Sección de Matemáticas
Universidad de La Laguna

Raquel Tapia Ramos

El anillo de Hamilton

The Hamilton ring

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, junio de 2022

Dirigido por
Evelia Rosa García Barroso

Evelia Rosa García Barroso
Departamento Matemáticas,
Estadística e Investigación
Operativa.
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A mi hermana Gara por jugar en silencio para que yo me concentrase.

A mis padres por estar siempre ahí.

A Evelia García, matemática a quien admirar y tener como referente.

A mis amigos encargados de duplicar alegrías y dividir penas.

Por último, se lo agradezco al tiempo que ha dado dulces salidas a amargas dificultades.

Raquel Tapia Ramos
La Laguna, 13 de junio de 2022

Resumen · Abstract

Resumen

Esta memoria consta de tres objetivos. El primero es la resolución de ecuaciones y sistemas de ecuaciones lineales de dos incógnitas. El segundo es la demostración del Teorema de los cuatro cuadrados de Lagrange, el cual establece que cualquier entero no negativo puede expresarse como suma de cuatro cuadrados; y en el tercero abordaremos la teoría de la factorización en irreducibles en los cuaterniones de Hurwitz.

En primera instancia, presentamos el anillo de Hamilton y ciertas propiedades con las que construiremos las pruebas de nuestros resultados principales. Posteriormente estudiamos el subanillo de los enteros de Hurwitz donde mostramos la existencia del algoritmo de división unilateral. También caracterizamos los elementos irreducibles en el anillo de Hurwitz lo que nos permitirá obtener una factorización única salvo unidades migratorias, metaconmutaciones y recombinaciones.

Palabras clave: *Anillo de Hamilton – Ecuación cuaterniónica – Cuaternión de Hurwitz y cuaternión Lipschitz –Teorema de los cuatro cuadrados de Lagrange – Factorización única en irreducibles.*

Abstract

This essay consists of three objetives. The first one is to solve quaternionic equations and linear quaternionic systems with two addends. The second one is to proof of Lagrange's Theorem of Four Squares, which establishes that any non-negative integer can be written as a sum of four squares. The third objetive covers the theory of the factorization into irreducible of the Hurwitz quaternions.
To do so, we introduce certain properties of the Hamilton ring, with which we will construct the proofs of our main results. Next, we study the subring of the Hurwitz integers in which we show the existence of one-sided division algorithm. We also characterize the irreducible elements in the Hurwitz ring which will allow us to obtain a unique factorization except for unit-migrations, metacommutations and recombinations.

Keywords: *Hamilton ring – Quaternion ecuation – Hurwitz quaternion and Lipschitz quaternion– Lagrange's theorem of four squares – Unique factorization into irreducible elements.*

Contenido

Introducción

Intuitivamente podemos pensar en el anillo de Hamilton como una extensión de los números complejos agregando 2 nuevas dimensiones. Etimológicamente la palabra cuaternión proviene del latín "quaterni"que se traduce como número de cuatro partes, hoy en día a los elementos del anillo de Hamilton se les conoce por cuaterniones. William R. Hamilton buscaba describir el espacio (tres dimensiones) en 1843 según explicó a John Craves. Dando un paseo por el puente de Brougham (Dublín) se dió cuenta que para extender los complejos del plano al espacio iba a necesitar añadir dos nuevas dimensiones, pues si incorporaba una nueva dimensión $\mathbf{j}$, tendría que incluir el producto $\mathbf{ij} = \mathbf{k}$. Grabó una inscripción con esta idea, hoy en día no se encuentra, pero la *Royal Irish Academy* erigió una placa conmemorativa en su lugar.

Sin embargo, debido a la naturaleza no conmutativa de los cuaterniones resultó más práctico y sencillo el uso de los vectores para describir el espacio físico. Aún así, los cuaterniones siempre han tenido sus defensores. James Clerk Maxwell formuló la Teoría clásica de la radiación electromagnética en notación cuaterniónica. También se han aplicado a la Teoría de la relatividad, la Cristalografía y la Mecánica cuántica del s. XX al describir el movimiento del spin de un electrón.

Los cuaterniones resultan muy útiles en la tecnología. Concretamente en la rotación y orientación de objetos, se han implantado desde Hollywood hasta la Nasa. En el cine se utilizan para describir la secuencia de movimientos y giros que debe realizar una cámara al grabar, por ejemplo se han utilizando en las películas de "Toy Story". Los astronautas monotorizan y controlan las posiciones de sus naves a través de los cuaterniones.
También se han incorporado en la navegación y en la dinámica de vuelos, las historias sobre el desarrollo del avión de combate F-16 cuentan que en una de la simulaciones de vuelo al atravesar el ecuador el F-16 reorientó la cabina. Usando programación cuaterniónica se dió solución a dicho desafío. Recientemente se

han incluido en la programación del Satélite Sentinel. En definitiva, para afrontar una cuestión de orientación 3D a día de hoy resulta más eficaz y eficiente apostar por métodos basados en cuaterniones.

Hoy en día los cuaterniones adquieren mucha relevancia en la informática por las ventajas computacionales que ofrecen, concretamente en robótica al secuenciar los movimientos que debe de realizar el brazo del robot. Además, el desarrollo de los drones está provocando que los cuaterniones obtengan más notoriedad y se inviertan recursos económicos en perfeccionar dichas herramientas. También destacamos que están presentes en los videojuegos y en los gráficos de computadora. Para conocer desde un punto de vista geométrico el plegamiento y disposición de las proteínas se utiliza software programado en notación cuaterniónica.

Los cuaterniones están más vivos que nunca pese a que ha transcurrido más de un siglo desde que Hamilton los formuló formalmente. Podemos encontrar estas aplicaciones y muchas más en [4].

Motivados por las numerosas aplicaciones que nos ofrecen los cuaterniones dedicamos esta memoria a comprender las matemáticas que hay detrás de los mismos.

1

Anillo de los cuaterniones de Hamilton

Comenzamos esta sección recogiendo la definición de cuaternión y algunas propiedades que verifican los elementos del anillo de los cuaterniones también conocido como el anillo de Hamilton. Además presentamos las distintas estructuras que se le pueden asociar a dicho anillo.

Definición 1.1. *Consideramos las siguientes matrices de* $\mathcal{M}_2(\mathbb{C})$

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad \text{donde } i = \sqrt{-1}.$$

Diremos que q *es un cuaternión o cuaternio si* $q = a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, *con* $a_i \in \mathbb{R}$, *para* $i \in \{0, 1, 2, 3\}$.

Denotaremos $\mathbb{H}$ al conjunto de los cuaterniones de Hamilton. La parte real o escalar de $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H}$ es $\Re(q) := a_0$ y la parte vectorial de q $\Im(q) := a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$.
Designamos por $\mathbb{H}_0$ al subconjunto de $\mathbb{H}$ formado por los cuaterniones con parte real nula. Luego, podemos escribir un cuaternión $q = a+v,\ a = \Re(q)$ y $v \in \mathbb{H}_0$.

El conjunto $\mathbb{H}$ es un subanillo de las matrices cuadradas de orden 2 con coeficiente en $\mathbb{C}$, con las operaciones $(+, \cdot)$ definidas en $\mathcal{M}_2(\mathbb{C})$. Observamos que

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1.$$

Las igualdades anteriores son conocidas como las reglas de Hamilton. Las mismas nos llevan a considerar la Tabla 1.1.

Lema 1.2. *Sean* $q = a_0+a_1\mathbf{i}+a_2\mathbf{j}+a_3\mathbf{k}, p = b_0+b_1\mathbf{i}+b_2\mathbf{j}+b_3\mathbf{k} \in \mathbb{H}$. *Su producto es*

$$\begin{aligned} qp = \big((a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)\mathbf{i} \\ +(a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3)\mathbf{j} + (a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1)\mathbf{k}\big). \end{aligned}$$

Demostración. Consecuencia inmediata de la Tabla 1.1.

$\cdot$	$b_0\mathbf{1}$	$b_1\mathbf{i}$	$b_2\mathbf{j}$	$b_3\mathbf{k}$
$a_0\mathbf{1}$	$a_0b_0\mathbf{1}$	$a_0b_1\mathbf{i}$	$a_0b_2\mathbf{j}$	$a_0b_3\mathbf{k}$
$a_1\mathbf{i}$	$a_1b_0\mathbf{i}$	$-a_1b_1\mathbf{1}$	$a_1b_2\mathbf{k}$	$-a_1b_3\mathbf{j}$
$a_2\mathbf{j}$	$a_2b_0\mathbf{j}$	$-a_2b_1\mathbf{k}$	$-a_2b_2\mathbf{1}$	$a_2b_3\mathbf{i}$
$a_3\mathbf{k}$	$a_3b_0\mathbf{k}$	$a_3b_1\mathbf{j}$	$-a_3b_2\mathbf{i}$	$-a_3b_3\mathbf{1}$

Tabla 1.1. Tabla producto.

De la Tabla 1.1 concluimos que el anillo $\mathbb{H}$ no es conmutativo ya que $\mathbf{ij} = \mathbf{k} \neq -\mathbf{k} = \mathbf{ji}$ pero es unitario pues $1 \in \mathbb{H}$. También deducimos que $\mathbb{H}$ no tiene divisores de cero, es decir, no existen $q, p \in \mathbb{H}$ no nulos tales que $qp = 0$ ó $pq = 0$. Comprobémoslo por reducción al absurdo.
Supongamos que existen $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, $p = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k} \in \mathbb{H}$ no nulos tales que $qp = 0$. Desarrollando el producto con el Lema 1.2 e igualando componente a componente se sigue que:

$$\begin{cases} a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 = 0 \\ a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 = 0 \\ a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3 = 0 \\ a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1 = 0. \end{cases}$$

Resolviendo el sistema llegamos a que a_l ó b_l es nulo para todo $l \in \{0, \ldots, 3\}$, lo cual es falso por hipótesis.
Además observamos que $q^{-1} = -q$ con $q \in \{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Para poder calcular el inverso para cualquier cuaternión necesitamos introducir el concepto de conjugado.

Definición 1.3. *Llamaremos conjugado de* $q \in \mathbb{H}$ *a* $\overline{q} = a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k} \in \mathbb{H}$.

Por tanto $q\overline{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2 = |q|^2$ donde $|\cdot|$ es la norma euclídea en $\mathbb{R}^4$, para todo $q \in \mathbb{H}$, (donde identificamos q con el vector (a_0, a_1, a_2, a_3)).

Lema 1.4. *Sea* $q \in \mathbb{H}$ *no nulo. Su inverso es* $q^{-1} = \frac{\bar{q}}{|q|^2}$.

Demostración. Por propiedades de la norma si $q \neq 0$ entonces $|q| \neq 0$. Además,

$$q\frac{\overline{q}}{|q|^2} = \frac{q\overline{q}}{|q|^2} = 1 \quad \text{y} \quad \frac{\overline{q}}{|q|^2}q = \frac{\overline{q}q}{|q|^2} = 1. \qquad \square$$

Seguidamente recogemos unas propiedades sobre el conjugado, donde las demostraciones se concluyen de aplicar la Definición 1.3.

Propiedades 1.1 *Sean* $q_1, q_2 \in \mathbb{H}$, *tenemos que*

1. $\overline{q_1q_2} = \overline{q_2}\ \overline{q_1}$,
2. $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$,
3. *Si* $q_1 \in \mathbb{R}$ *entonces* $q_1 = \overline{q_1}$.

Proposición 1.5. *Si* $q \in \mathbb{H}$ *es raíz de* $f(\xi) = \sum_{l=0}^{n} a_l \xi^l \in \mathbb{R}[\xi]$ *entonces* $f(\overline{q}) = 0$.

Demostración. Por hipótesis $f(q) = \sum_{l=0}^{n} a_l q^l = 0$. Tomando conjugados en ambos lados de la igualdad $\overline{\sum_{l=0}^{n} a_l q^l} = \overline{0}$. Aplicando Propiedades 1.1

$$0 = \overline{0} = \overline{\sum_{l=0}^{n} a_l q^l} = \sum_{l=0}^{n} \overline{a_l q^l} = \sum_{l=0}^{n} \overline{a_l}\ \overline{q}^l = \sum_{l=0}^{n} a_l \overline{q}^l = f(\overline{q}). \qquad \square$$

Proposición 1.6. *Todo cuaternión* $q \in \mathbb{H}$ *y su conjugado* $\bar{q}$ *son raíces del polinomio* $d_q(\xi) = \xi^2 - 2\Re(q)\xi + |q|^2 \in \mathbb{R}[\xi]$. *Si* $\Re(q) \neq 0$ *entonces* $d_q(\xi)$ *divide a cualquier otro polinomio con coeficientes reales de grado mayor o igual que él y que tenga a* q *como raíz.*

Demostración. Sean $q \in \mathbb{H}$ y la aplicación que evalúa en q todos los polinomios $\mathbb{R}[\xi]$, es decir

$$\begin{aligned} \varphi : \mathbb{R}[\xi] &\longrightarrow \mathbb{H} \\ f(\xi) &\longrightarrow f(q). \end{aligned}$$

Observamos que φ es homomorfismo de anillos.
Además su núcleo es $\mathrm{Ker}\varphi = \{f(\xi) \in \mathbb{R}[\xi] : f(q) = 0\}$. Veamos que coincide con el ideal de $\mathbb{R}[\xi]$ generado por $f(\xi)$, que denotaremos por $d_q(\xi)$.

Sea $s(\xi) = g(\xi)d_q(\xi) \in \big(d_q(\xi)\big)$, evaluando en q obtenemos que $s(q) = 0$, por lo tanto $s(\xi) \in \mathrm{Ker}\varphi$.

Para la otra inclusión, sea $f(\xi) \in \mathrm{Ker}\varphi$. Como $\mathbb{R}[\xi]$ es un dominio euclídeo dividimos $f(\xi)$ entre $d_q(\xi)$ esto es, existen unos únicos $s(\xi), r(\xi) \in \mathbb{R}[\xi]$ tales que $f(\xi) = s(\xi)d_q(\xi) + r(\xi)$ con $0 \leq \deg\big(r(\xi)\big) < 2$ o $r(\xi) = 0$. Evaluando en q, $0 = f(q) = s(q)d_q(q) + r(q) = r(q)$. Por la Proposición 1.5 sabemos que $r(\overline{q}) = 0$. Se sigue que $r(\xi) = 0$ o $\deg(\big(r(\xi)\big) \geq 2$ lo cual es absurdo. Por tanto, $f(\xi) = s(\xi)d_q(\xi)$ es decir $f(\xi) \in \big(d_q(\xi)\big)$, como queríamos demostrar.

Hemos probado que $\big(d_q(\xi)\big) = \mathrm{Ker}\varphi$. Luego, todo polinomio que tenga a q como raíz estará en el $\mathrm{Ker}\varphi$ y en el ideal generado por $d_q(\xi)$, por la definición de ideal concluimos que será dividido por $d_q(\xi)$. $\square$

Aunque $\mathbb{H}$ no es conmutativo si que podemos relacionar el producto, a derecha e izquierda, de dos cuaterniones con el siguiente lema.

Lema 1.7. *Si* $q, p \in \mathbb{H}$ *entonces* $qp = pq - 2\Im(q)\Im(p) - 2\langle p, q\rangle$, *donde* $\langle \cdot, \cdot \rangle$ *denota el producto escalar euclídeo en* $\mathbb{R}^4$.

Demostración. Sean $q = a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, p = b_0\mathbf{1} + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k} \in \mathbb{H}$.
Por el Lema 1.2 tenemos que

$$qp = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)\mathbf{1} + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)\mathbf{i}$$
$$+(a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3)\mathbf{j} + (a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1)\mathbf{k},$$
y
$$pq = (b_0a_0 - b_1a_1 - b_2a_2 - b_3a_3)\mathbf{1} + (b_0a_1 + b_1a_0 + b_2a_3 - b_3a_2)\mathbf{i}$$
$$+(b_0a_2 + b_2a_0 + b_3a_1 - b_1a_3)\mathbf{j} + (b_0a_3 + b_3a_0 + b_1a_2 - b_2a_1)\mathbf{k}.$$

Además,
$\Im(q)\Im(p) = -(b_1a_1+b_2a_2+b_3a_3)+(b_2a_3-b_3a_2)\mathbf{i}+(-b_1a_3+b_3a_1)\mathbf{j}+(b_1a_2-b_2a_1)\mathbf{k}$.
Luego, $\langle p, q\rangle = b_0a_0 + b_1a_1 + b_2a_2 + b_3a_3$.
Se sigue que $pq = qp - 2\Im(q)\Im(p) - 2\langle q, p\rangle$. □

1.2. Similitud entre dos cuaterniones

En esta sección demostraremos una serie de resultados que utilizaremos frecuentemente en el transcurso de esta memoria.

Definición 1.8. *Diremos que dos cuaterniones q_1, q_2 son similares, y lo denotaremos $q_1 \sim q_2$, si existe $\mu \in \mathbb{H}$ no nulo tal que $q_2 = \mu q_1 \mu^{-1}$.*

Proposición 1.9. *Ser similar es una relación de equivalencia.*

Demostración. Todo elemento está relacionado con el mismo, basta tomar $\mu = 1$.
También se cumple la propiedad simétrica pues si $q_1 \sim q_2$, entonces existe $\mu \in \mathbb{H}$ no nulo tal que $q_2 = \mu q_1 \mu^{-1}$. Multiplicando a la izquierda por μ^{-1} y a la derecha por μ obtenemos que $\mu^{-1}q_2\mu = q_1$ y se sigue que $q_2 \sim q_1$.
Por último, si $q_1 \sim q_2$ y $q_2 \sim q_3$, entonces existen $\mu, w \in \mathbb{H}$ no nulos tales que $q_2 = \mu q_1 \mu^{-1}$ y $q_3 = wq_2w^{-1}$. Sustituyendo esto es, $q_3 = w(\mu q_1 \mu^{-1})$ y por la asociatividad del producto $q_3 = (w\mu)q_1(w^{-1}\mu^{-1})$; por ende, $q_1 \sim q_3$. □

Teorema 1.10. ***(Caracterización de cuaterniones similares)***
Dos cuaterniones q_1 y q_2 son similares si y solo si tienen la misma norma y la misma parte real.

Demostración. Sea $q_1 = a + v$ donde $a = \Re(q)$ y $v \in \mathbb{H}_0$. Se tiene $|q_1|^2 = a^2 + v^2$.
Por hipótesis $q_1 \sim q_2$, o sea, $q_2 = \mu q_1 \mu^{-1}$, por ello, $|q_2|^2 = |\mu|^2|q_1|^2|\mu^{-1}|^2 = |q_1|^2$.
Además $q_2 = \mu(a + v)\mu^{-1} = a + \mu v\mu^{-1}$, de donde deducimos que $\Re(q_1) = \Re(q_2)$.

Para la otra implicación, suponemos que existen $q_1, q_2 \in \mathbb{H}$ tales que $|q_1| = |q_2|$ y $\Re(q_1) = \Re(q_2)$, por tanto, $q_1 = a + v$ y $q_2 = a + w$ con $a = \Re(q_1)$ y $v, w \in \mathbb{H}_0$.
Como $|a + v| = |a + w|$ se deduce que $|v| = |w|$. Veamos que $v \sim \mathbf{i}|v|$.
Sea $v = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$. Tomamos $\mu := (|v| + a_1) - a_2\mathbf{j} - a_3\mathbf{k}$. Por el Lema 1.2 se tiene que $v\mu = \mu\mathbf{i}|v|$, luego, $v \sim \mathbf{i}|v| = \mathbf{i}|w| \sim w$. Es decir, existe $\lambda \in \mathbb{H}$ no nulo tal que $v = \lambda w \lambda^{-1}$, sumando a en ambos lados de la igualdad tenemos,

$$a + v = a + \lambda w\lambda^{-1} = a\lambda\lambda^{-1} + \lambda w\lambda^{-1} = \lambda a\lambda^{-1} + \lambda w\lambda^{-1} = \lambda(a + w)\lambda^{-1}$$

luego, $q_1 \sim q_2$. □

Como consecuencia inmediata tenemos:

Corolario 1.11. *Sea $q = a + v \in \mathbb{H}$. Entonces $q \sim a \pm |v|\mathbf{i}$. es decir, cualquier cuaternión es similar a dos números complejos.*

Observación 1.12. Por el Teorema 1.10 los cuaterniones similares a $\mathbf{i}$ son aquellos $q \in \mathbb{H}$ tales que $\Re(q) = 0$ y $|q| = 1$, es decir son $q = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H}$ tales que $a_1^2 + a_2^2 + a_3^2 = 1$. Se sigue que las soluciones de la ecuación $d_{\mathbf{i}}(\xi) = \xi^2 + 1 = 0$ están en correspondencia con los puntos de S^2.

1.3. Estructuras asociadas a los cuaterniones

Con lo visto podemos pensar en los cuaterniones como un anillo no conmutativo unitario donde todo elemento no nulo admite inverso, es decir, $\mathbb{H}$ es un anillo de división. En particular $\mathbb{H}$ es grupo aditivo no abeliano. A continuación vamos a considerar otras estructuras en $\mathbb{H}$.

1.3.1. Los cuaterniones como espacio vectorial real

Veamos que $\mathbb{H}$ es isomorfo a $\mathbb{R}^4$ como $\mathbb{R}$-espacio vectorial, donde $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ es una base. Tenemos que $\mathbb{H} \subseteq \mathcal{M}_2(\mathbb{C})$ y $\mathcal{M}_2(\mathbb{C})$ es un $\mathbb{C}$-espacio vectorial de dimensión 4, donde $\{e_1, e_2, e_3, e_4\}$ es una base con:

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad e_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Por tanto si $q \in \mathcal{M}_2(\mathbb{C})$ tenemos :
$q = z_1e_1 + z_2e_2 + z_3e_3 + z_3e_3 \quad$ con $\quad z_l = a_l + b_li \in \mathbb{C}, \quad l = 1, 2, 3, 4.$

$$q = \begin{pmatrix} a_1 + b_1i & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_2 + b_2i \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ a_3 + b_3i & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a_4 + b_4i \end{pmatrix}$$
$$= a_1e_1 + b_1 \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix} + a_2e_2 + b_2 \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix} + a_3e_3 + b_3 \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix} + a_4e_4 + b_4 \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix}.$$

Denotamos: $\overline{e_1} = \begin{pmatrix} i & 0 \\ 0 & 0 \end{pmatrix}, \quad \overline{e_2} = \begin{pmatrix} 0 & i \\ 0 & 0 \end{pmatrix}, \quad \overline{e_3} = \begin{pmatrix} 0 & 0 \\ i & 0 \end{pmatrix}$ y $\overline{e_4} \begin{pmatrix} 0 & 0 \\ 0 & i \end{pmatrix}.$

Luego, $\{e_1, \overline{e}_1, e_2, \overline{e}_2, e_3, \overline{e}_3, e_4, \overline{e}_4\}$ es un sistema generador y una base de $\mathcal{M}_2(\mathbb{C})$ como $\mathbb{R}$-espacio vectorial. Además $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathcal{M}_2(\mathbb{C})$ y son linealmente independientes cuando pensamos en $\mathcal{M}_2(\mathbb{C})$ como $\mathbb{R}$-espacio vectorial. Se sigue entonces que $\mathbb{H}$ es isomorfo a $\mathbb{R}^4$ como $\mathbb{R}$-espacio vectorial.
Además, si $\cong$ denota ser isomorfo, entonces como $\mathbb{R}^4 \cong \mathbb{C}^2$ tenemos $\mathbb{H} \cong \mathbb{C}^2$. En particular la aplicación

$$\begin{aligned} \phi : \mathbb{C}^2 &\longrightarrow \mathbb{H} \\ (z, z') &\longrightarrow \phi(z, z') = z + \mathbf{j}z'. \end{aligned} \tag{1.1}$$

es una correspondencia biyectiva, pues si $q \in \mathbb{H}$ entonces $q = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = (a + b\mathbf{i}) + \mathbf{j}(c - d\mathbf{i})$. Tomando $z = a + bi$, $z' = c - di \in \mathbb{C}$ tenemos que $q = z + \mathbf{j}z'$.

