es un ideal primo en D si y sólo si D/J es un dominio de integridad.

Demostración. Se supone que J es un ideal primo del anillo D, y como D/J es un anillo conmutativo con identidad, se necesita demostrar que no tiene divisores de cero.

Dados $z+J$ y $w+J$ en D/J, si $(z+J)(w+J)=0+J$ entonces $zw+J=0+J$ lo que significa que $zw-0=zw$ está en J, y como J es un ideal primo, entonces z está en J o w está en J, luego uno de los factores es el elemento cero J en D/J.

Ahora se supone que es un dominio de integridad, luego si zw está en J, entonces $(z+J)(w+J)$ es el elemento cero J en D/J, siempre que $z+J=J$ o $w+J=J$, es decir, z está en J o w está en J.

Teorema 11.9. El ideal N es un ideal primo en D.

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/