PESQUIMAT 26(2): 1–10 (2023) ISSN:1560-912X/ ISSN-E:1609-8439
https://doi.org/10.15381/pesquimat.v26i2.25686 Facultad de Ciencias Matemáticas – UNMSM

Clasificación de Álgebras de División Reales

Wilber Carrillo Flores [1] *y Alberto Mariano Rivero Zapata*[2]

Resumen: Este artículo pretende ofrecer un enfoque unificador para la teoría básica de las álgebras de división presentando la investigación del matemático alemán-estadounidense Max August Zorn, quien clasificó las álgebras de división alternativas. En la sección 1 se desarrolla la teoría básica de las álgebras de división reales. En la sección 2 se presenta el Proceso de Cayley-Dickson, que consiste en construir una álgebra extensión a partir de una álgebra provista de una conjugación, similar a la construcción de los números complejos a partir de los números reales. En la sección 3 se presentan las álgebras de división clásicas $\mathbb{R}$ (reales), $\mathbb{C}$ (complejos), $\mathbb{H}$ (cuaterniones) y $\mathbb{O}$ (octoniones) y se mencionan algunas de sus aplicaciones. En la sección 4 se presenta el teorema principal, que establece que las únicas (salvo isomorfismo) álgebras de división alternativas son: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$ (teorema de Zorn). Los teoremas de clasificación de las álgebras de división asociativas (Frobenius) y de las álgebras de división normadas (Hurwitz) se obtienen como corolarios del teorema de Zorn. Finalmente en la sección 5 se mencionan aplicaciones de las álgebras de división a la Geometría, Teoría de Números, Física Clásica, Física Moderna, Mecánica Cuántica y Criptografía.

Palabras clave: álgebra de división, conjugación, cuaternión, octonión.

Classification of Real Division Algebras

Abstract: This article aims to offer a unifying approach to the basic theory of division algebras by presenting the research of the German-American mathematician Max August Zorn, who classified alternative division algebras. In section 1 the basic theory of real division algebras is developed. Section 2 presents the Cayley-Dickson Process, which consists of constructing an extension algebra from an algebra provided with a conjugation, similar to the construction of complex numbers from real numbers. In Section 3 presents the classical division algebras $\mathbb{R}$ (real), $\mathbb{C}$ (complex), $\mathbb{H}$ (quaternions) and $\mathbb{O}$ (octonions) and mentions some of their applications. In section 4 the main theorem is presented, which establishes that the only (except isomorphism) alternative division algebras are: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$ (Zorn's theorem). The classification theorems of associative division algebras (Frobenius) and normed division algebras (Hurwitz) are obtained as corollaries of Zorn's theorem. Finally in section 5 applications of division algebras to Geometry, Number Theory, Classical Physics, Modern Physics, Quantum Mechanics and Cryptography are mentioned.

Keywords: algebra of division, conjugation, quaternion, octonion.

Recibido: 03/07/2023. *Aceptado:* 28/09/2023. *Publicado online:* 30/12/2023.

[1]UNMSM, Facultad de Ciencias Matemáticas. e-mail: wilber.carrillo_mat@unmsm.edu.pe
[2]UNMSM, Facultad de Ciencias Matemáticas, e-mail: ariveroz@unmsm.edu.pe

Introducción

En este artículo estudiaremos las álgebras de división sobre los números reales. El objetivo es establecer los teoremas de Frobenius, Hurwitz y Zorn, que clasifican: los $\mathbb{R}$-álgebras de división asociativas, normadas y alternativas respectivamente.

La clasificación de las álgebras de división reales comenzó en 1878, cuando Georg Frobenius demostró que existen exactamente tres de tales álgebras que son asociativas: los números reales $\mathbb{R}$, los números complejos $\mathbb{C}$ y los cuaterniones $\mathbb{H}$.

En 1898, 20 años después Adolph Hurwitz demostró que los octoniones $\mathbb{O}$ es la única álgebra de división real normada no asociativa.

