Miscelánea Matemática **50** (2009) 77–88 SMM

El teorema fundamental del álgebra sobre los cuaterniones

Ernesto Guerrero, Roger Pacheco y Efrén Pérez*
Facultad de Matemáticas
de la Universidad Autónoma de Yucatán
*jperezt@uady.mx

Resumen

Se enuncian propiedades de los anillos de polinomios oblicuos (skew-polynomial rings) y se clasifican las $I_{\mathbb{H}}-$derivaciones izquierdas de los cuaterniones $\mathbb{H}$. Se prueba que los anillos de polinomios oblicuos sobre $\mathbb{H}$, y que provienen de funciones $\mathbb{R}-$lineales, son equivalentes a $\mathbb{H}[x]$. Se demuestra que sobre dicho anillo se cumple el Teorema Fundamental del Álgebra.

1. Introducción

Los anillos de polinomios oblicuos, o *skew-polynomial rings*, son una generalización muy interesante de los polinomios usuales, la cual fue creada por Ore [9] y Wedderburn [5]. Los autores nos acercamos a este tema ya que, entre otras cosas, dichos polinomios sirven para clasificar los módulos de longitud finita de algunas álgebras de dimensión finita[1].

Tan interesantes nos parecieron dichos polinomios que decidimos escribir este artículo, con el que queremos generar curiosidad por los polinomios oblicuos, explicar por qué bajo condiciones de $\mathbb{R}-$linealidad todo anillo de polinomios oblicuos sobre los cuaterniones, $\mathbb{H}$, es equivalente a $\mathbb{H}[x]$ y probar que en este anillo todo polinomio, que no es cero ni unidad, se factoriza en polinomios de grado 1.

Para lograrlo elegimos la siguiente estructura:

En la sección 2 recordamos qué son los cuaterniones.

En la sección 3 definimos los polinomios oblicuos, utilizando una generalización de los coeficientes binomiales para composición de funciones; por supuesto que aparece el triángulo de Pascal y propiedades que son bien conocidas en las combinatorias usuales.

[1]Proyecto de investigación "Representaciones de álgebras de dimensión finita sobre el campo de los números reales"

A partir de la sección 4 nos restringimos al caso en que el anillo subyacente es un anillo de división. En dicha sección recopilamos herramientas muy bonitas que serán soporte para el resto del texto. Lo más notorio es que hay resultados sobre polinomios oblicuos muy parecidos a aquellos que aprendemos en la licenciatura respecto a polinomios usuales; como por ejemplo que sus ideales, izquierdos y derechos, son principales.

En la sección 5 clasificamos las $I_{\mathbb{H}}-$derivaciones izquierdas; nos extendimos un poco con esa prueba pues es fácil y es indispensable para que limitemos el análisis al anillo de polinomios $\mathbb{H}[x]$.

En la sección 6 probamos el teorema fundamental del álgebra sobre $\mathbb{H}[x]$.

En la sección 7 comentamos un poco acerca de generalizaciones de estos resultados.

2. $\mathbb{H}$ de Hamilton

Podemos considerar a los cuaterniones, denotados por $\mathbb{H}$, como el conjunto de las expresiones formales $a+bi+cj+dk$, donde a, b, c y d son números reales, junto con las siguientes operaciones:

1.- Suma: $(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')\,i+(c+c')\,j+(d+d')\,k$.

2.- Producto: $(a+bi+cj+dk)\,(a'+b'i+c'j+d'k) =$

$(aa'-bb'-cc'-dd')+(ab'+a'b+cd'-c'd)\,i$
$+(ac'+a'c-bd'+b'd)\,j+(ad'+a'd+bc'-b'c)\,k$.

En la segunda fórmula podemos ver las clásicas relaciones $i^2=j^2=k^2=-1$, $ij=k$, $jk=i$, $ki=j$, $ji=-k$, $kj=-i$, $ik=-j$.

