**Trabajo final de grado**

**GRADO DE MATEMÁTICAS**

**Facultad de Matemáticas**
**Universidad de Barcelona**

---

# Cuaterniones y octoniones

---

**Verónica Pericacho Allende**

Director: Ricardo García López
Realizado en: Departamento de Álgebra y Geometría. UB

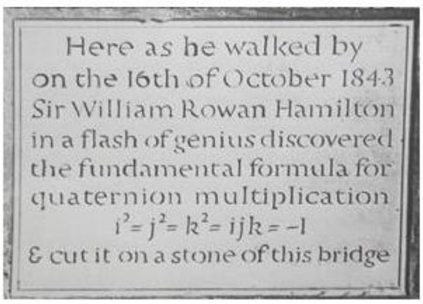
Barcelona, 20 de julio de 2013

Índice

# 1 Introducción

Los números naturales e incluso los racionales siempre han estado presentes a lo largo de la historia ya que se usaban para contar y para hacer particiones respectivamente. Pero históricamente, los matemáticos se han ido encontrando con la necesidad de ampliar los sistemas numéricos para resolver problemas algebraicos y geométricos. Gauss, Cauchy y otros matemáticos estaban familiarizados con los números complejos obtenidos a partir de de los reales por adición de una solución imaginaria $i$ de la ecuación $x^2 = -1$.

Sabemos que los complejos nos ayudan a estudiar cuestiones geométricas del plano, así por ejemplo, un giro en el plano no es más que la multiplicación por un número complejo de norma unidad. En 1835, William Rowan Hamilton (1805-1865) se planteó extender los números complejos a un sistema en dimensión tres, que pudiera jugar un papel geométrico en el espacio análogo al que desempeñan los números complejos en el plano. Según explica el propio Hamilton, el 16 de octubre de 1843, paseando por el puente de Brongham, que cruza el canal Real de Dublín, se dió cuenta de que necesitaba añadir una cuarta dimensión, comprendiendo así la estructura de los cuaterniones. Acto seguido grabó con la punta de su navaja, sobre una piedra del puente, la feliz idea (esta inscripción no se conserva hoy día). En el lugar donde Hamilton realizó el descubrimiento, la Royal Irish Academy erigió una placa conmemorativa.

Al día siguiente de su descubrimiento, Hamilton escribió una carta a su amigo John Graves en la que le decía:

*Una línea de especulación matemática muy curiosa se me ocurrió ayer, y sin duda la encontrarás interesante. Sabes que llevo mucho tiempo intentando una "Teoría de Ternas" análoga a la "Teoría de Pares" o a la representación geométrica de Mr. Warren de las cantidades imaginarias. Creo que descubrí ayer una "Teoría de Cuaternios", que incluye la "Teoría de Ternas" buscada.*

Hamilton partía de los números complejos $\mathbb{C} = \mathbb{R} + \mathbb{R}i$ y se dio cuenta de que, si añadía una nueva unidad imaginaria $j$, también debía añadir el producto $k = ij$. Graves decidió no pararse aquí, sino que añadió una unidad imaginaria adicional $l$, con lo que debía añadir los productos $il$, $jl$ y $kl$, obteniendo así una álgebra real de dimensión 8, que extiende la de los cuaterniones, y que hoy en día se conoce como el álgebra de los octoniones (o de los números de Cayley). Así, Graves formalizó los octoniones en 1844 e, independientemente, Cayley lo hizo en 1845.

### Resumen del trabajo en inglés

The first section of this work discusses algebras. Particularly, the algebras which interest us are division algebras, which are algebras over a field where division is always possible. Then we introduce quaternions. We show that quaternions are a non-commutative division algebra. Also we will see how can we express a quaternion through real and complex matrices of dimensions 2 and 4 respectively, and why the equation $z^2 + 1 = 0$ with $z \in \mathbb{H}$ has infinite solutions. In the last part of this section, we prove the Frobenius Theorem which affirms that the only division algebras of finite dimension over $\mathbb{R}$ are the real numbers, the complex numbers and the quaternions.

Hamilton discovered quaternions with the idea of using them to study rotations in 3-dimensional space. In the third section of this work we will see how to represent 3-dimensional rotations with unit quaternions.

We will introduce the octonions in the fourth part of this work. We will see that octonions form a non-associative division algebra.

In the next section we introduce the Cayley-Dickson construction for normed algebras. By this construction, we can obtain the complex numbers from the real numbers, the quaternions from the complex numbers and y the octonions from the quaternions.

Finally, we will see that we can define a cross product in $\mathbb{R}^n$ only if $n = 1, 3$ or $7$. We will use this fact to prove a theorem, asserting that the possible dimensions for a normed algebra over $\mathbb{R}$ are only $1, 2, 4, 8$. We will deduce from this statement a Theorem of Hurwitz which states that if $n \in \mathbb{N}$, the product of two sums of $n$ squares can be expressed as a sum of $n$ squares only if $n = 1, 2, 4, 8$.

# 2 El álgebra de los cuaterniones

## 2.1 Álgebras

**Definición**: Sea $A$ un anillo conmutativo unitario. Una $A$-álgebra es un $A$-módulo $E$ provisto de una aplicación $A$-bilineal:

$$\begin{aligned} w : E \times E &\to E \\ (x, y) &\mapsto w(x, y) \end{aligned}$$

Usualmente denotaremos $w(x, y)$ por $x \cdot y$.

**Definición**:

i) Se dice que $E$ es una $A$-álgebra asociativa si $x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \forall x, y, z \in E$.

ii) Se dice que $E$ tiene unidad si existe $1 \in E$ tal que $1 \cdot x = x \cdot 1 = x \quad \forall x \in E$.

iii) Sea $E$ una $A$-álgebra. Se define el centro de $E$ como:

$$Z(E) = \{x \in E \mid \forall y \in E \ x \cdot y = y \cdot x\}$$

Entonces, se dice que $E$ es una $A$-álgebra conmutativa si $Z(E) = E$ , es decir, si $x \cdot y = y \cdot x$ para cada $x, y \in E$.

**Observación**: Una $A$-álgebra asociativa con unidad siempre es un anillo unitario.

**Ejemplos**:

i) Todo anillo conmutativo $A$ es una $A$-álgebra tomando como $w$ el producto en $A$ como anillo.

ii) El $A$-módulo $M_{n\times n}(A)$ es una $A$-álgebra asociativa con el producto usual de matrices.

iii) Sea $f : A \to B$ un morfismo de anillos unitarios, donde $A$ es conmutativo, tal que $f(A) \subset Z(B)$. Entonces $B$ es una $A$-álgebra asociativa donde $w$ es la multiplicación como anillo.

iv) Sea $A$ un anillo conmutativo. Entonces, $A[x_1, ..., x_n]$ es una $A$-álgebra por iii).

**Definición**: Sean $E_1$, $E_2$ dos $A$-álgebras. Se dice que $f : E_1 \to E_2$ es un morfismo de $A$-álgebras si verifica:

- $f(x_1 + y_1) = f(x_1) + f(y_1) \quad \forall x_1, y_1 \in E_1$
- $f(\lambda x_1) = \lambda f(x_1) \quad \forall \lambda \in A, \ \forall x_1 \in E_1$
- $f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2) \quad \forall x_1, x_2 \in E_1$
- $f(1_{E_1}) = 1_{E_2}$ (si las álgebras son unitarias)

**Definición**: Sean $E, F$ dos $A$-álgebras, se dice que $F \subset E$ es una $A$-subálgebra si la inclusión $i : F \hookrightarrow E$ es morfismo de $A$-álgebras.

**Definición**: Sea $E$ una $A$-álgebra. Se dice que $E$ es una álgebra con división si para cada $a \in E, \ b \in E, \ b \neq 0$ existe un único $x \in E$ tal que $a = bx$ y existe un único $y \in E$ tal que $a = yb$.

**Observación**: Si $E$ es una $A$-álgebra asociativa y unitaria, la condición anterior es equivalente a que para cada $a \in E, \ a \neq 0$ exista un $y \in E$ tal que $ay = ya = 1_E$.

**Observación**: Si $A$ es un álgebra con división conmutativa, entonces $A$ es un cuerpo.

## 2.2 Los cuaterniones

**Definición**: El álgebra de los cuaterniones, que denotaremos por $\mathbb{H}$, es el $\mathbb{R}$-álgebra cuyo espacio vectorial subyacente es $\mathbb{R}^4$ y en el que, dados $(a_1, b_1, c_1, d_1), (a_2, b_2, c_2, d_2) \in \mathbb{R}^4$, la multiplicación está definida por:

$(a_1, b_1, c_1, d_1) \cdot (a_2, b_2, c_2, d_2) = (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2, \quad a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2, \quad a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2, \quad a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)$

Es inmediato comprobar que esta multiplicación es $\mathbb{R}$-bilineal.

Tomando la base $\{1, i, j, k\}$, donde $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$ , $j = (0, 0, 1, 0)$, $k = (0, 0, 0, 1)$, se tiene que todo $\alpha \in \mathbb{H}$ se escribe de manera única como $\alpha = a + bi + cj + dk$, donde $a, b, c, d \in \mathbb{R}$. Es decir, podemos representar los cuaterniones como:

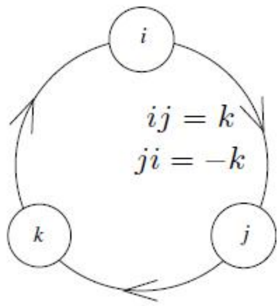
$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

La *tabla de multiplicación* de los elementos $1, i, j, k$ es:

| | $1$ | $i$ | $j$ | $k$ |
|---|---|---|---|---|
| $1$ | $1$ | $i$ | $j$ | $k$ |
| $i$ | $i$ | $-1$ | $k$ | $-j$ |
| $j$ | $j$ | $-k$ | $-1$ | $i$ |
| $k$ | $k$ | $j$ | $-i$ | $-1$ |

**Tabla 1**

La regla de multiplicación de los elementos de la base $\{i, j, k\}$ se puede recordar fácilmente mediante la siguiente figura:




Mientras los complejos son una extensión de los reales obtenida por adición de una unidad imaginaria $i$ tal que $i^2 = -1$, los cuaterniones son una extensión generada de manera análoga añadiendo unidades imaginarias $i$, $j$ y $k$ a los reales donde la multiplicación viene dada por la **Tabla 1**.

**Definición**:

i) Un cuaternión de la forma $a + 0i + 0j + 0k$, donde $a \in \mathbb{R}$, se llama real y un cuaternión de la forma $0 + bi + cj + dk$ se dice que es imaginario puro.

ii) Si $a + bi + cj + dk \in \mathbb{H}$, entonces se dice que $a$ es la parte escalar y $bi + cj + dk$ es la parte vectorial de dicho cuaternión.