En 1930, Max Zorn generalizó los resultados de Frobenius y Hurwitz, probando que $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$ son los únicas $\mathbb{R}$-álgebras de división alternativas.

En 1940 el topólogo Heinz Hopf demostró que (como espacios vectoriales) las $\mathbb{R}$-álgebras de división tienen necesariamente dimensión 2^n para algún entero $n \geq 0$. Por supuesto, los cuatro ejemplos clásicos muestran la existencia de $\mathbb{R}$-álgebras de división en dimensiones 1, 2, 4 y 8.

En 1958, Raoul Bott y John Milnor, e independientemente Michel Kervaire , probaron un resultado profundo que se conoce como el **(1, 2, 4, 8) Teorema :** si A es una $\mathbb{R}$-álgebra de división , entonces dim A = 1, 2, 4, 8.

1. Álgebras Reales o $\mathbb{R}$-Álgebras

Esta sección está basada en la sección 1 de [1].

Definición 1.1 *Una álgebra real o una $\mathbb{R}$-álgebra es una 4-upla ordenada $(A, +, \mu, m)$ que satisface las siguientes condiciones :*
(i) *$(A, +, \mu)$ es un espacio vectorial real , y*
(ii) *$m : A \times A \longrightarrow A$ es un mapeo bilineal , llamado multiplicación.*

(Se denota por $m(x, y) = xy$ para cualesquiera x , y en A).
Usualmente, por abuso de notación, se escribe: sea A una $\mathbb{R}$-álgebra, sobreentendiendo que es una 4-upla.

1.1. $\mathbb{R}$-Álgebras de División Normadas

Es importante resaltar que existen tres niveles de asociatividad. Una álgebra es fuertemente asociativa si la subálgebra generada por cualquier elemento es asociativa. Es alternativa si la subálgebra generada por cualesquiera dos elementos es asociativa. Finalmente, es asociativa si la subálgebra generada por cualesquiera tres elementos es asociativa.

Definición 1.2 *Una $\mathbb{R}$-álgebra $(A, +, \mu, m)$ es :*
***(a) alternativa** , si $\forall (x, y) \in A \times A : x(xy) = (xx)y$.*
***(b) asociativa** , si la multiplicación m es asociativa.*
***(c) de división** , si $A \neq 0$ y $\forall (x, y) \in A \times A : (xy = 0$ implica $(x = 0$ o $y = 0)$).*
***(d) conmutativa** , si la multiplicación m es conmutativa.*
***(e) unitaria** , si existe un elemento neutro multliplicativo.*

Definición 1.3 *Sea A una $\mathbb{R}$-álgebra unitaria. Se dice que A es una **álgebra de división normada** si A es de división y existe un producto interno $\langle , \rangle$ sobre A tal que*

$$\forall (x, y) \in A \times A : \langle xy, xy \rangle = \langle x, x \rangle \langle y, y \rangle \qquad (1)$$

Observación: El producto interno $\langle , \rangle$ induce una norma $\| \|$ definida por

$$\|x\| = \sqrt{\langle x, x \rangle}$$

(1) es equivalente a la siguiente condición :

$$\forall (x, y) \in A \times A : \|xy\| = \|x\| \, \|y\|$$

En este caso se dice que **la norma permite composición**.

Lema 1.1 *Toda álgebra real alternativa tiene las siguientes propiedades :*
***(i) la ley "flexible" :** $x(yx) = (xy)x$, para cualesquiera $x, y \in A$.*
***(ii) la identidad de Moufang :** $(zx)(yz) = z(xy)z$, para cualesquiera $x, y, z \in A$.*
Si definimos x^n para $n \in \mathbb{Z}^+$ recursivamente por $x^1 = x, \ldots, x^{n+1} = x^n x$, entonces
***(iii)** $x^m x^n = x^{m+n}$ para cualesquiera $m, n \in \mathbb{Z}^+$*

Proposición 1.1 *Las siguientes afirmaciones sobre una álgebra real A , son equivalentes:*
***(i)** A es de división.*
***(ii)** $A \neq 0$ y para cualesquiera $a, b \in A$, con $b \neq 0$, las ecuaciones $bx = a$ e $yb = a$ tienen soluciones únicas $x, y \in A$.*

Corolario 1.1 *Sea A una $\mathbb{R}$-álgebra de división. Si A es alternativa, entonces A es unitaria.*

Proposición 1.2 *Si A es una $\mathbb{R}$-álgebra de división normada, entonces A es alternativa.*

La demostración de la proposición 1.2 la podemos ver en la pagina 17 de [1].