Es conocido que $\mathbb{H}$ es un anillo de división no conmutativo, que el centro de $\mathbb{H}$ es $\mathbb{R}$ y que la dimensión de $\mathbb{H}$, como $\mathbb{R}-$espacio vectorial, es 4.

Los cuaterniones fueron descritos por primera vez en 1843 por Sir William Rowan Hamilton, quien buscaba generalizar a los complejos.

Es posible encontrar reediciones de trabajos de Hamilton, como [4], en donde se puede apreciar el comienzo geométrico de los teoremas acerca de los cuaterniones.

3. Polinomios oblicuos, torcidos y diferenciales

Expresemos con más claridad los términos a emplear, comenzando por una definición que nos hace recordar al cálculo diferencial.

En este artículo todo anillo es asociativo y con unitario. Recordemos que si $\tau : R \to R$ es un endomorfismo del anillo R entonces, o es el endomorfismo cero, o manda a 1_R en 1_R.

Definición 3.1 Sean R un anillo y $\tau : R \to R$ un endomorfismo del anillo R. Diremos que una función $\delta : R \to R$ es una $\tau-$*derivación izquierda* si δ es aditiva y además, para cada $r, s \in R$, se cumple que

$$\delta(rs) = \tau(r)\delta(s) + \delta(r)s.$$

Al conjunto de las $\tau-$derivaciones lo vamos a denotar por $\mathrm{Der}(\tau)$.

Definición 3.2 Si $\tau : R \to R$ es un endomorfismo de anillos y $c \in R$, tenemos la $\tau-$*derivación interna* $\delta_{\tau,c}$ dada por $\delta_{\tau,c}(r) = \tau(r)c - cr$.

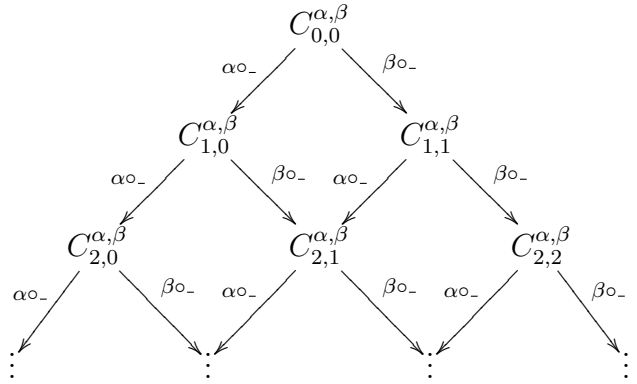
Al conjunto de las $\tau-$derivaciones internas lo denotaremos por $\mathrm{Inder}(\tau)$.

Observación 3.3 $\mathrm{Der}(\tau)$ es un grupo abeliano bajo la suma usual de funciones. Además $\mathrm{Inder}(\tau)$ es un subgrupo de $\mathrm{Der}(\tau)$.

Con estas nociones se construyen los polinomios oblicuos. En los polinomios usuales los coeficientes binomiales $C(n, m)$ son una herramienta estándar y aquí vamos a mostrar una generalización.

Definición 3.4 Sean R un anillo y $\alpha : R \to R$ y $\beta : R \to R$ funciones aditivas. Para $n, m \in \mathbb{N} \cup \{0\}$ con $n \geq m$ definimos $C^{\alpha,\beta}_{n,m} : R \to R$ como la suma de todas las formas de componer m funciones β con $n - m$ funciones α; por ejemplo $C^{\alpha,\beta}_{2,1} = \alpha \circ \beta + \beta \circ \alpha$, mientras que $C^{\alpha,\beta}_{3,1} = \alpha^2 \circ \beta + \alpha \circ \beta \circ \alpha + \beta \circ \alpha^2$. Por comodidad definimos $C^{\alpha,\beta}_{0,0} = I_R$ (identidad en R) y, cuando $n < m$, $C^{\alpha,\beta}_{n,m} = 0$.

Esta idea nos permite desarrollar el correspondiente triángulo de Pascal:



donde las flechas indican composición y cada nodo es la suma de las composiciones que indican las flechas.

