Cuaterniones

José Luis Tábara

jltabara@gmail.com

Índice

1. Introducción

Definición 1.1 *Sean k y K dos cuerpos no necesariamente conmutativos. Llamamos* extensión de cuerpos *a cualquier morfismo de cuerpos $\varphi : k \to K$, y lo denotamos $k \hookrightarrow K$.*

Como un morfismo de cuerpos siempre es inyectivo, podemos suponer, sin pérdida de generalidad, que k es un subcuerpo de K.

Dada una extensión de cuerpos $k \hookrightarrow K$, el cuerpo K adquiere una estructura de espacio vectorial sobre el subcuerpo k, realizando la multiplicación de escalares por la izquierda

$$\begin{array}{ccc} k \times K & \to & K \\ (\lambda, a) & \to & \lambda \cdot a \end{array}$$

Llamamos grado de la extensión, y denotamos $[K : k]$, a la dimensión del k-espacio vectorial K. Decimos que la extensión es finita, si el grado de la extensión es finito.

La extensión $\mathbb{R} \hookrightarrow \mathbb{C}$ es de grado 2 y por lo tanto finita. Sin embargo $\mathbb{C}$ carece de extensiones finitas y conmutativas.

Proposición 1.1 *Si $\mathbb{C} \hookrightarrow K$ es una extensión finita y K es conmutativo, la extensión debe de ser de grado 1 y por lo tanto $\mathbb{C}$ coincide con K.*

Demostración.

Sea $a \in K$. Consideremos la aplicación

$$\begin{array}{rccc} \phi_a : & \mathbb{C}[x] & \to & K \\ & p(x) & \to & p(a) \end{array}$$

Dicha aplicación es un morfismo de anillos (debido a que K es conmutativo). Como el anillo de polinomios es un espacio vectorial de dimensión infinita, la aplicación no puede ser inyectiva. El ideal que forma su núcleo está generado por un polinomio. Como K es un cuerpo, necesariamente el polinomio generador es irreducible. Al ser $\mathbb{C}$ algebraicamente cerrado, dicho polinomio es de la forma $x - z$ con $z \in \mathbb{C}$. Pero entonces

$$\phi_a(x - z) = 0 \quad \Rightarrow \quad a - z = 0$$

y ambos cuerpos coinciden. $\square$

Observación.

El generador del núcleo de ϕ_a es lo que habitualmente se denomina polinomio mínimo de a. Todo elemento de una extensión finita posee polinomio mínimo. $\square$

Por lo tanto las únicas extensiones finitas de $\mathbb{C}$ deben de ser no conmutativas. A mediados del siglo XIX Hamilton descubrió una extensión finita de $\mathbb{C}$, que es el cuerpo de los cuaterniones. Posteriormente Frobenius demostró que, salvo isomorfismos, esa era la única extensión finita de los complejos.

2. El modelo matricial

Existen muchos métodos distintos para construir el cuerpo de los cuaterniones. Cada uno de estos métodos dará lugar a un modelo. Evidentemente se puede tomar un único modelo y deducir de él todas las propiedades. Sin embargo, cierto tipo de propiedades parecen adecuarse más a un modelo que a otro. Es por ello que nosotros, en contra de la norma habitual, seguiremos el "camino de espinas" y realizaremos distintas construcciones del cuerpo cuaternionico, demostrando, eso sí, que todas son isomorfas.

Consideremos el subconjunto

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in M_2(\mathbb{C}) \text{ con } a, b \in \mathbb{C} \right\}$$

La suma y el producto de elementos de $\mathbb{H}$ es nuevamente un elemento de $\mathbb{H}$. Por lo tanto $\mathbb{H}$ es un anillo. Veamos que todo elemento no nulo es invertible.

El determinante de un elemento

$$\det \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = a\overline{a} + b\overline{b} = |\,a|^2 + |\,b|^2$$

es no nulo si la matriz es no nula. La matriz inversa es

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}^{-1} = \frac{1}{|\,a|^2 + |\,b|^2} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix}$$

que es también un elemento de $\mathbb{H}$.

Definición 2.1 *Llamamos* cuerpo de los cuaterniones *al conjunto* $\mathbb{H}$ *dotado de la suma y el producto matriciales.*

Este será nuestro primer modelo de $\mathbb{H}$. Lo llamaremos modelo matricial. Utilizando este modelo se pueden deducir, de modo sencillo, algunos resultados referentes a $\mathbb{H}$ y a la relación que guarda este nuevo cuerpo con el cuerpo real y el complejo.

Propiedades.

- Tomando dos elementos arbitrarios se observa que, en general, el producto no es conmutativo.
- La aplicación de $\mathbb{R}$ en $\mathbb{H}$ que manda al número real λ al cuaternión $\lambda\,\mathrm{Id}$ es un morfismo inyectivo de anillos. Como el anillo de matrices es un espacio vectorial de dimensión finita, la extensión $\mathbb{R} \hookrightarrow \mathbb{H}$ es de grado finito.
- Los múltiplos reales de la identidad conmutan con todos los elementos de $\mathbb{H}$. Es más, si q conmuta con todos los elementos de $\mathbb{H}$, entonces $q = \lambda\mathrm{Id}$ con $\lambda \in \mathbb{R}$ (realizar la comprobación en dos casos: el primero con $a = i$ y $b = 0$ y el segundo con $a = 0$ y $b = 1$). Hemos demostrado que el centro de $\mathbb{H}$ es un cuerpo isomorfo a $\mathbb{R}$.

De la misma forma que hemos inyectado $\mathbb{R}$ en $\mathbb{H}$, intentamos inyectar el cuerpo complejo. Para ello consideramos el morfismo natural del cuerpo en su anillo de matrices

$$z \to z\,\mathrm{Id} = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$$

Sin embargo, la imagen de este morfismo no está contenida en $\mathbb{H}$. Por ello construimos otro morfismo

$$z \to \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$$

Este es un morfismo de anillos inyectivo y su imagen si está contenida en $\mathbb{H}$. Da lugar entonces a una extensión $\mathbb{C} \hookrightarrow \mathbb{H}$ que nuevamente es de grado finito. Via este nuevo morfismo podemos considerar que $\mathbb{C} \subset \mathbb{H}$. Naturalmente la inclusión anterior de $\mathbb{R}$ en los cuaterniones es la restricción de esta nueva inclusión.