1.3.2. Los cuaterniones como álgebra

Recordamos la definición de álgebra:

Definición 1.13. *Sea $(V_K, +, \cdot)$ un espacio vectorial sobre un cuerpo K. Diremos que $(V_K, +, \cdot)$ es un álgebra sobre K si existe una aplicación, es decir, si existe $\cdot : V_K \times V_K \longrightarrow V_K$ que cumple:*

(i) $u \cdot (v + w) = uv + uw$, *para todo* $u, v, w \in V_K$,
(ii) $(v + w) \cdot u = vu + wu$, *para todo* $u, v, w \in V_K$,
(iii) $u \cdot (\lambda v) = (\lambda u)v = \lambda uv$, *para todo* $u, v \in V_K$, *y para todo* $\lambda \in K$.

Tomamos como espacio vectorial el propio $\mathbb{H}$, por ser $\mathbb{H} \cong \mathbb{R}^4$ como espacio vectorial con las operaciones ya descritas del anillo de Hamilton. Obsérvese que el cuaternión, $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ corresponde en coordenadas cartesianas con $q = (a_0,\ a_1,\ a_2,\ a_3) \in \mathbb{R}^4$. Entonces $\mathbb{H}$ es un álgebra.

Definición 1.14. *Sean $(V_K, +, \cdot)$ un álgebra sobre un cuerpo K, y B un subconjunto de V_K. Diremos que B es una subálgebra de V_K si B es un subespacio vectorial de V_K con estructura de álgebra utilizando las operaciones $(+, \cdot)$ definidas en V_K.*

Proposición 1.15. *Sea $q = a + v \in \mathbb{H}$ tal que v es no nulo. El subálgebra generada por q es isomorfa a $\mathbb{C}$.*

Demostración. Cualquier cuaternión se puede escribir como, $q = a + tw$, con $a = \Re(q)$, $t = |v|$ y $w = \frac{v}{|v|} \in \mathbb{H}_0$. Como $v \neq 0$ sabemos que $|q| \neq 0$. Por construcción $\Re(w) = 0$ y $|w| = 1$. Además, por la Observación 1.12 sabemos que $w^2 = -1$. Afirmamos que $\langle q \rangle = \langle 1, w \rangle$: el contenido hacia la derecha es claro. Por otra parte observamos que $1 = q^{-1}q \in \langle q \rangle$ y puesto que $q, 1 \in \langle q \rangle$ tenemos $w = \dfrac{q - a \cdot 1}{t} = \dfrac{q}{t} - \dfrac{a \cdot 1}{t} \in \langle q \rangle$.
Considerando el isomorfismo $\varphi : \langle 1, w \rangle \longrightarrow \mathbb{C}$ tal que $\varphi(a + bw) = a + bi$ concluimos que $\langle q \rangle \cong \mathbb{C}$. □

De la Observación 1.12 deducimos que la ecuación

$$\xi^2 + 1 = 0$$

tiene infinitas soluciones. Es natural preguntarse si existen métodos generales que nos permitan resolver ecuaciones cuaterniónicas. ¿Cómo deben de ser estas ecuaciones? ¿Es posible contabilizar el número de soluciones que nos proporcionan? Estas preguntas nos sirven de motivación e introducción al siguiente capítulo.

2

Métodos de resolución de ecuaciones cuaterniónicas

En este capítulo estudiaremos diferentes métodos de resolución de ecuaciones cuaterniónicas atendiendo a su grado. Además, se incluye la resolución de sistemas de ecuaciones lineales con dos incógnitas.

2.1. Ecuaciones cuaterniónicas de grado 1

En lo que sigue nos hemos basado en el trabajo [1]. A continuación, planteamos un procedimiento para resolver ecuaciones del tipo

$$p_1 \xi q_1 + \cdots + p_n \xi q_n = r \qquad p_i, q_i, r \in \mathbb{H} \qquad 1 \leq i \leq n. \tag{2.1}$$

Resolver (2.1) se reduce a resolver un sistema lineal en $\mathbb{R}$. Para ello, tenemos que tener en cuenta los siguiente conceptos.

Definición 2.1. *Sean $p, q \in \mathbb{H}$. Llamamos "multiplicar por la izquierda" a la aplicación:*

$$\begin{aligned} L_p : \mathbb{H} &\longrightarrow \mathbb{H} \\ t &\longrightarrow L_p(t) = pt. \end{aligned}$$

Llamamos "multiplicar por la derecha" a la aplicación:

$$\begin{aligned} R_q : \mathbb{H} &\longrightarrow \mathbb{H} \\ t &\longrightarrow R_q(t) = tq. \end{aligned}$$

Ya hemos visto que $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ es una base de $\mathbb{H}$ como $\mathbb{R}$-espacio vectorial. Luego, se demuestra que ambas aplicaciones son lineales.
Seguidamente, veamos cuáles son las matrices asociadas a las aplicaciones L_p y R_q.

Proposición 2.2. *Sea $p = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$, entonces la matriz asociada a la aplicación lineal L_p es:*

$$\mathcal{L}_p = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & c & b & a \end{pmatrix}.$$

De la misma manera si $q = \tilde{a} + \tilde{b}\mathbf{i} + \tilde{c}\mathbf{j} + \tilde{d}\mathbf{k}$ *la matriz asociada a la aplicación lineal* R_q *es:*

$$\mathcal{R}_q = \begin{pmatrix} \tilde{a} & -\tilde{b} & -\tilde{c} & -\tilde{d} \\ \tilde{b} & \tilde{a} & -\tilde{d} & \tilde{c} \\ \tilde{c} & \tilde{d} & \tilde{a} & -\tilde{b} \\ \tilde{d} & \tilde{c} & \tilde{b} & \tilde{a} \end{pmatrix}.$$

Demostración. Para obtener la matriz asociada, calculamos la imagen de la base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ con la aplicación lineal L_p :

- $L_p(\mathbf{1}) = \mathbf{1}p = (1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k})(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = p = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$.
- $L_p(\mathbf{i}) = \mathbf{i}p = (0 + \mathbf{i} + 0\mathbf{j} + 0\mathbf{k})(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = -b + a\mathbf{i} + d\mathbf{j} - c\mathbf{k}$.
- $L_p(\mathbf{k}) = \mathbf{k}p = (0 + 0\mathbf{i} + 0\mathbf{j} + \mathbf{k})(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = -d + c\mathbf{i} - b\mathbf{j} + a\mathbf{k}$.
- $L_p(\mathbf{k}) = \mathbf{k}p = (0 + 0\mathbf{i} + 0\mathbf{j} + \mathbf{k})(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = -d + c\mathbf{i} - b\mathbf{j} + a\mathbf{k}$.

De manera similar obtenemos la matriz $\mathcal{R}_q$ asociada a la aplicación lineal R_q. □

Sabemos que el anillo de los cuaterniones no es conmutativo pero sí es asociativo. Por tanto, $(L_p \circ R_q)(\xi) = p(\xi q) = (p\xi)q = (R_q \circ L_p)(\xi)$ para todo $\xi \in \mathbb{H}$. Equivalentemente esto es $\mathcal{R}_q \circ \mathcal{L}_p = \mathcal{L}_p \circ \mathcal{R}_q$. Denotaremos por $\hat{p}$ al vector de $\mathbb{R}^4$ asociado a $p \in \mathbb{H}$.
Por tanto, resolver la ecuación (2.1) equivale a resolver el sistema de ecuaciones reales en forma matricial $(\mathcal{L}_{p_1}\mathcal{R}_{q_1} + \cdots + \mathcal{L}_{p_n}\mathcal{R}_{q_n})\hat{\xi} = \hat{r}$ con $\hat{\xi}, \hat{r} \in \mathbb{R}^4$.

Para reforzar esta idea presentamos un ejemplo.

Ejemplo 2.3. (Ecuación de Sylvester)
Queremos resolver la ecuación $\mathbf{i}\xi + \xi\mathbf{j} = \mathbf{i} + \mathbf{j}$.
Se trata de una ecuación lineal de grado 1, con $p_1 = \mathbf{i}, q_1 = 1 = p_2,$ y $q_2 = \mathbf{j}$.
Aplicando la Proposición 2.2 obtenemos:

$$\mathcal{L}_{p_1} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \mathcal{R}_{q_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \mathcal{L}_{p_2}, \quad \mathcal{R}_{q_2} = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

El objetivo es determinar $a, b, c, d \in \mathbb{R}$ tales que $\tilde{\xi} = (a, b, c, d)$ cumpla $M\hat{\xi} = \hat{r}$ con $M := \mathcal{L}_{p_1}\mathcal{R}_{q_1} + \mathcal{L}_{p_2}\mathcal{R}_{q_2}$.
Por tanto, buscamos resolver el sistema

$$\begin{cases} -b-c=0 \\ a-d=1 \\ a-d=1 \\ b+c=0, \end{cases} \quad \text{es decir,} \quad \begin{cases} b+c=0 \\ a-d=1. \end{cases} \tag{2.2}$$

Obsérvese que las matrices $M = \begin{pmatrix} 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ y $M^* = \begin{pmatrix} 0 & -1 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 1 \\ 1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$ son respectivamente la matriz asociada al sistema (2.2) y su matriz ampliada. Nos encontramos bajo las hipótesis del teorema de Rouché-Frobenius, los rangos de M y M^* coinciden y son iguales a dos, se sigue que el sistema (2.2) es compatible indeterminado con infinitas soluciones. Resolviendo dicho sistema, las soluciones de la ecuación de Sylvester son $\xi = \lambda + \mu(\mathbf{i}-\mathbf{j}) + (\lambda-1)\mathbf{k}$ con $\lambda, \mu \in \mathbb{R}$.

2.2. Ecuaciones cuaterniónicas de grado 2

En esta sección planteamos un método de resolución para las ecuaciones cuadráticas unilaterales de la forma $\bar{a}\xi^2 + \bar{b}\xi + \bar{c} = 0$ con $\bar{a} \neq 0$, $\bar{a}, \bar{b}, \bar{c} \in \mathbb{H}$. Multiplicando por el inverso de $\bar{a}$, tenemos

$$\xi^2 + b\xi + c = 0, \quad \text{donde} \quad b = \bar{a}^{-1}\bar{b} \text{ y } c = \bar{a}^{-1}\bar{c}. \tag{2.3}$$

Supondremos entonces, sin pérdida de generalidad, que la ecuación a resolver es mónica. Cabe señalar que la ecuación cuadrática bilateral $\xi^2 + \alpha_1\xi + \xi\beta_1 + \alpha_0 = 0$, con $\alpha_1, \beta_1, \alpha_0 \in \mathbb{H}$, se puede reducir a (2.3) realizando el cambio de variable $\xi = \zeta - \frac{\beta_1}{2}$. En efecto,

$$\left(\zeta - \frac{\beta_1}{2}\right)^2 + \alpha_1\left(\zeta - \frac{\beta_1}{2}\right) + \left(\zeta - \frac{\beta_1}{2}\right)\beta_1 + \alpha_0,$$

es decir,
$$\zeta^2 - \cancel{\zeta\beta_1} + \frac{\beta_1^2}{4} + \alpha_1\zeta - \frac{\alpha_1\beta_1}{2} + \cancel{\zeta\beta_1} - \frac{\beta_1^2}{2} + \alpha_0,$$

y obtenemos una ecuación del tipo (2.3) donde $b = \alpha_1$ y $c = -\frac{\beta_1^2}{4} - \frac{\alpha_1\beta_1}{2} + \alpha_0$. Sea ξ_0 una solución de la ecuación (2.3). Denotamos:

$$T = 2\Re(\xi_0) = \xi_0 + \bar{\xi}_0, \qquad N = \xi_0\bar{\xi}_0 = |\xi_0|^2. \tag{2.4}$$

Por la Proposición 1.6 sabemos que $\xi_0^2 - T\xi_0 + N = 0$. Además $\xi_0^2 + b\xi_0 + c = 0$. Restando ambas expresiones tenemos

$$(b+T)\xi_0 + c - N = 0. \tag{2.5}$$

En el siguiente esquema presentamos todos los casos para resolver (2.3). Para el caso 1 y 2 nos hemos basado en la referencia [5] y para el caso 3 hemos seguido la referencia [1].

$$
\begin{cases}
\textbf{Caso 1: } b,c \in \mathbb{R} \begin{cases} \textbf{Caso 1.1: si } b^2 < 4c \to \xi_0 = -\dfrac{b}{2} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}, \\ \qquad\qquad \text{con } \beta,\gamma,\delta \in \mathbb{R} \text{ tal que} \\ \qquad\qquad \beta^2+\gamma^2+\delta^2 = c - \frac{b^2}{4}. \\ \textbf{Caso 1.2: si } b^2 \geq 4c \to \xi_0 = \dfrac{-b \pm \sqrt{b^2-4c}}{2}. \end{cases} \\
\textbf{Caso 2: } b \in \mathbb{R}, c \notin \mathbb{R} \to \xi_0 = \dfrac{-b}{2} \pm \dfrac{\rho}{2} \mp \dfrac{c_1}{\rho}\mathbf{i} \mp \dfrac{c_2}{\rho}\mathbf{j} \mp \dfrac{c_3}{\rho}\mathbf{k}. \\
\qquad\qquad c = (c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}). \\
\qquad\qquad \rho = \sqrt{\dfrac{(b^2-4c_0) + \sqrt{(b^2-4c_0)^2 + 16(c_1^2+c_2^2+c_3^2)}}{2}}. \\
\textbf{Caso 3: } b \notin \mathbb{R} \equiv \begin{cases} T^3 + (B-2N)T + D = 0 \\ N^2 - (B+T^2)N + E = 0. \end{cases} \\
\qquad \text{con } B = 1 + 2\Re(c) \in \mathbb{R}, \\
\qquad\quad E = |c|^2 \in \mathbb{R}, \\
\qquad\quad D = -c\mathbf{i} + \mathbf{i}\bar{c} \in \mathbb{R}. \\
\qquad\qquad\quad \downarrow \\
\qquad\quad \xi_0 = \dfrac{\mathbf{i}-T}{|\mathbf{i}+T|^2}(c-N). \\
\qquad\qquad \begin{cases} \textbf{Caso 3.1: } D \neq 0 \to T = \pm\sqrt{z_0}. \\ \qquad\qquad\qquad N = \dfrac{T^3+BT+D}{2T}, \\ \text{con } z_0 \text{ raíz positiva de P(z).} \\ P(z) := z^3 + 2Bz^2 + (B^2-4E)z - D^2 = 0. \\ \textbf{Caso 3.2: } D = 0 \to \begin{cases} \text{si } B^2 - 4E \geq 0 \\ \qquad\downarrow \\ T = 0. \\ N = \dfrac{B \pm \sqrt{B^2-4E}}{2}. \\ \\ \text{si } B^2 - 4E < 0 \\ \qquad\downarrow \\ T = \sqrt{2\sqrt{E} - B}. \\ N = +\sqrt{E}. \end{cases} \end{cases}
\end{cases}
$$

Caso 1: $b, c \in \mathbb{R}$. Resolvemos la ecuación (2.3) en el cuerpo de los números complejos. Luego,

$$\xi_0 = \frac{-b \pm \sqrt{b^2-4c}}{2}.$$

Proposición 2.4. *Sea $\xi_0 \in \mathbb{H}$. Supongamos que b y $c \in \mathbb{R}$ en (2.3). Entonces ξ_0 es una solución de (2.3) si y solo si $u^{-1}\xi_0 u$ es solución de (2.3) para todo $u \in \mathbb{H} \setminus \{0\}$.*

Demostración. Basta observar que $(u^{-1}\xi_0 u)(u^{-1}\xi_0 u) + b(u^{-1}\xi_0 u) + c = u^{-1}(\xi_0^2 + b\xi_0 + c)u$. □

Atendiendo al signo del discriminante de la ecuación (2.3) distinguimos dos subcasos:

Caso 1.1: $b^2 < 4c$. Observamos que $\xi_0 = \dfrac{-b \pm \sqrt{4c - b^2}\mathbf{i}}{2}$ es solución de (2.3). Por la Proposición 2.4, también serán soluciones todos los cuaterniones similares a ξ_0. Esto quiere decir que, para todo $q \in \mathbb{H}$ no nulo

$$q^{-1}\frac{-b \pm \sqrt{4c - b^2}\mathbf{i}}{2}q =: \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \in \mathbb{H} \text{ será solución de la ecuación (2.3).}$$

El Teorema 1.10 nos indica cómo construir cuaterniones similares. Dos cuaterniones similares han de tener la misma parte real, por ello, $\Re(\alpha+\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k}) = \Re(\xi_0)$, es decir, $\alpha = -\frac{b}{2}$. La caracterización también indica que tienen la misma norma. Luego,

$$|\xi_0| = \sqrt{\frac{b^2 + 4c - b^2}{4}} = \sqrt{c} = \sqrt{\tfrac{b^2}{4} + \beta^2 + \gamma^2 + \delta^2}.$$

Si elevamos al cuadrado para eliminar la raíz cuadrada y despejamos, obtenemos $c - \frac{b^2}{4} = \beta^2 + \gamma^2 + \delta^2$. Por tanto, el conjunto de soluciones de (2.3) es:

$$\left\{ q^{-1}\frac{-b \pm \sqrt{4c - b^2}\mathbf{i}}{2}q \ : \ q \neq 0 \right\} = \left\{ \frac{-b}{2} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \ : \ \beta^2 + \gamma^2 + \delta^2 = c - \frac{b^2}{4} \right\}.$$

Ilustremos este método con el siguiente ejemplo.

Ejemplo 2.5. Encontremos las soluciones de $2\xi^2 - 4\xi + 6\xi = 0$.
Multiplicando por $\frac{1}{2}$ obtenemos la ecuación equivalente $\xi^2 - 2\xi + 3 = 0$.
Es decir $b = -2$ y $c = 3$, $b^2 = 4 < 4c = 4 \cdot 3$, podemos concluir que nos encontramos en el Caso 1.1. Por tanto,

$$\xi_0 = \frac{2 \pm \sqrt{12 - 4}\mathbf{i}}{2} = 1 \pm \sqrt{2}\mathbf{i},$$

y el conjunto de todas las soluciones de la ecuación $2\xi^2 - 4\xi + 6\xi = 0$ es

$$\left\{ 1 + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \text{ tal que } \beta^2 + \gamma^2 + \delta^2 = 2 \right\}.$$

Caso 1.2: $b^2 \geq 4c$. En este caso, $\xi_0 = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2} \in \mathbb{R}$.
Como consecuencia de la caracterización de cuaternión similar, podemos concluir que el cuaternión real ξ_0 solo es similar a sí mismo. Por ende, a lo sumo en este caso existen dos soluciones, ambas reales. De nuevo, pongamos un ejemplo.

Ejemplo 2.6. Calculemos las soluciones de $\xi^2 + 4\xi + 1 = 0$.
Como $b^2 = 16 > 4c = 4$ estamos ante el Caso 1.2 donde hay dos soluciones que son:

$$\xi_0 = \frac{-4 \pm \sqrt{16 - 4}}{2} = -2 \pm \sqrt{3} \in \mathbb{R}.$$

Caso 2: $b \in \mathbb{R}, c \neq \mathbb{R}$. Escribimos $c = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} \in \mathbb{H}$.
En este caso buscamos $\xi_0 = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ tal que cumpla (2.3), es decir,

$$\begin{aligned} 0 &= \xi_0^2 + b\xi_0 + c \\ &= (x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k})^2 + b(x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}) + (c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}) \\ &= (x_0^2 - x_1^2 - x_2^2 - x_3^2 + 2x_0x_1\mathbf{i} + 2x_0x_2\mathbf{j} + 2x_0x_3\mathbf{k}) + \\ &+ bx_0 + bx_1\mathbf{i} + bx_2\mathbf{j} + bx_3\mathbf{k} + c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}. \end{aligned}$$

Igualando componente a componente:

$$\begin{cases} x_0^2 - x_1^2 - x_2^2 - x_3^2 + bx_0 + c_0 = 0 \\ 2x_0x_1 + bx_1 + c_1 = 0 \\ 2x_0x_2 + bx_2 + c_2 = 0 \\ 2x_0x_3 + bx_3 + c_3 = 0. \end{cases} \tag{2.6}$$

De manera equivalente,

$$\begin{cases} (x_0 + \frac{b}{2})^2 - x_1^2 - x_2^2 - x_3^2 = \frac{b^2}{4} - c_0 \\ (2x_0 + b)x_1 = -c_1 \\ (2x_0 + b)x_2 = -c_2 \\ (2x_0 + b)x_3 = -c_3. \end{cases} \tag{2.7}$$

Como $c \notin \mathbb{R}$, $\Im(c) = c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} \neq 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$ entonces $c_i \neq 0$ para algún $i = 1, 2, 3$. Observando (2.7) concluimos que $2x_0 + b \neq 0$.
Luego, basta resolver para x_i en las tres últimas ecuaciones de (2.7), obteniendo,

$$x_i = -\frac{c_i}{2x_0 + b} \quad \text{con } i = 1, 2, 3. \tag{2.8}$$

Con el objetivo de encontrar una expresión para x_0 sustituimos (2.8) en la primera ecuación de (2.7): $\left(x_0 + \frac{b}{2}\right)^2 - \left(\frac{c_1}{2x_0+b}\right)^2 - \left(\frac{c_2}{2x_0+b}\right)^2 - \left(\frac{c_3}{2x_0+b}\right)^2 = \left(\frac{b}{2}\right)^2 - c_0$.
y operando $(2x_0 + b)^4 - (b^2 - 4c_0)(2x_0 + b)^2 - 4(c_1^2 + c_2^2 + c_3^2) = 0$. Por tanto,
$(2x_0 + b)^2 = \dfrac{(b^2 - 4c_0) + \sqrt{(b^2 - 4c_0)^2 + 16(c_1^2 + c_2^2 + c_3^2)}}{2} \geq 0.$
Descartamos que $(2x_0 + b)^2 = \dfrac{(b^2 - 4c_0) - \sqrt{(b^2 - 4c_0)^2 + 16(c_1^2 + c_2^2 + c_3^2)}}{2}$ pues $(2x_0 + b)^2 > 0$.
Llamamos $\rho := \sqrt{\dfrac{(b^2 - 4c_0) + \sqrt{(b^2 - 4c_0)^2 + 16(c_1^2 + c_2^2 + c_3^2)}}{2}} \neq 0$ pues $c \notin \mathbb{R}$.
Luego, $(2x_0 + b)^2 = \rho^2$, entonces,

$$x_0 = \frac{-b \pm \rho}{2}. \tag{2.9}$$

Por (2.9) y (2.8), se sigue que,

$$\xi_0 = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k} = \frac{-b}{2} \pm \frac{\rho}{2} \mp \frac{c_1}{\rho}\mathbf{i} \mp \frac{c_2}{\rho}\mathbf{j} \mp \frac{c_3}{\rho}\mathbf{k}.$$

Pongamos un ejemplo.

Ejemplo 2.7. Queremos resolver $-\mathbf{i}\xi^2 - \sqrt{2}\mathbf{i}\xi + \mathbf{j} - \mathbf{k} = 0$.
Multiplicando a la izquierda por $-\mathbf{i}^{-1} = \mathbf{i}$ obtenemos $\xi^2 + \sqrt{2}\xi + \mathbf{j} + \mathbf{k} = 0$.
Como $\sqrt{2} \in \mathbb{R}$ y $c = \mathbf{j} + \mathbf{k} \notin \mathbb{R}$, nos encontramos bajo las condiciones del Caso 2.