1.2. Conjugación sobre una $\mathbb{R}$-álgebra

Definición 1.4 *Sea A una $\mathbb{R}$-álgebra. Una **conjugación** sobre A es un mapeo $x \longrightarrow x^*$ de A en sí misma que satisface las siguientes condiciones:*
(i) $\forall x \in A : (x^*)^* = x$;
(ii) $\forall (x, y) \in A \times A : (xy)^* = y^* x^*$
El par ordenado $(A, *)$ es llamado una $*$- álgebra.

Se dice que una $*$-álgebra A es
(i) real si $\forall x \in A : x^* = x$;
(ii) es adecuadamente normada si $\forall x \in A : x + x^* \in \mathbb{R}$ y $xx^* = x^*x > 0$ si $x \neq 0$
Si A es adecuadamente normada, se definen $Re(x) = \dfrac{(x + x^*)}{2}$ e $Im(x) = \dfrac{(x - x^*)}{2}$ y se define la norma sobre A como $\|x\| = \sqrt{xx^*}$, además
A tiene inversos multiplicativos dados por $x^{-1} = \dfrac{x^*}{\|x\|^2}$

2. El Proceso de Cayley-Dickson

En esta sección la referencia es la sección 3 de [1] y 2.4 de [4].

2.1. Extensiones de Cayley-Dickson

Definición 2.1 *Sea A una $*$-álgebra. **La extensión de Cayley-Dickson**, denotada A', es la $*$-álgebra $A \times A$ con las siguientes operaciones:*
(1) Conjugación: $(a, b)^* = (a^*, b)$
(2) Adición: $(a, b) + (c, d) = (a + c, b + d)$
(3) Multiplicación por escalares: $\lambda(a, b) = (\lambda a, \lambda b)$
(4) Multiplicación: $(a, b)(c, d) = (ac – db^*, a^*d + cb)$
para cualesquiera $a, b, c, d \in A$, $\lambda \in \mathbb{R}$.

Denotando $A' = A \oplus A$, se tiene las álgebras de división clásicas: $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}$ (números complejos), $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}$ (cuaterniones) y $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}$ (octoniones) salvo isomorfismo.

2.2. Propiedades de las extensions de Cayley-Dickson

Teorema 2.1 *Para toda $*$-álgebra A se tiene:*
(i) *A' es real solo si $A = 0$.*
(ii) *A es real (y por lo tanto conmutativa) $\Longleftrightarrow$ A' es conmutativa.*
(iii) *A es conmutativa y asociativa $\Longleftrightarrow$ A' es asociativa.*
(iv) *A es asociativa y bien-normada $\Longleftrightarrow$ A' es alternativa y bien-normada.*
(v) *A es bien-normada $\Longleftrightarrow$ A' es bien-normada.*

Corolario 2.1 ***(a)*** *$\mathbb{R}$ es una $*$-álgebra adecuadamente normada conmutativa y asociativa.*
(b) *$\mathbb{C}$ es una $*$-álgebra adecuadamente normada conmutativa y asociativa.*
(c) *$\mathbb{H}$ es una $*$-álgebra adecuadamente normada asociativa.*
(d) *$\mathbb{O}$ es una $*$-álgebra adecuadamente normada alternativa.*
Por lo tanto $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$ son $\mathbb{R}$-álgebras de división.

3. Las $\mathbb{R}$-Álgebras de División Clásicas

Las álgebras de división reales clásicas son $\mathbb{R}$ (los números reales), $\mathbb{C}$ (los números complejos), $\mathbb{H}$ (los cuaterniones) y $\mathbb{O}$ (los octoniones o números de Cayley).