3. El modelo complejo

Teniendo en cuenta estas inclusiones, podemos dotar a $\mathbb{H}$ de una estructura de espacio vectorial real o complejo, realizando la multiplicación de escalares por la izquierda. En el caso real es indiferente que la multiplicación se realice por la derecha o por la izquierda, puesto que $\mathbb{R}$ está contenido en el centro de $\mathbb{H}$. Sin embargo en el caso complejo es fundamental, pues si multiplicamos por la derecha obtenemos otra estructura de espacio vectorial.

Consideremos las matrices

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Veamos que el par de matrices anteriores forma una base del espacio vectorial complejo. La independencia lineal es clara y además tenemos que

$$a + bj = \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & \overline{b} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$$

Por lo tanto todo cuaternión se puede escribir de modo único como una expresión de la forma $a+bj$. Este será nuestro segundo modelo de los cuaterniones, que lo llamaremos modelo complejo.

Para trabajar con este modelo debemos indicar cuales son las operaciones de suma y producto. La suma se realiza componente a componente

$$(a+bj)+(c+dj)=(a+c)+(d+b)j$$

Para introducir la multiplicación basta con indicar dos reglas simples, que son las llamadas

Reglas de conmutación.

- $j^2=-1$
- $zj=j\overline{z}$ donde $\overline{z}$ es el complejo conjugado de z.

Aplicando estas reglas, la multiplicación de dos cuaterniones es

$$(a+bj)\cdot(c+dj)=ac+adj+bjc+bjdj=$$
$$ac+adj+b\overline{c}j+bjj\overline{d}=(ac-b\overline{d})+(ad+b\overline{c})j$$

En realidad, la suma y el producto los hemos introducido para que sea cierto el siguiente

Corolario 3.1 *La aplicación*

$$a+bj\to\begin{pmatrix} a & b \\ -\overline{b} & \overline{a}\end{pmatrix}$$

es un isomorfismo de cuerpos entre el modelo complejo y el modelo matricial.

4. El modelo real

De modo similar, si consideramos en $\mathbb{H}$ la estructura de espacio vectorial real tenemos la base estandard

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Todo cuaternión se escribe de modo único como

$$q = a + bi + cj + dk \text{ con } a, b, c, d \in \mathbb{R}$$

Este es nuestro tercer modelo de $\mathbb{H}$ y es con el que inicialmente trabajó Hamilton. Lo llamaremos modelo real o modelo hamiltoniano. Utilizando las propiedades de las matrices $\{i, j, k\}$ proponemos las siguientes

Reglas de conmutación.

- $i^2 = j^2 = k^2 = -1$
- $ij = -ji = k; \quad jk = -kj = i; \quad ki = -ik = j$

Como los elementos de $\mathbb{R}$ pertenecen al centro, con estas reglas podemos realizar la multiplicación de cualquier par de cuaterniones. Operando, observamos que

$$q = a + bi + cj + dk = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix} = (a + bi) + (c + di)j$$

que nos proporciona el isomorfismo entre el modelo real y el resto de modelos.

Observación.

En algunos casos la letra i indica una matriz y en otros indica la unidad imaginaria. No existe peligro de confusión, puesto que al inyectar $\mathbb{C}$ en $\mathbb{H}$ a la unidad imaginaria i le corresponde la matriz i. $\square$

5. El modelo vectorial

La notación empleada sugiere que todo cuaternión se puede escribir, formalmente, como la suma de un escalar y de un vector tridimensional del espacio euclídeo

$$q = a + \mathbf{v} \text{ donde } \mathbf{v} \text{ es el vector } bi + cj + dk$$

Este es el modelo vectorial de $\mathbb{H}$. La multiplicación de dos cuaterniones se realiza en este modelo mediante la fórmula

$$(a + \mathbf{u}) \cdot (b + \mathbf{v}) = (ab - \langle \mathbf{u}, \mathbf{v} \rangle) + (a\mathbf{v} + b\mathbf{u} + \mathbf{u} \wedge \mathbf{v})$$

donde tanto el producto escalar como el vectorial son los canónicos ($\{i, j, k\}$ es una base ortonormal orientada positivamente). La comprobación de esta fórmula se puede realizar fácilmente utilizando el modelo real. No nos debe extrañar la aparición de un producto vectorial, pues las reglas de conmutación de los cuaterniones $\{i, j, k\}$ son idénticas a las propiedades que verifican los vectores unitarios respecto al producto vectorial. La aparición de un producto escalar con signo negativo está asociada a la reglas que proporcionan los cuadrados de los elementos de la base.

En particular, si los dos cuaterniones tienen únicamente parte vectorial

$$\mathbf{u} \cdot \mathbf{v} = -\langle \mathbf{u}, \mathbf{v} \rangle + \mathbf{u} \wedge \mathbf{v}$$

que nos indica la gran relación existente entre el producto de cuaterniones y la estructura de espacio euclídeo tridimensional. Utilizando este resultado se deducen una serie de

Propiedades.

- Podemos construir el producto escalar de dos vectores tridimensionales a partir de la multiplicación de cuaterniones

$$\langle \mathbf{u}, \mathbf{v} \rangle = -\frac{\mathbf{u} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{u}}{2}$$

El módulo del vector se calcula con

$$\| \mathbf{u} \| = \sqrt{-\mathbf{v} \cdot \mathbf{v}}$$

- Lo mismo se puede hacer con el producto vectorial

$$\mathbf{u} \wedge \mathbf{v} = \frac{\mathbf{u} \cdot \mathbf{v} - \mathbf{v} \cdot \mathbf{u}}{2}$$

- Con las dos propiedades anteriores también se puede construir el producto mixto

$$[\mathbf{u}, \mathbf{v}, \mathbf{w}] = \frac{\mathbf{w} \cdot \mathbf{v} \cdot \mathbf{u} - \mathbf{u} \cdot \mathbf{v} \cdot \mathbf{w}}{2}$$

- Si los vectores u y v son ortonormales, su producto es un cuaternión que posee únicamente parte vectorial. Los vectores $\mathbf{u}, \mathbf{v}, \mathbf{w} = \mathbf{u} \cdot \mathbf{v}$ forman una base ortonormal y positivamente orientada. Además cumplen unas reglas de conmutación similares a las que cumplen los cuaterniones $\{i, j, k\}$.

