Universidad Nacional Autónoma
de México

Facultad de Ciencias

Una familia compleja: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$
Sistemas numéricos y sus geometrías

T E S I S

PARA OBTENER EL TÍTULO DE:

Matemático

QUE PRESENTA:

Isvi René Aguilar Sánchez

TUTOR:

Dr. Pierre Michel Bayard

Ciudad Universitaria, Cd. Mx., 2022

Agradecimientos

לך אלי: לך אלי תשוקתי בך חשקי ואהבתי לך לבי וכליותיי לך רוחי ונשמתי ...

Expreso mi profundo y pleno agradecimiento a todo lo que hace posible que esté aquí, a quienes desde antes que naciera me esperaron y me brindaron la oportunidad de estar, me guiaron y me colmaron de incontables disposiciones para mi crecimiento, así como con quienes compartí este crecimiento. A quienes, sin saberlo o quizá sí, sembraron una semilla en mi jardín que tal vez no pudieron ver, pero ahora es un fascinante árbol, aún con muchos frutos por dar y madurar. A quienes la providencia acercó nuestros caminos y con quienes comparto esta hermosa experiencia de estar vivo... cual gotas de agua en el océano, me compartieron la inmensidad y también fueron un motivo para culminar esta etapa y comenzar otro ciclo... A quien me inspiró a seguir el camino del corazón y con quien ha resultado natural y genuino compartir la vida...

El tema y el impulso inicial para iniciar este trabajo fue debido, respectivamente, a Andrés G. por su trabajo de tesis sobre rotaciones y cuaterniones, y a Bernardo F. por su insistencia, antídoto contra mi desidia de ese entonces. A Pierre M. Bayard quien amablemente aceptó ser mi tutor, con quien pude compartir el gusto por el tema presentado.

Agradezco a todos los que amablemente comparten información, contestan preguntas y aclaran dudas sobre multitud de temas en el famoso internet, facilitando y agilizando en varios aspectos y niveles este trabajo, desde precisiones teóricas concernientes a las matemáticas, hasta cuestiones técnicas en cuanto al formato y la presentación.

הללויה אודה יהוה בכל־לבב בסוד ישרים ועדה

גדלים מעשי יהוה דרושים לכל־חפציהם

הוד־והדר פעלו וצדקתו עמדת לעד

זכר עשה לנפלאותיו חנון ורחום יהוה

טרף נתן ליראיו יזכר לעולם בריתו

כח מעשיו הגיד לעמו לתת להם נחלת גוים

מעשי ידיו אמת ומשפט נאמנים כל־פקודיו

סמוכים לעד לעולם עשוים באמת וישר

פדות שלח לעמו צוה־לעולם בריתו קדוש ונורא שמו

ראשית חכמה יראת יהוה שכל טוב לכל־עשיהם תהלתו עמדת לעד

CONTENIDO

1

INTRODUCCIÓN

Se puede afirmar que los números han sido una herramienta indispensable a lo largo de la historia de la humanidad. Desde contar a la idea abstracta de cantidad, pasando por la ordenación. Llegando a propuestas tan interesantes como equiparar una versión «un poco más elaborada» de los números reales, $\mathbb{R}^3$, con el espacio en el que habitamos; o incluso con $\mathbb{R}^4$ en la teoría de relatividad, eso sí, con una estructura más «compleja», en la que también literalmente tienen que ver los números complejos, sistema de números que expande las posibilidades de los reales, mediante una unidad imaginaria i. De hecho, este sistema $\mathbb{C}$, también tiene un papel protagónico en la teoría cuántica. No sobra mencionar que son las dos ramas de la física moderna protagónicas en estos tiempos. Sin embargo, la cosa no termina aquí, pues resulta que otro sistema que incluye tres unidades imaginarias, que por cierto resultó ser de gran utilidad también para la física y en la teoría de espacios vectoriales a tal nivel que por éste se debe el uso de la ahora tradicional notación de i, j, k para los vectores básicos ortonormales de $\mathbb{R}^3$, dicho sistema es el de los cuaterniones: $\mathbb{H}$. Si tres unidades imaginarias resultaron interesantes, ¿podremos considerar más, cuántas más? La respuesta depende, como muchas cosas, de cuánto estamos dispuestos a dejar. Un punto que parece apenas razonable es perder la asociatividad, una propiedad por demás práctica, esto pasa con siete unidades imaginarias en los llamados octoniones: $\mathbb{O}$. ¿Por qué interesarnos en todo esto? Basta responder que por gusto, pero podemos ahondar en explicaciones: con cada generalización que puede hacerse, podemos notar (a veces) con más claridad propiedades que podrían parecer sosas en un principio; basta traer a colación la historia de «Planilandia» y cómo ver las cosas desde «arriba» nos permite notar más detalles que antes; cada sistema incluye a los anteriores, por lo que encontramos nuevas maneras de reconocer lo que ya conocíamos. Y finalmente para las mentes pragmáticas, ya hemos mencionado que estos sistemas numéricos han servido a la física de manera fructífera, y los octoniones no son la excepción, de hecho hay quienes han visto en éstos una posible conexión entre la ahora famosa teoría de cuerdas con su propuesta de espacio de diez dimensiones y ciertas simetrías de un espacio proyectivo de $\mathbb{O}$.

Daremos un breve paseo por algunas de las propiedades de estos sistemas, en particular los octoniones. Nos hemos inspirado en las exposiciones de John C. Baez (2002, *The Octonions*), y Tevian Dray y Corinne A. Manogue (2015, *The Geometry of the Octonions*). Complementando la exposición al situarla en un contexto general, siguiendo a Schafer (1966) y Voight (2021). Finalmente, mencionamos que uno de los objetivos de este texto es servir como presentación o introducción a estos sistemas numéricos, para quienes estén interesados más en la parte concreta, pueden lanzarse directamente a la segunda parte de este texto donde se presentan las propiedades básicas, así como algunas interpretaciones geométricas, de $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$, incluyendo cómo tratar con álgebras que no son conmutativas como $\mathbb{H}$ o ni siquiera asociativas, pero sí alternativas como $\mathbb{O}$, al respecto de estos últimos aspectos se pueden encontrar más detalles en la primera parte del texto, misma donde quienes estén más interesados en la parte abstracta de la construcción de estás álgebras y posibles generalizaciones teóricas podrán encontrar un detallado tratamiento. En la parte de apéndices pueden encontrarse algunas definiciones y propiedades que se usan en las primeras partes y que podrían considerar como requerimientos mínimos para seguir la exposición del texto, y que ahora mencionamos: nociones básicas de teoría de conjuntos, álgebra lineal y una pizca de álgebra abstracta, en particular la de estructuras algebraicas como grupos, anillos y módulos.

Nota sobre el uso de estilos tipográficos enfáticos y de puntuación. Usamos **negrita** para resaltar palabras que se refieren a definiciones clave para la exposición, así fácilmente hallarlas; *inclinada* para nombres alternativos a definiciones clave o para definiciones secundarias, o bien simplemente enfatizar; y comillas «» para palabras o frases cuyo uso (no tan literal) se entiende por analogía, enfatizando que es una manera de expresarse. Finalmente, cuando hacemos una demostración, la colocamos entre los símbolos $\triangleright$ $\triangleleft$.

Parte I

CONSTRUCCIONES ABSTRACTAS GENERALES

2

ÁLGEBRAS

La idea es presentar el sistema de los octoniones, pasando por los complejos y cuaterniones, abriendo camino de la manera más general posible. Podríamos simplemente definirlos en unos cuantos pasos y ver qué propiedades resultan. Pero consideramos que esto sería como atrapar un ave y tratar de estudiarla en una jaula; ciertamente algo aprenderemos, pero adentrarnos en su hábitat y estudiarla ahí resultaría más enriquecedor, claro que tendríamos que enfrentarnos a algunos desafíos. En nuestro caso, el hábitat en el que nos aventuramos (en esta sección) es el de las álgebras abstractas, luego tendremos la oportunidad de capturar por un momento a nuestras aves y revisar sus alas y bello plumaje. Además de esta motivación, este enfoque tiene otra ventaja, situarlo en un contexto general, permite mostrar cómo se han generalizado nociones inspiradas en sistemas numéricos y el «estado de conocimiento» en el que se encuentra este tema.

2.1 PRIMERAS DEFINICIONES Y PROPIEDADES

A continuación comenzamos estableciendo algunas definiciones y algunos resultados importantes para las siguientes secciones. Vale mencionar que como es usual, cuando hablemos de estructuras algebraicas, para referirnos a un conjunto con una estructura usemos el mismo nombre del conjunto, por ejemplo, el campo de los números reales, lo denotamos como $\mathbb{R}$, en vez de $(\mathbb{R}, +, \cdot, 0, 1)$. Es un uso pragmático del lenguaje y fácilmente se puede distinguir si nos referimos al conjunto como tal o al conjunto con la estructura conforme al contexto.

En lo que sigue consideraremos un **campo** $(\mathbb{K}, +, , 0, 1)$, denotando su multiplicación, yuxtaponiendo los elementos en cuestión: ab. Vale mencionar que asumimos nociones básicas de la teoría de conjuntos y para nosotros $\mathbb{N} = \{0, 1, 2, ...\}$. Un repaso sobre estructuras algebraicas y álgebra lineal puede encontrarse en los apéndices al final, donde mencionamos con más detalle varias de las propiedades que en lo que sigue usaremos. Vale mencionar que seguimos el ya usual enfoque de la teoría de categorías, considerando estructuras y los morfismos que las preservan. La mayoría de las definiciones, así como algunos resultados que presentamos a continuación se basan en los textos de Voight (2021) y Schafer (1966), la exposición sigue más la de éste último y considera al primero para algunos detalles.

Un **álgebra** A sobre un campo $\mathbb{K}$ (o $\mathbb{K}$-álgebra) es un $\mathbb{K}$-espacio vectorial con una operación binaria $\mathbb{K}$-bilineal llamada producto o multiplicación (que denotaremos yuxtaponiendo el par de elementos y usando paréntesis cuando sea necesario), tal que $\forall a, b \in A$ y $\forall \lambda \in \mathbb{K}$:

(1) $a(b+c) = ab + ac$ y $(b+c)a = ba + ca$
leyes distributivas izquierda y derecha, respectivamente.

(2) $(\lambda a)b = \lambda(ab) = a(\lambda b)$ asociatividad con escalares.

Si además el producto es asociativo o conmutativo, se dice que el álgebra es asociativa o conmutativa, respectivamente. Si el producto tiene un neutro (o unidad; derecho e izquierdo), se denotará como e y el álgebra será llamada **unital**; cabe recordar que este neutro resulta ser único. Cuando sea claro a qué campo nos referimos podemos omitir mencionarlo; también omitiremos el uso de paréntesis cuando no haya ambigüedad, por ejemplo, por (2) podemos escribir simplemente λab. Más aún tenemos que $(\lambda_1 a)(\lambda_2 b) = (\lambda_1 \lambda_2)ab$, pues, por la asociatividad de la acción de escalares (propiedad de espacios vectoriales), tenemos que $(\lambda_1 a)(\lambda_2 b) = \lambda_1(a(\lambda_2 b)) = \lambda_1(\lambda_2 ab) = (\lambda_1 \lambda_2)ab$.

Una $\mathbb{K}$-**subálgebra** B de una $\mathbb{K}$-álgebra A es un subconjunto $B \subseteq A$ tal que al restringir las operaciones de A a B, resulta que éste es una $\mathbb{K}$-álgebra. Notemos que en el caso de álgebras unitales, $\mathbb{K}e = \{ke : k \in \mathbb{K}\} \subseteq A$ es una subálgebra de A. Un **ideal** (bilateral) es un subconjunto $I \subseteq A$ tal que cumple: i) $\forall x, y \in I$: $x - y \in I$, ii) $\forall a \in A$, $\forall x \in I$: $ax, xa \in I$. Un álgebra A tiene al menos dos ideales $\{0\}$ y la misma A, que llamamos triviales o impropios, cualquier otro ideal es llamado **ideal propio**, un álgebra con sólo dos ideales, es decir, sin ideales propios es llamada **simple**.

Un **morfismo** de $\mathbb{K}$-álgebras es una función $f : A \longrightarrow B$ entre $\mathbb{K}$-álgebras que preserva la suma, la acción por cualquier escalar en $\mathbb{K}$ y el producto, i. e. $f(a + a') = f(a) + f(a')$, $f(\lambda a) = \lambda f(a)$, y $f(ab) = f(a)f(b)$ (es decir es $\mathbb{K}$-lineal y preserva productos); si las álgebras son unitales, además ha de preservar las unidades: $f(e_A) = e_B$. Un **isomorfismo** entre dos álgebras es un morfismo $f : A \longrightarrow B$ de álgebras invertible (existe un morfismo inverso: $g : B \longrightarrow A$ tal que $f \circ g = Id_A$ y $g \circ f = Id_B$). Cuando exista un isomorfismo entre álgebras diremos que éstas son isomorfas y lo denotamos como $A \cong B$. De hecho tenemos un ejemplo, $\mathbb{K}$ mismo es una $\mathbb{K}$-álgebra con el producto y multiplicación con escalares coincidiendo, más aún $\mathbb{K} \cong \mathbb{K}e$: Consideremos la proyección $p : \mathbb{K}e \longrightarrow \mathbb{K}$ definida como $p(\lambda e) = \lambda$ y la «inclusión» $i : \mathbb{K} \longrightarrow \mathbb{K}e$, como $i(\lambda) = \lambda e$. Claramente una es inversa de la otra, veamos que son morfismos de álgebras. La $\mathbb{K}$-linealidad se tiene por las conocidas propiedades de asociación de escalares y distributividad de un espacio vectorial, tenemos, para $\kappa, \lambda_1, \lambda_2 \in \mathbb{K}$:

$$\begin{aligned} p\left(\kappa(\lambda_1 e) + \lambda_2 e\right) &= p\left((\kappa\lambda_1)e + \lambda_2 e\right) = p\left((\kappa\lambda_1 + \lambda_2)e\right) \\ &= \kappa\lambda_1 + \lambda_2 = \kappa p(\lambda_1 e) + p(\lambda_2 e), \text{ y} \end{aligned}$$

$$\begin{aligned} i\left(\kappa\lambda_1 + \lambda_2\right) &= \left(\kappa\lambda_1 + \lambda_2\right)e = \kappa\lambda_1 e + \lambda_2 e \\ &= \kappa(\lambda_1 e) + \lambda_2 e = \kappa i(\lambda_1) + i(\lambda_2). \end{aligned}$$

Y como $(\lambda_1 e)(\lambda_2 e) = (\lambda_1\lambda_2)e$, también preservan productos:

$$p\left((\lambda_1 e)(\lambda_2 e)\right) = p\left((\lambda_1\lambda_2)e\right) = \lambda_1\lambda_2 = p(\lambda_1 e)p(\lambda_2 e),$$

$$i(\lambda_1\lambda_2) = (\lambda_1\lambda_2)e = (\lambda_1 e)(\lambda_2 e) = i(\lambda_1)i(\lambda_2).$$

Finalmente, es claro que $p(e) = p(1e) = 1$ e $i(1) = 1e = e$ (que $\forall a \in A : 1a = a$ es una propiedad de espacio vectorial). Entonces cada álgebra unital tiene una «copia»isomorfa de $\mathbb{K}$ como subálgebra.

Dada una $\mathbb{K}$-álgebra A, definimos su **dimensión** como su dimensión como $\mathbb{K}$-espacio vectorial, la denotamos $\dim(A)$. Como tenemos la noción de que un subespacio vectorial puede ser generado por un conjunto de vectores, también tenemos una noción para álgebras: dado un conjunto finito $X = \{a_1, ..., a_n\} \subset A$ y una $\mathbb{K}$-subálgebra B de A, decimos que B es **generada** por X (o X genera a B) cuando B es la mínima subálgebra de A que contiene a X (considerando el orden dado por la contención); también tenemos la noción de (in)dependencia lineal y de base. Resulta interesante que al contar un álgebra con la noción de base, debido a (1) y (2), podemos caracterizar el producto en ésta a través de las **constantes de estructura** que aparecen en la expresión de los productos de los elementos de una base $\{a_1, ..., a_n\}$:

$$a_i a_j = \sum_{k=1}^{n} \lambda_{ijk} a_k,$$

siendo $\lambda_{ijk} \in \mathbb{K}$ las n^3 constantes de estructura (donde hemos supuesto que el álgebra tiene dimensión finita n) que dependen de dicha base. Para aclarar a qué nos referimos con caracterizar el producto consideremos $x = \sum_{i=1}^{n} x_i a_i$, $y = \sum_{i=1}^{n} y_i a_i$, con $x_i, y_i \in \mathbb{K}$ para $i \in \{1, ..., n\}$, así tenemos que

$$xy = (x_1 a_1 + ... + x_n a_n)(y_1 a_1 + ... + y_n a_n) = \sum_{j=1}^{n}\sum_{i=1}^{n} x_j y_i a_j a_i.$$

Con lo que nos basta conocer los productos $a_i a_j$ para conocer cualquier producto en el álgebra.

Como vemos, no requerimos propiedades como asociatividad o conmutatividad del producto, como a veces se suele definir. Así queda bien definido algo como $a^2 = aa$, pero resulta ambiguo lo que pueda significar a^3, si $a(aa)$ o $(aa)a$. Lo que sí, tenemos manera de «medir» qué tan conmutativo es un producto mediante el **conmutador**, $[-,-] : A \times A \longrightarrow A$, definido como $[a,b] = ab - ba$ (que resulta ser la función constante o si y sólo si el producto es conmutativo); también tenemos manera de hacerlo para la asociatividad, con el **asociador** $(-,-,-) : A \times A \times A \longrightarrow A$ definido como $(a,b,c) = (ab)c - a(bc)$ (que resulta ser la constante o si y sólo si el producto es asociativo). Tenemos como propiedades bastante útiles que el conmutador es $\mathbb{K}$-bilineal y el asociador es $\mathbb{K}$-trilineal. Comprobar la linealidad en cada entrada es similar en cada caso, depende de la distributividad, por eso presentamos aquí solo para la primera: Sean $\lambda \in \mathbb{K}$ y $a, a', b, c \in A$. De paso mencionamos que aprovechando que la suma de A es asociativa y conmutativa omitiremos paréntesis, usándolos cuando nos parezca útil enfatizar; otro pragmatismo típico que seguiremos será denotando $a + (-b)$ como $a - b$.

Para el conmutador:

$$\begin{aligned}
[\lambda a + a', b] &= (\lambda a + a')b - b(\lambda a + a') \\
&= (\lambda a)b + a'b - b(\lambda a) - ba' \\
&= \lambda(ab) - \lambda(ba) + a'b - ba' \\
&= \lambda[a,b] + [a',b],
\end{aligned}$$

en donde cada igualdad se cumple debido a: la definición de conmutador, la distributividad, la asociatividad con escalares y reorganizando términos gracias a las propiedades de $+$, y la distributividad de la acción de escalares (propiedad de espacio vectorial). Argumentos casi idénticos sustentan lo siguiente.

Para el asociador:

$$\begin{aligned}
(\lambda a + a', b, c) &= ((\lambda a + a')b + a'b)c - (\lambda a + a')(bc) \\
&= (\lambda ab)c + (a'b)c - (\lambda a(bc) + a'(bc)) \\
&= \lambda(ab)c + (a'b)c - \lambda a(bc) - a'(bc) \\
&= \lambda((ab)c - a(bc)) + (a'b)c - a'(bc) \\
&= \lambda(a,b,c) + (a',b,c).
\end{aligned}$$

Ya que mencionamos la asociatividad, hay una propiedad que requiere la asociatividad solo de ciertos productos, llamada alternatividad: una $\mathbb{K}$-álgebra es **alternativa** cuando $\forall a, b \in A$, $a^2 b := (aa)b = a(ab)$ y $ba^2 := b(aa) = (ba)a$, llamadas leyes alternativas izquierda y derecha, respectivamente, y en términos del asociador esto es $(a,a,b) = 0 = (b,a,a)$. Se le llama así a esta propiedad por la alternancia de signo del asociador al «permutar sus entradas»: siendo $\sigma \in S_3$ una permutación de $\{1,2,3\}$, pasa que $(a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}) = sgn(\sigma)(a_1, a_2, a_3)$. Podemos comprobarlo mediante la trilinealidad del asociador; notemos que cualquier permutación de $\{1,2,3\}$ puede expresarse como la composición de estas dos:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \text{y} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

En lo que sigue consideraremos $a, b, c, d \in A$. La comprobación es similar en ambos casos, veamos el de la primera, por la ley alternativa derecha tenemos y la trilinealidad:

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

Por lo tanto $(a_1, a_3, a_2) = (a, c, b) = -(a, b, c) = -(a_1, a_2, a_3)$.

La asociatividad es una propiedad a la que quizá estamos acostumbrados, pues en muchas ramas de la matemática la tenemos casi simpre. No contar con ella podría parecer abrumador, incluso en el caso de la alternatividad, sin embargo, como hemos visto, el asociador nos es de mucha ayuda. Veamos dos propiedades más que cumplen las álgebras alternativas:

$$\text{Ley flexiva:} \qquad a(ba) = (ab)a.$$

Esta equivale a que $(a, b, a) = 0$, lo cual tenemos por la alternatividad del asociador $(a, b, a) = -(a, a, b) = -0 = 0$. Estos nos permite expresar aba sin ambigüedad en álgebras alternativas.

$$\begin{aligned} \text{Identidades de Moufang:} \quad & ((ca)c)b = c(a(cb)) \\ & b(c(ac)) = ((bc)a)c \\ & (cb)(ac) = c(ba)c. \end{aligned}$$

Debidas a la matemática Ruth Moufang (1935). Probaremos la segunda, usando las propiedades que hemos visto del asociador, la alternatividad y sumando ceros muy «convenientes»:

$$\begin{aligned}
&((bc)a)c - b(c(ac)) \\
&\quad = ((bc)a)c - (bc)(ac) + (bc)(ac) - b(c(ac)) \\
&\quad = (bc, a, c) + (b, c, ac) \\
&\quad = -(a, bc, c) - (b, ac, c) \\
&\quad = -(a(bc))c + a((bc)c) - (b(ac))c + b((ac)c) \\
&\quad = (-a(bc) - b(ac))c + a((bc)c) + b((ac)c) \\
&\quad = (-a(bc) - b(ac))c + a(bc^2) + b(ac^2) \\
&\qquad + (ab)c^2 - (ab)c^2 + (ba)c^2 - (ba)c^2 \\
&\quad = (-a(bc) - b(ac))c + (-(ab)c^2 + a(bc^2)) + (-(ba)c^2 + b(ac^2)) \\
&\qquad\quad + (ab)c^2 + (ba)c^2 \\
&\quad = (-a(bc) - b(ac))c - (a, b, c^2) - (b, a, c^2) + (ab)c^2 + (ba)c^2 \\
&\quad = (-a(bc) - b(ac))c - (a, b, c^2) + (a, b, c^2) + (ab)c^2 + (ba)c^2 \\
&\quad = (-a(bc) - b(ac))c + (ab)c^2 + (ba)c^2 \\
&\quad = \big(-a(bc) - b(ac) + (ab)c + (ba)c\big)\, c \\
&\quad = \big((ab)c - a(bc) + (ba)c - b(ac)\big)\, c \\
&\quad = \big((a, b, c) + (b, a, c)\big)\, c \\
&\quad = \big((a, b, c) - (a, b, c)\big)\, c \\
&\quad = 0c = 0.
\end{aligned}$$

Finalmente dos propiedades que nos serán útiles:

$$(b, ca, c) = -(b, c, a)c \quad \text{y}$$

$$(b, ca, d) + (b, ca, c) = -(b, c, a)d - (b, d, a)c.$$

Para la primera usamos la segunda identidad de Moufang en la tercera igualdad:

$$\begin{aligned}
(b, ca, c) &= (b(ca))c - b((ca)c) \\
&= (b(ca))c - b(c(ac)) \\
&= (b(ca))c - ((bc)a)c \\
&= (b(ca) - (bc)a)c \\
&= -((bc)a - b(ca))c \\
&= -(b, c, a)c.
\end{aligned}$$

Para la segunda, usando la primera propiedad, tenemos que

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

y por la trilinealidad del asociador y la distributividad, desarrollando cada lado de esta igualdad tenemos:

$$\begin{aligned}(b,(d+c)a,d+c) &= (b,da+ca,d+c)\\ &= (b,da,d)+(b,da,c)+(b,ca,d)+(b,ca,c),\end{aligned}$$

$$\begin{aligned}-(b,d+c,a)(d+c) &= \big(-(b,d,a)-(b,c,a)\big)\,(d+c)\\ &= (b,d,a)d-(b,d,a)c-(b,c,a)d-(b,c,a)c\\ &= (b,da,d)-(b,d,a)c-(b,c,a)d+(b,ca,c),\end{aligned}$$

donde hemos usando nuevamente la primera propiedad, ahora en la última igualdad. Con esto tenemos que

$$\begin{aligned}(b,da,d)+&(b,da,c)+(b,ca,d)+(b,ca,c)\\ &= (b,da,d)-(b,d,a)c-(b,c,a)d+(b,ca,c),\end{aligned}$$

despejando y anulando términos, queda finalmente

$$(b,ca,d)+(b,da,c) = -(b,d,a)c-(b,c,a)d.$$

Ahora, un resultado muy útil en álgebras alternativas, debido a Emil Artin:

Teorema 2.1. *Sea A una $\mathbb{K}$-álgebra alternativa. Consideremos dos elementos $a, b \in A$, entonces la subálgebra generada por éstos es asociativa. Así una $\mathbb{K}$-álgebra A es alternativa si y solo si cualesquiera dos elementos generan una subálgebra alternativa.*

Seguimos la prueba que presenta Schafer (1966) con algunas modificaciones. $\triangleright$ Sean p, q y r productos de n_p, n_q y n_r factores, cada factor siendo a o b, sendos con alguna distribución de paréntesis ($n_p, n_q, n_r \in \mathbb{N}^+$). Para comprobar la asociatividad en el subálgebra generada nos basta entonces comprobar que $(p,q,r) = 0$. Lo haremos por inducción sobre $n = n_p + n_q + n_r$. Para $n < 3$ no hay nada que probar, nuestra base comienza en $n = 3$, como en este caso los tres p, q y r están conformados por un factor y como necesariamente dos de ellos coinciden, $(p,q,r) = 0$ por alguna de las leyes alternativas o la ley flexiva. Supongamos que se cumple para m, siendo $3 < m < n$. Entonces, como $1 \leq n_p, n_q, n_r < n$, en cada uno de p, q y r no se requieren paréntesis. Como tenemos tres productos conformados por dos elementos, al menos dos productos coinciden en su primer factor, sigamos el caso en que q y r empiezan con a (en el caso de fueran p y q u otro caso, podemos volver al primer caso permutando, lo cual nos añadiría a lo más un signo «menos», lo cual no afecta, pues al final vemos que el asociador es cero y $-0 = 0$). Tenemos tres casos: 1) $n_q = n_r = 1$, entonces $q = a$ y $r = a$, y la ley alternativa izquierda nos da $(p, q, r) = (p, a, a) = 0$. 2) Solo se cumple uno de los dos $n_q > 1$ o $n_r > 1$, supongamos que el primero. Entonces $q = aq'$ (siendo q' el resto de factores de q), y por tanto, por la propiedad que dijimos que sería útil (la primera) tenemos

$$(p, q, r) = (p, aq', a) = -(p, a, q')a = 0,$$

por la hipótesis de inducción, ya que $n_{q'} = n_q - 1$ y así $n_p + n_{q'} + n_r = n - 1 < n$. 3) Ambos $n_q, n_r > 1$. Entonces podemos escribir $q = aq'$ y $r = ar'$ (con r' el resto de factores de r), así tenemos, usando la (segunda) propiedad que dijimos nos sería útil, sustituyendo a, b, c, d por q', ar', a, p respectivamente, queda

$$(ar', aq', p) + (ar', pq', a) = -(ar', a, q')p - (ar', p, q')a,$$

despejando tenemos que

$$-(ar', aq', p) = (ar', pq', a) + (ar', a, q')p + (ar', p, q')a,$$

con esto se satisface:

$$\begin{aligned}
(p, q, r) &= (p, aq', ar') \\
&= -(ar', aq', p) \\
&= (ar', pq', a) + (ar', a, q')p + (ar', p, q')a \\
&= (ar', pq', a) + (r, a, q')p + (r, p, q')a \\
&= (ar', pq', a) + 0p + 0a \\
&= -(pq', ar', a) \\
&= (pq', a, r')a = 0a = 0.
\end{aligned}$$

Donde la segunda y sexta igualdades se deben a la alternancia del asociador y los ceros en la quinta y séptima, a la hipótesis de inducción: en la quinta tenemos $(r, a, q') = 0$ pues $n_r + n_a + n_{q'} = n_r + 1 + n_q - 1 = n_r + n_q < n_p + n_q + n_r = n$ (ya que $n_p \geq 1$), y $(r, p, q') = 0$ pues $n_r + n_p + n_{q'} = n_r + n_p + n_q - 1 = n - 1 < n$, finalmente, en la séptima (pq', a, r') debido a que $n_{pq'} + n_a + n_{r'} = (n_p + n_q - 1) + 1 + (n_r - 1) = n_r + n_p + n_q - 1 = n - 1 < n$. ◁

Veamos qué pasa cuando tratamos con álgebras unitales, una propiedad interesante concierne a la subálgebra $\mathbb{K}e$:

Proposición 2.2. *En una $\mathbb{K}$-álgebra unital A, considerando los productos que involucren uno o más elementos de su subálgebra $\mathbb{K}e$, se cumple que los de tres elementos son asociativos, y los de dos elementos son conmutativos.*

$\triangleright$ Nos basta comprobar el caso en el que involucra un elemento de $\mathbb{K}e$. Sean $a, b \in A$ y $c = ke \in \mathbb{K}e \subset A$. De inmediato, por la $\mathbb{K}$-linealidad del asociador tenemos:

$$\begin{aligned}(a, c, b) = (a, ke, b) &= k(a, e, b) \\ &= k\left((ae)b - a(eb)\right) = k(ab - ab) = k0 = 0.\end{aligned}$$

De manera similar $(c, a, b) = 0 = (a, b, c)$, gracias a que e es la unidad de A. Ahora, por la asociatividad con escalares, de inmediato tenemos que

$$ac = a(ke) = k(ae) = ka = k(ea) = (ke)a = ca. \quad \triangleleft$$

Ahora veamos algunas propiedades concernientes a la división e inversos. Primero notemos que para toda $\mathbb{K}$-álgebra A tenemos para cada $a \in A$ dos funciones $\mathbb{K}$-lineales: multiplicación por a a la izquierda y a la derecha, respectivamente, $L_a, R_a : A \longrightarrow A$ definidas como $L_a(b) = ab$ y $R_a(b) = ba$; éstas como el asociador resultan muy útiles cuando no contamos con la asociatividad, por ejemplo la alternatividad equivale a que $(L_a)^2 := L_a \circ L_a = L_{a^2}$ y $(R_a)^2 = R_{a^2}$ para todo $a \in A$.

Una $\mathbb{K}$-álgebra A (no trivial: $A \neq \{0\}$) es un **álgebra con división** cuando $\forall a, b \in A$ tal que $a \neq 0$, las ecuaciones:

$$ax = b, \qquad ya = b$$

tienen soluciones únicas $x, y \in A$. Esto equivale a decir que L_a y R_a tienen inversos. Dados dos elementos $a \neq 0$ y $b \neq 0$, se dice que son **divisores de cero** si $ab = 0 = ba$. Es claro que entonces un álgebra con división no tiene divisores de cero (pues 0 no sería la única solución de $ax = 0$). Sin embargo, en general, no son equivalentes, solo en dimensiones finitas: Para $a \in A - \{0\}$, L_a y R_a son inyectivas si y solo si no hay divisores de cero, y para el caso de un álgebra de dimensión finita, la inyectividad basta para asegurar que una función $\mathbb{K}$-lineal $A \longrightarrow A$ tiene inverso; así, para *dimensión finita, ser un álgebra con división equivale a no tener divisores de cero*.

En un álgebra unitaria podemos definir inversos multiplicativos: un elemento b es un **inverso** de a cuando $ba = e = ab$. La unicidad de los inversos la tenemos al requerir la asociatividad, así podemos denotar un inverso como a^{-1}. Considerando un álgebra unital alternativa, las nociones de ser álgebra con división y que todo $a \neq 0$ tenga inverso multiplicativo a^{-1}, coinciden.

2.2 Álgebras con involución

Una **álgebra con involución** A sobre $\mathbb{K}$, es una $\mathbb{K}$-álgebra con una operación involutiva, llamada usualmente involución $* : A \longrightarrow A$ tal que es $\mathbb{K}$-lineal y $\forall a, b \in A$:

(3) $(a^*)^* = a$

(4) $(ab)^* = b^*a^*$.

Nota: Esta es similar a la definición de álgebra-* para la cual $\mathbb{K} = \mathbb{C}$ e involucra, en vez de $\mathbb{K}$-linealidad, linealidad con conjugación compleja: $\forall \lambda \in \mathbb{C}$: $(\lambda a + b)^* = \bar{\lambda} a^* + b^*$ (Cf. Davidson (1996) y Khalkhali (2013)). Esto resulta útil para la teoría de álgebras C^*, para nuestros fines, requerimos la $\mathbb{K}$-linealidad. Mencionamos esta nota para vincular lo que vemos con otras ramas de la matemática y quizá inspirar así nuevos senderos a seguir.

Un **morfismo de álgebras con involución** es un morfismo de $\mathbb{K}$-álgebras que preserva la involución. Un **isomorfismo** entre dos álgebras con involución es lo que podemos esperar conforme a lo que hemos visto: un morfismo de álgebras con involución con un morfismo de álgebras con involución inverso.

Las álgebras con involución que estaremos tratando serán unitales y cumplen además:

(5) $aa^* \in \mathbb{K}e$.

Podemos llamarlas álgebras con *involución cuadrática*, por una razón que en breve será evidente.

Con las definiciones anteriores, de inmediato, tenemos dos propiedades que nos serán útiles:

i) Para el neutro de la suma de A: $0^* = 0$.

   Esto, pues sabemos que para todo $a \in A$, $0 = 0a$ (siendo el 0 de la izquierda el neutro de la suma de A y el de la derecha un escalar del campo), y * es $\mathbb{K}$-lineal, así:

$$0^* = (0a)^* = 0(a^*) = 0.$$

ii) Siendo A un álgebra unital, $e^* = e$, y por tanto para todo $k \in \mathbb{K}$, $(ke)^* = ke$.

   Por las propiedades (3) y (4), y al ser e neutro del producto tenemos que:

$$e^*a = \left((e^*a)^*\right)^* = \left(a^*(e^*)^*\right)^* = (a^*e)^* = (a^*)^* = a$$

   Es decir, $e^*a = a$; análogamente $ae^* = a$. Entonces, por la unicidad del neutro de la multiplicación, $e^* = e$. Ahora, al ser * $\mathbb{K}$-lineal, para $k \in \mathbb{K}$ tenemos que $(ke)^* ke^* = ke$.

Schafer (1966) requiere, en vez de (5), que $a + a^*$, $aa^* = a^*a \in \mathbb{K}e$, sin embargo, como Voight (2021) lo muestra, esto último se sigue de

(5): Partiendo de que $(a+e)(a+e)^* = ke \in \mathbb{K}e$, y considerando la $\mathbb{K}$-linealidad de * y que $e^* = e$, como:

$$\begin{aligned}(a+e)(a+e)^* &= (a+e)(a^*+e^*) = (a+e)(a^*+e)\\ &= aa^* + ae + ea^* + e = aa^* + a + a^* + e.\end{aligned}$$

Entonces $a + a^* = ke - aa^* - e \in \mathbb{K}e$, pues $aa^* \in \mathbb{K}e$. Así $a + a^* = k'e \in \mathbb{K}e$, y recordando que los elementos de $\mathbb{K}e$ conmuntan con los de A en los productos (proposición 1.2), tenemos que $a(a+a^*) = (a+a^*)a$. Con lo que $aa + aa^* = a(a+a^*) = (a+a^*)a = aa + a^*a$, entonces, al sumar $-(aa)$ de ambos lados, queda $aa^* = a^*a$.

Recordemos ahora que una **forma cuadrática** se define como una función entre $\mathbb{K}$-espacios vectoriales $q : A \longrightarrow \mathbb{K}$ tal que:

Q1. $\forall a \in A\ \forall k \in \mathbb{K}$: $q(ka) = k^2 q(a)$.