Lema 3.1 *En las $\mathbb{R}$-álgebras $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$ existen conjugaciones que preservan la adición, es decir, en $A = \mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$:*

$$\forall (x, y) \in A \times A : \overline{x + y} = \bar{x} + \bar{y}$$

Además el mapeo

$$x \longrightarrow \|x\| = \sqrt{x\bar{x}}$$

define una norma en A.

Proposición 3.1 *En $A = \mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$, el mapeo*

$$(x, y) \longrightarrow \langle x, y \rangle = \frac{1}{2}(x\bar{y} + y\bar{x})$$

De $A \times A$ en $\mathbb{R}$ define un producto interno.
Además $(A, \langle , \rangle)$ es una R-álgebra de división normada.

Demostración. Sea $(x, y) \in A \times A$ arbitrario. Como $\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x, y \rangle$, entonces

$$\begin{aligned}
\langle x, y \rangle &= \frac{1}{2}\left(\|x + y\|^2 - \|x\|^2 - \|y\|^2\right) \\
&= \frac{1}{2}\left((x + y)\overline{(x + y)} - x\bar{x} - y\bar{y}\right) \\
&= \frac{1}{2}\left((x + y)(\bar{x} + \bar{y}) - x\bar{x} - y\bar{y}\right) \\
&= \frac{1}{2}\left(x\bar{y} + y\bar{x}\right)
\end{aligned}$$

Ahora veamos que $\langle x, y \rangle \langle x, y \rangle = \langle x, x \rangle \langle y, y \rangle$
En efecto:

$$\begin{aligned}
\langle x, x \rangle &= \frac{1}{2}\left(x\bar{x} + x\bar{x}\right) \\
&= x\bar{x}
\end{aligned}$$

Como $x, y, \bar{x}$ e $\bar{y}$ son elementos de la álgebra asociativa generada por $Im(x)$ e $Im(y)$, entonces

$$\begin{aligned}
\langle x, y \rangle \langle x, y \rangle &= (xy)\overline{(xy)} \\
&= (xy)(\bar{y}\bar{x}) \\
&= x(y\bar{y})\bar{x} \\
&= x \langle y, y \rangle \bar{x} \\
&= x\bar{x} \langle y, y \rangle \\
&= \langle x, x \rangle \langle y, y \rangle
\end{aligned}$$

3.1. Los Cuaterniones

En 1835, el matemático William Rowan Hamilton descubrió cómo tratar a los números complejos como parejas de números reales, hecho que relacionó a $\mathbb{C}$ con el plano y por ello, durante muchos años buscó inventar una álgebra más grande que pudiera relacionarse con la geometría tridimensional. Así, en 1843 descubrió la regla principal de los cuaterniones: $i^2 = j^2 = k^2 = ijk = -1$; y el resto de su vida lo dedicó a estudiarlos junto con sus aplicaciones a la geometría. Dada una base $1, q_2, q_3, q_4$ de $\mathbb{H}$ en la que, para $i, j, k = 1, 2, 3$

$$\begin{aligned}
1q_i = q_i 1 = q_i, \\
q_i^2 = q_j^2 = q_k^2 = -1, \\
q_i q_j = -q_j q_i, \\
(q_i q_j) q_k = q_i (q_j q_k), \\
q_i q_{i+1} = q_{i+2}.
\end{aligned}$$

Para visualizar el comportamiento de estos elementos se presenta el siguiente cuadro en el que el elemento de la intersección de la m-ésima fila con la n-ésima columna es el resultado de multiplicar el elemento de la m-ésima fila con la n-ésima columna, para $m, n = 1, ..., 4$.