**Observación**: También se puede describir un cuaternión como una pareja:

$$q = (Re(q),\ Im(q)) \in \mathbb{H}$$

donde $Re(q) \in \mathbb{R}$, $Im(q) \in \mathbb{R}^3$. Entonces, dados $(Re(q_1), Im(q_1)),((Re(q_2), Im(q_2)) \in \mathbb{H}$, las fórmulas de la suma y el producto se pueden escribir en la forma:

- $(Re(q_1),\ Im(q_1))\ +\ ((Re(q_2), Im(q_2)) = (Re(q_1)\ +\ Re(q_2),\ Im(q_1)\ +\ Im(q_2))$
- $(Re(q_1),\ Im(q_1))\,((Re(q_2),\ Im(q_2)) = (Re(q_1)Re(q_2) - Im(q_1){\cdot}Im(q_2),\ \ Re(q_1)Im(q_2) + Re(q_2)Im(q_1)\ +\ Im(q_1) \times Im(q_2))$

donde $\cdot$ es el producto escalar y $\times$ es el producto vectorial en $\mathbb{R}^3$.

**Observaciones**:

i) A diferencia de la multiplicación de los números reales o complejos, la multiplicación de los cuaterniones no es conmutativa (en general, $q_1q_2 \neq q_2q_1$). En la **Tabla 1** se ven claramente varios contraejemplos como:

$$ij = k \neq -k = ji$$

ii) Este hecho trae consecuencias como por ejemplo que a la hora de resolver una ecuación polinómica en $\mathbb{H}$, podemos encontrar un número de soluciones mayor que el grado del polinomio, o incluso infinitas soluciones.

**Ejemplo**: Si $z = (a, b, c, d) \in \mathbb{H}$, la ecuación $z^2 + 1 = 0$ tiene infinitas soluciones ya que:

$$z^2 + 1 = 0 \Rightarrow z^2 = -1 \Rightarrow a^2 - b^2 - c^2 - d^2 = -1;\ 2ab = 0;\ 2ac = 0;\ 2ad = 0.$$

Para satisfacer las tres últimas ecuaciones $a = 0$ ó bien $b,\ c,\ d = 0$. Este último caso es imposible ya que $b = c = d = 0$ implicaría que $a^2 = -1$ y llegaríamos a una contradicción porque $a \in \mathbb{R}$. De lo que deducimos que:

$$a = 0 \Rightarrow -b^2 - c^2 - d^2 = -1 \Rightarrow b^2 + c^2 + d^2 = 1$$

Así que la ecuación $z^2 + 1 = 0$ con $z \in \mathbb{H}$ tiene como soluciones los puntos la esfera $S^3 \subset \mathbb{R}^4$ de centro 0 y radio 1.

**Definición**: Sea $q = a + bi + cj + dk \in \mathbb{H}$. Se define:

i) El conjugado de $q$ como:

$$\bar{q} = a - bi - cj - dk$$

ii) La norma de $q$ como:

$$\|q\| = \sqrt{q\bar{q}} = \sqrt{a^2 + b^2 + c^2 + d^2} \in \mathbb{R}^+$$

(La norma de $q \in \mathbb{H}$ coincide con la norma usual en $\mathbb{R}^4$).

**Proposición**: Dados $p = a_1 + b_1 i + c_1 j + d_1 k,\ q = a_2 + b_2 i + c_2 j + d_2 k \in \mathbb{H},\ \alpha \in \mathbb{R}$ se verifica:

i) $\bar{\bar{p}} = p$

ii) $p\bar{p} = \bar{p}p$

iii) $\overline{qp} = \bar{p}\bar{q}$

iv) $\|\alpha q\| = |\alpha|\|q\|$

v) $\|pq\| = \|p\|\|q\|$ (multiplicatividad de la norma)

*Demostración*:

i) $\bar{p} = a_1 - b_1 i - c_1 j - d_1 k \Rightarrow \bar{\bar{p}} = a_1 + b_1 i + c_1 j + d_1 k = p$

ii) $p\bar{p} = (a_1 + b_1 i + c_1 j + d_1 k)(a_1 - b_1 i - c_1 j - d_1 k) = a_1^2 - a_1 b_1 - a_1 c_1 j - a_1 d_1 k + a_1 b_1 i + b_1^2 - b_1 c_1 k + b_1 d_1 j + a_1 c_1 j + b_1 c_1 k + c_1^2 - c_1 d_1 i + a_1 d_1 k - b_1 d_1 j + c_1 d_1 i + d_1^2 = a_1^2 + b_1^2 + c_1^2 + d_1^2$

$\bar{p}p = (a_1 - b_1 i - c_1 j - d_1 k)(a_1 + b_1 i + c_1 j + d_1 k) = a_1^2 + a_1 b_1 i + a_1 c_1 j + a_1 d_1 k - a_1 b_1 i + b_1^2 - b_1 c_1 k + b_1 d_1 j - a_1 c_1 j + b_1 c_1 k + c_1^2 - c_1 d_1 i - a_1 d_1 k - b_1 d_1 j + c_1 d_1 i + d_1^2 = a_1^2 + b_1^2 + c_1^2 + d_1^2$

iii) $\bar{p}\bar{q} = (a_1 - b_1 i - c_1 j - d_1 k)(a_2 - b_2 i - c_2 j - d_2 k) = a_1 a_2 - b_1 a_2 i - c_1 a_2 j - d_1 a_2 k - a_1 b_2 i - b_1 b_2 + c_1 b_2 k - d_1 b_2 j - a_1 c_2 j - b_1 c_2 k - c_1 c_2 + d_1 c_2 i - a_1 d_2 k + b_1 d_2 j - c_1 d_2 i - d_1 d_2 = (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (-a_1 b_2 - b_1 a_2 - c_1 d_2 + d_1 c_2)i + (-a_1 c_2 + b_1 d_2 - c_1 a_2 - d_1 b_2)j + (-a_1 d_2 - b_1 c_2 + c_1 b_2 - d_1 a_2)k = \overline{qp}$

iv) $\|\alpha q\| = \sqrt{\alpha q \overline{\alpha q}} = |\alpha| \sqrt{\bar{q} q} = |\alpha| \|q\|$

v) $\|pq\| = \sqrt{pq\overline{pq}} = \sqrt{pq\bar{q}\bar{p}} = \sqrt{p\bar{p}}\|q\| = \|p\|\|q\|$

**Definición**: Se define el inverso multiplicativo de un cuaternión no nulo $q$ como:

$$q^{-1} = \frac{\bar{q}}{q\bar{q}} = \frac{\bar{q}}{\|q\|^2}$$

**Observación**: Podemos dividir dos cuaterniones $p$ y $q$ de dos maneras distinas: $pq^{-1} = p\frac{\bar{q}}{\|q\|^2}$ ó $q^{-1}p = \frac{\bar{q}}{\|q\|^2}p$.

**Proposición**: $\mathbb{H}$ es una $\mathbb{R}$-álgebra asociativa en la que todo elemento no nulo tiene inverso (es un álgebra con división).

*Demostración*: Por definición $\mathbb{H}$ es un $\mathbb{R}$-espacio vectorial. La multiplicación:

$$w : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$$

es $\mathbb{R}$-bilineal y es asociativa. Esto último basta comprobarlo para los elementos $1, i, j, k$ y se tiene:

$$(ij)k = i(jk);\ (ji)k = j(ik);\ (ik)j = i(kj);\ (ki)j = k(ij);\ (jk)i = j(ki);\ (kj)i = k(ji).$$

Por otro lado, sea $q \in \mathbb{H},\ q \neq 0$. Se tiene:

$$qq^{-1} = q\frac{\bar{q}}{\|q\|^2} = 1 = q^{-1}q$$

luego $\mathbb{H}$ es un anillo con división.

En las siguientes tres proposiciones se explica que $\mathbb{C}$ es una subálgebra de $\mathbb{H}$ y que $\mathbb{H}$ es subálgebra de $M_{2\times 2}(\mathbb{C})$ y $M_{4\times 4}(\mathbb{R})$. Así, cualquier cuaternión se puede expresar mediante una matriz $M_{2\times 2}(\mathbb{C})$ y también mediante una matriz $M_{4\times 4}(\mathbb{R})$.

**Proposición**: La aplicación:

$$\begin{aligned} i_0 : \mathbb{C} &\hookrightarrow \mathbb{H} \\ a+bi &\mapsto a+bi \end{aligned}$$

es un morfismo inyectivo de $\mathbb{R}$-álgebras (análogamente para $a+bi \mapsto a+bj$ ó $a+bi \mapsto a+bk$).

*Demostración*

Dados $x = a+bi,\ y = c+di \in \mathbb{C},\ \lambda \in \mathbb{R}$, se verifica:

- $i_0(x+y) = i_0((a+bi)+(c+di)) = i_0((a+c)+(b+d)i) = (a+c)+(b+d)i = (a+bi)+(c+di) = i_0(a+bi)+i_0(c+di) = i_0(x)+i_0(y)$
- $i_0(\lambda x) = i_0(\lambda(a+bi)) = i_0(\lambda a+\lambda bi) = \lambda a+\lambda bi = \lambda(a+bi)i = \lambda i_0(a+bi) = \lambda i_0(x)$
- $i_0(xy) = i_0((a+bi)(c+di)) = i_0((ac-bd)+(ad+bc)i) = (ac-bd)+(ad+bc)i = (a+bi)(c+di) = i_0(a+bi)i_0(c+di) = i_0(x)i_0(y)$
- $i_0(1) = 1$

**Proposición**: La aplicación:

$$\begin{aligned} i_1 : \mathbb{H} &\hookrightarrow M_{2\times 2}(\mathbb{C}) \\ a+bi+cj+dk &\mapsto \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \end{aligned}$$

es un morfismo inyectivo de $\mathbb{R}$-álgebras.

*Demostración*

Dados $q = a_1+b_1i+c_1j+d_1k, p = a_2+b_2i+c_2j+d_2k \in \mathbb{H},\ \lambda \in \mathbb{R}$:

- $i_1(q+p) = i_1((a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k) =$
$$= \begin{pmatrix} (a_1+a_2)+(b_1+b_2)i & (c_1+c_2)+(d_1+d_2)i \\ -(c_1+c_2)+(d_1+d_2)i & (a_1+a_2)-(b_1+b_2)i \end{pmatrix} =$$
$$= \begin{pmatrix} a_1+b_1 i & c_1+d_1 i \\ -c_1+d_1 i & a_1-b_1 i \end{pmatrix} + \begin{pmatrix} a_2+b_2 i & c_2+d_2 i \\ -c_2+d_2 i & a_2-b_2 i \end{pmatrix} = i_1(q)+i_2(p)$$

- $i_1(\lambda q) = i_1(\lambda a_1+\lambda b_1 i+\lambda c_1 j+\lambda d_1 k) = \begin{pmatrix} \lambda a_1+\lambda b_1 i & \lambda c_1+\lambda d_1 i \\ -\lambda c_1+\lambda d_1 i & \lambda a_1-\lambda b_1 i \end{pmatrix} = \lambda \begin{pmatrix} a_1+b_1 i & c_1+d_1 i \\ -c_1+d_1 i & a_1-b_1 i \end{pmatrix} =$
$\lambda i_1(q)$

- $i_1(qp) = i_1((a_1a_2-b_1b_2-c_1c_2-d_1d_2)+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)i+(a_1c_2-b_1d_2+c_1a_2+d_1b_2)j+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)k) = a'+b'i+c'j+d'k = \begin{pmatrix} a'+b'i & c'+d'i \\ -c'+d'i & a'-b'i \end{pmatrix} =$
$\begin{pmatrix} a_1+b_1 i & c_1+d_1 i \\ -c_1+d_1 i & a_1-b_1 i \end{pmatrix} + \begin{pmatrix} a_2+b_2 i & c_2+d_2 i \\ -c_2+d_2 i & a_2-b_2 i \end{pmatrix} = i_1(q)i_1(p)$

- $i_1(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

**Proposición**: Si $q \in \mathbb{H}$, se tiene que:

i) $i_1(\bar{q}) = \overline{i_1(q)}^T$

ii) $\|q\|^2 = det(i_1(q))$

*Demostración*

i) $\bar{q} = a-bi-cj-dk \Longrightarrow \begin{pmatrix} a-bi & -c-di \\ c-di & a+bi \end{pmatrix}$

ii) $\begin{vmatrix} a+bi & c+di \\ -c+di & a-bi \end{vmatrix} = (a+bi)(a-bi)-(c+di)(-c+di) = a^2+b^2-(-d^2-c^2) = a^2+b^2+c^2+d^2 =$
$\|q\|^2$

**Observación**: Esta representación matricial nos da un isomorfismo entre $\mathbb{S}^3 = \{(x_0^2, x_1^2, x_2^2, x_3^2) \in \mathbb{R}^4 : x_0^2+x_1^2+x_2^2+x_3^2 = 1\} = \{q \in \mathbb{H} : \|q\| = 1\}$ y $SU(2)$ que es el grupo de las matrices complejas de dimensión $2\times 2$ que tienen por inversas sus adjuntas y cuyo determinante es igual a 1.

