Quaternions: animais parecidos com os números complexos

Hugo Cattarucci Botós

Instituto de Ciências Matemáticas e de Computação
Universidade de São Paulo
hugocbotos@gmail.com

Resumo

Muito da geometria plana pode ser feita usando números complexos: podemos calcular a área de certas figuras e realizar rotações por exemplo. Infelizmente, $\mathbb{R}^3$ não admite uma multiplicação decente que se comporte tão maravilhosamente quanto a dos números complexos. No entanto, $\mathbb{R}^4$ admite tal estrutura milagrosa. Nesse espaço surge o que se chama de quaternions, animais bastante parecidos com os números complexos. Meu objetivo é apresentá-los e mostrar quão eficientes são para a geometria espacial.

1. Números complexos e geometria plana

Em algum momento da História, matemáticos perceberam que, a fim de resolver equações polinomiais, um novo tipo de sistema numérico era necessário. Com apenas números reais é impossível resolver a equação $x^2 + 1 = 0$. No entanto, se adicionássemos um novo número i satisfazendo $i^2 = -1$ então poderíamos fatorar a equação acima

$$x^2 + 1 = (x + i)(x - i)$$

e daí teríamos que as soluções do problema são i e $-i$. Repare que isso não é tão estranho. Matemáticos sempre tiveram esse mau hábito de inventar novos números para resolver problemas que antes não conseguiam. As frações mesmo surgiram para resolver problemas como $3x = 2$.

Como sabemos da escola, o próximo passo para entender os polinômios é considerar pares da forma $a + bi$, que são chamados de números complexos, onde $a, b \in \mathbb{R}$. O conjunto de todos números complexos é denotado por $\mathbb{C}$. Vou assumir que você, caro leitor, esteja familiarizado com esses números e suas operações básicas.

Um dos resultados do grande matemático Carl Friedrich Gauss foi provar que esses números bastam para resolver equações polinomiais, isto é, se temos um polinômio não nulo P com coeficientes complexos então P admite uma raiz $z \in \mathbb{C}$. Esse teorema é conhecido como Teorema Fundamental da Álgebra e pelo nome você pode deduzir sua relevância na Matemática.

Uma das boas surpresas da vida é que $\mathbb{C}$, que a priori é uma entidade puramente algébrica, sirva para geometria. O conjunto $\mathbb{C}$ forma um espaço vetorial bidimensional sobre $\mathbb{R}$ com base $1, i$, ou seja, $\mathbb{C}$ e $\mathbb{R}^2$ são isomorfos. A diferença entre esses dois espaços é a multiplicação e essa diferença é enorme como veremos a seguir.

Vejamos algumas interpretações geométricas dos números complexos. Se temos dois números $z_1 = x_1 + ix_2$ e $z_2 = y_1 + iy_2$ então podemos considerar

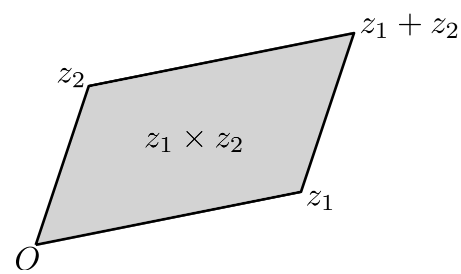
$$\overline{z_1}z_2 = (x_1 - ix_2)(y_1 + iy_2) = x_1y_1 + x_2y_2 + i(x_1y_2 - x_2y_1).$$

A parte real da expressão acima é o produto interno $\langle z_1, z_2 \rangle$ e a parte imaginária, que denotaremos por $z_1 \times z_2$, é a área orientada do paralelogramo de vértices 0, z_1, z_2 e $z_1 + z_2$. Assim temos

$$\langle z_1, z_2 \rangle = \mathrm{Re}(\overline{z_1} z_2) \quad \text{e} \quad z_1 \times z_2 = \mathrm{Im}(\overline{z_1} z_2).$$

O produto $z_1 \times z_2$ é o produto vetorial disfarçado. Podemos identificar o vetor $a + ib$ com o vetor $(a, b, 0)$ em $\mathbb{R}^3$ e assim executar o produto vetorial usual

$$(x_1, x_2, 0) \times (y_1, y_2, 0) = (0, 0, x_1 y_2 - x_2 y_1).$$



Repare que a terceira coordenada do vetor acima é o que chamamos de $z_1 \times z_2$. Na geometria analítica aprendemos que o produto vetorial $v_1 \times v_2$ de $v_1, v_2 \in \mathbb{R}^3$ nos fornece a área do paralelogramo cujos lados são v_1 e v_2 juntamente com sua orientação. No nosso contexto de geometria plana, isso significa que $z_1 \times z_2$ é a área orientada do paralelogramo cujos vértices são 0, z_1, z_2 e $z_1 + z_2$.