.	1	q_1	q_2	q_3
1	1	q_1	q_2	q_3
q_1	q_1	-1	q_3	$-q_2$
q_2	q_2	$-q_3$	-1	q_1
q_3	q_3	$-q_2$	$-q_1$	-1

Cuadro 1: Tabla de multiplicación en $\mathbb{H}$. El elemento ubicado en la intersección de la fila m-ésima y la columna n-ésima con $m, n = 1, ..., 4$ es el resultado de multiplicar el elemento de la fila m-ésima y la columna n-ésima.

Los cuaterniones se pueden expresar como pares de números complejos. Los cuaterniones $a + bi + cj + dk$ se pueden escribir de la siguiente forma

$$a + bi + cj + dk = a + bi + cj + dij = (a + bi) + (c + di)j = z_1 + z_2 j$$

con z_1 y z_2 números complejos.
Para demostrar que el producto de cuaterniones es asociativo se utilizará la notación compleja y las propiedades de la operación conjugación de números complejos (conjugado de la suma es suma de conjugados y conjugado del producto es producto de conjugados) y la siguiente identidad:

$$z_1 j = (a + bi)j = aj + bk = ja - jib = j(a - bi) = j\bar{z_1}$$

El producto de cuaternios en forma compleja será, por consiguiente:

$$(z_1 + z_2 j)(w_1 + w_2 j) = (z_1 w_1 - z_2 \bar{w_2})(z_1 w_2 + z_2 \bar{w_1})j$$

y a partir de aquí, fácilmente se prueban las propiedades asociativa del producto y la distributiva del producto respecto a la suma.

3.2. Los Octoniones

Hamilton compartió su descubrimiento con John T. Graves por medio de una carta de 8 páginas, en la que describía todo lo relativo a los cuaterniones. En diciembre del mismo año, Graves respondió a la carta con una en la que mostraba el comportamiento de la álgebra 8-dimensional, a la cual llamaba "octaves". Allí demostró que esta era una álgebra de división normada y la usó para expresar el producto de dos sumas de ocho cuadrados perfectos como otra suma de ocho cuadrados perfectos (lo que se conoce como el teorema de los 8 cuadrados, que previamente había sido descubierto por el matemático danés Carl Ferdinand Degen).
Por otro lado, Arthur Cayley venía trabajando en los cuaterniones desde que Hamilton anunció su existencia y empezó a profundizar en la relación con las funciones hiperelípticas y es en marzo de 1845 cuando publica un artículo en el Philosophical Magazine con sus resultados y como soporte de ellos, da una breve descripción de los octoniones y a partir de esto, los octoniones se conocen como los números de Cayley.
Los octoniones ($\mathbb{O}$) se obtienen al duplicar los cuaterniones ($\mathbb{H}$), es decir, $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}$ y a su vez los cuaterniones al duplicar los complejos $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}$. Luego pueden considerarse como 8-uplas de números reales, donde cada octonión es una combinación lineal sobre $\mathbb{R}$ de las llamadas unidades del octonión $e_0; e_1; e_2; e_3; e_4; e_5; e_6; e_7$; donde e_0 es la unidad escalar y puede identificarse con el 1, y las reglas de suma y multiplicación pueden derivarse de las mismas operaciones para cuaterniones. De esta forma se obtienen 480 posibles definiciones para la multiplicación de octoniones,

aunque las álgebras resultantes son isomorfas entre sí y realmente no es importante mirar qué regla de multiplicación se utiliza. Así definidos, los octoniones resultan ser una álgebra de división no conmutativa ni asociativa, de hecho, junto con $\mathbb{R}, \mathbb{C}$ y $\mathbb{H}$ resultan ser las únicas álgebras de división de dimensión finita (teorema de Hurwitz) y cuentan con propiedades interesantes de analizar y estudiar.
Aunque los octoniones pasaron desapercibidos durante muchos años por su aparente falta de aplicación y relación con la física y la geometría, últimamente se han encontrado relaciones con los grupos de Lie, la teoría de cuerdas, la relatividad especial, la lógica cuántica e incluso con el procesamiento de señales (relacionado con series de Fourier), lo que los ha vuelto más populares en las áreas de estudio de la matemática.