**Proposición**: La aplicación:

$$\begin{aligned} i_2 : \mathbb{H} &\hookrightarrow M_{4\times4}(\mathbb{R}) \\ a + bi + cj + dk &\mapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \end{aligned}$$

es un morfismo inyectivo de $\mathbb{R}$-álgebras.

*Demostración*

Dados $q = a_1 + b_1 i + c_1 j + d_1 k, p = a_2 + b_2 i + c_2 j + d_2 k \in \mathbb{H}$, $\lambda \in \mathbb{R}$:

- $i_2(q + p) = i_2((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k) =$
$$= \begin{pmatrix} a_1 + a_2 & b_1 + b_2 & c_1 + c_2 & d_1 + d_2 \\ -(b_1 + b_2) & a_1 + a_2 & -(d_1 + d_2) & c_1 + c_2 \\ -(c_1 + c_2) & d_1 + d_2 & a_1 + a_2 & -(b_1 + b_2) \\ -(d_1 + d_2) & -(c_1 + c_2) & b_1 + b_2 & a_1 + a_2 \end{pmatrix} =$$
$$= \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ -b_1 & a_1 & -d_1 & c_1 \\ -c_1 & d_1 & a_1 & -b_1 \\ -d_1 & -c_1 & b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 & -d_2 & c_2 \\ -c_2 & d_2 & a_2 & -b_2 \\ -d_2 & -{}_2c & b_2 & a_2 \end{pmatrix} = i_2(q)i_2(p)$$

- $i_2(\lambda q) = \lambda a_1 + \lambda b_1 i + \lambda c_1 j + \lambda d_1 k = \begin{pmatrix} \lambda a_1 & \lambda b_1 & \lambda c_1 & \lambda d_1 \\ -\lambda b_1 & \lambda a_1 & -\lambda d_1 & \lambda c_1 \\ -\lambda c_1 & \lambda d_1 & \lambda a_1 & -\lambda b_1 \\ -\lambda d_1 & -\lambda c_1 & \lambda b_1 & \lambda a_1 \end{pmatrix} = \lambda \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ -b_1 & a_1 & -d_1 & c_1 \\ -c_1 & d_1 & a_1 & -b_1 \\ -d_1 & -c_1 & b_1 & a_1 \end{pmatrix} =$
$\lambda i_2(q)$

- $i_2(qp) = i_2((a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i + (a_1c_2 - b_1d_2 + c_1a_2 +$

$$d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k) = a' + b'i + c'j + d'k = \begin{pmatrix} a' & b' & c' & d' \\ -b' & a' & -d' & c' \\ -c' & d' & a' & -b' \\ -d' & -c' & b' & a' \end{pmatrix} =$$

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ -b_1 & a_1 & -d_1 & c_1 \\ -c_1 & d_1 & a_1 & -b_1 \\ -d_1 & -c_1 & b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 & -d_2 & c_2 \\ -c_2 & d_2 & a_2 & -b_2 \\ -d_2 & -c_2 & b_2 & a_2 \end{pmatrix} = i_2(q)i_2(p)$$

- $i_2(1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

**Proposición**: Si $q \in \mathbb{H}$, se tiene que:

i) $i_2(\bar{q}) = \overline{i_2(q)}^T$

ii) $\|q\|^4 = det(i_2(q))$

*Demostración*

i) $\bar{q} = a - bi - cj - dk \Longrightarrow \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$

ii) $\begin{vmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{vmatrix} = a \begin{vmatrix} a & -d & c \\ d & a & -b \\ -c & b & a \end{vmatrix} - (-1)b \begin{vmatrix} b & c & d \\ d & a & -b \\ -c & b & a \end{vmatrix} - c \begin{vmatrix} b & c & d \\ a & -d & c \\ -c & b & a \end{vmatrix} - (-1)d \begin{vmatrix} b & c & d \\ a & -d & c \\ d & a & -b \end{vmatrix} =$

$a^4b^4c^4d^4 + 2(a^2b^2 + a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + c^2d^2) = (a^2 + b^2 + c^2 + d^2)^2 = \|q\|^4$

## 2.3 El Teorema de Frobenius

**Teorema**: Sea $D$ una $\mathbb{R}$-álgebra con división tal que $dim_{\mathbb{R}} D < +\infty$. Entonces $D$ es isomorfa a $\mathbb{R}, \mathbb{C}$ ó $\mathbb{H}$.

*Demostración*

Sea la aplicación:

$$h : \mathbb{R} \to D$$
$$x \mapsto x \cdot 1_D$$

$h$ es inyectiva y es un morfismo de anillos, lo que permite considerar $\mathbb{R}$ como un subanillo de $D$. Si $h$ es un isomorfismo, $D \cong \mathbb{R}$.

Supongamos $D \ncong \mathbb{R}$. Entonces podemos tomar $d \in D - \mathbb{R}$ y denotar:

$$\mathbb{R} < d >= \{\alpha + \beta d \mid \alpha, \beta \in \mathbb{R}\}$$

**Lema 1**: Sea $D$ una $\mathbb{R}$-álgebra con división tal que $D \ncong \mathbb{R}$ y sean $d \in D - \mathbb{R}$ y $\mathbb{R} < d >= \{\alpha + \beta \mid \alpha, \beta \in \mathbb{R}\}$. Entonces:

i) $\mathbb{R} < d >$ es un subconjunto conmutativo maximal de $D$

ii) $\mathbb{R} < d >$ es un cuerpo isomorfo a $\mathbb{C}$

iii) $\mathbb{R} < d >= \{x \in D \mid x \cdot d = d \cdot x\}$

*Demostración del lema 1*

i) Sea $\mathbb{R} < d > \subset F \subset D$, donde $F$ es subespacio conmutativo y de dimensión maximal entre entre los subespacios conmutativos que contienen a $\mathbb{R} < d >$.

Si $x \in D$ conmuta con los elementos de $F$ entonces se cumple que $F + \mathbb{R}x$ es conmutativo ya que:

$\forall f_1, f_2 \in F,\ \lambda, \mu \in \mathbb{R}\ \ (f_1 + \lambda x)(f_2 + \mu x) = f_1 f_2 + f_1 \mu x + \lambda x f_2 + \lambda x \mu x = f_2 f_1 + \mu x f_1 + f_2 \lambda x + \mu x \lambda x = (f_2 + \mu x)(f_1 + \lambda x)$

Como $F$ es maximal y $F + \mathbb{R}x$ es conmutativo entonces $F + \mathbb{R}x = F$ y por lo tanto $x \in F$. Así, $F$ es subconjunto conmutativo maximal de $D$.

ii) Ahora bien, si $x \in F$ y $x \neq 0$ entonces $x^{-1} \in F$ puesto que:

$$\forall y \in F \quad xy = yx \Rightarrow x^{-1}y = yx^{-1}$$

Así, $F$ es un cuerpo (obviamente es subanillo de $D$).

Como $\mathbb{R} \subset F$ es una extensión finita y $F \ncong \mathbb{R}$, por el teorema fundamental del álgebra, se tiene que $F \cong \mathbb{C}$.

En particular, se tiene que:

$$dim_{\mathbb{R}} F = 2$$

$$dim_{\mathbb{R}} \mathbb{R} < d >= 2$$

Esto implica que $F = \mathbb{R} < d >$.

iii) Si $\in D$ conmuta con $d \in D - \mathbb{R} \Longrightarrow x \in D$ conmuta con los elementos de $F = \mathbb{R} < d >$ $\Longrightarrow \; x \in F = \mathbb{R} < d >$

Por el lema 1, $D$ contiene un subanillo ($\mathbb{R} < d >$) isomorfo a $\mathbb{C}$. Entonces $\exists i \in D$ tal que $i^2 = -1$ y podemos identificar $\mathbb{R} < i >$ con $\mathbb{C}$.

Así, $D$ tiene una estructura de $\mathbb{C}$-espacio vectorial dada por la multiplicación (por la izquierda):

$$\lambda \in \mathbb{C}, \; x \in D \Rightarrow \lambda \cdot x$$

Entonces podemos considerar:

$$T : D \to D$$
$$x \mapsto x \cdot i$$

que es un endomorfismo del $\mathbb{C}$-espacio vectorial $D$.

Como $T^2 = -Id$, los únicos posibles valores propios de $T$ son $\pm i$.

Sean:

$D^+ = \{x \in D \mid xi = ix\}$ el conjunto de los vectores propios de valor propio $+i$.

$D^- = \{x \in D \mid xi = -ix\}$ el conjunto de los vectores propios de valor propio $-i$.

Es obvio que $D^+ \cap D^- = \{0\}$. Además, $D = D^+ \oplus D^-$ pues si $x \in D$, entonces:

$$x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi)$$

donde $\frac{1}{2}(x - ixi) \in D^+$ y $\frac{1}{2}(x + ixi) \in D^-$ pues:

- $(x - ixi)i = xi - ixii = xi - ix(-1) = xi + ix$

  $i(x - ixi) = ix - iixi = ix - (-1)xi = ix + xi$

- $(x + ixi)i = xi + ixii = xi + ix(-1) = xi - ix = 0$

  $i(x + ixi) = ix + iixi = ix + (-1)xi = ix - xi = 0$

Se tiene además:

a) $D^+ \cong \mathbb{C}$

Es cierto ya que $\mathbb{C} = \mathbb{R} < i > =$ elementos que conmutan con $i = D^+$.

b) $x, y \in D^- \Rightarrow x \cdot y \in D^+$

Pues $i(xy) = x(-1)y = -xiy = -xy(-i) = (xy)i$.

Si $D^- = 0$ entonces $D \cong \mathbb{C}$.

Supongamos $D^- \neq 0$, entonces tenemos que probar que $D \cong \mathbb{H}$.