Proposición 3.5 *Sean R un anillo y $\alpha : R \to R$ y $\beta : R \to R$ funciones aditivas. Entonces, para $n, m, a \in \mathbb{N} \cup \{0\}$ se cumple lo siguiente:*

a) $C_{n,m}^{\alpha,\beta}$ *tiene* $C(n,m)$ *sumandos.*

b) $\beta \circ C_{n,m}^{\alpha,\beta} + \alpha \circ C_{n,m+1}^{\alpha,\beta} = C_{n+1,m+1}^{\alpha,\beta}$.

c) $C_{n+a,m}^{\alpha,\beta} = \sum_{i=0}^{m} C_{n,i}^{\alpha,\beta} \circ C_{a,m-i}^{\alpha,\beta}$.

d) Si β es un endomorfismo de anillos y α es una $\beta-$derivación izquierda entonces, para $r, s \in R$, tenemos que $C_{n,m}^{\alpha,\beta}(rs) = \sum_{j=m}^{n} C_{n,j}^{\alpha,\beta}(r)\, C_{j,m}^{\alpha,\beta}(s)$.

Comentario acerca de la demostración: (a), (b) y (c) pueden ser obtenidos casi directamente de las definiciones.

Para el inciso (d), los casos $C_{1,0}^{\alpha,\beta}$ y $C_{m,m}^{\alpha,\beta}$ con $m \in \mathbb{N} \cup \{0\}$ son claros, luego usamos el inciso (b) para probar por inducción sobre n que la afirmación es cierta para $C_{n,m}^{\alpha,\beta}$.

Algo se ha trabajado, pero la siguiente definición vale la pena.

Definición 3.6 Sean R un anillo, $\tau : R \to R$ un endomorfismo de anillos y $\delta : R \to R$ una $\tau-$derivación izquierda. El *anillo de polinomios oblicuos* $R[x; \tau, \delta]$ es el $R-$módulo izquierdo de las expresiones formales

$$r_0 + r_1 x + r_2 x^2 + ... + r_m x^m$$

donde $r_i \in R$ y $m \in \mathbb{N} \cup \{0\}$, junto con la multiplicación que se obtiene de extender linealmente a

$$x^n r = \sum_{i=0}^{n} C_{n,i}^{\delta,\tau}(r) x^i \qquad (1)$$

A $R[x;\tau,0]$ se le llama también *anillo de polinomios torcidos* (twisted polynomial ring), mientras que a $R[x;I_R,\delta]$ se le conoce como un *anillo de polinomios diferenciales* (differential polynomial ring).

Observación 3.7 Notemos que la fórmula (1) proviene de la aplicación sucesiva de la identidad $xr = \tau(r)x + \delta(r)$; cuando $\delta = 0$ se obtiene la multiplicación por la derecha girando o torciendo (twisting) a la izquierda vía τ. Cuando $\delta \neq 0$ podemos imaginar la multiplicación a la derecha como "girar a la izquierda y bajar un grado", lo que es un movimiento oblicuo (skew).

Proposición 3.8 *Sean R un anillo, $\tau : R \to R$ un endomorfismo de anillos y $\delta : R \to R$ una $\tau-$derivación izquierda, entonces $R[x;\tau,\delta]$ es un anillo.*

Bosquejo de demostración: La prueba es larga, pero etapas importantes de la misma son las identidades $x^n(x^m r) = x^{n+m}r$, la cual se demuestra utilizando el inciso (c) de 3.5, y $(xr)(x^n s) = x(rx^n s)$, para la cual se usa el inciso (d) de 3.5. □

Veamos cómo lucen estas ideas en situaciones concretas:

Ejemplo 3.9 La identidad $I_{\mathbb{H}} : \mathbb{H} \to \mathbb{H}$ es un automorfismo y la función cero en los cuaterniones es una $I_{\mathbb{H}}-$derivación izquierda, luego $\mathbb{H}[x;I_{\mathbb{H}},0]$ es un anillo de polinomios oblicuos, que al mismo tiempo es de polinomios torcidos y de polinomios diferenciales. Debido a que en este caso la multiplicación es igual que la de los polinomios usuales, en lo sucesivo denotaremos $\mathbb{H}[x;I_{\mathbb{H}},0] = \mathbb{H}[x]$.