3.2.1. Álgebra de Octoniones

Los elementos de $\mathbb{O}$ son expresiones de la forma

$$x = x_\infty + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7$$

con $x_t \in \mathbb{R}$ para $0 \leq t \leq 1$ y $x_\infty = Re(x)$, el cual constituye el álgebra sobre los reales generados por unidades $e_1, ..., e_7$ que satisfacen

$$\begin{aligned} e_i^2 &= -1 \\ e_ie_j &= -e_je_i \\ (e_ie_j)e_k &= -e_i(e_je_k) \end{aligned}$$

para $1 \leq i \leq 7$ y todos los índices en módulo 7.
Por otro lado, el conjugado de un octonión x está dado por

$$\bar{x} = x_\infty - x_1e_1 - x_2e_2 - x_3e_3 - x_4e_4 - x_5e_5 - x_6e_6 - x_7e_7$$

y dados dos octoniones x y y es sencillo comprobar que $\overline{xy} = \bar{y}\bar{x}$. También es posible definir su módulo

$$|x|^2 = x\bar{x} = x_\infty^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2$$

4. Clasificación de las Álgebras de División Reales Alternativas

En esta sección consideramos el teorema principal. Este teorema de Max August Zorn , publicado en 1930 , generalizó los resultados de Frobenius (clasificación de $\mathbb{R}$-álgebras de división asociativas) y de Hurwitz (clasificación de $\mathbb{R}$-álgebras de división normadas), probando que $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$ son las únicas (salvo isomorfismo) $\mathbb{R}$-álgebras de división alternativas; y esto implica como consecuencias inmediatas los teoremas de Frobenius y de Hurwitz. Max August Zorn fue un matemático alemán nacionalizado estadounidense. Trabajó en las áreas del álgebra abstracta, teoría de grupos y análisis numérico. Es famoso por el lema de Zorn, una herramienta poderosa de teoría de conjuntos, que se puede aplicar a un amplio abanico de artefactos matemáticos como espacios vectoriales, conjuntos ordenados, etc. El lema de Zorn fue descubierto por primera vez por Kazimierz Kuratowski en 1922, y después de forma independiente, por Zorn en 1935.

En lo que sigue, D denotará una $\mathbb{R}$-álgebra de división alternativa fija.

Lema 4.1 *Si $x \in D$, entonces $x^2 \in Rx + R$ (aquí R es naturalmente isomorfa a la imagen del mapeo $\lambda \longrightarrow \lambda 1$, de $\mathbb{R}$ en D)*

Lema 4.2 *Si $D \neq R$, entonces existe $i \in D$ tal que $i^2 = -1$ y $C := R + Ri$ es una $\mathbb{R}$-álgebra isomorfa a $\mathbb{C}$, la $\mathbb{R}$-álgebra de los números complejos. Se tiene $C = \{x \in D : xi = ix\}$, y denotando $C^- := \{x \in D : xi = -ix\}$, resulta $D = C \oplus C^-$*

Lema 4.3 *Si $x, y \in D$ anticonmutan, entonces x^2 e y conmutan.*

Lema 4.4 *Si $x, y \in D$ anticonmutan, entonces $x(yz) = -y(xz)$ y $(zx)y = -(zy)x$ para todo $z \in D$.*

Lema 4.5 *Si $D \not\subseteq C$, entonces existe $j \in C^-$ tal que $j^2 = -1$, y $H := C + Cj$ es isomorfo a $\mathbb{H}$. Además, escribiendo $k := ij$, $H = \{x \in D : xk = (xi)j\}$, y haciendo $H^- := \{x \in D : xk = -(xi)j\}$ tenemos $D = H \oplus H^-$.*

Lema 4.6 *Si $x \in H^-$, entonces x anticonmuta con i, j y k.*

Lema 4.7 *Si $D \not\subseteq H$, entonces existe $h \in H^-$ tal que $h^2 = -1$.*

Teorema 4.1 (Zorn) *Si A es una álgebra de división real alternativa , entonces A es isomorfa a una de las siguientes álgebras : $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$*