Se $z \in \mathbb{C}$ então sua parte real é dada por $\mathrm{Re}(z) = \frac{z + \bar{z}}{2}$ e sua parte imaginária é dada por $\mathrm{Im}(z) = \frac{z - \bar{z}}{2i}$. Desse jeito obtemos as seguintes belas identidades

$$\langle z_1, z_2 \rangle = \mathrm{Re}(\overline{z_1} z_2) = \frac{\overline{z_1} z_2 + \overline{\overline{z_1} z_2}}{2} = \frac{\overline{z_1} z_2 + z_1 \overline{z_2}}{2},$$

$$z_1 \times z_2 = \mathrm{Im}(\overline{z_1} z_2) = \left(\frac{\overline{z_1} z_2 - \overline{\overline{z_1} z_2}}{2i} \right) = \frac{\overline{z_1} z_2 - z_1 \overline{z_2}}{2i}.$$

Uma das mais famosas fórmulas da Matemática é a a fórmula de Euler

$$e^{i\theta} = \cos(\theta) + i\mathrm{sen}(\theta) \quad \forall \theta \in \mathbb{R}.$$

Antes de discutirmos para que ela serve, permita-me verificar sua validade. Sabemos do cálculo que a exponencial é dada pela série a seguir

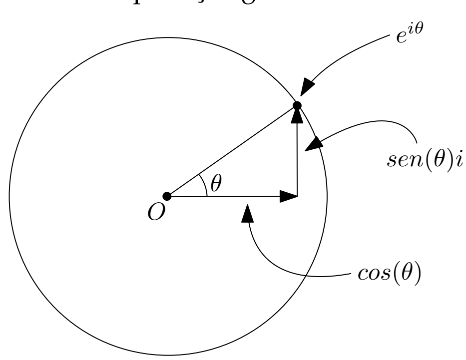
$$e^{i\theta} = 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \cdots$$

Usando que $i^2 = -1$ e rearranjando os termos obtemos

$$e^{i\theta} = \left(1 - \frac{\theta^2}{2!} + \cdots \right) + i \left(\theta - \frac{\theta^3}{3!} + \cdots \right) = \cos(\theta) + i\mathrm{sen}(\theta),$$

onde fizemos uso das expansões de Taylor de $\cos(\theta)$ e $\mathrm{sen}(\theta)$. Assim, finalizamos a prova da fórmula de Euler. Repare que ao fazermos $\theta = \pi$ obtemos a famosa identidade $1 + e^{i\pi} = 0$, que envolve cinco números especiais: 0, 1, e, π e i.

A figura a seguir nos fornece a interpretação geométrica de $e^{i\theta}$.



Na figura temos que $e^{i\theta}$ é o ponto do círculo de raio 1 obtido ao realizarmos uma rotação do ponto 1 em torno de 0 por um ângulo θ.

Como todo número complexo z aponta em uma direção $e^{i\theta}$ temos que $z = re^{i\theta}$ para algum r não negativo, onde θ é o ângulo entre 1 e z com respeito a 0. Como $|z| = |re^{i\theta}| = r$, concluímos que $z = |z|e^{i\theta}$, que é a representação em coordenada polar do número complexo z.

Desta forma, se temos dois números complexos z_1 e z_2 então podemos escrevê-los como sendo $z_1 = |z_1|e^{\theta_1}$ e $z_2 = |z_2|e^{i\theta_2}$. Ao multiplicarmos z_1 e z_2 obtemos $z_1 z_2 = |z_1||z_2|e^{i(\theta_1+\theta_2)}$. Portanto, ao multiplicarmos dois números complexos multiplicamos os módulos e somamos os ângulos. Em outras palavras, se fixarmos z_1 por exemplo então $z_1 z_2$ é obtido girando z_1 um ângulo θ_2 e dilatando-o por um fator $|z_2|$.

Assim, se temos um número complexo z e um ângulo θ então $e^{i\theta}z$ é o que obtemos ao rotacionarmos z por um ângulo θ, ou seja, a aplicação $z \mapsto e^{i\theta}z$ é a rotação dada pelo ângulo θ. Isto ocorre de forma similar nos quaternions: rotações do espaço euclidiano tridimensional serão escritas usando multiplicação de quaternions.

Mas por que o conjunto $\mathbb{C}$ existe? Até então apenas aceitamos isso por fé: fingimos que existe um objeto místico i satisfazendo $i^2 = -1$ e saímos fazendo conta.

A seguir vou construir elementos que funcionam iguaizinhos aos nossos números complexos e assim vou batizá-los de números complexos. A construção que farei não é a única possível[1], mas é mesmo assim especial porque me permitirá construir os quaternions mais tarde.