Q2. La función $(,)_q : A \times A \longrightarrow \mathbb{K}$, definida como $(a,b)_q = q(a+b) - q(a) - q(b)$, es $\mathbb{K}$-bilineal.

Asumiendo que tratamos con espacios de dimensión finita n, una forma cuadrática q es **no degenerada** cuando la forma bilineal asociada $(,)_q$ lo es, y eso último ocurre cuando para todo $a \in A - \{0\}$, existe algún $b \in A$ tal que $(a,b)_q \neq 0$ (esto equivale a que para cualquier $a \in A$, si para todo $b \in A$ pasa que $(a,b)_q = 0$, entonces $a = 0$); cabe notar que dicha forma bilineal resulta ser **simétrica**: $(a,b)_q = (b,a)_q$, pues la conmutatividad de la suma nos da $q(a+b) - q(a) - q(b) = q(b+a) - q(b) - q(a)$, y por eso no requerimos que la propiedad se dé en ambas entradas por separado. Otros nombres que se le dan a esta propiedad es **no singular**, o **regular**.

Un **álgebra de composición** A es una $\mathbb{K}$-álgebra con involución (de dimensión finita) con una forma cuadrática $n : A \longrightarrow \mathbb{K}$ no degenerada tal que respeta el producto, esto es $\forall a, b \in A$: $n(ab) = n(a)n(b)$ y cumple que

$$n(a) = aa^*.$$

En donde hemos identificado $\mathbb{K}e$ con $\mathbb{K}$, es decir denotamos el $k \in \mathbb{K}$ tal que $aa^* = ke$, como aa^*; podemos justificar la identificación que mencionamos recordando que $\mathbb{K}e \cong \mathbb{K}$ como $\mathbb{K}$-álgebras. Cabe notar que entonces podemos denotar la unidad del álgebra con e, como lo hemos hecho, o con 1, según queramos enfatizar. Ahora vemos un interesante resultado de requerir (5).

Proposición 2.3. *Toda $\mathbb{K}$-álgebra A con involución que cumple (5), i. e., $\forall a \in A$: $aa^* \in \mathbb{K}e$, tiene una forma cuadrática natural definida como $N(a) = aa^*$.*

▷ Para un álgebra con involución, de acuerdo con (5), tenemos que $aa^* \in \mathbb{K}e$. Considerando que $\mathbb{K}e \cong \mathbb{K}$ y la consiguiente identificación de éstos, podemos ver que definiendo $N(a) = aa^*$, obtenemos una forma cuadrática, más aún $N(e) = ee^* = ee = e = 1$. Para la propiedad Q1 basta usar la $\mathbb{K}$-linealidad de * (y las asociatividades con escalares), así:

$$N(\kappa a) = (\kappa a)(\kappa a)^* = (\kappa a)(\kappa a^*) = (\kappa\kappa)(aa^*) = \kappa^2 N(a).$$

Y para Q2, tenemos:

$$\begin{aligned}
&(\lambda a + b, c)_N \\
&\quad = N\big((\lambda a + b) + c\big) - N(\lambda a + b) - N(c) \\
&\quad = \big((\lambda a + b) + c\big)\big((\lambda a + b) + c\big)^* - (\lambda a + b)(\lambda a + b)^* - cc^* \\
&\quad = (\lambda a + b + c)(\lambda a^* + b^* + c^*) - (\lambda a + b)(\lambda a^* + b^*) - cc^* \\
&\quad = \lambda^2 aa^* + \lambda ab^* + \lambda ac^* + \lambda ba^* + bb^* + bc^* + \lambda ca^* + cb^* + cc^* \\
&\qquad\quad - (\lambda^2 aa^* + \lambda ab^* + \lambda ba^* + bb^*) - cc^* \\
&\quad = \lambda ac^* + \lambda ca^* + bc^* + cb^* \\
&\quad = \lambda(ac^* + ca^*) + bc^* + cb^*.
\end{aligned}$$

Por un lado, y por otro,

$$\begin{aligned}
&\lambda(a, c)_N + (b, c)_N \\
&\quad = \lambda\big(N(a + c) - N(a) - N(c)\big) + \big(N(b + c) - N(b) - N(c)\big) \\
&\quad = \lambda\big((a + c)(a + c)^* - aa^* - cc^*\big) + \big((b + c)(b + c)^* - bb^* - cc^*\big) \\
&\quad = \lambda(aa^* + ac^* + ca^* + cc^* - aa^* - cc^*) + bb^* + bc^* + cb^* - bb^* - cc^* \\
&\quad = \lambda(ac^* + ca^*) + bc^* + cb^*.
\end{aligned}$$

Con lo que $(\lambda a + b, c)_N = \lambda(a, c)_N + (b, c)_N$, es decir, es $\mathbb{K}$-lineal en la entrada derecha. Análogamente se tiene la $\mathbb{K}$-linealidad izquierda, de hecho debido a la conmutatividad y asociatividad de la suma en A, la misma prueba funciona al reordenar términos; así $(,)_N$ es $\mathbb{K}$-bilineal. $\triangleleft$

Así, las álgebras con involución que hemos definido y que cumplen (5), son *casi* álgebras de composición, requerimos de algunas propiedades adicionales para poder asegurar que N sea no degenerada y preserve productos; luego volvemos a este asunto. Con esto vemos la importancia de que una involución cumpla (5), incluso, varios nombres se les han dado a las involuciones que cumplen dicha propiedad (Voight, 2021): *involución principal*, *conjugación*, Voight prefiere *involución estándar*, y nosotros preferimos un nombre que hiciera referencia a que dicha propiedad permite definir una forma cuadrática natural: **involución cuadrática**.

Ahora veremos uno de los resultados más famosos al respecto de éstas álgebras, planteado primero por Adolf Hurwitz y desarrollado por más matemáticos. Lo presentamos parafraseando el enunciado de Schafer (1966), donde también puede encontrarse una prueba del mismo.

Teorema 2.4. *Sea A una $\mathbb{K}$-álgebra unital, con $\mathbb{K}$ de característica distinta de 2. Existe una forma cuadrática $N(a)$ que hace a A un álgebra de composición, si y sólo si A es (salvo isomorfismos) alguna de las siguientes álgebras:*

a) $\mathbb{K}e$

b) $\mathbb{K} \oplus \mathbb{K}$ *la suma directa*

c) Un campo cuadrático separable $\mathcal{S}$ sobre $\mathbb{K}$

d) Un álgebra de Hamilton $\mathcal{H}$ sobre $\mathbb{K}$

e) Un álgebra de Cayley $\mathcal{C}$ sobre $\mathbb{K}$.

Con lo que las posibles dimensiones de A son: 1, 2, 4 y 8. Más aún, si $A = \mathbb{K}e$, entonces $N(ae) = a^2$, y en otro caso $N(a) = aa^*$.

En el siguiente capítulo conoceremos las álgebras de Hamilton y de Cayley.

3

LA CONSTRUCCIÓN DE CAYLEY-DICKSON

3.1 CONSTRUCCIÓN GENERAL

Sea A una $\mathbb{K}$-álgebra unital de dimensión finita con involución cuadrática (i. e. cumple (5) de la sección pasada). Queremos «construir» otra álgebra con las mismas propiedades y que contenga a A como subálgebra (salvo isomorfismos), con la misma unidad. Esto resulta posible mediante la **construcción o proceso de Cayley-Dickson**:

Definimos esta nueva álgebra como $\mathfrak{C}(A) = A \times A$ con la suma y acción por escalares definida coordenada a coordenada, y multiplicación definida como

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2 + \mu b_2 b_1^*, a_1^* b_2 + a_2 b_1),$$

con $\mu \in \mathbb{K}$ fijo, e involución definida como

$$(a, b)^* = (a^*, -b).$$

Nota: Schafer (1966) requiere que $\mu \neq 0$, pero aquí no habrá tal restricción salvo lo especifiquemos. Esto nos traerá consecuencias que iremos mencionando.

Teorema 3.1. *Con estas operaciones, $\mathfrak{C}(A)$ es en efecto una $\mathbb{K}$-álgebra unital con involución cuadrática (i. e. cumple $\forall x \in \mathfrak{C}(A) : xx^* \in \mathbb{K}e$); siendo $(e, 0)$ su unidad.*

$\triangleright$ Que es un $\mathbb{K}$-espacio vectorial con las operaciones definidas coordenada a coordenada es un hecho bien conocido, de hecho considerando sólo la estructura de espacio vectorial tenemos que $\dim(\mathfrak{C}(A)) = \dim(A \times A) = 2\dim(A)$, pero nos interesa que sea un álgebra con involución. Veamos que se cumplen el resto de propiedades que involucran la multiplicación e involución. Sean $\lambda \in \mathbb{K}$ y $a, a_1, a_2, b, b_1, b_2, c, c_1, c_2, d, d_1, d_2 \in A$. Primero veamos que se cumple la asocitividad con escalares del producto:

$$\begin{aligned}
\big(\lambda(a,b)\big)\,(c,d) &= (\lambda a, \lambda b)(c,d) \\
&= \big((\lambda a)c + \mu d(\lambda b)^*, (\lambda a)^* d + c(\lambda b)\big) \\
&= \big((\lambda a)c + \mu d(\lambda b^*), (\lambda a^*) d + c(\lambda b)\big) \\
&= \big(\lambda ac + \lambda(\mu d b^*), \lambda a^* d + \lambda cb\big) \\
&= \big(\lambda(ac + \mu d b^*), \lambda(a^* d + cb)\big) \\
&= \lambda\,\big(ac + \mu d b^*, a^* d + cb\big) \\
&= \lambda\,\big((a,b)(c,d)\big)\,.
\end{aligned}$$

Cada igualdad se cumple respectivamente pues: el escalar actúa coordenada a coordenada por definición, la definición del producto en $\mathfrak{C}(A)$, * es $\mathbb{K}$-lineal, asociatividad con escalares del producto de A, distributividad de escalares (propiedad de $\mathbb{K}$-espacio vectorial de A), y nuevamente, el escalar actúa coordenada a coordenada. De manera similar tenemos que $\lambda\,\big((a,b)(c,d)\big) = (a,b)\,\big(\lambda(c,d)\big)$.

Ahora, veamos que la multiplicación es bilineal:

$$\begin{aligned}
&\big(\lambda(a_1,b_1) + (a_2,b_2)\big)\,(c,d) \\
&= \big((\lambda a_1, \lambda b_1) + (a_2,b_2)\big)\,(c,d) \\
&= (\lambda a_1 + a_2, \lambda b_1 + b_2)(c,d) \\
&= \big((\lambda a_1 + a_2)c + \mu d(\lambda b_1 + b_2)^*, (\lambda a_1 + a_2)^* d + c(\lambda b_1 + b_2)\big) \\
&= \big((\lambda a_1 + a_2)c + \mu d(\lambda b_1^* + b_2^*), (\lambda a_1^* + a_2^*) d + c(\lambda b_1 + b_2)\big) \\
&= \big((\lambda a_1 c + a_2 c) + (\mu d)(\lambda b_1^*) + (\mu d) b_2^*, (\lambda a_1^* d + a_2^* d) + (\lambda c b_1 + c b_2)\big) \\
&= \big((\lambda a_1 c + a_2 c) + (\lambda(\mu d) b_1^* + \mu d b_2^*), (\lambda a_1^* d + a_2^* d) + (\lambda c b_1 + c b_2)\big) \\
&= \big((\lambda a_1 c + a_2 c) + (\lambda(\mu d b_1^*) + \mu d b_2^*), (\lambda a_1^* d + a_2^* d) + (\lambda c b_1 + c b_2)\big) \\
&= \big((\lambda a_1 c + \lambda(\mu d b_1^*)) + (a_2 c + \mu d b_2^*), (\lambda a_1^* d + \lambda c b_1) + (a_2^* d + c b_2)\big) \\
&= (\lambda a_1 c + \lambda(\mu d b_1^*), \lambda a_1^* d + c b_1) + (a_2 c + \mu d b_2^*, a_2^* d + c b_2) \\
&= \lambda(a_1 c + \mu d b_1^*, a_1^* d + c b_1) + (a_2 c + \mu d b_2^*, a_2^* d + c b_2) \\
&= \lambda(a_1,b_1)(c,d) + (a_2,b_2)(c,d).
\end{aligned}$$

En cada paso se cumple la igualdad respectivamente pues: el escalar actúa en cada coordenada, la suma se hace coordenada a coordenada, la definición del producto, * es $\mathbb{K}$-lineal, la asociatividad con escalares del producto y la distributividad del producto sobre la suma en A, la asociatividad con escalares del producto, de nuevo la asociatividad con escalares, asociatividad y conmutatividad de la suma en A, la suma es coordenada a coordenada, el escalar actúa en cada coordenada, y la definición del producto. De manera similar tenemos que

$$(c,d)\,\big(\lambda(a_1,b_1) + (a_2,b_2)\big) = \lambda(c,d)(a_1,b_1) + (c,d)(a_2,b_2).$$

Pasamos a ver la distributividad del producto sobre la suma en $\mathfrak{C}(A)$, aquí comprobamos la distributividad izquierda:

$$\begin{aligned}
&(a,b)\left((c_1,d_1)+(c_2,d_2)\right)\\
&\qquad=(a,b)(c_1+c_2,d_1+d_2)\\
&\qquad=\left(a(c_1+c_2)+\mu(d_1+d_2)b^*,a^*(d_1+d_2)+(c_1+c_2)b\right)\\
&\qquad=\left((ac_1+ac_2)+\mu(d_1b^*+d_2b^*),(a^*d_1+a^*d_2)+(c_1b+c_2b)\right)\\
&\qquad=\left((ac_1+ac_2)+(\mu d_1b^*+\mu d_2b^*),(a^*d_1+a^*d_2)+(c_1b+c_2b)\right)\\
&\qquad=\left((ac_1+\mu d_1b^*)+(ac_2+\mu d_2b^*),(a^*d_1+c_1b)+(a^*d_2+c_2b)\right)\\
&\qquad=(ac_1+\mu d_1b^*,a^*d_1+c_1b)+(ac_2+\mu d_2b^*,a^*d_2+c_2b)\\
&\qquad=(a,b)(c_1,d_1)+(a,b)(c_2,d_2).
\end{aligned}$$

La justificación de cada paso es: definición de suma, distributividad en A, distributividad de escalares (propiedad de $\mathbb{K}$-espacio vectorial de A), asociatividad y conmutatividad de la suma en A, definición de suma y definición de producto. Similarmente se tiene la derecha:

$$\left((a_1,b_1)+(a_2,b_2)\right)(c,d)=(a_1,b_1)(c,d)+(a_2,b_2)(c,d).$$

Resulta inmediato, debido que $0^*=0$, $e^*=e$ y a las conocidas propiedades de 0 con respecto al producto y la multiplicación por escalar, ver que $(e,0)$ es el neutro de este producto:
$(e,0)(c,d)=(ec+\mu d0^*,e^*d+c0)=(c+\mu d0,ed+c0)=(c,d)$ y
$(a,b)(e,0)=(ae+\mu 0b^*,a^*0+eb)=(a,b)$.

Pasemos ahora a las propiedades relativas a la involución. Por la definición de la involución en $\mathfrak{C}(A)$, las propiedades de * en A y las conocidas propiedades que involucran inversos aditivos y el producto en A, se tiene que $\left((a,b)^*\right)^*=(a^*,-b)^*=\left((a^*)^*,-(-b)\right)=(a,b)$. También tenemos, por un lado:

$$\begin{aligned}
\left((a,b)(c,d)\right)^*&=\left(ac+\mu db^*,a^*d+cb\right)^*\\
&=\left((ac+\mu db^*)^*,-(a^*d+cb)\right)\\
&=\left((ac)^*+(\mu db^*)^*,-a^*d-cb\right)\\
&=\left(c^*a^*+\mu(b^*)^*d^*,-a^*d-cb\right)\\
&=\left(c^*a^*+\mu bd^*,-a^*d-cb\right).
\end{aligned}$$

Y por otro:

$$\begin{aligned}
(c,d)^*(a,b)^*&=(c^*,-d)(a^*,-b)\\
&=\left(c^*a^*+\mu bd^*,(c^*)^*(-b)+a^*(-d)\right)\\
&=\left(c^*a^*+\mu bd^*,-cb-a^*d\right)\\
&=\left(c^*a^*+\mu bd^*,-a^*d-cb\right).
\end{aligned}$$

Con lo que $\big((a,b)(c,d)\big)^* = (c,d)^*(a,b)^*$.

Resta ver que es $\mathbb{K}$-lineal en $\mathfrak{C}(A)$, para lo cual usamos fundamentalmente la $\mathbb{K}$-linealidad de * en A, además de las definiciones de las operaciones en $\mathfrak{C}(A)$:

$$\begin{aligned}\big(\lambda(a,b)+(c,d)\big)^* &= (\lambda a + c, \lambda b + d)^* = \big((\lambda a + c), -(\lambda b + d)\big)\\ &= (\lambda a^* + c^*, -\lambda b - d) = (\lambda a^*, -\lambda b) + (c^*, -d)\\ &= \lambda(a^*, -b) + (c^*, -d) = \lambda(a,b)^* + (c,d)^*.\end{aligned}$$

Finalmente, recordando que $N(a) := aa^* \in \mathbb{K}e \cong \mathbb{K}$, tenemos:

$$\begin{aligned}(a,b)(a,b)^* &= (a,b)(a^*,-b) = (aa^* + \mu(-b)b^*, a^*(-b) + a^*b)\\ &= (aa^* - \mu bb^*, -a^*b + a^*b) = (aa^* - \mu bb^*, 0)\\ &= (N(a) - \mu N(b), 0) = ((N(a) - \mu N(b))e, 0)\\ &= (N(a) - \mu N(b))(e,0) \in \mathbb{K}(e,0).\end{aligned}$$

Con todo esto hemos comprobado que $\mathfrak{C}(A)$ es una $\mathbb{K}$-álgebra con involución unital, con $(e,0)$ como unidad, que cumple la propiedad (5) de la sección anterior, tiene una involución cuadrática. $\triangleleft$

Ahora notemos que $A' = \{(a,0) : a \in A\} \subset \mathfrak{C}(A)$ es una subálgebra de ésta isomorfa a A: es claro que la función $\iota : A \longrightarrow A'$, con $\iota(a) = (a,0)$, es $\mathbb{K}$-lineal con inversa la proyección $\pi(a,b) = a$ (claramente también $\mathbb{K}$-lineal) restringida en su dominio a A'. Y también son morfismos de álgebras con involución: Como, $(a,0)(b,0) = (ab + \mu 00^*, a^*0 + b0) = (ab + 0, 0+0) = (ab,0)$, para ι tenemos que $\iota(a)\iota(b) = (a,0)(b,0) = (ab,0) = \iota(ab)$ y también tenemos que $\iota(a)^* = (a,0)^* = (a^*,-0) = (a^*,0) = \iota(a^*)$; mientras que para π, tenemos $\pi\big((a,0)\big)\,\pi\big((c,0)\big) = ac = \pi\big((ab,0)\big) = \pi\big((a,0)(b,0)\big)$ y también $\pi\big((a,0)^*\big) = \pi(a^*,-0) = \pi(a^*,0) = a^* = \pi(a,0)^*$.

Aunque esto puede resultar interesante por sí mismo, poder definir una nueva álgebra con involución a partir de una dada y que esta nueva incluya una versión isomorfa de la original, surgen dos preguntas: ¿por qué definimos el producto así? y ¿es la única manera de obtener un álgebra con involución así a partir de una dada?

Para responder a la primera, haremos uso de algunas definiciones e identificaciones que nos dan una primera idea, que quizá pudo ya sospecharse al comprobar la propiedad (5). Primero definamos $v = (0,e)$, y notemos que $vA' := \{(0,e)(a,0) : (a,0) \in A'\} = \{(0,a) : a \in A\}$, esto pues $(0,e)(a,0) = (0a + \mu 0e^*, 0^*0 + ae) = (0+0, 0+a) = (0,a)$. Con esto, considerando a $\mathfrak{C}(A)$ como espacio vectorial, es claro que éste es la suma directa de A' y vA'. Más aún, identificando los elementos de A' con los de A, esto es $(a,0) = a$, tenemos que $(a,b) = a + vb$ (así $\mathfrak{C}(A) = A \oplus vA$ como espacio vectorial). De esta forma las operaciones de suma, producto e involución en $\mathfrak{C}(A)$ toman la forma:

$$(a+vb)+(c+vd)=(a+c)+v(b+d)$$
$$(a+vb)(c+vd)=(ac+\mu db^*)+v(a^*d+cb)$$
$$(a+vb)^*=a^*-vb.$$

Que nos recuerdan a las operaciones definidas en $\mathbb{C}$. Con una ligera modificación en la involución y con el detalle de que $v^2=\mu$, pues

$$\begin{aligned} vv &= (0,e)(0,e)=(00+\mu ee^*, 0^*e+0e) \\ &= (0+\mu ee, 0+0)=(\mu e, 0) \\ &= \mu(e,0)\in\mathbb{K}(e,0). \end{aligned}$$

Nota: Conforme a las identificaciones que hemos hecho de $\mathbb{K}e\cong\mathbb{K}$, anotaremos $0+v0$ como 0 simplemente, y $v^2=\mu$; también escribiremos $0+vb$ como vb, así tenemos, por ejemplo $(vb)^2=(0+vb)(0+vb)=0+bb^*+v(0+0)=bb^*+v0=bb^*$. Entonces, podemos pensar en $\mathfrak{C}(A)$ como una extensión del álgebra con involución A obtenida a añadirle un nuevo elemento v (y los de la forma $a+vb$ necesarios para hacerla un álgebra con involución) tal que $v^2=\mu e'=\mu$, con e' siendo la unidad de esta extensión. Es decir, el proceso de Cayley-Dickson es una generalización de la idea intuitiva de extender el álgebra de $\mathbb{R}$ para incluir un elemento i tal que $i^2=-1$, aplicable a cualquier álgebra con involución. Con esto nos podemos preguntar ¿es $\mathbb{R}$ un álgebra con involución? Si es así, ¿cuál es la involución de $\mathbb{R}$? Pues $\mathbb{R}$ es una $\mathbb{R}$-álgebra con involución trivial, es decir, su involución es la identidad $^*=id_{\mathbb{R}}$.

Para responder a la segunda, el teorema 2.4 (Hurwitz) ya nos adelanta algo, esperaremos hasta la siguiente sección para detallar un poco más acerca de esta cuestión.

3.2 algunos resultados

Ahora que conocemos el proceso de Cayley-Dikson, nos interesa conocer qué otras relaciones hay entre el álgebra de la que se parte A y esta nueva álgebra $\mathfrak{C}(A)$. Antes veremos una propiedad que nos permite tratar la alternatividad con la involución.

Proposición 3.2. *En una $\mathbb{K}$-álgebra A con involución cuadrática se cumple que $\forall a,b,c\in A$:*

$$(a^*,b,c)=-(a,b,c),\quad (a,b^*,c)=-(a,b,c)\quad y\quad (a,b,c^*)=-(a,b,c);$$

más aún, las leyes alternativas equivalen a que $\forall a,b\in A$

$$(a,a^*,b)=0=(b,a,a^*).$$

▷ En cuanto a la primera parte mostraremos la primera igualdad (las otras son análogas). Usando el conocido «truco» de sumar un cero conveniente y luego asociando tenemos por la linealidad del asociador y recordando que (5) nos dice que $a + a^* = ke \in \mathbb{K}e$:

$$\begin{aligned}(a^*, b, c) &= ((a + a^*) - a, b, c)\\ &= (ke, b, c) - (a, b, c) = 0 - (a, b, c) = -(a, b, c).\end{aligned}$$

Ya que $(a, ke, b) = 0$ por la proposición 2.2. Para la segunda parte de la proposición requerimos los casos particulares de la primera: $(a, a^*, b) = -(a, a, b)$ y $(b, a, a^*) = -(b, a, a)$, de los cuales es claro que equivalen a las leyes alternativas. ◁

Ahora sí, un primer resultado es el siguiente:

Teorema 3.3. *Siendo A un álgebra alternativa con involución cuadrática, esto es, que cumple (5), A es un álgebra asociativa si y solo si $\mathfrak{C}(A)$ es alternativa.*

▷ Supongamos que A es asociativa. Sean $x, y \in \mathfrak{C}(A)$, así $x = a + vb$ y $y = c + vd$ para ciertos $a, b, c, d \in A$. Por la proposición anterior, basta que veamos que $(x, x^*, y) = 0 = (y, x, x^*)$. Usando la definición de producto en $\mathfrak{C}(A)$:

$$\begin{aligned}(x, x^*, y) &= (xx^*)y - x(x^*y)\\
&= (x, x^*)y - x((a + vb)^*(c + vd))\\
&= (xx^*)y - x((a^* - vb)(c + vd))\\
&= (xx^*)y - (a + vb)((a^*c - \mu db^*) + v(ad - cb))\\
&= (xx^*)y - \left(a(a^*c - \mu db^*) + \mu(ad - cb)b^*\right)\\
&\qquad - v\left(a^*(ad - cb) + (a^*c - \mu db^*)b\right)\\
&= (xx^*)y - \left(a(a^*c) - \mu a(db^*) + \mu(ad)b^* - \mu(cb)b^*\right)\\
&\qquad - v\left(a^*(ad) - a^*(cb) + (a^*c)b - \mu(db^*)b\right)\\
&= (xx^*)y - \left(a(a^*c) - \mu(cb)b^*\right) - v\left(a^*(ad) - \mu(db^*)b\right)\\
&\qquad - \mu\left((ad)b^* - a(db^*)\right) - v\left((a^*c)b - a^*(cb)\right)\\
&= (xx^*)y - \left((aa^*)c - \mu(bb^*)c\right) - v\left(a^*ad - \mu bb^*d\right) \qquad \ddagger\\
&\qquad - \mu\,(a, d, b^*) - v\,(a^*, c, b)\\
&= (xx^*)y - \left(aa^* - \mu bb^*\right)(c + vd)\\
&\qquad - \mu\,(a, d, b^*) - v\,(a^*, c, b)\\
&= \left(aa^* - \mu bb^*\right)(c + vd) - \left(aa^* - \mu bb^*\right)(c + vd)\\
&\qquad - \mu\,(a, d, b^*) - v\,(a^*, c, b)\\
&= 0 - \mu\,(a, d, b^*) - v\,(a^*, c, b)\\
&= 0 + v0.\end{aligned}$$

En ‡ usamos que A es alternativa por hipótesis y hemos aprovechado que $b^*b = bb^* \in \mathbb{K}e$ y que los elementos de $\mathbb{K}e$ conmutan con los de A en los productos (proposición 2.2). En la última igualdad tenemos que los asociadores de anulan por que suponemos que A es asociativa. Así $(x, x^*, y) = 0$ y por tanto $\mathfrak{C}(A)$ es alternativa.

Ahora supongamos que $\mathfrak{C}(A)$ es alternativa, considerando $x = a^* + vb$, $y = c + v0$. Por los cálculos anteriores tenemos que

$$0 = (x, x^*, y) = -\mu(a^*, 0, b^*) - v(a, c, b) = 0 - v(a, c, b)$$

Lo cual implica que $(a, c, b) = 0$, siendo $a, b, c \in A$ arbitrarios, esto es que A es asociativa. ◁

Ahora algunas definiciones antes de que pasemos a más resultados. Una **álgebra de Hamilton** o **cuaterniónica** es un álgebra con involución que cumple (5) de dimensión 4 obtenida mediante el proceso de Cayley-Dickson aplicado a una álgebra bidimensional (que puede ser $\mathbb{K} \oplus \mathbb{K}$ o bien un campo cuadrático separable sobre $\mathbb{K}$) tomando $\mu \neq 0$ en ambos casos. En Voight (2021) se define como una $\mathbb{K}$-álgebra tetradimensional B para la cual existen $i, j \in B$ tales que e, i, j, ij forman una base como espacio vectorial y satisfacen:

$$i^2 = a, \quad j^2 = b, \quad \text{y} \quad ji = -ij$$

para ciertos $a, b \in \mathbb{K}e - \{0\}$ (ambas definiciones se refieren a la misma entidad). Un **álgebra de Cayley** u **octoniónica** es una álgebra con involución que cumple (5) de dimensión 8 obtenida mediante el proceso de Cayley-Dickson con $\mu \neq 0$. Un álgebra con involución A es **real** cuando $^* = id_A$.

Las álgebras cuaterniónicas son álgebras asociativas (y simples centrales, Schafer (1966), p. 47) *Nota*: Una $\mathbb{K}$-álgebra A es simple central cuando los productos de Kronecker, i. e. las $\mathbb{K}$-álgebras definidas para los productos tensoriales $K \otimes_{\mathbb{K}} A$ con el producto definido por la distributividad, resultan ser simples para toda extensión K del campo $\mathbb{K}$. Como son asociativas, entonces tenemos que las álgebras de Cayley u octoniónicas son alternativas. De hecho, tenemos el siguiente:

Teorema 3.4. *Dada una $\mathbb{K}$-álgebra A con involución * que satisface (5): $\forall a \in A$: $aa^* \in \mathbb{K}e$. Se cumple lo siguiente*

a) *Si A es real, entonces también es conmutativa.*

b) *Si $car(\mathbb{K}) \neq 2$, entonces $\mathfrak{C}(A)$ no es real.*

c) *$\mathfrak{C}(A)$ es conmutativa si y solo si A es real.*

d) *$\mathfrak{C}(A)$ es asociativa si y solo si A es conmutativa y asociativa.*

e) $\mathfrak{C}(A)$ *es alternativa si y solo si* A *es asociativa.*

▷ Para comprobar esto haremos uso de la definición del producto en $\mathfrak{C}(A)$ usando la notación $a + vb$ para ahorrarnos paréntesis. Sean $x, y, z \in \mathfrak{C}(A)$, así $x = a + vb$, $y = c + vd$, y $z = f + vg$, con $a, b, c, d, f, g \in A$ (es útil recordar que $x = y$ si y solo si $a = c$ y $b = d$). Para a), por las propiedades de * y al suponer que A es real tenemos que:

$$ab = (ab)^* = b^* a^* = ba.$$

Esto es, A es conmutativa.

Para b), supongamos que $car(\mathbb{K}) \neq 2$. Tenemos por definición que:

$$x^* = (a + vb)^* = a^* - vb \neq a + vb = x.$$

Para el caso en que $b \neq 0$, pues evidentemente $b \neq -b$, pues eso implicaría que $2b = 0$ y por tanto que $b = 0$. Así que $\mathfrak{C}(A)$ no puede ser real.

Pasemos al caso c), tenemos que:

$$xy = (a + vb)(c + vd) = ac + \mu db^* + v(a^* d + cb) \text{ y}$$

$$yx = (c + vd)(a + vb) = ca + \mu bd^* + v(c^* b + ad),$$

de lo cual resulta evidente que si A es real (y por tanto conmutativa), entonces $xy = yx$, i. e. $\mathfrak{C}(A)$ sería conmutativa. Por otro lado si $\mathfrak{C}(A)$ es conmutativa para $(a, 0), v := (0, e) \in \mathfrak{C}(A)$, resulta que (aquí usaremos la notación de pares ordenados para evitar confusiones):

$$\begin{aligned}(0, a^*) &= (0 + 0, a^* e + 0) = (a, 0)(0, e) \\ &= (0, e)(a, 0) = (0 + 0, 0 + a) = (0, a).\end{aligned}$$

Así $a = a^*$, por tanto, A es real.

Para el caso d) consideraremos los productos:

$$\begin{aligned}(xy)z &= \left(ac + \mu db^* + v(a^* d + cb)\right)(f + vg) \\ &= (ac + \mu db^*)f + \mu g(a^* d + cb)^* \\ &\quad + v\left((ac + \mu db^*)^* g + f(a^* d + cb)\right) \\ &= (ac + \mu db^*)f + \mu g(d^* a + b^* c^*) \\ &\quad + v\left((c^* a^* + \mu bd^*)g + f(a^* d + cb)\right) \\ &= (ac)f + \mu(db^*)f + \mu g(d^* a) + \mu g(b^* c^*) \\ &\quad + v\left((c^* a^*)g + \mu(bd^*)g + f(a^* d) + f(cb)\right),\end{aligned}$$

$$\begin{aligned}
x(yz) &= (a+vb)\left(cf+\mu gd^* + v(c^*g+fd)\right)\\
&= a(cf+\mu gd^*) + \mu(c^*g+fd)b^*\\
&\qquad + v\left(a^*(c^*g+fd) + (cf+\mu gd^*)b\right)\\
&= a(cf) + \mu a(gd^*) + \mu(c^*g)b^* + \mu(fd)b^*\\
&\qquad + v\left(a^*(c^*g) + a^*(fd) + (cf)b + \mu(gd^*)b\right)\\
&= a(cf) + \mu(fd)b^* + \mu a(gd^*) + \mu(c^*g)b^*\\
&\qquad + v\left(a^*(c^*g) + \mu(gd^*)b + a^*(fd) + (cf)b\right).
\end{aligned}$$

En donde, en la última igualdad sólo hemos reorganizado términos para comparar más fácilmente las dos expresiones finales de $(xy)z$ y $x(yz)$. Claramente si A es asociativa y conmutativa, entonces $\mathfrak{C}(A)$ es asociativa. Por otro lado si ahora suponemos que $\mathfrak{C}(A)$ es asociativa, tomando $x = a + v0$, $y = c + v0$ y $z = f + v0$, casi todos los términos en dos las expresiones de arriba se anulan, excepto el primero, como suponemos que $(xy)z = x(yz)$, tenemos que $(ac)f = a(cf)$, con lo cual resulta que A es asociativa (lo cual también podíamos argumentarlo recordando que $A \cong A' \subset \mathfrak{C}(A)$). Ahora tomando $x = 0 + ve$, $y = c + v0$ y $z = f + v0$, nuevamente se anulan casi todos los términos, exceptuando, esta vez, al último; como $(xy)z = x(yz)$, tenemos que $fc = f(ce) = (cf)e = cf$, así que A también es conmutativa.

En cuanto al caso e), ya lo comprobamos en el teorema anterior, pero lo pusimos nuevamente para recolectar estos resultados. $\triangleleft$

Considerando este teorema, a partir de aquí, asumiremos que la característica $car(\mathbb{K}) \neq 2$. Sabemos que el proceso de Cayley-Dickson requiere partir de un álgebra con involución para construir otra, y ¿qué mejor?, de hecho tenemos una, $\mathbb{K}$ mismo es una $\mathbb{K}$-álgebra con involución con el producto y multiplicación con escalares coincidiendo y operación involutiva la identidad $id_{\mathbb{K}}$. Entonces en cada paso $t \in \mathbb{N}$ podemos elegir una $\mu_t \in \mathbb{K}$ (siendo el paso 0 no hacer nada), usamos la *notación* $(\mathfrak{C}(A), \mu)$ cuando sea necesario especificar la μ particular. Como es evidente, obtenemos una sucesión de álgebras con involución que cumplen (5): $aa^* \in \mathbb{K}e$, cuyas dimensiones van duplicándose (2^t). Pero para álgebras alternativas el proceso no llega a más de tres pasos:

Proposición 3.5. *Cualquier álgebra de Cayley es no asociativa.*

$\triangleright$ De hecho el teorema anterior nos dice que al partir del campo $\mathbb{K}$ considerado como $\mathbb{K}$-álgebra real ($*= id_{\mathbb{K}}$), como ésta es asociativa y conmutativa, tenemos que $\mathfrak{C}(A)$ es no real (pues $car(\mathbb{K}) \neq 2$), asociativa y conmutativa; así $\mathfrak{C}^2(A) := \mathfrak{C}(\mathfrak{C}(A))$ es asociativa, pero no conmutativa; $\mathfrak{C}^3(A)$ es no asociativa ni conmutativa, pero sí alternativa; y a partir de $\mathfrak{C}^4(A)$ resultarán álgebras no alternativas. Así que las $\mathbb{K}$-álgebras cuaterniónicas son no conmutativas, y las de Cayley u octoniónicas son no asociativas, pero alternativas. $\triangleleft$

Ahora veremos qué relaciones hay en el caso de formas cuadráticas no degeneradas, y la división y los inversos multiplicativos.