Por tanto, $\rho = \sqrt{\frac{2+\sqrt{2^2+16(1+1)}}{2}} = 2$.
Se sigue que las soluciones son: $\xi_0 = -\frac{\sqrt{2}}{2} \pm 1 \mp \frac{1}{2}\mathbf{j} \pm \frac{1}{2}\mathbf{k}$.
Concluimos que el conjunto de soluciones de la ecuación cuadrática estudiada es:

$$\left\{ \frac{1}{2}\left(2 - \sqrt{2} - \mathbf{j} - \mathbf{k}\right),\ \frac{-1}{2}\left(2 + \sqrt{2} - \mathbf{j} - \mathbf{k}\right) \right\}.$$

Caso 3: $b \notin \mathbb{R}$. Todo cuaternión $q \in \mathbb{H}$ con $|q| \neq 0$ se reescribe como:

$$q = \Re(q) + |\Im(q)| \left(\frac{\Im(q)}{|\Im(q)|}\right), \quad \text{con} \left|\frac{\Im(q)}{|\Im(q)|}\right| = 1.$$

En el caso que nos ocupa $b \notin \mathbb{R}$, por ende, $\Im(b) \neq 0$. Esto implica que $|b| \neq 0$.
Se sigue que $b = s + tw$ donde $s = \Re(b)$, $t = |\Im(b)|$ y $w = \frac{\Im(b)}{|\Im(b)|}$.
Por la propia construcción de w sabemos que, $\Re(w) = 0$ y $|w| = 1$.

Como $b \neq 0$, definimos el cambio de variable $\mu = \frac{1}{t}(\xi + \frac{s}{2})$ entonces $\xi = t\mu - \frac{s}{2}$.
Sustituyendo en (2.3), $\left(t\mu - \frac{s}{2}\right)^2 + b\left(t\mu - \frac{s}{2}\right) + c = 0$. Desarrollando la entidad notable y usando la asociatividad en el producto, $t^2\mu^2 + (-st + bt)\mu + c'' = 0$ donde $c'' = \frac{s^2}{4} - \frac{s}{2}b + c$.
Como $b = s + tw$ se tiene que, $t^2\mu^2 + (t^2w)\mu + c'' = 0$, es decir, $\mu^2 + w\mu + c' = 0$ donde $c' = \frac{c''}{t^2}$, tiene sentido pues $t = |b| \neq 0$.

Por consiguiente resolver la ecuación (2.3) equivale a resolver la ecuación

$$\mu^2 + w\mu + c' = 0, \qquad \text{donde } \Re(w) = 0 \text{ y } |w| = 1. \tag{2.10}$$

Por el Teorema 1.10 sabemos que los cuaterniones w e $\mathbf{i}$ son similares, es decir, existe $q \in \mathbb{H}$ no nulo tal que $w = q\mathbf{i}q^{-1}$. Por otro lado, considerando $\mu = qzq^{-1}$ y sustituyendo estas nuevas expresiones en (2.10)

$$(qzq^{-1})(qzq^{-1}) + (q\mathbf{i}q^{-1})(qzq^{-1}) + c' = 0.$$

Multiplicando a la izquierda por q^{-1}, a la derecha por q y haciendo uso de la asociatividad entre cuaterniones obtenemos

$$z^2 + \mathbf{i}z + q^{-1}c'q = 0. \tag{2.11}$$

Así pues, resolver (2.10) equivale a resolver (2.11). Para no variar con la notación usada hasta el momento resolveremos (2.3) tomando $b = \mathbf{i}$ y $c = q^{-1}c'q = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} \in \mathbb{H}$. Sea $\xi_0 \in \mathbb{H}$ raíz de dicha ecuación.
De (2.5) sabemos, $(\mathbf{i}+T)\xi_0 + (c - N) = 0$. Aclaramos que $(\mathbf{i}+T) \neq 0$ pues de lo contrario $\mathbf{i} = -T \in \mathbb{R}$ lo cual es absurdo. Por tanto, $\xi_0 = -(\mathbf{i}+T)^{-1}(c-N)$.

Por el Lema 1.4, $(\mathbf{i}+T)^{-1} = \dfrac{-\mathbf{i}+T}{|\mathbf{i}+T|^2}$. En definitiva,

$$\xi_0 = \frac{\mathbf{i}-T}{|\mathbf{i}+T|^2}(c-N). \tag{2.12}$$

Desarrollando el producto de (2.12)

$$\begin{aligned}
\xi_0 &= \frac{1}{1+T^2}(\mathbf{i}c - N\mathbf{i} - Tc + TN) \\
&= \frac{1}{1+T^2}(-c_1 + c_0\mathbf{i} - c_3\mathbf{j} + c_2\mathbf{k} - N\mathbf{i} - Tc_0 - Tc_1\mathbf{i} - Tc_2\mathbf{j} - Tc_3\mathbf{k} + TN) \\
&= \frac{1}{1+T^2}\Big[(-c_1 - Tc_0 + TN) + (c_0 - Tc_1 - N)\mathbf{i} + (-c_3 - Tc_2)\mathbf{j} + (c_2 - Tc_3)\mathbf{k}\Big].
\end{aligned}$$

Sustituyendo en (2.4) tenemos $T = 2\Re(\xi_0) = \frac{2}{1+T^2}(-c_1 - Tc_0 + TN)$ o equivalentemente $T + T^3 = 2(-c_1 - Tc_0 + TN)$, es decir, $T^3 + T + 2c_1 + 2c_0T - 2TN = 0$.
Llamamos:

$$\begin{cases} B = 1 + 2\Re(c) \in \mathbb{R}. \\ D = -c\mathbf{i} + \mathbf{i}\bar{c} = c_1 - c_0\mathbf{i} - c_3\mathbf{j} + c_2\mathbf{k} + c_1 + c_0\mathbf{i} + c_3\mathbf{j} - c_2\mathbf{k} = 2c_1 \in \mathbb{R}. \end{cases} \tag{2.13}$$

$$T^3 + (B - 2N)T + D = 0. \tag{2.14}$$

Por otro lado,

$$\begin{aligned}
N = \xi_0\bar{\xi_0} &= \frac{1}{(1+T^2)^2}\Big[(-c_1 - Tc_0 + TN)^2 + (c_0 - Tc_1 - N)^2 + (-c_3 - Tc_2)^2 + (c_2 - Tc_3)^2\Big] \\
&= \frac{c_1^2 - 2(N - c_0)c_1T + (N - c_0)^2T^2}{(1+T^2)^2} + \frac{c_0^2 - 2(Tc_1 + N)c_0 + (Tc_1 + N)^2}{(1+T^2)^2} \\
&+ \frac{c_3^2 + 2Tc_3c_2 + T^2c_2^2}{(1+T^2)^2} + \frac{c_2^2 - 2c_2c_3T + T^2c_3^2}{(1+T^2)^2}.
\end{aligned}$$

Si desarrollamos para simplificar términos obtenemos,

$$\begin{aligned}
N = \frac{1}{(1+T^2)^2}\ \Big[\ &|c|^2 - \cancel{2Nc_1T} + \cancel{2c_0c_1T} + N^2T^2 - 2Nc_0T^2 + c_0^2T^2 - \cancel{2c_0c_1T} \\
&- 2Nc_0 + c_1^2T^2 + \cancel{2Nc_1T} + N^2 + \cancel{2c_3c_2T} + T^2c_2^2 - \cancel{2c_3c_2T} + T^2c_3^2\Big].
\end{aligned}$$

Luego,

$$N = \frac{1}{(1+T^2)^2}\Big[|c|^2 + N^2T^2 - 2Nc_0T^2 - 2Nc_0 + |c|^2T^2 + N^2\Big].$$

Por ello,

$$N = \frac{1}{(1+T^2)^2}\Big[(1+T^2)|c|^2 + (1+T^2)N^2 - (1+T^2)2Nc_0\Big] = \frac{1}{1+T^2}\Big[|c|^2 + N^2 - 2Nc_0\Big].$$

Entonces, $(1+T^2)N = N^2 - 2c_0N + |c|^2$. Agrupando términos, $N^2 - (1+2c_0+T^2)N + |c|^2 = 0$. Por (2.13) esto es:

$$N^2 - (B+T^2)N + E = 0, \tag{2.15}$$

donde $E = |c|^2$.
A continuación veamos que el sistema en las incógnitas N y T, formado por (2.14) y (2.15) tiene dos soluciones reales que cumplen que $N \geq 0$, estas soluciones serán las que resolverán la ecuación (2.3). Para ello, necesitamos tener en cuenta los siguientes resultados.

Proposición 2.8. *Si $B < 0$ entonces $B^2 - 4E < 0$.*

Demostración. Por hipótesis $B < 0$, entonces $1 + 2\Re(c) < 0$ luego $2\Re(c) < -1$. Tomamos $c = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}$ entonces $c - \bar{c} = 2c_1\mathbf{i} + 2c_2\mathbf{j} + 2c_3\mathbf{k}$. Por tanto, $(c-\bar{c})^2 = (c-\bar{c})(c-\bar{c}) = -4(-c_1^2 - c_2^2 - c_3^2) = -|c-\bar{c}|^2 \leq 0$.

Obsérvese que $4(\Re(c)^2 - |c|^2) = 4(-c_1^2 - c_2^2 - c_3^2) = -|c-\bar{c}|^2 \leq 0$.
Por consiguiente, $B^2 - 4E = (1+2\Re(c))^2 - 4|c|^2 = 1 + 4\Re(c) + 4\Re(c)^2 - 4|c|^2 = 1 + 2\Re(c) + 2\Re(c) + 4\Re(c)^2 - 4|c|^2 = B + 2\Re(c) + 4(\Re(c)^2 - |c|^2) < 0 - 1 - 0 < 0$. □

Caso 3.1: $D \neq 0$.

Con la siguiente proposición presentamos una fórmula explícita para calcular (2.4). Posteriormente, aplicaremos la fórmula (2.12) obteniendo ξ_0, raíz de (2.3).

Proposición 2.9. *Si $D \neq 0$ las soluciones reales del sistema formado por (2.14) y (2.15) vienen dadas por $T = \pm\sqrt{z}$ y $N = \frac{T^3+BT+D}{2T}$ con z la única solución positiva de $Z^3 + 2BZ^2 + (B^2 - 4E)Z - D^2 = 0$.*

Demostración. Despejando N de (2.14) obtenemos que $N = \frac{T^3+BT+D}{2T}$. Sustituyendo N en (2.15) tenemos que $T^6 + 2BT^4 + (B^2 - 4E)T^2 - D^2 = 0$.
Realizando el cambio de variable $Z = T^2$ obtenemos

$$P(Z) := Z^3 + 2BZ^2 + (B^2 - 4E)Z - D^2 \in \mathbb{R}[x].$$

Veamos que tiene exactamente una única raíz real positiva. Por el Teorema Fundamental de Álgebra $P(z)$ tiene exactamente tres raíces t_1, t_2 y $t_3 \in \mathbb{C}$. Por tanto,

$$P(z) = z^3 + 2Bz^2 + (B^2 - 4E)Z - D^2 = (z - t_1)(z - t_2)(z - t_3)$$
$$= z^3 + -(t_1 + t_2 + t_3)z^2 + (t_1t_2 + t_1t_3 + t_2t_3)z - t_1t_2t_3. \tag{2.16}$$

Puesto que el número de raíces complejas tiene que ser par y el conjugado de una raíz es raíz, analizamos dos casos: si $t_1 \in \mathbb{R}$ y $t_2, t_3 = \overline{t_2} \in \mathbb{C}$. Igualando los términos independientes en (2.16) obtenemos que $-D^2 = -t_1|t_2|^2 < 0$, es decir $D^2 = t_1|t_2|^2 \geq 0$, de donde se deduce que $t_1 \in \mathbb{R}^+$. Si $t_1, t_2, t_3 \in \mathbb{R}$, puesto que $D^2 = t_1t_2t_3 > 0$, se sigue que al menos hay una raíz real positiva. Sin pérdida de generalidad tomamos $t_1 > 0$ y $t_2t_3 > 0$. Igualando el resto de coeficientes en (2.16) obtenemos

$$B^2 - 4E = t_1t_2 + t_1t_3 + t_2t_3 \tag{2.17}$$
$$2B = -(t_1 + t_2 + t_3). \tag{2.18}$$

Si $t_2, t_3 > 0$, por (2.18) $B < 0$, aplicando el Lema 2.8 obtenemos que $B^2 - 4E < 0$ lo que contradice 2.17. Por tanto, concluimos que la única raíz positiva es t_1. □

Ilustremos el Caso 3.1 con un ejemplo.

Ejemplo 2.10. Queremos encontrar las soluciones de $\xi^2 + \mathbf{i}\xi + \frac{1}{\sqrt{2}}\mathbf{i} = 0$.
Tomamos $c = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} = \frac{1}{\sqrt{2}}\mathbf{i}$. Corroboramos que $D = 2c_1 = \frac{2}{\sqrt{2}} = \sqrt{2} \neq 0$.
A continuación calculamos: $B = 1 + 2c_0 = 1$ y $E = |c|^2 = \frac{1}{2}$.
Usando la Proposición 2.9 afirmamos que $P(z) = z^3 + 2z^2 - z - 2$ tiene una única raíz positiva $z_0 = 1$. Por tanto, $T = \pm 1$, de nuevo, utilizando la Proposición 2.9 obtenemos dos posibles soluciones:

- Si $T = 1$ entonces $N = \frac{1+1+\sqrt{2}}{2} = 1 + \frac{\sqrt{2}}{2}$. Por (2.12), $\xi_0 = \frac{1}{2} - \frac{1+\sqrt{2}}{2}\mathbf{i}$.
- Si $T = -1$ entonces $N = \frac{-1-1+\sqrt{2}}{-2} = 1 - \frac{\sqrt{2}}{2}$. Por (2.12), $\xi_1 = -\frac{1}{2} - \frac{1-\sqrt{2}}{2}\mathbf{i}$.

Caso 3.2: $D = 0$
La estructura de este caso es idéntica al caso anterior, presentamos fórmulas explícitas para calcular (2.4). De acuerdo con la expresión de ξ_0 dada en (2.12) resolveremos (2.3).

Proposición 2.11. *Si $D = 0$ las soluciones del sistema formado por (2.14) y (2.15) son:*

I)	$T = 0$,	$N = \frac{1}{2}(B \pm \sqrt{B^2 - 4E})$	*si* $B^2 - 4E \geq 0$.
II)	$T = \sqrt{2\sqrt{E} - B}$,	$N = +\sqrt{E}$	*si* $B^2 - 4E < 0$.

Demostración. Por hipótesis $D = 0$ entonces $T = 0$ es solución de (2.14). Resolviendo (2.15) vemos que $N = \frac{1}{2}(B \pm \sqrt{B^2 - 4E}) \geq 0$.
Si $T \neq 0$, entonces de (2.14) tenemos $T^2 + B - 2N = 0$. Despejando T^2 y sustituyendo en (2.15) obtenemos que $N = +\sqrt{E} \geq 0$. Descartamos $N = -\sqrt{E}$ pues $N \geq 0$. Se sigue que $T = \sqrt{2\sqrt{E} - B}$. Comprobemos que $T \in \mathbb{R}$: $0 \leq T^2 = 2\sqrt{E} - B$, si y solo si $2\sqrt{E} \geq B$, luego $4E \geq B^2$. En otras palabras, $T = \sqrt{2\sqrt{E} - B} \in \mathbb{R}$ si $B^2 - 4E \leq 0$. □

Los siguientes ejemplos ilustran el Caso 3.2.

Ejemplo 2.12. Resolvamos $\xi^2 + \mathbf{i}\xi + \frac{3}{2} + \frac{1}{2}\mathbf{j} + \frac{\sqrt{2}}{2}\mathbf{k} = 0$,
donde $c = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} = \frac{3}{2} + \frac{1}{2}\mathbf{j} + \frac{\sqrt{2}}{2}\mathbf{k}$.
En este caso, $D = 2c_1 = 0$ y $B^2 - 4E = 16 - 12 = 4 \geq 0$.
Como podemos ver, nos encontramos bajo las condiciones de la Proposición 2.11 caso I), luego, $T = 0$ y $N = 3$ ó $N = 1$. Utilizando (2.12) concluimos que las soluciones buscadas son:

$$\xi_0 \in \left\{ \frac{1}{2}\left(-3\mathbf{i} - \sqrt{2}\mathbf{j} + \mathbf{k}\right), \quad \frac{1}{2}\left(\mathbf{i} - \sqrt{2}\mathbf{j} + \mathbf{k}\right) \right\}.$$

Ejemplo 2.13. Hallar los ξ_0 que cumplen $\xi^2 + \mathbf{i}\xi + \mathbf{k} = 0$, donde $c = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} = \mathbf{k}$.
Como $D = 2c_1 = 0$, y $B^2 - 4E = 1 - 4 \leq 0$ podemos aplicar la Proposición 2.11 caso II). Por tanto, $T = \sqrt{2 - 1} = 1$ y $N = 1$. Teniendo en cuenta la fórmula (2.12) la solución de la ecuación cuadrática es:

$$\xi_0 = \frac{1}{2}(1 - \mathbf{i} - \mathbf{j} - \mathbf{k}).$$

2.3. Ecuaciones cuaterniónicas de grado n

En las próximas páginas presentamos un método de resolución de ecuaciones cuaterniónicas unilaterales de grado n, es decir, veremos cómo resolver expresiones de la forma:

$$\xi^n - a_{n-1}\xi^{n-1} - a_{n-2}\xi^{n-2} - \ldots - a_1\xi - a_0 = 0 \quad \text{con } a_i \in \mathbb{H}, \qquad 0 \leq i \leq n-1. \tag{2.19}$$

Comprobaremos que para resolver (2.19) basta con encontrar los autovalores de una determinada matriz con coeficientes complejos denotada por $\tilde{M}$. Este método está motivado en el estudio realizado en [3] y [11]. También [1] discute este tipo de ecuaciones.

Definición 2.14. *Llamaremos* ***matriz compañera*** *del polinomio (2.19) a la matriz*

$$M = \begin{pmatrix} a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \in \mathcal{M}_n(\mathbb{H}). \tag{2.20}$$

Sea $Q = (q_{ij}) \in \mathcal{M}_n(\mathbb{H})$, con coeficientes de la forma $q_{ij} = q_{ij}^0 + q_{ij}^1\mathbf{i} + q_{ij}^2\mathbf{j} + q_{ij}^3\mathbf{k}$. Por la aplicación dada en (1.1) tiene sentido definir:

$$Q = \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n1} & q_{n2} & \cdots & q_{nn} \end{pmatrix} = \begin{pmatrix} q_{11}^0 + q_{11}^1\mathbf{i} & q_{12}^0 + q_{12}^1\mathbf{i} & \cdots & q_{1n} \\ q_{21}^0 + q_{21}^1\mathbf{i} & q_{22}^0 + q_{22}^1\mathbf{i} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n1}^0 + q_{n1}^1\mathbf{i} & q_{n2}^0 + q_{n2}^1\mathbf{i} & \cdots & q_{nn} \end{pmatrix} + \mathbf{j} \begin{pmatrix} q_{11}^2 - q_{11}^3\mathbf{i} & q_{12}^2 - q_{12}^3\mathbf{i} & \cdots & q_{1n} \\ q_{21}^2 - q_{21}^3\mathbf{i} & q_{22}^2 - q_{22}^3\mathbf{i} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n1}^2 - q_{n1}^3\mathbf{i} & q_{n2}^2 - q_{n2}^3\mathbf{i} & \cdots & q_{nn} \end{pmatrix}$$

$$= Z + \mathbf{j}W = \begin{pmatrix} z_{11} & z_{12} & \cdots & z_{1n} \\ z_{21} & z_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1} & z_{n2} & \cdots & z_{nn} \end{pmatrix} + \mathbf{j} \begin{pmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ w_{n1} & w_{n2} & \cdots & w_{nn} \end{pmatrix}, \quad \text{con} \quad Z, W \in \mathcal{M}_n(\mathbb{C}).$$

Asociada a Q tenemos la matriz compleja $\tilde{Q}$ de la forma siguiente:

$$\tilde{Q} = \left(\begin{array}{c|c} Z & -\overline{W} \\ \hline W & \overline{Z} \end{array}\right) \in \mathcal{M}_{2n}(\mathbb{C}).$$

donde los coeficientes de las matrices $\overline{Z}$ y $\overline{W}$ son $z_{kl} = q_{kl}^0 - q_{kl}^1 i$ y $w_{kl} = q_{kl}^2 + q_{kl}^3 i$ respectivamente para todo $k, l \in \{1, \ldots n\}$.
Si construimos la matriz compleja asociada a la matriz M descrita en (2.20) obtenemos:

$$\tilde{M} = \left(\begin{array}{ccc|ccc} a_{n-1}^0 + a_{n-1}^1 i & \cdots & a_0^0 + a_0^1 i & -a_{n-1}^2 + a_{n-1}^3 i & \cdots & -a_0^2 + a_0^3 i \\ 1 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & 0 & \vdots & \cdots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \\ \hline a_{n-1}^2 - a_{n-1}^3 i & \cdots & a_0^2 - a_0^3 i & a_{n-1}^0 - a_{n-1}^1 i & \cdots & a_0^0 - a_0^1 i \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{array}\right) \in \mathcal{M}_{2n}(\mathbb{C}). \tag{2.21}$$

En lo que sigue comprobaremos que si conocemos los autovalores de la matriz $\tilde{M}$ dada en (2.21), seremos capaces de determinar los autovalores de la matriz M definida en (2.20). A continuación, enunciamos a modo de recordatorio una serie de resultados que utilizaremos con posterioridad.
Vamos a comenzar recordando la definición formal de autovalor por la derecha de una matriz de $\mathcal{M}_n(\mathbb{H})$.

Definición 2.15. *Diremos que $\lambda \in \mathbb{H}$ es un autovalor por la derecha de la matriz $A \in \mathcal{M}_n(\mathbb{H})$ si existe $v \in \mathbb{H}^n$ no nulo tal que $Mv = v\lambda$.*
Al vector v lo denominaremos autovector asociado a λ por la derecha o λ-autovector por la derecha.

El conjunto de λ-autovectores por la derecha no es un espacio vectorial debido a la no conmutatividad del anillo de Hamilton.

Para ilustrar la teoría consideraremos de nuevo el Ejemplo 2.10 planteado en la Sección 2.2, a medida que vamos avanzando retomaremos dicho ejemplo, en particular corroboraremos que el conjunto de λ-autovectores por la derecha no es un espacio vectorial.

Ejemplo 2.16. Encontrar las soluciones de $\xi^2 + \mathbf{i}\xi + \frac{1}{\sqrt{2}}\mathbf{i} = 0$.
La matriz compañera dada en (2.20) es

$$M = \begin{pmatrix} -\mathbf{i} & -\frac{\mathbf{i}}{\sqrt{2}} \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{H}).$$

Atendiendo a la fórmula (2.21) la matriz compleja asociada a M es

$$\tilde{M} = \left(\begin{array}{cc:cc} i & -\frac{i}{\sqrt{2}} & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & i & \frac{i}{\sqrt{2}} \\ 0 & 0 & 1 & 0 \end{array}\right) \in \mathcal{M}_4(\mathbb{C}).$$

Con el software MATLAB sabemos que los autovalores de $\tilde{M}$ son:

$$\begin{aligned} \lambda_1 &= \frac{1}{2} + \frac{1+\sqrt{2}}{2}i, & \overline{\lambda_1} &= \frac{1}{2} - \frac{1+\sqrt{2}}{2}i, \\ \lambda_2 &= -\frac{1}{2} + \frac{-1+\sqrt{2}}{2}i, & \overline{\lambda_2} &= -\frac{1}{2} - \frac{-1+\sqrt{2}}{2}i. \end{aligned} \tag{2.22}$$

Y los autoespacios o espacios propios asociados a los autovalores $\lambda_1, \overline{\lambda_1}, \lambda_2$ y $\overline{\lambda_2}$ de la matriz $\tilde{M}$ son respectivamente:

$$V_{\lambda_1} = \left\{ \alpha \begin{pmatrix} 0 \\ 0 \\ \frac{1}{2} + \frac{1+\sqrt{2}}{2} i \\ 1 \end{pmatrix} : \alpha \in \mathbb{R} \right\}, \qquad V_{\overline{\lambda_1}} = \left\{ \alpha \begin{pmatrix} \frac{1}{2} - \frac{1+\sqrt{2}}{2} i \\ 1 \\ 0 \\ 0 \end{pmatrix} : \alpha \in \mathbb{R} \right\},$$

$$V_{\lambda_2} = \left\{ \alpha \begin{pmatrix} -\frac{1}{2} + \frac{-1+\sqrt{2}}{2} i \\ 1 \\ 0 \\ 0 \end{pmatrix} : \alpha \in \mathbb{R} \right\}, \qquad V_{\overline{\lambda_2}} = \left\{ \alpha \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{2} - \frac{-1+\sqrt{2}}{2} i \\ 1 \end{pmatrix} : \alpha \in \mathbb{R} \right\}.$$

Obsérvese que los anteriores conjuntos son espacios vectoriales sobre $\mathbb{C}^4$.