**Lema 2**: $dim_{\mathbb{C}} D^- = 1$.

*Demostración del lema 2*

Sea $\alpha \in D^-$, $\alpha \neq 0$. La aplicación:

$$\varphi : D \to D$$
$$x \mapsto x \cdot \alpha$$

es $\mathbb{C}$-lineal e inversible (el inverso es $x \mapsto x \cdot \alpha^{-1}$).

Por b):

$$\varphi(D^-) = D^+$$

$$\varphi(D^+) = D^-$$

Como $D^+ \cong \mathbb{C} \Rightarrow dim_{\mathbb{C}} D^+ = 1 \Rightarrow dim_{\mathbb{C}} D^- = 1$.

**Lema 3**: $\alpha^2 \in \mathbb{R}$ y $\alpha^2 < 0$.

*Demostración del lema 3*

Por el lema 1, $\mathbb{R} < \alpha >$ es un cuerpo, así $\alpha^2 \in \mathbb{R} < \alpha >$. Por otro lado, $\alpha^2 \in \mathbb{C}$ por a) y b). Entonces se tiene que $\alpha^2 \in \mathbb{C} \cap \mathbb{R} < \alpha >= \mathbb{R}$.

Falta ver que $\alpha^2 < 0$. Si suponemos que $\alpha^2 > 0$, entonces $x^2 - \alpha^2 = 0$ tiene dos soluciones reales distintas, además de una tercera solución $\alpha$. Así, $\alpha^2$ tiene dos raíces en $\mathbb{R}$ y una raíz $\alpha$. Este hecho nos lleva a una contradicción, ya que $\alpha^2$ tendría tres raíces en $\mathbb{R} < \alpha >= \mathbb{C}$.

Sea $j = \dfrac{\alpha}{\sqrt{-\alpha^2}}$, entonces $j^2 = -1$. Sea $k = ij$.
Por el lema 2, $dim_{\mathbb{C}} D^- = 1$, entonces $dim_{\mathbb{R}} D^- = 2$. Por otro lado, $dim_{\mathbb{C}} D^+ = 1$ de manera que $dim_{\mathbb{R}} D^+ = 2$. Finalmente, como $D = D^+ \oplus D^-$, entonces $dim_{\mathbb{R}} D = 4$.

Como $i(ij) = i(-ji) = -(ij)i$, entonces $j, k \in D^-$. Además, $j, k$ son $\mathbb{R}$-independientes, luego $j, k$ generan $D^-$ sobre $\mathbb{R}$.

Como $1, i$ generan $D^+$ sobre $\mathbb{R}$ y $j, k$ generan $D^-$ sobre $\mathbb{R}$, se tiene que $D$ está generado por $1, i, j, k$ sobre $\mathbb{R}$.

Las relaciones:

$$i^2 = -1,\ j^2 = -1,\ k = ij,\ ij = -ji,\ ik = -ki$$

son las mismas que las que definen $\mathbb{H}$. Así, $D \cong \mathbb{H}$.

# 3 Rotaciones en el espacio de dimensión tres

Consideremos un vector $\vec{n} = (n_1, n_2, n_3) \in \mathbb{R}^3$ unitario, entonces se puede expresar una rotación de ángulo $\theta$ que tiene como eje de rotación el vector $\vec{n}$ mediante la llamada *fórmula de Rodrigues*:

$$R(\vec{n}, \theta)(\vec{v}) = (\cos\theta)\vec{v} + (\sin\theta)\ (\vec{n} \times \vec{v}) + (1 - \cos\theta)\ (\vec{n} \cdot \vec{v})\vec{n}$$

donde $\vec{v} \in \mathbb{R}^3$.

En esta sección veremos que $R(\vec{n},\theta)$ se puede representar mediante cuaterniones imaginarios puros utilizando el hecho de que existe una biyección entre $\mathbb{R}^3$ e $Im\mathbb{H}$:

$$\begin{aligned} \tau : \mathbb{R}^3 &\longleftrightarrow Im\mathbb{H} \\ (\alpha,\beta,\gamma) &\mapsto \alpha i + \beta j + \gamma k \end{aligned}$$

**Proposición**: Sean $R(\vec{n},\theta) : \mathbb{R}^3 \to \mathbb{R}^3$ una rotación y $T_q : Im\mathbb{H} \to Im\mathbb{H}$ la transformación que envía el cuaternión imaginario puro $p$ al producto de cuaterniones $q\ p\ \bar{q}$, donde $q = \cos\frac{1}{2}\theta + (n_1 i + n_2 j + n_3 k)\sin\frac{1}{2}\theta$. Entonces el siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathbb{R}^3 & \xrightarrow{R(\vec{n},\theta)} & \mathbb{R}^3 \\ \tau \updownarrow & & \updownarrow \tau \\ Im\mathbb{H} & \xrightarrow{T_q} & Im\mathbb{H} \end{array}$$

De manera que, a cada rotación tridimensional le corresponde un cuaternión unitario y viceversa. Observemos que $q\ p\ \bar{q} = q\ p\ q^{-1}$ ya que como $\|q\| = 1 \Rightarrow q^{-1} = \bar{q}$.

*Demostración*:

Supongamos que un vector $\vec{v} \in \mathbb{R}^3$ rota un ángulo $\theta$ alrededor de un eje, determinado por el vector unitario $\vec{n} = (n_1, n_2, n_3) \in \mathbb{R}^3$. Y sea $\vec{u} = R(\vec{n},\theta)(\vec{v})$.

Podemos asociar a cada vector el cuaternión correspondiente:

$$\vec{v} \longleftrightarrow q_{\vec{v}} = (0,\vec{v})$$

$$\vec{u} \longleftrightarrow q_{\vec{u}} = (0,\vec{u})$$

Como $q = \cos\frac{1}{2}\theta + (n_1 i + n_2 j + n_3 k)\sin\frac{1}{2}\theta$, si denotamos $\alpha = \cos\frac{1}{2}\theta$ y $\beta = \sin\frac{1}{2}\theta$, podemos expresar $q$ de la siguiente forma:

$$q = \alpha + (\beta n_1)i + (\beta n_2)j + (\beta n_3)k = (\alpha, \beta\vec{n})$$

Observemos que:

$$\|q\| = \sqrt{q\bar{q}} = \sqrt{\alpha^2 + \beta^2 n_1^2 + \beta^2 n_2^2 + \beta^2 n_3^2} = \sqrt{\alpha^2 + \beta^2(n_1^2 + n_2^2 + n_3^3)} = \sqrt{\alpha^2 + \beta^2} = 1$$

Calculamos el producto $q\ q_{\vec{v}}\ \bar{q}$ usando las propiedades del producto escalar y el producto vectorial, entonces obtenemos:

$$q\ q_{\vec{v}}\ \bar{q} = (\alpha, \beta\vec{n})(0, \vec{v})(\alpha, -\beta\vec{n}) = (0,\ \vec{v} + 2\beta\alpha\ \vec{n} \times \vec{v} + 2\beta^2\ \vec{n} \times (\vec{n} \times \vec{v}))$$

Si utilizamos las identidades:

$$\sin\alpha = 2\sin\frac{1}{2}\theta\cos\frac{1}{2}\theta = 2\beta\alpha$$

$$1 - \cos\theta = 2\sin^2\frac{1}{2}\theta = 2\beta^2$$

Se tiene que $q\ q_{\vec{v}}\ \bar{q} = (0,\ \vec{v} + (\sin\theta)\ \vec{n} \times \vec{v} + (1 - \cos\theta)\ \vec{n} \times (\vec{n} \times \vec{v}))$.

Ahora utilizando la identidad: $\vec{n} \times (\vec{n} \times \vec{v}) = (\vec{n} \cdot \vec{v})\vec{n} - (\vec{n} \cdot \vec{n})\vec{v} = (\vec{n} \cdot \vec{v})\vec{n} - v$ (por ser $\vec{v}$ unitario), obtenemos la *fórmula de Rodrigues*:

$$q\ q_{\vec{v}}\ \bar{q} = (0,\ (\cos\theta)\vec{v} + (\sin\theta)\ (\vec{n} \times \vec{v}) + (1 - \cos\theta)\ (\vec{n} \cdot \vec{v})\vec{n})$$

Por lo tanto:

$$q\ q_{\vec{v}}\ \bar{q} = q_{\vec{u}} \longleftrightarrow \vec{u} = (\cos\theta)\vec{v} + (\sin\theta)\ (\vec{n} \times \vec{v}) + (1 - \cos\theta)\ (\vec{n} \cdot \vec{v})\vec{n}$$

Con esto se ha demostrado que el producto de cuaterniones $q\ q_{\vec{v}}\ \bar{q}$ corresponde vía $\tau$ con una rotación de ángulo $\theta$ alrededor del eje $\vec{n}$.

**Corolario**: La composición de rotaciones en $\mathbb{R}^3$ es una rotación en $\mathbb{R}^3$.

*Demostración*: Sea $p \in Im\mathbb{H}$. La rotación alrededor del eje $\vec{n} = (n_1, n_2, n_3)$ con un ángulo $\theta$ se corresponde con:

$$Im\mathbb{H} \xrightarrow{T_q} \mathbb{H}$$
$$p \longmapsto q\ p\ \bar{q}$$

donde $q = \cos\frac{1}{2}\theta + (n_1 i + n_2 j + n_3 k)\sin\frac{1}{2}\theta$.

Ahora rotemos el cuaternión imaginario puro $q\ p\ \bar{q}$ alrededor de un eje $\vec{n'} = (n'_1, n'_2, n'_3)$ con un ángulo $\theta'$:

$$Im\mathbb{H} \xrightarrow{T_{q'}} \mathbb{H}$$
$$q\ p\ \bar{q} \longmapsto q'(q\ p\ \bar{q})\bar{q'} = (q'q)\ p\ (\overline{qq'})$$

donde $q' = \cos\frac{1}{2}\theta' + (n_1'i + n_2'j + n_3'k)\sin\frac{1}{2}\theta'$.

Observamos que $T_{q'} \circ T_q = T_{q'q}$ que corresponde a una rotación en $\mathbb{R}^3$ por la proposición anterior.

**Observación**: A veces es más eficaz usar cuaterniones para representar una rotación tridimensional que usar matrices de rotación ya que la necesidad de almacenaje de datos es menor y por lo tanto el coste computacional de su manejo es mucho más rentable. Por el contrario, la visualización de la rotación es menos intuitiva usando cuaterniones.

**Ejemplo**: *El truco del cinturón*

Consiste en fijar un extremo de un cinturón y rotar el otro extremo un ángulo de 360°(1 vuelta) o bien de 720° (2 vueltas) sobre su eje más largo. La idea es desdoblar el cinturón con movimientos que no cambien la orientación de los extremos. Lo que resulta interesante es que para el giro de 360° es imposible desdoblarlo, como se muestra en la **Figura 1**. Sin embargo, para el giro de 720° sí es posible hacerlo, como se muestra en la **Figura 2**.

Tomemos en cada punto del cinturón un sistema de referncia. Cuando el cinturón no está deformado, todos los sistemas de referencia son la identidad y por lo tanto, si $t$ representa el parámetro que describe el cinturón, se tiene el cuaternión $q(t) = (1,0,0,0)$. En particular, en el extremo inicial del cinturón ($t = 0$) se tiene $q(0) = (1,0,0,0)$.