Veamos que el proceso de Cayley-Dickson, cuando tomamos $\mu \neq 0$, también nos da una forma cuadrática $N_{\mathfrak{C}(A)}$ no degenerada si partimos de un álgebra A con una forma cuadrática N no degenerada:$\triangleright$ Consideremos de nuevo $x = a + vb, y = c + vd$, así tenemos para la forma $\mathbb{K}$-bilineal

$$\begin{aligned}(x,y)_{N_{\mathfrak{C}(A)}} &= N_{\mathfrak{C}(A)}(x+y) - N_{\mathfrak{C}(A)}(x) - N_{\mathfrak{C}(A)}(y) \\ &= N_{\mathfrak{C}(A)}(a+c+v(b+d)) - N_{\mathfrak{C}(A)}(a+vb) - N_{\mathfrak{C}(A)}(c+vd) \\ &= N(a+c) - \mu N(b+d) - N(a) + \mu N(b) - N(c) + \mu N(d) \\ &= N(a+c) - N(a) - N(c) - \mu(N(b+d) - N(b) - N(c)) \\ &= (a,c)_N - \mu(b,d)_N.\end{aligned}$$

Con esto, resulta que si para todo $y = c + vd \in \mathfrak{C}(A)$ pasa que $(x,y)_{N_{\mathfrak{C}(A)}} = 0$, tenemos que $(a,c)_N = \mu(b,d)_N$. En particular para $c = 0$, como $\mu \neq 0$, entonces tenemos que para todo $d \in A$: $(b,d)_N = 0$, y como N es no degenerada, esto implica que $b = 0$. Ahora, para $d = 0$, tenemos entonces que para todo $c \in A$: $(a,c)_N = 0$, esto es $a = 0$, pues N es no degenerada. Por lo tanto $a = 0 = b$, i. e. $x = 0 + v0 = 0$, esto nos dice que $N_{\mathfrak{C}(A)}$ es no degenerada $\triangleleft$ y establecemos lo siguiente:

Proposición 3.6. *Para una $\mathbb{K}$-álgebra A con involución cuadrática (i. e. que cumple (5)), considerando la forma cuadrática $N_A(a) = aa^*$, y aplicando el proceso de Cayley-Dickson con $\mu \neq 0$, tenemos que si N es no degenerada, entonces $N_{\mathfrak{C}(A)}$ también lo es.*

Ahora, para el caso de un álgebra alternativa con involución cuadrática tenemos que la forma cuadrática natural en esta, $N(a) = aa^*$, permite hacerla un álgebra de composición, si N es no degenerada. $\triangleright$ Para esto definiremos de una vez la parte «real» y la parte «imaginaria» de un elemento: En una $\mathbb{K}$-álgebra A con involución cuadrática, definimos la **parte real** y la **imaginaria de un elemento** $a \in A$, respectivamente, como:

$$Re(a) = \frac{1}{2}(a + a^*), \qquad Im(a) = \frac{1}{2}(a - a^*).$$

Evidentemente $a = Re(a) + Im(a)$ y $a^* = Re(a) - Im(a)$, así que tanto a como a^* son elementos del álgebra generada por los dos elementos $Re(a), Im(a) \in A$. Recordemos que por el teorema de Artin (teorema 2.1), siendo A alternativa, el álgebra generada por los dos elementos $Re(a), Im(a) \in A$, es una subálgebra asociativa de A. Por lo tanto tenemos que:

$$N(ab) = (ab)(ab)^* = (ab)(b^*a^*) = a(bb^*)a^* = (bb^*)(aa^*) = N(a)N(b).$$

En las últimas dos igualdades hemos usado la conmutatividad con los elementos de $\mathbb{K}e$.$\triangleleft$ Resumimos esto mediante la siguiente:

Proposición 3.7. *Una $\mathbb{K}$-álgebra alternativa con involución cuadrática cuya forma cuadrática $N(a) = aa^*$ es no degenerada, es un álgebra de composición.*

También podemos definir la **parte real** y la **parte imaginaria de una álgebra** A con involución cuadrática, respectivamente como

$$Re(A) = \{a \in A : Im(a) = 0\} = \{a \in A : a = a^*\} \quad \text{y}$$

$$Im(A) = \{a \in A : Re(a) = 0\} = \{a \in A : a + a^* = 0\} = \{a \in A : a^* = -a\}.$$

Entonces un **elemento** a es **real** si $a = a^*$ y es **imaginario** si $a^* = -a$. Más aún, es claro que como espacio vectorial se tiene que $A = Re(A) \oplus Im(A)$.

Considerando las dos proposiciones anteriores, cabe notar que cuando partimos de $\mathbb{K}$ con $* = id_{\mathbb{K}}$, tenemos que $N_{\mathbb{K}}(\kappa) = \kappa^2$, y claramente $(\kappa, \lambda)_{N_{\mathbb{K}}} = 2\kappa\lambda$, siendo $\mathbb{K}$ un campo, $N_{\mathbb{K}}$ resulta ser no degenerada. Por lo tanto partiendo del álgebra de composición $\mathbb{K}$ obtenemos mediante el proceso de Cayley-Dickson una sucesión de álgebras de composición hasta el tercer paso, tomando $\mu \neq 0$ en cada iteración.

Llamaremos **$\mathbb{K}$-álgebras de Cayley-Dickson** a las álgebras obtenidas mediante el proceso de Cayley-Dickson aplicado a $\mathbb{K}$ cierta cantidad de veces o iteraciones, incluyendo a $\mathbb{K}$ (la iteración 0). Cabe notar que para un álgebra de Cayley-Dickson $\mathcal{A}$ se tiene que $Re(\mathcal{A}) = \mathbb{K}$, pues para t la última iteración, $a_{t'}^* - v_t b_{t'} = a_{t'} + v_t b_{t'}$, implica que $b_{t'} = 0$, siendo $t' = t - 1$ la iteración anterior, así, sucesivamente se concluye que $b_t = b_{t-1} = ... = b_1 = 0$, i. e. $a_{t-1} + v_t b_{t-1} = a_0 + v_t 0 \in \mathbb{K}e$. Antes de indagar en otras propiedades, veremos la muy útil:

Proposición 3.8. *Dada un álgebra unital alternativa A con involución cuadrática. Si una subálgebra $B \subset A$, cumple las siguientes condiciones: $1 \in B$, hay un $v \in A - B$ tal que $v^2 = \mu \in \mathbb{K}$ y para todo $b \in B$ $bv = vb^*$ (o equivalentemente $b^*v = vb$), entonces la multiplicación en el subespacio vectorial $B \oplus vB \subseteq A$, que es la que se sigue por la propiedad distributiva de A, resulta ser la definida en el proceso de Cayley-Dickson; más aún, si $\mu \neq 0$ y $v^* = -v$, el mismo subespacio $B \oplus vB$ resulta ser el álgebra obtenida mediante el proceso de Cayley-Dickson: $(\mathfrak{C}(B), \mu)$.*

▷ Sean B y v como en la hipótesis. Para probarla usaremos las siguientes identidades válidas para $\forall a, b \in B$:

$$a(vb) = v(a^*b) \qquad (va)b = v(ba) \qquad (va)(vb) = \mu ba^*.$$

Para corroborar la primera, por ser A alternativa, tenemos que $(v, a^*, b) = -(a^*, v, b)$, así, considerando las hipótesis sobre v y que $a + a^* \in \mathbb{K}$, tenemos que

$$
\begin{aligned}
0 &= (v, a^*, b) + (a^*, v, b) \\
&= (va^*)b - v(a^*b) + (a^*v)b - a^*(vb) \\
&= (va^*)b - v(a^*b) + (va)b - a^*(vb) \\
&= (va^* + va)b - v(a^*b) - a^*(vb) \\
&= (v(a + a^*))b - a^*(vb) - v(a^*b) \\
&= (a + a^*)vb - a^*(vb) - v(a^*b) \\
&= ((a + a^*) - a^*)vb - v(a^*b) \\
&= a(vb) - v(a^*b).
\end{aligned}
$$

Para la segunda, algo similar ocurre. Para la tercera, usamos la tercera identidad de Moufang que satisface A por ser un álgebra alternativa, así tenemos que

$$
\begin{aligned}
(va)(vb) &= (va)(b^*v) = v((ab^*)v) = v(v(ab^*)^*) \\
&= v(v(ba^*)) = v^2ba^* = \mu ba^*.
\end{aligned}
$$

Mediante las tres identidades verificamos que para $(a + vb), (c + vd) \in B \oplus vB$, por la distributividad del producto,

$$
\begin{aligned}
(a + vb)(c + vd) &= ac + a(vd) + (vb)c + (vb)(vd) \\
&= ac + v(a^*d) + v(bc) + \mu bd^* \\
&= ac + \mu bd^* + v(a^*d + bc).
\end{aligned}
$$

Con lo cual comprobamos que la multiplicación en $B \oplus vB$ es la definida en el proceso de Cayley-Dickson. Ahora supongamos que $\mu \neq 0$ y $v^* = -v$. Con esto tenemos que $(a + vb)^* = a^* + (vb)^* = a^* + b^*v^* = a^* - b^*v = a^* - vb$, así que la involución en $B \oplus vB$ es la definida en el proceso de Cayley-Dickson. Solo nos resta ver que podemos identificar B y vB espacios vectoriales, es decir, definir un isomorfismo de $\mathbb{K}$-espacios vectoriales entre ambos, pues así $B \oplus vB \cong B \oplus B$ como espacios vectoriales y entonces $B \oplus vB$, por cómo son sus operaciones, es el álgebra obtenida mediante la construcción de Cayley-Dickson para dicha μ. Esto es fácil, definamos $r : B \longrightarrow vB$ como $r(b) = vb$, así es claramente es $\mathbb{K}$-lineal y suprayectiva, y también inyectiva, pues su núcleo es $\{0\}$: si $0 = r(b) = vb$, entonces $0 = v0 = v(vb) = v^2b = \mu b$, como $\mu \neq 0$, esto implica que $b = 0$; por tanto r es un isomorfismo. $\triangleleft$

Ahora trataremos la división, para lo cual, partiremos de la siguiente:

Proposición 3.9. *Un álgebra alternativa A, con involución cuadrática, es un álgebra con división si y solo si $\forall a \in A - \{0\}$: $N(a) \neq 0$, en tal caso cada $a \in A - \{0\}$ tiene inverso.*

▷ Supongamos que $\forall a \in A - \{0\}$: $N(a) \neq 0$, así, como $aa^* = a^*a = N(a)$, tenemos que $a^*(ab) = (a^*a)b = (aa^*)b = N(a)b$. Como $N(a) \in \mathbb{K}e \cong \mathbb{K}$, existe $N(a)^{-1}$, más aún, evidentemente tenemos que $N(a)^{-1}L_{a^*}$ es la inversa de L_a, pues

$$\begin{aligned} N(a)^{-1}L_{a^*}(L_a(b)) &= N(a)^{-1}L_{a^*}(ab) \\ &= N(a)a^*(ab) = N(a)^{-1}N(a)b = 1b = b, \end{aligned}$$

y también $L(a)N(a)^{-1}L_{a^*}(b) = b$. Análogamente para R_a, tenemos su inversa $N(a)^{-1}R_{a^*}$, por lo tanto A es un álgebra con división. Ahora, si existiera $a \in A$ tal que $a \neq 0$ y $0 = N(a) := aa^* = a^*a$, evidentemente a y a^* serían divisores de cero, así que no puede ser un álgebra con división; por lo tanto, si A es un álgebra con división, entonces $\forall a \in A - \{0\}$: $N(a) \neq 0$. De hecho en estos casos (con unidad, alternatividad e involución), cada elemento $a \neq 0$ tiene inverso multiplicativo: $\frac{1}{N(a)}a^* = N(a)^{-1}a^*$. ◁

Estaremos tratando con estas álgebras construidas mediante el proceso de Cayley-Dickson hasta la tercera iteración, así todas serán álgebras unitales alternativas con involución. Podemos encontrarnos con un álgebra con división o una con divisores de cero, estas últimas pueden provenir de haber tomado $\mu = 0$ en una o varias iteraciones, en este caso las llamaremos álgebras **duales**, o pueden provenir de iteraciones todas con $\mu \neq 0$, en este caso las llamamos álgebras **escindidas**.

Como *nota* citamos un resultado concerniente a la división, es un corolario de teorema de Wedderburn-Artin (Voight, 2021, p. 96) que nos dice que un álgebra cuaterniónica es simple central y que en el caso de no ser un álgebra de división, es isomorfa a la de las matrices de 2×2 sobre $\mathbb{K}$: $M_2(\mathbb{K})$. Para las álgebras de Cayley, tenemos un resultado similar (Schafer, 1966, p. 52, 72): una álgebra de Cayley escindida es única (salvo isomorfismos), y es la obtenida al aplicar el proceso de Cayley-Dickson al álgebra cuaterniónica escindida $M_2(\mathbb{K})$ con $\mu = 1$, esto es $(\mathfrak{C}(M_2(\mathbb{K})), 1)$. Schafer (1966) considera $\mu \neq 0$ es su definición del procesos de Cayley-Dickson, por lo que las únicas álgebras con divisores de cero que considera son las escindidas; en nuestro caso, al admitir $\mu = 0$ obtenemos otras álgebras con divisores de cero, pero no isomorfas a estas escindidas. Esto lo corroboramos más adelante.

Veremos un resultado que nos facilita saber cuándo estamos tratando con la misma álgebra salvo isomorfismo, este resultado se atribuye al matemático Nathan Jacobson. Para ver este resultado, daremos otro breve paseo por la teoría de formas cuadráticas.

En el párrafo siguiente, nos hemos basado en Lam (2005) y Artin (1957) para los detalles. Llamamos **espacio cuadrático** (V, q) a un $\mathbb{K}$-espacio vectorial V y una forma cuadrática q definida para éste; como sabemos, con esto tenemos una forma bilineal $(,)_q$ que nos permite definir la nociones de «tamaño» y «ortogonalidad». Definimos la **suma ortogonal** de dos espacios cuadráticos (V_1, q_1) y (V_2, q_2), como el espacio cuadrático $(V_1 \perp V_2, q_1 \perp q_2)$, donde $V_1 \perp V_2 = V_1 \oplus V_2$ y $q_1 \perp q_2$ es la forma cuadrática para $V_1 \oplus V_2$ definida como $q_1 \perp q_2(v_1, v_2) = q_1(v_1) + q_2(v_2)$. Un *isomorfismo entre espacios cuadráticos* es un isomorfismo de espacios vectoriales $\varphi : V_1 \longrightarrow V_2$ tal que $\forall u \in V_1$: $q_2(\varphi(u)) = q_1(u)$, también se dice que es una **isometría** y decimos que son espacios isométricos y lo denotamos $(V_1, q_1) \cong (V_2, q_2)$, o que las **formas cuadráticas son equivalentes** denotándolo también como $q_1 \cong q_2$; en tal caso también se cumple que para todo $u, v \in V_1$: $(\varphi(u), \varphi(v))_{q'} = (u, v)_q$, pues φ es lineal y así tenemos que

$$\begin{aligned}(\varphi(u), \varphi(v))_{q'} &= (\varphi(u) + \varphi(v)) - q'(\varphi(u)) - q'(\varphi(v)) \\ &= q'(\varphi(u+v)) - q'(\varphi(u)) - q'(\varphi(v)) \\ &= q(u+v) - q(u) - q(v) = (u,v)_q q'.\end{aligned}$$

Dado un espacio cuadrático (V, q), el **complemento ortogonal** de un subconjunto $U \subseteq V$ es el subespacio $U^\perp = \{w \in V : \forall u \in U (w, u)_q = 0\}$ (que en efecto es subespacio por la bilinealidad de $(,)_q$); notemos que no necesariamente pasa que $V = U \perp U^\perp$, se requieren algunas condiciones adicionales, por ejemplo, que q sea no degenerada, que U sea un subespacio y $q|_U$ sea no degenerada, como lo vemos en Artin (1957) (parte del teorema 3.5, p. 117) y que mencionamos porque nos servirá más adelante:

Dado un espacio bilineal no singular V, y un subespacio U; este U es no singular si y solo si $U^\perp$ es no singular. En cuyo caso se tiene que $V = U \perp U^\perp$.

Un $\mathbb{K}$-**espacio bilineal** es un $\mathbb{K}$-espacio vectorial V con una forma bilineal $(,) : V \times V \longrightarrow \mathbb{K}$. La terminología de no singular se usa cuando la forma bilineal es no singular (i. e. es no degenerada) y corresponde a que

$$\{u \in V : \forall v \in V,\ (v, u) = 0\} = \{u \in V : \forall v \in V,\ (u, v) = 0\} = \{0\},$$

es decir, los núcleos de la forma bilineal son, ambos, el subespacio cero o trivial, y usada con subespacios $U \subseteq V$, se refiere a que la forma bilineal restringida a tal subespacio; claramente la noción de que un (sub)espacio sea no singular equivale a que $U \cap U^\perp = \{0\}$, y claro que tenemos la noción de espacio «singular» como aquel que no cumple tal propiedad. Artin llama a una forma bilineal estructura métrica y de ahí que a un *isomorfismo de espacios bilineales* le llame isometría, término que ya vimos y que se aplica para un isomorfismo de espacios vectoriales $\varphi : V \longrightarrow W$ tal que $(\varphi(u), \varphi(v))_W = (u, v)_V$, donde $(,)_W$ y $(,)_V$ son las formas bilineales correspondientes a cada espacio bilineal.

En nuestro contexto tenemos lo siguiente: un álgebra unital $\mathcal{A}$ con involución cuadrática y su forma cuadrática $N(a) = aa^*$ se puede descomponer como $\mathbb{K} \perp \mathbb{K}^\perp$ (recordemos que hemos identificado $\mathbb{K} \cong \mathbb{K}e$), esto se debe a que si $b \in \mathbb{K}^\perp$, entonces para todo $k \in \mathbb{K}$ tenemos que $0 = (b,k)_N = bk^* + kb^* = bk + kb^* = kb + kb^* = 2k(b + b^*)$, por lo tanto $b + b^* = 0$, así $\mathbb{K} \cap \mathbb{K}^\perp = \{0\}$; de hecho podemos notar que $\mathbb{K} = Re(\mathcal{A})$ y $\mathbb{K}^\perp = Im(\mathcal{A})$, con esto podemos expresar cualquier $a \in \mathcal{A}$ como $k + b$, con $k \in \mathbb{K}$ y $b \in \mathbb{K}^\perp$, más aún, como $k^* = k$ y $b^* = -b$, tenemos que

$$\begin{aligned} N(a) &= (k+b)(k+b)^* = (k+b)(k^* + b^*) \\ &= kk^* + kb^* + bk^* + bb^* = kk + k(b-b) + bb^* \\ &= k^2 + bb^* = N_{\mathbb{K}}(k) + N_{\mathbb{K}^\perp}(b). \end{aligned}$$

Siendo $N_{\mathbb{K}}$ y $N_{\mathbb{K}^\perp}$ la restricción de N respectivamente a $\mathbb{K}$ y $\mathbb{K}^\perp$, claramente son formas cuadráticas y así tenemos que $N = N_{\mathbb{K}} \perp N_{\mathbb{K}^\perp} = N_{Re(\mathcal{A})} \perp N_{Im(\mathcal{A})}$.

Ahora mencionamos uno de los resultados más célebres en esta área, el teorema de Witt, cuya demostración aparece en Artin (1957), teorema 3.9, p. 121 (una versión sólo para formas cuadráticas en Lam (2005), p. 14); nombrado en honor al matemático Ernst Witt. Antes, hace falta mencionar que dos espacios bilineales $(V, (,)_V)$ y $(W, (,)_W)$ son isométricos cuando existe un isomorfismo de $\mathbb{K}$-espacios vectoriales $\sigma : V \longrightarrow W$ tal que $\forall u, v \in V\ (u,v)_V = (\sigma(u), \sigma(v))_W$. Noción que coincide con la de espacios cuadráticos considerando la forma bilineal $(,)_q$ relacionada con una forma cuadrática q.

Dados dos espacios bilineales no singulares isométricos V y V'. Una isometría entre dos subespacios $\sigma : U \subseteq V \longrightarrow U' \subseteq V'$ puede extenderse a una isometría entre los espacios que los contienen $\overline{\sigma} : V \longrightarrow V'$, i. e. $\overline{\sigma}|_U = \sigma$ y $\overline{\sigma}[U^\perp] = U'^\perp$.

Finalmente algunas definiciones que nos serán útiles, dado un espacio bilineal V, decimos que $v \in V$ es un **vector isotrópico** cuando $(v,v) = 0$ y un subespacio $U \subseteq V$ es un **subespacio isotrópico** cuando $\forall u, v \in U$ ocurre que $(u,v) = 0$; con lo cual, que $U \neq \{0\}$ y U sea isotrópico implica que es también un espacio singular; por cierto, un ejemplo de espacio isotrópico es el subespacio $\{0\}$ (el único espacio isotrópico no singular). Vale mencionar que una relación entre estos dos conceptos de isotropía se da cuando la forma bilineal es simétrica (es decir, $\forall u, v \in V : (u,v) = (v,u)$), en tal caso, si todo vector en V es isotrópico, entonces V es isotrópico, o la contrapositiva equivalente: *dado un espacio no isotrópico V, existe algún vector $v \in V$ no isotrópico* que nos será útil; siendo fácil verificarlo, pues que todo vector en V sea isotrópico implica que para $u, v \in V$ arbitrarios, como $0 = (u+v, u+v) = (u,u) + (u,v) + (v,u) + (v,v) = 0 + (u,v) + (v,u) + 0$, entonces $(u,v) = -(v,u)$, y como suponemos que $(,)$ es simétrica también tenemos que $(u,v) = (v,u)$, por lo tanto $-(v,u) =$

(v,u), así que $(v,u)=0$, es decir V es isotrópico. Cabe mencionar que en nuestro contexto partimos de formas cuadráticas (obtenidas de la involución que a propósito hemos llamado involución cuadrática); pero como hemos podido apreciar, resulta interesante ver qué pasa si se parte de formas bilineales, como hace Artin (1957) en el capítulo III.

Para ver la prueba del teorema de Jacobson que a continuación enunciamos, nuevamente seguimos a Schafer (1966) (teorema 2.23, p. 71) y nos será útil el siguiente lema. (Aclaramos que estaremos usando las letras N y N' para las formas cuadráticas correspondientes, considerando las restricciones en cada caso):

Lema 3.10. *Sea $\mathcal{C}$, un álgebra de Cayley-Dickson alternativa, y consideremos una subálgebra propia $\mathcal{B}\subset\mathcal{C}$ y $\mathcal{B}\neq\mathcal{C}$, que también podemos considerar como un espacio bilineal con la forma bilineal $(,)_N$ inducida por la forma cuadrática $N(a)=aa^*$. Si $\mathcal{B}$ es tal que $1\in\mathcal{B}$ y es no isotrópica, entonces existe una subálgebra $\mathcal{D}\subseteq\mathcal{C}$ tal que $\mathcal{D}=\mathcal{B}\oplus v\mathcal{B}$ y es el álgebra obtenida mediante el proceso de Cayley-Dickson aplicado a $\mathcal{B}$ para cierta $\mu\in\mathbb{K}$ con $\mu=N(v)$ y $v\in\mathcal{B}^{\perp}$.*

Que comprobamos haciendo uso de la proposición 3.8. $\triangleright$ Primero notemos que la involución de $\mathcal{C}$ induce una en $\mathcal{B}$; primero, de que $1\in\mathcal{B}$ se sigue que $\mathbb{K}1\subseteq\mathcal{B}$, entonces, para $b\in\mathcal{B}$, tenemos que $b+b^*\in\mathbb{K}1\subseteq\mathcal{B}$ y entonces $b^*=(b+b^*)-b\in\mathcal{B}$. Siendo $\mathcal{B}\neq\{0\}$ no isotrópico, es también no singular y por lo mencionado antes, tenemos que $\mathcal{C}=\mathcal{B}\perp\mathcal{B}^{\perp}$, $\mathcal{B}^{\perp}$ es no isotrópica también, y hay un vector no isotrópico $v\in\mathcal{B}^{\perp}$, que en nuestro contexto significa que

$$0\neq(v,v)_N=vv^*+v^*v=2vv^*,$$

así digamos que $N(v)=vv^*=-\mu\in\mathbb{K}-\{0\}$. Por otro lado, tenemos que $v+v^*=v1+1v^*=v1^*+1v^*=(v,1)_N=0$, pues $v\in\mathcal{B}^{\perp}$ y $1\in\mathcal{B}$, así $v^*=-v$, y por tanto $v^2=-vv^*=\mu$; con esto también tenemos que para todo $b\in\mathcal{B}$: $bv=vb^*$, pues $vb^*-bv=vb^*+bv^*=(v,b)_N=0$. Ahora veremos que $v\mathcal{B}\subseteq\mathcal{B}^{\perp}$; para esto usaremos que $\forall a,b,c\in A$

$$(ab)c+((ab)c)^*=a(bc)+(a(bc))^*,$$

para comprobarlo notemos que debido a la proposición 1.6, $\forall a,b,c\in A$

$$(a,b,c)=-(c,b,a)=-(-1)^3(c^*,b^*,a^*)=(c^*,b^*,a^*),$$

con lo que se cumple la serie de igualdades en cada columna

$$\begin{aligned}(ab)c-a(bc)&=(c^*b^*)a^*-c^*(b^*a^*)\\(ab)c+c^*(b^*a^*)&=(c^*b^*)a^*+a(bc)\\(ab)c+c^*(ab)^*&=(bc)^*a^*+a(bc)\\(ab)c+((ab)c)^*&=(a(bc))^*+a(bc).\end{aligned}$$

Ahora, considerando $a, b \in \mathcal{B}$, como $a^* \in \mathcal{B}$ tenemos que $ba^* \in \mathcal{B}$, así $(v, ba^*)_N = 0$; entonces, lo anterior nos permite asegurar la segunda igualdad en

$$\begin{aligned}(va, b)_N &= (va)b^* + ((va)b^*)^* \\ &= v(ab^*) + (v(ab^*))^* = (v, (ab^*)^*) = (v, ba^*)_N = 0.\end{aligned}$$

Por tanto $va \in \mathcal{B}^\perp$, siento $a \in \mathcal{B}$ arbitrario, entonces $v\mathcal{B} \subseteq \mathcal{B}^\perp$; así podemos considerar $\mathcal{B} \oplus v\mathcal{B}$. Con esto hemos reunido las hipótesis necesarias en la proposición 3.8 y por tanto $\mathcal{B} \oplus v\mathcal{B} = (\mathfrak{C}(\mathcal{B}), \mu)$, con lo que probamos el lema. ◁

Teorema 3.11. *Sean $n \in \{1, 2, 3\}$ y $\mu_1, \mu_2, \mu_3, \mu'_1, \mu'_2, \mu'_3 \in \mathbb{K} - \{0\}$; así dos álgebras de Cayley-Dickson $\mathcal{A} = (\mathfrak{C}^n(\mathbb{K}), \mu_1, ..., \mu_n)$ y $\mathcal{A}' = (\mathfrak{C}^n(\mathbb{K}), \mu'_1, ..., \mu'_n)$ (alternativas pues $n \leq 3$) son isomorfas si y solo si sus formas cuadráticas correspondientes, N y N', son equivalentes (es decir, son isomorfas como álgebras con involución si y solo si son isomorfas como espacios cuadráticos).*

▷ Al ser $\mathcal{A}$ y $\mathcal{A}'$ álgebras unitales, ambas contienen una «copia isomorfa» de $\mathbb{K}$, que para facilitar los cálculos identificaremos ($\mathbb{K}e \cong \mathbb{K} \cong \mathbb{K}e'$, denotando con 1 la unidad en las tres). Supongamos que $\mathcal{A} \cong \mathcal{A}'$ y que $t : \mathcal{A} \longrightarrow \mathcal{A}'$ es el isomorfismo de álgebras unitales con involución que lo corrobora, entonces es claro que (por definición) es $\mathbb{K}$-lineal, también $t(1) = 1$ y $t(a^*) = (t(a))^*$, y preserva productos; más aún como $aa^* \in \mathbb{K}$ para cualquier $a \in \mathcal{A}$, tenemos que

$$\begin{aligned}N(t(a)) &= (t(a))(t(a))^* \\ &= t(a)t(a^*) = t(aa^*) \\ &= t((aa^*)1) = aa^*t(1) = aa^*(1) = aa^* = N(a),\end{aligned}$$

con lo cual hemos mostrado que sus formas cuadráticas son equivalentes. De hecho podemos notar que esta implicación se cumple en general para cualesquiera dos álgebras unitales con involución cuadrática isomorfas.

Ahora probaremos la implicación en sentido contrario. Supongamos que las formas cuadráticas de $\mathcal{A}$ y $\mathcal{A}'$, respectivamente N y N', son equivalentes, esto es, son espacios cuadráticos isométricos. Si $\mathcal{B} \subset \mathcal{A}$ y $\mathcal{B}' \subset \mathcal{A}'$ son respectivamente subálgebras no isotrópicas con unidad e involución, y tenemos un isomorfismo de álgebras unitales con involución $h_0 : \mathcal{B} \longrightarrow \mathcal{B}'$, con lo que son isométricos, conforme a lo visto en la primera implicación del teorema; entonces el teorema de Witt nos dice que existe una extensión de h_0, como isometría, digamos $\overline{h_0} : \mathcal{A} \longrightarrow \mathcal{A}'$, así $\overline{h_0}[\mathcal{B}^\perp] = \mathcal{B}'^\perp$, con lo que también $\mathcal{B}^\perp$ y $\mathcal{B}'^\perp$ son isométricos, considerando las restricciones de N y N' correspondientes. Ahora, como $\mathcal{B}$ es no isotrópica, por lo visto en la prueba del lema 3.10, entonces existe un vector no isotrópico $v \in \mathcal{B}^\perp$ con $N(v) = vv^* = -\mu \in \mathbb{K} - \{0\}$; sea

$v' = \overline{h_0}(v) \in \mathcal{B}'^{\perp}$, así, como $1 \in \mathcal{B}'$, tenemos que $0 = (v', 1)_{N'} = v'1^* + 1(v')^* = v' + (v')^*$, así que $(v')^* = -v'$, entonces $(v')^2 = -v'(v')^* = \mu$, pues $v'(v')^* = \overline{h_0}(v)(\overline{h_0}(v))^* = N'(\overline{h_0}(v)) = N(v)$, así que v' es no isotrópico, por tanto podemos considerar a las subálgebras $\mathcal{B} \oplus v\mathcal{B}$ y $\mathcal{B}' \oplus v'\mathcal{B}'$ como las obtenidas mediante el proceso de Cayley-Dickson, respectivamente para $\mu = N(v)$ y $\mu' = N(v') = \mu$. De inmediato podemos definir un isomorfismo de álgebras unitales con involución entre éstas, como $h : \mathcal{B} \oplus v\mathcal{B} \longrightarrow \mathcal{B}' \oplus v'\mathcal{B}'$, $h(a + vb) = h_0(a) + v'h_0(b)$, para $a, b \in \mathcal{B}$; claramente es $\mathbb{K}$-lineal, preserva la unidad 1 y respeta productos, pues h_0 lo hace (así lo supusimos), para muestra, sean $a, b, c, d \in \mathcal{B}$, así

$$\begin{aligned}
&h\left((a + vb)(c + vd)\right) \\
&\quad = h(ac + \mu db^* + v(a^*d + cb)) \\
&\quad = h_0(ac + \mu db^*) + v'h_0(a^*d + cb) \\
&\quad = h_0(a)h_0(c) + \mu h_0(d)h_0(b)^* + v'\left(h_0(a)^*h_0(d) + h_0(c)h_0(b)\right) \\
&\quad = \left(h_0(a) + v'h_0(b)\right)\left(h_0(c) + v'h_0(d)\right) = h(a + vb)h(c + vd).
\end{aligned}$$

Finalmente, tenemos

$$\begin{aligned}
h\left((a + vb)^*\right) &= h(a^* - vb) \\
&= h_0(a)^* - v'h_0(b) \\
&= \left(h_0(a) + v'h_0(b)\right)^* = h(a + vb)^*.
\end{aligned}$$

Después de todo esto podemos finalmente probar el teorema. Como cada álgebra $\mathcal{A}$ y $\mathcal{A}'$ tiene una copia isomorfa de $\mathbb{K}$, y claramente $\mathbb{K}$ es no isotrópica, podemos partir de dicho isomorfismo de álgebras unitales con involución y aplicar lo anterior, lo cual lo podemos hacer pues $n \leq 3$ y así $\mathcal{A}$ y $\mathcal{A}'$ son alternativas, por tanto tenemos que $\mathcal{C} = \mathbb{K} \oplus v\mathbb{K} \subseteq \mathcal{A}$ y $\mathcal{C}' = \mathbb{K} \oplus v'\mathbb{K} \subseteq \mathcal{A}'$ son álgebras unitales con involución isomorfas, para ciertos $v \in \mathcal{A} - \mathbb{K}$ y $v' \in \mathcal{A}' - \mathbb{K}$; si $dim(\mathcal{A}) = dim(\mathcal{A}') = 2$, con esto ya terminamos, si no, podemos partir de este isomorfismo y tendremos un isomorfismo entre $\mathcal{H} = \mathcal{C} \oplus w\mathcal{C} \subseteq \mathcal{A}$ y $\mathcal{H}' = \mathcal{C}' \oplus w'\mathcal{C}' \subseteq \mathcal{A}'$, para ciertos $w \in \mathcal{A} - \mathcal{C}$ y $w' \in \mathcal{A}' - \mathcal{C}'$, si $dim(\mathcal{A}) = dim(\mathcal{A}') = 2^2 = 4$, con esto terminamos, si no, volvemos a aplicar un razonamiento similar y como $dim(\mathcal{A}) = dim(\mathcal{A}') \leq 2^3 = 8$, necesariamente tenemos el isomorfismo entre $\mathcal{A}$ y $\mathcal{A}'$ que buscamos. $\triangleleft$

Antes de pasar a ver ejemplos concretos con $\mathbb{K} = \mathbb{R}$, planteamos algunas propiedades que cumplen estas álgebras en general, una es la siguiente:

Proposición 3.12. *Dada un álgebra con involución cuadrática A, entonces para cualquier $b \in Im(A) = \mathbb{K}^{\perp}$ se cumple que*

$$b^* = -b \qquad y \qquad b^2 = -N(b) \in \mathbb{K}.$$

Con esto podemos probar que un isomorfismo de álgebras $f : A \longrightarrow A'$ entre dos álgebras con involución cuadrática es un morfismo de álgebras con involución (y también una isometría), además $f[Im(A)] \subseteq Im(A')$.

▷ Ya habíamos visto que para $b \in \mathbb{K}^{\perp} = Im(A)$ se tiene que $b + b^* = 0$ cuando tratamos propiedades de espacios cuadráticos y bilineales, más aún, como $N(b) = bb^* = -bb = -b^2$, por tanto tenemos ambas igualdades.

Para probar la última parte, sean A y A' dos álgebras con involución cuadrática y $f : A \longrightarrow A'$ un isomorfismo de álgebras, es decir una función $\mathbb{K}$-lineal que preserva productos y $f(1) = 1$, entonces queremos probar que también preserva la involución, para esto veremos varias propiedades interesantes. De la $\mathbb{K}$-linealidad se sigue que para todo $k \in Re(A) = \mathbb{K}$, $f(k) \in Re(A') = \mathbb{K}$, pues tenemos que $f(k) = f(k1) = kf(1) = k1 = k$. Por otro lado, es claro que un $b \in A$ cumple que $b \in Im(A)$ si y solo si $b \notin \mathbb{K}$, lo cual se sigue de que $Im(A) = \mathbb{K}^{\perp}$; siendo f un isomorfismo de álgebras, tiene una inversa f^{-1}, esto nos ayuda a probar que $b \in Im(A)$ implica que $f(b) \in Im(A')$, pues tenemos que si $f(b) \in \mathbb{K}$, entonces $b = f^{-1}(f(b)) = f^{-1}(f(b)1) = f(b)f^{-1}(1) = f(b)1 = f(b)$ (pues f^{-1} también es morfismo de álgebras), esto es, $b \in \mathbb{K}$, por tanto $b \notin \mathbb{K}$ implica $f(b) \notin \mathbb{K}$, que es lo queríamos comprobar, así $f[Im(A)] \subseteq Im(A')$; ahora tomamos $a \in A$, como

$$Re(f(a)) + Im(f(a)) = f(a) = f(Re(a) + Im(a)) = f(Re(a)) + f(Im(a)),$$

y sabemos que $A' = Re(A') \oplus Im(A')$, $f(Re(a)) \in Re(A')$ y $f(Im(a)) \in Im(A')$, tenemos que $Re(f(a)) = f(Re(a))$ e $Im(f(a)) = f(Im(a))$. Esto por sí mismo es muy útil, pero tenemos aún, ya que con esto podemos probar que f es una isometría, primero notemos que para $b \in Im(A)$, como $f(b) \in Im(A')$, tenemos:

$$-N'(f(b)) = (f(b))^2 = f(b^2) = f(-N(b)) = -N(b)f(1) = -N(b),$$

pues para $k \in Re(A) = \mathbb{K}$ tenemos que $N(k) = k^2$, y de manera similar concluimos que $N'(f(k)) = N(k)$; entonces tenemos que

$$\begin{aligned}
N'(f(a)) = f(a)f(a)^* &= \left(Re(f(a)) + Im(f(a))\right)\left(Re(f(a)) + Im(f(a))\right)^* \\
&= \left(Re(f(a)) + Im(f(a))\right)\left(Re(f(a))^* + Im(f(a))^*\right) \\
&= \left(Re(f(a)) + Im(f(a))\right)\left(Re(f(a)) - Im(f(a))\right) \\
&= \left(Re(f(a))\right)^2 - \left(Im(f(a))\right)^2 \\
&= \left(f(Re(a))\right)^2 - \left(f(Im(a))\right)^2 \\
&= N'\left(f(Re(a))\right) + N'\left(f(Im(a))\right) \\
&= N\left((Re(a))\right) + N\left((Im(a))\right) = N(a).
\end{aligned}$$

Esto nos asegura que para todo $a, a' \in A$, se satisface que $(f(a), f(a'))_{N'} = (a, a')_N$ (una propiedad que vimos cuando definimos las isometrías). Esto último nos permite, finalmente, comprobar que f preserva involuciones, pues $f(a)^* = (f(a) + f(a)^*) - f(a) = (f(a)1^* + f(a)^*1) - f(a) = (f(a), 1)_{N'} - f(a)$, así:

$$\begin{aligned} f(a)^* &= (f(a), 1)_{N'} - f(a) \\ &= (f(a), f(1))_{N'} - f(a) \\ &= (a, 1)_N - f(a) \\ &= f\left((a, 1)_N\right) - f(a) \\ &= f\left((a, 1)_N - a\right) = f(a^*). \end{aligned}$$

Cabe mencionar que este resultado nos indica que en el caso de isomorfismos entre álgebras con involución cuadrática no se requiere que preserven involuciones, pues basta con que preserve productos y $1 \mapsto 1$. $\triangleleft$

Ahora aprovecharemos para ver algunos detalles concernientes a lo que podemos llamar una base «canónica» para un álgebra de Cayley-Dickson.