Bosquejo de la demostración: Apliquemos el marco estructural anterior con D = A.
Si $D = \mathbb{R}$, no hay nada que probar, por el lema 4.1. En caso contrario , D contiene una $\mathbb{R}$-álgebra isomorfa a $\mathbb{C}$, por el lema 4.2.
Si $D = \mathbb{C}$, no hay nada que probar. En caso contrario, por el lema 4.5, D contiene una $\mathbb{R}$-álgebra isomorfa a $\mathbb{H}$.
Si $D = \mathbb{H}$, entonces no hay nada que probar. Ahora supongamos que D no está contenida en $\mathbb{H}$. En este caso, por los lemas 4.5 y 4.7, $D = H \oplus H^-$ y existe $h \in H^-$ tal que $h^2 = -1$. El mapeo $T : D \longrightarrow D$ definido por $T(x) = xh$ define un automorfismo lineal. Como D es alternativa , entonces T tiene un inverso T^{-1}, definido por $T^{-1}(x) = -xh$. Se observa que T intercambia H y H^-. Por lo tanto $dim(H^-) = dim(H) = 4$ y en consecuencia $dim(D) = 8, H^- = Hh, \{h, ih, jh, kh\}$ es una base de H^- y $\{1, i, j, k, h, ih, jh, kh\}$ es una base de D. Calculando la tabla de multiplicación para esta base, se comprueba que D es isomorfa a $\mathbb{O}$.

Corolario 4.1 (Frobenius) *Si A es una $\mathbb{R}$-álgebra de división asociativa, entonces A es isomorfa a una de las siguientes álgebras: $\mathbb{R}, \mathbb{C}, \mathbb{H}$.*

Demostración. Como A es asociativa, entonces es alternativa. Por el teorema de Zorn, A es isomorfa a una de las siguientes álgebras: $\mathbb{R}, \mathbb{C}, \mathbb{H}$, pues $\mathbb{O}$ (octoniones) no es asociativa.

Corolario 4.2 (Hurwitz) *Si A es una $\mathbb{R}$-álgebra de division normada, entonces A es isomorfa a una de las siguientes álgebras: $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$.*

Demostración. Por la proposición 1.2, A es alternativa; luego por el teorema de Zorn, A es isomorfa a una de las siguientes álgebras: $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$.

5. Aplicaciones

Algunas aplicaciones de las álgebras de división normadas: $\mathbb{R}, \mathbb{C}, \mathbb{H}$ y $\mathbb{O}$ son las siguientes:
(1) Describir unificadamente estructuras geométricas sobre variedades Riemannianas. Ver Geometric Structures on Riemannian Manifolds , Naichung Conan Leung , Survey in Differential Geometry XVI.
(2) Probar en teoría de números, por ejemplo, el teorema de Lagrange que establece que todo número natural puede expresarse como suma de cuatro cuadrados perfectos. Ver Cuaterniones un tema de Teoría de Números Revista N 21 Octubre 2010 sección temas de Matemática, www.mendomatica.mendoza.edu.ar
(3) Representar rotaciones en el espacio tridimensional , con representaciones no singulares más compactas y más rápidas , comparadas con las representaciones matriciales.
(4) Representar, en gráficos por computadora, la orientación de un objeto en un espacio tridimensional.

5.1. Álgebras en la Física Clásica

En 1679, después de conocer la geometría analítica creada por Descartes y Fermat , Leibnitz le manifiesta a Huygens lo siguiente: "la Física no podrá avanzar más , a no ser que se encuentre un nuevo método de análisis más geométrico , que permita expresar y operar con direcciones tan directamente como el álgebra (de los números reales) representa y opera con las magnitudes (el concepto de longitud en la geometría analítica) " Leibnitz, en la búsqueda de un modelo matemático apropiado para el desarrollo de la Física, entreveía el Álgebra Geométrica creada por Clifford entre los años 1873 y 1879 conjugando las álgebras de Hamilton (1843) y de Grassmann (1844). El Álgebra Geométrica unifica y simplifica el estudio y aplicación de los Complejos y Cuaterniones.
En el siglo XX, en 1920, Heisenberg manifiesta que la Física requiere una matemática completamente nueva que incluya álgebras no conmutativas. En respuesta a esto Pauli y Dirac recrean el Álgebra Geométrica recurriendo a Álgebras de Matrices. En 1966 aparece el aporte de Hestenes (D. Hestenes Space-Time Algebra , Gordon and Breach 1966 y D. Hestenes New Foundations for Classical Mechanics , Kluwer Academic Publishers 1993) (una " álgebra de matrices sin matrices ").