Rotamos el cinturón alrededor de su eje más largo, digamos el eje $z$, con un ángulo $\theta$. Con la notación que hemos usado anteriormente, esto quiere decir que $\vec{n} = (0,0,1)$ y entonces:

$$q(t) = (\cos\frac{t\theta}{2}, 0, 0, \sin\frac{t\theta}{2})$$

En la **Figura 3** se muestra el cinturón como una secuencia de sistemas de referencia determinados por esta rotación.

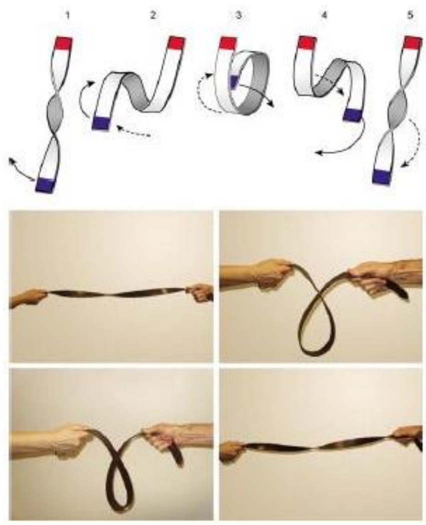


**Figura 1:** El truco del cinturón con 360 grados

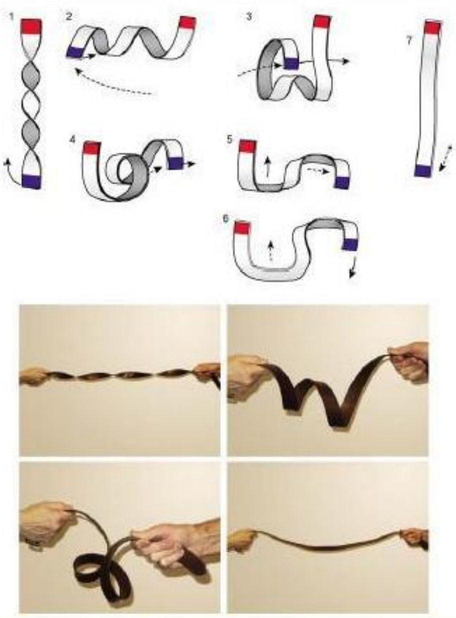


**Figura 2:** El truco del cinturón con 720 grados

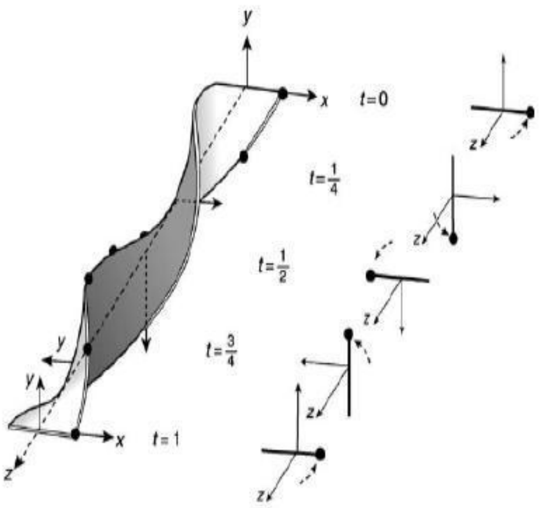



**Figura 3**

De esta manera, si rotamos el cintuón con un ángulo $\theta = 2\pi$ (una vuelta), entonces:

$$q(0) = (1, 0, 0, 0)$$

$$q(t) = (\cos t\pi, 0, 0, \sin 2t\pi)$$

$$q(1) = (-1, 0, 0, 0)$$

Sin embargo, si rotamos el cintuón con un ángulo $\theta = 4\pi$ (dos vueltas), entonces:

$$q(0) = (1, 0, 0, 0)$$

$$q(t) = (\cos 2t\pi, 0, 0, \sin t\pi)$$

$$q(1) = (1, 0, 0, 0)$$

Así, si rotamos el cinturón dos vueltas obtenemos el cuaternión inicial ($q(0) = q(1) = (1, 0, 0, 0)$) y por lo tanto el cinturón quedará de la misma forma en la que lo teníamos en un principio (desdoblado). Pero esto no pasa si lo rotamos una única una vuelta, ya que en este caso, no obtenemos el cuaternión inicial ($q(0) = (1, 0, 0, 0) \neq (-1, 0, 0, 0) = q(1)$) y por lo tanto el cinturón no quedará desdoblado como lo teníamos en el inicio.

# 4 Los octoniones

**Definición**: El álgebra de los octoniones, que denotaremos por $\mathbb{O}$, es un $\mathbb{R}$-álgebra cuyo espacio vectorial subyacente es $\mathbb{R}^8$. Tomando la base $\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$, donde

$1 = (1, 0, ..., 0)$ y $e_i = (0, ..., 1^{i)}, ...0)$, podemos representar los octoniones como:

$$\mathbb{O} = \{a_0 + \sum_{i=1}^{7} a_i e_i \mid a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{R}\}$$

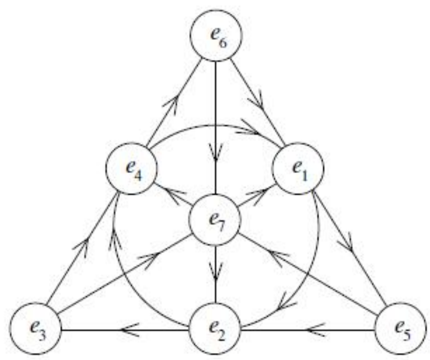
La multiplicación se define sobre esta base por la *tabla de multiplicación*:

| | $1$ | $e_1$ | $e_2$ | $e_3$ | $e_4$ | $e_5$ | $e_6$ | $e_7$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $e_1$ | $e_2$ | $e_3$ | $e_4$ | $e_5$ | $e_6$ | $e_7$ |
| $e_1$ | $e_1$ | $-1$ | $e_4$ | $e_7$ | $-e_2$ | $e_6$ | $-e_5$ | $-e_3$ |
| $e_2$ | $e_2$ | $-e_4$ | $-1$ | $e_5$ | $e_1$ | $-e_3$ | $e_7$ | $-e_6$ |
| $e_3$ | $e_3$ | $-e_7$ | $-e_5$ | $-1$ | $e_6$ | $e_2$ | $-e_4$ | $e_1$ |
| $e_4$ | $e_4$ | $e_2$ | $-e_1$ | $-e_6$ | $-1$ | $e_7$ | $e_3$ | $-e_5$ |
| $e_5$ | $e_5$ | $-e_6$ | $e_3$ | $-e_2$ | $-e_7$ | $-1$ | $e_1$ | $e_4$ |
| $e_6$ | $e_6$ | $e_5$ | $-e_7$ | $e_4$ | $-e_3$ | $-e_1$ | $-1$ | $e_2$ |
| $e_7$ | $e_7$ | $e_3$ | $e_6$ | $-e_1$ | $e_5$ | $-e_4$ | $-e_2$ | $-1$ |

**Tabla 2**

Y se extiende a $\mathbb{O}$ por asociatividad y $\mathbb{R}$-bilinealidad.

La regla de multiplicación de los elementos de la base de los octoniones se puede recordar fácilmente a través de *plano de Fano*:




que está formado por siete puntos y siete líneas orientadas (el circulo central lo consideramos como una línea). Cada uno de los puntos corresponde a un elemento de la base imaginaria de los octoniones. Para obtener el resultado de la multiplicación de dos elementos de la base, tan solo tenemos que seguir la línea que los une teniendo en cuenta su orientación.

**Observación**: La multiplicación de los octoniones no es asociativa (en general, $w_1(w_2w_3) \neq (w_1w_2)w_3$). En la **Tabla 2** se ven claramente varios contraejemplos como:

$$e_1(e_2e_3) = e_6 \neq -e_6 = (e_1e_2)e_3$$

**Definición**: Dado $u = u_0 + \sum_{i=i}^{7} u_ie_i \in \mathbb{O}$, se define:

i) $Re(u) = u_0$

ii) $Im(u) = \sum_{i=i}^{7} u_ie_i$

**Definición**: Sea $u = u_0 + \sum_{i=i}^{7} u_ie_i \in \mathbb{O}$. Se define:

i) El conjugado de $u$ como:

$$\overline{u} = u_0 - \sum_{i=i}^{7} u_ie_i$$

ii) La norma de $u$ como:

$$\|u\| = \sqrt{u\overline{u}}$$

**Definición**: Se define el inverso multiplicativo de un octonión no nulo $u$ como:

$$u^{-1} = \frac{\bar{u}}{u\bar{u}} = \frac{\bar{u}}{\|u\|^2}$$

**Proposición**: $\mathbb{O}$ es una $\mathbb{R}$-álgebra en la que todo elemento no nulo tiene inverso (es un álgebra con división).

*Demostración*: Por definición $\mathbb{O}$ es un $\mathbb{R}$-espacio vectorial. La multiplicación:

$$w : \mathbb{O} \times \mathbb{O} \to \mathbb{O}$$

es $\mathbb{R}$-bilineal.

Sea $u \in \mathbb{O},\ u \neq 0$, se tiene:

$$uu^{-1} = u\frac{\bar{u}}{\|u\|^2} = 1 = u^{-1}u$$

luego $\mathbb{O}$ es un anillo con división.

**Observación**: En la sección 2.2 vimos que $\mathbb{H}$ es una subálgebra de $M_{2\times 2}(\mathbb{C})$ y de $M_{4\times 4}(\mathbb{R})$, pero esto no ocurre con $\mathbb{O}$ ya que el álgebra de las matrices cuadradas reales o complejas es asociativa y en cambio $\mathbb{O}$ no lo es.

# 5 La construcción de Cayley-Dickson

**Definición**: Sea $A$ una $\mathbb{R}$-álgebra unitaria con una aplicación lineal:

$$\begin{aligned} \alpha : A &\to A \\ a &\mapsto \alpha(a) = \bar{a} \end{aligned}$$

que verifica:

i) $\bar{\bar{a}} = a \quad \forall a \in A$

ii) $\overline{ab} = \bar{b}\bar{a} \quad \forall a, b \in A$

Diremos que $A$ es una $\mathbb{R}$-álgebra unitaria con involución.