Teorema 3.13. *Sea un álgebra de Cayley-Dickson $\mathcal{A}$ de dimensión 2^n, $n \in \mathbb{N}^+$. Los elementos v_i que definimos en el proceso de Cayley-Dickson nos sirven para definir una base*

$$1, v_1, v_2, v_2v_1, v_3, v_3v_1, v_3v_2, v_3v_2v_1, ...$$

Más aún, exceptuando 1, el resto de elementos de la base anticonmutan entre sí. Con esto podemos calcular la forma cuadrática para cada $a \in \mathcal{A}$, pues $a = 1a_1 + v_1a_2 + v_2a_3 + v_2v_1a_4 + ...$, y entonces:

$$N(a) = a_1^2 - \mu_1 a_2^2 - \mu_2 a_3^2 + \mu_2\mu_1 a_4^2 + ...$$

Finalmente, cuando en alguna iteración $t \in \{1, ..., n\}$ se tomó $\mu_t = 0$, entonces $\mathcal{A}$ tiene divisores de cero de la forma $v_t b$, con $b \neq 0$ un elemento de la iteración anterior $t-1$; si $t = n$ (es la última iteración), entonces el álgebra obtenida no es simple.

$\triangleright$ Por cómo se define el producto en el proceso de Cayley-Dickson, en cada iteración obtenemos elementos de la forma $a + v_t b$, siendo a y b elementos de la iteración anterior $t-1$ y $v_t = (0, 1)$, con 1 la unidad de la iteración anterior (identificable con el 1 de $\mathbb{K}$), así, es claro que los elementos $u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, ...$, definidos respectivamente como:

$$1, v_1, v_2, v_2v_1, v_3, v_3v_1, v_3v_2, v_3v_2v_1, ...,$$

forman una base para $\mathcal{A}$, pues por ejemplo, para $n = 2$, tenemos que cualquier elemento es de la forma $(1a + v_1b) + v_2(1c + v_1d) = 1a + v_1b +$

$v_2c + v_2v_1d$, para ciertos $a, b, c, d \in \mathbb{K}$. Calculando, podemos ver cómo es parte de la tabla de multiplicación

$$\begin{array}{ccccccc}
 & 1 & v_1 & v_2 & v_2v_1 & v_3 & \cdots \\
1 & 1 & v_1 & v_2 & v_2v_1 & v_3 & \cdots \\
v_1 & v_1 & \mu_1 & -v_2v_1 & -\mu_1 v_2 & -v_3v_1 & \cdots \\
v_2 & v_2 & v_2v_1 & \mu_2 & \mu_2 v_1 & -v_3v_2 & \cdots \\
v_2v_1 & v_2v_1 & \mu_1 v_2 & -\mu_2 v_1 & -\mu_2\mu_1 & -v_3v_2v_1 & \cdots \\
v_3 & v_3 & v_3v_1 & v_3v_2 & v_3v_2v_1 & \mu_3 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Podemos notar que para $i, j \geq 2$, anticonmutan: $u_iu_j = -u_ju_i$, y que los elementos de la diagonal son sólo productos de μ_i, esto se cumple en general, como ahora comprobamos. Es claro que para $t \in \{1, ..., n\}$ se tiene que $v_t^2 = \mu_t$. Notemos que podemos representar los u_i, para $i \geq 2$ con la ayuda de funciones estrictamente crecientes $\sigma_{k_i} : \{1, ..., k_i\} \longrightarrow \{1, ..., n\}$ (donde k_i es la cantidad de factores que conforman a u_i), así, para $j_1, j_2 \in \{1, ..., k_i\}$, si $j_2 > j_1$, entonces $\sigma_{k_i}(j_2) > \sigma_{k_i}(j_1)$, que de acuerdo a cada $i \in \{2, 3, ..., 2^n\}$ expresan $u_i = \prod_{j=1}^{k_i} v_{\sigma_{k_i}(j)}$, en la cual adoptamos la convención de que los productos se aplican a la izquierda: por ejemplo $\prod_{j=1}^{k} v_j = v_k \left(...v_3(v_2(v_1))...\right)$. Más aún proponemos que en general se tiene

$$u_i^2 = (-1)^{k_i+1} \prod_{j=1}^{k_i} \mu_{\sigma_{k_i}(j)}.$$

Probamos mediante inducción para n. Los casos $n = 1$ y $n = 2$ los vimos en la tabla de multiplicación. Supongamos que se cumple para $n - 1$ y veamos que se cumple para n: Para u_l con $l \in \{2, 3..., 2^n\}$ se tienen dos casos, 1) $u_l = u_l + v_n0$, es decir, no aparece v_n en su expresión y por tanto $l \in \{2, 3, ..., 2^{n-1}\}$, y 2) sí aparece, entonces $u_l = 0 + v_nu_{i_l}$, donde u_{i_l} es un básico de la iteración anterior, i. e. $i_l \in \{2, 3, ...2^{n-1}\}$. Para el primer caso, de inmediato, por la hipótesis de inducción

$$(u_l + v_n0)(u_l + v_n0) = u_l^2 + v_n0 = u_l^2 = (-1)^{k_l+1} \prod_{j=1}^{k_l} \mu_{\sigma_{k_l}(j)}.$$

Para el segundo caso

$$u_l^2 = (0 + v_nu_{i_l})(0 + v_nu_{i_l}) = \mu_n u_{i_l} u_{i_l}^* + v_n0 = -\mu_n u_{i_l}^2,$$

recordando que $u_{i_l} \in Im(\mathcal{A})$ y así $u_{i_l}^* = -u_{i_l}$; por otro lado, por la hipótesis de inducción tenemos que $u_{i_l}^2 = (-1)^{k_{i_l}+1} \prod_{j=1}^{k_{i_l}} \mu_{\sigma_{k_{i_l}}(j)}$, entonces considerando $\sigma : \{1, ..., k_{i_l} + 1 = k_l\} \longrightarrow \{1, ..., n\}$ definida como $\sigma(j) =$

$\sigma_{k_{i_l}}(j)$ para $1 \leq j \leq k_{i_l}$ y $\sigma(k_{i_l}+1) = n$, tenemos que $\sigma = \sigma_{k_l}$, siendo σ_{k_l} la función que esperamos para u_l, y así tenemos que

$$u_l^2 = -\mu_n u_{i_l}^2 = (-1)^{(k_{i_l}+1)+1} \prod_{j=1}^{k_{i_l}+1} \mu_{\sigma(j)} = (-1)^{k_l+1} \prod_{j=1}^{k_l+1} \mu_{\sigma_{k_l}(j)}.$$

Ahora probemos la *anticonmutatividad*. Supongamos que, para $i \neq j$, con $i, j \in \{2, 3, ..., 2^{n-1}\}$, se cumple $u_i u_j = -u_j u_i$. Para $i, j \in \{2, 3, ..., 2^n\}$, con $i \neq j$, tenemos tres casos: i) $2 \leq i, j \leq 2^{n-1}$, ii) $2 \leq i \leq 2^{n-1} < j \leq 2^n$, y iii) $2^{n-1} < i, j \leq 2^n$, es decir, se tiene que i) $u_i = u_i + v_n 0$ y $u_j = u_j + v_n 0$, ii) $u_i = u_i + v_n 0$ y $u_j = 0 + v_n u_{k_j}$, o iii) $u_i = 0 + v_n u_{k_i}$ y $u_j = 0 + v_n v_{k_j}$, con $k_i, k_j \in \{2, 3, ..., 2^{n-1}\}$; claramente, en el primer caso la hipótesis de inducción nos da inmediatamente que $(u_i + v_n 0)(u_j + v_n 0) = u_i u_j + v_n 0 = u_i u_j = -u_j u_i = -u_j u_i + v_n 0 = (u_j + v_n 0)(u_i + v_n 0)$. Para el segundo tenemos (recordando que $u_i^* = -u_i$, pues $u_i \in Im(\mathcal{A})$) que

$$\begin{aligned} u_i u_j &= (u_i + v_n 0)(0 + v_n u_{k_j}) \\ &= 0 + v_n(u_i^* u_{k_j}) \\ &= -v_n(u_i u_{k_j}), \end{aligned}$$

$$\begin{aligned} u_j u_i &= (0 + v_n u_{k_j})(u_i + v_n 0) \\ &= 0 + v_n(u_i u_{k_j}) \\ &= v_n(u_i u_{k_j}). \end{aligned}$$

Por tanto $u_i u_j = -u_i u_j$. Finalmente para el tercer caso tenemos

$$\begin{aligned} u_i u_j &= (0 + v_n u_{k_i})(0 + v_n u_{k_j}) \\ &= \mu_n(u_{k_j} u_{k_i}^*) + v_n 0 \\ &= -\mu_n(u_{k_j} u_{k_i}), \end{aligned}$$

$$\begin{aligned} u_j u_i &= (0 + v_n u_{k_j})(0 + v_n u_{k_i}) \\ &= \mu_n(u_{k_i} u_{k_j}^*) + v_n 0 \\ &= -\mu_n(u_{k_i} u_{k_j}) \\ &= \mu_n(u_{k_j} u_{k_i}). \end{aligned}$$

En donde, en la última igualdad aplicamos la hipótesis de inducción, por tanto, también en este caso $u_i u_j = -u_i u_j$.

Ahora veamos cómo calcular $N(a)$, $a \in \mathcal{A}$, sabiendo que

$$a = 1a_1 + v_1 a_2 + v_2 a_3 + v_2 v_1 a_4 + ... = \sum_{i=1}^{2^n} u_i a_i, \quad \text{con } a_i \in \mathbb{K}.$$

Como es claro que, para $i > 1$, $u_i \in Im(\mathcal{A})$, entonces $u_i^* = -u_i$ y por tanto $u_i u_i^* = -u_i^2$, así $a^* = 1a_1 - v_1 a_2 - v_2 a_3 - ... = a_1 - \sum_{i=2}^{2^n} u_i a_i$ y

$$\begin{aligned} N(a) = aa^* &= \left(a_1 + \sum_{i=2}^{2^n} u_i a_i\right)\left(a_1 - \sum_{i=2}^{2^n} u_i a_i\right) \\ &= a_1^2 - \sum_{i=2}^{2^n} u_i^2 a_i^2 \\ &= a_1^2 - \sum_{i=2}^{2^n} (-1)^{k_i+1} \prod_{j=1}^{k_i} \mu_{\sigma_{k_i}(j)} a_i^2 \\ &= a_1^2 + \sum_{i=2}^{2^n} (-1)^{k_i} \prod_{j=1}^{k_i} \mu_{\sigma_{k_i}(j)} a_i^2 \\ &= a_1^2 - \mu_1 a_2^2 - \mu_2 a_3^2 + \mu_2\mu_1 a_4^2 - \mu_3 a_5^2 + \mu_3\mu_1 a_6^2 + ... \end{aligned}$$

Ahora supongamos que para algún $t \in \{1, ..., n\}$ se tomó $\mu_t = 0$ en alguna iteración, así los elementos de la forma $v_t b$ con $b \neq 0$ siendo un elemento de la iteración anterior $t-1$, resultan ser divisores de cero: considerando la definición del producto en esa iteración tenemos

$$(v_t b)(v_t b') = (0 + v_t b)(0 + v_t b') = 0 + \mu_t b' b^* + v_t(0b' + 0b) = 0.$$

Lo interesante de este tipo de divisores es que no existen en las álgebras escindidas: consideremos un álgebra de Cayley-Dickson escindida $\mathcal{A}'$, i. e. tiene divisores de cero, pero en ninguna iteración se tomó $\mu = 0$; sea $\dim(\mathcal{A}') = 2^n$, con $n \in \mathbb{N}^+$, la última iteración; suponiendo que el producto $(a + v_m b)(c + v_m d) = 0$, tenemos que $ac + \mu_m d b^* = 0$ y $a^* d + cb = 0$, si además, suponemos que alguno a, b, c o d es cero, recordando que $\mu_m \neq 0$, concluimos que su pareja correspondiente es cero o los otros dos lo son, por ejemplo, si $a = 0$, entonces $b = 0$ o $c = 0 = d$, es decir uno de los factores es cero, lo cual contradice que $\mathcal{A}'$ es escindida, por tanto concluimos que ninguno de estos cuatro elementos puede ser cero en ninguna iteración. En cambio en un álgebra dual sí tenemos divisores de cero de la forma $0 + v_t b$ o $v_t b + v_n 0$, según t sea la última iteración o no, por tanto las álgebras escindidas y las duales no pueden ser isomorfas, como habíamos adelantado antes. Es interesante notar que si la última iteración se hace con $\mu_n = 0$ obtenemos un álgebra no simple, es decir, podemos encontrar un ideal propio: Sea $I = \{x + v_n y : x = 0\}$, donde x, y son elementos de la iteración anterior, es claro que es un subconjunto propio de $\mathcal{A}$ y para todo $v_n b, v_n b' \in I$, $v_n b - v_n b' = v_n(b - b') \in I$, pues $b - b'$ es un elemento del álgebra de la iteración anterior, además para todo $a \in \mathcal{A}$ tenemos que $a = x_a + v_n y_a$ y así $a(v_n b) = (x_a + v_n y_a)(0 + v_n b) = 0 + \mu_n b y_a^* + v_n(x_a^* b + 0) = v_n(x_a^* b) \in I$, y $(v_n b)a = (0 + v_n b)(x_a + v_n y_a) = 0 + \mu_n y_a b^* + v_n(0 + x_a b) = v_n(x_a^* b) \in I$, pues $x_a^* b$ y $x_a b$ son elementos del álgebra de la iteración anterior, por tanto, I es en efecto un ideal (bilateral) propio. $\triangleleft$

4

EJEMPLOS CON $\mathbb{R}$

4.1 ÁLGEBRAS NORMADAS Y ORTOGONALIDAD

En esta parte nos fijaremos en álgebras sobre $\mathbb{R}$, por lo que podremos hacer uso de propiedades conocidas de este campo, como el orden y el valor absoluto $|\quad|$. Primero tenemos la siguiente definición:

Una $\mathbb{R}$-álgebra **normada** A es una $\mathbb{R}$-álgebra con una norma $\|.\| : A \longrightarrow \mathbb{R}$, es decir, cumple que $\forall \lambda \in \mathbb{R}\ \forall a, b \in A$:

$\|a\| \geq 0$ (no negativa),

$\|\lambda a\| = |\lambda|\|a\|$ (homogénea),

$\|a + b\| \leq \|a\| + \|b\|$ (desigualdad del triángulo),

$\|a\| = 0$ implica $a = 0$ (definida positiva, junto con la primera).

Y dicha norma es tal que $\forall a, b \in A$:

$$\|ab\| \leq \|a\|\|b\|.$$

Si A es unital, $||e|| = 1$. Un morfismo de $\mathbb{R}$-álgebras normadas es lo mismo que un morfismo de $\mathbb{R}$-álgebras; puede haber morfismos contractivos, expansivos o isométricos.

En nuestro contexto, las álgebras con involución cuadrática, tenemos el resultado siguiente:

Teorema 4.1. *Para una $\mathbb{R}$-álgebra de composición A, podemos obtener una norma para esta álgebra, partiendo de su forma cuadrática que denotamos como N, cuando $\forall a \in A$: $N(a) \geq 0$ (es no negativa); más aún el proceso de Cayley-Dickson nos da una forma cuadrática con la misma propiedad (no negativa) cuando $\mu < 0$ y $\mathfrak{C}(A)$ es alternativa, por tanto, en este caso $\mathfrak{C}(A)$ también es normada e incluso con división.*

Podemos requerir en vez de composición que A sea una $\mathbb{R}$-álgebra alternativa con involución cuadrática cuya forma cuadrática es no degenerada, con esto y bajo el supuesto de que $\forall a \in A$: $N(a) \geq 0$ obtenemos, además, que A sea un álgebra con división.

▷ Definamos $\|a\| = \sqrt{N(a)}$, lo cual tiene sentido pues $N(a) \in \mathbb{R}$ y estamos requiriendo que $N(a) \geq 0$. Consideremos $a, b \in A$ y $\lambda \in \mathbb{R}$, evidentemente se cumple que $\|a\| \geq 0$ y $\|\lambda a\| = \sqrt{N(\lambda a)} = \sqrt{\lambda^2 N(a)} = |\lambda|\sqrt{N(a)} = |\lambda|\|a\|$, por otro lado, como $N(ab) = N(a)N(b)$ por ser A álgebra de composición, entonces $\|ab\| = \|a\|\|b\|$. Pasemos a probar la desigualdad del triángulo, lo cual equivale a probar que

$$N(a+b) \leq \left(\sqrt{N(a)} + \sqrt{N(b)}\right)^2.$$

El caso $a = 0 = b$ es inmediato:

$$N(0+0) = N(0) = 00^* = 0 = 0^2 = \left(\sqrt{0} + \sqrt{0}\right)^2.$$

Ahora supongamos que $a \neq 0 \neq b$, notemos que $ab^* + ba^* = ab^* + (ab^*)^* \in \mathbb{R}$, así que $ab^* + ba^* \leq |ab^* + ba^*|$. Si tuviéramos que $|ab^* + ba^*| \leq 2\sqrt{N(a)N(b)}$, podríamos asegurar la última desigualdad y por tanto tendríamos lo que buscamos probar en:

$$\begin{aligned} N(a+b) &= (a+b)(a+b)^* = (a+b)(a^* + b^*) \\ &= aa^* + ab^* + ba^* + bb^* \\ &= N(a) + ab^* + ba^* + N(b) \\ &\leq N(a) + |ab^* + ba^*| + N(b) \\ &\leq N(a) + 2\sqrt{N(a)N(b)} + N(b) = \left(\sqrt{N(a)} + \sqrt{N(b)}\right)^2. \end{aligned}$$

Veamos entonces que, de hecho, sí lo tenemos y es, nada menos que, la desigualdad de Cauchy-Schwarz. Para esto usaremos la forma bilineal asociada (que resulta ser un producto interior). Notemos para empezar que para todo $a, b \in A$ tenemos:

$$\begin{aligned} (a,a)_N &= N(a+a) - N(a) - N(a) \\ &= (a+a)(a+a)^* - aa^* - aa^* \\ &= 2aa^* = 2N(a) \geq 0, \end{aligned}$$

$$\begin{aligned} (a,b)_N &= N(a+b) - N(a) - N(b) \\ &= (a+b)(a+b)^* - aa^* - bb^* \\ &= ab^* + ba^* \\ &= ba^* + ab^* = (b,a)_N. \end{aligned}$$

Denotemos como $N_a := \sqrt{(a,a)_N}$, así por lo anterior y la bilinealidad, y conmutatividad del producto del campo $\mathbb{R}$, tenemos que:

$$\begin{aligned}
0 &\leq (N_a b \pm N_b a, N_a b \pm N_b a)_N \\
&= N_a^2 (b,b)_N \pm N_b N_a (a,b)_N \pm N_a N_b (a,b)_N + N_b^2 (a,a)_N \\
&= N_a^2 N_b^2 \pm N_b N_a (a,b)_N \pm N_b N_a (a,b)_N + N_b^2 N_a^2 \\
&= 2N_a^2 N_b^2 \pm 2N_a N_b (a,b)_N .
\end{aligned}$$

Por lo tanto, como $N_a = \sqrt{(a,a)_N} = \sqrt{2aa^*} > 0$, pues $a \neq 0$ y análogamente $N_b > 0$ se sigue:

$$\begin{aligned}
\mp 2N_a N_b (a,b)_N &\leq 2N_a^2 N_b^2 \\
\mp (a,b)_N &\leq N_a N_b .
\end{aligned}$$

Esto es $(a,b)_N \leq N_a N_b$ y $-N_a N_b \leq (a,b)_N$, es decir, $|(a,b)_N| \leq N_a N_b$ (que es una versión de la desigualdad de Cauchy-Schwarz). Por lo tanto:

$$|ab^* + ba^*| = |(a,b)_N| \leq N_a N_b = \sqrt{2aa^*}\sqrt{2bb^*} = 2\sqrt{N(a)N(b)}.$$

Así hemos probado casi todas las propiedades requeridas. Solo resta verificar que $\|a\| = 0$ implica que $a = 0$, para lo cual usaremos la desigualdad de Cauchy-Schwarz y que $(,)_N$ sea no degenerada: Si $\|a\| = 0$, entonces tenemos que $aa^* = 0$ y por tanto $N_a = \sqrt{2(0)} = 0$; con lo que para cualquier $b \in A$ tenemos que

$$0 \leq |(a,b)_N| \leq N_a N_b = 0N_b = 0.$$

Así que $|(a,b)_N| = 0$, concluimos que para todo $b \in A$ $(a,b)_N = 0$, por lo tanto $a = 0$ (no degeneración). Con esto tenemos que $N(a) = 0$ si y solo si $a = 0$ (es claro que $N(0) = 00^* = 0$) y por tanto $\|a\| = 0$ si y solo si $a = 0$.

Ahora comprobemos que estas propiedades las conserva $N_{\mathfrak{C}(A)}$ cuando $\mathfrak{C}(A)$ resulta ser alternativa y tomamos $\mu < 0$. Como se puede notar, en lo anterior casi todo se sustenta en que para todo $a \in A$: $N(a) \geq 0$ y N es no degenerada; por la proposición 3.6 tenemos ya casi todo listo, pues $N_{\mathfrak{C}(A)}$ resulta ser no degenerada, más aún, como suponemos que $\mathfrak{C}(A)$ es alternativa tenemos que $N_{\mathfrak{C}(A)}(xy) = N_{\mathfrak{C}(A)}(x)N_{\mathfrak{C}(A)}(y)$, i. e. $\mathfrak{C}(A)$ es un álgebra de composición (proposición 3.7). Entonces nos basta verificar que $N_{\mathfrak{C}(A)}(x) \geq 0$, para todo $x \in \mathfrak{C}(A)$, para establecer que $\mathfrak{C}(A)$ es normada. Esto es fácil, siendo $x = a + vb \in \mathfrak{C}(A)$, como $\mu < 0$, tenemos que

$$N_{\mathfrak{C}(A)}(x) = N(a) - \mu N(b) \geq 0,$$

pues $N(a), N(b) \geq 0$.

Entre las propiedades que vimos antes, en particular, $\mathfrak{C}(A)$ cumple que $N(a) = 0$ si y solo si $a = 0$; esto aunado a la alternatividad que suponemos en $\mathfrak{C}(A)$ nos permite concluir que $\mathcal{C}(A)$ es un álgebra con división, debido a la proposición 3.9. Vemos que la alternatividad es un nexo entre varias propiedades, otro ejemplo lo tenemos en la prueba de la última parte del teorema: si suponemos que A es un álgebra alternativa con involución cuadrática cuya forma cuadrática es no degenerada, de hecho, obtenemos que es un álgebra de composición (proposición 3.7), pero el supuesto de ser alternativa nos permite usar el argumento de antes (proposición 3.9) para concluir que, además, A es con división. $\triangleleft$ Ahora pasamos a otro asunto.

Es interesante notar que la noción de ortogonalidad que definimos en general en las álgebras con involución cuadrática (y por tanto en las de Cayley-Dickson) en los casos particulares de $\mathbb{R}$, con $\mu_t = -1$ en cada iteración, nos da la noción usual. Sea $\mathcal{A}$ una $\mathbb{R}$-álgebra de Cayley-Dickson, conforme lo definimos, $a, b \in \mathcal{A}$ son ortogonales cuando $0 = (a,b)_N$, y recordando que $(a,b)_N = ab^* + b^*a = Re(ab^*)$ y considerando la expresión mediante la base «canónica», $a = a_1 + v_1a_2 + v_2a_3 + v_2v_1a_4 + ...$, y similarmente para b; entonces, haciendo los cálculos podemos notar que en general

$$\begin{aligned} Re(ab^*) = a_1b_1 - \mu_1a_2b_2 - \mu_2a_3b_3 + \mu_2\mu_1a_4b_4 \\ - \mu_3a_5b_5 + \mu_3\mu_1a_6b_6 + \mu_3\mu_2a_7b_7 - \mu_3\mu_2\mu_1a_8b_8 + ... \end{aligned}$$

Con lo que considerando $\mu_t = -1$ en cada iteración, nos da

$$\begin{aligned} (a,b)_N = Re(ab^*) = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 \\ + a_5b_5 + a_6b_6 + a_7b_7 + a_8b_8 + ... \end{aligned}$$

Que no es más que la expresión del producto interior usual en un espacio sobre $\mathbb{R}$, por lo que $(,)_N$ generaliza al producto interior usual. A propósito, ya que tratamos la ortogonalidad, podemos considerar la «forma diagonal». Considerando la base canónica $u_1 = 1, u_2 = v_1, u_3 = v_2, u_4 = v_2v_1, ...$ podemos notar que la forma $\mathbb{R}$-bilineal $(,)_N$ permite definir una matriz A asociada a esta base $A_{ij} = (u_i, u_j)_N$ (apéndice sobre álgebra lineal y grupos de morfismos clásicos). Por el teorema 3.13, tenemos que

$$(u_i, u_i)_N = 2u_iu_i^* = -2u_i^2 = 2N(u_i)$$

y también que

$$(u_i, u_j)_N = u_iu_j^* + u_ju_i^* = -u_iu_j - u_ju_i = -u_iu_j - (-u_iu_j) = 0.$$

Con lo que usando la forma bilineal $\frac{1}{2}(,)_N$ obtenemos una matriz diagonal cuyos elementos de la diagonal son

$$A_{ii} = N(u_i) = -u_i^2 = -(-1)^{k_i+1}\prod_{j=1}^{k_i}\mu_{\sigma_{k_i}(j)} = (-1)^{k_i}\prod_{j=1}^{k_i}\mu_{\sigma_{k_i}(j)}.$$

Podemos definir la **forma diagonal** «canónica» de la forma cuadrática N como $(N(u_1), N(u_2), N(u_3), N(u_4), ...) = (1, -\mu_1, -\mu_2, \mu_2\mu_1, ...)$. Por otro lado, tenemos la siguiente:

Proposición 4.2. *En una $\mathbb{R}$-álgebra de Cayley-Dickson, $\mathcal{A}$, tal que en cada iteración se tomó $\mu_t = -1$ se tiene que para cualesquiera $a, b \in Im(\mathcal{A})$, son ortogonales, i. e. $(a, b)_N = 0$, si y solo si anticonmutan: $ab = -ba$.*

▷ Considerando su expresión en términos de la base canónica, esta vez, como $a \in Im(\mathcal{A})$, tenemos $a = u_1 0 + u_2 a_2 + u_3 a_3 + ...$ y de manera similar b. Entonces, considerando que los elementos de la base canónica anticonmutan $u_i u_j = -u_j u_i$, para $i, j \geq 2$, y en este caso cumplen que $u_i^2 = -1$ (conforme a lo visto en el teorema 3.13) y que $(,)_N$ es simétrica, tenemos:

$$\begin{aligned}
ab &= \left(\sum_{i=1}^{2^n} u_i a_i\right)\left(\sum_{j=1}^{2^n} u_j b_j\right) \\
&= \sum_{i=1}^{2^n}\sum_{j=1}^{2^n} u_i u_j a_i b_j \\
&= \sum_{k=1}^{2^n} u_k^2 a_k b_k + \sum_{i\neq j} u_i u_j a_i b_j \\
&= \sum_{k=1}^{2^n} -a_k b_k + \sum_{\substack{i\neq j,\\ i,j\geq 2}} u_i u_j a_i b_j \\
&= -(a,b)_N + \sum_{\substack{i\neq j,\\ i,j\geq 2}} -u_j u_i a_i b_j \\
&= -(b,a)_N - \sum_{\substack{i\neq j,\\ i,j\geq 2}} u_j u_i b_j a_i,
\end{aligned}$$

donde hemos podido asumir que $i, j \geq 2$, pues $a_0 = 0 = b_1$, ya que $a, b \in Im(\mathcal{A})$. Similarmente y en menos pasos obtenemos

$$\begin{aligned}
-ba &= -\left(\sum_{k=1}^{2^n} u_k^2 b_k a_k + \sum_{i\neq j} u_j u_i b_j a_i\right) \\
&= -(b,a)_N - \sum_{\substack{i\neq j,\\ i,j\geq 2}} u_j u_i b_j a_i,
\end{aligned}$$

de lo cual se sigue inmediatamente que $ab = -ba$ si y solo si $(a, b) = (b, a) = 0$. ◁

4.2 PRIMER ENCUENTRO CON LA FAMILIA COMPLEJA

Podemos definir directamente a los números complejos, cuaterniones y octoniones, respectivamente, como $\mathbb{C} = (\mathbb{R}, -1)$, $\mathbb{H} = (\mathfrak{C}^2(\mathbb{R}), -1)$ y $\mathbb{O} = (\mathfrak{C}^3(\mathbb{R}), -1)$, es decir, tomando $\mu_1 = \mu_2 = \mu_3 = -1$ en cada iteración del proceso de Cayley-Dickson. ¿Por qué tomamos -1 y no otro valor?, ¿qué motivación seguimos? Es lo que tratamos a continuación.

Teorema 4.3. *Las únicas álgebras con división normadas son $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$.*

Teorema 4.4. *Las únicas álgebras alternativas con división son $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$.*

Teorema 4.5. *Toda álgebra con división tiene dimensión 1, 2, 4 u 8.*

$\triangleright$ La existencia la tenemos debido al proceso de Cayley-Dickson y las propiedades que hemos visto en esta y la sección anterior, en particular porque son álgebras alternativas y $\|a\| = 0$ si y solo si $a = 0$, por tanto tenemos álgebras con división en cada caso (proposición 3.9). La unicidad la obtenemos del teorema 2.4 al asegurarnos que un álgebra de composición como éstas tiene que ser una de Cayley-Dickson, solo nos restaría ver que no importa la elección de μ que se haga en cada iteración, eso lo veremos a continuación.

Teorema 4.6. *Para el caso de $\mathbb{R}$, no importa qué μ se tome, aplicar el proceso de Cayley-Dickson nos da tres álgebras distintas según $\mu < 0$, $\mu = 0$ o $\mu > 0$, es decir, las álgebras obtenidas de distintos $\mu < 0$ son isomorfas, y así para $\mu > 0$ y $\mu = 0$. Esto para las iteraciones $n \leq 3$.*

$\triangleright$ Partamos de una $\mathbb{R}$-álgebra de Cayley-Dickson A de dimensión finita (pudiendo ser $\mathbb{R}$ y de $dim(A) \leq 2^{n-1}$) y consideremos $\mu_1, \mu_2 \in \mathbb{R} - \{0\}$. Queremos enfatizar que no estamos suponiendo ninguna propiedad de A, en cambio, queremos notar propiedades del álgebra que resulta del proceso de Cayley-Dickson. Por el teorema 3.11, nos basta encontrar una isometría o equivalencia de formas cuadráticas para las álgebras $\mathcal{A}_1 = (\mathfrak{C}(A), \mu_1)$ y $\mathcal{A}_2 = (\mathfrak{C}(A), \mu_2)$, con sus formas cuadráticas respectivas N_1 y N_2. Considerando $h : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$, definida como $h(a + vb) = a + v'kb$, donde $a, b \in A$, $v = (0, 1) \in \mathcal{A}_1$, $v' = (0, 1) \in \mathcal{A}_2$ y

$$k = \pm\sqrt{\mu_2^{-1}\mu_1},$$

claramente es $\mathbb{R}$-lineal y tiene inversa cuando $\mu_1\mu_2 > 0$, es decir, cuando $\mu_1, \mu_2 > 0$ o $\mu_1, \mu_2 < 0$, siendo $h^{-1}(a + v'b) = a + vk^{-1}b$. Más aún, es isometría, pues $N_2(h(a + vb)) = N_2(a + v'kb) = N(a) - \mu_2 k^2 N(b) = N(a) - \mu_2\mu_2^{-1}\mu_1 N(b) = N(a) - \mu_1 N(b) = N_1(a + vb)$; por tanto, por el teorema 3.11, ambas álgebras son isomorfas. Para ver que las álgebras $\mathcal{A}_1$ y $\mathcal{A}_2$ *no* son isomorfas cuando $\mu_1\mu_2 < 0$ (i. e. tienen signos opuestos), nos basta comprobar que cuando $\mu > 0$, entonces el álgebra obtenida tiene divisores de cero: como sabemos que no importa qué μ tomemos, mientras su valor sea positivo, para *facilitar* los cálculos, consideremos $\mu = 1$ así los elementos $x = 1 + v1 = 1 + v \neq 0$ y $x^* = 1 + v(-1) = 1 - v \neq 0$, y $xx^* = N(x) = 1 - \mu 1 = 1 - 1 = 0 = 0 + v0$, con lo que x y x^* son divisores de cero. Notemos que $N(v) = vv^* = 0 - 1 = -1$ y $v^2 = (0 + v)(0 + v) = 0 + 1 + v(0 + 0) = 1$; entonces, podemos pensar que $(\mathfrak{C}(A), \mu)$ es una extensión de A, obteniendo un álgebra con involución tal que incluye un nuevo elemento v tal que $v^2 = 1$. De vuelta a nuestro asunto, tenemos que con una $\mu > 0$ obtenemos una álgebra escindida, i. e. con divisores de cero, mientras que con $\mu < 0$, por el teorema 4.1, obtenemos una con división, por tanto no pueden ser isomorfas. Para el caso de $\mu = 0$, por lo visto en la última parte del teorema 3.13, sabemos que el álgebra obtenida tiene divisores de cero de la forma $0 + v_t b$ o $v_t b + v_n 0$ y por tanto no es isomorfa a las anteriores, de hecho el álgebra obtenida con $\mu = 0$ no es simple ($I = \{a + vb \in A : a = 0\}$ es un ideal propio), a diferencia de las álgebras escindidas o con división. ◁◁

Las propiedades que presentan estas álgebras son las que más solemos relacionar con la idea de operaciones numéricas, incluyendo las del producto: existencia de inversos multiplicativos, asociatividad en el producto de tres de estas álgebras, y al menos alternatividad en la última, y en ciertos casos también división, también la noción de «tamaño», dado por la forma cuadrática. Vemos también cómo el proceso de Cayley-Dickson nos conduce a una versión más abstracta (álgebra general) al disminuir alguna propiedad que cumpla el producto en cada paso: $\mathbb{R}$ es asociativa conmutativa y real (la involución es trivial: $^* = id_{\mathbb{R}}$); $\mathbb{C}$ es asociativa y conmutativa, pero no real, $\mathbb{H}$ es asociativa, pero no conmutativa ni real; y $\mathbb{O}$ no es real, conmutativa ni asociativa, pero sí, alternativa. Hasta aquí, todas son álgebras con división. Es interesante notar que $\mathfrak{C}(\mathbb{O}) = \mathfrak{C}^4(\mathbb{R})$ con $\mu = -1$, resulta ser un álgebra no alternativa y tampoco con división, cuyos elementos son llamados *sedeniones*; no es con división pues tiene divisores de cero, para ver un ejemplo, usaremos la base canónica que vimos para un álgebra de Cayley-Dickson $1, v_1, v_2, v_2 v_1, ...$, recordando que

$v_i \in \mathbb{K}^{\perp}$ y por tanto $v_i^* = -v_i$, que v_1, v_2, v_3 cumplen la alternatividad y que $\mu_1 = ... = \mu_4 = -1$:

$$
\begin{aligned}
&(v_1v_3 + v_4v_2)(v_2v_3 + v_4v_1) \\
&\quad = (v_1v_3)(v_2v_3) + \mu_4 v_1 v_2^* + v_4((v_1v_3)^* v_1 + (v_2v_3)v_2) \\
&\quad = -(v_3v_1)(v_2v_3) + v_4((v_3^* v_1^*)v_1 + (v_2v_3)v_2) \\
&\quad = -v_3((v_1v_2)v_3) + (-1)v_1(-v_2) + v_4((v_3v_1)v_1 + (v_2v_3)v_2) \\
&\quad = -v_3(-v_3(v_1v_2)) + v_1v_2 + v_4(v_3(v_1v_1) - (v_3v_2)v_2) \\
&\quad = (v_3v_3)(v_1v_2) + v_1v_2 + v_4(v_3(v_1v_1) - v_3(v_2v_2)) \\
&\quad = (-1)(v_1v_2) + v_1v_2 + v_4(v_3(-1) - v_3(-1)) \\
&\quad = -v_1v_2 + v_1v_2 + v_4(-v_3 + v_3) \\
&\quad = 0 + v_4 0 = 0.
\end{aligned}
$$

Entonces los sedeniones tampoco es un álgebra de composición pues no cumple que $N(ab) = N(a)N(b)$. Si continuamos aplicando el proceso con $\mu = -1$, tenemos nuevas álgebras no alternativas sin división, para las cuales puede ser interesante investigar qué propiedades «dejan» de cumplir respecto a las anteriores. Esto en cuanto a continuar iterando el proceso, pero en cuanto a qué otras propiedades se presentan de acuerdo a la $\mu \in \mathbb{R}$, aún nos tiene sorpresas.