Comecemos a construção. Considere o espaço $\mathbb{C}$ das matrizes da forma

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix},$$

onde $a, b \in \mathbb{R}$. Repare que

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = aE + bI,$$

onde $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ e $I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

A matriz E pertence a $\mathbb{C}$ e se comporta como o número 1, pois se $A \in \mathbb{C}$ então $EA = AE = A$, e a matriz I também pertence a $\mathbb{C}$ e se comporta como o número i, pois

$$I^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -E.$$

Todo elemento de $\mathbb{C}$ se escreve como $aE + bI$, onde $a, b \in \mathbb{R}$. Se multiplicarmos dois elementos $a_1E + b_1I$ e $a_2E + b_2I$ de $\mathbb{C}$, o que é válido porque sempre podemos multiplicar duas matrizes 2×2, obtemos

$$(a_1E + b_1I)(a_2E + b_2I) = (a_1a_2 - b_1b_2)E + (a_1b_2 + a_2b_1)I,$$

que é um elemento de $\mathbb{C}$. Assim, a multiplicação está bem definida[2]. Com essas duas operações, esse espaço se comporta exatamente como queríamos e dessa forma podemos simplesmente definir

$$a + ib := aE + bI.$$

Logo, os números complexos existem.

[1]Poderíamos por exemplo definir $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$.

[2]Poderia acontecer de multiplicarmos dois elementos de $\mathbb{C}$ e obtemos algo que não está em $\mathbb{C}$, felizmente isso não ocorre.

2. O $\mathbb{R}^3$ não tem uma multiplicação legal igual a dos complexos

Gostaríamos que $\mathbb{R}^3$ tivesse uma multiplicação legal igual a dos complexos e assim poderíamos usá-la para fazer geometria espacial. Infelizmente, esse sonho é impossível[3], tal multiplicação não existe. Sejamos mais precisos.

Definição 1 *Considere o espaço vetorial real A com uma operação de multiplicação que associa a cada dois vetores x e y um terceiro vetor xy tal que as seguintes propriedades sejam satisfeitas:*

1. $\alpha(xy) = (\alpha x)y = x(\alpha y) \quad \forall x, y \in A, \forall \alpha \in \mathbb{R}$;
2. $(x + y)z = xz + yz \quad \forall x, y, z \in A$;
3. $x(y + z) = xy + xz \quad \forall x, y, z \in A$;
4. *Existe* $e \neq 0$ *tal que* $xe = ex = x \quad \forall x \in A$;
5. *Dados* $a \neq 0$ *e* b *em* A *existe um único* $x \in A$ *satisfazendo* $ax = b$ *e existe um único* $y \in A$ *satisfazendo* $ya = b$.

Dizemos então que A é uma álgebra de divisão real.

O elemento e no item 4 se chama unidade (ou 1 para os íntimos) e a quinta e última propriedade nos diz que sempre podemos resolver equações da forma $ax = b$ e $ya = b$ desde que $a \neq 0$. Na prática, precisamos apenas saber resolver as equações $ax = e$ e $ya = e$ onde $a \neq 0$. Se temos, por exemplo, a equação $ax = b$ e sabemos que a' satisfaz $aa' = e$ então $x = a'b$ resolve a equação $ax = b$. Para uma lista detalhada dos axiomas que definem uma álgebra de divisão veja a referência [1].

Tanto $\mathbb{R}$ quanto $\mathbb{C}$ são álgebras de divisão reais. A unidade em ambos é o número 1 e o último item é satisfeito porque podemos tomar $x = y = b/a$.

Repare que não dizemos nada sobre a álgebra de divisão real A ser comutativa ou associativa[4]. Os quaternions, que veremos a seguir, são associativos e não comutativos.

Teorema 2 *O espaço $\mathbb{R}^3$ não admite uma multiplicação que o torne em uma álgebra de divisão real.*

Demonstração: Faremos a prova por absurdo. Suponha que o espaço $\mathbb{R}^3$ admite uma multiplicação $(x, y) \mapsto xy$ que o torne em uma álgebra de divisão real. Para cada $a \in \mathbb{R}^3$ considere a transformação linear $f_a(x) = ax$ de $\mathbb{R}^3$ em $\mathbb{R}^3$. Se $\mathcal{L}(\mathbb{R}^3)$ é o espaço das transformações lineares de $\mathbb{R}^3$ em $\mathbb{R}^3$ então a função $a \mapsto f_a$ é uma transformação linear de $\mathbb{R}^3$ em $\mathcal{L}(\mathbb{R}^3)$. Assim, a função $a \mapsto f_a$ é contínua[5] e, consequentemente, a função $g : \mathbb{R}^3 \to \mathbb{R}$ dada por $g(a) = \det(f_a)$ é contínua.

Note que $f_e(x) = ex = x$ e $f_{-e}(x) = -ex = -x$, ou seja,

$$g(e) = \det \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = 1 \quad \text{e} \quad g(-e) = \det \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix} = -1.$$

Se $U = \mathbb{R}^3 \setminus \{0\}$ então $g(U)$ é um intervalo[6] contendo 1 e -1 porque U é conexo e $e, -e \in U$. Em particular $0 \in g(U)$ e, consequentemente, existe $a \in U$ satisfazendo $g(a) = \det(f_a) = 0$. Pela

[3] Nem todo sonho vira realidade.

[4] A álgebra A é associativa se $a(bc) = (ab)c$ para todo $a, b, c \in A$ e comutativa se $ab = ba$ para todo $a, b \in A$. As álgebras de divisão reais $\mathbb{R}$ e $\mathbb{C}$ são comutativas e associativas.