Para poder obtener los autovalores por la derecha de la matriz M dada en (2.20) y sus respectivos λ-autovectores asociados por la derecha necesitamos tener en cuenta los siguientes resultados.

Todo $\lambda = a + bi \in \mathbb{C}$ se puede identificar con $a + b\mathbf{i} \in \mathbb{H}$. Dicha identificación permite identificar a su vez los vectores de $\mathbb{C}^n$ como vectores de $\mathbb{H}^n$. Esta identificación la usaremos constantemente en el resto del capítulo.

Teorema 2.17. *Sea $\lambda = a + bi \in \mathbb{C}$. Entonces λ es autovalor de la matriz $\tilde{M}$ dada en (2.21), con autovector $(A\ B)^T$ donde $A, B \in \mathbb{C}^n$ si y solo si $\lambda = a + b\mathbf{i} \in \mathbb{H}$ es autovalor por la derecha de la matriz M descrita en (2.20) con autovector por la derecha $A + \mathbf{j}B$.*

Demostración. Por hipótesis y por la Definición 2.15 tenemos,

$$\tilde{M} \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} A \\ B \end{pmatrix} \lambda.$$

Esto es,

$$\begin{cases} ZA - \overline{W}B = A\lambda \\ WA + \overline{Z}B = B\lambda. \end{cases} \tag{2.23}$$

Del sistema (2.23) podemos escribir la siguiente igualdad:

$$(ZA - \overline{W}B) + \mathbf{j}(WA + \overline{Z}B) = A\lambda + \mathbf{j}B\lambda.$$

Aplicando que $Z\mathbf{j} = \mathbf{j}\overline{Z}$ y $W\mathbf{j} = \mathbf{j}\overline{W}$, se tiene que $-\overline{W} = \mathbf{j}^2\overline{W} = \mathbf{j}\mathbf{j}\overline{W} = \mathbf{j}W\mathbf{j}$.
Esto es, $ZA + \mathbf{j}W\mathbf{j}B + \mathbf{j}WA + Z\mathbf{j}B = A\lambda + \mathbf{j}B\lambda$.
Sacando factor común de $A + \mathbf{j}B$ obtenemos, $(Z + \mathbf{j}W)(A + \mathbf{j}B) = (A + \mathbf{j}B)\lambda$.
Por tanto, hemos llegado a que $M(A + \mathbf{j}B) = (A + \mathbf{j}B)\lambda$. □

Proposición 2.18. *Si λ es autovalor de la matriz compleja $\tilde{M}$ descrita en (2.21) con autovector $(A\ B)^T$ donde $A, B \in \mathbb{C}^n$, entonces $\overline{\lambda}$ también es autovalor de la matriz $\tilde{M}$ con autovector $(\overline{B}\ \ -\overline{A})^T$.*

Demostración. Retomando el sistema (2.23) con el conjugado de λ, obtenemos:

$$\begin{cases} ZA - \overline{W}B = A\overline{\lambda} \\ WA + \overline{Z}B = B\overline{\lambda}. \end{cases} \quad \text{Tomando conjugados,} \quad \begin{cases} \overline{ZA} - W\overline{B} = \overline{A}\lambda \\ \overline{WA} + Z\overline{B} = \overline{B}\lambda. \end{cases}$$

De manera equivalente, $(\overline{ZA} + \overline{WA}) + \mathbf{j}(-\overline{W} + Z\overline{B}) = \overline{A}\lambda + \mathbf{j}\overline{B}\lambda$.
De nuevo siguiendo un razonamiento análogo al de la demostración del Teorema 2.17 deducimos la condición buscada pues $(Z + \mathbf{j}W)(\overline{B} + \mathbf{j}\overline{A}) = (\overline{B} + \mathbf{j}\overline{A})\lambda$. □

Ejemplo 2.19. Retomemos el Ejemplo 2.16. Por el Teorema 2.17 los autovalores de $\tilde{M}$ descritos de manera explícita en (2.22) son los autovalores por la derecha de la matriz M. Veamos como obtener los λ_i-autovectores por la derecha de la matriz M para $i = 1, 2$.
Un autovector de $\tilde{M}$ asociado a λ_1 es $u_{\lambda_1} = \begin{pmatrix} 0 & 0 & \frac{1}{2} + \frac{1+\sqrt{2}}{2}i & 1 \end{pmatrix}^T$.
Un autovector de $\tilde{M}$ asociado a λ_2 es $u_{\lambda_2} = \begin{pmatrix} -\frac{1}{2} + \frac{-1+\sqrt{2}}{2}i & 1 & 0 & 0 \end{pmatrix}^T$.

Por la Proposición 2.18 y aplicando de nuevo el Teorema 2.17 obtenemos que

$$\begin{aligned} v_{\lambda_1} &= 0 + \mathbf{j}\left(\tfrac{1}{2} + \tfrac{1+\sqrt{2}}{2}\mathbf{i} \quad 1\right)^T = \left(\tfrac{1}{2}\mathbf{j} - \tfrac{1+\sqrt{2}}{2}\mathbf{k} \quad \mathbf{j}\right)^T, \\ v_{\overline{\lambda_1}} &= \left(\tfrac{1}{2} - \tfrac{1+\sqrt{2}}{2}\mathbf{i} \quad 1\right)^T + \mathbf{j}0 = \left(\tfrac{1}{2} - \tfrac{1+\sqrt{2}}{2}\mathbf{i} \quad 1\right)^T, \\ v_{\lambda_2} &= \left(-\tfrac{1}{2} + \tfrac{-1+\sqrt{2}}{2}\mathbf{i} \quad 1\right)^T + \mathbf{j}0 = \left(-\tfrac{1}{2} + \tfrac{-1+\sqrt{2}}{2}\mathbf{i} \quad 1\right)^T, \\ v_{\overline{\lambda_2}} &= 0 + \mathbf{j}\left(-\tfrac{1}{2} - \tfrac{-1+\sqrt{2}}{2}\mathbf{i} \quad 1\right)^T = \left(-\tfrac{1}{2}\mathbf{j} + \tfrac{-1+\sqrt{2}}{2}\mathbf{k} \quad \mathbf{j}\right)^T, \end{aligned}$$

son autovectores de M por la derecha asociados a $\lambda_1, \overline{\lambda_1}, \lambda_2$ y $\overline{\lambda_2}$ respectivamente.

Veamos que el conjunto de los λ_1-autovectores asociados a la matriz M, es decir,

$$\mathbf{V}_{\lambda_1} = \left\{ \alpha \left(\frac{1}{2}\mathbf{j} - \frac{1+\sqrt{2}}{2}\mathbf{k} \quad \mathbf{j} \right)^T : \alpha \in \mathbb{R} \right\}$$

no es un espacio vectorial. En efecto, si V_λ fuese un espacio vectorial para todo $q \in \mathbb{H}$ y para todo $v \in \mathbf{V}_\lambda$ tendríamos que $qv \in V_\lambda$. En particular si tomamos: $q = \mathbf{i}$ y $v = \left(\frac{1}{2}\mathbf{j} - \frac{1+\sqrt{2}}{2}\mathbf{k} \quad \mathbf{j}\right)^T$ llegamos a que

$$qv = \left(\frac{1}{2}\mathbf{k} + \frac{1+\sqrt{2}}{2}\mathbf{j} \quad \mathbf{k} \right)^T = \alpha \left(\frac{1}{2}\mathbf{j} - \frac{1+\sqrt{2}}{2}\mathbf{k} \quad \mathbf{j} \right)^T \tag{2.24}$$

lo cual es absurdo pues no existe ningún $\alpha \in \mathbb{R}$ tal que cumple (2.24). Debido a que en V_λ no podemos definir la operación externa concluimos que no es un espacio vectorial.

Proposición 2.20. *Sea $\lambda_1 \in \mathbb{H}$ un autovalor de la matriz M definida en (2.20) con autovector v_1. Si λ_2 es similar a λ_1, es decir, $\lambda_2 = \mu\lambda_1\mu^{-1}$ con $\mu \neq 0$ entonces λ_2 también es autovalor de M y uno de sus autovectores es $v_2 = v_1\mu^{-1}$.*

Demostración. Por hipótesis y por la Definición 2.15, sabemos que, $Mv_1 = v_1\lambda_1$. Multiplicando por el inverso de μ, obtenemos, $Mv_1\mu^{-1} = v_1\lambda_1\mu^{-1}$.
Por hipótesis $\lambda_1 \sim \lambda_2$ luego, $Mv_1\mu^{-1} = v_1\lambda_1\mu^{-1} = v_1\mu^{-1}\lambda_2\mu\mu^{-1} = v_1\mu^{-1}\lambda_2$.
Concluimos que $Mv_2 = v_2\lambda_2$. □

Teorema 2.21. *Sea M la matriz compañera dada en (2.20). Si $v = (\varphi_1,\ \varphi_2, \ldots, \varphi_n)$ es un λ-autovector de la matriz M, entonces $\varphi_n \neq 0$.*

Demostración. Por hipótesis y por la Definición 2.15, $Mv = v\lambda$, esto es,

$$\left.\begin{aligned} a_{n-1}\varphi_1 + a_{n-2}\varphi_2 + \ldots + a_0\varphi_n &= \varphi_1\lambda \\ \varphi_1 &= \varphi_2\lambda \\ &\vdots \\ \varphi_{n-1} &= \varphi_n\lambda. \end{aligned}\right\} \tag{2.25}$$

Si $\varphi_n = 0$, sustituyendo ascendentemente obtenemos que $\varphi_1 = \ldots = \varphi_n = 0$.
Luego $v = 0$, lo cual es falso. □

Corolario 2.22. *Sean $u = (\alpha_1, \ldots, \alpha_n)$ y $v = (\beta_1, \ldots, \beta_n)$ dos autovectores asociados al mismo autovalor λ. Entonces u, v son iguales si y solo si tienen la última componente igual.*

Demostración. Si $u = v$ serán iguales componente a componente, en particular $\alpha_n = \beta_n$. Para el recíproco, consideramos $\alpha_n = \beta_n$. Por el sistema (2.25) sabemos que $\alpha_{n-1} = \alpha_n\lambda = \beta_{n-1}$ y resolviendo de manera ascendente concluimos que todas las componentes de u y v tienen que ser iguales. □

Definición 2.23. *Diremos que λ' es un autovalor de privilegiado de M si existe un λ'-autovector $v' = (\varphi_1,\ \varphi_2 \ldots, \varphi_n)$ que cumple que $\varphi_n = 1$.*

Observación 2.24. Por la Proposición 2.20 y el Teorema 2.21 podemos afirmar que si $\lambda \in \mathbb{H}$ es un autovalor de la matriz M entonces siempre es posible encontrar un autovalor privilegiado, tomando $\lambda' = \varphi_n\lambda\varphi_n^{-1}$ y donde un λ'-autovector asociado es $v' = v\varphi_n^{-1}$.

Estamos interesados en localizar los autovalores privilegiados. El siguiente teorema deja patente la importancia de encontrar dichos autovalores.

Teorema 2.25. *Sea $\lambda' \in \mathbb{H}$. Todo λ' es un autovalor privilegiado de la matriz M si y solo si es raíz del polinomio (2.19).*

Demostración. Por hipótesis λ' es autovalor de la matriz M descrita en (2.20). Utilizando el sistema (2.25) tenemos:

$$\begin{aligned} a_{n-1}\varphi_1\varphi_n^{-1} + a_{n-2}\varphi_2\varphi_n^{-1} + \ldots + a_0\varphi_n\varphi_n^{-1} &= \varphi_1\varphi_n^{-1}\lambda, \\ \varphi_1\varphi_n^{-1} &= \varphi_2\varphi_n^{-1}\lambda, \\ &\vdots \\ \varphi_{n-1}\varphi_n^{-1} &= \lambda. \end{aligned}$$

Si resolvemos ascendentemente, $a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0 = \lambda^n$.
Por tanto, λ' es raíz del polinomio (2.19).
Recíprocamente, sea ξ_0 una raíz del polinomio (2.19) Por lo tanto,

$$a_{n-1}\xi_0^{n-1} - a_{n-2}\xi_0^{n-2} - \ldots - a_1\xi_0 - a_0 = \xi_0^n.$$

Si definimos $\varphi_n = 1$ y $\varphi_{i-1} = \varphi_i\xi_0$ para todo $i = 1, \ldots, n$ llegamos a que

$$\begin{aligned} a_{n-1}\xi_0^{n-1} - a_{n-2}\xi_0^{n-2} - \ldots - a_1\xi_0 - a_0 &= \varphi_1\xi_0 \\ \varphi_1 &= \varphi_2\xi_0 \\ &\vdots \\ \varphi_{n-1} &= \xi_0. \end{aligned}$$

Por el sistema (2.25) sabemos que ξ_0 es autovalor, además por construcción $\varphi_n = 1$ luego es un autovalor privilegiado. □

En definitiva, para encontrar las raíces de (2.19) bastará con construir la matriz $\tilde{M}$ y calcular sus los autovalores. Por el Teorema 2.17 conoceremos los autovalores de la matriz M. Gracias a la Observación 2.24 podemos encontrar un autovalor privilegiado a partir de cualquier autovalor. Y por el Teorema 2.25 sabemos que los autovalores privilegiados son raíces de la ecuación (2.19).
Para afinar más este método, tenemos en cuenta que cada λ-autovector tiene asociado la siguiente clase de similitud $[\lambda] := \{q\lambda q^{-1}$ tal que $q \in \mathbb{H}, q \neq 0\}$.

Proposición 2.26. *Cada clase de equivalencia genera una única raíz del polinomio 2.19*

Demostración. La existencia de la raíz por el Teorema 2.25 equivale a probar la existencia de un autovalor privilegiado, que ya hemos probado por la Observación 2.24. Veamos la unicidad por reducción al absurdo.
Sean λ y λ_1 dos raíces diferentes del polinomio (2.19) tal que están en la misma clase. Por el Teorema 2.25 tanto λ como λ_1 son autovalores privilegiados.
Por la Observación 2.24 sabemos que $\lambda' = \varphi_n\lambda\varphi_n^{-1}$. Como λ es un autovalor privilegiado $\lambda' = 1\lambda 1 = \lambda$ lo cual es absurdo pues contradice las hipótesis. □

Proposición 2.27. *Sea λ autovalor de la matriz (2.20). Si tiene k autovectores distintos entre sí y no proporcionales entonces el polinomio (2.19) tiene infinitas raíces.*

Demostración. Tomamos $\{\tilde{v}_1, \dots, \tilde{v}_k\}$ una $\mathbb{C}$-base del autoespacio $V(\lambda) \subset \mathbb{C}^{2n}$. Gracias al Teorema 2.17 obtenemos $v_1, \dots, v_k \in \mathbb{H}^n$ son k λ-autovectores de la matriz M dada en (2.20) y en virtud del sistema (2.15) $v_i = (\varphi_1^i \ \cdots \ \varphi_n^i)$ con $\varphi_j^i = \varphi_{j+1}^i \lambda$ para $i \in \{1, \dots, k\}$ y $j \in \{1, \dots, n-1\}$. Se sigue que $\varphi_n^1, \dots, \varphi_n^k$ son $\mathbb{C}$-independientes en $\mathbb{H}$ debido a que $\{\tilde{v}_1, \dots, \tilde{v}_k\}$ es una $\mathbb{C}$-base.
Además por la Proposición 2.24 sabemos que los autovalores privilegiados son de la forma $\lambda' = \mu\lambda\mu^{-1}$ donde μ es cualquier $\mathbb{C}-$combinación lineal de $\varphi_n^1, \dots, \varphi_n^k$, variando sobre todos los posibles cuaterniones similares a λ, es decir, hay infinitos autovalores privilegiados por el Teorema 2.25 concluimos que el polinomio (2.19) existen infinitas raíces. □

Para aplicar las herramientas que nos proporcionan estos resultados reanudados el Ejemplo 2.19.

Ejemplo 2.28. Aplicando el Teorema 2.25 sabemos que las únicas raíces son:

$$\overline{\lambda_1} = \frac{1}{2} - \frac{1+\sqrt{2}}{2}\mathbf{i}, \quad \text{y} \quad \lambda_2 = -\frac{1}{2} + \frac{-1+\sqrt{2}}{2}\mathbf{i}.$$

Obsérvese que por el Corolario 1.11 sabemos que $\overline{\lambda_1} \sim \lambda_1$ y $\overline{\lambda_2} \sim \lambda_2$ y gracias a la Proposición 2.26 podemos corroborar que generan la misma raíz que λ_1 y λ_2.

Este ejemplo sirve para motivar la última parte de esta sección. En el ejemplo hemos obtenido dos soluciones, tiene sentido preguntarse para $n = 2$, ¿cuántas soluciones podremos obtener?
Sean $\lambda_1, \overline{\lambda_1}, \lambda_2, \overline{\lambda_2}$ los autovalores de M. Atendiendo al valor que tomen podemos contabilizar el número de soluciones de la siguiente forma:

- $\boldsymbol{\lambda_1 \neq \overline{\lambda_1} \neq \lambda_2 \neq \overline{\lambda_2}}$. Todos los autovalores son complejos y toman valores distintos. Por la Proposición 2.26 sabemos que hay dos soluciones posibles. El ejemplo que hemos presentado pertenece a este caso.

- $\boldsymbol{\lambda_1 = \overline{\lambda_1} = \lambda_2 = \overline{\lambda_2}}$, es decir, todos los autovalores toman el mismo valor real. Independientemente de la multiplicidad del autovalor existe una única solución pues solo podemos encontrar un autovalor privilegiado $\lambda' = \varphi_n \lambda_1 \varphi_n^{-1}$ donde φ_n es la última componente de uno de sus autovectores asociados. Como $\lambda_1 \in \mathbb{R}$ podemos conmutar, es decir, $\lambda' = \lambda_1 \varphi_n \varphi_n^{-1} = \lambda_1$. Luego solo existe un único autovalor privilegiado y aplicando el Teorema 2.25 concluimos que solo existe una única raíz.

- $\lambda_1 = \overline{\lambda_1} \neq \lambda_2 = \overline{\lambda_2}$. En otras palabras hay dos autovalores reales distintos con multiplicidad dos. Por la caracterización de cuaterniones similares dada en el Teorema 1.10 sabemos que λ_1 no es similar a λ_2. Además, gracias a la Proposición 2.26 concluimos que hay dos soluciones λ_1 y λ_2 serán las raíces buscadas.

- $\lambda_1 = \overline{\lambda_1}$ y $\lambda_2 \neq \overline{\lambda_2}$. Tenemos un autovalor real con multiplicidad dos y dos autovalores complejos. Se razona de forma análoga a los casos anteriores. La Proposición 2.26 nos indica que existen dos raíces.

- $\lambda_1 = \lambda_2$ y $\overline{\lambda_1} = \overline{\lambda_2}$, hay doy autovalores complejos con multiplicidad dos. Debido a la Proposición 2.27 exiten infinitas raíces.

2.4. Cálculo de raíces cuaterniónicas

Un caso particular de ecuaciones de grado n es encontrar raíces n-ésimas de un cuaternión dado. El primero en resolver ecuaciones de la forma

$$\xi^n - q = 0 \qquad \text{con } q \in \mathbb{H}, \tag{2.26}$$

fue Niven en [10]. A continuación planteamos un método basado en el trabajo [1]. Recordamos que $\mathbb{H}$ es un anillo no conmutativo. A diferencia de $\mathbb{C}$, mostraremos que el número de raíces n-ésimas de un cuaternión puede ser infinito.
Más concretamente demostraremos que los distintos casos que se presentan en $\mathcal{H}$ son los recogidos en la Tabla 2.1

Si $q \in \mathbb{H}\backslash\mathbb{R}$ con $n \geq 2$	existen n raíces.
Si $q \in \mathbb{R}$ con $n > 2$	existen infinitas raíces.
Si $q \in \mathbb{R}^+$ con $n = 2$	existen dos raíces.
Si $q \in \mathbb{R}^-$ con $n = 2$	existen infinitas raíces.

Tabla 2.1. Raíces n-ésimas de un cuaternión

Proposición 2.29. *Sean $q = a + v \in \mathbb{H}$ y $n \in \mathbb{Z}^+$, entonces existe $\lambda_n \in \mathbb{R}$ tal que $\Im(q^n) = \lambda_n \Im(q)$.*

Demostración. Si $q \in \mathbb{R}$ el resultado es trivial. Por otro lado, si $q \notin \mathbb{R}$ podemos escribir, $q = |q|(\cos\sigma + \omega \operatorname{sen}\sigma)$ con $\omega = \frac{v}{|v|}$ y $\sigma \in (o, \pi)$ es el ángulo que forma q con el eje real en el plano $\langle 1, w\rangle$.
Por tanto, $\cos\sigma = \frac{a}{|q|}$ y $\operatorname{sen}\sigma = \frac{v}{|q|}$.
Probaremos el resultado por inducción sobre n: Si $n = 1$ el resultado es trivial. Suponemos cierto para $n - 1$ y veamos que es cierto para n.

$$\begin{aligned} q^n = q^{n-1}q &= \Big(|q|^{n-1}(\cos{(n-1)\sigma} + \omega \operatorname{sen}{(n-1)\sigma})\Big)|q|(\cos\sigma + \omega \operatorname{sen}\sigma) \\ &= |q|^n\Big(\cos{(n-1)\sigma}\cos\sigma - \operatorname{sen}{(n-1)\sigma}\operatorname{sen}\sigma\Big) + \omega\Big(\cos{(n-1)\sigma}\operatorname{sen}\sigma + \operatorname{sen}{(n-1)\sigma}\cos\sigma\Big)\Big) \\ &= |q|^n\Big(\cos{((n-1)\sigma + \sigma} + w\operatorname{sen}{((n-1)\sigma + \sigma}\Big) = |q|^n(\cos n\sigma + w\operatorname{sen} n\sigma). \end{aligned}$$

Tomando $\lambda_n = |q|^{n-1}\frac{\operatorname{sen} n\sigma}{\operatorname{sen}\sigma}$ tenemos que

$$\lambda_n\Im(q) = |q|^{n-1}\frac{\operatorname{sen} n\sigma}{\operatorname{sen}\sigma}\cdot|q|\omega\operatorname{sen}\sigma = |q|^n\omega\operatorname{sen} n\sigma = \Im(q^n).$$

□

Los siguientes teoremas demuestran los resultados de la Tabla (2.1).