5.2. Modelos para la Formulación de la Mecánica Cuántica

Diversas clases de objetos algebraicos nos ayudan a formular modelos que nos permiten entender mejor fenómenos físicos, como las álgebras de Clifford para describir el espín, y los números complejos en la formulación de la Mecánica Cuántica. Intentos de hacer una cuantización de la gravedad se han llevado a cabo con una Relatividad General compleja. Al construir modelos que describen tales fenómenos físicos, el introducir un sistema de números diferente a los números reales tales como los cuaterniones y los octoniones, por ejemplo, producen diversas soluciones a estos modelos. Las álgebras de Jordan se introdujeron en un intento por encontrar una formulación de la Mecánica Cuántica que aliviara lo siguiente:
1. Producto de matrices Hermíticas no es Hermítica, a menos que conmuten.
2. Producto por un escalar no es Hermítico, a menos que el escalar sea real.

5.3. Los Cuaterniones y los Octoniones en la Criptografía

La criptografía se refiere a la ciencia o arte de diseñar criptosistemas. Su principal propósito es la protección de los intereses de las partes de una comunicación. Un criptosistema es un dispositivo diseñado para brindar tal protección. Se encripta la información de manera que solo pueda ser utilizada por quien esté autorizado.
La criptografía puede dividirse, en dos ramas: **simétrica**, que encripta y desencripta los mensajes con una única clave compartida,y **asimétrica**, que por un lado logra el intercambio seguro de claves y por el otro elcifrado de mensajes usando una clave pública y otra privada, hoy día con herramientas de la teoría de números. El uso de números hipercomplejos que forman algebras no conmutativas, para su uso en PQC (Criptografía Post Cuantica) se limita entonces, a cuaterniones y octoniones (ver[2]).

6. Conclusión

Se logró el objetivo de unificar la teoría básica de las $\mathbb{R}$-álgebras de división centrando el desarrollo en la teoria básica de las $\mathbb{R}$-álgebras de división alternativas y se ha motivado su estudio mencionando aplicaciones a la Geometría, Teoría de números, Física Clásica , Física Teórica Moderna, Computación y Criptografía.
En conclusión, el Teorema de Zorn resume todos los resultados teóricos alcanzados.

Referencias bibliográficas

[1] Badger Matthew. *Division Algebras over the Real Numbers*. University of Pittsburg.

[2] Kamlofsky , Jorge A. – Hecht Juan P (2017). *Post-Quantum Cryptography Using Hyper-Complex Numbers*. Universidad de Buenos Aires, Argentina, XXIII Congreso Argentino de Ciencias de la Computación.

[3] Martinez-Merino, Aldo (2017). *Números Hiper-Complejos y su relación con la Física, Universidad de Guanajuato México*.

[4] Moreno Garzon, Andres R. – Toquica Arenas, Diana A. (2019). *Octoniones : construcción, geometría y aplicaciones*.

[5] Rodriguez Bouza , Victor. *Sobre los Cuaterniones, Algebras de Lie y Matrices de Pauli, Teoria Basica y Aplicaciones, Métodos Matemáticos I*.

[6] Sanchez Muñoz, José M. (2011). *Historias de Matemática, Hamilton y el Descubrimiento de los Cuaterniones, Revista de Investigación Pensmiento Matemático*.

[7] Vera, Edgar (2018). *¿ Física Teórica y Octoniones ?*. UNMSM, Lima-Perú.