6. Conjugación y estructura euclídea

A la hora de dar definiciones intentaremos no utilizar ningún modelo específico. Pero otras veces necesitamos recurrir a un modelo. Cuando hagamos esto veremos cual es la definición adecuada en los otros modelos. La cuestión de elegir un modelo u otro en muchos casos es simplemente la comodidad.

Definición 6.1 *Dado* $q = \left(\begin{smallmatrix} a & b \\ -\overline{b} & \overline{a} \end{smallmatrix}\right)$ *llamamos* congujado*, y denotamos* $\overline{q}$*, a la matriz traspuesta conjugada*

$$\overline{q} = q^* = \begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix}$$

La conjugación cuaternionica guarda una estrecha relación con la conjugación habitual en el campo complejo. Muchas de las propiedades son generalizaciones directas del caso complejo. Todas se deducen de modo natural utilizando las propiedades de las matrices traspuestas conjugadas.

Propiedades.

- Si $q \in \mathbb{H}$ entonces $\overline{q} \in \mathbb{H}$. Además $\overline{q+r} = \overline{q} + \overline{r}$.
- $\overline{q \cdot r} = (q \cdot r)^* = r^* \cdot q^* = \overline{r} \cdot \overline{q}$ aplicando la conocida propiedad de la trasposición. La conjugación $q \to \overline{q}$ es un antimorfismo de anillos.
- $\overline{\overline{q}} = (q^*)^* = q$. La conjugación es involutiva. Es inyectiva y epiyectiva.
- Si $q \in \mathbb{C} \subset \mathbb{H}$ esta conjugación coincide con la conjugación compleja. No puede existir confusión entre las dos, a pesar de que denoten del mismo modo.

Si $q = a + b \cdot j$ entonces

$$\overline{q} = \overline{a} + \overline{b \cdot j} = \overline{a} + \overline{j} \cdot \overline{b} = \overline{a} - b \cdot j$$

donde hemos utilizado que $\overline{j} = -j$ y las reglas de conmutación. Ya sabemos como se realiza la conjugación en el modelo complejo. Pasando al modelo real, si

$$q = a + bi + cj + dk \quad \Rightarrow \quad \overline{q} = a - bi - cj - dk$$

puesto que $\overline{i} = -i$, $\overline{j} = -j$ y $\overline{k} = -k$ y que la conjugación sobre los reales es la identidad. En el modelo vectorial

$$q = a + \mathbf{v} \quad \Rightarrow \quad \overline{q} = a - \mathbf{v}$$

Definición 6.2 *Llamamos* norma *de un cuaternión q a*

$$N(q) = q\overline{q}$$

La definición introducida utiliza únicamente el concepto de conjugación y es independiente del modelo. Ahora particularizaremos en cada uno de los modelos conocidos

Si $q = a + bj$ operando se obtiene que

$$N(q) = (a + bj)(\overline{a} - bj) = a\overline{a} - abj + bj\overline{a} - bjbj$$

Utilizando las reglas de conmutación, los dos términos intermedios se eliminan y el último término se transforma en $b\overline{b}$. Finalmente

$$N(a+bj) = |\,a|^2 + |\,b|^2$$

Hemos probado que la norma de cualquier cuaternión es siempre un número real no negativo.

En los demás modelos se pueden realizar demostraciones análogas o bien utilizar el resultado conocido ya para el modelo complejo. En el modelo matricial se tiene que

$$N\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = \begin{pmatrix} |\,a|^2 + |\,b|^2 & 0 \\ 0 & |\,a|^2 + |\,b|^2 \end{pmatrix}$$

en el modelo real

$$N(a+bi+dj+dk) = a^2+b^2+c^2+d^2$$

y en modelo vectorial

$$N(a+\mathbf{v}) = a^2 + \langle\, \mathbf{v}, \mathbf{v}\,\rangle$$

Propiedades

- $N(q) = 0$ si y solo si $q = 0$ y además $N(q) = N(\overline{q})$ utilizando, por simplicidad, el modelo real.
- En el modelo matricial, la norma se puede calcular con determinantes

$$N\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = a\overline{a} + b\overline{b} = \det\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$$

- $N(qr) = N(q)N(r)$. Si trabajamos en el modelo matricial, esta propiedad se deriva del hecho de que $\det(AB) = \det(A)\det(B)$.

- Si q es no nulo, construimos $q' = \overline{q}/N(q)$. Observamos que

$$qq' = q\frac{\overline{q}}{N(q)} = \frac{q\overline{q}}{N(q)} = 1$$

de donde $q^{-1} = \overline{q}/N(q)$, fórmula análoga a la del análisis complejo.

7. Estructura euclídea

Hemos visto que, en el modelo real, la norma de un cuaternión coincide con el cuadrado de la longitud del correspondiente vector de $\mathbb{R}^4$. Esto permite introducir una estructura euclídea en $\mathbb{H}$, definida a partir únicamente de la estructura algebraica del cuerpo cuaternionico. Recordemos que conocida la norma de un espacio euclídeo, se puede recuperar el producto escalar utilizando la identidad de polarización

$$\langle x, y \rangle = \frac{\| x + y \|^2 - \| x \|^2 - \| y \|^2}{2}$$

Esto nos conduce a la siguiente

Definición 7.1 *Llamamos* producto escalar *de dos cuaterniones a*

$$\langle q, r \rangle = \frac{N(q+r) - N(q) - N(r)}{2} = \frac{q\overline{r} + r\overline{q}}{2}$$

Respecto a este producto escalar, $\mathbb{H}$ es un modelo de espacio euclídeo de dimensión cuatro.

Propiedades.