Teorema 2.30. *Sean $q \in \mathbb{H}\setminus\mathbb{R}$ y $n \in \mathbb{N}$, entonces el cuaternión q tiene exactamente n raíces n-ésimas.*

Demostración. Sean $q = a + v \in \mathbb{H}$ con $a = \Re(q), v = \Im(q)$ y $\alpha \in \mathbb{H}$ tal que $\alpha^n = q$. Sabemos que $\alpha \notin \mathbb{R}$. Por la Proposición 1.15 afirmamos que $\langle\alpha\rangle \cong \mathbb{C}$, y $\langle q\rangle \cong \mathbb{C}$. Como $q = \alpha^n \in \langle\alpha\rangle$ entonces $\langle q\rangle \subseteq \langle\alpha\rangle$ y necesariamente $\langle q\rangle = \langle\alpha\rangle$ por ser isomorfos. Por ello, el cálculo de las raíces de q se reduce al cálculo de raíces en $\mathbb{C}$. Aplicando el Teorema Fundamental del Álgebra concluimos la demostración. □

Teorema 2.31. *Todo real no nulo tiene infinitas raíces n-ésimas en $\mathbb{H}$, excepto si es positivo y $n = 2$.*

Demostración. Comenzamos distinguiendo dos casos:

- Si $n = 2$ debemos resolver $\xi^2 - t = 0$ con $t \in \mathbb{R}$. Como hemos visto en la Sección 2.2:
  - Si $t > 0$ entonces $\xi_0 = \pm\sqrt{t}$. Luego, hay dos raíces reales.
  - Si $t < 0$ hay infinitas raíces cuadradas de la forma $\xi_0 = \sqrt{-t}\omega$ con $\Re(\omega) = 0$ y $|w| = 1$.

- Si $n > 2$ buscamos resolver $\xi^n = t$; por la demostración de la Proposición 2.29 podemos escribir $\xi = |\xi|(\cos\sigma + \omega\operatorname{sen}\sigma)$ con $\Re(\omega) = 0$ y $\sigma \in (0, \pi)$. De nuevo, distinguimos dos subcasos:
  - Si $\xi \in \mathbb{R}$ existen raíces reales de t y son finitas.
  - Si $\xi \notin \mathbb{R}$ podemos escribir $\xi = a + v$, con $v \neq 0$. Además, teniendo en cuenta la Proposición 1.15 $\langle\xi\rangle = \langle 1, v\rangle \cong \mathbb{C}$ y resolvemos en $\mathbb{C}$, de nuevo, utilizando el Teorema Fundamental del Álgebra tenemos n soluciones. Puesto que n se mueve con total libertad concluimos que hay infinitas soluciones. □

Seguidamente, visualicemos cómo calcular las raíces de un cuaternión.

Ejemplo 2.32. Sea $q = \sqrt{6}+\mathbf{i}+\mathbf{j}$. Para hallar las raíces cuartas de q comenzamos calculando $|q| = \sqrt{8}$ y $\sigma = \arctan \frac{\sqrt{2}}{\sqrt{6}} \in (0, \pi)$.
Esto nos lleva a escribir $q = \sqrt{8}(\cos \frac{\pi}{6} + \omega \operatorname{sen} \frac{\pi}{6})$ con $\omega = \frac{\mathbf{i}+\mathbf{j}}{\sqrt{2}}$. Por tanto, las raíces son de la forma:

$$\xi_k = \sqrt[8]{8}\left(\cos\left(\frac{\pi}{6} + \frac{2k\pi}{4}\right) + \omega \operatorname{sen}\left(\frac{\pi}{6} + \frac{2k\pi}{4}\right)\right) \text{ con } k = 0, 1, 2, 3.$$

En las Secciones 2.1, 2.2, 2.3 y 2.4 hemos visto que todas las ecuaciones cuaterniónicas con un único término de grado máximo tienen al menos una solución, esto nos lleva a presentar el siguiente corolario.

Corolario 2.33. *Todo polinomio $p(\xi) \in \mathbb{H}[\xi]$ con un único término de grado máximo tiene al menos una raíz en $\mathbb{H}$.*

Corolario 2.33 corresponde con el Teorema Fundamental del Álgebra en los cuaterniones demostrado por primera vez por Niven y Eilenberg en [9]. Niven también abordó la resolución de ecuaciones quaterniónicas con un único término de grado máximo, como se puede comprobar en [8], obteniendo resultados análogos a los presentados en esta memoria.

2.5. Sistema de ecuaciones lineales de 2 incógnitas

Para los siguiente párrafos nos hemos inspirado en el trabajo [6]. Hasta ahora hemos tratado ecuaciones lineales de distintos grados, veamos cómo abordar el siguiente sistema en las incógnitas x e y.

$$\begin{cases} ayb + cxd = e \\ pyq + rxs = t \end{cases} \quad \text{con } a, b, c, d, e, p, q, r, s, t \in \mathbb{H}. \tag{2.27}$$

Observamos que si $a \neq 0$ ó $b \neq 0$, despejamos x de la primera ecuación de (2.27) y sustituimos en la segunda, obtenemos una única ecuación lineal de grado 1, que sabemos resolver por la Sección 2.1. Supongamos entonces que $a \neq 0 \neq b$. Multiplicando la primera ecuación del sistema (2.27) por $\bar{a}$ a la izquierda y por $\bar{b}$ a la derecha tenemos

$$|a|^2 y |b|^2 + \bar{a}cxd\bar{b} = \bar{a}e\bar{b}.$$

Puesto que por hipótesis a, b son no nulos podemos despejar y en la ecuación anterior y sustituirla en la segunda ecuación de (2.27); obteniendo

$$p\left(\frac{\bar{a}e\bar{b} - \bar{a}cxd\bar{b}}{|a|^2|b|^2}\right) q + rxs = t \text{ entonces } \frac{p\bar{a}e\bar{b}q}{|a|^2|b|^2} - \frac{p\bar{a}cxd\bar{b}q}{|a|^2|b|^2} + rxs = t,$$

es decir,

$$-\frac{p\bar{a}cxd\bar{b}q}{|a|^2|b|^2}+rxs=t-\frac{p\bar{a}e\bar{b}q}{|a|^2|b|^2}$$

lo que equivale a resolver:

$$\alpha x\beta+rxs=\gamma,$$

con $\alpha=-\dfrac{p\bar{a}c}{|a|^2|b|^2}$, $\beta=d\bar{b}q$, $\gamma=t-\dfrac{p\bar{a}e\bar{b}q}{|a|^2|b|^2}$ y $x=x_0+x_1\mathbf{i}+x_2\mathbf{j}+x_3\mathbf{k}\in\mathbb{H}$.

Usando el Lema 1.7,

$$\begin{aligned}\alpha x\beta&=\alpha\Big(\beta x-2\Im(\beta)\Im(x)-2\langle\Im(\beta),\Im(x)\rangle\Big)\\&=\alpha\beta(x_0+\Im(x))-2\alpha\Im(\beta)\Im(x)-2\alpha\langle\Im(\beta)\Im(x)\rangle\\&=\alpha\beta x_0+\Big(\alpha\beta-2\alpha\Im(\beta)\Big)\Im(x)-2\alpha\langle\Im(\beta),\Im(x)\rangle\Big).\end{aligned}$$

De forma análoga, $rxs=rsx_0+\Big(rs-2r\Im(s)\Big)\Im(x)-2r\langle\Im(s),\Im(x)\rangle$.
Se sigue que,

$$\begin{aligned}\alpha x\beta+rxs=\underbrace{(\alpha\beta+rs)}_{\sigma}x_0+&\underbrace{\Big(\Big(\alpha\beta-2\alpha\Im(\beta)+rs-2r\Im(s)\Big)\mathbf{i}-2\alpha\beta_1-2rs_1\Big)}_{\varphi}x_1+\\&+\underbrace{\Big(\Big(\alpha\beta-2\alpha\Im(\beta)+rs-2r\Im(s)\Big)\mathbf{j}-2\alpha\beta_2-2rs_2\Big)}_{\psi}x_2+\\&+\underbrace{\Big(\Big(\alpha\beta-2\alpha\Im(\beta)+rs-2r\Im(s)\Big)\mathbf{k}-2\alpha\beta_3-2rs_3\Big)}_{\phi}x_3=\end{aligned}$$

$$\begin{aligned}&=\Big(\sigma_0+\sigma_1\mathbf{i}+\sigma_2\mathbf{j}+\sigma_3\mathbf{k}\Big)x_0+\Big(\varphi_0+\varphi_1\mathbf{i}+\varphi_2\mathbf{j}+\varphi_3\mathbf{k}\Big)x_1\\&+\Big(\psi_0+\psi_1\mathbf{i}+\psi_2\mathbf{j}+\psi_3\mathbf{k}\Big)x_2+\Big(\phi_0+\phi_1\mathbf{i}+\phi_2\mathbf{j}+\phi_3\mathbf{k}\Big)x_3=\gamma_0+\gamma_1\mathbf{i}+\gamma_2\mathbf{j}+\gamma_3\mathbf{k}.\end{aligned}$$

O de manera equivalente, buscamos resolver el siguiente sistema:

$$\begin{cases}\sigma_0x_0+\varphi_0x_1+\psi_0x_2+\phi_0x_3=\gamma_0\\ \sigma_1x_0+\varphi_1x_1+\psi_1x_2+\phi_1x_3=\gamma_1\\ \sigma_2x_0+\varphi_2x_1+\psi_2x_2+\phi_2x_3=\gamma_2\\ \sigma_3x_0+\varphi_3x_1+\psi_3x_2+\phi_3x_3=\gamma_3.\end{cases}$$

Esto reduce el problema inicial a resolver un sistema real lineal con 4 ecuaciones y 4 incógnitas.

Ilustremos el método descrito con un ejemplo.

Ejemplo 2.34. Calculamos las soluciones del siguiente sistema

$$\begin{cases} (1+2\mathbf{j})y(-\mathbf{i}-\mathbf{k}) + (\mathbf{i}-\mathbf{j})x\mathbf{k} = 2-\mathbf{i}-\mathbf{k} \\ (2\mathbf{i}+3\mathbf{k})y\mathbf{i} + (\mathbf{j}+\mathbf{k})x2\mathbf{j} = -4-3\mathbf{i}+2\mathbf{k}. \end{cases}$$

donde,

$$\begin{array}{lllll} a = 1+2\mathbf{j}, & b = -\mathbf{i}-\mathbf{k}, & c = \mathbf{i}-\mathbf{j}, & d = \mathbf{k}, & e = 2-\mathbf{i}-\mathbf{k}, \\ p = 2\mathbf{i}+3\mathbf{k}, & q = \mathbf{i}, & r = \mathbf{j}+\mathbf{k}, & s = 2\mathbf{j}, & t = 4-3\mathbf{i}+2\mathbf{k}. \end{array}$$

Comenzamos calculando:

$$\begin{aligned} \alpha &= -\frac{p\bar{a}c}{|a|^2|b|^2} = -\frac{(2\mathbf{i}+3\mathbf{k})(1-2\mathbf{j})(\mathbf{i}-\mathbf{j})}{|1+2\mathbf{j}|^2|-\mathbf{i}-\mathbf{k}|^2}, \\ \beta &= d\bar{b}q = \mathbf{k}(\mathbf{i}+\mathbf{k})\mathbf{i}, \\ \gamma &= t - \frac{p\bar{a}e\bar{b}q}{|a|^2|b|^2} = (4-3\mathbf{i}+2\mathbf{k}) - \frac{(2\mathbf{i}+3\mathbf{k})(1-2\mathbf{j})(2-\mathbf{i}-\mathbf{k})(\mathbf{i}+\mathbf{k})\mathbf{i}}{|1+2\mathbf{j}|^2|-\mathbf{i}-\mathbf{k}|^2}. \end{aligned}$$

Por el Lema 1.2 obtenemos que:

$$\alpha = \frac{8+\mathbf{i}+\mathbf{j}+8\mathbf{k}}{10}, \quad \beta = -\mathbf{i}-\mathbf{k}, \quad \gamma = \frac{-24-16\mathbf{i}+2\mathbf{j}+2\mathbf{k}}{10}.$$

Por tanto,

$$\begin{aligned} \alpha x\beta + rxs = &-\frac{1}{10}(11+29\mathbf{i}+7\mathbf{j}+7\mathbf{k})x_0 + \frac{1}{10}(-13+13\mathbf{i}+9\mathbf{j}+9\mathbf{k})x_1 \\ &+ \frac{1}{10}(-7-7\mathbf{i}-29\mathbf{j}-11\mathbf{k})x_2 + \frac{1}{10}(9+9\mathbf{i}-27\mathbf{j}+37\mathbf{k})x_3 \\ &= \frac{1}{10}(25+9\mathbf{i}+5\mathbf{j}+\mathbf{k}). \end{aligned}$$

De manera equivalente esto es,

$$\begin{cases} -11x_0 - 13x_1 - 7x_2 + 9x_3 = -24 \\ -29x_0 + 13x_1 - 7x_2 - 9x_3 = -16 \\ -7x_0 + 9x_1 - 29x_2 - 27x_3 = 2 \\ -7x_0 + 9x_1 - 11x_2 + 37x_3 = 2. \end{cases}$$

Como vemos, hemos reducido el sistema de ecuaciones cuaterniónicas de partida en un sistema lineal real de cuatro ecuaciones y cuatro incógnitas. Resolviendo obtenemos que $x = 1+\mathbf{i}$. Se sigue entonces que

$$y = \frac{\bar{a}e\bar{b} - \bar{a}cxd\bar{b}}{|a|^2|b|^2} = \frac{(1-2\mathbf{j})(2-\mathbf{i}-\mathbf{k})(\mathbf{i}+\mathbf{k}) - (1-2\mathbf{j})(\mathbf{i}-\mathbf{j})(1+\mathbf{i})\mathbf{k}(\mathbf{i}+\mathbf{k})}{10} = \mathbf{k}.$$

3

Teoría de Números

En la primera sección de este capítulo demostraremos el Teorema de los cuatro cuadrados de Lagrange, el cual establece que cualquier entero no negativo se puede expresar como suma de cuatro cuadrados y para ello utilizaremos los cuaterniones de Hurwitz. Niven también trabajó con ellos en [7]. Dedicaremos la segunda sección a introducir la teoría de factorización única en dichos cuaterniones. Para el desarrollo de este capítulo hemos consultado [2] y [12].

3.1. Cuaterniones de Hurwitz

Definición 3.1. *Diremos que $q \in \mathbb{H}$ es un entero de Hurwitz o un cuaternión de Hurwitz si q pertenece al conjunto*

$$\mathcal{H} = \left\{ \frac{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}}{2} \in \mathbb{H} : \begin{array}{c} a_i \in \mathbb{Z} \text{ para todo } 0 \leq i \leq 3 \text{ y} \\ a_0 \equiv a_1 \equiv a_2 \equiv a_3 \pmod 2 \end{array} \right\}.$$

Proposición 3.2. *El conjunto de los enteros de Hurwitz es un subanillo de $\mathbb{H}$.*

Demostración. Por definición $\mathcal{H} \subset \mathbb{H}$. Además, el conjunto de los enteros de Hurwitz es distinto de vacío pues $1 = \frac{2+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}}{2} \in \mathcal{H}$.
Sean $q_1, q_2 \in \mathcal{H}$, es decir, $q_1 = \frac{a_0+a_1\mathbf{i}+a_2\mathbf{j}+a_3\mathbf{k}}{2}$ y $q_2 = \frac{b_0+b_1\mathbf{i}+b_2\mathbf{j}+b_3\mathbf{k}}{2}$, para ciertos $a_i, b_i \in \mathbb{Z}$ con $i \in \{0, \ldots, 3\}$. Tenemos $q_1 - q_2 = \frac{a_0-b_0+(a_1-b_1)\mathbf{i}+(a_2-b_2)\mathbf{j}+(a_3-b_3)\mathbf{k}}{2} \in \mathcal{H}$ pues $a_i - b_i \equiv a_i + b_i \pmod 2$ con $0 \leq i \leq 3$.
Veamos que el producto de $\mathbb{H}$ es ley de composición interna de $\mathcal{H}$. Por Lema 1.2 tenemos que $q_1q_2 = \tilde{a_0} + \tilde{a_1}\mathbf{i} + \tilde{a_2}\mathbf{j} + \tilde{a_3}\mathbf{k} \in \mathcal{H}$ con $\tilde{a_0} = a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3$, $\tilde{a_1} = \tilde{c_1} + a_2b_3 - a_3b_2$, $\tilde{a_2} = \tilde{c_2} + a_3b_1 - a_1b_3$, y $\tilde{a_3} = \tilde{c_3} + a_1b_2 - a_2b_1$ donde $\tilde{c_i} = a_0b_i + a_ib_0$ para $1 \leq i \leq 3$. Además $a_ib_j \equiv a_ib_k$ y $a_ib_j \equiv -a_ib_j \pmod 2$ para $0 \leq i, j, k \leq 3$ pues $b_j \equiv b_k \pmod 2$, luego $\tilde{a_0} \equiv \tilde{a_1} \equiv \tilde{a_2} \equiv \tilde{a_3} \pmod 2$. □

Definición 3.3. *Diremos que $q \in \mathbb{H}$ es un cuaternión de Lipschitz o entero de Lipschitz si todas sus componentes son números enteros, es decir, si q pertenece al conjunto*

$$\mathcal{L} = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H} : a_i \in \mathbb{Z} \text{ para todo } 0 \leq i \leq 3\} \subset \mathcal{H}.$$

Proposición 3.4. *El conjunto de los enteros de Lipschitz es un subanillo de* $\mathcal{H}$.

Demostración. Sea $q \in \mathcal{L}$, luego $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} = \frac{2a_0 + 2a_1\mathbf{i} + 2a_2\mathbf{j} + 2a_3\mathbf{k}}{2} \in \mathcal{H}$, por tanto $\mathcal{L} \subset \mathcal{H}$. Además, el conjunto de los enteros de Lipschitz es distinto de vacío pues $1 = 1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k} \in \mathcal{L}$.
Sean $q_1, q_2 \in \mathcal{L}$, es decir, $q_1 = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ y $q_2 = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$, para ciertos $a_i, b_i \in \mathbb{Z}$ con $0 \leq i \leq 3$.
Tenemos $q_1 - q_2 = a_0 - b_0 + (a_1 - b_1)\mathbf{i} + (a_2 - b_2)\mathbf{j} + (a_3 - b_3)\mathbf{k} \in \mathcal{L}$ pues $a_i - b_i \in \mathbb{Z}$ para todo $i \in \{0, \ldots, 3\}$.
Por otro lado utilizando el Lema 1.2 tenemos que el producto de $\mathbb{H}$ también es ley de composición interna de $\mathcal{L}$. □

Lema 3.5. *El conjunto de los cuaterniones de Hurwitz coincide con el conjunto* $A = \left\{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} + a_4\mathbf{h} \text{ tal que } \mathbf{h} = \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} \text{ y } a_i \in \mathbb{Z} \text{ con } 0 \leq i \leq 4\right\}$.

Demostración. Sea $q = \frac{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}}{2} \in \mathcal{H}$, $a_0 \equiv a_1 \equiv a_2 \equiv a_3$ (mód 2). Si $a_i = 2m_i$, con $m_i \in \mathbb{Z}$ con $0 \leq i \leq 3$ entonces $q = m_0 + m_1\mathbf{i} + m_2\mathbf{j} + m_3\mathbf{k} + 0\mathbf{h} \in A$. En caso contrario $a_i = 2m_i + 1$, con $m_i \in \mathbb{Z}$ para todo $0 \leq i \leq 3$ luego $q = m_0 + m_1\mathbf{i} + m_2\mathbf{j} + m_3\mathbf{k} + 1 \cdot \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} \in A$. Por otra parte, $\mathcal{L} \subset \mathcal{H}$ como hemos visto en la demostración de la Proposición 3.4. Además, $\mathbf{h} \in \mathcal{H}$ puesto que todo elemento de A es de la forma $q + a_4 h$ con $q \in \mathcal{L}$ y $a_4 \in \mathbb{Z}$ se sigue que $A \subset \mathcal{H}$. □

Corolario 3.6. *Todo cuaternión* $q \in \mathcal{H} \setminus \mathcal{L}$ *se expresa de forma única como* $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} + \mathbf{h}$, *donde* $a_i \in \mathbb{Z}$ *para* $i \in \{0, \ldots, 3\}$.

Demostración. Sea $q = \tilde{a_0} + \tilde{a_1}\mathbf{i} + \tilde{a_2}\mathbf{j} + \tilde{a_3}\mathbf{k} + \tilde{a_4}h \in \mathcal{H} \setminus \mathcal{L}$ con $\tilde{a_4} = 2m + 1 \in \mathbb{Z}$, pues si $\tilde{a_4} = 2m$ entonces $q = (\tilde{a_0} + m) + (\tilde{a_1} + m)\mathbf{i} + (\tilde{a_2} + m)\mathbf{j} + (\tilde{a_3} + m)\mathbf{k} \in \mathcal{L}$ lo cual es falso por hipótesis.
Por tanto, $q = \tilde{a_0} + \tilde{a_1}\mathbf{i} + \tilde{a_2}\mathbf{j} + \tilde{a_3}\mathbf{k} + (2m + 1)\mathbf{h} = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} + \mathbf{h}$ donde $a_i = \tilde{a_i} + m$ con $0 \leq i \leq 3$.

Corolario 3.7. *El cuadrado de la norma de cualquier entero de Hurwitz es un número natural.*

Demostración. Si $q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathcal{L}$ entonces $|q|^2 = a_0^2 + a_1^2 + a_2^2 + a_3^2 \in \mathbb{N}$. Si $q \in \mathcal{H} \setminus \mathcal{L}$ por el Corolario 3.6 $q = q_0 + \mathbf{h}$ donde $q_0 \in \mathcal{L}$, multiplicando a ambos lados por $\mathbf{h}^{-1}$ tenemos que $\mathbf{h}^{-1}q = \mathbf{h}^{-1}q_0 + 1$. Tomando $|\cdot|^2$ a ambos lados de la igualdad y aplicando el Lema 1.2 se tiene que $|q|^2 = (a_0 - a_1 - a_2 - a_3 + 1)^2 + (a_1 - a_0 + a_3 - a_3)^2 + (a_2 - a_3 + a_0 + a_1)^2 + (a_3 + a_2 - a_1 + a_0)^2 \in \mathbb{N}$. □

Proposición 3.8. ***(Caracterización de las unidades)***
Sea $q \in \mathcal{H}$ *no nulo,* q *es una unidad en* $\mathcal{H}$ *si y solo si su norma vale 1. En particular, las unidades de* $\mathcal{H}$ *son*

$$\mathcal{H}^* = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}, \pm\mathbf{h}\}.$$

Demostración. Suponemos que q es una unidad en $\mathcal{H}$, es decir, existe $q^{-1} \in \mathcal{H}$ tal que $qq^{-1} = 1$. Tomando $|\cdot|^2$ a ambos lados $|qq^{-1}|^2 = |q|^2|q^{-1}|^2 = 1$, entonces $|q|^2 = \frac{1}{|q^{-1}|^2}$. Por el Corolario 3.7 $|q|^2, |q^{-1}|^2 \in \mathbb{N}$, luego $|q|^2 = 1$, por tanto, $|q| = 1$. Recíprocamente sea $q \in \mathcal{H} \subset \mathbb{H}$. Por el Lema 1.4, el inverso de q es $q^{-1} = \frac{\overline{q}}{|q|^2} = \overline{q} \in \mathcal{H}$. Se sigue que q es una unidad en $\mathcal{H}$. □

Proposición 3.9. *Para cualesquiera $q_1, q_2 \in \mathcal{H}$ no nulos existen $r, s, r', s' \in \mathcal{H}$ tales que*

$$\begin{aligned} q_1 &= sq_2 + r, \quad \textit{donde} \ \ |r|^2 < |q|^2 \quad \textit{(división por la izquierda)} \\ q_1 &= q_2 s' + r', \quad \textit{donde} \ \ |r'|^2 < |q|^2 \quad \textit{(división por la derecha).} \end{aligned}$$

Demostración. Probaremos la división por la izquierda, la demostración para dividir por la derecha es análoga.
Sean $q_1, q_2 \in \mathcal{H} \subset \mathbb{H}$. Como $\mathbb{H}$ es un anillo de división y $q_2 \neq 0$ existe $q_2^{-1} \in \mathbb{H}$ tal que $q_2 q_2^{-1} = 1 \in \mathcal{H}$ pues $\mathcal{H}$ es un subanillo. A continuación, aproximamos cada coeficiente de $q_1 q_2^{-1}$ a su número entero más cercano por redondeo, estos serán los coeficientes de un entero de Lipschitz que denotaremos t.
Definimos $\tilde{r} = q_1 q_2^{-1} - t$. Por construcción las componentes de $\tilde{r}$ pertenecen al intervalo $[-\frac{1}{2}, \frac{1}{2}]$, y tenemos que, $|\tilde{r}|^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$. Obsérvese que si $|\tilde{r}| = 1$ por el Corolario 3.7 sabemos que $\tilde{r}$ es una unidad en el anillo de Hurwitz, por tanto $q_1 q_2^{-1} = \tilde{r} + t \in \mathcal{H}$.
Analizamos dos casos. Si $q_1 q_2^{-1} \in \mathcal{H}$, tomamos $s = q_1 q_2^{-1}$ y $r = 0$, además $0 < |q_2|^2$. Si $q_1 q_2^{-1} \notin \mathcal{H}$, sabemos que $|\tilde{r}| < 1$ tomamos $s = t$ y $r = \tilde{r} q_2$, además, $|r|^2 = |\tilde{r}|^2 |q_2|^2 < |q_2|^2$. □

Consideramos el siguiente ejemplo para ilustrar el algoritmo de división.