Ejemplo 3.10 En los complejos $\mathbb{C}$ tenemos el clásico $\mathbb{R}-$automorfismo dado por la conjugación $\tau(a+bi) = a - bi = \overline{a+bi}$; luego en $\mathbb{C}[x;\tau,0]$ se tiene para cada $\lambda \in \mathbb{C}$ que $x^n\lambda = \overline{\lambda}x^n$ si n es impar y que $x^n\lambda = \lambda x^n$ si n es par, por lo que es sencillo multiplicar polinomios:

$$\left(\sum_{i=0}^{n} \lambda_i x^i\right)\left(\sum_{j=0}^{m} \mu_j x^j\right) = \sum_{u=0}^{n+m}\left(\sum_{t=0}^{u} \lambda_t \tau^t(\mu_{u-t})\right)x^u.$$

Debemos notar que para toda $\mu \in \mathbb{C}$ se cumple que $\delta : \mathbb{C} \to \mathbb{C}$, dada por $\delta(a+ib) = \mu b$, es una $\tau-$derivación izquierda.

Ejemplo 3.11 Consideramos el automorfismo identidad $I_{\mathbb{H}} : \mathbb{H} \to \mathbb{H}$ y la $I_{\mathbb{H}}-$derivación izquierda dada por $\delta(a+bi+cj+dk) = dj - ck$, para obtener el anillo $\mathbb{H}[x;I_{\mathbb{H}},\delta]$. Es sencillo verificar, para $h \in \mathbb{H}$ la identidad

$$x^n h = \sum_{i=0}^{n} C_{n,i}^{\delta,\tau}(h)x^i = \sum_{i=0}^{n} C(n,i)\delta^{n-i}(h)x^i.$$

Además, para $m, n \in \mathbb{N}$ y $m \equiv n \bmod(4)$ se cumple que $\delta^m = \delta^n$.

4. Polinomios oblicuos sobre anillos de división

De ahora en adelante D es un anillo de división, $\tau : D \to D$ es un automorfismo (endomorfismo de anillos biyectivo), δ una $\tau-$derivación izquierda y $D[x;\tau,\delta]$ el correspondiente anillo de polinomios oblicuos. En este contexto hay propiedades interesantes, algunas de las cuales enunciaremos a continuación y que son muy parecidas a las de los polinomios usuales:

Teorema 4.1 *Sea* $S = D[x;\tau,\delta]$.

a) S no tiene divisores de cero.

b) Para $\sum_{i=0}^{m} d_i x^m = f \in S$, *con* $d_m \neq 0$, *definimos* $\operatorname{grad}(f) = m$, *mientras que el polinomio cero tiene grado igual a* $-\infty$; *entonces para cualesquiera* $f, g \in S$ *se tiene que* $\operatorname{grad}(fg) = \operatorname{grad}(f)+\operatorname{grad}(g)$.

c) En S se cumple el algoritmo de la división por la izquierda, es decir que si $f \in S$ *y* $g \in S - \{0\}$ *entonces existen únicos* $q, r \in S$ *tales que* $f = qg + r$ *con* $r = 0$ *o* $\operatorname{grad}(r) < \operatorname{grad}(g)$.

d) Si L es un ideal izquierdo de S entonces es un ideal principal, es decir que hay al menos un elemento $g \in S$ *tal que* $L = Sg$; *en otras palabras, S es un dominio de ideales izquierdos principales.*

e) En S se cumple el algoritmo de la división por la derecha, es decir que si $f \in S$ *y* $g \in S - \{0\}$ *entonces existen únicos* $q, r \in S$ *tales que* $f = gq + r$ *con* $r = 0$ *o* $\operatorname{grad}(r) < \operatorname{grad}(g)$.

f) Si J es un ideal derecho de S entonces es un ideal principal, es decir que hay al menos un elemento $g \in S$ *tal que* $L = gS$; *en otras palabras, S es un dominio de ideales derechos principales.*

Para la prueba remitimos al lector a [5].