- Por construcción $N(q) = \langle q, q \rangle$.
- La base canónica es una base ortonormal. Comprobemos por ejemplo que i es ortogonal con j

$$\langle i, j \rangle = \frac{N(i+j) - N(i) - N(j)}{2} = \frac{2-1-1}{2} = 0$$

- En el modelo matricial

$$\langle\, q, r\, \rangle = \frac{1}{2}\mathrm{Tr}(q\overline{r})$$

8. Partes real e imaginaria

Definición 8.1 *Llamamos* parte real *de un cuaternión a*

$$\mathrm{Re}(q) = \frac{q+\overline{q}}{2}$$

y parte imaginaria *a*

$$\mathrm{Im}(q) = \frac{q-\overline{q}}{2}$$

Por construcción, tenemos que $q = \mathrm{Re}(q) + \mathrm{Im}(q)$. Los cuaterniones que no tienen parte real se dice que son imaginarios puros. Denotaremos por $\mathrm{Im}(\mathbb{H})$ al conjunto de cuaterniones imaginarios puros

$$\mathrm{Im}(\mathbb{H}) = \{q \in \mathbb{H} \text{ tales que } \mathrm{Re}(q) = 0\}$$

Es un subespacio vectorial real, pero no es un subespacio complejo.

Propiedades.

- $\mathrm{Re}(a + bi + cj + dk) = a$ e $\mathrm{Im}(a + bi + cj + dk) = bi + cj + dk$. El subespacio de los cuaterniones imaginarios es de dimensión 3 y es el ortogonal del eje real.

- $\mathrm{Re}(a+bj) = \mathrm{Re}(a)$. El conjunto de los imaginarios puros en este modelo es

$$\mathrm{Im}(\mathbb{H}) = \{\lambda i + bj \text{ donde } \lambda \in \mathbb{R} \text{ y } b \in \mathbb{C}\}$$

- En el modelo matricial, podemos calcular la parte real con la fórmula

$$\mathrm{Re}(q) = \frac{1}{2}\mathrm{Tr}(q)$$

obteniendo

$$\operatorname{Re}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = \frac{1}{2}(a + \overline{a}) = \operatorname{Re}(a)$$

- En el modelo vectorial, la parte imaginaria se identifica con la parte vectorial. Por eso algunos autores llaman parte vectorial de un cuaternión a lo que nosotros llamamos parte imaginaria.

- Utilizando el modelo real es claro que

$$\overline{(\operatorname{Re}(q) + \operatorname{Im}(q))} = \operatorname{Re}(q) - \operatorname{Im}(q)$$

  Entonces

$$N(q) = q\overline{q} = (\operatorname{Re}(q) + \operatorname{Im}(q))(\operatorname{Re}(q) - \operatorname{Im}(q)) = \operatorname{Re}(q)^2 - \operatorname{Im}(q)^2$$

  puesto que las partes reales e imaginarias conmutan. Como tenemos siempre que $\operatorname{Re}(q)^2 \leq N(q)$, se tiene que $\operatorname{Im}(q)^2$ es siempre un número real negativo o nulo. Solamente puede ser nulo si la parte imaginaria es nula. Esto nos lleva a otra posible definición de cuaternión imaginario puro: *un cuaternión q es imaginario puro si y solo si $q^2 < 0$.*

9. Problemas

Problema 1 Demostrar que si un cuaternión conmuta con i, con j y con k, entonces necesariamente q es un cuaternión real.

Problema 2 Asignemos a cada cuaternión una matriz real de orden 4

$$q = a + bi + cj + dk \quad \rightarrow \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

Este es otro modelo matricial de $\mathbb{H}$ que generalmente no se emplea debido a su tamaño. Sin embargo puede ser útil cuando se estudian las rotaciones generadas por los cuaterniones.

Problema 3 Demostrar que q y su conjugado tienen la misma norma.

Problema 4 Demostrar que $\mathrm{Re}(qr) = \mathrm{Re}(rq)$. Calcular dicho valor en algún modelo.

Problema 5 Sean q y r dos cuaterniones imaginarios puros. El producto $q \cdot r$ es imaginario puro si y solo si q y r son ortogonales (entendidos como vectores o como cuaterniones). En este caso qr es perpendicular tanto a r como a q.

Problema 6 Consideremos la ecuación $x^2 + 1 = 0$ en el cuerpo de los cuaterniones. La solución de esta ecuación forma una variedad bidimensional difeomorfa a S^2. En general la ecuación $x^2 = -r$ con $r \in \mathbb{R}^+$ tiene infinitas soluciones en $\mathbb{H}$. Sin embargo $x^2 = r$ con $r \in \mathbb{R}^+$ tiene solamente dos soluciones.

Problema 7 Sea $\mathbf{n}$ un cuaternión imaginario y unitario. Demostrar que la aplicación

$$\begin{array}{ccc} \mathbb{C} & \rightarrow & \mathbb{H} \\ a + bi & \rightarrow & a + b\mathbf{n} \end{array}$$

es un morfismo de cuerpos

Problema 8 Demostrar que $q \in \mathbb{R} \Leftrightarrow q = \overline{q}$ y que $q \in \mathrm{Im}(\mathbb{H}) \Leftrightarrow q = -\overline{q}$

10. Rotaciones

Para conocer totalmente una rotación de un plano euclídeo nos basta con un solo dato: el ángulo de rotación. Describir las rotaciones del espacio euclídeo tridimensional es ligeramente más complicado. Para conocer una rotación tridimensional debemos conocer la recta que permanece invariante por la rotación. Es lo que se denomina el eje de la rotación. Además debemos conocer el ángulo de giro que se produce en el plano perpendicular al eje de rotación. Normalmente para especificar una recta tomamos un vector unitario, de los dos posibles. Entonces, para especificar una rotación debemos dar un par $(\mathbf{u}, \alpha)$ donde $\mathbf{u}$ es un vector unitario y α un ángulo. Debemos tener en cuenta que el par $(-\mathbf{u}, \alpha)$ describe la misma rotación.

Seguir con este procedimiento en dimensiones superiores o en geometrías distintas de la euclídea es sumamente tedioso. Por ello se suele emplear la notación matricial. Una rotación de un espacio euclídeo de cualquier dimensión es una matriz M de determinante positivo que cumple $M \cdot M^t = \mathrm{Id}$. En otras geometrías el método es similar, pero en este caso la matriz debe cumplir $M \cdot G \cdot M^t = G$ donde G es la matriz de la métrica.