Ejemplo 3.10. Calculamos la división por la izquierda de $\frac{11}{2} + \frac{7}{2}\mathbf{i} - \frac{7}{2}\mathbf{j} - \frac{19}{2}\mathbf{k}$ entre $3\mathbf{i} - 4\mathbf{j}$.
Tomamos $q_1 = \frac{11}{2} + \frac{7}{2}\mathbf{i} - \frac{7}{2}\mathbf{j} - \frac{19}{2}\mathbf{k} = 5 + 3\mathbf{i} - 4\mathbf{j} - 10\mathbf{k} + \mathbf{h} \in \mathcal{H}$ y $q_2 = 3\mathbf{i} - 4\mathbf{j} \in \mathcal{L} \subset \mathcal{H}$.
Por el Lema 1.4 sabemos que $q_2^{-1} = \frac{-3\mathbf{i}+4\mathbf{j}}{25}$, luego $q_1 q_2^{-1} = \frac{49}{50} + \frac{43}{50}\mathbf{i} + \frac{101}{50}\mathbf{j} + \frac{7}{50}\mathbf{k} \notin \mathcal{H}$ y $t = 1 + \mathbf{i} + 2\mathbf{j} \in \mathcal{L}$. Se sigue que $\tilde{r} = q_1 q_2^{-1} - t = \frac{1}{50} - \frac{7}{50}\mathbf{i} + \frac{1}{50}\mathbf{j} + \frac{7}{50}\mathbf{k}$.
Aplicando la Proposición 3.9, $s = t = 1 + \mathbf{i} + 2\mathbf{j}$ y $r = \tilde{r}q = \frac{1}{2} + \frac{1}{2}\mathbf{i} + \frac{1}{2}\mathbf{j} + \frac{1}{2}\mathbf{k} = \mathbf{h} \in \mathcal{H}$ además, $|r|^2 = 1 < |q_2|^2 = 25$.
Concluimos que $\frac{11}{2} + \frac{7}{2}\mathbf{i} - \frac{7}{2}\mathbf{j} - \frac{19}{2}\mathbf{k} = (1 + \mathbf{i} + 2\mathbf{j})(3\mathbf{i} - 4\mathbf{j}) + (\frac{1}{2} + \frac{1}{2}\mathbf{i} + \frac{1}{2}\mathbf{j} + \frac{1}{2}\mathbf{k})$.
Obsérvese que $r = \mathbf{h} \notin \mathcal{L}$, esto ilustra por qué en el subanillo $\mathcal{L}$ de $\mathcal{H}$ no podemos definir un algoritmo de división respecto de la $|\cdot|^2$.

El siguiente corolario nos indica que el anillo de los cuaterniones de Hurwitz es un dominio de ideales a la derecha y a la izquierda.

Corolario 3.11.

1. *Todo ideal a la derecha I de $\mathcal{H}$ es de la forma $I = \mathcal{H}a$ para algún $a \in I$.*
2. *Todo ideal a la izquierda J de $\mathcal{H}$ es de la forma $J = b\mathcal{H}$ para algún $b \in J$.*

Demostración. Sea I un ideal a la derecha de $\mathcal{H}$. Si $I = \{0\}$ entonces $a = 0$. Asumimos que $I \neq \{0\}$. Probaremos que $I = \mathcal{H}a$ donde $a \in I$ es tal que $|a|^2 = \text{mín}\{|z|^2 : z \in I\}$. Veamos que $I \supset \mathcal{H}a$. Por la Proposición 3.9, para cualquier $q_1 \in I$ existen $r, s \in \mathcal{H}$ tales que $q_1 = sa + r \in I$ y $|r|^2 < |a|^2$. Además, $r \in I$, pues $q_1 \in I$. De la definición de a tenemos que $r = 0$, es decir, $q_1 = sa$. Por lo tanto, $I \subseteq \mathcal{H}a$.
Como I es un ideal a la derecha y $a \in I$, sabemos que $q_2 a \in I$ para cualquier $q_2 \in \mathcal{H}$, luego $\mathcal{H}a \subset I$. Concluimos que $I = \mathcal{H}a$.
De forma análoga se demuestra cuando J es un ideal a la izquierda. □

Veamos un ejemplo.

Ejemplo 3.12. Consideremos

$$I = \left\{ (a_0 + a_2) + (a_1 + a_3)\mathbf{i} + (a_2 - a_0)\mathbf{j} + (a_3 - a_1)\mathbf{k} \ : \ a_i \in \mathbb{Z},\ 0 \leq i \leq 3 \right\}.$$

El conjunto I es un ideal a la derecha de $\mathcal{H}$. En efecto, $I \subset \mathcal{L} \subset \mathcal{H}$. A su vez, $0 \in I$ pues basta tomar $a_i = 0$ para todo $0 \leq i \leq 3$. Además para cualesquiera $z, w \in I$ y $q \in \mathcal{H}$ se tiene que $z + w \in I$ y $qw \in I$. Veamos que I es un ideal principal, concretamente $I = \mathcal{H}(1 - \mathbf{j})$.
Si $z \in I$ entonces existen $a_i \in \mathbb{Z}$ con $0 \leq i \leq 3$ tales que

$$\begin{aligned} z &= (a_0 + a_2) + (a_1 + a_3)\mathbf{i} + (a_2 - a_0)\mathbf{j} + (a_3 - a_1)\mathbf{k} \\ &= a_0(1 - \mathbf{j}) + a_1(\mathbf{i} - \mathbf{k}) + a_2(1 + \mathbf{j}) + a_3(\mathbf{i} + \mathbf{k}). \end{aligned}$$

Sustituyendo $\mathbf{k} = \mathbf{ij}$, y sacando factor de $\mathbf{i}$ obtenemos que

$$\begin{aligned} z &= (a_0 + a_1\mathbf{i})(1 - \mathbf{j}) + (a_2 + a_3\mathbf{i})(1 + \mathbf{j})(1 - \mathbf{j})^{-1}(1 - \mathbf{j}) \\ &= \Big((a_0 + a_1\mathbf{i}) + (a_2 + a_3\mathbf{i})(1 + \mathbf{j})(1 - \mathbf{j})^{-1} \Big)(1 - \mathbf{j}) \in \mathcal{H}(1 - \mathbf{j}). \end{aligned}$$

Para la segunda inclusión, si $z \in \mathcal{H}(1-\mathbf{j})$ entones $z = (a_0+a_1\mathbf{i}+a_2\mathbf{j}+a_3\mathbf{k})(1-\mathbf{j})$, Por el Lema 1.2 se tiene que $z = (a_0+a_2)+(a_1+a_3)\mathbf{i}+(a_2-a_0)\mathbf{j}+(a_3-a_1)\mathbf{k} \in I$.

Es natural preguntarse si $\mathcal{L}$ también es un dominio de ideales principales a la derecha y a la izquierda, la respuesta es que no. Para ello consideremos el siguiente ejemplo.

Ejemplo 3.13. Consideramos el ideal $\mathcal{L}q_1 + \mathcal{L}q_2$ con $q_1 = 1 + \mathbf{j}$ y $q_2 = 2 - \mathbf{k}$. Veamos por reducción al absurdo que no es un ideal principal.
Suponemos que $\mathcal{L}(1+\mathbf{j})+\mathcal{L}(2-\mathbf{k}) = \mathcal{L}b$ para cierto $b \in \mathcal{L}$. En particular, existen $x, y \in \mathcal{L}$ tales que $1 + \mathbf{j} = xb$ y $2 - \mathbf{k} = yb$, tomando $|\cdot|^2$ en ambas expresiones obtenemos que $2 = |x|^2|b|^2$ y $5 = |y|^2|b|^2$ donde, por el Corolario 3.7, $|x|^2, |b|^2$ y $|y|^2 \in \mathbb{N}$ pues $x, y, b \in \mathcal{L} \subset \mathcal{H}$. Por consiguiente, $|b|^2 = 1$ y se deduce que b es una unidad y por tanto $\mathcal{L}(1 + \mathbf{j}) + \mathcal{L}(2 - \mathbf{k}) = \mathcal{L}$. En particular, existen $a, b \in \mathcal{L}$ tales que $a(1 + \mathbf{j}) + b(2 - \mathbf{k}) = 1$, tomando $|\cdot|^2$ a ambos lados de la igualdad obtenemos que $1 = 2|a|^2 + 5|b|^2$ lo cual es falso pues $|a|^2, |b|^2 \in \mathbb{N}$.

Seguidamente demostramos una serie de resultados que necesitaremos para la prueba del Teorema de Langrange.

Lema 3.14. *Si $\mathsf{p} \in \mathbb{Z}$ es un número primo entonces existe $q = 1 + u_1\mathbf{i} + u_2\mathbf{j} \in \mathcal{L}$ tal que $u_i \not\equiv 0 \pmod{\mathsf{p}}$ con $i = 1, 2$ y $|q|^2 \equiv 0 \pmod{\mathsf{p}}$.*

Demostración. Observemos que demostrar este lema equivale a encontrar $u_i \in \mathbb{Z}$, con $i \in \{1, 2\}$ tales que $u_i \not\equiv 0 \pmod{\mathsf{p}}$ y $1 + u_1^2 + u_2^2 \equiv 0 \pmod{\mathsf{p}}$.
Si $\mathsf{p} = 2$ basta tomar $u_1 = 1$ y $u_2 = 0$, luego asumimos que p es impar. Veamos que los elementos

$$\overline{0}^2, \overline{1}^2, \overline{2}^2, \ldots, \left(\overline{\frac{p-1}{2}}\right)^2 \in \mathbb{Z}_{\mathsf{p}} \tag{3.1}$$

son diferentes dos a dos.
Sean $x, y \in \left\{0, \ldots, \frac{\mathsf{p}-1}{2}\right\} \subseteq \mathbb{Z}$ tales que $\overline{x}^2 = \overline{y}^2$, tenemos que ver que $\overline{x} = \overline{y}$. Como $\overline{x}^2 - \overline{y}^2 = \overline{0}$ sigue que $(\overline{x} - \overline{y})(\overline{x} + \overline{y}) = \overline{0}$ en $\mathbb{Z}_{\mathsf{p}}$. Por hipótesis p es primo luego $\mathbb{Z}_{\mathsf{p}}$ es un cuerpo y por tanto dominio de integridad, $\overline{x} + \overline{y} = \overline{0}$ ó $\overline{x} - \overline{y} = \overline{0}$. Si $\overline{x} + \overline{y} = \overline{0}$ entonces $x + y$ es múltiplo de p lo que implica que necesariamente $\overline{x} = 0 = \overline{y}$. Si $\overline{x} - \overline{y} = \overline{0}$ entonces $\overline{x} = \overline{y}$.

En lo que sigue denotaremos por C al conjunto formado por los elementos de (3.1). Consideramos ahora los siguientes subconjuntos de $\mathbb{Z}_{\mathsf{p}}$:

$$A = \left\{\overline{1} + \overline{0}^2,\ \overline{1} + \overline{1}^2, \ldots, \overline{1} + \left(\overline{\frac{\mathsf{p}-1}{2}}\right)^2\right\} = \overline{1} + C \text{ entonces } \sharp A = \sharp C = \frac{\mathsf{p}+1}{2}$$

$$B = \left\{-\overline{0}^2,\ -\overline{1}^2, \ldots, -\left(\overline{\frac{\mathsf{p}-1}{2}}\right)^2\right\} = -C \text{ entonces } \sharp B = \sharp C = \frac{\mathsf{p}+1}{2}.$$

Obsérvese que $\sharp(A \cup B) = \sharp A + \sharp B - \sharp(A \cap B) = \mathsf{p} + 1 - \sharp(A \cap B)$. Como en $\mathbb{Z}_{\mathsf{p}}$ hay p elementos y $A \cup B \subset \mathbb{Z}_{\mathsf{p}}$ deducimos que $\sharp(A \cap B) \geq 1$, es decir $A \cap B \neq \emptyset$. Luego existen al menos $0 \leq u_1, u_2 \leq \frac{\mathsf{p}-1}{2}$ tales que $1 + u_1^2 \equiv -u_2^2 \pmod{\mathsf{p}}$.
Por lo tanto, concluimos que $1 + u_1^2 + u_2^2 \equiv 0 \pmod{\mathsf{p}}$ y por la definición de u_i sabemos que p no divide a u_i para $i = 1, 2$. □

Proposición 3.15. *El producto de dos números naturales que son sumas de cuatro cuadrados de enteros es de nuevo la suma de cuatro cuadrados de enteros.*

Demostración. Sean $m = |q_1|^2$ y $n = |q_2|^2$ con $q_1, q_2 \in \mathcal{L}$, dos números naturales que son la suma de cuatro cuadrados de enteros, entonces $mn = |q_1 q_2|^2$ es suma de cuatro cuadrados de enteros. □

Recordamos que $q \in \mathcal{H} \setminus \mathcal{H}^*$ no nulo es irreducible en Hurwitz si para cualesquiera $p_1, p_2 \in \mathcal{H}$ tales que $q = p_1 p_2$ se tiene que $p_1 \in \mathcal{H}^*$ ó $p_2 \in \mathcal{H}^*$.

Lema 3.16. *Si $\mathsf{p} \in \mathbb{Z}$ es un número primo impar entonces para ciertos $b, q \in \mathcal{H}$ se tiene que $\mathcal{H}\mathsf{p} \subsetneq \mathcal{H}\mathsf{p} + \mathcal{H}q = \mathcal{H}b \subsetneq \mathcal{H}$.*

Demostración. Del Lema 3.14 existe $q = 1 + u\mathbf{i} + v\mathbf{j} \in \mathcal{L} \subset \mathcal{H}$ tal que p divide a $|q|^2$.
Veamos la primera inclusión. Sabemos que $q \in \mathcal{H}\mathsf{p} + \mathcal{H}q$ pues $q = 0\mathsf{p} + 1q$. Si $q \in \mathcal{H}\mathsf{p}$ entonces $2q \in \mathcal{L}\mathsf{p}$ luego $2 + 2u\mathbf{i} + 2v\mathbf{j} = z\mathsf{p}$ para cierto $z \in \mathcal{L}$, en particular $2 = \Re(z)\mathsf{p} \in \mathbb{Z}$, por tanto p divide a 2 lo cual es falso pues p es primo impar.
Demostraremos la segunda inclusión por reducción al absurdo. Supongamos que $\mathcal{H}\mathsf{p} + \mathcal{H}q = \mathcal{H}$. En particular $1 \in \mathcal{H}\mathsf{p} + \mathcal{H}q$ es decir $1 = k\mathsf{p} + lq$ para ciertos $k, l \in \mathcal{H}$. Se sigue que $lq = 1 - k\mathsf{p}$. Tomando $|\cdot|^2$,

$$|l|^2|q|^2 = |lq|^2 = (1 - k\mathsf{p})(1 - \overline{k}\mathsf{p}) = 1 - (k + \overline{k})\mathsf{p} + k\overline{k}\mathsf{p}^2 = 1 - 2\Re(k)\mathsf{p} + |k|^2\mathsf{p}^2$$

lo que significa $|l|^2|q|^2| \equiv 1 \pmod{\mathsf{p}}$, pero $|q|^2 \equiv 0 \pmod{\mathsf{p}}$, y obtenemos un absurdo.
Puesto que la suma de ideales a derecha es ideal y aplicando el Corolario 3.11 sabemos que, $\mathcal{H}\mathsf{p} + \mathcal{H}q = \mathcal{H}b$ para algún $b \in \mathcal{H}$ con $|b| \neq 1$, de lo contrario b sería unidad y por tanto $\mathcal{H}\mathsf{p} + \mathcal{H}q = \mathcal{H}$ lo cual es falso como hemos visto. □

Proposición 3.17. *Sea $\mathsf{p} \in \mathbb{Z}$ un número primo impar, entonces $\mathsf{p} = |m|^2$ para cierto $m \in \mathcal{H}$.*

Demostración. Por el Lema 3.16 existe $q = 1 + u\mathbf{i} + v\mathbf{j} \in \mathcal{H}$ tal que $\mathcal{H}\mathsf{p} \subsetneq \mathcal{H}\mathsf{p} + \mathcal{H}q \subsetneq \mathcal{H}$. En particular $\mathsf{p} = mb$ para algún $m \in \mathcal{H}$ tal que $|m| \neq 1$, por tanto, p es reducible en el anillo de los enteros de Hurwitz.
Por otro lado, $\mathsf{p} = |m|^2$, pues $\mathsf{p}^2 = |mb|^2 = |m|^2|b|^2$ donde $|m|^2, |b|^2 \neq 1$. □

Lema 3.18. *Para cualquier $m \in \mathcal{H} \setminus \mathcal{L}$ existe $\delta \in \{\frac{\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2}\} \subset \mathcal{H}^*$ tal que $\delta m \in \mathcal{L}$.*

Demostración. Sea $m = \frac{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}}{2} \in \mathcal{H} \setminus \mathcal{L}$. Por definición $a_i \equiv 1 \pmod 2$, para $i \in \{0, \ldots, 3\}$, es decir que todos los coeficientes de m son impares, lo que nos lleva a escribir $a_i = 4\tilde{a}_i + e_i$, con $e_i \in \{\pm 1\}$ y $\tilde{a}_i \in \mathbb{Z}$ para todo $0 \leq i \leq 3$. Por tanto, $m = 2(\tilde{a}_0 + \tilde{a}_1\mathbf{i} + \tilde{a}_2\mathbf{j} + \tilde{a}_3\mathbf{k}) + \frac{e_0 + e_1\mathbf{i} + e_2\mathbf{j} + e_3\mathbf{k}}{2}$. Tomando $\delta = \frac{e_0 - e_1\mathbf{i} - e_2\mathbf{j} - e_3\mathbf{k}}{2}$, tenemos que $m\delta = (\tilde{a}_0 + \tilde{a}_1\mathbf{i} + \tilde{a}_2\mathbf{j} + \tilde{a}_3\mathbf{k})(e_0 - e_1\mathbf{i} - e_2\mathbf{j} - e_3\mathbf{k}) + 1 \in \mathcal{L}$. □

Teorema 3.19. ***(Teorema de los cuatro cuadrados de Lagrange)*** *Todo número entero positivo puede expresarse como suma de cuatro cuadrados enteros.*

Demostración. Por la Proposición 3.15 bastará probar que se cumple para los números primos impares (pues $2 = 1^2 + 1^2 + 0^2 + 0^2$).
Sea p un número primo impar, por la Proposición 3.17 sabemos que $\mathsf{p} = |m|^2$ para cierto $m = \frac{a_0+a_1\mathbf{i}+a_2\mathbf{j}+a_3\mathbf{k}}{2} \in \mathcal{H}$. Si $m \in \mathcal{L}$ hemos concluido pues p es la suma de cuatro cuadrados enteros. Si $m \notin \mathcal{L}$, por el Lema 3.18 existe $\delta \in \mathcal{H}^*$ tal que $m' := m\delta \in \mathcal{L}$ luego $|m'| = |\delta m| = |m|$. □

3.2. Factorización única de los cuaterniones de Hurwitz

En esta sección presentamos cómo obtener una factorización en irreducibles en el anillo de los cuaterniones de Hurwitz logrando cierta unicidad. Además, veremos una caracterización para los elementos irreducibles en $\mathcal{H}$.

Observemos que $10\mathbf{j} + 10\mathbf{k} = 10(\mathbf{j} + \mathbf{k}) = (1 + 3\mathbf{i})(1 - 3\mathbf{i})(\mathbf{j} + \mathbf{k})$. Los coeficientes del primer factor son $(1, 3, 0, 0)$ y los coeficientes del segundo factor son $(1, -3, 0, 0)$. También $10\mathbf{j} + 10\mathbf{k} = (1 + 3\mathbf{j})(1 - 3\mathbf{j})(\mathbf{j} + \mathbf{k})$. En este caso los coeficientes del primer factor son $(1, 0, 3, 0)$ y los coeficientes del segundo factor son $(1, 0, -3, 0)$. Diremos que dos descomposiciones son *equivalentes por recombinación* si una se obtiene de la otra por recombinación de los coeficientes factor a factor respetando el orden. Es decir, recombinando los coeficientes $(1, 3, 0, 0)$ podemos obtener los coeficientes $(1, 0, 3, 0)$. De manera análoga repetimos el procedimiento con el segundo factor.
Por tanto, $10\mathbf{j} + 10\mathbf{k} = (1 + 3\mathbf{i})(1 - 3\mathbf{i})(\mathbf{j} + \mathbf{k}) = (1 + 3\mathbf{j})(1 - 3\mathbf{j})(\mathbf{j} + \mathbf{k})$. son dos descomposiciones equivalentes por recombinación.
Para evitar esta situación presentamos los cuaterniones primitivos, posteriormente extenderemos la teoría para cuaterniones no primitivos.

Definición 3.20. *Diremos que $q \in \mathcal{H}$ es primitivo si sus coeficientes son coprimos, es decir, si no existen $m \in \mathbb{Z}, m > 1$ y $q' \in \mathcal{H}$ tales que $q = mq'$. En caso contrario diremos que m divide a q.*

A continuación demostramos una serie de resultados que nos serán útiles para lograr la *factorización única* de los cuaterniones de Hurwitz.