En los polinomios usuales es clásica la técnica de cambiar de variable; también funciona en este tipo de polinomios oblicuos:

Proposición 4.2 *Sean* $D[x;\tau,\delta]$, $b \in D - \{0\}$, $c \in D$ *e* $y = bx + c$; *entonces todo elemento de* $D[x;\tau,\delta]$ *se puede escribir de manera única como un polinomio sobre* y. *Más aún, este cambio de variable determina un automorfismo* $\tau' : D \to D$ *dado por* $\tau'(d) = b\tau(d)b^{-1}$, *así como una* $\tau'-$*derivación izquierda* $\delta' : D \to D$ *dada por* $\delta'(d) = b\delta(d) + cd - b\tau(d)b^{-1}c$. *En particular*

$$D[x;\tau,\delta] = D[y;\tau',\delta'].$$

Bosquejo de demostración: En 3.7 se comentó que la forma de multiplicar polinomios queda determinada por el resultado de multiplicar escalares por la derecha, así que es suficiente con que calculemos yd : de la fórmula (1) obtenemos que $xd = \tau(d)\,x + \delta(d)$, luego

$$\begin{aligned} yd &= (bx + c)\,d \\ &= b\tau(d)x + b\delta(d) + cd \\ &= b\tau(d)b^{-1}bx + b\delta(d) + cd \\ &= b\tau(d)b^{-1}(bx + c) - b\tau(d)b^{-1}c + b\delta(d) + cd \\ &= (b\tau(d)b^{-1})\,y + b\delta(d) + cd - b\tau(d)b^{-1}c \end{aligned}$$

Dejamos al lector verificar el resto de las afirmaciones. □

Definición 4.3 Para cada $b \in D$ hay un automorfismo $\sigma_b(d) : D \to D$ dado por $\sigma_b = bdb^{-1}$; a este tipo de automorfismos se les llama *automorfismos internos.*

Proposición 4.4 *Todos los automorfismos* $\mathbb{R}-$*lineales de* $\mathbb{H}$ *son internos.*

Este resultado es bien conocido, pero el lector interesado puede encontrar una prueba con un mínimo de herramientas en el escrito [1].

Corolario 4.5 *Si* τ *es* $\mathbb{R}-$*lineal entonces* $\mathbb{H}[x;\tau,\delta]$ *es igual a* $\mathbb{H}[y; I_{\mathbb{H}}, \delta']$ *vía un cambio de variable.*

Demostración: Por 4.4 sabemos que $\tau = \sigma_b$ para algún $b \in D$; luego, como ya vimos en 4.2, el cambio de variable $y = b^{-1}x$ nos deja con $\tau' = I_{\mathbb{H}}$. □

Ejemplo 4.6 Como en el ejemplo 3.10 sea $\mathbb{C}[x;\tau,\delta]$, donde τ es la conjugación y $\delta(\lambda) = \mu\mathrm{Im}(\lambda)$; [2] entonces, mediante el cambio de variable $y = x + \frac{i}{2}\mu$ y usando 4.2 obtenemos que

$$\mathbb{C}[x;\tau,\delta] = \mathbb{C}[y;\tau,0].$$

[2] $\mathrm{Im}(\lambda)$ es la parte imaginaria de λ.

5. Las $I_{\mathbb{H}}-$derivaciones izquierdas $\mathbb{R}-$lineales son internas

En 4.5 vimos como en $\mathbb{H}[x;\tau,\delta]$ podemos simplificar a τ; ahora queremos eliminar a δ.