11. Cuaterniones unitarios

Denotamos por Sp(1) al conjunto de los cuaterniones de norma unidad. Este conjunto es un subgrupo respecto a la multiplicación. En forma matricial

$$\mathrm{Sp}(1) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \text{ tales que } |\,a|^2 + |\,b|^2 = 1 \right\}$$

que coincide exactamente con el grupo SU(2). En el modelo real

$$\mathrm{Sp}(1) = \{a + bi + cj + dk \text{ tales que } a^2 + b^2 + c^2 + d^2 = 1\}$$

lo que demuestra que el conjunto soporte del grupo es la esfera $S^3 \subset \mathbb{R}^4$. El cálculo del inverso de un cuaternión unitario es muy simple, puesto que

$$q^{-1} = \frac{\overline{q}}{N(q)} = \overline{q}$$

Lema 11.1 *Todo cuaternión unitario se puede escribir en la forma*

$$q = \cos(\theta/2) + \operatorname{sen}(\theta/2)\mathbf{u}$$

siendo $\mathbf{u}$ *un vector unitario.*

Demostración.

Todo cuaternión admite una descomposición en la forma $q = a + \mathbf{v}$, donde $\mathbf{v}$ es un vector no necesariamente unitario. Normalizando dicho vector podemos escribir el mismo cuaternión en la forma $q = a + \lambda\mathbf{u}$ donde $\mathbf{u}$ si es unitario. Si calculamos la norma de este vector obtenemos $N(q) = |\,a|^2 + |\,\lambda|^2$. Si el cuaternión es unitario tenemos que

$$|\,a|^2 + |\,\lambda|^2 = 1$$

y podemos encontrar un único ángulo θ que cumpla las condiciones

$$a = \operatorname{sen}(\theta/2) \qquad \lambda = \cos(\theta/2)$$

demostrando el resultado. $\square$

Observación.

Otros autores intentan encontrar un ángulo que cumplan

$$a = \operatorname{sen}(\theta) \qquad \lambda = \cos(\theta)$$

Como existen dos ángulos que cumplen la condición anterior, para obtener una solución única deben considerar únicamente ángulos menores que dos rectos. El desarrollo de toda la teoría es enteramente similar.

Si $\mathbf{n}$ es un cuaternión imaginario unitario, tenemos que $\mathbf{n} \cdot \mathbf{n} = -1$ y las potencias siguientes se pueden calcular del mismo modo. Podemos definir la exponencial de un vector $\theta\mathbf{n}$ utilizando el desarrollo en serie de la exponencial. En este caso no vamos a tener ningún problema de convergencia. Calculemos la exponencial

$$1 + \theta\mathbf{n} + \frac{\theta^2\mathbf{n}^2}{2} + \frac{\theta^3\mathbf{n}^3}{3!} + \frac{\theta^4\mathbf{n}^4}{4!} + \frac{\theta^5\mathbf{n}^5}{5!} \dots$$

donde hemos tenido en cuenta que θ y $\mathbf{n}$ conmutan. Utilizando el conocimiento de las potencias de $\mathbf{n}$ y sacando factor común $\mathbf{n}$ se obtiene

$$\left(1 - \frac{\theta^2}{2} + \frac{\theta^4}{4!} + \cdots\right) + \left(\theta + -\frac{\theta^3}{3!} + \frac{\theta^5}{5!} + \cdots\right)\mathbf{n}$$

que son precisamente las series del seno y del coseno.

Corolario 11.2 *Si* $\mathbf{n}$ *es un vector unitario, entonces*

$$\exp(\theta\mathbf{n}) = \cos(\theta) + \operatorname{sen}(\theta)\mathbf{n}$$

Utilizando el lema anterior, observamos que todo elemento del grupo $\mathrm{Sp}(1)$ se puede escribir como la exponencial de un cuaternión imaginario. Este cuaternión imaginario no es único, debido a la periodicidad de las funciones trigonométricas.

12. Cuaterniones y rotaciones

El cuerpo de cuaterniones actua sobre si misma por conjugación. Dicha operación respeta gran parte de las estructuras de las que está dotado el cuerpo de cuaterniones. En particular conserva la estructura euclídea.

Proposición 12.1 *Dado* $q \in \mathrm{Sp}(1)$ *denotamos por* $R_q : \mathrm{Im}(\mathbb{H}) \to \mathrm{Im}(\mathbb{H})$ *a la función* $R_q(u) = quq^{-1}$*. La aplicación*

$$\begin{array}{rccc} R: & \mathrm{Sp}(1) & \to & \mathrm{SO}(3,\mathbb{R}) \\ & q & \to & R_q \end{array}$$

es un morfismo de grupos epiyectivo con núcleo $\mathbb{Z}_2$.

Demostración.

Dividiremos la demostración en varios pasos simples, pues este esquema se utilizará más adelante.

1) R_q deja invariante $\mathrm{Im}(\mathbb{H})$.
$u \in \mathrm{Im}(\mathbb{H})$ si y solo si $\mathrm{Tr}(u) = 0$. Calculamos la traza de $R_q(u)$

$$\mathrm{Tr}(R_q(u)) = \mathrm{Tr}(quq^{-1}) = \mathrm{Tr}(qq^{-1}u) = \mathrm{Tr}(u) = 0$$

2) R_q es lineal y biyectiva.
Es $\mathbb{R}$-lineal, puesto que $\mathbb{R}$ pertenece al centro de $\mathbb{H}$. Si $R_q(u) = 0$, entonces $quq^{-1} = 0$ y despejando u obtenemos que $u = 0$. R_q es inyectiva y por razones dimensionales también es epiyectiva.