Lema 3.21. *Sean $q_1, q_2, q_3 \in \mathcal{H}$ tales que $|q_2|^2 = \mathsf{p}$ número primo de $\mathbb{Z}$. Si p divide a $q_1q_2q_3$ y p no divide a q_1q_2 entonces p divide a q_2q_3.*

Demostración. Consideramos los ideales a derecha $\mathcal{H}\mathsf{p}$ y $\mathcal{H}q_1q_2$. Por el Corolario 3.11 existe $\alpha \in \mathcal{H}\mathsf{p} + \mathcal{H}q_1q_2$ tal que $\mathcal{H}\mathsf{p} + \mathcal{H}q_1q_2 = \mathcal{H}\alpha$. En particular $\mathsf{p} = q\alpha$

para algún $q \in \mathcal{H}$, entonces $|\alpha|^2$ divide a p^2. Puesto que por hipótesis p es un número primo se sigue que $|\alpha|^2 = 1, \mathsf{p}^2$ ó p.
Caso 1: si $|\alpha|^2 = \mathsf{p}^2$, puesto que $\mathsf{p} = q\alpha$ tomando $|\cdot|^2$ a ambos lados de la igualdad $\mathsf{p}^2 = |q|^2\mathsf{p}^2$, luego $q \in \mathcal{H}^*$. Por consiguiente $\alpha \in \mathcal{H}\mathsf{p}$ y en particular $q_1, q_2 \in \mathcal{H}\mathsf{p}$, de donde se deduce que, p divide a q_1q_2 lo cual es una contradicción.
Caso 2: si $|\alpha|^2 = 1$ entonces α es una unidad de $\mathcal{H}$ y $\mathcal{H}\mathsf{p} + \mathcal{H}q_1q_2 = \mathcal{H}$. En particular, existen $x, y \in \mathcal{H}$ tales que $x\mathsf{p} + yq_1q_2 = 1$, luego $yq_1q_2 = 1 - x\mathsf{p}$. Tomando $|\cdot|^2$ a ambos lados de la igualdad obtenemos $|yq_1q_2|^2 = |1 - x\mathsf{p}|^2$, es decir $|yq_1|^2\mathsf{p} = |1 - x\mathsf{p}|^2$ y por tanto, $|1 - x\mathsf{p}|^2 \equiv 0$ (mód p). Es decir si $x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ entonces $(1 - x_0\mathsf{p})^2 + (x_1\mathsf{p})^2 + (x_2\mathsf{p})^2 + (x_3\mathsf{p})^2 = z\mathsf{p}$ para algún $z \in \mathbb{Z}$. Operando obtenemos que $1 = (2x_0 - x_0^2\mathsf{p} - x_1^2\mathsf{p} - x_2^2\mathsf{p} - x_3^2\mathsf{p})\mathsf{p} \in \mathbb{Z}$, lo cual es falso pues p es un número primo de $\mathbb{Z}$ y no divide a 1.
Se sigue entonces que $|\alpha|^2 = \mathsf{p}$. Por otra parte, puesto que $\mathcal{H}\mathsf{p} + \mathcal{H}q_1q_2 = \mathcal{H}\alpha$ existen $x, y \in \mathcal{H}$ tales que $x\mathsf{p} + yq_1q_2 = \alpha$, sustituyendo $\mathsf{p} = \overline{q_2}q_2$ y sacando factor común obtenemos $(x\overline{q_2} + yq_1)q_2 = \alpha$. Como $|\alpha|^2 = \mathsf{p} = |q_2|^2$ entonces $|x\overline{q_2} + y\overline{q_1}|^2 = 1$ y deducimos que $x\overline{q_2} + yq_1 = u \in \mathcal{H}^*$. Luego $x\mathsf{p} + yq_1q_2 = uq_2$, multiplicando a ambos lados por q_3 y aplicando que p divide a $q_1q_2q_3$ llegamos a que p divide a uq_2q_3. Pero p no divide a u, si lo hiciera $\lambda\mathsf{p} = u$ para cierto $\lambda \in \mathcal{H}$ y tomando $|\cdot|^2$ a ambos lados se obtendría que $|\lambda|^2\mathsf{p}^2 = |u|^2 = 1$. Por tanto, p dividiría a 1 lo cual es absurdo.
Concluimos que p no divide a u y por hipótesis p divide a $q_1q_2q_3$, por tanto p divide a q_2q_3. □

Lema 3.22. *Sean $m \in \mathbb{Z}$ y $q_1, q_2 \in \mathcal{H}$. Si m divide a q_1q_2 y $mcd(m, \overline{q_1}q_1) = 1$ entonces m divide a q_2.*

Demostración. Por la identidad de Bézout existen $r, s \in \mathbb{Z}$ tales que $rm + s\overline{q_1}q_1 = 1$. Multiplicando a ambos lados por q_2 obtenemos $rmq_2 + s\overline{q_1}q_1q_2 = q_2$. Por hipótesis esto es $rmq_2 + s\overline{q_1}mt = q_2$, para cierto $t \in \mathcal{H}$, es decir, $m(rq_2 + s\overline{q_1}t) = q_2$ luego m divide a q_2. □

Corolario 3.23. *Sean $\mathsf{p}_1, \mathsf{p}_2$ dos números enteros coprimos distintos. Si p_1 divide a $q \in \mathcal{H}$ y p_2 divide a q entonces $\mathsf{p}_1\mathsf{p}_2$ divide a q.*

Demostración. Sea $q = \mathsf{p}_1\alpha$ para algún $\alpha \in \mathcal{H}$. Por hipótesis p_2 divide a $\mathsf{p}_1\alpha$. Además $mcd(\mathsf{p}_2, \mathsf{p}_1^2) = 1$ pues p_2 y p_1 son coprimos. Por el Lema 3.22 sabemos que p_2 divide a α, en otras palabras, existe $\beta \in \mathcal{H}$ tal que $\mathsf{p}_2\beta = \alpha$; multiplicando a ambos lados por p_1 obtenemos $\mathsf{p}_1\mathsf{p}_2\beta = \mathsf{p}_1\alpha = q$, finalmente concluimos que $\mathsf{p}_1\mathsf{p}_2$ dividen a q. □

Definición 3.24. *Diremos que $q_1, q_2 \in \mathcal{H}$ son coprimos si $mcd(|q_1|^2, |q_2|^2) = 1$.*

Corolario 3.25. *Sean $q_1, q_2 \in \mathcal{H}$. Si q_1 y q_2 son primitivos y coprimos entonces q_1q_2 es primitivo.*

Demostración. Supongamos por reducción al absurdo, que q_1q_2 no es primitivo. Entonces existen $q \in \mathcal{H}$ y $m \in \mathbb{Z}$ tales que $q_1q_2 = mq$, luego $|q_1|^2|q_2|^2 = m^2|q|^2$. Por hipótesis q_1 y q_2 son coprimos en $\mathcal{H}$, es decir no existe ningún $m \in \mathbb{Z} \setminus \{\pm 1\}$ que divida a $|q_i|^2$ simultáneamente con $i = 1, 2$. Si m no divide a q_1 obtenemos que m divide a q_2 lo cual es absurdo pues q_2 es primitivo por hipótesis, análogamente si m no divide a q_2 llegamos a que m divide a q_1 lo cual es falso, pues q_1 es primitivo. □

Lema 3.26. *Sean $q_1, q_2, q_1', q_2' \in \mathcal{H} \setminus \mathcal{H}^*$ tales que $|q_i|^2 = |q_i'|^2$ con $i = 1, 2$ y $q_1q_2 = q_1'q_2'$. Si q_1 y q_2 son coprimos entonces existe $u \in \mathcal{H}^*$ tal que $q_2' = uq_2$.*

Demostración. Sea $m := |q_2|^2 = q_2\overline{q_2}$. Por hipótesis $q_1q_2 = q_1'q_2'$, multiplicando por $\overline{q_2}$ obtenemos $q_1m = q_1'q_2'\overline{q_2}$, es decir que m divide a $q_1'q_2'\overline{q_2}$. Además, $mcd(|q_1'|^2, m) = mcd(|q_1|^2, m) = 1$. Aplicando el Lema 3.22 sabemos que m divide a $q_2'\overline{q}_2$, en otras palabras $q_2'\overline{q_2} = um = uq_2\overline{q}_2$ para cierto $u \in \mathcal{H}$. Es decir, $q_2' = uq_2$ de donde deducimos que $u \in \mathcal{H}^*$ pues $|q_2|^2 = |q_2'|^2 = |u|^2|q_2|^2$ y por tanto necesariamente $|u|^2 = 1$. □

Definición 3.27. *Diremos que $q \in \mathcal{H}$ admite una factorización en irreducibles si existen $q_1, \ldots, q_n \in \mathcal{H}$ irreducibles tales que $q = q_1 \ldots q_n$.*
Diremos que la factorización es única salvo unidad migratoria si de existir otra factorización es de la forma

$$q = q_1'q_2' \cdots q_{n-1}'q_n' = q_1u_1^{-1}u_1q_2 \cdots q_{n-1}u_{n-1}^{-1}u_{n-1}q_n,$$

con $q_1' = q_1u_1^{-1}$, $q_i' = u_{i-1}q_iu_i^{-1}$, $q_n' = u_{n-1}q_n$ y $u_i \in \mathcal{H}^*$, donde $2 \leq i \leq n-1$.

Teorema 3.28. *Sea $q \in \mathcal{H}$ un elemento primitivo. Si $|q|^2 = \mathsf{p}_1 \cdots \mathsf{p}_n$ es una factorización en números primos en $\mathbb{Z}$ donde importa el orden de escritura, entonces existen $q_1, \ldots, q_n \in \mathcal{H}$ irreducibles tales que $q = q_1 \cdots q_n$ es una factorización en irreducibles única salvo unidad migratoria con $|q_i|^2 = \mathsf{p}_i$, $1 \leq i \leq n$.*

Demostración. Comenzamos probando la existencia de la factorización de q por inducción sobre n. Para $n = 1$, basta tomar $q_i = q$. Suponemos cierto para $n-1$. Veamos que si es cierto para n.
Por hipótesis $|q|^2 = \mathsf{p}_1 \cdots \mathsf{p}_n$ luego p_n divide a $|q|^2$. Por el Corolario 3.11 sabemos que $\mathcal{H}\mathsf{p}_n + \mathcal{H}q = \mathcal{H}\alpha$ es un ideal principal por la derecha. De la demostración del Lema 3.21 tenemos que $|\alpha|^2 = \mathsf{p}_n$. Tomando $q_n := \alpha$ afirmamos que es un factor por la derecha de q, esto es $q = q'q_n$ donde necesariamente q' es primitivo, ya que q' por la hipótesis de inducción es un producto de primitivos.
Concluimos que $q = q_1 \cdots q_n$ donde $|q_i|^2 = \mathsf{p}_i$.

Probaremos la unicidad de la factorización por inducción sobre n. Para $n = 1$ se cumple por construcción. Veamos para $n = 2$. Supongamos $q = q_1q_2 = q_1'q_2'$ con $|q_i|^2 = |q_i'|^2$, $i = 1, 2$. Entonces $q_1q_2\overline{q}_2 = q_1\mathsf{p}_2 = q_1'q_2'\overline{q}_2'$, es decir p_2 divide a $q_1'q_2'\overline{q}_2'$.

Teniendo en cuenta la primitividad de q y aplicando el Lema 3.21 sabemos que p_2 divide a $q_2'\overline{q_2'}$.
Además, $q_2'\overline{q_2} = u\mathsf{p}_2 = uq_2\overline{q_2}$ luego $q_2' = uq_2$ y $q_1' = uq_1$ con $u \in \mathcal{H}^*$. Suponemos cierto para $n-1$. Demostremos para n.
Supongamos $q = q_1 \cdots q_n = q_1' \cdots q_n'$ tal que $|q_i|^2 = |q_i'|^2 = \mathsf{p}_i$ con $0 \leq i \leq n$. Por tanto, $q_1 \cdots q_n\overline{q}_n = q_1' \cdots q_n'\overline{q}_n$, luego p_n divide a $(q_1' \cdots q_{n-1}')q_n'\overline{q}_n$. Además, p no divide a $q_1' \cdots q_{n-1}'$, de lo contrario $q = \mathsf{p}xq_n'$ para cierto $x \in \mathcal{H}$ lo cual es falso pues q es primitivo. De nuevo, nos encontramos bajo las hipótesis del Lema 3.21 por tanto p_n divide a $q_n'\overline{q}_n$.
Como p_n no divide $q = q_1' \cdots q_{n-1}'q_n'$ pues q es primitivo obtenemos que $q_n'\overline{q}_n = u\mathsf{p}_n = \mu q_n\overline{q}_n$ para algún $\mu \in \mathcal{H}$. Se sigue que $\mathsf{p}_n' = \mu\mathsf{p}_n$ con $\mu \in \mathcal{H}^*$. Tomando $u_{n-1} = \mu$ hemos probado que $\mathsf{p}_n' = u_{n-1}\mathsf{p}_n$. Recapitulando,

$$q_1 \cdots q_n = q_1' \cdots q_n' = q_1 \cdots q_{n-1}'u_{n-1}\mathsf{p}_n.$$

Por la hipótesis de inducción existen $u_i \in \mathcal{H}^*$ tales que $q_i' = u_{i-1}q_iu_i^{-1}$ con $2 \leq i \leq n-1$ y $q_1' = q_1u_1^{-1}$. □

Ilustremos con un ejemplo el resultado del Teorema 3.28.

Ejemplo 3.29. Veamos cómo factorizar en irreducibles $q = 1 + \mathbf{i} + 2\mathbf{j}$.
Obsérvese que q es primitivo pues sus coeficientes son coprimos. Además $|q|^2 = 6 = 3 \cdot 2$. El Teorema 3.28 nos proporciona un método para encontrar $q_1, q_2 \in \mathcal{H}$ tales que $q = q_1q_2$ es una factorización en irreducibles con $|q_1|^2 = 3$ y $|q_2|^2 = 2$.
Por el Corolario 3.11 sabemos que el ideal $\mathcal{H}2 + \mathcal{H}(1 + \mathbf{i} + 2\mathbf{j}) \subset \mathcal{H}$ es un ideal principal, generado por $\alpha \in \mathcal{H}2 + \mathcal{H}(1 + \mathbf{i} + 2\mathbf{j})$ tal que $|\alpha|^2 = \text{mín}\{|z|^2 : z \in \mathcal{H}2 + \mathcal{H}(1 + \mathbf{i} + 2\mathbf{j})\}$. La demostración del Lema 3.21 nos indica que $|\alpha|^2 = 2$.
Podemos tomar $\alpha = 1 + \mathbf{i} = -\mathbf{j}2 + 1(1 + \mathbf{i} + 2\mathbf{j}) \in \mathcal{H}2 + \mathcal{H}(1 + \mathbf{i} + 2\mathbf{j})$. También podemos tomar $\alpha = \mathbf{j} - \mathbf{k} = 1 \cdot 2 + \mathbf{j}(1 + \mathbf{i} + 2\mathbf{j}) \in \mathcal{H}2 + \mathcal{H}(1 + \mathbf{i} + 2\mathbf{j})$, es decir, $\alpha = \mathbf{j}(1 + \mathbf{i})$. En general, $\alpha = u(1 + \mathbf{i})$ con $u \in \mathcal{H}^*$. Tal y como nos muestra el Teorema 3.28 esto provocará diferentes factorizaciones en irreducibles equivalentes por la unidad migratoria u.
Para simplificar nuestros cálculos tomamos $u = 1$. Se sigue que $q_2 = \alpha = 1 + \mathbf{i}$. Por tanto $q_1 = qq_2^{-1} = (1 + \mathbf{i} + 2\mathbf{j})(1 + \mathbf{i})^{-1}$. Por el Lema 1.7 y el Lema 1.4 obtenemos que $q_1 = 1 + \mathbf{j} + \mathbf{k}$.
Por el Teorema 3.28 concluimos que $q = (1 + \mathbf{j} + \mathbf{k})(1 + \mathbf{i})$ es una factorización en irreducibles.

Para corroborar que efectivamente $(1 + \mathbf{j} + \mathbf{k})$ y $(1 + \mathbf{i}) \in \mathcal{H}$ son elementos irreducibles presentamos la siguiente caracterización de los elementos irreducibles en $\mathcal{H}$ con el siguiente corolario.

Corolario 3.30. *Sea $q \in \mathcal{H} \setminus \mathcal{H}^*$, q es irreducible si y solo si $|q|^2 = \mathsf{p}$, para algún p número primo.*

Demostración. Supongamos que $|q|^2 \in \mathbb{N}$ no es un entero primo, entonces la factorización en primos de $|q|^2$ tiene al menos dos factores. Aplicando el Teorema 3.28 se sigue que q admite al menos una factorización como producto de dos irreducibles, luego q no es irreducible.
Para la otra implicación procedemos por reducción al absurdo. Suponemos que q no es irreducible, es decir existen $q_1, q_2 \in \mathcal{H} \setminus \mathcal{H}^*$ tales que $q = q_1 q_2$, tomando $|\cdot|^2$ obtenemos que $\mathsf{p} = |q_1|^2|q_2|^2$. Por hipótesis p es un número primo luego $|q_i|^2 = 1$, para algún $i = 1, 2$. Por la Proposición 3.8 tenemos $q_i \in \mathcal{H}^*$ lo cual es absurdo. □

Recordamos que $q \in \mathcal{H} \setminus \mathcal{H}^*$ no unidad es un elemento primo en $\mathcal{H}$ si para cualesquiera $x, y \in \mathcal{H}$ tales que q divide a xy entonces q divide a x ó q divide a y.

Aunque $\mathcal{H}$ es un anillo con división euclídea a derecha y a izquierda como hemos visto en la Proposición 3.9 y aunque los ideales a derecha y a izquierda son principales, según hemos demostrado en el Corolario 3.11, ser elemento primo y ser elemento irreducible no es equivalente en el anillo $\mathcal{H}$, como muestra el siguiente ejemplo:

Ejemplo 3.31. Sean $q = -1 + \mathbf{i} - \mathbf{j} - 2\mathbf{k}$, $x = \frac{2+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}$, $y = 1 + \mathbf{i} \in \mathcal{H}$. Por el Corolario 3.30 sabemos que q es irreducible pues $|q|^2 = 1 + 1 + 1 + 2^2 = 7$. Además q divide por la izquierda a xy pues $q = (\mathbf{j} - \mathbf{k})xy$.
Por el Lema 1.2 tenemos que:

$$x^{-1} = \frac{\overline{x}}{|x|^2} = \frac{2(2 - \mathbf{i} - \mathbf{j} - \mathbf{k})}{7} \quad \text{y} \quad y^{-1} = \frac{1 - \mathbf{i}}{2}.$$

Veamos que q no es primo en $\mathcal{H}$

$$qx^{-1} = \frac{2(-4 + 2\mathbf{i} + 2\mathbf{j} - 5\mathbf{k})}{7} \notin \mathcal{L}, \qquad qy^{-1} = \frac{2\mathbf{i} + \mathbf{j} - 3\mathbf{k}}{2} \notin \mathcal{L},$$
$$x^{-1}q = \frac{2(-4 + 4\mathbf{i} - 4\mathbf{j} - \mathbf{k})}{7} \notin \mathcal{L}, \qquad y^{-1}q = \frac{2\mathbf{i} - 3\mathbf{j} - \mathbf{k}}{2} \notin \mathcal{L}.$$

Como q no divide por la izquierda ni por la derecha a x ni a y concluimos que q no es primo.

Observación 3.32. En el Ejemplo 3.29 obtenemos una factorización en irreducibles para $q = 1 + \mathbf{i} + 2\mathbf{j} = (1 + \mathbf{j} + \mathbf{k})(1 + \mathbf{i})$. ¿Es esta una factorización única salvo unidad migratoria? La respuesta es que no pues $|q|^2 = 6 = 3 \cdot 2 = 2 \cdot 3$. Si aplicamos el Teorema 3.28 buscando $q_1, q_2 \in \mathcal{H}$ tales que $q = q_1 q_2$ con $|q_1|^2 = 2$ y $|q_2|^2 = 3$ obtenemos por ejemplo que $q = (\mathbf{j} + \mathbf{k})(1 + \mathbf{i} - \mathbf{j})$. Además estas dos factorizaciones son diferentes pues $1 + \mathbf{j} + \mathbf{k} \neq u(\mathbf{j} + \mathbf{k})$ para cualquier $u \in \mathcal{H}^*$. Si fuesen iguales tomando $|\cdot|^2$ a ambos lados de la igualdad obtendríamos $3 = 2$ lo cual es absurdo.
Tampoco estas factorizaciones en irreducibles son equivalentes por recombinación pues $1 + \mathbf{j} + \mathbf{k}$ no tiene el mismo número de coeficientes no nulos que $\mathbf{j} + \mathbf{k}$.

Para poder justificar completamente la unicidad en la factorización necesitamos introducir los conceptos que se presentan a continuación.

Definición 3.33. *Diremos que $q_1, q_2 \in \mathcal{H}$ cumplen la condición de meta-conmutación si existen $q_1', q_2' \in \mathcal{H}$ tales que $|q_1|^2 = |q_1'|^2 = \mathsf{p}_1$ y $|q_2|^2 = |q_2'|^2 = \mathsf{p}_2$ son números primos y $q_1 q_2 = q_2' q_1'$.*
Además diremos que $q_1 q_2$ es modelado por $\mathsf{p}_1\mathsf{p}_2$.

Corolario 3.34. *Sean $q_1, q_2 \in \mathcal{H}$ tales que $|q_1 q_2|^2 = \mathsf{p}_1\mathsf{p}_2$ donde p_1 y p_2 son primos distintos con $|q_1|^2 = \mathsf{p}_1$ y $|q_2|^2 = \mathsf{p}_2$. Entonces $q_1 q_2$ es modelado por $\mathsf{p}_1\mathsf{p}_2$ de forma única salvo unidad migratoria.*

Demostración. Obsérvese que q_1, y q_2 son primitivos. De lo contrario $q_i = m_i q_i'$ con $m_i \in \mathbb{Z}$, $m > 1$ donde $i = 1, 2$. Tomando $|\cdot|^2$ a ambos lados de la igualdad obtenemos que $\mathsf{p}_i = m_i^2 |q_i'|^2$. Es decir m_i^2 divide a p, lo cual es una contradicción pues p es primo en $\mathbb{Z}$.
Por el Corolario 3.25 $q_1 q_2$ es primitivo, basta aplicar el Teorema 3.28 a $q_1 q_2$. □

Definición 3.35. *Diremos que se produce una fusión si dado p un entero primo tal que p divide a $q_1 \cdots q_n$ entonces p divide a $q_{i-1} q_i$, es decir, si $q_i = \overline{q}_{i-1} u$ donde $u \in \mathcal{H}^*$ para todo $2 \leq i \leq n$.*

¿Es posible a partir de una meta-conmutación obtener una fusión? El siguiente ejemplo da respuesta negativa a nuestra pregunta.

Ejemplo 3.36. Sean $q_1, q_2 \in \mathcal{H}$ tales que $|q_1|^2 = \mathsf{p}_1$ $|q_2|^2 = q_2\overline{q_2} = \mathsf{p}_2$ y $q_1 q_2 \overline{q_2}$ es una factorización modelada por $\mathsf{p}_1\mathsf{p}_2^2$.
Por la condición meta-conmutación podemos factorizar $q_1 q_2$ como $q_2' q_1'$ modelado por $\mathsf{p}_2\mathsf{p}_1$. Luego la factorización $q_2' q_1' q_2$ modelada por $\mathsf{p}_2\mathsf{p}_1\mathsf{p}_2$ no permite una fusión.