[5] Em dimensão finita, transformações lineares são sempre contínuas.

[6] Lembre-se que função contínua leva conexo em conexo e na reta os únicos conexos são os intervalos.

ultima propriedade que aparece na definição 1, existe $a' \in \mathbb{R}^3$ tal que $aa' = e$. Desta forma, $f_a \circ f_{a'}(x) = aa'x = x$, ou seja, $f_a \circ f_{a'} = id$ e, portanto, $\det(f_a)\det(f_{a'}) = 1$, que é uma contradição porque $\det(f_a) = 0$. ∎

Utilizando o mesmo argumento podemos provar o teorema acima para $\mathbb{R}^n$ com n ímpar diferente de 1, para $n = 1$ o argumento é inválido porque $U = \mathbb{R} \setminus \{0\}$ é desconexo.

3. Quaternions

Nossa construção de $\mathbb{C}$ nos permite pensar que o número $a + ib$ é a matriz

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}. \tag{3}$$

Um quaternion é uma matriz da forma

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}$$

onde z e w são números complexos. Repare que na matriz (3) não há conjugados, no entanto, se definirmos o conjugado de um número real como sendo ele mesmo então as duas matrizes têm mesmo formato. Deixemos nossos quaternions mais parecidos com números complexos.

Se $z = a + ib$ e $w = c + id$ então

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$$

de onde segue a identidade

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Se escrevermos

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad \text{e} \quad K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

então

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = aE + bI + cJ + dK.$$

Assim, podemos dizer que um quarternion é uma matriz da forma $aE + bI + cJ + dK$ onde $a, b, c, d \in \mathbb{R}$. O conjunto de todos os quaternions é denotado por $\mathbb{H}$ e claramente é um espaço vetorial real.

Repare que essas 4 matrizes E, I, J e K são linearmente independentes sobre $\mathbb{R}$ e formam uma base de $\mathbb{H}$, ou seja, $\mathbb{H}$ é um espaço vetorial real de dimensão 4.

A soma de dois quaternions é a soma vetorial. Queremos também multiplicar quaternions e por isso precisamos entender quais relações as matrizes E, I, J e K satisfazem entre si, por exemplo,

$$I^2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -E$$

e analogamente $J^2 = K^2 = -E$.

Além disso, existem relações da forma

$$IJ = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = K$$

e fazendo cálculos análogos ao acima obtemos

$$IJ = -JI = K, \quad KI = -IK = J, \quad JK = -KJ = I. \tag{4}$$

Em resumo, as seguintes relações são verdadeiras

$$I^2 = J^2 = K^2 = -E, \quad IJ = -JI = K, \quad KI = -IK = J, \quad JK = -KJ = I.$$

Em breve mostraremos que tais identidades têm interpretações geométricas simples, então não fique tão preocupado em decorá-las. Por essas relações sabemos elevar os elementos E, I, J e K a potências naturais ou multiplicá-los entre si. Assim, se multiplicarmos dois quarternions, o que é válido porque sempre podemos multiplicar matrizes 2×2, obtemos um novo quaternion. Além disso, essa multiplicação é associativa, isto é, se $u, v, w \in \mathbb{H}$ então $(uv)w = u(vw)$. Isto é verdade porque multiplicação para matrizes em geral é associativa quando nossos coeficientes são números reais ou complexos.

No entanto, a multiplicação não é comutativa já que $IJ = -JI \neq JI$.

Como E é a matriz identidade segue que E funciona como o número 1, isto é, $Eu = uE = u$ para todo $u \in \mathbb{H}$. Repare que com isso só falta a quinta propriedade da definição 1 para concluirmos que $\mathbb{H}$ é uma álgebra de divisão real. Verificaremos isso em breve.

A partir de agora usaremos uma notação mais enxuta e canônica para quaternions. Denotaremos $aE + bI + cJ + dK$ por $a + bi + cj + dk$, ou seja, nessa nova notação $1 = E$, $i = I$, $j = J$ e $k = K$.

Desta forma nosso espaço $\mathbb{H}$ é formado pelos números da forma $a + bi + cj + dk$, com $a, b, c, d \in \mathbb{R}$, e são válidas as seguintes relações

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

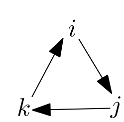
Repare que se nos restringirmos aos números da forma $a = a + 0i + 0j + 0k$ então obtemos os números reais e se nos restringirmos aos números da forma $a + bi = a + bi + 0j + 0k$ então obtemos os números complexos, ou seja, são válidas as inclusões $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$[7].

Quanto a aritmética, podemos somar e multiplicar números de $\mathbb{H}$ de forma similar ao que fazemos em $\mathbb{C}$. Por exemplo, se $u = 1 + i$ e $v = j + k$ então

$$uv = (1 + i)(j + k) = 1j + 1k + ij + ik = j + k + k + -j = 2k.$$

O único cuidado que devemos ter é que não podemos usar $uv = vu$ para quaisquer $u, v \in \mathbb{H}$.