3) R_q es una isometría.
Para que una aplicación conserve el producto escalar basta con que conserve la norma que induce dicho producto escalar. Como $N(q) = \| q \|^2$, basta con la conservación de la norma cuaterniónica.

$$N(R_q(u)) = \det(quq^{-1}) = \det(u) = N(u)$$

4) R es morfismo de grupos.
Tenemos que demostrar que $R_{qr} = R_q R_r$.

$$R_{qr}(h) = (qr)h\ (qr)^{-1} = qrhr^{-1}q^{-1} = qR_r q^{-1} = R_q R_r(h)$$

5) Núcleo de R
Si q está en el núcleo tenemos.

$$R_q(u) = u \quad \text{si y solo si} \quad quq^{-1} = u \quad \text{si y solo si} \quad qu = uq$$

El núcleo es entonces $\mathrm{Ker}(R) = \mathrm{Sp}(1) \cap \mathbb{R} = \{\mathrm{Id}, -\mathrm{Id}\}$

6) Epiyectividad.

La demostraremos a continuación. □

Hemos visto que a todo cuaternión de módulo unidad se le puede asociar una rotación. Estamos interesados en conocer efectivamente cual es dicha rotación. Recordemos que una rotación del espacio euclídeo tridimensional viene determinado por dos datos: el primero es el eje de giro y el segundo es el ángulo de giro.

Proposición 12.2 *Sea* $\mathbf{v}$ *imaginario y unitario. La rotación correspondiente al cuaternión*

$$q = \cos(\theta/2) + \operatorname{sen}(\theta/2)\mathbf{v}$$

tiene por eje la recta generada por el vector $\mathbf{v}$ *y por ángulo de giro* θ*.*

Demostración.

Como q es unitario, $q^{-1} = \overline{q}$. Veamos que $\mathbf{v}$ permanece invariante por la acción de q.

$$R_q(v) = q \cdot \mathbf{v} \cdot \overline{q} = (\cos(\theta/2) + \operatorname{sen}(\theta/2)\mathbf{v}) \cdot \mathbf{v} \cdot (\cos(\theta/2) - \operatorname{sen}(\theta/2)\mathbf{v}) = \mathbf{v}$$

donde hemos tenido en cuenta que $\mathbf{v} \cdot \mathbf{v} = -1$.

Si $\mathbf{u}$ es un vector unitario y ortogonal a $\mathbf{v}$, entonces

$$R_q(\mathbf{u}) = q \cdot \mathbf{u} \cdot \overline{q} = \cos(\theta) \cdot \mathbf{u} + \operatorname{sen}(\theta) \cdot \mathbf{v} \wedge \mathbf{u}$$

Como $\{\mathbf{v}, \mathbf{u}, \mathbf{v} \wedge \mathbf{u}\}$ es una base positivamente orientada, el efecto de R_q sobre el plano perpendicular a $\mathbf{v}$ es una rotación de ángulo θ. $\square$

Observación.

Este resultado nos permite demostrar que $R : \mathrm{Sp}(1) \to \mathrm{SO}(3, \mathbb{R})$ es epiyectiva. Dada una rotación arbitraria A (que no sea la identidad) tendrá un eje y un ángulo de giro. Si $\mathbf{v}$ es un vector unitario del eje y θ el ángulo de giro, se tiene que $R_q = A$, donde $q = \cos(\theta/2) + \operatorname{sen}(\theta/2) \cdot \mathbf{v}$. $\square$

13. Dimensión 4

Del mismo modo $\mathbb{H}$ es un modelo de espacio euclídeo de dimensión cuatro. Siguiendo argumentos análogos se demuestra la

Proposición 13.1 *La aplicación*

$$\begin{array}{rccc} R: & \mathrm{Sp}(1)\times\mathrm{Sp}(1) & \to & \mathrm{SO}(4,\mathbb{R}) \\ & (q_1,q_2) & \to & R_{q_1,q_2} \end{array}$$

donde $R_{q_1,q_2}(u) = q_1\cdot u\cdot q_2^{-1}$*, es un morfismo de grupos epiyectivo cuyo núcleo es* $\mathbb{Z}_2$*.*

Demostración.

Los primeros pasos son similares. Demostraremos únicamente la epiyectividad.

Denotemos por λ_q la aplicación $\lambda_q(r) = qr$. Si q es unitario, esta aplicación es una isometría de $\mathbb{H}$, por conservar la norma cuaternionica. Sea A una isometría arbitraria de $\mathbb{H}$. El cuaternión $q = A(1)$ es de norma unidad. La composición $\lambda_{\overline{q}}A$ es una isometría que cumple

$$\lambda_{\overline{q}}A(1) = \lambda_{\overline{q}}(q) = 1$$

y deja invariante el subespacio $\mathbb{R}$. Por lo tanto también deja invariante su ortogonal, que es $\mathrm{Im}(\mathbb{H})$. Por la proposición anterior $\lambda_{\overline{q}}A = R_r$ y esto prueba la epiyectividad. $\square$

14. Geometría de Minkoski

En sus trabajos sobre relatividad especial, Minkoski multiplicó la coordenada temporal por la unidad imaginaria. Operando formalmente, al calcular la norma de un vector, aparecían tres cuadrados con signo más y uno con signo menos. Sin en vez de multiplicar la coordenada temporal por i, multiplicamos las otras tres por i obtenemos también un modelo del espacio de

Minkoski. Vamos a seguir esta intuición para construir un modelo matricial de una métrica de signatura $(3,1)$.

Sea F el subespacio real de $M_2(\mathbb{C})$ generado por las matrices

$$1=\begin{pmatrix}1&0\\0&1\end{pmatrix}\qquad \alpha=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\qquad \beta=\begin{pmatrix}0&-i\\i&0\end{pmatrix}\qquad \gamma=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

Todo elemento de F se expresa como

$$a1+b\alpha+c\beta+d\gamma=\begin{pmatrix}a-b&ic-d\\-ic-d&a+b\end{pmatrix}$$

Pero este espacio F que acabamos de construir no es ni más ni menos que el subespacio de las matrices hermíticas bidimensionales. Si calculamos el determinante de un elemento de este espacio obtenemos $a^2-b^2-c^2-d^2$. Hemos construido un modelo de espacio de signatura $(3,1)$ donde la forma cuadrática se calcula con un determinante. Además la base que hemos construido es ortogonal respecto a este producto escalar. En la siguiente proposición se pueden probar todos los detalles, salvo la epiyectividad, que nos conduciría a un estudio más detallado de la geometría de Minkoski, que no vamos a abordar en este momento.