4.3 ¿QUÉ SE OBTIENE PARA CADA CASO DE $\mu \in \mathbb{R}$?

Acotamos esta pregunta a las primeras tres iteraciones del proceso de Cayley-Dickson, en las cuales obtenemos álgebras alternativas. El teorema 4.6 nos indica que cada vez que apliquemos la construcción de Cayley-Dickson no hace falta considerar cada caso particular de $\mu \in \mathbb{R}$, solo tres son distintos y por facilidad en los cálculos, podemos tomar $\mu \in \{-1, 0, 1\}$.

El teorema 4.1 nos dice qué obtenemos para $\mu = -1$, partiendo de $\mathbb{R}$ iterando el proceso de Cayley-Dickson tres veces: $\mathbb{R}$-álgebras de composición alternativas *normadas con división*, de hecho, por los teoremas siguientes (4.3 y 4.4), dichas álgebras son, salvo isomorfismos, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$. Podemos decir más al respecto para la primera iteración, recordando lo que mencionábamos cuando presentamos la construcción general de Cayley-Dickson, podemos pensar que $\mathfrak{C}(\mathbb{R})$ con $\mu < 0$ es una extensión de $\mathbb{R}$ que resulta ser un álgebra con involución tal que incluye un nuevo elemento v tal que $v^2 = \mu < 0$ ($v = 0 + v1$); esto es un tipo particular de números hipercomplejos uniparamétricos (Harkin y Harkin, 2004; Yaglom, 1968), que ahora sabemos, son isomorfos, como álgebras con involución, a $\mathbb{C}$; en general se estipula que $v^2 = p + vq$, con $p, q \in \mathbb{R}$, lo que nos lleva al estudio de los números hipercomplejos.

Con $\mu = 1$, podemos definir los *complejos escindidos*, *cuaterniones escindidos* y *octoniones escindidos*, respectivamente, como

$$\mathbb{C}' = (\mathfrak{C}(\mathbb{R}), 1),$$

$$\mathbb{H}' = (\mathfrak{C}^2(\mathbb{R}), \mu_1 = -1, \mu_2 = 1) = (\mathfrak{C}(\mathbb{C}), 1), \text{ y}$$

$$\mathbb{O}' = (\mathfrak{C}^3(\mathbb{R}), \mu_1 = -1, \mu_2 = -1, \mu_3 = 1) = (\mathfrak{C}(\mathbb{H}), 1),$$

es decir, tomar $\mu_t = 1$ en la última iteración del proceso de Cayley-Dickson. Sabemos de estas álgebras, por las proposiciones 3.6 (partimos de $\mathbb{K}$ que es no degenerado), 3.7 y lo visto en la prueba del teorema 4.6, que son álgebras (alternativas) de composición, pero no con división, pues contienen divisores de cero. En cuanto a $\mathbb{C}'$, que podemos pensar como una extensión de $\mathbb{R}$ que incluye un nuevo elemento v tal que $v^2 = 1$, resulta ser un sistema de «números» ya conocido desde el siglo XIX, también llamados *números dobles* y fueron descritos y usados por William K. Clifford, también son llamados números complejos *hiperbólicos*; siendo $\mathbb{C}$ números complejos *elípticos*, esto conforme a cómo se ven los «círculos» en cada plano representado por estos números (Harkin y Harkin, 2004).

Para $\mu = 0$, por la proposición 3.6, sabemos que no se puede asegurar que la forma cuadrática del álgebra obtenida mediante el proceso de Cayley-Dikcson sea no degenerada. Estos son llamados *números duales* y también son conocidos desde el siglo XIX, presentes en los trabajos de Eduard Study, también son llamados números complejos *parabólicos* (Harkin y Harkin, 2004) y nosotros los denotaremos como $\mathbb{C}_0$. Sabemos que forman un álgebra no simple (última parte del teorema 3.13). Regresando a la formulación general de los hipercomplejos, se sabe que como anillos, los hipercomplejos con $v^2 = p + vq$, $p, q \in \mathbb{R}$, son isomorfos a $\mathbb{C}$, $\mathbb{C}_0$ o $\mathbb{C}'$, respectivamente, cuando $\frac{1}{4}(p + q^2)$ es negativo, cero o positivo (Yaglom, 1968).

También podemos preguntarnos qué obtenemos para más iteraciones. Para responder a esto, el teorema 3.13 nos es de gran utilidad para definir isomorfismos entre las álgebras obtenidas del proceso de Cayley-Dickson con distintas μ. Sean A y A' dos álgebras de Cayley-Dickson de igual dimensión $\leq 2^3$, y sean sus bases «canónicas», respectivas, $\{1, v_1, v_2, v_2 v_1, ...\}$ y $\{1, v_1', v_2', v_2' v_1', ...\}$. Sabemos que al asignar biyectivamente (uno a uno) los elementos de una base $\{u_i\}$ a los de la otra $\{u_j'\}$, podemos definir un isomorfismo lineal $\varphi : A \longrightarrow A'$, siendo $a = \sum_i u_i a_i \in A$, con $a_i \in \mathbb{K}$, como $\varphi\left(\sum_i u_i a_i\right) = \sum_i \varphi(u_i) a_i$, más aún requiriendo que $\varphi(1) = 1$ y que los productos de básicos se preserven $\varphi(u_i u_j) = \varphi(u_i)\varphi(u_j)$, obtenemos un morfismo de álgebras pues en efecto, preserva productos en general:

$$\begin{aligned}\varphi\left(\sum_i u_i a_i \sum_j u_j b_j\right) &= \varphi\left(\sum_i \sum_j u_i u_j a_i b_j\right)\\ &= \sum_i \sum_j \varphi(u_i)\varphi(u_j) a_i b_j\\ &= \sum_i \varphi(u_i) a_i \sum_j \varphi(u_j) b_j\\ &= \varphi\left(\sum_i u_i a_i\right)\varphi\left(\sum_j u_j b_j\right).\end{aligned}$$

Esto nos basta para que también preserve la involución, pues sabemos que para $u_i \neq 1$ se tiene que $u_i \in Im(A)$ y por tanto $u_i^* = -u_i$, análogamente para A', así $\varphi(u_i^*) = \varphi(-u_i) = -\varphi(u_i) = \varphi(u_i)^*$, con lo cual, como la involución es $\mathbb{K}$-lineal, se cumple para todo elemento $\varphi\left((\sum_i u_i a_i)^*\right) = \varphi\left(\sum_i u_i^* a_i\right) = \sum_i \varphi(u_i)^* a_i = \left(\sum_i \varphi(u_i) a_i\right)^* = \left(\varphi(\sum_i u_i a_i)\right)^*$.

Entonces solo requerimos hacer una asignación uno a uno de los elementos de una base u_i a los de la otra u_j' tal que $1 \mapsto 1$ y preserve los productos de básicos, para así obtener un isomorfismo de álgebras con involución entre A y A'. Una manera de reconocer qué asignaciones preservan productos involucra considerar $u_i^2 = (-1)^{k_i+1}\prod_{j=1}^{k_i} \mu_{\sigma_{k_i}(j)}$ (seguimos usando el teorema 3.13), pues si, por ejemplo, consideramos álgebras de dimensión 2^2 con $(\mu_1 = -1, \mu_2 = 1)$ y $(\mu_1' = 1, \mu_2' = 1)$ respectivamente, tenemos que $v_1^2 = -1$, $v_2^2 = 1$ y $(v_2 v_1)^2 = 1$ para la primera, y para la otra $(v_1')^2 = 1$, $(v_2')^2 = 1$ y $(v_2' v_1')^2 = -1$, con lo cual podemos hacer la asignación para φ:

$$\begin{aligned} 1 &\mapsto 1\\ v_1 &\mapsto v_2' v_1'\\ v_2 &\mapsto v_2'\\ v_2 v_1 &\mapsto v_1',\end{aligned}$$

la cual en efecto preserva productos de básicos pues $\varphi(v_2)\varphi(v_1) = v_2'(v_2' v_1') = (v_2')^2 v_1' = v_1' = \varphi(v_2 v_1)$, recordando que hasta la tercera iteración podemos usar que las álgebras obtenidas son alternativas. Esto se relaciona con la forma diagonal canónica de la forma cuadrática que mencionamos antes

$$(N(u_1), N(u_2), N(u_3), N(u_4), ...) = (1, -\mu_1, -\mu_2, \mu_2\mu_1, ...),$$

recordando que $N(u_i) = -u_i^2$, para $i > 1$. Esto nos ayuda a identificar las álgebras que son isomorfas según la $\mu_t \in \{-1, 0, 1\}$ que se tome en las tres primeras iteraciones, pues nos basta notar que su forma diagonal canónica contiene los mismos elementos, aunque posiblemente en orden distinto, exceptuando el primer 1 pues sabemos que todas han de comenzar por 1; siguiendo el ejemplo de antes, tenemos que la forma diagonal para la primera álgebra es $(1,1,-1,-1)$, y para la segunda, $(1,-1,-1,1)$; esto es de hecho una manera de expresar la ley de inercia de Sylvester que nos indica que la cantidad de elementos positivos, negativos y ceros en la diagonalización de una matriz simétrica (proveniente de una forma cuadrática) es invariante (independiente de la base con respecto a la cual se use). Se puede ver que entonces, partiendo de $\mathbb{R}$, obtenemos tres álgebras distintas para la primera iteración $\mathbb{C}$, $\mathbb{C}_0$ y $\mathbb{C}'$, que ya las conocemos; en la segunda iteración obtenemos cinco distintas $\mathbb{H}$, $\mathbb{H}_0$, $\mathbb{H}_{00}$, $\mathbb{H}'_0$ y $\mathbb{H}'$ y para la tercera, siete $\mathbb{O}$, $\mathbb{O}_0$, $\mathbb{O}_{00}$, $\mathbb{O}_{000}$, $\mathbb{O}'_{00}$, $\mathbb{O}'_0$ y $\mathbb{O}'$. A continuación expresamos la forma diagonal canónica de cada una:

$$\begin{aligned}
\mathbb{C} &: (1,1) \\
\mathbb{C}_0 &: (1,0) \\
\mathbb{C}' &: (1,-1) \\
\mathbb{H} &: (1,1,1,1) \\
\mathbb{H}_0 &: (1,1,0,0) \\
\mathbb{H}_{00} &: (1,0,0,0) \\
\mathbb{H}'_0 &: (1,-1,0,0) \\
\mathbb{H}' &: (1,1,-1,-1)
\end{aligned}
\qquad
\begin{aligned}
\mathbb{O} &: (1,1,1,1,1,1,1,1) \\
\mathbb{O}_0 &: (1,1,1,1,0,0,0,0) \\
\mathbb{O}_{00} &: (1,1,0,0,0,0,0,0) \\
\mathbb{O}_{000} &: (1,0,0,0,0,0,0,0) \\
\mathbb{O}'_{00} &: (1,-1,0,0,0,0,0,0) \\
\mathbb{O}'_0 &: (1,1,-1,-1,0,0,0,0) \\
\mathbb{O}' &: (1,1,1,1,-1,-1,-1,-1)
\end{aligned}$$

Con esto encontramos una justificación a nuestra notación, usamos la forma primada $'$ para indicar que alguno o algunos v_i cumplen que $N(v_i) = -1$, es decir $v_i^2 = 1$, usamos uno, dos o tres subíndices 0 para indicar, si uno, dos o los tres v_i cumplen que $N(v_i) = 0$, esto es, $v_i^2 = 0$.

Parte II

LA FAMILIA COMPLEJA NORMADA

5

LOS COMPLEJOS $\mathbb{C}$: REVISIÓN DE PROPIEDADES

En esta y las siguientes dos secciones, nos hemos basado en la interesante exposición de Dray y Manogue (2015), presentando un poco de historia y algunas propiedades particulares; asumiremos los resultados que vimos en la parte anterior. En particular, para presentar más detalles sobre los números complejos, en esta sección consideramos también el conciso, pero profundo, texto de Moskowitz (2002).

5.1 GENERALIDADES

Primero haremos un repaso de algunas de las propiedades de los números complejos, pues haremos uso de éstas en nuestro posterior tratamiento de los cuaterniones y octoniones. De hecho, con los números complejos empieza la historia de considerar nuevos elementos para encontrar soluciones a ecuaciones polinomiales (en particular ecuaciones cúbicas, pues algunas soluciones reales requieren usar números complejos para obtenerlas) y poder operar estos con el resto de números. Se suelen atribuir a Rafael Bombelli los primeros intentos por formalizar las reglas aritméticas de los números complejos (en 1572; quien también formalizó las reglas para operar con números negativos). Reglas que se siguen de la idea intuitiva de operar con números compuestos por una parte «ordinaria» y otra que tuviera un nuevo elemento que diera cuenta de la raíz de números negativos, considerando la distributividad del producto sobre la suma y la propiedad de que el cuadrado de este nuevo elemento es un número negativo.

Sabemos que estos números los podemos denotar como parejas ordenadas $(a, b) \in \mathbb{R}^2$ o como $a + ib$, donde $i^2 = -1$; usando la letra i, pues corresponde al término «imaginario», nombre dado por René Descartes (en 1637) para este nuevo elemento con la «singular» propiedad de ser $\sqrt{-1}$. En la construcción general de Cayley-Dickson usamos genéricamente v en vez de esta i u otras letras; vale mencionar que también los encontramos escritos como $a + bi$, pero al ser un sistema conmutativo, resulta irrelevante. Veamos la relación entre la construcción de Cayley-Dickson que vimos y la nomenclatura tradicional. Consideremos $x = a + ib$, $y = c + id$; la *conjugación* que se suele denotar con una barra superior, es una involución cuadrática, siendo

$$x^* = \overline{x} = a^* - ib = a - ib,$$

recordando que $a \in \mathbb{R}$ y ahí la involución es trivial ($id_{\mathbb{R}}$). Tenemos que al suponer la ley distributiva y considerar $i^2 = -1$, la multiplicación de dos elementos compuestos da

$$xy = (a + ib)(c + id) = (ac - db) + i(ad + cb),$$

que es la multiplicación que definimos en la construcción general. La norma, llamada también *módulo complejo*, es

$$\|x\| = \sqrt{N(x)} = \sqrt{xx^*} = \sqrt{a^2 + b^2}.$$

Cuando $x \neq 0$, su inverso es

$$x^{-1} = \frac{x^*}{xx^*} = \frac{x^*}{\|x\|^2}.$$

Además tenemos que $\|x\|\|y\| = \|xy\|$, una propiedad incluida en la definición de álgebra de composición; es interesante que equivale a que

$$(a^2 + b^2)(c^2 + d^2) = (ac - db)^2 + (ad + cb)^2,$$

la llamada regla de dos cuadrados: «el producto de la suma de *dos* cuadrados es otra suma de *dos* cuadrados». Ahora vamos a tratar la geometría de los números complejos. Ya que podemos representar a los complejos en $\mathbb{R}^2$, podemos usar no solo las coordenadas cartesianas, también las polares, así tenemos, para $x \neq 0$, que $x = (r_x, \theta_x)$, donde $r_x = \|x\|$ y θ_x es el ángulo medido desde el eje «horizontal» generado por $(1, 0)$ hasta el segmento de línea que une al origen 0 y x, a este ángulo se le llama el *argumento* de x, denotado $\arg(x)$, notemos que $\arg(x) \in [0, 2\pi)$. Considerando esto también podemos escribir

$$x = r_x \left(\cos(\theta) + i sen(\theta)\right),$$

de manera casi única con ciertos $r_x, \theta \in \mathbb{R}$; decimos casi única pues, para θ, salvo múltiplos enteros de 2π, lo es, ya que para $\theta' = \arg(x) + 2k\pi$, con $k \in \mathbb{Z}$, también podemos escribir $x = r_x \left(\cos(\theta') + i sen(\theta')\right)$. Así, los elementos de la circunferencia unitaria $\mathbb{S}^1_{\mathbb{C}} = \{z \in \mathbb{C} : \|z\| = 1\}$ nos bastan para indicar cualquier ángulo; con esto podemos también expresar $x = \|x\| \frac{x}{\|x\|}$, con $\frac{x}{\|x\|} \in \mathbb{S}^1_{\mathbb{C}}$.

Ahora pasamos a ver la famosa fórmula de Leonhard Euler, para lo cual, primero veremos la función exponencial compleja, misma que nos trae otras interesantes sorpresas. La exponencial compleja se puede definir directamente mediante una serie de potencias, siendo $z \in \mathbb{C}$,

$$e^z = \exp(z) = \sum_{n \in \mathbb{N}} \frac{z^n}{n!},$$

la cual converge absolutamente para todo $z \in \mathbb{C}$, y uniformemente en subconjuntos compactos de $\mathbb{C}$, considerando la topología inducida por la métrica inducida por la norma. La convergencia absoluta es consecuencia de que es un álgebra de composición, pues $N(z^2) = N(z)N(z)$ nos da, por inducción, que $\|z^n\| = N(z^n) = N(z)^n = \|z\|^n$, con lo que $\|e^z\| = \sum_{n \in \mathbb{N}} \frac{\|z^n\|}{n!} = e^{\|z\|}$, que es la exponencial real. También tenemos la «clásica» definición $e^z = \lim_{n \to \infty} (1 + \frac{z}{n})^n$. Reunimos algunas propiedades típicas, cuya demostración puede encontrarse en Moskowitz (2002), por ejemplo.

$\forall z, w \in \mathbb{C}$, $\forall t \in \mathbb{R}$:

$$e^{z+w} = e^z e^w, \quad (e^z)^{-1} = e^{-z} \quad \text{y} \quad \|e^{tz}\| = \|e^z\|^t.$$

También podemos definir directamente mediante serie de potencias a las funciones trigonométricas:

$$\mathrm{sen}(z) = \sum_{n \in \mathbb{N}} (-1)^n \frac{z^{2n+1}}{(2n+1)!} \quad \text{y} \quad \cos(z) = \sum_{n \in \mathbb{N}} (-1)^n \frac{z^{2n}}{(2n)!}.$$

De lo que se sigue que $e^{iz} = \cos(z) + i\mathrm{sen}(z) \in \mathbb{S}^1_{\mathbb{C}}$, en particular $e^{2\pi i} = 1$ (la famosa identidad); con la cual tenemos, para $k \in \mathbb{Z}$, que $e^z = e^z e^{2k\pi i} = e^{z+2k\pi i}$, mostrando que la exponencial compleja es una función periódica, de periodo $2\pi i$. Entonces, podemos escribir $z = \|z\| e^{i \arg(z)}$, y por consiguiente tenemos

$$zw = \|z\|\|w\| e^{i \arg(z)} e^{i \arg(w)} = \|z\|\|w\| e^{i(\arg(z) + \arg(w))}.$$

Por tanto $\arg(zw) = \arg(z) + \arg(w)$, que no otra cosa que una manera de expresar la identidad trigonométrica para la suma de ángulos; también podemos usar la notación más compacta que vimos antes

$$zw = r_z r_w e^{i\theta_z} e^{i\theta_w},$$

con $\theta_z = \arg(z)$ y $\theta_w = \arg(w)$. Finalmente veamos una propiedad concerniente a la norma de la exponencial compleja: si $z = a + ib$, también tenemos que $\|e^z\| = \|e^a\|\|e^{ib}\| = |e^a| 1 = e^{Re(z)}$. Hasta aquí nuestro breviario de propiedades.

5.2 DESCRIPCIÓN DE $SO(2)$, $U(1)$ Y $O(2)$

Antes de comenzar propiamente esta sección, mencionamos que esta y las secciones que traten sobre geometría asumen algunos detalles que pueden encontrarse en Ramírez-Galarza y Seade-Kuri (2002), capítulo 1. Ahora sí, empecemos. De acuerdo a lo que vimos antes, podemos decir que la multiplicación compleja, $zw = r_z r_w e^{i\theta_z} e^{i\theta_w}$, es reescalar el tamaño de z por un factor de r_w y rotarlo un ángulo de θ_w; entonces multiplicar por $w \in \mathbb{C}$ fijo nos da una homotecia (expansión o contracción) combinada con una rotación del plano $\mathbb{R}^2$ que representa a $\mathbb{C}$. Al considerar un w de «tamaño» unitario, es decir, $\|w\| = 1$ obtenemos sólo rotaciones. Esto nos da dos pistas, la primera es que como $\|w\| = ww^*$, consideremos al grupo unitario

$$\begin{aligned} U(1) &= \{w \in M_{1\times 1}(\mathbb{C}) : w^{*t} w = I_1\} \\ &= \{w \in \mathbb{C} : w^* w = 1\} \\ &= \{e^{i\theta} \in \mathbb{C} : \theta \in [0, 2\pi)\}. \end{aligned}$$

Por otro lado, al ser rotaciones del plano, nos sugiere al grupo $SO(2)$, pues, en efecto este grupo representa las rotaciones del plano: Si $M \in SO(2)$, entonces $M^t M = I_2$ y $\det(M) = 1$, y considerando

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

entonces tenemos que

$$\begin{aligned} \begin{pmatrix} a^2 + c^2 & ab + cd \\ ba + dc & b^2 + d^2 \end{pmatrix} &= \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= M^t M \\ &= I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

es decir, $a^2 + c^2 = 1 = b^2 + d^2$ y $ab + cd = 0$, la primera de las cuales nos permite notar que no puede ser que $a = 0 = c$ ni $b = 0 = d$, respectivamente, alguna es distinta de cero; también nos dan que

$$b^2 = 1 - d^2 \quad \text{y} \quad c^2 = 1 - a^2, \quad \text{y} \quad ab = -cd.$$

Vemos que la tercera igualdad implica que $a^2 b^2 = c^2 d^2$; sustituyendo en esta igualdad, la información dada por las dos primeras, nos da la siguiente serie de igualdades:

$$\begin{aligned} a^2 b^2 &= c^2 d^2 \\ a^2(1 - d^2) &= (1 - a^2) d^2 \\ a^2 - a^2 d^2 &= d^2 - a^2 d^2 \\ a^2 &= d^2. \end{aligned}$$

Por tanto $d = sa$, con $s \in \{-1, 1\}$. Cálculos similares nos dan que $c^2 = b^2$ y por tanto $b = tc$, con $t \in \{-1, 1\}$. Recordando que $ab = -cd$, tenemos que $tac = -sac$, i. e. $t = -s$, de lo cual resulta que b y d han de tener signos opuestos. Ahora, como $ad - bc = \det(M) = 1$, lo anterior implica que

$$\pm a^2 \pm c^2 = a(\pm a) - (\mp c)c = 1,$$

lo cual solo puede ocurrir si tomamos $d = +a$ y por tanto $b = -c$. Entonces

$$M = \begin{pmatrix} a & -c \\ c & a \end{pmatrix},$$

y queda solo la ecuación $a^2 + c^2 = 1$, que representa una circunferencia, i. e. $a = \cos(\theta)$ y $c = sen(\theta)$, y entonces

$$M = \begin{pmatrix} \cos\theta & -sen\theta \\ sen\theta & \cos\theta \end{pmatrix},$$

así, M representa una rotación del plano por un ángulo de θ.

Lo anterior nos dice que podemos estudiar las rotaciones del plano $\mathbb{R}^2$ mediante la multiplicación de números complejos unitarios, pues en otras palabras tenemos un isomorfismo de grupos $t : SO(2) \longrightarrow U(1)$, definido como

$$t\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a + ib.$$

Más aún, podemos representar estos grupos en la circunferencia $\mathbb{S}^1_{\mathbb{C}}$.

La historia no termina aquí, pues la conjugación compleja significa geométricamente una reflexión del plano con respecto al eje vertical o «imaginario», el generado por i; por otro lado, cualquier reflexión en el plano puede obtenerse como la composición de rotaciones y una reflexión fija: si consideramos una línea recta cuyo ángulo de su pendiente sea θ, la reflexión del plano con respecto a esta línea viene dada por

$$e^{i\theta}\left(e^{-i\theta}(z)\right)^*,$$

donde $z \in \mathbb{C}$ es el punto al que le aplicamos la reflexión. Y como sabemos que $O(2)$ está conformado por las rotaciones $SO(2)$ y las reflexiones del plano $\mathbb{R}^2$ (Ramírez-Galarza y Seade-Kuri, 2002), con esto concluimos que las operaciones de $\mathbb{C}$ nos bastan para describir $O(2)$.

6

LOS CUATERNIONES $\mathbb{H}$

6.1 DOS REPRESENTACIONES Y GENERALIDADES

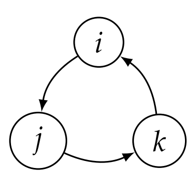
Tomando como punto de partida a los complejos, podemos preguntarnos qué pasa si incluimos una nueva unidad imaginaria j, es decir, una raíz de -1; si se pretende obtener una nueva álgebra que incluya a ambas unidades, hace falta proponer qué da ij. Esta y otras preguntas relacionadas rondaron la cabeza de William Rowan Hamilton por un largo rato, no consiguiendo definir satisfactoriamente un álgebra tridimensional, hasta que un 16 de octubre de 1843, le «llegó» la inspiración, considerando que $ij = k$ debía ser otra unidad imaginaria, incluso, por la emoción, grabó en un puente de Dublín la relación fundamental que figuraba en su mente

$$i^2 = j^2 = k^2 = ijk = -1.$$

Entonces la multiplicación de unidades debía ser cíclica y anticonmutar:

$$ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

Esto tiene una representación linda:



Donde las flechas indican un producto positivo en ese sentido, por ejemplo, ij da k, pero en sentido contrario a la flecha, uno negativo: ji da $-k$.

El mismo Hamilton propuso darles el nombre de cuaterniones haciendo alusión a sus cuatro generadores 1, i, j, k; ahora usamos la notación $\mathbb{H}$ para denotar el conjunto de cuaterniones en honor a Hamilton. Podemos representarlos naturalmente en $\mathbb{R}^4$, considerando como base a $\{1, i, j, k\}$, así $q \in \mathbb{H}$ se expresa como $q = 1q_1 + iq_2 + jq_3 + kq_4$, con $q_1, ..., q_4 \in \mathbb{R}$; considerando que $k = ij$, también tenemos que $q = (q_1 + iq_2) + (q_3 + iq_4)j$, con lo que también podemos representarlos como una pareja de números complejos $q = (c_1, c_2)$ en $\mathbb{C}^2$, o como una suma $q = c_1 + c_2 j$, lo que nos lleva a poder representarlos como

$$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j.$$

Ésta es la semilla de la construcción de Cayley-Dickson. Veamos cómo se corresponde ésta con nuestra definición. Para el producto, considerando la construcción de Cayley-Dickson sean $x = (x_1 + v_1 x_2) + v_2(x_3 + v_1 x_4)$ y $y = (y_1 + v_1 y_2) + v_2(y_3 + v_1 y_4)$, entonces el producto toma la forma

$$\begin{aligned}
xy &= (x_1 + v_1 x_2)(y_1 + v_1 y_2) + \mu_2 (y_3 + v_1 y_4)(x_3 + v_1 x_4)^* \\
&\qquad + v_2 \left((x_1 + v_1 x_2)^* (y_3 + v_1 y_4) + (y_1 + v_1 y_2)(x_3 + v_1 x_4) \right) \\
&= (x_1 + v_1 x_2)(y_1 + v_1 y_2) + \mu_2 (y_3 + v_1 y_4)(x_3^* - v_1 x_4) \\
&\qquad + v_2 \left((x_1^* - v_1 x_2)(y_3 + v_1 y_4) + (y_1 + v_1 y_2)(x_3 + v_1 x_4) \right) \\
&= x_1 y_1 + \mu_1 y_2 x_2^* + v_1 (x_1^* y_2 + y_1 x_2) \\
&\qquad + \mu_2 \left(y_3 x_3^* - \mu_1 x_4 y_4^* + v_1(-y_3^* x_4 + x_3^* y_4) \right) \\
&\qquad + v_2 \Big(x_1^* y_3 - \mu_1 y_4 x_2^* + v_1 (x_1 y_4 - y_3 x_2) \\
&\qquad\qquad + y_1 x_3 + \mu_1 x_4 y_2^* + v_1 (y_1^* x_4 + x_3 y_2) \Big) \\
&= x_1 y_1 + \mu_1 y_2 x_2^* + \mu_2 y_3 x_3^* - \mu_2 \mu_1 x_4 y_4^* \\
&\qquad + v_1 \left(x_1^* y_2 + y_1 x_2 - \mu_2 y_3^* x_4 + \mu_2 x_3^* y_4 \right) \\
&\qquad + v_2 \left(x_1^* y_3 - \mu_1 y_4 x_2^* + y_1 x_3 + \mu_1 x_4 y_2^* \right) \\
&\qquad + v_2 v_1 \left(x_1 y_4 - y_3 x_2 + y_1^* x_4 + x_3 y_2 \right).
\end{aligned}$$

Entonces considerando que $x_s, y_t \in \mathbb{R}$, para $s, t \in \{1, ..., 4\}$, tenemos que $x_s^* = x_s$, $y_t^* = y_t$, y conmutan entre sí; además $\mu_1 = \mu_2 = -1$, entonces, re-ordenando para la notación $v_1, v_2, v_2 v_1$, tenemos que

$$\begin{aligned}
xy = x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4 \\
+ v_1 \left(x_1 y_2 + x_2 y_1 - x_3 y_4 + x_4 y_3 \right) \\
+ v_2 \left(x_1 y_3 + x_2 y_4 + x_3 y_1 - x_4 y_2 \right) \\
+ v_2 v_1 \left(x_1 y_4 - x_2 y_3 + x_3 y_2 + x_4 y_1 \right).
\end{aligned}$$

Ahora, considerando $x = 1x_1 + ix_2 + jx_3 + kx_4$, $y = 1y_1 + iy_2 + jy_3 + ky_4$, tenemos que la notación i, j, k da

$$\begin{aligned}
xy = x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4 \\
+ i(x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3) \\
+ j(x_1 y_3 - x_2 y_4 + x_3 y_1 + x_4 y_2) \\
+ k(x_1 y_4 + x_2 y_3 - x_3 y_2 + x_4 y_1).
\end{aligned}$$

Vemos que los signos en ambas expresiones, con i, j, k y con $v_1, v_2, v_2 v_1$, no corresponden exactamente; como pudimos notar en la expresión como parejas de complejos usamos $(q_1 + iq_2) + (q_3 + iq_4)j$ con j a la *derecha* para que obtuviéramos ij, la notación «clásica», pero si lo escribimos como en la construcción de Cayley-Dickson, a la *izquierda*, necesitamos un signo menos: $(q_1 + iq_2) + j(q_3 - iq_4)$, lo que nos hace pensar que la asignación

$$1q_1 + iq_2 + jq_3 + kq_4 \quad \mapsto \quad 1q_1 + v_1q_1 + v_2q_2 + v_2v_i(-q_4),$$

relaciona ambas, y en efecto, con este signo menos en la última coordenada, en una u otra notación, se igualan ambas expresiones; esto indica el cambio de base $1 \leftrightarrow 1$, $i \leftrightarrow v_1$, $j \leftrightarrow v_2$ y $k = ij \leftrightarrow -v_2v_1$ que las relaciona. Esto solo se debe a la elección en el orden de multiplicación de i y j, conforme a la lectura; no es algo relevante, pues sabemos que estudiamos el sistema, por los teoremas de unicidad que vimos en la parte anterior; cabe mencionar que la notación i, j, k es más cómoda para hacer cálculos por eso optamos seguir con ésta el resto del capítulo, sin embargo no es tan fácilmente generalizable como lo es la notación v_1, v_2, v_2v_1.

Además de las propiedades que ya conocemos sobre la involución, que también es llamada conjugación como con los complejos, $q^* = 1q_1 - iq_2 - jq_3 - kq_4$, y los inversos multiplicativos $q^{-1} = \frac{1}{qq^*}q^* = \frac{1}{\|q\|}q^*$, también tenemos que $\|x\|\|y\| = \|xy\|$, para $x, y \in \mathbb{H}$, que no es más que la llamada regla de cuatro cuadrados: «el producto de la suma de *cuatro* cuadrados es otra suma de *cuatro* cuadrados», como vemos:

$$\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\
&\quad = (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_2y_1 + x_1y_2 - x_4y_3 + x_3y_4)^2 \\
&\qquad + (x_3y_1 + x_4y_2 + x_1y_3 - x_2y_4)^2 + (x_4y_1 - x_3y_2 + x_2y_3 + x_1x_4)^2.
\end{aligned}$$

6.2 EL PRODUCTO PUNTO Y EL PRODUCTO CRUZ EN UNO, GEOMETRÍA

Presentamos una sección particular para este tema, pues buscamos enfatizar esta interesante propiedad que es el origen de la notación $\hat{\imath}$, $\hat{\jmath}$ y $\hat{k}$ en el álgebra vectorial tridimensional. Considerando la asignación biyectiva $\varphi : \mathbb{R}^3 \longrightarrow Im(\mathbb{H})$, definida como

$$r = (r_x, r_y, r_z) = r_x\hat{\imath} + r_y\hat{\jmath} + r_z\hat{k} \quad \mapsto \quad ir_x + jr_y + kr_z,$$

la cual es claramente $\mathbb{R}$-lineal, tenemos para $r, s \in \mathbb{R}^3$, siguiendo los cálculos del producto en $\mathbb{H}$ que vimos:

$$\begin{aligned}
\varphi(r)\varphi(s) = &-r_xs_x - r_ys_y - r_zs_z \\
&+ i(r_ys_z - r_zs_y) \\
&+ j(-r_xs_z + r_zs_x) \\
&+ k(r_xs_y - r_ys_x).
\end{aligned}$$

De lo cual es claro que puede representar el producto punto y cruz:

$$-Re(\varphi(r)\varphi(s)) = r \cdot s, \quad \text{y} \quad \varphi^{-1}\left(Im(\varphi(r)\varphi(s))\right) = r \times s.$$

Sigue un poco de la geometría de $\mathbb{H}$. Primero veamos que esto del producto punto y cruz no es solo una expresión linda, también nos ayuda a establecer propiedades sobre los cuaterniones, como la que sigue:

Dados dos cuaterniones $x, y \in \mathbb{H} - \{0\}$, tenemos que conmutan, esto es $xy = yx$, si y solo si son «paralelos», esto es $y = rx$, para cierto $r \in \mathbb{R}$.