La existencia de $1_A \in A$ nos permite considerar la aplicación:

$$\begin{aligned} \mathbb{R} &\hookrightarrow A \\ a &\mapsto a 1_A \end{aligned}$$

**Definición**: Si $A$ es una $\mathbb{R}$-álgebra unitaria con involución, diremos que $A$ verifica la condición de Cayley-Dickson si:

i) $a + \bar{a} \in \mathbb{R} \quad \forall a \in A$

ii) $a\bar{a} = \bar{a}a > 0 \quad \forall a \in A,\ a \neq 0$

**Lema**: Si $A$ es una $\mathbb{R}$-álgebra unitaria con involución que verifica la condición de Cayley-Dickson, se puede definir una norma sobre $A$ por:

$$\|a\|^2 = a\bar{a}$$

*Demostración*: Veamos que, efectivamente, es una norma:

i) $\|a\| = (a\bar{a})^{1/2} \geq 0 \quad \forall a \in A$

ii) $\|a\| = 0 \Leftrightarrow a\bar{a} = 0 \Leftrightarrow a = 0$

iii) $\|ka\| = \sqrt{ka\overline{ka}} = \sqrt{k^2 a\bar{a}} = |k|\sqrt{a\bar{a}} = |k|\|a\| \quad \forall a \in A, \ \forall k \in \mathbb{R}$

iv) $\|a+b\|^2 = (a+b)\overline{(a+b)} = (a+b)(\bar{a}+\bar{b}) = a\bar{a} + a\bar{b} + b\bar{a} + b\bar{b} = \|a\|^2 + a\bar{b} + \overline{a\bar{b}} + \|b\|^2 = \|a\|^2 + 2Re(a\bar{b}) + \|b\|^2 \leq \|a\|^2 + 2\|Re(a\bar{b})\| + \|b\|^2 \leq \|a\|^2 + 2\|a\bar{b}\| + \|b\|^2 = \|a\|^2 + 2\|a\|\|b\| + \|b\|^2 = (\|a\| + \|b\|)^2 \Rightarrow \|a+b\| \leq \|a\| + \|b\| \quad \forall a, b \in A$ (Desigualdad triangular)

Entonces, es posible definir el inverso multiplicativo de $a \in A$, $a \neq 0$ por:

$$a^{-1} = \frac{\bar{a}}{\|a\|^2}$$

Además, la norma es multiplicativa ya que:

$$\|ab\|^2 = (ab)\overline{(ab)} = ab\bar{b}\bar{a} = a(b\bar{b})\bar{a} = \|a\|^2\|b\|^2$$

**Definición**: Sea $A$ una $\mathbb{R}$-álgebra con involución que verifica la condición de Cayley-Dickson. Entonces la construcción de Cayley-Dickson proporciona una nueva álgebra $A'$ con involución que verifica la condición de Cayley-Dickson, los elementos de la cual son los pares $(a,b) \in A^2$. La multiplicación en $A'$ se define por:

$$(a,b)(c,d) = (ac - b\bar{d}, ad + b\bar{c}) \quad \forall (a,b),(c,d) \in A' \tag{1}$$

y la conjugación como:

$$\overline{(a,b)} = (\bar{a}, -b) \quad \forall (a,b) \in A' \tag{2}$$

**Lema**: $A'$ verifica la condición de Cayley-Dickson.

*Demostración*: Se tiene que verificar:

i) $(a,b) + \overline{(a,b)} = (a,b) + (\bar{a}, -b) = (a+\bar{a}, b-b) = (a+\bar{a}, 0) \in \mathbb{R} \quad \forall (a,b) \in A'$

ii) $(a,b)\overline{(a,b)} = (a,b)(\bar{a},-b) = (a\bar{a}+\bar{b}b, -ab+b\bar{\bar{a}}) = (a\bar{a}+\bar{b}b, 0) > 0 \quad \forall (a,b) \in A'$

**Observación**: Esta construcción produce una secuencia de $\mathbb{R}$-álgebras, cada una con dimensión doble de la anterior.

**Ejemplos**:

i) Si aplicamos la construcción de Cayley-Dickson a $\mathbb{R}$ con $\alpha = id$, obtenemos $\mathbb{C}$:

$$(a,b)(c,d) = (ac-bd, ad+bc) \quad \forall (a,b),(c,d) \in \mathbb{C}$$

$$\overline{(a,b)} = (a,-b)$$

ii) Aplicando la construcción de Cayley-Dickson a $\mathbb{C}$ con $\alpha$ la conjugación en los complejos, obtenemos $\mathbb{H}$:

$$(a,b)(c,d) = (ac-b\bar{d}, ad+b\bar{c}) \quad \forall (a,b),(c,d) \in \mathbb{H}$$

Además, en la sección de cuaterniones, ya vimos que el conjugado de un cuaternión $(a,b)$ está definido como:

$$\overline{(a,b)} = (\bar{a},-b)$$

iii) También obtenemos $\mathbb{O}$ si aplicamos la la construcción de Cayley-Dickson a $\mathbb{H}$ con $\alpha$ la conjugación en los cuaterniones. Podemos definir un octonión como un par de cuaterniones, el producto y la conjugación se corresponden con (1) y (2).

**Observación**: Esta construcción nos permite entender de manera unificada la cadena $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$. En cada paso de la construcción de Cayley-Dickson, el álgebra va perdiendo propiedades. En primer lugar perdemos el hecho de que cada elemento es su propio conjugado, después perdemos conmutatividad, y finalmente perdemos la asociatividad. En el siguiente paso de la construcción de Cayley-Dickson se pierde la propiedad de ser un álgebra con división.

# 6 El Teorema de Hurwitz

Sea $n \in \mathbb{N}$, Hurwitz se planteó el problema de que si el producto de dos sumas de $n$ cuadrados se puede expresar como una suma de $n$ cuadrados.

Observemos que si $z_1 = (a_1, a_2), z_2 = (b_1, b_2) \in \mathbb{C}$, se tiene que:

$$\|z_1\|^2\|z_2\|^2 = \|z_1z_2\|^2 \Rightarrow (a_1^2 + a_2^2)(b_1^2 + b_2^2) = (a_1b_1 - a_2b_2)^2 + (a_1b_2 + a_2b_2)^2$$

De manera que, podemos expresar el producto de dos sumas de 2 cuadrados como una suma de 2 cuadrados.

En la sección de 2.2 vimos que la norma en $\mathbb{H}$ es multiplicativa, de manera que si $q_1 = (a_1, a_2, a_3, a_4), q_2 = (b_1, b_2, b_3, b_4) \in \mathbb{H}$, se tiene que:

$$\|q_1\|^2\|q_2\|^2 = \|q_1q_2\|^2 \Rightarrow (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2, b_4^2) = A_1^2 + A_2^2 + A_3^2 + A_4^2$$

donde $A_1, A_2, A_3, A_4$ son las componentes del cuaternión que resulta de multiplicar $q_1q_2$. Así que, el producto de dos sumas de 4 cuadrados se puede expresar como una suma de 4 cuadrados.

Esto también ocurre en el caso de $\mathbb{O}$. De hecho, en 1898, Hurwitz demostró que si $a_1, ..., a_n, b_1, ..., b_n$ son variables, entonces si existe una fórmula del tipo:

$$(a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) = A_1^2 + \cdots + A_n^2$$

donde $A_1, ..., A_n$ son de la forma:

$$A_i = \sum_{j,k=1}^{n} c_{ijk}a_jb_k$$

con $c_{ijk} \in \mathbb{R}$, necesariamente $n = 1, 2, 4$ ó 8.

En esta sección veremos una versión del teorema de Hurwitz que afirma que un álgebra normada de dimensión finita sobre $\mathbb{R}$ tiene dimensión $1, 2, 4$ ó 8. Para poder llegar a demostrar este teorema, previamente estudiaremos para qué dimensiones es posible definir un “producto vectorial” en $\mathbb{R}^n$. Veremos que esto sólo es posible si $n = 1, 3$ ó 7.

Sean $a, b, c \in \mathbb{R}^n$, $\lambda \in \mathbb{R}$ y sea $\times$ un producto que verifica los siguientes axiomas:

Ax.1: $a \times b = -(b \times a)$

Ax.2: $a \times (b + c) = (a \times b) + (a \times c)$

Ax.3: $\lambda(a \times b) = (\lambda a) \times b$

Ax.4: $a \cdot (a \times b) = 0$

Ax.5: $|a \times b| = [|a|^2|b|^2 - (a \cdot b)^2]^{1/2}$

donde $\cdot$ y $|\ |$ denotan el producto escalar y la norma respectivamente.

**Observación**: Suponiendo ciertos Ax.1, Ax.2, Ax.3 y Ax.4, entonces Ax.5 es equivalente a que si $a, b \in \mathbb{R}$ son tales que $|a| = |b| = 1$ y $a \cdot b = 0$ entonces $|a \times b| = 1$.

**Proposición 1**: Sean $a, b, c \in \mathbb{R}^n$ y sea $\times$ un producto que verifica los 5 axiomas anteriores, entonces se verifica:

i) $(a \times b) \cdot c = -[b \cdot (a \times c)]$

ii) $a \times (b \times c) - c \times (a \times b) = 2(a \cdot c)b - (b \cdot c)a - (a \cdot b)c$

*Demostración*

i) Cambiando $a$ por $a + c$ en Ax.4 y usando Ax.1, Ax.2 y Ax.4, se obtiene:

$$0 = (a+c) \cdot ((a+c) \times b) = (a+c) \cdot [-(b \times (a+c))] = (a+c) \cdot [-((b \times a) + (b \times c))] =$$
$$= -[(a+c) \cdot (b \times a) + (c+a) \cdot (b \times c)] = -[a \cdot (b \times a) + c \cdot (b \times a) + a \cdot (b \times c) + c \cdot (b \times c)] =$$
$$= -[c \times (a \times b) + a \cdot (b \times c)] \Rightarrow c \cdot (b \times a) = -[a \cdot (b \times c)]$$

Cambiando $a$ por $b$ y $b$ por $a$ obtenemos lo que se quería demostrar.

ii) Podemos escribir Ax.5 como:

$$(a \times b) \cdot (a \times b) = (a \cdot a)(b \cdot b) - (a \cdot b)^2$$

De la misma manera que en i) se ha cambiado $a$ por $a+c$, en este caso se debe cambiar $b$ por $b + d$ en esta última igualdad, y aplicando bilinealidad, simetria y cancelando lo que vale 0, se obtiene:

$$(a \times b) \cdot (a \times d) = (a \cdot a)(b \cdot d) - (a \cdot b)(a \cdot d)$$

aplicando i) y la linealidad del producto escalar, se tiene:

$$-[a \times (a \times b)] \cdot d = [(a \cdot a)b - (a \cdot b)a] \cdot d \Rightarrow -[a \times (a \times b)] = [(a \cdot a)b - (a \cdot b)a] \Rightarrow$$

$$\Rightarrow a \times (a \times b) = (a \cdot b)a - (a \cdot a)b \qquad (*)$$

Finalmente, cambiando $a$ por $a + c$ en esta última expresión se llega a ii). Para ello, primero hagamos el cambio en la parte de la izquierda de la desigualdad i apliquemos Ax.1, Ax.2 y Ax.4:

$(a+c)\times((a+c)\times b) = (a+c)\times[-(b\times(a+c))] = (a+c)\times[-((b\times a)(b\times c))] = -[(a+c)\times((b\times a)(b\times c))] = [(b\times a)(b\times c)]\times(a+c) = [(b\times a)+(b\times c)]\times a + [(b\times a)+(b\times c)]\times c = -[a\times(b\times a)+a\times(b\times c)+c\times(b\times a)+c\times(b\times c)] = -[a\times(b\times c)+c\times(b\times a)] = -a\times(b\times c)+c\times(a\times b)$

Ahora, hagamos el cambio de $a$ por $a+c$ en la parte de la derecha y apliquemos también Ax.1, Ax.2 y Ax.4:

$[(a+c)\cdot b](a+c) - [(a+c)\cdot(a+c)]b = (a\cdot b + c\cdot b)(a+c) - [(a\cdot b)a + 2(a\cdot c)b + (c\cdot b)c] = (a\cdot b)a + (c\cdot b)a + (a\cdot b)c + (c\cdot b)c - (a\cdot b)a - 2(a\cdot c)b - (c\cdot b)c = -2(a\cdot c)b + (c\cdot b)a + (a\cdot b)c$

Y como $a\times(a\times b) = (a\cdot b)a - (a\cdot a)b$, entonces $-a\times(b\times c) + c\times(a\times b) = -2(a\cdot c)b + (c\cdot b)a + (a\cdot b)c$.