Observación 5.1 Si $\delta : D \to D$ es una $\tau-$derivación izquierda entonces $\delta(1) = \delta(1\cdot 1) = \tau(1)\delta(1) + \delta(1)1 = 1\delta(1) + \delta(1)1$ nos lleva a que $\delta(1) = 0$. Entonces, si F es un subcampo de D y δ es $F-$lineal, tendremos para cada $z \in F$ que $\delta(z) = z\delta(1) = 0$. También es cierto que si $\delta(z) = 0$ entonces $\delta(dz) = \delta(d)z$.

Teorema 5.2 *Sean $\tau : \mathbb{H} \to \mathbb{H}$ un automorfismo que fija a $\mathbb{R}$ y δ_1 una $\tau-$derivación izquierda que es $\mathbb{R}-$lineal; entonces hay un cambio de variable $y = bx + u$ tal que*

$$\mathbb{H}[x;\tau,\delta_1] = \mathbb{H}[y;I_{\mathbb{H}},0].$$

Demostración: Por 4.5 hay un cambio de variable $x' = bx$ tal que $\mathbb{H}[x;\tau,\delta_1] = \mathbb{H}[x';I_{\mathbb{H}},\delta]$.

Por 4.2 δ es $\mathbb{R}-$lineal, así que es suficiente con conocer $\delta(i)$, $\delta(j)$ y $\delta(k)$ para poder determinar $\delta(h)$ para cualquier $h \in \mathbb{H}$. Note que la $\mathbb{R}-$linealidad de δ implica que $\delta(\mathbb{R}) = \{0\}$.

Supongamos que $w \in \{i,j,k\}$ y denotemos

$$\delta(w) = a_w + b_w i + c_w j + d_w k. \tag{1}$$

Dado que $w^2 = -1$ se sigue que $0 = \delta(-1) = \delta(ww) = w\delta(w) + \delta(w)w$, por lo tanto

$$w\delta(w) = -\delta(w)w.$$

Luego, si $w = i$ entonces $i\delta(i) = -\delta(i)i$, lo que con la notación de la ecuación 4.1 es equivalente a que $a_i i - b_i + c_i k - d_i j = -a_i i + b_i + c_i k - d_i j$, así que $a_i = b_i = 0$ y $\delta(i) = c_i j + d_i k$.

Del mismo modo se verifica que $\delta(j) = b_j i + d_j k$ y que $\delta(k) = b_k i + c_k j$.

Combinando estos resultados se tienen las identidades

$$\begin{aligned} \delta(ij) &= i\delta(j) + \delta(i)j \\ \delta(k) &= i(b_j i + d_j k) + (c_i j + d_i k)j \\ b_k i + c_k j &= -b_j - d_j j - c_i - d_i i \end{aligned}$$

y por lo tanto $b_j = -c_i$, $b_k = -d_i$ y $c_k = -d_j$. De $jk = i$ y $ki = j$ obtenemos identidades similares, por lo que podemos afirmar que

$$\delta(i) = c_i j + d_i k, \qquad \delta(j) = -c_i i + d_j k \quad \text{y} \quad \delta(k) = -d_i i - d_j j.$$

Ahora sea $u = -\frac{d_j}{2} i + \frac{d_i}{2} j - \frac{c_i}{2} k$; es fácil verificar que

$$\begin{aligned} iu - ui &= i\left(-\frac{d_j}{2} i + \frac{d_i}{2} j - \frac{c_i}{2} k\right) - \left(-\frac{d_j}{2} i + \frac{d_i}{2} j - \frac{c_i}{2} k\right) i \\ &= \frac{d_j}{2} + \frac{d_i}{2} k + \frac{c_i}{2} j - \frac{d_j}{2} + \frac{d_i}{2} k + \frac{c_i}{2} j \\ &= d_i k + c_i j = \delta(i). \end{aligned}$$

Similarmente se verifica que $ju - uj = \delta(j)$ y $ku - uk = \delta(k)$. Luego $\delta(h) = hu - uh$, es decir que δ es la $I_{\mathbb{H}}-$derivación interna $\delta_{I_{\mathbb{H}},u}$. Mediante el cambio de variable $y = x' + u$ se tiene por 4.2 que $\delta' = \delta - \delta_{I_{\mathbb{H}},u} = 0$. □

6. Factorizando en polinomios lineales

Recordemos que $\mathbb{H}[x; I_{\mathbb{H}}, 0]$ lo denotamos por $\mathbb{H}[x]$.