Ahora probamos tal afirmación, sean $x, y \in \mathbb{H} - \{0\}$ y denotemos $Re(x) = x_r$, $Im(x) = x_i$ y análogamente para y, así, considerando que los elementos de $\mathbb{R}$ conmutan con todos los de $\mathbb{H}$, tenemos que

$$\begin{aligned} xy = (x_r + x_i)(y_r + y_i) &= x_r y_r + x_r y_i + x_i y_r + x_i y_i \\ &= x_r y_r + x_r y_i + y_r x_i + x_i y_i, \end{aligned}$$

$$\begin{aligned} yx = (y_r + y_i)(x_r + x_i) &= y_r x_r + y_r x_i + y_i x_r + y_i x_i \\ &= x_r y_r + x_r y_i + y_r x_i + y_i x_i, \end{aligned}$$

por lo que, $xy = yx$ si y solo si $Im(x)Im(y) = Im(y)Im(x)$. Entonces nos basta considerar las partes imaginarias de los factores. A continuación usaremos la notación $\hat{x} = \varphi^{-1}(x)$:

$$\begin{aligned} x_i y_i &= Re(x_i y_i) + Im(x_i y_i) \\ &= -\hat{x}_i \cdot \hat{y}_i + \varphi\left(\hat{x}_i \times \hat{y}_i\right), \end{aligned}$$

$$\begin{aligned} y_i x_i &= Re(y_i x_i) + Im(y_i x_i) \\ &= -\hat{y}_i \cdot \hat{x}_i + \varphi\left(\hat{y}_i \times \hat{x}_i\right) \\ &= -\hat{x}_i \cdot \hat{y}_i + \varphi\left(-\hat{x}_i \times \hat{y}_i\right), \end{aligned}$$

donde la última igualdad se cumple pues sabemos que el producto punto es conmutativo, y el cruz, anticonmutativo; de esto es claro que $x_i y_i = y_i x_i$ si y solo si $\hat{x}_i \times \hat{y}_i = -\hat{x}_i \times \hat{y}_i$ y esto pasa si y solo si $\hat{x}_i \times \hat{y}_i = 0$, es decir, $\hat{x}_i$ e $\hat{y}_i$ son vectores paralelos, lo cual ocurre si y solo si $\hat{y}_i = r\hat{x}_i$, para cierto $r \in \mathbb{R}$, esto es, $y_i = r x_i$.

Es interesante que los elementos imaginarios de $\mathbb{H}$ tienen propiedades como los imaginarios complejos, pero con más «grados de libertad», por ejemplo, sabemos que para todo $b \in Im(\mathbb{H})$ tenemos que $b^* = -b$ y $b^2 = -N(b) < 0$, en particular si $\|b\| = 1$, entonces $b^2 = -1$, así que tenemos infinitas raíces de -1. Denotamos $\mathbb{S}^2_{Im(\mathbb{H})} = \{q \in Im(\mathbb{H}) : \|q\| = 1\}$, con la notación de una 2-esfera, pues es claro que forman una esfera que podemos situar en $\mathbb{R}^3$ conforme a la asignación que vimos antes. Con estos imaginarios unitarios $u \in \mathbb{S}^2_{Im(\mathbb{H})}$ podemos considerar las subálgebras generadas por $\{1, u\}$, cuyos elementos son de la forma $1a + ub = a + ub$, con $a, b \in \mathbb{R}$, claramente son isomorfas a $\mathbb{C}$, podemos denotarlas $\mathbb{C}_u$, y lo interesante es que podemos usar todo lo que sabemos de los complejos en estas. Así, podemos expresar cualquier $q \in \mathbb{H}$ como:

$$q = \|q\| e^{u_q \theta_q} = r_q \left(\cos(\theta_q) + u_q sen(\theta_q) \right),$$

siendo

$$u_q = \begin{cases} \frac{1}{\|Im(q)\|} Im(q) & \text{si } \|Im(q)\| \neq 0 \\ 0 & \text{si } \|Im(q)\| = 0, \end{cases}$$

con $\theta_q = \arg(u_q)$, $r_q = \|q\|$. También podemos expresarlo como $q = a_q + u_q b_q$, para ciertos $a_q, b_q \in \mathbb{R}$, y como sabemos que $q = Re(q) + Im(q)$, resulta que $a_q = Re(q)$ y $u_q b_q = Im(q)$; también tenemos la relación: $a_q = r_q \cos(\theta_u)$, $b_q = r_q sen(\theta_u)$. En otras palabras, u_q nos dice la «dirección imaginaria» de q y θ_q el ángulo formado por el eje «real» (generado por 1) y q, el cual se ubica en el plano $1u_q$ (no confundir con la notación del producto).

Sea $q \in \mathbb{H}$ y consideremos la **conjugación por un elemento** $p \in \mathbb{H} - \{0\}$, esto es pqp^{-1}; para el caso en que p y q conmuten, tenemos que $pqp^{-1} = q$, veamos qué pasa en el caso general. Notemos que sin pérdida de generalidad podemos tomar $\|p\| = 1$, pues no importa el tamaño de p:

$$\|pqp^{-1}\| = \|p\|\|q\|\|p^{-1}\| = \|p\|\|q\|\|p\|^{-1} = \|q\|,$$

además, así tenemos que $p^{-1} = p^*$. Por otro lado, recordemos que la noción de ortogonalidad $(,)_N = 0$ resulta ser la usual para $\mathbb{R}^4$, entonces consideremos una base ortonormal (i. e. ortogonal y cuyos elementos son unitarios), digamos $\{r, \iota, \xi, \kappa\}$, tal que un elemento sea real y el resto imaginarios, así, $r = 1 \in Re(\mathbb{H}) \cong \mathbb{R}$, y el resto $\iota, \xi, \kappa \in Im(\mathbb{H})$, con $\kappa = \iota\xi$, con lo cual, ι, ξ y κ anticonmutan entre sí (proposición 4.2), entonces podemos escribir $q = c_1 + c_2\xi$, con $c_1, c_2 \in \mathbb{C}_\iota$. Veamos un caso fácil, considerar $p = \iota$, así, como los elementos de $\mathbb{C}_\iota$ conmutan entre sí, tenemos:

$$\begin{aligned} pqp^{-1} &= \iota(c_1 + c_2\xi)\iota^* = \iota c_1 \iota^* + \iota c_2 \xi \iota^* \\ &= c_1 \iota\iota^* - c_2 \iota\iota^* \xi = c_1 - c_2 \xi, \end{aligned}$$

lo cual nos indica que la conjugación por un $p = \iota$ es una rotación de 180° en el plano $\xi\kappa$ (notemos que lo único que requerimos estrictamente es la ortogonalidad de la base); resultados análogos tenemos para los otros básicos: expresando $q = c_1' + c_2'\kappa$, con $c_1', c_2' \in \mathbb{C}_\xi$, tenemos que $\xi q \xi^{-1} = c_1' - c_2'\iota$, esto es, la conjugación por ξ es una rotación de 180° en el plano $\kappa\iota$, y la conjugación por κ, es una en el plano $\iota\xi$. Así, al conjugar $q = e^{\iota\theta}$ por ξ, tenemos una rotación en el plano $\kappa\iota$ y en particular $\xi e^{\iota\theta}\xi^* = e^{-\iota\theta}$, con lo que

$$\xi e^{\iota\theta} = e^{-\iota\theta}\xi.$$

Esta relación nos será muy útil, pero primero concluyamos nuestro análisis de la conjugación por un elemento, ahora veamos qué pasa si tomamos $p = e^{\iota\theta}$ para conjugarlo con $q = c_1 + c_2\xi$, recordando que $c_1, c_2 \in \mathbb{C}_\iota$ y que los elementos de $\mathbb{C}_\iota$ conmutan entre sí:

$$\begin{aligned} pqp^{-1} &= e^{\iota\theta}(c_1 + c_2\xi)e^{-\iota\theta} \\ &= e^{\iota\theta}c_1e^{-\iota\theta} + e^{\iota\theta}c_2\xi e^{-\iota\theta} \\ &= c_1e^{\iota\theta}e^{-\iota\theta} + c_2e^{\iota\theta}e^{-(-\iota\theta)}\xi \\ &= c_1 + c_2e^{2\iota\theta}\xi. \end{aligned}$$

Con esto tenemos que la conjugación por $e^{\iota\theta}$ es una rotación de 2θ en el plano $\xi\kappa$, y cálculos similares muestran que la conjugación por $e^{\xi\theta}$ es una rotación de 2θ en el plano $\kappa\iota$, y conjugación por $e^{\kappa\theta}$, una en el plano $\iota\xi$. Entonces podemos describir cualquier rotación en los planos formados por imaginarios unitarios ortogonales (ortonormales), esto lo usaremos en la siguiente sección. Antes, veamos que con todas estas relaciones podemos ver qué significa geométricamente la multiplicación de cuaterniones. Sean $p, q \in \mathbb{H}$, sabemos que podemos expresar $p = \|p\|e^{u_p\theta_p}$, para hacer coincidir la notación que usamos antes, definamos $\iota = u_p$ y $\theta = \theta_p$, así $p \in \mathbb{C}_\iota \subset \mathbb{H}$, y entonces, partiendo de ι podemos considerar una base ortonormal que lo incluya: $\{1, \iota, \xi, \kappa = \iota\xi\}$ (para esto basta considerar un ξ unitario ortogonal a ι); con esto tenemos que $q = c_1 + c_2\xi$ para ciertos $c_1, c_2 \in \mathbb{C}_\iota$, con lo que

$$\begin{aligned} pq &= \|p\|e^{\iota\theta}(c_1 + c_2\xi) \\ &= \|p\|(e^{\iota\theta}c_1 + e^{\iota\theta}c_2\xi) \\ &= \|p\|(c_1e^{\iota\theta} + c_2e^{\iota\theta}\xi), \end{aligned}$$

donde hemos usado que los elementos de $\mathbb{C}_\iota$ conmutan entre sí, ahora veamos qué pasa con la multiplicación cambiando lugares:

$$\begin{aligned} qp &= (c_1 + c_2\xi)\|p\|e^{\iota\theta} \\ &= \|p\|(c_1e^{\iota\theta} + c_2\xi e^{\iota\theta}) \\ &= \|p\|(c_1e^{\iota\theta} + c_2e^{-\iota\theta}\xi), \end{aligned}$$

así tenemos que la multiplicación consiste en reescalar el tamaño de q por un factor de $\|p\|$ y efectuar rotaciones en los planos generados por 1 y el unitario $\iota = u_p$, la «dirección imaginaria» de p, y por un elemento ortogonal a este, ξ y $\kappa = \iota\xi$, siendo la rotación del plano 1ι de $\theta = \theta_p$, y la del plano $\xi\kappa$ de θ o $-\theta$, según se multiplique p a la izquierda o derecha, respectivamente.

Ya que mencionamos que hay una relación entre los cuaterniones y la rotaciones, al respecto cabe mencionar que varios matemáticos antes de Hamilton ya habían notado esta relación aunque ellos no los llamaran cuaterniones, describieron algunas de sus propiedades, por ejemplo, Olinde Rodrigues en 1840, Carl Friedrich Gauss en 1819, e incluso Leonhard Euler (Pujol, 2012).

6.3 descripción de $SO(3)$ y $SO(4)$

En $\mathbb{R}^2$ y $\mathbb{R}^3$ la noción de rotación se suele asociar con un giro de un plano entorno a un punto o un eje (ortogonal al plano) fijo, respectivamente. En espacios de más dimensiones, los grados de libertad nos permiten abstraer la idea, y no solo «girar» un plano y dejar el espacio ortogonal fijo, sino girar varios planos ortogonales a la vez. Considerando un espacio vectorial V con una forma bilineal simétrica o una forma cuadrática y su correspondiente forma bilineal (simétrica) asociada, denotando cualquiera de las dos como $(,)$, podemos definir la noción generalizada de «tamaño» (u,u) y la de ortogonalidad $(u,v)=0$ o «ángulo» entre vectores (u,v). Así podemos definir una rotación general como una transformación del espacio que deja al origen fijo, preserva tamaños (forma cuadrática), ángulos u ortogonalidad (forma bilineal) y orientación ($\det > 0$), que es la que representan los grupos ortogonales especiales generalizados $SO\left(V,(,)\right)$ (apéndice sobre álgebra multilineal y grupos de morfismos clásicos). Para ver cómo se relacionan ambas nociones de rotación, volvemos a citar un resultado que podemos encontrar en Artin (1957) (teorema 3.22) o en un lenguaje más cercano al actual, en Grove (2002) (proposición 6.13):

Sea (V,q) un $\mathbb{K}$-espacio cuadrático (car$(\mathbb{K}) \neq 2$) de dimensión $n \geq 3$. Si τ es una isometría tal que su matriz asociada T (respecto a cualquier base) cumple que $\det(T)=1$, i. e. $T \in SO\left(V,(,)_q\right)$, entonces τ puede expresarse como el producto de $2k$ «medios giros», con $2k \leq n$.

Un *medio giro* (o *giro de 180°*) es una isometría σ de V de la forma $\sigma = -1_U \perp 1_{U^\perp}$, siendo U un subespacio de dimensión 2, donde $(-)1_U$ es la función (menos) identidad: $(-)1_U(x) = (-)x$ (vale recordar la notación que vimos en la sección 2.2 cuando tratamos con espacios bilineales y cuadráticos). El nombre de estos no es en vano, pues corresponden a girar 180° un plano dejando invariante el espacio ortogonal a dicho plano. Para girar cualquier plano nos basta saber girar los planos generados por los básicos (los vectores de una base $\{b_1,...,b_n\}$ del espacio). Esto último es fácil y sabemos cómo representar las matrices correspondientes: los básicos del espacio ortogonal quedan inalterados, mientras que los dos correspondientes al plano que se gira se modifican solo en las coordenadas correspondientes a estos mismos conforme al ángulo que se gira y que podemos expresar con senos y cosenos. Para $n = 3$ tenemos, por ejemplo:

$$R_{b_1b_2}(\theta) = R_{xy}(\theta) = \begin{pmatrix} \cos\theta & -sen\theta & 0 \\ sen\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$R_{b_2b_3}(\theta) = R_{yz}(\theta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -sen\theta \\ 0 & sen\theta & \cos\theta \end{pmatrix},$$

$$R_{b_3b_1}(\theta) = R_{zx}(\theta) = \begin{pmatrix} sen\theta & 0 & \cos\theta \\ 0 & 1 & 0 \\ \cos\theta & 0 & -sen\theta \end{pmatrix},$$

donde hemos usado también la notación clásica para los ejes x, y, z. Para concluir la idea, lo que decimos es que estos tres tipos de matrices nos bastan para expresar cualquier matriz de $SO(3)$, es decir, el grupo $SO(3)$ puede generarse mediante $\{R_{xy}(\theta), R_{yz}(\theta), R_{zx}(\theta) : \theta \in [0, 2\pi)\}$, esto es, cada $M \in SO(3)$ es un producto de este tipo de matrices de rotación de los planos generados por los básicos. En general, para n, usando la combinatoria tenemos $\binom{n}{2} = \frac{1}{2}n(n-1)$ planos generados por los n básicos (son las combinaciones de dos elementos tomados de un conjunto de n elementos sin importar el orden en que se tomen).

Con esto en mente, recordemos lo que obtuvimos para la multiplicación de cuaterniones en sus tres versiones, multiplicación izquierda, derecha y conjugación por un elemento, expresándolo con la base canónica, sea $p, q \in \mathbb{H}$, con $\|p\| = 1$, digamos $p = e^{i\theta}$, expresemos $q = c_1 + c_2 j$, con $c_1, c_2 \in \mathbb{C}_i$, entonces

$$pq = c_1 e^{i\theta} + c_2 e^{i\theta} j, \qquad qp = c_1 e^{i\theta} + c_2 e^{-i\theta} j, \qquad pqp^{-1} = c_1 + c_2 e^{2i\theta} j.$$

Con esto es claro que la conjugación por $p = e^{\frac{1}{2}i\theta}$ corresponde a $R_{jk}(\theta)$, y análogamente tenemos que la conjugación por $e^{\frac{1}{2}j\theta}$ y por $e^{\frac{1}{2}k\theta}$, corresponden respectivamente a $R_{ki}(\theta)$ y $R_{ij}(\theta)$. Entonces tenemos una relación entre $SO(3)$ y el grupo multiplicativo generado por la conjugación por estos elementos. Para el caso tridimensional tenemos aún más, las transformaciones que preservan tamaño, ortogonalidad y orientación son justamente las rotaciones efectuadas en un plano a la vez, ya que no tenemos suficientes grados de libertad para hallar otro plano en el espacio ortogonal a dicho plano, entonces solo hallamos una línea o eje ortogonal, el llamado eje de rotación. Es decir, $SO(3)$ consta de las rotaciones de todos los posibles planos de $\mathbb{R}^3$ que pasen por el origen; y conforme a lo que vimos, incluyendo la identificación de $Im(\mathbb{H})$ y $\mathbb{R}^3$, dada una rotación de θ en cualquier plano, nos basta tomar un vector unitario u ortogonal a tal plano (un vector normal al plano) y entonces la rotación será representada mediante la conjugación por $e^{\frac{1}{2}u\theta}$ o por su negativo $-e^{\frac{1}{2}u\theta}$. En otras palabras, tenemos una relación dos a uno entre el subgrupo multiplicativo de unitarios de $\mathbb{H}$ y $SO(3)$, por lo cual tendríamos una biyección al considerar el cociente por $\mathbb{Z}_2 = \{0, 1\} \cong \{1, -1\}$ (según se use notación de suma o producto), lo cual tiene sentido, pues es un subgrupo normal y el cociente es en efecto un grupo, como esperamos. Entonces, el grupo multiplicativo de unitarios, $\mathbb{S}^3_{\mathbb{H}} = \{p \in \mathbb{H} : \|p\| = 1\}$, es el *doble cubriente* de $SO(3)$; también podemos considerar a las transformaciones dadas al conjugar por cada unitario en $\mathbb{H}$, con lo cual, la igualdad de funciones nos ahorra el cociente y así tenemos:

$$
\begin{aligned}
SO(3) &\cong \{u \in \mathbb{H} : \|u\| = 1\}/\mathbb{Z}_2 = \mathbb{S}^3_{\mathbb{H}}/\mathbb{Z}_2 \\
&\cong \{p\,\_\,p^{-1} : \mathbb{H} \longrightarrow \mathbb{H} \mid p \in \mathbb{S}^3_{\mathbb{H}}\},
\end{aligned}
$$

donde hemos usado la notación $p\,\_\,p^{-1}$ para denotar dónde se coloca el argumento de la función o transformación: $p\,\_\,p^{-1}(q) = pqp^{-1}$. Vale mencionar que estas asignaciones son morfismos de grupos, es decir, preservan la operación de grupo, considerando el producto de matrices como operación en $SO(3)$ (cuyo neutro es I_3) y la multiplicación en $\mathbb{S}^3_{\mathbb{H}}$ y la composición de transformaciones (cuyo neutro es conjugar por 1), respectivamente; entonces tenemos un isomorfismo entre ambos grupos. Por otro lado, podemos comprobar lo que afirmamos de las transformaciones, primero, conjugar por p y por $-p$ dan lo mismo: $(-p)q(-p)^{-1} = (-p)q(-p^{-1}) = -(-pqp^{-1}) = pqp^{-1}$; además si pasa que para algún $r \in \mathbb{H}$, con $\|r\| = 1$, se tiene que $r\,\_\,r^{-1} = p\,\_\,p^{-1}$ (como funciones), en particular, tenemos que $r = rrr^{-1} = prp^{-1}$, por tanto $rp = pr$, así que, por lo que vimos antes, debe ser que son paralelos y como $\|p\| = 1 = \|r\|$, tenemos que $r = -p$. Más aún, lo que nos muestra el primer isomorfismo es la identificación de antípodas en la 3-esfera, $\mathbb{S}^3_{\mathbb{H}}$, lo cual es el llamado espacio proyectivo $\mathbb{P}^3(\mathbb{R})$ y nos indica cómo es la topología de $SO(3)$.

Hasta aquí hemos podido expresar las rotaciones en los tres planos generados por los básicos imaginarios i, j, k, si expresamos las rotaciones de los planos restantes: $1i$, $1j$ y $1k$, podemos generar todas las rotaciones del espacio tetradimensional $\mathbb{R}^4$, esto es, $SO(4)$. Esto lo podemos hacer mediante la multiplicación por ambos lados, sea $p = e^{i\theta}$ y $q = c_1 + c_2 j$, con $c_1, c_2 \in \mathbb{C}_i$:

$$\begin{aligned} pqp &= e^{i\theta}(c_1 + c_2 j)e^{i\theta} \\ &= e^{i\theta}c_1 e^{i\theta} + e^{i\theta}c_2 j e^{i\theta} \\ &= c_1 e^{2i\theta} + c_2 e^{i\theta}e^{-i\theta} j \\ &= c_1 e^{2i\theta} + c_2 j, \end{aligned}$$

lo cual es una rotación del plano $1i$ por 2θ; cálculos similares muestran que $e^{\frac{1}{2}i\theta}\_\, e^{\frac{1}{2}i\theta}$ corresponde a $R_{1i}(\theta)$, $e^{\frac{1}{2}j\theta}\_\, e^{\frac{1}{2}j\theta}$ a $R_{1j}(\theta)$ y $e^{\frac{1}{2}k\theta}\_\, e^{\frac{1}{2}k\theta}$ a $R_{1k}(\theta)$. Entonces, de nuevo, al considerar que las transformaciones correspondientes a $e^{\frac{1}{2}k\theta}$ y $-e^{\frac{1}{2}k\theta}$ coinciden, podemos afirmar que tenemos dos series de relaciones dos a uno que denotamos mediante $\sim$, considerando $u, v, w \in \{i, j, k\}$ (distintos entre sí) y $\theta \in [0, 2\pi)$:

$$e^{\frac{1}{2}u\theta}\_\, e^{-\frac{1}{2}u\theta} \leftrightarrow e^{\frac{1}{2}u\theta} \sim R_{vw}(\theta) \text{ y}$$

$$e^{\frac{1}{2}u\theta}\_\, e^{\frac{1}{2}u\theta} \leftrightarrow e^{\frac{1}{2}u\theta} \sim R_{1u}(\theta),$$

donde en el lado izquierdo consideramos funciones $\mathbb{H} \longrightarrow \mathbb{H}$, en medio, elementos de $\mathbb{S}^3_{\mathbb{H}}$ y a la derecha, elementos de $SO(4)$. Por otro lado, sabemos que $SO(4)$ es generado por esos seis tipos de rotaciones, entonces tenemos

$$SO(4) = \left\langle \left\{ R_{vw}(\theta), R_{1u}(\theta) : u, v, w \in \{i, j, k\}, \theta \in [0, 2\pi) \right\} \right\rangle,$$

donde la notación representa al grupo generado por un subconjunto, esto es, dado un subconjunto $X \subseteq G$ de un grupo G:

$$\langle X \rangle = \{ g \in G : \exists S_g \subseteq X \, (g = \textstyle\prod_{s \in \hat{S}_g} s, \, |S_g| \in \mathbb{N}) \},$$

siendo $\hat{S}_g = S_g \cup S_g^{-1}$, con $S_g^{-1} = \{s^{-1} : s \in S_g\}$, son los elementos de G que pueden expresarse como el producto finito de elementos e inversos de elementos tomados de X, en nuestro caso el grupo G es el conjunto de matrices ortogonales $O(4)$. Ya que hemos repasado esta noción de grupo generado se nos ocurre que podemos decir algo al respecto de $SO(4)$ mediante las relaciones que mencionamos con $\mathbb{S}^3_{\mathbb{H}}$ y en efecto, veremos varias maneras en que esto se puede expresar, por lo que vimos antes, primero podemos afirmar que entonces

$$SO(4) \cong \left\langle \{ e^{\frac{1}{2}u\theta}\_\, e^{-\frac{1}{2}u\theta},\, e^{\frac{1}{2}u\theta}\_\, e^{\frac{1}{2}u\theta} : \mathbb{H} \longrightarrow \mathbb{H} \mid u, v, w \in \{i, j, k\}, \theta \in [0, 2\pi) \} \right\rangle.$$

Para ver otras relaciones, comencemos por notar que las rotaciones que representan la multiplicación izquierda y derecha, las cuales giran dos planos ortogonales por el mismo ángulo (llamadas *isoclínicas*, por cierto), también pueden generar $SO(4)$: definimos, considerando la multiplicación

$$\begin{array}{ll} \text{por la izquierda} & \text{por la derecha} \\ S^+_{jk}(\theta) = R_{jk}(\theta)R_{1i}(\theta) \sim e^{i\theta}\_ & S^-_{jk}(\theta) = R_{jk}(\theta)R_{1i}(-\theta) \sim \_e^{-i\theta} \\ S^+_{ki}(\theta) = R_{ki}(\theta)R_{1j}(\theta) \sim e^{j\theta}\_ & S^-_{ki}(\theta) = R_{ki}(\theta)R_{1j}(-\theta) \sim \_e^{-j\theta} \\ S^+_{ij}(\theta) = R_{ij}(\theta)R_{1k}(\theta) \sim e^{k\theta}\_ & S^-_{ij}(\theta) = R_{ij}(\theta)R_{1k}(-\theta) \sim \_e^{-k\theta}, \end{array}$$

donde hemos empleado el símbolo $\sim$ para denotar las correspondencias de la transformación y la matriz. También tenemos biyecciones, $e^{u\theta}\_ \leftrightarrow e^{u\theta} \in \mathbb{S}^3_{\mathbb{H}}$ y $\_e^{-u\theta} \leftrightarrow e^{-u\theta} \in \mathbb{S}^3_{\mathbb{H}}$, para $u = i, j, k$, como las que antes conocimos (considerando la conjugación por un elemento y multiplicación por ambos lados), por tanto tenemos relaciones de la forma $S^+_{vw}(\theta) \sim e^{u\theta}$ y $S^-_{vw}(\theta) \sim e^{-u\theta}$. Por otro lado, considerando estas rotaciones isoclínicas y la asociatividad de la multiplicación, tenemos que, por ejemplo:

$$S^+_{jk}(\tfrac{1}{2}\theta)S^-_{jk}(\tfrac{1}{2}\theta) \sim e^{\frac{1}{2}i\theta}\_\, e^{-\frac{1}{2}i\theta} \sim R_{jk}(\theta) \text{ y}$$

$$S^+_{jk}(\tfrac{1}{2}\theta)S^-_{jk}(-\tfrac{1}{2}\theta) \sim e^{\frac{1}{2}i\theta}\_\, e^{\frac{1}{2}i\theta} \sim R_{1i}(\theta),$$

y de manera análoga, podemos expresar la correspondencia de las otras cuatro rotaciones $R_{ki}(\theta)$ y $R_{1j}(\theta)$, y $R_{ij}(\theta)$ y $R_{1k}(\theta)$; con lo que

$$\begin{aligned} SO(4) &= \left\langle \{S^\pm_{jk}(\theta), S^\pm_{ki}(\theta), S^\pm_{ij}(\theta) : \theta \in [0, \pi)\} \right\rangle \\ &\cong \left\langle \{e^{\frac{1}{2}u\theta}\_,\ \_e^{\frac{1}{2}u\theta} : \mathbb{H} \longrightarrow \mathbb{H} \mid u, v, w \in \{i, j, k\}, \theta \in [0, 2\pi)\} \right\rangle. \end{aligned}$$

Tenemos más aún: como ya notamos, la asociatividad de la multiplicación nos permite notar que para $p, r \in \mathbb{S}^3_{\mathbb{H}}$, tenemos que $(pq)r = p(qr)$, en otras palabras, para las rotaciones isoclínicas correspondientes, digamos S_p y S_r, se tiene que $S_r(S_p(q)) = S_p(S_r(q))$, esto es, conmutan: $S_rS_p = S_pS_r$. Como la composición de funciones es asociativa, entonces podemos acomodar todas las rotaciones correspondientes a multiplicaciones por la izquierda como factores a la izquierda en un producto de rotaciones, y lo propio con las correspondientes a las multiplicaciones por la derecha, así $SO(4) \cong$

$$\left\langle \{S^+_{jk}(\theta), S^+_{ki}(\theta), S^+_{ij}(\theta) : \theta \in [0, \pi)\} \times \{S^-_{jk}(\theta), S^-_{ki}(\theta), S^-_{ij}(\theta) : \theta \in [0, \pi)\} \right\rangle.$$

Esto nos da una idea interesante para describir la topología de $SO(4)$, consideremos las funciones $p\_r : \mathbb{H} \longrightarrow \mathbb{H}$, con $p, r \in \mathbb{S}^3_{\mathbb{H}}$, para las cuales es claro que con $(p, r) \in \mathbb{S}^3_{\mathbb{H}} \times \mathbb{S}^3_{\mathbb{H}}$ y $(-p, -r) \in \mathbb{S}^3_{\mathbb{H}} \times \mathbb{S}^3_{\mathbb{H}}$ obtenemos la misma función; además el grupo generado por los $e^{\frac{1}{2}u\theta}$ que involucran los básicos $u \in \{i, j, k\}$, resulta ser toda la 3-esfera en cada caso, por lo que

$$\begin{aligned} SO(4) &\cong \{p\_r : \mathbb{H} \longrightarrow \mathbb{H} \mid p, r \in \mathbb{S}^3_{\mathbb{H}}\} \\ &\cong \mathbb{S}^3_{\mathbb{H}} \times \mathbb{S}^3_{\mathbb{H}} / \mathbb{Z}_2. \end{aligned}$$

Lo cual nos indica que $\mathbb{S}^3_{\mathbb{H}} \times \mathbb{S}^3_{\mathbb{H}}$ es el doble cubriente de $SO(4)$.

7

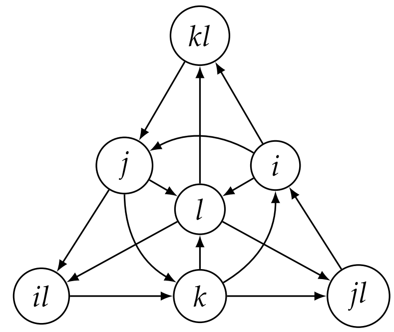
LOS OCTONIONES $\mathbb{O}$

7.1 REPRESENTACIONES Y GENERALIDADES

Seguimos agregando unidades imaginarias... Después de que Hamilton concibiera la relación fundamental de los cuaterniones, compartió esto con su amigo John Thomas Graves escribiéndole una carta. Cerca de dos meses después, Graves respondió describiendo un sistema que llamó *octavas*, incluyendo siete unidades imaginarias. Independientemente, en 1845, Arthur Cayley también describió a este sistema con ocho básicos, una unidad real y siete imaginaras; por eso también son llamados números de Cayley. Luego, Leonard Eugene Dickson mostró el proceso para definir los octoniones partiendo de los cuaterniones, así como de los cuaterniones partiendo de los complejos (Dickson, 1919), de ahí el nombre del proceso que presentamos y fue el foco de la primera parte. Pero volvamos al asunto de los, también llamados en concordancia a sus «hermanos menores», octoniones denotados con su correspondiente letra $\mathbb{O}$. Si agregamos otra unidad imaginaria a los cuaterniones, digamos l, resulta necesario decir qué da il, ij e kl, y resulta que para que obtengamos un álgebra debe ser que estos tres también sean unidades imaginarias, es decir, raíces de -1. Como con los cuaterniones, incluir una nueva unidad imaginaria en $\mathbb{C}$ implicó incluir otra unidad, en este caso incluir otra en $\mathbb{H}$ implica incluir otras tres, esto no es más que una versión del teorema de Hurwitz (teorema 2.4). Con estas siete unidades imaginarias y la unidad real 1 se puede representar cualquier octonión

$$x = 1x_1 + ix_2 + jx_3 + kx_4 + lx_5 + ilx_6 + jlx_7 + klx_8,$$

con $x_1, ..., x_8 \in \mathbb{R}$, es decir podemos representar a los octoniones en $\mathbb{R}^8$. Sin embargo, aún nos hace falta mencionar lo que dan el resto de productos entre estas unidades imaginarias (con la real ya sabemos que 1 es la unidad del álgebra), para lo cual hacemos uso de otra linda representación, esta vez mediante un diagrama que también representa al espacio proyectivo de siete puntos y siete líneas, también llamado plano de Fano en honor al matemático Gino Fano, y vale mencionar que el círculo interior es una línea. Las flechas en una misma línea indican un producto positivo en ese sentido: $(il)k = jl$, pero en sentido contrario, negativo $k(il) = -jl$.



Para ejemplificar más el uso de esta representación aquí mostramos los productos que representa la base (línea horizontal) del triángulo:

$$(il)k = jl,\ k(jl) = il,\ (jl)(il) = k,\ k(il) = -jl,\ (jl)k = -il \text{ y } (il)(jl) = -k.$$

Recordemos que en este sistema no se cumple la asociatividad, como podemos comprobar y para lo cual usaremos un punto para enfatizar que nos referimos al producto entre dos elementos y no a su resultado, que denotamos yuxtaponiendo, esto solo para enfatizar, pues sabemos que representan la misma entidad, así tenemos: $(i \cdot j)l = (k)l = kl$ mientras que $i(j \cdot l) = i(jl) = -kl$; podríamos decir que estos productos son antiasociativos, es interesante notar que no es una propiedad general, ya que algunas tercias de productos sí cumplen la asociatividad y otras la «antiasociatividad».

Otra manera en que podemos representar a los octoniones es considerando que cualquier $x \in \mathbb{O}$ se puede expresar como

$$x = (x_1 + ix_2 + jx_3 + kx_4) + (x_5 + ix_6 + jx_7 + kx_8)l = q_1 + q_2 l,$$

con $q_1, q_2 \in \mathbb{H}$, es decir, mediante parejas de cuaterniones en $\mathbb{H}^2$ o más específicamente $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}l$. También podemos representarlo como

$$\begin{aligned} x &= (x_1 + ix_2) + (x_3 + ix_4)j + (x_5 + ix_6)l + (x_7 + i(-x_8))jl \\ &= c_1 + c_2 j + c_3 l + c_4 jl, \end{aligned}$$

con $c_1, ..., c_4 \in \mathbb{C}$, esto es, mediante tétradas de números complejos en $\mathbb{C}^4$ como $\mathbb{C} \oplus \mathbb{C}j \oplus \mathbb{C}l \oplus \mathbb{C}jl$. Podemos notar que en esta representación «clásica» (con i, j, k, l) estamos considerando productos de básicos a la *derecha*, mientras que en la construcción de Cayley-Dickson los consideramos a la *izquierda*, lo cual nos lleva a signos «menos» al cambiar de una a otra; lo cual sabemos que no tiene importancia, pues representan al mismo sistema $\mathbb{O}$. También cabe mencionar que pudimos definir el producto de otra manera, ligeramente distinta a la de la construcción de Cayley-Dickson que presentamos, con tal de que los productos aparecieran a la derecha, sin embargo, insistimos, los teoremas de unicidad salvo isomorfismo que vimos nos dicen que todos los caminos que tomemos nos llevan al mismo lugar, y seguiremos la notación clásica por su fácil uso.

Ahora veamos algunas particularidades, tenemos para $x, y \in \mathbb{O}$, que su producto es:

$$\begin{aligned} xy = &(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8) \\ &+ i(x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7) \\ &+ j(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6) \\ &+ k(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5) \\ &+ l(x_1y_5 - x_2y_6 - x_3y_7 - x_4y_8 + x_5y_1 + x_6y_2 + x_7y_3 + x_8y_4) \\ &+ il(x_1y_6 + x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 + x_6y_1 - x_7y_4 + x_8y_3) \\ &+ jl(x_1y_7 + x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 + x_7y_1 - x_8y_2) \\ &+ kl(x_1y_8 - x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2 + x_8y_1). \end{aligned}$$

La involución queda $x^* = x_1 - ix_2 - jx_3 - kx_4 - lx_5 - ilx_6 - jlx_7 - klx_8$, y los inversos $x^{-1} = \frac{1}{xx^*}x^* = \frac{1}{\|x\|}x^*$, y de hecho, que la norma preserve productos (propiedad de álgebras de composición) significa una nueva regla de cuadrados, esta vez de ocho.

7.2 ¿Cómo trabajar con la no asociatividad de $\mathbb{O}$?