A figura a direita é um lembrete das regras de multiplicação. Se escolhermos três vértices u, v e w no triângulo e esses forem escolhidos seguindo a ordem das setas então $uv = w$, caso contrário teremos $uv = -w$. Por exemplo, se escolhemos j, k e i então vemos que a escolha obedece a ordem do diagrama, ou seja, $jk = i$, no entanto, se tivéssemos tomado j, i e k então estamos no oposto da orientação das setas, ou seja, $ji = -k$.



Análogo ao que fazemos com números complexos, se $u = a + bi + cj + dk$ então definimos seu conjugado como sendo $\overline{u} = a - bi - cj - dk$.

[7] Repare que há vários jeitos de representar $\mathbb{C}$ em $\mathbb{H}$, por exemplo, os números $a + bj$ podem também ser vistos como números complexos já que $j^2 = -1$.

O espaço $\mathbb{H}$, visto como espaço vetorial real, é essencialmente o $\mathbb{R}^4$, já que podemos identificar $a + bi + cj + dk$ com (a, b, c, d). Assim, temos em $\mathbb{H}$ o produto interno usual de $\mathbb{R}^4$. Mais precisamente,

$$\langle x_1 + x_2 i + x_3 j + x_4 k, y_1 + y_2 i + y_3 j + y_4 k \rangle = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4.$$

Em particular $|a + ib + cj + dk| = \sqrt{a^2 + b^2 + c^2 + d^2}$.

Análogo aos complexos temos a seguinte fórmula.

Teorema 5 *Se $u \in \mathbb{H}$ então $u\overline{u} = \overline{u}u = |u|^2$.*

Demonstração: Nessa prova usarei a notação matricial. Se $u = a + bi + cj + dk$ então sabemos que

$$u = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix}$$

onde $z = a + bi$ e $w = c + di$. O conjugado $\overline{u}$ é a matriz adjunta de u [8]. De fato,

$$\overline{u} = aE - bI - cJ - dK = \begin{bmatrix} a - ib & -c - id \\ c - id & a + ib \end{bmatrix} = \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix}$$

ou seja,

$$\overline{u} = u^* = \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix}.$$

Portanto, temos

$$u\overline{u} = \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \begin{bmatrix} \overline{z} & -w \\ \overline{w} & z \end{bmatrix} = \begin{bmatrix} |z|^2 + |w|^2 & 0 \\ 0 & |z|^2 + |w|^2 \end{bmatrix} = (|z|^2 + |w|^2)E$$

e como $|z|^2 + |w|^2 = a^2 + b^2 + c^2 + d^2 = |u|^2$, segue que $u\overline{u} = |u|^2$.

Analogamente, $\overline{u}u = |u|^2$. ∎

Teorema 6 *As seguintes propriedades são válidas:*

- *Se $u, v \in \mathbb{H}$ então $\overline{uv} = \overline{v}\,\overline{u}$.*
- *Se $u, v \in \mathbb{H}$ então $|uv| = |u||v|$.*
- *Se $u \in \mathbb{H} \setminus \{0\}$ então $u^{-1} = \overline{u}/|u|^2$ satisfaz $uu^{-1} = u^{-1}u = 1$.*

Demonstração: O primeiro item sai por um argumento matricial simples. Basta notar que em notação matricial a expressão pode ser escrita como $(uv)^* = v^* u^*$.

O segundo item segue da seguinte observação: $|uv|^2 = uv\overline{uv} = uv\overline{v}\,\overline{u} = u|v|^2\overline{u} = |u|^2|v|^2$.

O terceiro item segue direto do teorema anterior. ∎

Observe que o último item nos garante que $\mathbb{H}$ é uma álgebra de divisão real, já que se $u, v \in \mathbb{H}$ e $u \neq 0$ então as equações $ux = v$ e $yu = v$ são resolvidas por $x = u^{-1}v$ e $y = vu^{-1}$, respectivamente.

[8] Se A é uma matriz com entradas complexas então sua adjunta é a matriz A^* obtida conjugando cada entrada de A e tomando a transposta. Por propriedades básicas de transposta temos que $(AB)^* = B^* A^*$

4. Quaternions e geometria

Nossa meta é entender a geometria do espaço euclidiano de dimensão 3 fazendo uso dos quaternions. O espaço tridimensional que estudaremos é o subespaço $\mathbb{E}$ de $\mathbb{H}$ gerado por i, j e k. Em outras palavras, um vetor u de $\mathbb{E}$ é da forma $u = ai + bj + ck$ onde $a, b, c \in \mathbb{R}$. Identificaremos $\mathbb{E}$ e $\mathbb{R}^3$ já que podemos reescrever $ai + bj + ck$ como (a, b, c) e vice-versa. O produto interno e a norma de $\mathbb{E}$ são os herdados de $\mathbb{H}$.