Proposición 14.1 *Sea*

$$\begin{array}{rccc} R: & \mathrm{Sl}(2,\mathbb{C}) & \to & \mathrm{O}(\mathrm{Herm}(2)) \\ & g & \to & R_g \end{array}$$

donde $R_g(u)=g\cdot u\cdot g^*$. R es un morfismo epiyectivo sobre la componente conexa de la unidad con núcleo $\mathbb{Z}_2$.

El espacio F' generado por las matrices $\{1,\alpha,\gamma\}$ es justamente el ortogonal a β. Si $g\in \mathrm{Sl}(2,\mathbb{R})$ se tiene que $R_g(\beta)=\beta$ y por lo tanto induce una isometría del espacio F' que es un modelo de espacio con signatura $(2,1)$. Con estas observaciones se prueba la

Proposición 14.2 *Sea*

$$\begin{array}{rccc} R: & \mathrm{Sl}(2,\mathbb{R}) & \to & \mathrm{O}(2,1) \\ & g & \to & R_g \end{array}$$

donde $R_g(u) = g \cdot u \cdot g^t$*. R es un morfismo epiyectivo sobre la componente conexa con núcleo* $\mathbb{Z}_2$*.*

Observación.

Para aquellos que dominen la teoría de los grupos de Lie, esbozaremos una prueba de la epiyectividad de todos los morfismos con los que hemos trabajado.

Es claro que todos los grupos con los que hemos tratado son subgrupos cerrados de grupos matriciales y por lo tanto son grupos de Lie (teorema del subgrupo cerrado de Cartan). Los morfismos de grupos son asimismo diferenciables. Como los grupos entre los que actua el morfismo son de la misma dimensión y tienen núcleo discreto, la diferencial del morfismo es un isomorfismo de álgebras de Lie. Integrando dichos morfismos se construye un isomorfismo local entre entornos de la unidad. Se concluye entonces la epiyectividad sobre la componente conexa.

Problemas

Problema 9 Sea $q \in \mathrm{Sp}(1)$. La aplicación

$$\begin{array}{rccc} \lambda_q : & \mathbb{H} & \to & \mathbb{H} \\ & Y & \to & qY \end{array}$$

es una isometría. Demostrar que la multiplicación por la derecha, ρ_q, es también una isometría.

Problema 10 Encontrar la matriz de λ_q en la base estandard. Demostrar que los vectores fila de dicha matriz son perpendiculares entre si. Si q tiene módulo unidad, entonces la matriz es ortogonal. Probar también que su determinante es positivo. Concluir que λ_q y ρ_q pertenecen a $\mathrm{SO}(4,\mathbb{R})$ si q es unitario.

Problema 11 Demostrar que matricialmente $\lambda_{\overline{q}} = (\lambda_q)^t$. Utilizar este hecho para demostrar que λ_q es una matriz ortogonal si q es unitario.

Problema 12 Pretendemos demostrar que todo automorfismo de álgebras de $\mathbb{H}$ es un rotación de $\mathrm{Im}(\mathbb{H})$ y viceversa.

- Si q es unitario entonces R_q es un automorfismo de álgebras ($\mathrm{SO}(\mathrm{Im}(\mathbb{H}) \subset \mathrm{Aut}(\mathbb{H}))$
- Sabiendo que $q \in \mathrm{Im}(\mathbb{H}) \Leftrightarrow q \cdot q \leq 0$ demostrar que todo automorfismo deja invariante el subespacio imaginario y sobre $\mathbb{R}$ es la identidad.
- Si φ es automorfismo, entonces $\{\varphi(i), \varphi(j), \varphi(k)\}$ es una base ortonormal del hiperplano imaginario. Demostrar que dicha base está positivamente orientada, lo que implica la inclusión que nos faltaba.

Problema 13 Sea ξ_q el endomorfismo adjunto

$$\xi_q(p) = qpq^{-1}$$

Demostrar que $\xi_q = \xi_r$ si y solo si q y r son proporcionales.

Problema 14 Probar que

$$\mathrm{Re}(p) = \mathrm{Re}(qpq^{-1})$$

y que

$$\mathrm{N}(\mathrm{Im}(p)) = \mathrm{N}(\mathrm{Im}(qpq^{-1}))$$

Problema 15 Si q es un cuaternión puro de norma unidad, entonces R_q es el giro de π radianes alrededor del eje q. Como estas rotaciones generan el grupo de las rotaciones, esta es otra forma de demostrar la epiyectividad de la aplicación R.

Problema 16 Si q es un cuaternión imaginario puro, entonces

$$\sigma(r) = -q \cdot r \cdot q^{-1}$$

es la simetría respecto al hiperplano perpendicular a q. Como el grupo ortogonal está generado por simetrías, utilizar este resultado para probar la epiyectividad del morfismo $R : \mathrm{Sp}(1) \to \mathrm{SO}(3, \mathbb{R})$.

Problema 17 Sea $q = a + \mathbf{v}$ un cuaternión no necesariamente unitario. R_q es una rotación cuyo eje es $\langle \mathbf{v} \rangle$ y cuyo ángulo de giro θ se obtiene de

$$\tan\left(\frac{\theta}{2}\right) = \frac{\sqrt{N(\mathbf{v})}}{|\,a|}$$

Problema 18 Dados dos cuaterniones imaginarios puros, q y q', que tengan la misma norma, existe un cuaternión imaginario r puro tal $q' = r \cdot q \cdot r^{-1}$

15. Extensiones finitas no conmutativas

De ahora en adelante supondremos que $\mathbb{R} \hookrightarrow K$ es una extensión finita, posiblemente no conmutativa y que $\mathbb{R}$ está contenido en el centro de K, lo que equivale a que todo número real conmute con todo elemento de K. La siguiente definición es una generalización del concepto ya estudiado en el caso complejo y cuarternionico.

Definición 15.1 *En las condiciones anteriores, decimos que un elemento $u \in K$ es* imaginario *si $u^2 = u \cdot u$ es un número real menor o igual que cero. El conjunto de todos los elementos imaginarios lo denotaremos por I.*

Fijaremos la siguiente notación: las letras λ y μ denotarán números reales. La letra z denotará un elemento arbitrario de K y u y v denotarán elementos imaginarios.