Definición 3.37. *Diremos que $q \in \mathcal{H}$ es un p-puro si $|q|^2 = \mathsf{p}^n$ con p número primo para algún $n \in \mathbb{Z}^+$.*

Proposición 3.38. *Si $q \in \mathcal{H}$ es un p-puro para algún $n \in \mathbb{Z}^+$ y p divide a $q = q_1 \cdots q_n$ entonces existe una fusión.*

Demostración. Si p divide a $q_{n-1} q_n$ hemos acabado. En caso contrario llamamos i al menor índice tal que p no divide a $q_i \cdots q_n$ (al menos $i \geq 2$). Por tanto, p divide a $q_{i-1} q_i \cdots q_n$ y p no divide a $q_i \ldots q_n$. Aplicando el Lema 3.21 p divide a $p_{i-1} p_i$ para todo $2 \leq i \leq n$. □

Lema 3.39. *Sean $q, q_1, q_1', \ldots, q_n, q_n' \in \mathcal{H}$ tales que $q = q_1 \ldots q_n = q_1' \ldots q_n'$ donde $|q_i|^2 = |q_i'|^2$ para todo $i = 1, \ldots, n$. Si $mcd(|q_j|^2, |q_n|^2) = 1$ con $1 \leq j \leq n$, entonces existen $u_i \in \mathcal{H}^*$ tales que $q_i' = u_i q_i$ para todo $i = 1, \ldots, n$.*

Demostración. Por inducción sobre n. Si $n = 1$ basta tomar $u = 1$. Supongamos cierto para n. Veamos si es cierto para $n+1$.
Si $q_1 \dots q_{n-1}(q_n q_{n+1}) = q'_1 \dots q'_{n-1}(q'_n q'_{n+1})$, por la hipótesis de inducción $q'_i = u_i q_i$ con $i = 1, \dots, n-1$ y $q'_n q'_{n+1} = u_n q_n q_{n+1}$ con $u_i \in \mathcal{H}^*$ para todo $i = 1, \dots, n$. Multiplicando por u_n^{-1} a ambos lados obtenemos que $u_n^{-1} q'_n q'_{n+1} = q_n q_{n+1}$. Por el Lema 3.26 sabemos que existe $\tilde{u} \in \mathcal{H}^*$ tal que $c = \tilde{u}^{-1} u_n^{-1} q'_n$ y $q_{n+1} = \tilde{u} q'_{n+1}$. Tomando $|\cdot|^2$ obtenemos $|q_n|^2 = |q'_n|^2 = |(u_n \tilde{u})^{-1} q'_n|^2$, entonces $u_n \tilde{u} \in \mathcal{H}^*$, multiplicando por $u_n \tilde{u}$ a ambos lados, $u_n \tilde{u} q_n = q'_n$. Concluimos que $q'_i = u_i q_i$ para todo $0 \leq i \leq n+1$. □

Definición 3.40. *Sean $q \in \mathcal{H}$ no unidad y $\mathsf{p}_1^{k_1} \cdots \mathsf{p}_n^{k_n} \in \mathbb{Z}$ con $\mathsf{p}_1 < \mathsf{p}_n$ donde p_i entero primo y $k_i \in \mathbb{Z}^+$ para $1 \leq i \leq n$. Diremos que $|q|^2 = \mathsf{p}_1^{k_1} \cdots \mathsf{p}_n^{k_n} \in \mathbb{Z}$ es el modelo estándar de q.*

Definición 3.41. *Diremos que $q \in \mathcal{H} \setminus \mathcal{H}^*$ admite una factorización en bloques si $q = q_1 \cdots q_n$ donde cada $q_i \in \mathcal{H}$ es un p_i-puro y $|q_i|^2 = \mathsf{p}_i^{k_i}$, con $i = 1, \dots, n$.*

Observación 3.42. Para cualquier factorización de $q \in \mathcal{H}$ modelada en el modelo estándar, podemos asociar la factorización en bloques, para ello basta muliplicar todos aquellos factores cuya norma sea p_i y al producto lo denotaremos por q_i.

Observación 3.43. Dadas dos factorizaciones de $q \in \mathcal{H}$ en bloques modeladas en el modelo estándar están relacionadas por el Lema 3.39 y por ello, diremos que las factorizaciones modeladas en el modelo estándar son iguales salvo unidad de migración.

Definición 3.44. *Sea $\mathsf{p} \in \mathbb{Z}$ un número primo tal que $\mathsf{p} = |q_1|^2 = q_1 \overline{q_1} = |q_2|^2 = q_2 \overline{q_2}$ para ciertos $q_1, q_2 \in \mathcal{H}$. Diremos que $q_1 \overline{q_1} u_1$ es una recombinación de $q_2 \overline{q_2} u_2$ donde $u_1, u_2 \in \mathcal{H}^*$ que denotaremos por $q_1 \overline{q_1} u_1 \leftrightarrow q_2 \overline{q_2} u_2$.*

Lema 3.45. *Sea $q \in \mathcal{H}$ es un $\mathsf{p}-$puro tal que $q = q_1 \dots q_n$ es una factorización en irreducibles si p divide a q, entonces p divide a $q_1 q_2$.*

Demostración. Por inducción sobre n. Para $n = 2$ se tiene $q = q_1 q_2$. Como p divide a q se sigue que p divide a $q_1 q_2$. Suponemos que es cierto para $n-1$. Veamos que es cierto para n.
Si $q = (q_1 \cdots q_{n-1}) q_n$ podemos asumir que p no divide a $q_1 \cdots q_{n-1}$ pues en caso contrario concluimos que es cierto aplicando la hipótesis de inducción. Además puesto que q no divide a $(q_1 \cdots q_{n-2}) q_{n-1}$, aplicando el Lema 3.21 sabemos que p divide a $q_{n-1} q_n$, es decir existe $e \in \mathcal{H} \subset \mathbb{H}$ tal que $e\mathsf{p} = q_{n-1} q_n$. Por el Lema 1.4 existe $e^{-1} \in \mathbb{H}$ tal que $e e^{-1} = 1$, multiplicando a la derecha por e^{-1} obtenemos que $\mathsf{p} = e^{-1} q_{n-1} q_n = \overline{q_n} q_n$ puesto que q es $\mathsf{p} - puro$ y q_n irreducible; de donde se deduce que $e^{-1} q_{n-1} \in \mathcal{H}$, por tanto e es unidad en $\mathcal{H}$.
Luego,

$$q = q_1 \cdots q_{n-2}q_{n-1}q_n = q_1 \cdots \underbrace{q_{n-2}e}_{q'_{n-2}} \underbrace{e^{-1}q_{n-1}}_{\overline{q_n}} q_n = q_1 \cdots q'_{n-2}\overline{q'_{n-2}}q'_{n-2}$$

Obsérvese que estamos realizando una unidad migratoria y la recombinación $\overline{q_n}q_n \leftrightarrow \overline{q'_{n-2}}q'_{n-2}$. Tomamos $z := q'_{n-2}\overline{q'_{n-2}}$. Como p divide a q sabemos que p divide a $q_1 \cdots q_{n-1}z$. Hemos reducido al caso $n-1$ y aplicando la hipótesis de inducción concluimos que p divide a q_1q_2. □

Proposición 3.46. *Si $q \in \mathcal{H}$ es $\mathsf{p}-$puro tal que $|q|^2 = \mathsf{p}^n, n \in \mathcal{Z}^+$ entonces dadas dos factorizaciones $q = q_1 \cdots q_n = q'_1 \cdots q'_n$ podemos relacionarlas mediante unidades de migración y recombinaciones.*

Demostración. Si q es primitivo, por el Teorema 3.28 dadas dos factorizaciones sabemos que las podemos relacionar por unidad de migración.
Si q no es primitivo procedemos por inducción sobre n. Si $n = 1$, por el Corolario 3.30 q es irreducible, y cualquier factorización es de la forma $q = uq_1$ con $u \in \mathcal{H}^*$. Si $n = 2$, $q = q_1q_2 = q'_1q'_2$ y $q\overline{q} = \mathsf{p}^2$; multiplicando a ambos lados por $q^{-1} \in \mathbb{H}$ obtenemos que p divide a q, es decir $\mathsf{p}u = q$ para cierto $u \in \mathcal{H}$. Tomando $|\cdot|^2$ a ambos lados $\mathsf{p}^2 = |u|^2\mathsf{p}^2$, de donde se deduce que $u \in \mathcal{H}^*$. Por tanto, $q = q_1q_2 = \mathsf{p}u = q_1\overline{q_1}$ luego $q_2 = \overline{q_1}u$. De manera análoga obtenemos que $q'_2 = \overline{q'_1}u$. Por ello $q_1q_2 = q_1\overline{q_1}u = q'_1\overline{q'_1}u = q'_1q'_2$ y esto es una recombinación.
Suponemos cierto para $n-1$ y demostraremos que es cierto para n. De nuevo p divide a q. Por el Lema 3.39 sabemos que p divide a q_1q_2 y puesto que q es p-primo obtenemos $q_1q_2 = q$. Análogamente podemos comprobar $q'_1q'_2 = q = q_1q_2$. El resto de factores $q_3, \ldots, q_n$ sabemos que están relacionados por una serie de unidades de migración y recombinaciones que deducimos de la hipótesis de inducción. □

El siguiente teorema da sentido al trabajo realizado en las páginas previas, puesto que prueba lo que venimos buscando al principio de la sección, para dos factorizaciones en irreducibles de $q \in \mathcal{H}$ podemos obtener una factorización a partir de la otra y por tanto relacionar ambas para lograr la *unicidad*.

Teorema 3.47. *Si $q \in \mathcal{H}$ no unidad tal que $q = q_1 \cdots q_n = q'_1 \cdots q'_n$ son dos factorizaciones en irreducibles entonces ambas factorizaciones están relacionadas por una serie de unidades de migración, meta-conmutaciones y recombinaciones.*

Demostración. Comenzamos probando el siguiente diagrama

$$\begin{array}{ccc} q_1 \cdots q_n & \xrightarrow{\Omega} & q'_1 \cdots q'_n \\ \downarrow{\scriptstyle \phi} & \circlearrowright & \downarrow{\scriptstyle \varphi} \\ q_1^{(1)} \cdots q_n^{(1)} & \xrightarrow[\psi]{} & q_1^{(2)} \cdots q_n^{(2)} \end{array}$$

Las aplicaciones ϕ y ψ denotan una serie de meta-conmutaciones que conducen a los modelos estándar $q_1^{(1)} \cdots q_n^{(n)}$ y $q_1^{(2)} \cdots q_n^{(2)}$ respectivamente.
La aplicación φ construye una factorización en bloques a partir de una factorización modelada en el modelo estándar, lo que posible por la Observación 3.42. Además por la Observación 3.43 y la Proposición 3.46 sabemos que podemos relacionar ambas por unidad de migración y recombinaciones.
Obsérvese que todos los procesos descritos hacen conmutativo el diagrama. □

Para concluir, ilustramos el Teorema 3.47 con el siguiente ejemplo.

Ejemplo 3.48. Consideramos $(\mathbf{j}-\mathbf{k})(1+\mathbf{i}+\mathbf{j})(1-\mathbf{i}-\mathbf{j})$ y $(1+\mathbf{j}+\mathbf{k})(1+\mathbf{i})(1+\mathbf{i}-\mathbf{k})$ dos factorizaciones en irreducibles de $q = 3\mathbf{j} - 3\mathbf{k}$. Veamos que son equivalentes por: meta-conmutación, unidad de migración y recombinación.

$$q = (\mathbf{j} - \mathbf{k})3$$

Por tanto, una factorización q modelada en el modelo estándar es

$$q = (\mathbf{j} - \mathbf{k}) \underbrace{(1 + \mathbf{i} + \mathbf{j})}_{q_1} \underbrace{(1 - \mathbf{i} - \mathbf{j})}_{\overline{q_1}}.$$

Realizando la recombinación $q_1\overline{q_1} \leftrightarrow (1 - \mathbf{i} + \mathbf{k})(1 + \mathbf{i} - \mathbf{k}) = q_2\overline{q_2}$, obtenemos

$$q = (\mathbf{j} - \mathbf{k}) \underbrace{(1 - \mathbf{i} + \mathbf{k})}_{q_2} \underbrace{(1 + \mathbf{i} - \mathbf{k})}_{\overline{q_2}}.$$

Por migración de unidades entre el primer y el segundo factor obtenemos

$$q = (\mathbf{j} - \mathbf{k})\mathbf{i}\mathbf{i}^{-1}(1 - \mathbf{i} + \mathbf{k})(1 + \mathbf{i} - \mathbf{k}) = (\mathbf{j} + \mathbf{k})(1 + \mathbf{i} - \mathbf{j})(1 + \mathbf{i} - \mathbf{k}).$$

Por la Observación 3.32 tenemos la meta-conmutación $(\mathbf{j} + \mathbf{k})(1 + \mathbf{i} - \mathbf{j}) = (1 + \mathbf{j} + \mathbf{k})(1 + \mathbf{i})$, luego

$$q = (1 + \mathbf{j} + \mathbf{k})(1 + \mathbf{i})(1 + \mathbf{i} - \mathbf{k}).$$

Conclusiones

A lo largo de esta memoria hemos estudiado el anillo de Hamilton y algunas de sus propiedades algebraicas. Hemos considerado otras estructuras para dicho anillo lo que nos ha permitido estudiar diferentes métodos de resolución de ecuaciones cuaterniónicas atendiendo a su grado.

El problema de determinar las soluciones de una ecuación cuaterniónica de grado n, se resuelve con el cálculo de los autovalores de una matriz compleja. En particular, hemos propuesto otros métodos de resolución para grado uno, grado dos y raíces de grado n.
Los resultados obtenidos nos han permitido contabilizar el número de soluciones de las ecuaciones cuaterniónicas. Finalizamos el capítulo presentando el Teorema Fundamental del Álgebra en los cuaterniones, el cual establece que dado un polinomio no constante con un único término de mayor grado tendrá al menos un cero en $\mathbb{H}$.

En el Capítulo 3 profundizamos en el estudio del subanillo de los enteros de Hurwitz y los enteros de Lipschitz para demostrar el Teorema de los cuatro cuadrados de Lagrange, el cual establece que, cualquier entero positivo n se puede expresar como suma de cuatro cuadrados, es decir, $n{=}a_0^2 + a_1^2 + a_2^2 + a_3^2$ con $a_i \in \mathbb{Z}$ para todo $0 \leq i \leq 3$. Un refinamiento de este teorema es la conocida como Conjetura 1-3-5 de Zhi-Wei Sun publicada en 2016, la cual no se ha incluido en esta memoria. Zhi-Wei Sun afirma que es posible elegir $a_i \in \mathbb{Z}$ para $0 \leq i \leq 3$ de tal manera que $a_0+3a_1+5a_0$ también sea un cuadrado perfecto. El estudio de esta conjetura es una continuación natural del trabajo recogido en esta memoria.

Bibliografía

[1] Cao, D. et alls. Ecuaciones Cuaterniónicas. *La Gaceta de la RSME*, 2016, vol. 19, nº 1, pp. 57–66.

[2] Conway, J.H, F. y Smith, D.A. On Quaternions and Octonions. The Hurwitz Integral Quaternions *A K Peters, Ltd*, 2002, pp. 55–64.

[3] De Leo, S. et alls. Zeros of unilateral quaternionic Polynomials. *Electronic Journal of Linear Algebra (ELA), International Linear Algebra Society*, 2006, vol. 15, pp. 297–313

[4] Hanson, A.J. Visualizing Quaternions. *The Morgan Kaufmann Series in Interative 3D Techology*, 2006, pp. 35–137.

[5] Huang, L. y So. W. Quadratic Formulas for Quaternions. *Applied Mathematics Letters*, 2002, vol. 15, pp. 533–540.

[6] İpek, A. On The Solutions of Linear Matrix Quaternionic Equations and Their Systems. *Mathematica Aeterna*, 2016, vol 6, nº 6, pp. 907–921.

[7] Niven, I. A note on the Number Theory of quaternions. *Duke. Math*, 1946, vol 13, nº 3, 397–400.

[8] Niven, I. Equations in cuaterniones, *Amer.Math*, vol 48, 1941, pp 654–661.

[9] Niven, I. et alls. The "Fundamental Theorem of Algebra"for quaternions, *Amer. Math*, 1944, vol 50, 246–248.

[10] Niven, I. The roots of a quaternion. *Amer. Math*, 1942, vol 49, pp 386–388.

[11] Macías-Virgós, E. et alls. Left Eigen Values of 2x2 symplectic matrices. *Electronic Journal of Linear Algebra (ELA), International Linear Algebra Society*, 2009, vol 18, pp. 274–280.

[12] Perng, C. et alls. Factorization of Hurwitz Quaternions. *International Mathematical Forum*, 2012, vol 7, nº 43, pp. 2143–2156.

Hamilton ring

Sección de Matemáticas
Universidad de La Laguna

Raquel Tapia Ramos
Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu0101231464@ull.edu.es

Abstract

Industry and technology demand to know the position and movements of objects in three-dimensional space. Today to meet the aforementioned need, quaternionic tools are used. In this work we algebraically analyze the quaternions also known as the Hamilton ring.

1. Introduction

Hamilton in 1843 said that q is a quaternion or cuaternio if $q = a_0\mathbf{1} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, with $a_i \in \mathbb{R}$, for all $i \in \{0,1,2,3\}$ where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},\ \mathbf{k} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},\ i = \sqrt{-1}.$$

This unit and noncommutative ring denoted by $\mathbb{H}$ verifies the following table with the product

*	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Moreover,$\mathbb{H}$ is isomorphic to $\mathbb{R}^4$ as $\mathbb{R}$-vector space.

2. Quaternionic Equations

An interesting problem, and only partially solved, is the study of quaternionic equations.

Degree one: The method to solve a quaternionic equation of degree one of the form

$$p_1\xi q_1 + \cdots + p_n\xi q_n = r \quad p_i, q_i, r \in \mathbb{H} \quad 1 \le i \le n,$$

consists in solving a linear real system with four equations and four unknowns.

Degree two: A quadratic generated polynomial with a unique highest degree term can be reduced to the following quadratic standard polynomial

$$\xi^2 + b\xi + c = 0 \quad \text{with} \quad b, c \in \mathbb{H}.$$

It is posible to find an explicit formula for the roots. We distinguish the following cases:

$$\begin{cases} \textbf{Case 1: } b, c \in \mathbb{R} \begin{cases} \textbf{Caso 1.1: if } b^2 < 4c \to \xi_0 = -\frac{b}{2} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}, \\ \qquad \text{with } \beta, \gamma, \delta \in \mathbb{R} \text{ such that} \\ \qquad \beta^2 + \gamma^2 + \delta^2 = c - \frac{b^2}{4}. \\ \textbf{Case 1.2: if } b^2 \ge 4c \to \xi_0 = \frac{-b \pm \sqrt{b^2 - 4c}}{2}. \end{cases} \\ \textbf{Case 2: } b \in \mathbb{R}, c \notin \mathbb{R} \to \xi_0 = \frac{-b}{2} \pm \frac{\rho}{2} \mp \frac{c_1}{\rho}\mathbf{i} \mp \frac{c_2}{\rho}\mathbf{j} \mp \frac{c_3}{\rho}\mathbf{k}. \\ \qquad c = (c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}). \\ \qquad \rho = \sqrt{\frac{(b^2 - 4c_0) + \sqrt{(b^2 - 4c_0)^2 + 16(c_1^2 + c_2^2 + c_3^2)}}{2}}. \\ \textbf{Case 3: } b \notin \mathbb{R} \equiv \begin{cases} T^3 + (B - 2N)T + D = 0 \\ N^2 - (B + T^2)N + E = 0. \end{cases} \\ \qquad \text{with } B = 1 + 2\Re(c) \in \mathbb{R}, \\ \qquad E = |c|^2 \in \mathbb{R}, \\ \qquad D = -c\mathbf{i} + \mathbf{i}\bar{c} \in \mathbb{R}. \\ \qquad \downarrow \\ \qquad \xi_0 = \frac{\mathbf{i} - T}{|\mathbf{i} + T|^2}(c - N). \end{cases}$$

$$\textbf{Case 3.1: } D \neq 0 \to T = \pm\sqrt{z_0}. \quad N = \frac{T^3 + BT + D}{2T},$$
with z_0 positive root of $P(z)$.
$P(z) := z^3 + 2Bz^2 + (B^2 - 4E)z - D^2 = 0.$

$$\textbf{Case 3.2: } D = 0 \to \begin{cases} \text{if } B^2 - 4E \ge 0 \\ \qquad \downarrow \\ T = 0, \\ N = \frac{B \pm \sqrt{B^2 - 4E}}{2}. \\ \text{if } B^2 - 4E < 0 \\ \qquad \downarrow \\ T = \sqrt{2\sqrt{E} - B}. \\ N = +\sqrt{E}. \end{cases}$$

Degree n: In general it is rather difficult to find an explicit formula for the roots. Perng proposed a method to solve unilateral equations of degree n in the Hamilton ring of the form

$\xi^n - a_{n-1}\xi^{n-1} - a_{n-2}\xi^{n-2} - \ldots - a_1\xi - a_0 = 0$ with $a_i \in \mathbb{H},\ 0 \le i \le n-1$.

The strategy can be summarized in 3 steps:

- Translating the quaternionic problem in an eigenvalue problem in the complex field.
- Finding its eigenvectors.
- Obtaning the quaternionic solution.

3. Quaternionic Systems

By means of arithmetic operations the quaternionic system with two unknowns and two addens of the form

$$\begin{cases} ayb + cxd = e \\ pyq + rxs = t \end{cases} \text{ con } a, b, c, d, e, p, q, r, s, t \in \mathbb{H}, \qquad (1)$$

could be converted into a classical real linear system with four unknowns. Then the solutions of the system (1) are obtanined from linear algebra.

4. Number Theory

A quaternion $q \in \mathbb{H}$ is a *Hurwitz quaternion* if its coefficients are integers or half integers.

One of the main properties of this subring in $\mathbb{H}$ also known as the Hurwitz integers, denoted by $\mathcal{H}$, is the existence of one-sided division algorithm.

Consequently, using Hurwitz quaternions one can prove:

Lagrange's Theorem of Four Squares (1770): Any non-negative integer can be written as a sum of four squares.

- The units in $\mathcal{H}$ are those whose norms are 1.
- The irreducible in $\mathcal{H}$ are those whose norms are primes in $\mathbb{Z}$.

The theory of the factorization into irreducible in $\mathcal{H}$ is established:

Theorem. Let $q \in \mathcal{H}$. Then there exists $q_1, \ldots, q_n \in \mathcal{H}$ irreducible such that $q = q_1 \cdots q_n$ is a factorization into irreducible which is unique up: metacommutations, unit-migrations, and recombinations.

Example:
$$\begin{aligned} 3\mathbf{j} - 3\mathbf{k} &= (1 + \mathbf{j} + \mathbf{k})(1 + \mathbf{i})(1 + \mathbf{i} - \mathbf{k}) \\ &\overset{*}{=} (\mathbf{j} + \mathbf{k})(1 + \mathbf{i} - \mathbf{j})(1 + \mathbf{i} - \mathbf{k}) \\ &= (\mathbf{j} + \mathbf{k})\mathbf{i}\mathbf{i}^{-1}(1 + \mathbf{i} - \mathbf{j})(1 + \mathbf{i} - \mathbf{k}) \\ &= (\mathbf{j} - \mathbf{k})\underbrace{(1 - \mathbf{i} + \mathbf{k})(1 + \mathbf{i} - \mathbf{k})}_{3} \\ &= (\mathbf{j} - \mathbf{k})\overbrace{(1 + \mathbf{i} + \mathbf{j})(1 - \mathbf{i} - \mathbf{j})}. \end{aligned}$$

$^*|1 + \mathbf{j} + \mathbf{k}|^2 = |1 + \mathbf{i} - \mathbf{j}|^2,\ |1 + \mathbf{i}|^2 = |1 + \mathbf{i} - \mathbf{j}|^2$, where $|\cdot|$ denoted the Euclidean norm.

$\mathcal{H}(1 + \mathbf{j} + \mathbf{k})(1 + \mathbf{i}) = \mathcal{H}(\mathbf{j} + \mathbf{k})(1 + \mathbf{i} - \mathbf{j})$. For any $q \in \mathcal{H}$ the right ideal of the multiples of q is $\mathcal{H}q$.

References

[1] De Leo, S. et alls. Zeros of unilateral quaternionic Polynomials. *Electronic Journal of Linear Algebra (ELA), International Linear Algebra Society*, 2006, vol. 15, pp. 297–313.

[2] Huang, L. y So. W. Quadratic Formulas for Quaternions. *Applied Mathematics Letters*, 2002, vol. 15, pp. 533–540.

[3] İpek, A. On The Solutions of Linear Matrix Quaternionic Equations and Their Systems. *Mathematica Aeterna*, 2016, vol 6, n. 6, pp. 907–921.

[4] Perng, C. et alls. Factorization of Hurwitz Quaternions. *International Mathematical Forum*, 2012, vol 7, n. 43, pp. 2143–2156.