Calculemos uv onde $u, v \in \mathbb{E}$. Se $u = u_1 i + u_2 j + u_3 k$ e $v = v_1 i + v_2 j + v_3 k$ então

$$\begin{aligned} uv &= (u_1 i + u_2 j + u_3 k)(v_1 i + v_2 j + v_3 k) \\ &= -u_1 v_1 - u_2 v_2 - u_3 v_3 + (u_2 v_3 - u_3 v_2) jk + (u_1 v_3 - u_3 v_1) ik + (u_1 v_2 - u_2 v_1) ij \\ &= -(u_1 v_1 + u_2 v_2 + u_3 v_3) + (u_2 v_3 - u_3 v_2) i + (u_3 v_1 - u_1 v_3) j + (u_1 v_2 - u_2 v_1) k. \end{aligned}$$

A parcela $u_1 v_1 + u_2 v_2 + u_3 v_3$ é o produto interno $\langle u, v \rangle$ e a parcela $(u_2 v_3 - u_3 v_2) i + (u_3 v_1 - u_1 v_3) j + (u_1 v_2 - u_2 v_1) k$ é o produto vetorial[9] $u \times v$. Portanto, temos a seguinte identidade:

$$uv = -\langle u, v \rangle + u \times v.$$

Por simetria temos $vu = -\langle v, u \rangle + v \times u = -\langle u, v \rangle - u \times v$ e somando uv e vu obtemos

$$\langle u, v \rangle = -\frac{uv + vu}{2} \tag{7}$$

e subtraindo uv de vu temos

$$u \times v = \frac{uv - vu}{2}. \tag{8}$$

Assim, temos que as operações básicas usadas em geometria espacial se escrevem de jeito elementar usando multiplicação sobre os quaternions.

A identidade (7) nos garante que $uv + vu = 0$ se, e só se, $\langle u, v \rangle = 0$, ou seja, u e v anti-comutam, isto é, $uv = -vu$, se, e só se, u e v são perpendiculares. Já a identidade (8) nos diz que u e v comutam se, e só se, u e v são paralelos[10]. Em particular, as identidades $ij = -ji$, $ik = -ki$ e $ik = -ki$ são válidas porque i, j, k é uma base ortonormal.

Repare também que se u e v são perpendiculares então $uv = -vu$ e, consequentemente, pela identidade (8) temos

$$u \times v = uv.$$

Se u, v, w é uma base ortonormal então $uv = w$ ou $uv = -w$. Diremos que essa base é positivamente orientada se $uv = w$, ou seja, se os vetores u, v e w satisfazem a regra da mão direita.

Agora considere os vetores $u, v, w \in \mathbb{E}$ tais que

$$u^2 = v^2 = w^2 = -1,\ uv = -vu = w\,,\ vw = -wv = u \text{ e } wu = -uw = v. \tag{9}$$

A identidade $u^2 = -1$ nos diz que $|u| = 1$. De fato, como $u \in \mathbb{E}$ temos que $\overline{u} = -u$ e, portanto, $|u|^2 = u\overline{u} = -u^2 = 1$. Pelo mesmo motivo temos $|v| = 1$ e $|w| = 1$. As identidades $uv = -vu$, $vw = -wv$ e $wu = -uw$ nos garantem que os vetores u, v, w são dois a dois ortogonais. E a identidade $uv = w$ nos diz que os vetores u, v, w estão positivamente orientados. Assim, as relações (9) afirmam que u, v, w é base ortonormal positivamente orientada. Fica claro a partir daí que as relações que definem os quaternions têm caráter geométrico, elas simplesmente dizem que

[9] Como $\mathbb{E}$ e $\mathbb{R}^3$ estão identificados temos o produto vetorial em $\mathbb{E}$.

[10] Lembre-se que $u \times v = 0$ somente quando u e v são linearmente dependentes.

a base i, j, k é uma base ortonormal que satisfaz a regra da mão direita. Como existem infinitas bases satisfazendo essas especificações, não há nada de especial sobre i, j, k.

A essa altura do campeonato está claro o poder da álgebra como linguagem da geometria. Com somente uma operação conseguimos trivializar toda a geometria analítica.

Considere agora a esfera tridimensional $\mathbb{S}^3 = \{u \in \mathbb{H} : |u| = 1\}$. Para cada $u \in \mathbb{S}^3$ temos que u se escreve unicamente como $a.1 + v$ onde $a \in \mathbb{R}$ e $v \in \mathbb{E}$. Se $n = v/|v|$ então temos $u = a.1 + |v|n$ onde n é unitário, isto é, $|n| = 1$. Como $1 \perp n$ podemos aplicar o teorema de Pitágoras e obter $1 = |u|^2 = a^2 + |v|^2$, ou seja, existe θ tal que $a = \cos(\theta)$ e $|v| = \sin(\theta)$. Assim temos

$$u = \cos(\theta) + \sin(\theta)n,$$

ou seja, todo ponto da esfera pode ser escrito como $\cos(\theta) + \operatorname{sen}(\theta)n$ para algum $n \in \mathbb{E}$ unitário.