**Observación**: Si $a, b, c \in \mathbb{R}^n$ son ortogonales entre sí, entonces la igualdad ii) de la proposición anterior se escribiría como:

$$a\times(b\times c) = c\times(a\times b) \qquad (**)$$

A partir de ahora, supondremos que $\times$ es un producto que verifica Ax.1, Ax.2 y Ax.4 y Ax.5.

**Definición**: Sea $\times$ un producto en $\mathbb{R}^n$. Un subespacio $A$ de $\mathbb{R}^n$ es cerrado bajo $\times$ si $A\times A \subset A$.

**Definición**: Sea $\times$ un producto en $\mathbb{R}^n$. Un subespacio $B$ de $\mathbb{R}^n$ se dice que es estable bajo $A\times$, donde $A \subseteq \mathbb{R}^n$, si $A\times B \subset B$.

**Proposición 2**: Sea $A \subseteq \mathbb{R}^n$ y sea $B$ un subespacio de $\mathbb{R}^n$. Si $B$ es estable bajo $A\times$, entonces $B^\perp = \{c \mid c \in \mathbb{R}^n,\ b\cdot c = 0\ \forall b \in B\}$ también lo es.

*Demostración*: Se tiene que demostrar:

$$A\times B \subset B \Rightarrow A\times B^\perp \subset B^\perp$$

Si $c \in B^\perp$, entonces para todo $a \in A$ y $b \in B$, aplicando i) de la proposición 1, se tiene que:

$$b \cdot (a \times c) = -[(a \times b) \cdot c] = 0 \text{ ya que } A \times B \subset B$$

Por lo tanto, para cualquier $b \in B$, $b \perp (a \times c)$ y entonces $a \times c \in B^{\perp}$.

**Proposición 3**: Sea $A$ un subespacio de $\mathbb{R}^n$ que es cerrado bajo $\times$ y tiene una base ortonormal $\{f_1, ..., f_k\}$. Sea $b \in A^{\perp}$. Entonces los vectores $\{b, f_1 \times b, ..., f_k \times b\}$ son de $A^{\perp}$ y son ortogonales entre sí y de la misma norma que $b$. En particular, si $b$ es un vector unitario, $\{b, f_1 \times b, ..., f_k \times b\}$ es un conjunto ortonormal de k+1 elementos de $A^{\perp}$.

*Demostración*: Por la proposición 2 se tiene que $\{b, f_1 \times b, ..., f_k \times b\} \subseteq A^{\perp}$. Ahora bien, por Ax.4, se tiene que $b \cdot (f_i \times b) = 0$ y además aplicando Ax.1, i) de la proposición 1 y $(*)$, se tiene que :

$(f_i \times b) \cdot (f_j \times b) = (b \times f_i) \cdot (b \times f_j) = -[b \times (b \times f_i) \cdot f_j] = -[(b \cdot f_i)b - (b \cdot b)f_i] \cdot f_j =$

$= (b \cdot b)(f_i \cdot f_j) = 0$

Por lo tanto los vectores $b, f_1 \times b, ..., f_k \times b$ son ortogonales entre sí.

Finalmente, por Ax.5:

$$|f_i \times b| = [|f_i|^2 \cdot |b|^2 - (f_i \cdot b)^2]^{1/2} = [|f_i|^2 \cdot |b|^2]^{1/2} = (|b|^2)^{1/2} = |b|$$

**Observación**: En $\mathbb{R}$ todos los vectores son paralelos, así que la única opción de tener un producto vectorial sería $v \times w = 0$ para todo $v, w \in \mathbb{R}$ que no verifica el Ax.5 ya que $|v \times w| = (1^2 1^2 - 0^2)^{1/2} = 1$. En $\mathbb{R}^2$ no se tiene producto vectorial ya que el vector $v \times w$ es ortogonal a $v \in \mathbb{R}^2$ y a $w \in \mathbb{R}^2$, lo que implica que $v \times w = 0$, pero esto no puede pasar si estos vectores son ortogonales y unitarios pues en ese caso por el Ax.5 se tendría que $|v \times w| = (1^2 1^2 - 0^2)^{1/2} = 1$.

**Observación**: Si $e_1, e_2$ son un par de vectores ortonormales de $\mathbb{R}^n$, entonces por Ax.5 se tiene que:

$$|e_1 \times e_2| = [|e_1|^2 |e_2|^2 - (e_1 \cdot e_2)^2]^{1/2} = (1 - 0)^{1/2} = 1$$

Denotaremos $H$ el subespacio de $\mathbb{R}^n$ formado por $\{e_1, e_2, e_3\}$, donde $e_3 = e_1 \times e_2$.

**Proposición 4**: $H$ es cerrado bajo $\times$.

*Demostración*: Hay que demostrar que $H \times H \subset H$. Por la bilinealidad de $\times$, basta comprobarlo para los elementos de la base, para ello usaremos Ax.1 y $(*)$:

$$e_2 \times e_3 = e_2 \times (e_1 \times e_2) = -[e_2 \times (e_2 \times e_1)] = -[(e_2 \cdot e_1)e_2 - (e_2 \cdot e_2)e_1] = e_1$$

Se demuestra análogamente para $e_3 \times e_1 = e_2$.

**Observación**: La base $\{e_1, e_2, e_3\}$ tiene la misma tabla de multiplicar que la base $\{i, j, k\}$ de $\mathbb{R}^3$ con el producto vectorial usual.

**Observación**: Cualquier vector $a \in \mathbb{R}^n$ se puede expresar como:

$$a = \sum_{i=1}^{3}(a \cdot e_i)e_i + [a - \sum_{i=1}^{3}(a \cdot e_i)e_i]$$

donde $\sum_{i=1}^{3}(a \cdot e_i)e_i \in H$ y $a - \sum_{i=1}^{3}(a \cdot e_i)e_i \in H^{\perp}$.

**Proposición 5**: Si $H = \mathbb{R}^n$, entonces $n = 3$ o bien $n \geq 7$.

*Demostración*: Si $H = \mathbb{R}^n$, entonces $n = 3$ o bien se podría encontrar un vector unitario $m \in H^{\perp}$. Supongamos el último caso. Entonces por la proposición 3, el conjunto $\{m, e_1 \times m, e_2 \times m, e_3 \times m\}$ es ortonormal en $H^{\perp}$ y el conjunto $\{e_1, e_2, e_3, m, e_1 \times m, e_2 \times m, e_3 \times m\}$ es ortonormal en $\mathbb{R}^n$, por lo tanto $n \geq 7$.

**Proposición 6**: Sea $C$ el subespacio de $\mathbb{R}^n$ generado por $\{e_1, e_2, e_3, m, e_1 \times m, e_2 \times m, e_3 \times m\}$, entonces $C$ es cerrado bajo $\times$.

*Demostración*: Hay que demostrar que $C \times C \subset C$. Para ello distingamos los cinco casos de productos que pueden ocurrir:

- $e_i \times e_j$ que está en $H$ por la proposición 4 y obviamente $H \subset C$.
- $e_i \times m$ que pertenece a $C$ por definición.

- $e_i \times (e_j \times m)$ que usando ii) de la proposición 1 y Ax.1 se tiene que:

  $e_i \times (e_j \times m) = 2(e_i \cdot m)e_j - (e_j \cdot m)e_i - (e_i \cdot e_j)m + m \times (e_i \times e_j) = -(e_i \times e_j) \times m - (e_i \cdot e_j)m \in C$

- $m \times (e_i \times m)$ que aplicando Ax.1 y $(*)$ se tiene que:

  $m \times (e_i \times m) = -m \times (m \times e_i) = (m \cdot m)e_i - (m \cdot e_i)m = e_i \in C$

- $(e_i \times m)(e_j \times m)$ que por Ax.1, por $(**)$ y por el caso anterior, se obtiene lo siguiente:

  $(e_i \times m)(e_j \times m) = (m \times e_i) \times (m \times e_j) = e_j \times [(m \times e_i) \times m] = e_j \times [m \times (e_i \times m)] = e_j \times e_i \in C$

**Observación**: Un vector $a \in \mathbb{R}^n$ lo podemos escribir de la siguiente manera:

$$a = [\textstyle\sum_{i=1}^{3}(a \cdot e_i)e_i + (a \cdot m)m + \sum_{i=1}^{3}(a \cdot (e_i \times m))(e_i \times m)] +$$
$$+[a - \textstyle\sum_{i=1}^{3}(a \cdot e_i)e_i - (a \cdot m)m - \sum_{i=1}^{3}(a \cdot (e_i \times m))(e_i \times m)]$$

donde $[\sum_{i=1}^{3}(a \cdot e_i)e_i + (a \cdot m)m + \sum_{i=1}^{3}(a \cdot (e_i \times m))(e_i \times m)] \in C$ y $[a - \sum_{i=1}^{3}(a \cdot e_i)e_i - (a \cdot m)m - \sum_{i=1}^{3}(a \cdot (e_i \times m))(e_i \times m)] \in C^{\perp}$. Por lo tanto, si $C = \mathbb{R}^n$, entonces $n = 7$ o bien es posible encontrar un vector unitario $n \in C^{\perp}$.

**Teorema**: Si existe un producto vectorial en $\mathbb{R}^k$ tal que satisface Ax.1, Ax.2, Ax.3, Ax.4 y Ax.5, entonces $k = 1, 3$ ó 7.

*Demostración*: Ya hemos visto que si $k \leq 3$, entonces existe un producto vectorial sólo si $k = 3$ y que si $k > 3$, entonces sólo puede existir un producto vectorial si $k \geq 7$. Ahora bien, si $k > 7$, se puede encontrar un vector unitario $n \in C^{\perp}$, donde $C$ es el subespacio de $\mathbb{R}^k$ que hemos construido anteriormente. Vamos a demostrar que la suposición de la existencia de este vector $n$ nos lleva a una contradicción. En efecto, en el caso de que exista $n$, entonces $m \times n$ es también un vector unitario (por Ax.5) en $C^{\perp}$. Sea $p = m \times n$, entonces también podemos escribir $p \times m = n$ (demostración análoga a la de la proposición 4). Ahora hagamos los siguientes cálculos para $i \neq j$:

- $(e_i \times m) \times (e_j \times n) = (e_i \times m) \times (e_j \times (p \times m))$ ya que $n = p \times m$

$= (e_i \times m) \times (m \times (e_j \times p))$ por $(**)$

$= (e_j \times p) \times ((e_i \times m) \times m)$ por $(**)$

$= (e_j \times p) \times (m \times (m \times e_i))$ por Ax.1

$= (e_j \times p) \times [(m \cdot e_i)m - (m \cdot m)e_i]$ por $(*)$

$= -(e_j \times p) \times e_i = e_i \times (e_j \times p)$ por Ax.1

$= p \times (e_i \times e_j)$ por $(**)$

- $(e_j \times n) \times (e_i \times m) = (e_j \times n) \times (e_i \times (n \times p))$ ya que $m = n \times p$

$= -(e_j \times n) \times (e_i \times (p \times n))$ por Ax.1

$= -(e_j \times n) \times (n \times (e_i \times p))$ por $(**)$

$= -(e_i \times p) \times ((e_j \times n) \times n)$ por $(**)$

$= -(e_i \times p) \times (n \times (n \times e_j))$ por Ax.1

$= -(e_i \times p) \times ((n \cdot e_j)n - (n \cdot n)e_j)$ por $(*)$

$= -(e_i \times p) \times (-e_j) = -e_j \times (e_i \times p)$ por Ax.1

$= -p \times (e_j \times e_i)$ por $(**)$

$= p \times (e_i \times e_j)$ por Ax.1

Entonces se tiene que $(e_i \times m) \times (e_j \times n) = (e_j \times n) \times (e_i \times m)$, pero esto contradice al Ax.1 a no ser que el producto sea 0. Esta contradicción demuestra que el caso $k > 7$ no se puede dar.