Propiedades.

- Si $u \in I$ y $\lambda \in \mathbb{R}$ entonces $\lambda \cdot u$ es imaginario, puesto que

$$(\lambda \cdot u)^2 = \lambda^2 \cdot u^2 \leq 0$$

  donde hemos utilizado que los números reales conmutan con los elementos de la extensión.

- Si u es imaginario, entonces su inverso también lo es:

$$(u^{-1})^2 u^2 = 1 \quad \Rightarrow \quad (u^{-1})^2 \leq 0$$

- Si $z \in \mathbb{R} \cap I$, entonces $z = 0$.

En el caso de los complejos y de los cuaterniones, se tiene que todo elemento se puede descomponer como suma de un número real y un elemento imaginario. En general se tiene

Lema 15.1 *Todo elemento $z \in K$ se puede escribir, de modo único, en la forma*

$$z = \lambda + u \text{ con } \lambda \in \mathbb{R} \text{ y } u \in I$$

Demostración.

Sea $p(x)$ el polinomio mínimo de z. Como el polonomio es irreducible, entonces puede ser un polinomio de primer grado, o bien un polinomio de segundo grado sin raices reales. Estudiemos ambos casos.

Su $p(x)$ es de primer grado, es de la forma $x - \lambda$. Entonces

$$p(z) = 0 \quad \Rightarrow \quad z - \lambda = 0 \quad \Rightarrow \quad z = \lambda + 0$$

y obtenemos la descomposición.

Si $p(x)$ es de segundo grado, entonces es de la forma $x^2 - 2\lambda x + \mu$ con $\lambda^2 - \mu < 0$. Entonces el vector $z - \lambda$ cumple

$$(z - \lambda)^2 = z^2 - 2\lambda z + \lambda^2 = \lambda^2 - \mu < 0$$

y por lo tanto es un vector imaginario. Denotemoslo por u. Entonces

$$z - \lambda = u \quad \Rightarrow \quad z = \lambda + u$$

y obtenemos de nuevo la descomposición.

Pasemos ya a demostrar la unicidad. Supongamos que admite otra descomposición $z = \mu + v$. Restando obtenemos que

$$u = v + (\mu - \lambda)$$

Elevando al cuadrado

$$u^2 = v^2 + 2v(\mu - \lambda) + (\mu - \lambda)^2$$

que escribimos en la forma

$$u^2 - v^2 - (\mu - \lambda)^2 = 2v(\mu - \lambda)$$

El primer miembro es real y el segundo imaginario. Ambos deben ser nulos. Obtenemos que

$$2v(\mu - \lambda) = 0$$

lo que implica $v = 0$ o que $(\lambda - \mu) = 0$. De cualquiera de las dos condiciones se deduce rápidamente la unicidad. $\square$

Lema 15.2 *Sean u y v dos vectores imaginarios. Entonces $uv + vu$ es un número real.*

Demostración.

Supongamos que u, v y 1 son linealmente dependientes. Tenemos una relación

$$au + bv + c = 0 \quad \Rightarrow \quad au = -c - bv$$

Por la unicidad del lema anterior, como au es imaginario, necesariamente $c = 0$. Entonces o bien a o bien b son no nulos. Supongamos que a es no nulo. Entonces

$$u = -\frac{b}{a}v$$

e inmediatamente se deduce que

$$uv + vu = -\frac{b}{a}vv + v\left(-\frac{b}{a}\,v\right) = \frac{2b}{a}$$

que es un número real.

Supongamos ahora que los vectores son linealmente independientes. Descomponiendo tenemos

$$uv + vu = \lambda + w$$

Veamos que necesariamente w es nulo, pues en caso contrario se llega a una contradicción. Formamos una combinación lineal, tomando dos números reales r y s no nulos y descomponemos

$$ru + sv = \mu + w'$$

Elevamos al cuadrado

$$r^2u^2 + s^2v^2 + rs(uv + vu) = \mu^2 + w'^2 + 2\mu w'$$

Extrayendo la parte imaginaria de ambas expresiones obtenemos

$$rsw = 2\mu w'$$

Sustituyendo, obtenemos que

$$ru + sv = \mu + \frac{rs}{2\mu}w$$

identidad válida para valor de r y de s. Tomamos otros valores de las constantes r' y s' que no sean proporcionales a los que hemos elegido en primera instancia. Tenemos entonces

$$r'u + s'v = \mu' + \frac{r's'}{2\mu'}w$$

Multiplicando por un factor adecuado c podemos conseguir que los últimos sumandos de ambas expresiones sean iguales. Restando se obtiene

$$(r - cr')u + (s - cs')v = (\mu - c\mu')$$

Como las constantes no son proporcionales, se obtiene que u, v y 1 son linealmente dependientes, lo que es contradictorio. $\square$

Corolario 15.3 *Si u y v son imaginarios, entonces $u + v$ también. El conjunto I es un subespacio vectorial suplementario de $\mathbb{R}$.*

Demostración.

Si u, v y 1 son linealmente dependientes, entonces u y v son proporcionales y su suma es imaginaria.

Si u, v y 1 no son linealmente independientes, con las notaciones del lema anterior, si w es nulo, entonces $2\mu w'$ también es nulo. El vector w' no puede ser nulo, pues de lo contrario la terna de vectores volvería a ser linealmente dependiente. Solo queda la posibilidad de que μ sea nulo.

La invariancia en la multiplicación por escalares ya está demostrada y el lema 15.1 prueba que son suplementarios. $\square$

16. El teorema de Frobenius

Supongamos que en I existan dos vectores u y v tales que

$$u^2 = -1 \qquad v^2 = -1 \qquad w = uv \in I$$

En estas condiciones, los vectores u, v y w cumplen las reglas de conmutación de la base canónica $\{i, j, k\}$ de los cuaterniones imaginarios.

Demostremos primeramente que el inverso de uv es precisamente vu

$$(uv)(vu) = u(-1)u = (-1)(-1) = 1$$

Entonces

$$uv + vu = uv + (uv)^{-1}$$

Hemos visto que el primer miembro es real y el segundo es imaginario. Ambos son nulos. Por lo tanto

$$uv = -vu$$