Análogo aos números complexos define-se

$$e^{\theta n} = \sum_{k=0}^{\infty} \frac{(\theta n)^k}{k!}$$

e como $n^2 = -n\overline{n} = -|n|^2 = -1$ segue

$$e^{\theta n} = \left[\theta - \frac{\theta^3}{3!} + \cdots\right] + \left[1 - \frac{\theta^2}{2!} + \cdots\right] n = \cos(\theta) + \operatorname{sen}(\theta)n.$$

E desta forma obtemos a fórmula de Euler para quaternions

$$e^{\theta n} = \cos(\theta) + \operatorname{sen}(\theta)n.$$

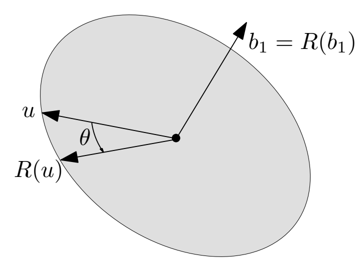
De maneira similar ao que ocorre nos números complexos, temos que $e^{\theta n}$ é um vetor de norma 1, ou seja, pertence a esfera $\mathbb{S}^3$. Além disso, como $e^{\theta n} = \cos(\theta) + \operatorname{sen}(\theta)n$ e $\overline{n} = -n$, a seguinte identidade é válida

$$\overline{e^{\theta n}} = \cos(\theta) - \operatorname{sen}(\theta)n = \cos(-\theta) + \operatorname{sen}(-\theta)n = e^{-\theta n}.$$

Sem muita surpresa, também valem as seguintes identidades: $e^{\theta_1 n} e^{\theta_2 n} = e^{(\theta_1 + \theta_2)n}$ e $e^0 = 1$.

A exponencial quaternionica é muito parecida com a dos números complexos. Geometricamente em $\mathbb{C}$ usamos a fórmula de Euler para parametrizar o cículo unitário $\mathbb{S}^1$ e aqui, no contexto dos quaternions, usamos a fórmula de Euler para parametrizar a esfera tridimensional $\mathbb{S}^3$.

Agora analisemos como funcionam as rotações de $\mathbb{E}$ usando quaternions. Considere uma rotação $R : \mathbb{E} \to \mathbb{E}$ de ângulo θ em torno do eixo dado pelo vetor unitário b_1. Faremos a descrição de R usando uma base ortonormal: existem mais dois vetores b_2, b_3 tais que b_1, b_2 e b_3 formam uma base ortonormal positivamente orientada ($b_3 = b_1 b_2$) e



$$\begin{aligned}
R(b_1) &= b_1, \\
R(b_2) &= \cos(\theta)b_2 + \operatorname{sen}(\theta)b_3, \\
R(b_3) &= -\operatorname{sen}(\theta)b_2 + \cos(\theta)b_3.
\end{aligned}$$

Note que como sabemos calcular R na base b_1, b_2 e b_3 então R está bem definida por ser linear.

Observação 10 *Toda isometria de $\mathbb{E}$ em $\mathbb{E}$ que tem determinante positivo é uma rotação e vice-versa. Assim, uma forma de definir rotação sem uso de base é a seguinte: Uma rotação de $\mathbb{E}$ é uma isometria com determinante positivo. Denotamos o espaço das rotações de $\mathbb{E}$ por $SO(3)$.*

Proposição 11 *Considere a rotação R de ângulo θ com eixo b_1 descrita acima. Se tomarmos $q = e^{\frac{\theta}{2}b_1}$ então $R(u) = qu\overline{q}$ para todo $u \in \mathbb{E}$.*

Demonstração: Considere a transformação linear $T(v) = qv\overline{q}$ com $v \in \mathbb{H}$. Não é claro ainda que essa aplicação leva vetores de $\mathbb{E}$ em $\mathbb{E}$. No entanto, mostraremos que $T(b_i)$ pertence a $\mathbb{E}$ para $i = 1, 2, 3$ de onde segue esse fato. Lembre-se que como b_1, b_2 e b_3 formam uma base ortonormal positivamente orientada valem as seguintes identidades

$$b_1^2 = b_2^2 = b_3^2 = -1\,, b_1b_2 = -b_2b_1 = b_3,\ b_2b_3 = -b_3b_2 = b_1 \text{ e } b_3b_1 = -b_3b_1 = b_2.$$

Pela expansão em série de $e^{\frac{\theta}{2}b_1}$ obtemos $qb_1 = b_1q$ e como $b_1^kb_2 = (-1)^kb_2b_1^k$ temos

$$qb_2 = \sum_{k=0}^{\infty}\left(\frac{\theta}{2}\right)^k b_1^kb_2 = \sum_{k=0}^{\infty}\left(\frac{\theta}{2}\right)^k(-1)^kb_2b_1^k = \sum_{k=0}^{\infty}\left(-\frac{\theta}{2}\right)^k b_2b_1^k = b_2\overline{q},$$

pois $\overline{q} = e^{-\frac{\theta}{2}b_1}$. Portanto, $qb_2 = b_2\overline{q}$ e analogamente $qb_3 = b_3\overline{q}$.