Como hicimos con los números complejos y los cuaterniones, podemos considerar la 7-esfera

$$\mathbb{S}^7_{\mathbb{O}} = \{x \in \mathbb{O} : \|x\| = 1\},$$

en particular para $s \in Im(\mathbb{O})$ tal que $\|s\| = 1$, podemos considerar la subálgebra generada por 1 y s:

$$\mathbb{C}_s = \{1a + sb \in \mathbb{O} : a, b \in \mathbb{R}\},$$

la cual hemos nombrado así porque evidentemente es isomorfa a la de los complejos. Esta subálgebra que podemos llamar «compleja» tiene las propiedades que ya conocemos de los complejos; con esto podemos expresar cualquier octonión $x \in \mathbb{O}$ como

$$x = \|x\|e^{s_x\theta_x} = r_x\left(\cos(\theta_x) + s_x sen(\theta_x)\right),$$

siendo

$$s_x = \begin{cases} \frac{1}{\|Im(x)\|}Im(x) & \text{si } \|Im(x)\| \neq 0 \\ 0 & \text{si } \|Im(x)\| = 0, \end{cases}$$

con $\theta_x = \arg(s_x)$, $r_x = \|x\|$; donde, s_x nos dice la «dirección imaginaria» de x y θ_x el ángulo formado por el eje «real» y x, el cual se ubica en el plano $1s_x$.

Podemos considerar dos unitarios imaginarios $s, t \in \mathbb{S}^6_{Im(\mathbb{O})}$ ortogonales (o equivalentemente que anticonmuten entre sí, por el teorema 4.2), así resulta que la subálgebra generada por $\{1, s, t, st\}$

$$\mathbb{H}_{s,t} = \{1a + sb + tc + std \in \mathbb{O} : a, b, c, d \in \mathbb{R}\},$$

es isomorfa (como álgebra) a la de los cuaterniones, veremos que esto nos es de gran utilidad. Entonces, para un octonión $x \in \mathbb{O}$, podemos considerar el álgebra compleja correspondiente; para dos, $x, y \in \mathbb{O}$, si el primero lo expresamos como $x = 1x_1 + \iota x_2$ para cierto unitario $\iota \in Im(\mathbb{O})$ y $x_1, x_2 \in \mathbb{R}$, para el segundo se requiere a lo más otra «dirección» imaginaria, digamos la de un unitario $\xi \in Im(\mathbb{O})$ ortogonal a ι, así podemos expresar $y = 1y_1 + \iota y_2 + \xi y_3 \in \mathbb{H}_{\iota,\xi}$, con $y_1, y_2, y_3 \in \mathbb{R}$; para un tercero, digamos $z \in \mathbb{O}$, se requiere a lo más otra dirección imaginaria independiente, digamos la de un $\lambda \in Im(\mathbb{O})$ unitario y ortogonal a los tres dependientes, $\iota, \xi, \iota\xi$ (dependientes porque el último depende de los primeros), entonces expresamos

$$z = 1z_1 + \iota z_2 + \xi z_3 + \iota\xi z_4 + \lambda z_5,$$

con $z_1, ..., z_5 \in \mathbb{R}$; solo hasta que consideremos un cuarto octonión w, posiblemente requerimos usar todos los ocho grados de libertad posibles para expresarlo, lo cual puede hacerse en términos de los tres unitarios imaginarios ortogonales que mencionamos, ι, ξ y λ, así

$$w = 1w_1 + \iota w_2 + \xi w_3 + \iota\xi w_4 + \lambda w_5 + \iota\lambda w_6 + \xi\lambda w_7 + (\iota\xi)\lambda w_8,$$

a estas tercias se les llama **tercias básicas** (Baez (2002)) pues definen una base ortonormal. Cabe notar que al considerar dos octoniones (y sus múltiplos escalares), los productos de estos cumplen la asociatividad, siendo elementos de la subálgebra cuaterniónica correspondiente, lo cual no es más que la propiedad que vimos resulta equivalente a ser álgebra alternativa y que nos da el teorema de Artin (teorema 2.1).

7.3 GEOMETRÍA Y EL PRODUCTO CRUZ EN 7 DIMENSIONES

Vimos que, para el caso de los cuaterniones, la biyección o identificación entre $Im(\mathbb{H})$ y $\mathbb{R}^3$ nos permitió expresar el producto punto y el producto cruz como el producto de imaginarios, respectivamente siendo su parte real e imaginaria. En el caso de los octoniones nos encontramos con algo similar, para facilitar la notación, identificamos $x = (x_2, x_3, ..., x_8) \in \mathbb{R}^7$

con $x = 0 + ix_2 + jx_3 + ... + klx_8 \in Im(\mathbb{O})$, así, el producto cruz en siete dimensiones puede definirse como:

$$\begin{aligned}
x \times y = Im(xy) \\
= \quad & i(x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7) \\
& + j(-x_2y_4 + x_4y_2 + x_5y_7 + x_6y_8 - x_7y_5 - x_8y_6) \\
& + k(x_2y_3 - x_3y_2 + x_5y_8 - x_6y_7 + x_7y_6 - x_8y_5) \\
& + l(-x_2y_6 - x_3y_7 - x_4y_8 + x_6y_2 + x_7y_3 + x_8y_4) \\
& + il(x_2y_5 - x_3y_8 + x_4y_7 - x_5y_2 - x_7y_4 + x_8y_3) \\
& + jl(x_2y_8 + x_3y_5 - x_4y_6 - x_5y_3 + x_6y_4 - x_8y_2) \\
& + kl(-x_2y_7 + x_3y_6 + x_4y_5 - x_5y_4 - x_6y_3 + x_7y_2).
\end{aligned}$$

Y a todo esto ¿qué es el producto cruz? En tres dimensiones es muy conocido y usado en varias aplicaciones, pero ¿cómo generalizarlo a más dimensiones? En Lounesto (2001), capítulo 7, podemos encontrar respuestas. Las propiedades básicas que definen al producto cruz en 3 dimensiones $\times : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ son: $\forall a, b \in \mathbb{R}^3$

- $(a \times b) \cdot a = 0 = (a \times b) \cdot b$: Ortogonalidad del producto a sus factores.
- $\|a \times b\| = \|a\|\|b\| sen(\theta)$: El tamaño representa el área que comprende en el paralelepípedo definido por a y b, siendo θ el ángulo entre éstos, este equivale a $\|a \times b\|^2 = \|a\|^2\|b\|^2 - (a \cdot b)^2$.

Estas pueden ayudarnos a definir una versión en más dimensiones. Este producto resulta ser $\mathbb{R}$-bilineal y anticonmutativo $a \times b = -b \times a$, con lo cual $a \times a = -a \times a$, esto es $a \times a = 0$. Siendo $a = (a_1, a_2, a_3) = a_1e_1 + a_2e_2 + a_3e_3$ y de manera similar b, y siendo $e_1 = (1, 0, 0), e_2 = (0, 1, 0), ...,$ los básicos canónicos, podemos escribirlo como

$$a \times b = \begin{vmatrix} e_1 & e_2 & e_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$$

En el caso de más dimensiones, digamos en $\mathbb{R}^n$, una posible generalización consiste en considerar el producto de $n-1$ factores, es decir una operación $n-1$-aria que nos da un vector ortogonal a éstos y cuya norma es igual al «hipervolumen» del «hiperparalelepípedo» definido por éstos; una manera de definir esto surge de la expresión mediante determinantes

$$\times(a, b, c, ...) = \begin{vmatrix} e_1 & e_2 & e_3 & ... \\ a_1 & a_2 & a_3 & ... \\ b_1 & b_2 & b_3 & ... \\ \vdots & \vdots & \vdots & \ddots \end{vmatrix}$$

Pero si buscamos un producto de dos factores que cumpla las propiedades de ortogonalidad y norma-área en n dimensiones resulta que solo existe para $n = 3$ y $n = 7$. En el caso de siete dimensiones se puede definir en términos de los básicos canónicos $e_1, e_2, ..., e_8$, considerando las relaciones $e_i \times e_j = -e_j \times e_i$, con $i, j \in \{1, ..., 8\}$, y considerando los índices módulo 7 en:

$$e_i \times e_{i+1} = e_{i+3}, \quad e_{i+1} \times e_{i+3} = e_i, \quad e_{i+3} \times e_i = e_{i+1}.$$

Extendiendo bilinealmente a todos los elementos de $\mathbb{R}^7$, i. e. para $a \times b = \sum_{i=1}^{7} a_i e_i \times \sum_{j=1}^{7} b_j e_j = \sum_{i=1}^{7} \sum_{i=1}^{7} (a_i b_j) e_i \times e_j$, claramente estas relaciones definitorias hacen que este producto cruz sea bilineal y anticonmutativo. Para notar cómo se relaciona esta definición con la que ya habíamos presentado en el contexto de los octoniones, basta considerar la asignación

$$\begin{aligned} e_1 &\leftrightarrow i \\ e_2 &\leftrightarrow j \\ e_3 &\leftrightarrow l \\ e_4 &\leftrightarrow ij = k \end{aligned} \qquad \begin{aligned} e_5 &\leftrightarrow jl \\ e_6 &\leftrightarrow -kl \\ e_7 &\leftrightarrow il, \end{aligned}$$

con la cual vemos cómo se cumplen las relaciones definitorias, mismas que podemos verificar en el plano de Fano, confirmando que lo que llamamos producto cruz en $Im(\mathbb{O})$ en efecto cumple las propiedades básicas que asociamos a éste (ortogonalidad a factores, norma-área, anticonmutatividad).

En el caso de 3 dimensiones la «dirección» ortogonal de $a \times b$ al plano donde se encuentren a y b (distintos de 0) es única y basta definir un sentido de orientación, derecho o izquierdo; en el caso de siete dimensiones no es así, por eso la importancia de esta definición; además en $\mathbb{R}^3$, $a \times b = c \times d$ implica que a, b, c y d estén en el mismo plano, algo que no necesariamente ocurre en siete dimensiones. Al situar el producto cruz en el contexto de los octoniones nos permiten definirlo naturalmente, pues, dados $x, y \in Im(\mathbb{O})$ podemos considerar alguna subálgebra $\mathbb{H}_{s,t}$ que los contenga y en ésta el producto cruz es el de 3 dimensiones y por tanto está definido en su dirección de manera única. Notemos más propiedades que desde la perspectiva de los octoniones son claras; dados $a, b \in Im(\mathbb{O})$, tenemos que

$$ab = Re(ab) + Im(ab) = -a \cdot b + a \times b,$$

y considerando que $ba = -b \cdot a + b \times a = -a \cdot b - a \times b$, con lo que $a \times b = \frac{1}{2}(ab - ba) = \frac{1}{2}[a, b]$; también podemos expresar el producto de octoniones en términos del producto real, escalar, punto y cruz, para $a = \alpha + A$, $b = \beta + B \in \mathbb{O}$, con $\alpha, \beta \in \mathbb{R}$ y $A, B \in Im(\mathbb{O})$, tenemos que

$$\begin{aligned} ab &= \alpha\beta + \alpha B + \beta A + AB \\ &= \alpha\beta + \alpha B + \beta A + Re(AB) + Im(AB) \\ &= \alpha\beta + \alpha B + \beta A - A \cdot B + A \times B. \end{aligned}$$

Finalmente, una propiedad interesante es que para 3 dimensiones, el producto cruz es invariante bajo $SO(3)$, algo que no ocurre para lo correspondiente en 7 dimensiones, en cambio es invariante bajo el grupo G_2, un subgrupo propio de $SO(7)$, el cual veremos con más detalle en la última sección.

En la siguiente sección veremos el significado geométrico de la multiplicación por uno y otro lado y la conjugación por un elemento dado, como vimos con los cuaterniones. Requerimos una propiedad que también cumplen los octoniones. Comencemos por considerar una base ortonormal $\{1, \iota, \xi, \kappa, \lambda, \iota\lambda, \xi\lambda, \lambda\kappa\}$ y notar que, para $q = 1a + \iota b + \xi c + \kappa d \in \mathbb{H}_{\iota,\xi}$, con $a, b, c, d \in \mathbb{R}$, tenemos que

$$\begin{aligned}
\lambda q &= \lambda(1a + \iota b + \xi c + \kappa d) \\
&= \lambda 1a + \lambda\iota b + \lambda\xi c + \lambda\kappa d \\
&= 1a\lambda - \iota b\lambda - \xi c\lambda - \kappa d\lambda \\
&= (1a - \iota b - \xi c - \kappa d)\lambda = q^*\lambda,
\end{aligned}$$

por lo tanto $\lambda q^* = q\lambda$, y de hecho sólo requerimos la ortogonalidad de los elementos de la base para usar el teorema 4.2.

7.4 DESCRIPCIÓN DE $SO(7)$ Y $SO(8)$

Para describir las rotaciones en $\mathbb{R}^7$ y $\mathbb{R}^8$, de acuerdo a lo que vimos al principio de la sección 5.3, nos basta saber cómo girar los planos generados por los básicos. Comencemos por reconocer que la conjugación por un unitario imaginario $\iota \in Im(\mathbb{O})$ representa una rotación isoclínica de 180° que deja al plano 1ι inalterado, para esto consideremos una base ortonormal que incluya a ι, digamos $\{1, \iota, \xi, \kappa = \iota\xi, \lambda, \iota\lambda, \xi\lambda, \kappa\lambda\}$, así, para cualquier $x \in \mathbb{O}$ tenemos que

$$x = 1x_1 + \iota x_2 + \xi x_3 + \kappa x_4 + \lambda x_5 + \iota\lambda x_6 + \xi\lambda x_7 + \kappa\lambda x_8,$$

y como tenemos solo dos octoniones, ι y x, sabemos que podemos situarnos en una subálgebra cuaterniónica asociativa y por tanto podemos expresar

$$\begin{aligned}
\iota x \iota^* &= \iota x(-\iota) \\
&= \iota(-\iota)x_1 + \iota\iota(-\iota)x_2 + \iota\xi(-\iota)x_3 + \iota\kappa(-\iota)x_4 + \iota\lambda(-\iota)x_5 \\
&\quad + \iota(\iota\lambda)(-\iota)x_6 + \iota(\xi\lambda)(-\iota)x_7 + \iota(\kappa\lambda)(-\iota)x_8 \\
&= x_1 + \iota x_2 - \xi x_3 - \kappa x_4 - \lambda x_5 - \iota\lambda x_6 - \xi\lambda x_7 - \kappa\lambda x_8,
\end{aligned}$$

donde hemos usado la distributividad, la anticonmtatividad debida a la ortogonalidad de los básicos y en especial la alternatividad para aligerar la notación pues tenemos por ejemplo

$$\begin{aligned}(\iota(\xi\lambda))(-\iota) &= -(\iota(\xi\lambda))(\iota) \\ &= -(-(\xi\lambda)\iota)(\iota) \\ &= \xi\lambda\iota^2 = -\xi\lambda = \iota^2(\xi\lambda) \\ &= -\iota(-\iota(\xi\lambda)) \\ &= -\iota((\xi\lambda)\iota) = \iota((\xi\lambda)(-\iota)),\end{aligned}$$

con lo que podemos escribir $\iota(\xi\lambda)(-\iota)$ sin ambigüedad, lo cual está de acuerdo con que consideramos solo dos octoniones y no tiene porqué haber asuntos con respecto a la asociatividad en el producto de estos, incluso en su expresión en términos de básicos.

Ahora revisamos una propiedad geométrica general de $\mathbb{R}^n$, $n \geq 3$: *cualquier rotación en un plano puede expresarse como el producto de dos rotaciones de 180° en planos ortogonales al primero*. Para ver esto, tomemos por ejemplo, una rotación de 2θ en el plano e_1e_2, entonces basta considerar una rotación de 180° del plano e_2e_3 ($R_{e_2e_3}(\pi)$) y una de 180° del plano por el origen ortogonal al unitario $u = \cos(\theta)e_1 + sen(\theta)e_2$ y que contenga a e_3 ($R_{ve_3}(\pi)$, donde $v = \cos(\theta)e_1 - sen(\theta)e_2$); esta idea tiene su origen en $\mathbb{R}^3$ donde se consideran rotaciones de 180° en torno a dos ejes que se sitúan en el plano que se quiere rotar y que forman un ángulo de θ entre ellos. Mediante la representación matricial de estas rotaciones, vemos que es así, donde abreviamos $\cos(\theta) = c_\theta$ y $sen(\theta) = s_\theta$:

$$R_{e_2e_3}(\pi) = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & -1 & 0 & 0 & \dots \\ 0 & 0 & -1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

y para la segunda rotación no hemos usado más que el cambio de base para rotar el plano ve_3 que equivale a rotar $-\theta$ el plano e_1e_2, luego rotar 180° el plano e_2e_3 y finalmente rotar θ el plano e_1e_2 nuevamente:

$$
\begin{aligned}
&R_{ve_3}(\pi)\\
&= \begin{pmatrix} c_\theta & -s_\theta & 0 & \dots \\ s_\theta & c_\theta & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & -1 & 0 & 0 & \dots \\ 0 & 0 & -1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} c_\theta & -s_\theta & 0 & \dots \\ s_\theta & c_\theta & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}\\
&= \begin{pmatrix} c_\theta^2 - s_\theta^2 & 2c_\theta s_\theta & 0 & 0 & \dots \\ 2c_\theta s_\theta & -(c_\theta^2 - s_\theta^2) & 0 & 0 & \dots \\ 0 & 0 & -1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}\\
&= \begin{pmatrix} \cos(2\theta) & -sen(2\theta) & 0 & 0 & \dots \\ sen(2\theta) & -\cos(2\theta) & 0 & 0 & \dots \\ 0 & 0 & -1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.
\end{aligned}
$$

El producto de ambas rotaciones es, en efecto, una rotación de 2θ en el plano e_1e_2, como podemos verificar enseguida:

$$
\begin{aligned}
&R_{ve_3}(\pi)R_{e_2e_3}(\pi)\\
&= \begin{pmatrix} \cos(2\theta) & -sen(2\theta) & 0 & 0 & \dots \\ sen(2\theta) & -\cos(2\theta) & 0 & 0 & \dots \\ 0 & 0 & -1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & -1 & 0 & 0 & \dots \\ 0 & 0 & -1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}\\
&= \begin{pmatrix} \cos(2\theta) & -sen(2\theta) & 0 & \dots \\ sen(2\theta) & \cos(2\theta) & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}.
\end{aligned}
$$

Cálculos similares funcionan para otros planos.

Ahora reunimos las ideas que vimos en los párrafos anteriores, tomando como ejemplo una rotación de 2θ en el plano ij, primero conjugamos por i para hacer la primera rotación de 180° y luego conjugamos por $u_\theta = i\cos(\theta) + jsen(\theta)$, así la rotación está dada, para $x \in \mathbb{O}$, por:

$$R_{ij}(2\theta)(x) = u_\theta \left(ix(-i)\right)(-u_\theta) = u_\theta(ixi)u_\theta,$$

expresión que no podemos simplificar más debido a la falta de asociatividad, lo cual es interesante, pues requerimos dos transformaciones para conseguir una rotación del plano, a diferencia de los sistemas numéricos anteriores. Es claro que, mediante transformaciones similares, podemos representar las rotaciones de los planos formados por parejas de los básicos imaginarios, i, j, k, l, il, jl, kl, y en general para cualquier pareja de unitarios $u, v \in \mathbb{S}^6_{Im(\mathbb{O})}$ ortogonales (i. e. tales que $u \cdot v = 0$ o equivalentemente $vu = -uv$) podemos expresar una rotación de 2θ en dicho plano como

$$(u\cos(\theta) + vsen(\theta))(u\_u)(u\cos(\theta) + vsen(\theta)).$$

Notemos que considerar $-\theta$ no nos da la misma transformación, tampoco considerar alguno (pero no ambos) $-u$ o $-v$, pero sí considerar ambos $-u$ y $-v$. Entonces podemos afirmar que $SO(7) \cong$

$$\left\langle \{(uc_\theta + vs_\theta)(u\_u)(uc_\theta + vs_\theta) : \mathbb{O} \longrightarrow \mathbb{O} \mid u, v \in \mathbb{S}^6_{Im(\mathbb{O})},\, u \cdot v = 0,\, \theta \in [0, \pi)\} \right\rangle.$$

De hecho, recordando que lo que estamos considerando son todas conjugaciones por unitarios imaginarios tenemos que

$$SO(7) \cong \left\langle \{p\_p^{-1} : \mathbb{O} \longrightarrow \mathbb{O} \mid p \in \mathbb{S}^6_{Im(\mathbb{O})}\} \right\rangle.$$

Enfatizamos que la no asociatividad del producto implica que esto no puede definir un morfismo de grupos, solo una biyección, además de la relevancia que tiene para servir como guía para describir un conjunto generador para $SO(7)$, algo que también será relevante en la descripción de $SO(8)$.

Veamos entonces, cómo describir $SO(8)$, sucede algo similar a lo que vimos con $SO(4)$ y $SO(3)$. Para esto requerimos considerar a la subálgebra compleja $\mathbb{C}_l$ y entonces considerar $\mathbb{O} = \mathbb{C}_l \perp \mathbb{C}_l^\perp$, con lo que $x \in \mathbb{O}$ puede expresarse como $x = re^{l\alpha} + x^\perp$, donde $x^\perp \in \mathbb{C}_l^\perp$. Por otro lado, tenemos que para $u \in \mathbb{S}^6_{Im(\mathbb{O})}$, $e^{u\theta} = \cos(\theta) + usen(\theta)$, de lo cual es claro que si $w \in Im(\mathbb{O})$ es ortogonal a u, tenemos que

$$e^{u\theta}w = w(e^{u\theta})^* = we^{-u\theta}.$$

Entonces, en nuestro caso, como en particular $x^\perp$ es ortogonal a l, tenemos que el producto por el unitario $e^{l\theta}$ por ambos lados (a la izquierda y a la derecha) aplicado a x es

$$\begin{aligned} e^{l\theta}xe^{l\theta} &= e^{l\theta}(re^{l\alpha} + x^\perp)e^{l\theta} \\ &= e^{l\theta}re^{l\alpha}e^{l\theta} + e^{l\theta}x^\perp e^{l\theta} \\ &= re^{l\theta}e^{l\alpha}e^{l\theta} + x^\perp e^{-l\theta}e^{l\theta} \\ &= re^{l\alpha+2\theta} + x^\perp. \end{aligned}$$

Lo cual evidentemente es una rotación del plano $1l$ por 2θ. Cálculos similares nos dan las rotaciones en los planos formados por 1 y las demás unidades imaginarias, y en general tenemos que para $p \in \mathbb{S}^7_{\mathbb{O}}$, podemos considerar que $p = e^{\lambda\theta}$ para cierto $\lambda \in \mathbb{S}_{Im(\mathbb{O})}$ y considerando una base ortonormal que lo contenga tenemos que $p\_p : \mathbb{O} \longrightarrow \mathbb{O}$ es una rotación de 2θ del plano 1λ, misma que obtendríamos al multiplicar por $-p$ por ambos lados. Con estas rotaciones y las rotaciones de los planos imaginarios que ya vimos, obtenemos que

$$\begin{aligned} SO(8) &\cong \Big\langle \{(uc_\theta + vs_\theta)(u\_u)(uc_\theta + vs_\theta) : \mathbb{O} \longrightarrow \mathbb{O} \mid u, v \in \mathbb{S}^6_{Im(\mathbb{O})}, u \cdot v = 0\} \\ &\qquad \cup \{ p\_p : \mathbb{O} \longrightarrow \mathbb{O} \mid p \in \mathbb{S}^7_{\mathbb{O}}\} \Big\rangle \\ &\cong \Big\langle \{q\_q^{-1} : \mathbb{O} \longrightarrow \mathbb{O} \mid q \in \mathbb{S}^6_{Im(\mathbb{O})}\} \cup \{ p\_p : \mathbb{O} \longrightarrow \mathbb{O} \mid p \in \mathbb{S}^7_{\mathbb{O}}\} \Big\rangle. \end{aligned}$$

Notemos que, de hecho, nos basta considerar la multiplicación por ambos lados, pues para $q \in \mathbb{S}^6_{Im(\mathbb{O})}$ tenemos que $q\_q^{-1} = q\_q^* = q\_(-q) = -(q\_q)$. Aún más, nos basta considerar la multiplicación por ambos lados por elementos de $\mathbb{S}^6_{Im(\mathbb{O})}$, algo que resulta sorprendente y que se debe a la no asociatividad. Veamos los detalles, para lo cual nos basamos en Manogue y Schray (1993) (un artículo, por demás interesante, en el cual encontramos una representación de las transformaciones de Lorentz en diez dimensiones). Comenzamos por establecer dos propiedades, primero, mediante las identidades de Moufang, para $x, y, z \in \mathbb{O}$, tenemos que $z(y(zxz)y)z = (zyz)x(zyz)$. Segundo, para $r, s \in \mathbb{S}^6_{Im(\mathbb{O})}$ ortogonales y por tanto tales que $rs = -sr$, tenemos que para cualquier $\theta \in [0, 2\pi)$, se cumple $e^{s\theta} = e^{-r\frac{\pi}{4}} e^{(r\cos(\theta)+s\mathrm{S}en(\theta))\frac{\pi}{2}} e^{-r\frac{\pi}{4}}$, lo cual podemos comprobar a continuación:

$$\begin{aligned} &e^{(r\cos(\theta)+s\mathrm{S}en(\theta))\frac{\pi}{2}} e^{-r\frac{\pi}{4}} \\ &= \left(\cos(\tfrac{\pi}{2}) + (r\cos(\theta) + ssen(\theta)sen(\tfrac{\pi}{2})\right)\left(\cos(-\tfrac{\pi}{4}) + rsen(-\tfrac{\pi}{4})\right) \\ &= \left(0 + (r\cos(\theta) + ssen(\theta)1\right)\left(\cos(-\tfrac{\pi}{4}) + rsen(-\tfrac{\pi}{4})\right) \\ &= -\cos(\theta)sen(\tfrac{-\pi}{4}) + r\cos(\theta)\cos(\tfrac{-\pi}{4}) + ssen(\theta)\cos(\tfrac{-\pi}{4}) + srsen(\theta)sen(\tfrac{-\pi}{4}) \\ &= \cos(\theta)sen(\tfrac{\pi}{4}) + r\cos(\theta)\cos(\tfrac{\pi}{4}) + ssen(\theta)\cos(\tfrac{\pi}{4}) + rssen(\theta)sen(\tfrac{\pi}{4}), \end{aligned}$$

donde hemos usado conocidas propiedades del coseno y seno, y la anticonmutatividad de los imaginarios r y s, por otro lado, como $\cos(\frac{\pi}{4}) = sen(\frac{\pi}{4})$, tenemos:

$$\begin{aligned} e^{r\frac{\pi}{4}} e^{s\theta} &= \left(\cos(\tfrac{\pi}{4}) + rsen(\tfrac{\pi}{4})\right)\left(\cos(\theta) + ssen(\theta)\right) \\ &= \cos(\theta)\cos(\tfrac{\pi}{4}) + r\cos(\theta)\cos(\tfrac{\pi}{4}) + ssen(\theta)\cos(\tfrac{\pi}{4}) + rssen(\theta)sen(\tfrac{\pi}{4}) \\ &= \cos(\theta)sen(\tfrac{\pi}{4}) + r\cos(\theta)\cos(\tfrac{\pi}{4}) + ssen(\theta)\cos(\tfrac{\pi}{4}) + rssen(\theta)sen(\tfrac{\pi}{4}). \end{aligned}$$

Conjuntando ambos resultados, tenemos que $e^{r\frac{\pi}{4}} e^{s\theta} = e^{(r\cos(\theta)+s\mathrm{S}en(\theta))\frac{\pi}{2}} e^{-r\frac{\pi}{4}}$ y por tanto lo que queríamos probar. Ahora veamos para qué nos sirven estas dos propiedades. Sea $p \in \mathbb{S}^7_{\mathbb{O}}$, entonces $p = e^{s\theta}$ para ciertos $s \in \mathbb{S}^6_{Im(\mathbb{O})}$ y $\theta \in [0, \pi)$, considerando $r \in \mathbb{S}^6_{Im(\mathbb{O})}$ ortogonal a s y $u = r\cos(\theta) + s sen(\theta) \in \mathbb{S}^6_{Im(\mathbb{O})}$, entonces tenemos que

$$\begin{aligned} pxp = e^{s\theta} x e^{s\theta} \\ &= (e^{-r\frac{\pi}{4}} e^{u\frac{\pi}{2}} e^{-r\frac{\pi}{4}}) x (e^{-r\frac{\pi}{4}} e^{u\frac{\pi}{2}} e^{-r\frac{\pi}{4}}) \\ &= \left(e^{-r\frac{\pi}{4}} \left(e^{u\frac{\pi}{2}} (e^{-r\frac{\pi}{4}} x e^{-r\frac{\pi}{4}}) e^{u\frac{\pi}{2}} \right) e^{-r\frac{\pi}{4}} \right) \\ &= \left(e^{-r\frac{\pi}{4}} \left((e^{u\frac{\pi}{4}})^2 (e^{-r\frac{\pi}{4}} x e^{-r\frac{\pi}{4}}) (e^{u\frac{\pi}{4}})^2 \right) e^{-r\frac{\pi}{4}} \right), \end{aligned}$$

con lo que vemos que puede expresarse como producto de multiplicaciones a ambos lados por elementos de la forma $e^{v\frac{\pi}{4}}$, con $v \in \mathbb{S}^6_{Im(\mathbb{O})}$, entonces constatamos que podemos parametrizar mediante estos elementos:

$$SO(8) \cong \left\langle \{ v\_ v : \mathbb{O} \longrightarrow \mathbb{O} \mid v \in \mathbb{S}^6_{Im(\mathbb{O})} \} \right\rangle.$$

Por otro lado, podemos notar que al considerar $x \in \mathbb{O}$ como $x = c_1 + c_2 i + c_3 j + c_4 k$, con $c_1, ..., c_4 \in \mathbb{C}_l$, tenemos que

$$\begin{aligned} e^{l\theta} x &= e^{l\theta}(c_1 + c_2 i + c_3 j + c_4 k) \\ &= e^{l\theta} c_1 + e^{l\theta}(c_2 i) + e^{l\theta}(c_3 j) + e^{l\theta}(c_4 k) \\ &= e^{l\theta} c_1 + (e^{l\theta} c_2) i + (e^{l\theta} c_3) j + (e^{l\theta} c_4) k, \end{aligned}$$

donde no hemos tenido dificultades con la asociatividad porque en cada caso se trata con dos unidades imaginarias, es decir, podemos usar la alternatividad de $\mathbb{O}$, esto es una rotación isoclínica de θ en los cuatro planos $1l$, $(il)i$, $(jl)j$ y $(kl)k$ a la vez; por otro lado como sabemos que $e^{l\theta} w = w e^{-l\theta}$ cuando w es ortogonal a l, tenemos que

$$\begin{aligned} x e^{l\theta} &= (c_1 + c_2 i + c_3 j + c_4 k) e^{l\theta} \\ &= c_1 e^{l\theta} + (c_2 i) e^{l\theta} + (c_3 j) e^{l\theta} + (c_4 k) e^{l\theta} \\ &= c_1 e^{l\theta} + (c_2 e^{-l\theta}) i + (c_3 e^{-l\theta}) j + (c_4 e^{-l\theta}) k, \end{aligned}$$

lo cual es una rotación de θ en el plano $1l$ y de $-\theta$ en los tres planos $(il)i$, $(jl)j$ y $(kl)k$ a la vez. Resultados análogos obtenemos al multiplicar por $e^{v\theta}$ a la izquierda o derecha, siendo $v \in \{i, j, k, l, il, jl, kl\}$ para los otros planos. Lo cual nos da un indicio de que las multiplicaciones izquierda y derecha también pueden servirnos para describir $SO(8)$. En efecto, sea $r, s, t \in \{i, j, k, l, il, jl, kl\}$, con $st = r$, entonces la multiplicación a la izquierda $e^{(s\cos(\theta) + t\mathbb{S}en(\theta)\frac{\pi}{2}}(e^{-s\frac{\pi}{2}}\_)$ resulta que gira los mismos planos que $e^{r\theta}\_$, por el mismo ángulo θ excepto por un signo menos para las partes de x que «anti-asocian» con s y t (lo cual comprobamos haciendo cálculos como los propuestos en Manogue y Schray (1993)), con lo cual componer ambas nos da una rotación de solo un plano y no cuatro a la vez, así podemos generar todas las rotaciones; de nuevo vemos cómo la falta de asociatividad tiene un papel de suma importancia. Cabe mencionar que nuevamente nos basta considerar $u \in \mathbb{S}^6_{Im(\mathbb{O})}$. Algo similar ocurre para la multiplicación a la derecha. Entonces tenemos que

$$\begin{aligned} SO(8) &\cong \left\langle \{ v\_ : \mathbb{O} \longrightarrow \mathbb{O} \mid v \in \mathbb{S}^6_{Im(\mathbb{O})} \} \right\rangle \\ &\cong \left\langle \{ \_\, v : \mathbb{O} \longrightarrow \mathbb{O} \mid v \in \mathbb{S}^6_{Im(\mathbb{O})} \} \right\rangle. \end{aligned}$$

Finalmente mencionamos, como una nota, que las tres representaciones están relacionadas, y de hecho que obtuviéramos tres a diferencia de los otros casos, es una manifestación más del concepto de «trialidad» que también es interesante. Estas últimas dos representaciones son llamadas «espinoriales» y tienen que ver, claro, con en concepto de espinor; también es interesante ver todo esto desde la perspectiva de las álgebras geométricas o de Clifford.

7.5 DESCRIPCIÓN DE G_2

Hasta ahora hemos tratado con los grupos $SO(n) \subset O(n)$ que podemos considerar como grupos de isometrías, siendo $SO(n)$ el subgrupo de isometrías que preservan la orientación; este último concepto se refiere a $\mathbb{R}$-espacios vectoriales con producto interior (y por tanto con norma y métrica) con orientación, es decir, consideramos espacios con bases orientadas y las transformaciones entre estos espacios preservan la orientación, que no es otra cosa que requerir que el determinante de la matriz asociada a la transformación sea 1. Considerando $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}\}$ como espacio vectorial o como álgebra según el contexto, lo que afirmamos es que hemos tratado las simetrías de $\mathbb{K}$ como espacio vectorial con producto interior con orientación (cuyo grupo podemos denotar como $SO(\mathbb{K})$ o $SO(Im(\mathbb{K}))$ según el caso), pero no hemos visto qué hay sobre sus simetrías como álgebra, es decir, considerar funciones $\mathbb{K}$-lineales $\mathbb{K} \longrightarrow \mathbb{K}$ que preserven el producto del álgebra y que tengan inversas con las mismas características, es decir, sean isomorfismos de álgebras; estas forman un grupo llamado el **grupo de automorfismos**, denotado $Aut(\mathbb{K})$. Notemos que en ambos casos la parte imaginaria es la que permite más simetrías, pues tanto isometrías como isomorfismos de álgebras (unitarias) asignan al $1 \in \mathbb{R}$ en 1 mismo, por lo que basta analizar lo que pasa en la parte imaginaria $Im(\mathbb{K})$. Es interesante que hasta ahora no lo hemos considerado porque no ha sido necesario, para el caso de $\mathbb{H}$, definimos isometrías asignando i, j, k a elementos de $Im(\mathbb{H})$ que sean ortogonales entre sí y con la misma orientación, lo cual asegura que la multiplicación sea preservada; lo que decimos es que

$$SO(3) = SO(Im(\mathbb{H})) \cong Aut(\mathbb{H}).$$

Para el caso de $\mathbb{K} = \mathbb{O}$ la situación cambia, pues como mencionamos al definir el producto cruz en 7 dimensiones, la orientación no nos basta, hay varios grados de libertad para definirlo, para ver los detalles, a continuación seguimos la exposición de Baez (2002). Conforme a lo que vimos sobre *tercias básicas* en la primera sección de este capítulo, éstas definen una base ortonormal que permite recuperar toda la multiplicación de $\mathbb{O}$, recapitulando lo que se requiere es una tercia de raíces de -1, esto es $\iota_1, \iota_2, \iota_3 \in \mathbb{S}^6_{Im(\mathbb{O})}$ tal que ι_2 es ortogonal a ι_1, e ι_3 es ortogonal a la subálgebra cuaterniónica generada por ι_1 e ι_2, es decir, ortogonal a ι_1, ι_2 e $\iota_1\iota_2$. De modo que definir un automorfismo $f \in Aut(\mathbb{O})$ corresponde definir una asignación tal que dada una tercia básica $\iota_1, \iota_2, \iota_3$, la tercia $f(\iota_1), f(\iota_2), f(\iota_3)$ también sea una tercia básica, esto quiere decir que podemos definir $f(\iota_1)$ como cualquier elemento de la 6-esfera $\mathbb{S}^6_{Im(\mathbb{O})}$, luego $f(\iota_2)$ como cualquier elemento de la 5-esfera ortogonal a $f(\iota_1)$, hasta aquí necesariamente tenemos que definir $f(\iota_1\iota_2) = f(\iota_1)f(\iota_2)$, finalmente podemos definir $f(\iota_3)$ como cualquier elemento de la 3-esfera de elementos ortogonales a $f(\iota_1)$, $f(\iota_2)$ y $f(\iota_1\iota_2)$, con lo cual obtenemos que $\dim(Aut(\mathbb{O})) = 6 + 5 + 3 = 14$.