Ahora falta definir un producto vectorial en $\mathbb{R}^7$ que verifique los cinco axiomas. Consideraremos la terna $(a, \lambda, b)$ donde $a, b \in \mathbb{R}^3$ y $\lambda \in \mathbb{R}$ bajo la correspondencia:

$$a_1 i_1 + \cdots + a_7 i_7 \to (a_1 i + a_2 j + a_3 k, a_4, a_5 i + a_6 j + a_7 k)$$

Esta correspondencia nos da las siguientes operaciones en $\mathbb{R}^7$:

- suma: $(a_1, \lambda_1, b_1) + (a_2, \lambda_2, b_2) = ((a_1 + a_2), \lambda_1 + \lambda_2, (b_1 + b_2))$

- multiplicación por un escalar: $k(a_1, \lambda_1, b_1) = (ka_1, k\lambda_1, kb_1)$

- producto escalar: $(a_1, \lambda_1, b_1) \cdot (a_2, \lambda_2, b_2) = (a_1 \cdot a_2) + \lambda_1 \lambda_2 + (b_1 \cdot b_2)$

- producto vectorial: $(a_1, \lambda_1, b_1) \times (a_2, \lambda_2, b_2) = ([\lambda_1 b_2 - \lambda_2 b_1 + (a_1 \times a_2) - (b_1 \times b_2)], [-(a_1 \cdot b_2) + (b_1 \cdot a_2)], [\lambda_2 a_1 - \lambda_1 a_2 - (a_1 \times b_2) - (b_1 \times a_2)]$

donde $a_1, a_2, b_1, b_2 \in \mathbb{R}^3$, $\lambda_1, \lambda_2 \in \mathbb{R}$.

Como el producto vectorial en $\mathbb{R}^3$ satisface los cinco axiomas, entonces se deduce de la definición anterior que este producto vectorial en $\mathbb{R}^7$ también los verifica.

**Definición**: Sea $K$ un cuerpo. Un álgebra normada $(A, |\ \ |)$ está formada por una $K$-álgebra $A$ y una norma $|\ \ | : A \to K$ tal que:

$$|xy| = |x||y| \quad \forall x, y \in A$$

**Teorema (de Hurwitz)**: Un álgebra normada de dimensión finita sobre $\mathbb{R}$ tiene dimensión $1, 2, 4$ ó $8$.

*Demostración*: Si $A$ es una $\mathbb{R}$-álgebra normada, entonces se tiene una norma $|\ \ | : A \to \mathbb{R}$ tal que $|xy| = |x||y| \quad \forall x, y \in A$. Esta norma nos define una aplicación $\mathbb{R}$-bilineal, simétrica y definida positiva:

$$<\ ,\ >: A \times A \to \mathbb{R}$$

ya que $< x, y >= \frac{1}{2}(< x + y, x + y > - < x, x > - < y, y >) = \frac{1}{2}(|x + y|^2 - |x|^2 - |y|^2) \quad \forall x, y \in A$.

Se tiene que:

$$|xy| = |x||y| \quad \forall x, y \in A \iff < xy, xy >=< x, x >< y, y > \quad \forall x, y \in A$$

Si en esta última expresión cambiamos $x$ por $x + z$, se tiene que:

$< (x + z)y, (x + z)y >=< (x + z), (x + z) >< y, y >$

$$\Downarrow$$

$< xy + zy, xy + zy >= (< x, x > +2 < z, x > + < z, z >) < y, y >$

$$\Downarrow$$

$< xy, xy > +2 < zy, xy > + < zy, zy >=< x, x >< y, y > +2 < z, x >< y, y > + < z, z >< y, y >$

$$\Downarrow$$

$< zy, xy >=< z, x >< y, y >$

$$\Downarrow \text{ cambiando } y \text{ por } y+w$$

$< z(y+w), x(y+w) >=< z, x >< y+w, y+w >$

$$\Downarrow$$

$< zy + zw, xy + xw >=< z, x > (< y, y > +2 < y, w > + < w, w >)$

$$\Downarrow$$

$< zy, xy > + < zy, xw > + < zw, xy > + < zw, xw >=< z, x >< y, y > +2 < z, x >< y, w > +$

$+ < z, x >< w, w >$

$$\Downarrow$$

$< zy, xw > + < zw, xy >= 2 < z, x >< y, w >$

$$\Downarrow$$

$< xy, zw > + < xw, zy >= 2 < x, z >< y, w >$

De esta última expresión sólo necesitaremos tres casos:

$$Caso\ 1 : < e, x >< y, y >=< y, xy >;\ Caso\ 1' : < x, x >< e, w >=< x, xw >$$

y

$$Caso\ 2 :\ 2 < z, e >< y, e >=< zy, e > + < z, y >$$

Ahora, sea $V$ el subespacio $(\mathbb{R}e)^{\perp}$ de $A = \mathbb{R}e \oplus (\mathbb{R}e)^{\perp}$ y definamos una operación $\times$ : $V \times V \to V$ por:

$$a \times b = ab + < a, b > e$$

Veamos que este producto verifica los cinco axiomas :

- $\times$ verifica el Ax.2 ya que: $a \times (b+c) = a(b+c) + < a, b+c > e = ab + < a, b > e + ac + < a, c > e = (a \times b) + (a \times c)$

- $\times$ verifica el Ax.3 ya que: $\lambda(a \times b) = \lambda(ab + < a, b > e) = \lambda ab + \lambda < a, b > e = \lambda ab + < \lambda a, b > e = (\lambda a) \times b$

- $\times$ verifica el Ax.4 ya que:

  – $< a \times b, b >=< ab + < a, b > e, b >=< ab, b > + << a, b > e, b >=$

$< ab, b > + < a, b >< e, b >=< ab, b >$ (ya que $< e, b >= 0$)

$=< e, a >< b, b >$ (por el $Caso$ 1)

$= 0$ (ya que $< e, a >= 0$)

– $< a, a \times b >=< a, ab + < a, b > e >=< a, ab > + < a, < a, b > e >=$

$=< a, ab > + < a, e >< a, b >=< a, ab >$ (ya que $< a, e >= 0$)

$=< e, b >< a, a >$ (por el $Caso$ 1)

$= 0$ (ya que $< e, b >= 0$)

Por lo tanto, $< a \times b, b >= 0 =< a, a \times b >$.

- $\times$ verifica el Ax.1 ya que:

  – $< -b \times a, b >=< -ba+ < -b, a > e, b >=< -ba, b > + < -b, a >< e, b >=$

  $=< -ba, b >$ (ya que $< e, b >= 0$)

  $=< e, -a >< b, b >$ (por el $Caso$ 1)

  $= 0$ (ya que $< e, -a >= 0$)

  – $< a, -b \times a >=< a, -ba+ < -b, a > e >=< a, -ba > + < a, e >< -b, a >=$

  $=< a, -ba >$ (ya que $< a, e >= 0$)

  $=< e, -b >< a, a >$ (por el $Caso$ 1)

  $= 0$ (ya que $< e, -b >= 0$)

  Por el Ax.4 sabemos que $< a \times b, b >= 0 =< a, a \times b >$ y ahora hemos visto que $< -b \times a, b >= 0 =< a, -b \times a >$. Entonces se tiene que $a \times b = -b \times a$.

- $\times$ verifica el Ax.5 ya que:

  $|a \times b|^2 =< a \times b, a \times b >=< ab + < a, b > e, ab + < a, b > e >=< ab, ab > + < ab, e >< a, b >$
  $+ < a, b >< e, ab > + < a, b >^2 < e, e >=< ab, ab > + < ab, e >< a, b > + < a, b >< e, ab >$
  $+ < a, b >^2$ (ya que $< e, e >= 1$)

  Por otro lado, se tiene que $< ab, e >= - < a, b >$ ya que:

  $< ab, e > + < a, b >= 2 < a, e >< b, e >$ (por el $Caso$ 2)

  $= 0$ (ya que $< a, e >=< b, e >= 0$)

De manera que:

$|a \times b|^2 = <ab, ab> - <a, b>^2 - <a, b>^2 + <a, b>^2 = <ab, ab> - <a, b>^2 =$

$= |a|^2|b|^2 - <a, b>^2$

Entonces aplicando el teorema anterior, se tiene que $dim_{\mathbb{R}}(V) = 0, 1, 3$ ó 7. De manera que, $dim_{\mathbb{R}}(A) = 1, 2, 4$ ó 8.

**Observación**: Se puede precisar más el teorema anterior y demostrar que si $A$ es un álgebra normada de dimensión finita sobre $\mathbb{R}$, entonces $A$ es isomorfa a $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ ó $\mathbb{O}$.

**Corolario (Teorema clásico de Hurwitz)**: Si $x_1, ..., x_n, y_1, ..., y_n$ son variables, entonces si existe una fórmula del tipo:

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = A_1^2 + \cdots + A_n^2$$

donde $A_1, ..., A_n$ son de la forma:

$$A_i = \sum_{j,k=1}^{n} c_{ijk} x_j y_k$$

con $c_{ijk} \in \mathbb{R}$, necesariamente $n = 1, 2, 4$ ó 8.

*Demostración*: Tomando $A = \mathbb{R}^n$ con el producto definido por $(x_1, ..., x_n)(y_1, ..., y_n) = (A_1, ..., A_n)$ y la norma euclídea, entonces se tiene que $A$ es un álgebra normada. Aplicando el teorema anterior, la dimensión de $A$ sólo puede ser $1, 2, 4$ ó 8.

# 7 Bibliografía


1. A.A.Albert., "Studies in modern algebra", *The Mathematical Asociation of America* Vol. 2 (1963).

2. Andrew J.Hanson., "Visualizing Quaternions" *Series in interactive 3D tecnhology*, Elsevier (2006).

3. Bertram Walsh., "The Scarcity of Cross Products on Euclidean Spaces", *Classroom Notes*, The American Mathematical Monthly, Vol. 74, (1967), pp. 188-194.

4. H.-D.Ebbinghaus, H.Hermes, F.Hirzebruch, M.Koecher, K.Mainzer, J.Neukirch, A.Prestel, R.Remmert., "Numbers", *Graduate Texts in Mathematics, Reading in Mathematics*, Springer-Velarg (1983).

5. John C. Baez., "The Octonions", *Departament of Mathematics*, University of California (2001).

6. R.S.Palais., "The Classification of real division algebras", *Mathematical Notes*, The American Mathematical Monthly, Vol. 75, (1968), pp. 366-368.