Logo,

$$\begin{aligned}
T(b_1) &= qb_1\overline{q} = b_1q\overline{q} = b_1e^{\frac{\theta}{2}b_1}e^{-\frac{\theta}{2}b_1} = b_1e^0 = b_1,\\
T(b_2) &= qb_2\overline{q} = q^2b_2 = e^{\theta b_1}b_2 = (\cos(\theta) + \operatorname{sen}(\theta)b_1)b_2 = \cos(\theta)b_2 + \operatorname{sen}(\theta)b_3,\\
T(b_3) &= qb_3\overline{q} = q^2b_3 = e^{\theta b_1}b_3 = (\cos(\theta) + \operatorname{sen}(\theta)b_1)b_3 = -\operatorname{sen}(\theta)b_2 + \cos(\theta)b_3.
\end{aligned}$$

Assim, T é uma transformação linear de $\mathbb{E}$ em $\mathbb{E}$ e coincide com R na base b_1, b_2, b_3, ou seja, $R = T$ em $\mathbb{E}$. ∎

Para mais informações sobre rotações e quaternions veja a referência [4].

5. Considerações finais

Para cada $q \in \mathbb{S}^3$ temos a rotação $R_q(v) = qv\overline{q}$ em $\mathbb{E}$. Repare que $R_{q_1} \circ R_{q_2} = R_{q_1q_2}$ e $R_q \circ R_{\overline{q}} = R_{\overline{q}} \circ R_q = Id$. Isso quer dizer $SO(3)$ é um grupo.

A esfera $\mathbb{S}^3$ também é um grupo. Se temos $u, v \in \mathbb{S}^3$ então $uv \in \mathbb{S}^3$ e se $u \in \mathbb{S}^3$ então $u\overline{u} = \overline{u}u = 1$. Esse grupo se chama $SU(2)$.

Assim, o que a proposição anterior diz é que existe uma função sobrejetora $R : SU(2) \to SO(3)$ que leva q na rotação R_q. Essa função é homomorfismo de grupos, isto é, para quaisquer $q_1, q_2 \in SU(2)$ temos que $R_{q_1q_2} = R_{q_1} \circ R_{q_2}$. O homomorfismo R não é injetor porque $R_{-q} = R_q$. No entanto, essa é a única redundância que esse mapa apresenta. Mais precisamente, dada uma rotação R_q só existem dois elementos de $\mathbb{S}^3$ que são levados a R_q pela aplicação R e esses pontos são os pontos q e $-q$. Por essa razão dizemos que tal aplicação é 2 para 1.

Essa aplicação é muito importante na teoria de grupos de Lie já que mostra que $SU(2)$ é o recobrimento universal do $SO(3)$. Como esse recobrimento é de 2 para 1 é possível tirar informações topológicas de $SO(3)$. Por exemplo, podemos mostrar que o primeiro grupo de homotopia de $SO(3)$ é $\mathbb{Z}/2\mathbb{Z}$.

Mais uma curiosidade que é facilmente obtida a partir desse mapa é que o espaço projetivo real $\mathbb{P}^3$, que é o conjunto de todas as retas passando por 0 em $\mathbb{H}$, pode ser identificado com $SO(3)$. A razão disso ser verdade é que $\mathbb{P}^3$ está em bijeção com o conjunto dos pares $\{q, -q\}$ onde $q \in \mathbb{S}^3$, pois uma reta de $\mathbb{P}^3$ corta em dois pontos antipodais de $\mathbb{S}^3$ e dois pontos antipodais de $\mathbb{S}^3$ determinam uma única reta passando pela origem.

Por fim, gostaria de avisá-los que a construção que fiz para os complexos e quaternions tem um nome, se chama construção de Cayley-Dickson. Assim como os quaternions são construídos a partir dos números complexos, começando-se com os quaternions obtemos os octonions. Na mesma proporção que quaternions são mais complicados que os números complexos, temos que os octonions são mais sofisticados que os quaternions. O conjunto dos octonions é denotado por $\mathbb{O}$ e também é uma álgebra de divisão, mas não é associativa nem comutativa. Para mais informações sobre a construção de Cayley-Dickson e octonions veja as referências [2], [3] e [5].

Referências

[1] MathWorld. Division Algebra.
`http://mathworld.wolfram.com/DivisionAlgebra.html`

[2] nLab. Cayley–Dickson construction.
`https://ncatlab.org/nlab/show/Cayley-Dickson+construction`

[3] Wikipedia. Cayley–Dickson construction.
`https://en.wikipedia.org/w/index.php?title=Cayley%E2%80%93Dickson_construction&oldid=818707025`

[4] Wikipedia. Quaternions and spatial rotation.
`https://en.wikipedia.org/wiki/Quaternions_and_spatial_rotation`

[5] Baez, John. The Octonions.
`http://math.ucr.edu/home/baez/octonions/octonions.html`