Todos los grupos $SO(n)$ son grupos de Lie, es decir, grupos con una estructura de variedad diferenciable que hace que las operaciones de grupo (incluyendo la de inversos) sean suaves (diferenciables); además están los grupos $SU(n)$ y $Sp(n)$, siendo estos últimos una versión de los llamados **grupos simplécticos**, mismos que representan las transformaciones $\mathbb{R}$-lineales que preservan un producto antisimétrico interior definido en el espacio $\mathbb{R}^{2n}$ (o isomorfo a este), donde antisimétrico se refiere a que $(b, a) = -(a, b)$, esto es (en esto seguimos a Dray y Manogue (2015)), definiendo la matriz

$$\Omega = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix},$$

siendo I_n la matriz identidad de $n \times n$, tenemos que son de la forma

$$Sp(2n, \mathbb{R}) = \{H \in M_{2n\times 2n}(\mathbb{R}) : H^t \Omega H = \Omega\}.$$

Entonces, considerando matrices con entradas complejas y tomando la intersección con $SU(2n)$, obtenemos la llamada **forma real compacta** de estos grupos simplécticos, que es

$$Sp(n) = \{H \in M_{2n\times 2n}(\mathbb{C}) : H^t \Omega H = \Omega, \quad H^{*t} H = I_{2n}\}.$$

Más aún, Baez (2002) nos propone una clarificante manera de considerar a estos, también llamados grupos «clásicos» de Lie:

$$SO(n) = \{H \in M_{n\times n}(\mathbb{R}) : H^t H = I_n \text{ y } \det(H) = 1\},$$

$$SU(n) = \{H \in M_{n\times n}(\mathbb{C}) : H^{*t}H = I_n \text{ y } \det(H) = 1\},$$

$$Sp(n) = \{H \in M_{n\times n}(\mathbb{H}) : H^t H = I_n\}.$$

A estos grupos les corresponden sus álgebras «clásicas» de Lie respectivas, y de hecho al estudiar estos temas, en 1887, el matemático Wilhelm Killing encontró seis álgebras de Lie «excepcionales», sin embargo, en 1894, Élie Cartan mostró que dos eran isomorfas, así que solo hay 5 álgebras excepcionales y por tanto 5 grupos excepcionales correspondientes. El adjetivo de «excepcionales» se usa porque en ese entonces éstas no correspondían al estudio de las simetrías relacionadas con los reconocidos $\mathbb{R}$, $\mathbb{C}$ o $\mathbb{H}$; como puede sospecharse, tienen que ver con los (entonces poco conocidos) octoniones $\mathbb{O}$. El grupo excepcional más pequeño (dimensionalmente) es de hecho $Aut(\mathbb{O})$ al cual también se le denota como G_2, nombre que el mismo Cartan le dio al notar este hecho en 1914.

Veamos que $G_2 \subset SO(7)$, sabemos que $f \in G_2$ es $\mathbb{R}$-lineal, preserva productos y $f(1) = 1$, entonces, recordando la última propiedad que nos presentó la proposición 3.12, sabemos que f es una isometría, además para todo $r \in Re(\mathbb{O}) = \mathbb{R}$, $f(r) = rf(1) = r1 = r$, entonces se sigue que $f|_{Im(\mathbb{O})}$ es una isometría también (hecho que también se sigue del teorema de Witt, pues $Im(\mathbb{O}) = \mathbb{R}^{\perp}$), de hecho, podemos considerar sólo $f|_{Im(\mathbb{O})}$ pues su parte real no aporta información, en otras palabras, considerar que $f : Im(\mathbb{O}) \longrightarrow Im(\mathbb{O})$, y así $f \in SO(7)$ o bien considerar la biyección $f \leftrightarrow f|_{Im(\mathbb{O})}$.

Ahora regresamos a lo que mencionamos en la primera sección del capítulo: el producto cruz en 7 dimensiones es invariante bajo G_2. Para ver esto, recordemos que en la prueba de la proposición 3.12, vimos que un morfismo de álgebras entre álgebras con involución cuadrática como f cumple que para todo $a \in \mathbb{O}$, $f(Re(a)) = Re(f(a))$ y $f(Im(a)) = Im(f(a))$, con lo cual tenemos, para $a, b \in Im(\mathbb{O})$, que $f(a \times b) = f(Im(ab)) = Im(f(ab)) = Im(f(a)f(b)) = f(a) \times f(b)$.

Podemos comentar algo más sobre el resto de grupos excepcionales. Lo primero que hay que mencionar es que esto tiene que ver con física y en particular física cuántica. Las observables son funciones que representan las propiedades del estado de un sistema, en otras palabras representan cantidades físicas que se pueden medir, en física clásica son funciones reales, mientras que en la cuántica suelen describirse mediante matrices hermitianas complejas, esto es matrices complejas cuadradas tales que coinciden con su conjugada transpuesta, las denotamos $\mathfrak{h}_n(\mathbb{C}) = \{M \in M_{n\times n}(\mathbb{C}) : M = M^{*t}\}$. Como «mediciones» de un sistema, las observables han de ser cerradas bajo la adición y multiplicación escalar, incluso puede considerarse un «álgebra de observables»; en el caso cuántico ésta resulta no asociativa. En 1932, Pascual Jordan investigó los axiomas mínimos que álgebras así debían de cumplir, el resultado es lo que ahora llamamos álgebras de Jordan (formalmente reales). Como suele suceder, éstas ya han sido clasificadas y sabemos que cada una es la suma directa de simples, lo que nos lleva a clasificar sólo a las simples, las cuales resultan pertenecer a alguna de las cuatro familias infinitas $\mathfrak{h}_n(\mathbb{R})$, $\mathfrak{h}_n(\mathbb{C})$, $\mathfrak{h}_n(\mathbb{H})$ con el producto $A \circ B = \frac{1}{2}(AB + BA)$, el álgebra $\mathbb{R}^n \oplus \mathbb{R}$ con cierto producto que involucra el producto interior, o a una familia «excepcional» $\mathfrak{h}_3(\mathbb{O})$ con el producto $A \circ B = \frac{1}{2}(AB + BA)$, es claro el uso del término y por tanto que se le llame a esta última, álgebra de Jordan excepcional. Resulta interesante que de éstas, solo la familia $\mathfrak{h}_n(\mathbb{C})$ parezca útil para la física, aún no sabemos si las otras lo puedan ser. La excepcional parece mostrar un camino prometedor en cuanto a ciertas relaciones que se han encontrado con la teoría de cuerdas y las 10 dimensiones, y no es por menos, pues esta álgebra es la piedra fundamental para varios conceptos interesantes que ahora vemos de pasada. Resulta que una $M \in \mathfrak{h}_3(\mathbb{O})$ resulta ser de la forma

$$M = \begin{pmatrix} \alpha & z & y^* \\ z^* & \beta & x \\ y & x^* & \gamma \end{pmatrix},$$

con $\alpha, \beta, \gamma \in \mathbb{R} \subset \mathbb{O}$ y podemos definir un «determinante» para estas matrices como $\det(M) = \alpha\beta\gamma - (\alpha\|x\|^2 + \beta\|y\|^2 + \gamma\|z\|^2) + Re(xyz)$. Llegamos a mencionar los espacios proyectivos $\mathbb{P}^k(\mathbb{R})$, también pueden definirse para $\mathbb{C}$ y $\mathbb{H}$ con ciertas consideraciones debido a la no conmutatividad, sin embargo, la no asociatividad de $\mathbb{O}$ hace que encontrar un análogo para este no sea tan evidente: definimos el plano proyectivo octoniónico $\mathbb{P}^2(\mathbb{O})$ de la siguiente manera, los puntos son las proyecciones $p \in \mathfrak{h}_3(\mathbb{O})$ (i. e. $p^2 = p$) de traza 1, esto los hace de la forma

$$p = \begin{pmatrix} x \\ y \\ z \end{pmatrix} (x^* y^* z^*) = \begin{pmatrix} xx^* & xy^* & xz^* \\ yx^* & yy^* & yz^* \\ zx^* & zy^* & zz^* \end{pmatrix},$$

con $x, y, z \in \mathbb{O}$ tales que $(xy)z = x(yz)$ y $\|x\|^2 + \|y\|^2 + \|z\| = 1$, y líneas proyecciones de la forma $1 - p$, con p un punto. Aunque no lo parezca esta definición está inspirada y generaliza la usual para espacios reales de cierta manera, en Baez (2002) podemos hallar más detalles, en la tercera sección de su artículo, justamente llamada geometría proyectiva octoniónica. Este $\mathbb{P}^2(\mathbb{O})$ cumple en efecto los axiomas para considerarse como un plano proyectivo y presenta interesantes propiedades, es una variedad de 16 dimensiones, es un ejemplo de plano en el que no se cumple la propiedad de Desargues y lo que resulta pertinente para nosotros en este momento, se relaciona con los grupos excepcionales. Siguiendo el orden dimensional, el siguiente grupo excepcional de Lie, después de G_2, es F_2, es de dimensión 52 y resulta ser el grupo de automorfismos $Aut(\mathfrak{h}_3(\mathbb{O}))$, e isomorfo al grupo de isometrías de $\mathbb{P}^2(\mathbb{O})$, entonces representa las transformaciones $\mathbb{R}$-lineales que preservan el determinante que mencionamos y la traza. Luego está E_6 de dimensión 78, y justamente tiene que ver con las transformaciones que solo preservan el determinante y con el grupo de colineaciones de $\mathbb{P}^2(\mathbb{O})$, esto es, las transformaciones que preservan la colinealidad de puntos, denotado como $\mathrm{Col}(\mathbb{P}^2(\mathbb{O}))$; además tenemos la interesante relación

$$\begin{tikzcd}
\mathrm{Spin}(9) \arrow[r] \arrow[d] & \mathrm{Isom}(\mathbb{P}^2(\mathbb{O})) \cong F_4 \arrow[d] \\
\mathrm{Spin}(9,1) \arrow[r] & \mathrm{Col}(\mathbb{P}^2(\mathbb{O})) \cong E_{6(-26)},
\end{tikzcd}$$

donde $E_{6(-26)}$ es la forma real no compacta de E_6 cuya forma de Killing tiene signatura -26. Por eso se dice que F_4 es a la geometría Euclidiana de dimensión 9, como $E_{6(-26)}$ es a la geometría Lorentziana de dimensión 10. Finalmente, los otros dos grupos excepcionales, E_7 y E_8, son respectivamente de dimensión 133 y 24, y aunque pueden considerarse como los grupos de simetrías de ciertos espacios que involucran octoniones, su descripción nos llevaría más allá de los objetivos de este trabajo.

Con esto damos por terminado nuestro paseo por estos interesantes sistemas numéricos; como cabe esperar, tuvimos la oportunidad de ver sólo unos cuantos detalles, esperando que esto sirva como un breviario para inspirar a quien le interesa incursionar en estos temas.

APÉNDICES

A

ESTRUCTURAS ALGEBRAICAS

En este primer apéndice plasmamos la definición y varias propiedades de algunas estructuras algebraicas, que aunque conocidas, no está de más recordarlas, en especial por algunos detalles que omitimos en las pruebas en el desarrollo del trabajo y que se deben a las propiedades de estas estructuras. Nos basamos en las definiciones de Mac Lane y Birkhoff (1999).

Un **grupo** es un conjunto G con una operación binaria (función) que podemos denotar como $\alpha : G \times G \longrightarrow G$ que satisface las siguientes propiedades o axiomas: $\forall a, b, c \in G$

$$\begin{aligned} \alpha\left(a, \alpha(b,c)\right) &= \alpha\left(\alpha(a,b), c\right) && \text{es asociativa} \\ \exists u \in G : ua &= a = au && \text{existe un neutro o unidad} \\ \exists a' \in G : aa' &= u = a'a && \text{existen inversos.} \end{aligned}$$

Es común que esta operación se denote de diversas maneras según sea el caso, por ejemplo $\alpha(a,b) = a + b$, ab, o $a \cdot b$. Como vemos es posible sólo yuxtaponer el par de elementos en cuestión. Debido a esta notación se le suele llamar grupo aditivo o multiplicativo según el caso. Cuando además la operación es conmutativa, i. e., cumple que $\forall a, b \in G$: $\alpha(a,b) = \alpha(b,a)$ decimos que el grupo es **conmutativo** o abeliano. Un subconjunto $H \subseteq G$ de un grupo es un **subgrupo** cuando $u \in H$ y es un grupo con la restricción de la operación binaria a éste. Decimos que un subgrupo $H \subseteq G$ es **generado** por un conjunto de elementos $X \subseteq G$ cuando H es un mínimo subgrupo de G que contiene a X (considerando el orden de la contención $\subseteq$), esto quiere decir que cualquier elemento de H puede expresarse como una combinación de elementos hecha al aplicar la operación binaria a una cantidad finita de elementos de X, incluyendo sus inversos; por ejemplo si $X = \{x_1, ..., x_n\}$ y consideramos la operación con la notación de producto, bien puede pasar que cierta $h \in H$ puede expresarse como $x_1^3 x_3 x_2^{-1}$. Sobre la notación, que H sea generado por X lo denotamos $H = \langle X \rangle$.

Un par de propiedades que se siguen de inmediato de estos tres axiomas es que el neutro u (también denotado como 0 o 1 según se denote la operación con el símbolo de suma o multiplicación respectivamente) es el único elemento que puede cumplir dicha propiedad en el grupo, y así también para cada $a \in G$ su inverso es único, por lo cual le suele dar nombre: $-a$ o a^{-1} (según se denote la operación como suma o multiplicación). Entonces, una manera de referirnos a un grupo sería indicando su operación y neutro: Por ejemplo $(\mathbb{Z}, +, 0)$, y como pragmatismo simplemente $\mathbb{Z}$ cuando por el contexto sea claro si nos referimos al conjunto o al conjunto y su estructura algebraica.

Cuando tratamos con grupos y funciones entre éstos, resultan útiles aquellas que preserven o respeten la estructura u operaciones. Consideremos dos grupos $(G, +, 0)$ y $(H, \cdot, 1)$, y una función $f : G \longrightarrow H$, ésta preserva las operación de grupo si $f(g_1 + g_2) = f(g_1) \cdot f(g_2)$, preserva neutro si $f(0) = 1$ y preserva inversos si $f(-a) = \big(f(a)\big)^{-1}$. Es interesante que al estar relacionadas las propiedades de neutro e inverso con la operación del grupo, una función que preserve la operación de grupo inmediatamente satisface las otras dos como podemos comprobar:

Como 0 es neutro en G sabemos que $0 + 0 = 0$, y al preservar f la operación de grupo y al ser 1 el neutro de H tenemos que $f(0) \cdot f(0) = f(0) \cdot 1$ pues $f(0) \cdot f(0) = f(0 + 0) = f(0) = f(0) \cdot 1$. Por otro lado, como $f(0) \in H$, existe su inverso, así, por la asociatividad de la operación en H se cumple que $f(0) = 1 \cdot f(0) = \Big((f(0))^{-1} \cdot f(0)\Big) \cdot f(0) = (f(0))^{-1} \cdot \big(f(0) \cdot f(0)\big) = (f(0))^{-1} \cdot \big(f(0) \cdot 1\big) = \Big((f(0))^{-1} \cdot f(0)\Big) \cdot 1 = 1 \cdot 1 = 1$ (que no es más que la ley de cancelación izquierda), así $f(0) = 1$. Ahora, sabemos que en G, $a + (-a) = 0$, así tenemos que $f(a) \cdot f(-a) = f(a + (-a)) = f(0) = 1$, y por la ley de cancelación izquierda tenemos $f(-a) = (f(a))^{-1}$.

Esto motiva la definición siguiente: Un **morfismo de grupos** es una función entre dos grupos que preserva la operación de grupo; un ejemplo que no puede faltar es el de la función identidad $id_G : G \longrightarrow G$ que claramente lo es. Un morfismo de grupos $f : G \longrightarrow H$ es un **isomorfismo** cuando existe un morfismo inverso para éste, esto es un morfismo de grupos $k : H \longrightarrow G$ tal que $k \circ f = id_G$ y $f \circ k = id_H$.

Un grupo cualquiera $(G, +, 0)$ también cumple la ley de cancelación derecha y las siguientes propiedades:

$$-0 = 0, \qquad -(-a) = a, \qquad -(a + b) = (-a) + (-b).$$

Dado un grupo $(G, \cdot, 1)$ no es necesario que nos limitemos a estudiar cómo actúa la operación en el conjunto G, también podemos hacer «actuar» a G sobre un conjunto X, definimos la **acción** como una función $a : G \times X \longrightarrow X$ tal que:

$$a(1, x) = x, \qquad a(g_1 \cdot g_2, x) = a\left(g_1, a(g_2, x)\right),$$

es decir, la función toma en cuenta el neutro y la operación del grupo. Pasemos ahora a conjuntos con dos operaciones binarias.

Un **anillo** $(R, +, \cdot, 0)$ es un conjunto R con dos operaciones binarias, $+$ y $\cdot$, tales que:

$$(R, +, 0) \quad \text{es un grupo conmutativo, y}$$

$$\forall a, b, c \in R, \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{y} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Las últimas dos igualdades son llamadas leyes distributivas derecha e izquierda, respectivamente, y para hacer más ligera la notación se suelen denotar

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ y} \quad (a + b) \cdot c = a \cdot c + b \cdot c,$$

algo que se suele llamar «ponderar las operaciones», primero se aplica el producto y luego la suma. Estas propiedades de distributividad son las que hacen que estén relacionadas ambas operaciones del anillo.

La operación $\cdot$ puede ser asociativa, conmutativa o ambas, en cada caso decimos que el anillo es *asociativo* o *conmutativo*; también puede existir un *neutro* (o *unidad*) para esta operación, lo podemos denotar como 1 y decimos que el anillo es *unital* y podemos denotarlo como $(R, +, \cdot, 0, 1)$. Es común que se tome como definición de anillo a lo que nosotros llamamos anillo asociativo unital, pero aquí preferimos no requerir propiedades adicionales a la segunda operación, salvo la interacción con la primera: las leyes distributivas. Hasta aquí nada evita que podamos tener que $0 = 1$, lo cual puede ocurrir y tendríamos lo que llamamos un anillo trivial, que es un conjunto con un solo elemento; más frecuentemente trataremos con anillos no triviales.

Los anillos presentan propiedades interesantes que tienen lugar debido a la interacción de las dos operaciones:

$$\forall a \in R : a \cdot 0 = 0 = 0 \cdot a$$

$$\forall a, b \in R : (-a) \cdot b = -(a \cdot b) = a(-b) \qquad \text{leyes de los signos.}$$

Un **morfismo de anillos** es una función que preserva las dos operaciones binarias, y en el caso de anillos unitarios que preserve el neutro del producto. Un isomorfismo es un morfismo que tiene morfismo inverso.

La **característica** de un anillo asociativo unital $(R, +, \cdot, 0, 1)$, denotada $car(R)$ es el *orden* de su unidad, esto es el mínimo número natural n tal que sumando 1 n veces da 0: $1 + ... + 1 = 0$, si no existe tal número decimos que su orden es ∞ (o 0 según gustos).

Ahora algunas estructuras algebraicas relacionadas, aquí estaremos requiriendo que el anillo sea asociativo para hacer más sencillas las definiciones. En un anillo R, dos elementos $a \neq 0$ y $b \neq 0$ se dice que son **divisores de cero** si $a \cdot b = 0 = b \cdot a$. Un *dominio entero* es un anillo asociativo unitario no trivial conmutativo sin divisores de cero. Una equivalencia de que un anillo asociativo unitario no trivial conmutativo K no tenga divisores de cero es que cumpla la ley de cancelación: $\forall a, b, c \in K: \quad a \cdot b = a \cdot c$ y $a \neq 0$, implican que $b = c$.

Un **anillo con división** es un anillo asociativo unital $(R, +, \cdot, 0, 1)$ en el que cada elemento $r \in R - \{0\}$ tiene inverso para la operación $\cdot$, i. e. existe r^{-1}. Esta propiedad aunada a la conmutatividad del producto implican la ley de cancelación y así todo anillo con división conmutativo es un dominio entero, y un **campo** es un anillo con división conmutativo.

Dado un anillo asociativo unitario R, un R**-módulo** o módulo sobre R es un grupo conmutativo M con una función $R \times M \longrightarrow M$, denotada yuxtaponiendo pares: $(\lambda, a) \mapsto \lambda a$, que es una acción del anillo sobre el grupo, esto es, cumple, $\forall \kappa, \lambda \in R$ y $\forall a, b \in M$:

$$\begin{aligned} \lambda(a+b) &= \lambda a + \lambda b && \text{distributividad sobre la operación del grupo} \\ (\kappa+\lambda)a &= \kappa a + \lambda a && \text{distributividad sobre la suma de escalares} \\ (\kappa\lambda)a &= \kappa(\lambda a) && \text{asociatividad de la acción por escalares} \\ 1a &= a && \text{acción neutral del neutro multiplicativo.} \end{aligned}$$

De las primeras dos propiedades se sigue que fijando $\lambda \in R$ y $a \in M$, se tiene las restricciones $M \cong \{\lambda\} \times M \longrightarrow M$ y $R \cong R \times \{a\} \longrightarrow M$ preservan la suma (son morfismos aditivos), y al ser las sumas respectivas parte de un grupo, esto implica que también preservan neutros e inversos de dicha operación: $\lambda 0 = 0$, $\lambda(-a) = -(\lambda a)$, y $0a = 0$, $(-\lambda)a = -(\lambda a)$.

A los elementos de M les llamamos *vectores*, y a los de R, *escalares*. De acuerdo a la notación que se use, puede que el neutro aditivo de R y el de M los denotemos ambos mediante 0, con lo cual el contexto despejará ambigüedades, si se refiere a un vector o un escalar.

Un **morfismo de** R**-módulos** es una función $f: M \longrightarrow N$ que preserva sumas y escalares:

$$f(a+b) = f(a) + f(b), \qquad f(\lambda a) = \lambda f(a).$$

Son conocidos comúnmente como transformaciones R-lineales. Dichos requerimientos equivalen al requerimiento que $\forall a, b \in M \ \forall \lambda \in R: f(\lambda a + b) = \lambda f(a) + f(b)$. Como cabe esperar, un isomorfismo es un morfismo para el cual existe un morfismo inverso. Cabe mencionar que además de la coherencia de tratar con funciones que respeten las estructuras algebraicas en cuestión, esto nos permite situar nuestra presentación en el contexto de la teoría de categorías.

B

ÁLGEBRA LINEAL Y GRUPOS DE MORFISMOS CLÁSICOS

Siguiendo la tónica del apéndice anterior aquí recordamos las definiciones concernientes a esta importante rama de la matemática: el álgebra lineal. Para esto nos inspiramos en Mac Lane y Birkhoff (1999) y para algunos detalles en Lluis-Puebla (2008), en ambos pueden consultarse los resultados «clásicos» de esta área. Un $\mathbb{K}$**-espacio vectorial** es un $\mathbb{K}$-módulo, siendo $\mathbb{K}$ un campo. Un $\mathbb{K}$-**subespacio vectorial** de un $\mathbb{K}$-espacio vectorial V es un subconjunto U tal que al considerar las restricciones de la suma y la acción por escalares (sobre todo $\mathbb{K}$) de V en U, resulta que U es un $\mathbb{K}$-espacio vectorial. Podemos definir el **espacio vectorial producto** finito de espacios vectoriales $\{V_i : i \in \{1, ..., r\}\}$, con $r \in \mathbb{N}^+$ y $r > 1$, como el producto cartesiano $\Pi_{i=1}^r V_i$ con las operaciones definidas coordenada a coordenada; la notación $V_1 \times ... \times V_r$ también es usual, y para un mismo espacio $V^r = V \times ... \times V$. Dado un espacio vectorial V y un conjunto de subespacios vectoriales de este, $\{U_i \subset V : i \in \{1, ..., r\}\}$, definimos el **espacio vectorial suma** de estos como

$$\textstyle\sum_{i=1}^r U_i = \{v \in V : \exists u_1 \in U_1, ..., \exists u_r \in U_r (v = \sum_{i=1}^r u_i)\} \subseteq V$$

con las restricciones de las operaciones de V; la notación $V_1 + ... + V_r$ también es usual; cuando la expresión es única, es decir, para cada $v \in \sum_{i=1}^r U_i$, existen únicos $u_i \in U_i$ tales que $v = \sum_{i=1}^r u_i$, se dice que se tiene una **suma directa**, denotada $U_1 \oplus ... \oplus U_r$, esto equivale a que para todo $s \in \{2, 3, ..., r\}$, se cumpla que $\bigcap_{i=1}^s U_i = \{0\}$. Los **morfismos de espacios vectoriales** son las transformaciones $\mathbb{K}$-lineales; una función m-lineal ($m \in \mathbb{N}^+$), es una función $\Pi_{i=1}^m V_i \longrightarrow W$ entre un producto de espacios y un espacio que es lineal en cada entrada: hay **bilineales, trilineales**, etcétera. *Nota*: Todas estas definiciones tienen su versión para cardinalidad arbitraria, pero nos basta el caso finito. Más definiciones: sea V un $\mathbb{K}$-espacio vectorial y un conjunto finito de vectores $X = \{v_1, ..., v_n\} \subset V$, decimos que a un subespacio U de V es **generado** por X cuando cada vector $u \in U$ se puede expresar como una combinación lineal de los vectores en dicho conjunto: $u = \lambda_1 v_1 + ... + \lambda_n v_n$, con ciertos $\lambda_1, ..., \lambda_n \in \mathbb{K}$ (otra manera de decir esto es que X genera el espacio vectorial U); el conjunto es **linealmente independiente** cuando cada vector del espacio generado por este conjunto se expresa como una *única* combinación lineal de los elementos de éste, lo cual equivale a que para cada colección $\lambda_1, ..., \lambda_n \in \mathbb{K}$, si $\lambda_1 v_1 + ... + \lambda_n v_n = 0$, entonces $\lambda_1 = ... = \lambda_n = 0$. Una **base** de un espacio vectorial es un conjunto de vectores que genera al espacio y es linealmente independiente. Todo espacio vectorial tiene al menos una base. La **dimensión** de un espacio vectorial V es la cardinalidad de alguna base de dicho espacio; la dimensión es un invariante, en el sentido de que cualquier otra base del espacio vectorial dado tiene la misma cardinalidad, la denotamos como $\dim(V)$. Para el caso de dimensión finita tenemos que si $\dim(V) = n$, entonces $V \cong \mathbb{K}^n$; así tenemos la base *canónica* $\{e_i = (0, ..., 1, ..., 0)\}$, siendo cada e_i una n-ada con ceros en todas sus coordenadas, excepto en la i-ésima, la cual es 1.

El estudio de las funciones lineales va de la mano con el de las matrices: dados dos $\mathbb{K}$-espacios vectoriales U y V, siendo $\dim(U) = m$, $\dim(V) = n \in \mathbb{N}^+$ y considerando bases respectivamente $\{u_1, ..., u_m\} \subset U$ y $\{v_1, ..., v_n\} \subset V$, podemos asociar a una función $\mathbb{K}$-lineal $t : U \longrightarrow V$, una matriz $T \in M_{n\times m}(\mathbb{K})$ con respecto a dichas bases, a saber, cada $t(u_i) = \sum_{j=1}^{n} a_{ij} v_j$ para ciertos $a_{ij} \in \mathbb{K}$, así tomamos $T = (a_{ij})$; con esto la función puede expresarse como $t(u) = Tu$, considerando al vector u como una matriz $m \times 1$ columna. Con esto también resulta evidente que las matrices pueden servirnos para difinir funciones lineales.

Las matrices también nos dan otra perspectiva para las formas bilineales. Sea V un $\mathbb{K}$-espacio vectorial, $\{b_1, ..., b_n\}$ una base para aquel, y $\alpha : V \times V \longrightarrow \mathbb{K}$ una forma bilineal. (Aquí seguimos a Artin (1957)) Notamos que los n^2 valores que toma la forma bilineal para los básicos $\alpha(b_i, b_j) = a_{ij} \in \mathbb{K}$, $1 \leq i, j \leq n$, definen todos los valores de la forma bilineal, pues para $u = \sum_{i=1}^{n} u_i b_i$, $v = \sum_{j=1}^{n} v_j b_j \in V$ ($u_i, v_j \in \mathbb{K}$), por la bilinealidad tenemos que

$$\alpha(u, v) = \sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j \alpha(b_i, b_j) = \sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j a_{ij}.$$

Así, definimos la matriz A cuyas entradas son a_{ij}, siendo i la posición en las filas y j en las columnas. Por otro lado, los vectores $v \in V$ son matrices de $1 \times n$, entonces podemos expresar la forma bilineal como el producto de matrices

$$\alpha(u, v) = u^t A v,$$

donde u^t es el transpuesto de u: $(u^t)_{ij} = u_{ji}$. Ahora, consideremos otro espacio vectorial W con una forma bilineal que denotamos β, y consideremos una isometría entre estos $h : V \longrightarrow W$ y la matriz, H, asociada a ésta con respecto a ciertas bases de V y W y también consideremos las matrices asociadas a las formas bilineales con respecto a esas mismas bases para

V y W, digamos A y B, respectivamente, entonces la condición de ser isometría implica que

$$u^t H^t B H v = (Hu)^t B (Hv) = (h(u), h(v))_W = (u, v) = u^t A v,$$

es decir, $H^t B H = A$; y para el caso de isometrías sobre el mismo espacio $V \longrightarrow V$, tenemos que $H^t A H = A$ (que es la relación de cambio de bases, pues un isomorfismo $V \longrightarrow V$ no es más que un cambio de base). Hasta aquí nada nos asegura que $\alpha(u, v) = u^t A v = 0$ implique que $\alpha(v, u) = v^t A u = 0$, esto no impide definir una noción de ortogonalidad «homogénea», para solucionarlo tenemos dos opciones: i) Definir una geometría simpléctica: asumir que para todo $u \in V$ se tiene que $\alpha(u, u) = 0$ y por tanto $\alpha(u, v) = -\alpha(v, u)$, en particular $\alpha(u, v) = 0$ implica que $\alpha(v, u) = -0 = 0$; o ii) Definir una geometría ortogonal: asumir que $\alpha(u, v) = \alpha(v, u)$, i. e. que es una forma simétrica. El mismo nombre ya nos adelantó lo que vamos a definir a continuación, asumiendo que α es simétrica, definimos el **grupo ortogonal generalizado** como

$$O(V, \alpha) = \{H \in M_{n\times n}(\mathbb{K}) : H^t A H = A\},$$

mismo que representa a las isometrías $V \longrightarrow V$ y justifica el nombre, pues éstas preservan la ortogonalidad definida mediante la forma bilineal $(u, v) = 0$; es también el grupo de simetrías que define la «geometría» del espacio, y decimos que es un grupo porque en efecto lo es considerando la composición, o en este caso, el producto de matrices como operación de grupo y matriz identidad el neutro. Cabe mencionar que en vez de partir de una forma bilineal simétrica podemos partir de una forma cuadrática $q : V \longrightarrow V$, considerar su forma bilineal asociada $(,)_q$ y usar esta última; ambos enfoques coinciden cuando $car(\mathbb{K}) \neq 2$. Notemos que la relación $H^t A H = A$ implica que

$$\begin{aligned}\det(A) &= det(H^t A H = A)\\ &= \det(H^t)\det(A)\det(H)\\ &= \det(H)\det(A)\det(H) = \det(H)^2\det(A),\end{aligned}$$

es decir, $\det(H) = \pm 1$, entonces podemos definir el **grupo ortogonal especial generalizado** como

$$SO(V, \alpha) = \{H \in M_{n\times n}(\mathbb{K}) : H^t A H = A \text{ y } \det(H) = 1\},$$

que representa a las isometrías que preservan la «orientación»; también llamado grupo de rotaciones generalizadas, pues para los casos $n = 2, 3$ corresponde a las isometrías que podemos considerar como rotaciones comunes. Hemos usado el adjetivo «generalizado» pues estas definiciones se hicieron considerando espacios sobre $\mathbb{R}$ con el producto interno estándar siendo la forma bilineal simétrica, para la cual su matriz asociada a la base canónica es la matriz identidad I_n; siendo $\dim(V) = n$, en este caso tenemos que $H^t H = H^t I_n H = I_n$ (lo cual sirve para definir a una matriz ortogonal, como aquella que cumple dicha relación), entonces tenemos los grupos clásicos:

$$O(n) = \{H \in M_{n\times n}(\mathbb{R}) : H^t H = I_n\},$$

$$SO(n) = \{H \in M_{n\times n}(\mathbb{R}) : H^t H = I_n \text{ y } \det(H) = 1\}.$$

Finalmente, podemos consideramos espacios vectoriales sobre $\mathbb{C}$ con el producto interior estándar para estos, que es una forma sesquilineal (en vez de bilineal, lineal en la primera entrada y lineal conjuga en la segunda: $f(\kappa_1 a + \kappa_2 b) = \kappa_1 f(a) + \kappa_2^* f(b)$, para $\kappa_1, \kappa_2 \in \mathbb{C}$), definida positiva. Los correspondientes grupos de matrices son llamados **grupos unitarios** y para definirlos se requiere la noción correspondiente: una matriz $M \in M_{n\times n}(\mathbb{C})$ es unitaria cuando $M^{*t} M = I_n \in M_{n\times n}(\mathbb{C})$, donde M^{*t} es la matriz conjugada transpuesta que involucra a la involución (también llamada conjugación compleja), siendo $(M^{*t})_{ij} = M^*_{ji}$.

$$U(n) = \{H \in M_{n\times n}(\mathbb{C}) : H^{*t} H = I_n\},$$

$$SU(n) = \{H \in M_{n\times n}(\mathbb{C}) : H^{*t} H = I_n \text{ y } \det(H) = 1\}.$$

REFERENCIAS

Artin, E. (1957). *Geometric Algebra*. Interscience Tracts in Pure and Applied Mathematics. John Wiley & Sons.

Baez, J. (2002). The octonions. *Bulletin of the American Mathematical Society*, 39(2):145–205.

Davidson, K. R. (1996). *C*-Algebras by Example*, volume 6 of *Fields Institute Monographs*. American Mathematical Society.

Dickson, L. E. (1919). On quaternions and their generalization and the history of the eight square theorem. *Annals of Mathematics*, 20(3):155–171.

Dray, T. y Manogue, C. A. (2015). *The Geometry of the Octonions*. World Scientific.

Grove, L. C. (2002). *Classical Groups and Geometric Algebra*, volume 39 of *Graduate Studies in Mathematics*. American Mathematical Society.

Harkin, A. A. y Harkin, J. B. (2004). Geometry of generalized complex numbers. *Mathematics magazine*, 77(2):118–129.

Khalkhali, M. (2013). *Basic Noncommutative Geometry*. EMS Series of Lectures in Mathematics. European Mathematical Society, (2 ed.) edition.

Lam, T.-Y. (2005). *Introduction to Quadratic Forms over Fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society.

Lluis-Puebla, E. (2008). *Algebra Lineal: Álgebra Multilineal y K-teoría Algebraica Clásica*. Publicaciones electrónicas. Sociedad Matemática Mexicana, (2 ed.) edition.

Lounesto, P. (2001). *Clifford Algebras and Spinors*, volume 286 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, (2 ed.) edition.

Mac Lane, S. y Birkhoff, G. (1999). *Algebra*, volume 330 of *Chelsea Publishing Series*. American Mathematical Society, (3 ed.) edition.

Manogue, C. A. y Schray, J. (1993). Finite lorentz transformations, automorphisms, and division algebras. *Journal of Mathematical Physics*, 34(8):3746–3767.

Moskowitz, M. A. (2002). *A Course in Complex Analysis in One Variable*. World Scientific.

Moufang, R. (1935). Zur struktur von alternativkörpern. *Mathematische Annalen*, 110(1):416–430.

Pujol, J. (2012). Hamilton, rodrigues, gauss, quaternions, and rotations: a historical reassessment. *Communications in Mathematical Analysis*, 13(2):1–14.

Ramírez-Galarza, A. I. y Seade-Kuri, J. (2002). *Introducción a la Geometría Avanzada*. Las Prensas de Ciencias.

Schafer, R. D. (1966). *An Introduction to Nonassociative Algebras*. Pure and Applied Mathematics. Academic Press.

Voight, J. (2021). *Quaternion Algebras*, volume 288 of *Graduate Text in Mathematics*. Springer.

Yaglom, I. M. (1968). *Complex Numbers in Geometry*. Academic Press.