En los polinomios oblicuos puede haber más formas de factorizar de las que estamos acostumbrados a ver en los polinomios usuales, por ejemplo, en $\mathbb{H}[x]$ se tiene que $x^2 + 1 = (x + q)(x - q)$, donde $q = bi + cj + dk$ y $b^2 + c^2 + d^2 = 1$. Esta conducta sin embargo no nos aleja demasiado de definiciones y resultados clásicos, como veremos a continuación.

Definición 6.1 Un elemento $p \in D[x; \tau, \delta]$ es irreducible si no es una unidad y si además $p = qt$ implica que q es unidad o que t es unidad.

Definición 6.2 Sea $S = D[x; \tau, \delta]$. Los elementos irreducibles p y q en S son *similares* si $S/Sp \cong S/Sq$ como $S-$módulos izquierdos.

Proposición 6.3 *La relación similitud es una relación de equivalencia y p es similar a q si y sólo si $S/pS \cong S/qS$ como $S-$módulos derechos.*

Observación 6.4 Sea $S = \mathbb{H}[x]$, entonces un isomorfismo de $S-$módulos $S/Sp \cong S/Sq$ también es un isomorfismo de $\mathbb{R}-$espacios vectoriales, luego deben de tener la misma dimensión. Por otro lado, no es difícil ver que $\dim_{\mathbb{R}}(S/Sp) = 4$ si y sólo si $\text{grad}(p) = 1$.

El siguiente resultado es el teorema 1.2.9 de [5].

Teorema 6.5 *(Análogo del Teorema Fundamental de la Aritmética) Sea* $g \in D[x;\tau,\delta] - \{0\}$; *entonces* g *tiene al menos una factorización en irreducibles* $g = p_1...p_m$, *la cual es única salvo orden y similitud: si* $g = q_1...q_n$ *es otra factorización en irreducibles entonces* $n = m$ *y hay una biyección* $\alpha : \{1,...,n\} \to \{1,...,n\}$ *tal que* p_i *es similar a* $q_{\alpha(i)}$.

Vamos a usar un simpático truco, el cual consiste en "aumentar el grado" para poder aplicar el Teorema Fundamental del Álgebra en los complejos.

Proposición 6.6 *Sea* $g \in \mathbb{H}[x]$ *tal que* $\text{grad}(g) \geq 1$; *entonces hay algún* $q \in \mathbb{H}[x]$ *tal que* gq *es un polinomio con coeficientes reales.*

Demostración: Sea $n = \text{grad}(g)$. Para cada $i \in \{0,1,...,4n\}$ tenemos, por 4.1 inciso (e), que $x^i = gq_i + r_i$ con $r_i = 0$ o $\text{grad}(r_i) < n$. Si hay alguna i tal que $r_i = 0$ entonces se ha cumplido el enunciado, en caso contrario, notemos que hay $4n+1$ remanentes r_i, mientras que la dimensión sobre los reales de los polinomios de $\mathbb{H}[x; I_{\mathbb{H}}, 0]$ con grado menor que n es precisamente $4n$. Esto significa que hay coeficientes reales c_i tales que $\sum_{i=0}^{4n} c_i r_i = 0$, por lo que

$$\sum_{i=0}^{4n} c_i x^i = g\left(\sum_{i=0}^{4n} c_i q_i\right)$$

□

Corolario 6.7 *Sea* $g \in \mathbb{H}[x]$ *tal que* $\text{grad}(g) \geq 1$; *entonces* g *se puede factorizar en polinomios lineales; en otras palabras se cumple el Teorema Fundamental del Álgebra. Además, todo polinomio irreducible es similar a un polinomio de la forma* $x - \lambda$, *con* λ *en los complejos.*

Demostración: Por 6.6 existe $q \in \mathbb{H}[x]$ tal que $gq \in \mathbb{R}[x]$, luego, por el Teorema Fundamental del Álgebra en los complejos, podemos factorizar $gq = (x-\mu_1)\cdots(x-\mu_m)$, donde cada μ_i es un complejo. Aplicando 6.5 se sigue que si p es un irreducible que divide a g entonces es similar a algún $x - \mu_i$. Por 6.4 p es de grado 1. □

7. Comentarios finales

Tal vez el lector se pregunte por nuestra insistencia en usar funciones $\mathbb{R}-$lineales en $\mathbb{H}[x;\tau,\delta]$, pero es que sin esa condición se incrementan las posibilidades: si bien una $I_{\mathbb{R}}-$derivación izquierda anula a los racionales $\mathbb{Q}$, el resto es muy "flexible", pues para cada elemento $r \in \mathbb{R}-\mathbb{Q}$ es posible construir alguna $I_{\mathbb{R}}-$derivación izquierda η tal que $\eta(r) \neq 0$. Más aún, si η es una $I_{\mathbb{R}}-$derivación izquierda entonces $\delta : \mathbb{H} \to \mathbb{H}$ dada por $\delta(a+bi+cj+dk) = \eta(a)+\eta(b)i+\eta(c)j+\eta(d)k$ es una $I_{\mathbb{H}}-$derivación izquierda; así que hay una infinidad no numerable de $I_{\mathbb{H}}-$derivaciones izquierdas que no son $\mathbb{R}-$lineales.

Las afirmaciones previas no son difíciles de probar y el lector puede encontrarlas demostradas con detalle en [10].

También queremos comentar que 6.7, en términos de la existencia de raíces, es conocido desde los tiempos de la segunda guerra mundial (ver [2] o [7]), aunque casos particulares ya habían sido demostrados por el creador de los cuaterniones (pp. 277-292 de [4]). En la literatura actual, como por ejemplo 16.14 y 16.15 de [6], puede uno encontrar versiones del Teorema Fundamental del Álgebra para anillos que son generalizaciones de los cuaterniones.

Referencias

[1] A. Can, E. Guerrero, E. Pérez, *Automorfismos de* $\mathbb{H}$, por aparecer en Eureka.

[2] S. Eilenberg, I. Niven, *The Fundamental Theorem of Algebra for Quaternions*, Bull. Amer. Math. Soc., Vol. 50, pp. 246-248, 1944.

[3] K. R. Goodearl, R. B. Warfield, Jr. An Introduction to Noncommutative Noetherian Rings, 2nd edition, London Mathematical Society, Student Texts 61, Cambridge Universtity Press, 2004.

[4] Sir W. R. Hamilton. Quaternions, third edition, Vol. I, Chelsea Publishing Company, 1969.

[5] N. Jacobson. Finite-Dimensional Division Algebras over Fields, Springer-Verlag, 1996.

[6] T. Lam. A First Course in Noncommutative Rings, 2dn ed., Springer-Verlag, 2001.

[7] M. Leum, M. F. Smiley, *A Matric Proof of the Fundamental Theorem of Algebra for Real Quaternions*, The American Mathematical Monthly, Vol. 60, No. 2, pp. 99 -100, Feb 1953.

[8] J. C. McConnell, J. C. Robson. Noncommutative Noetherian Rings, Graduate Studies in Mathematics, Vol. 30, American Mathematical Society, 2001.

[9] O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc., Vol. 35, No. 3 (1933), pp. 559-584.

[10] Roger Benito Pacheco Castro, Tesis de licenciatura *Polinomios Torcidos y Representaciones de Álgebras de Dimensión Finita Sobre los Números Reales*, Facultad de Matemáticas de la Universidad Autónoma de Yucatán, 29 de mayo del 2009.