UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea Triennale in Matematica

Tesi di Laurea

QUATERNIONI E OTTONIONI

Relatore:
Prof.ssa LUISA FIOROT

Laureanda:
GIADA STROBBE

ANNO ACCADEMICO 2016-2017
21 Aprile 2017

Ai miei genitori

Indice

1 Quaternioni **6**

1.1 Storia 6

1.2 Forma vettoriale 8

1.3 Forma matriciale 13

2 Relazioni fra quaternioni e rotazioni nello spazio **17**

2.1 Rappresentazione polare 17

2.2 Relazione tra $\mathbb{H}^1$ e $SO_3(\mathbb{R})$ 20

2.3 Relazione tra $SU_2(\mathbb{C})$ e $SO_3(\mathbb{R})$ 23

2.4 Slerp 24

3 Ottonioni **26**

3.1 Storia 26

3.2 Forma vettoriale 26

3.3 La costruzione di Cayley-Dickson 36

3.4 Sedenioni 38

4 Teoremi di Frobenius e Hurwitz **39**

4.1 Teorema di Frobenius 39

4.2 Teorema di Hurwitz 42

4.3 I prodotti vettoriali 47

Introduzione

Già nel '500 matematici come Tartaglia, Bombelli e Cardano, cimentandosi nel problema della risoluzione delle equazioni algebriche, erano arrivati a introdurre i numeri complessi. A quell'epoca risultò abbastanza difficile accettare l'unità immaginaria i tale che $i^2 = -1$, dal momento che era un concetto non reale; ci volle Gauss per darne una vera e propria interpretazione: ogni numero complesso $a + ib$ rappresentava il punto di coordinate (a, b) sul piano. Quindi si arrivò a vedere che, in quel modo, si poteva costruire un'estensione bidimensionale di $\mathbb{R}$.

Successivamente si cercò di estendere i numeri complessi su un numero maggiore di dimensioni spaziali. Nel 1843 fu Hamilton che, dopo aver ricercato senza successo un'estensione tridimensionale, ne formulò una con dimensione quattro: i quaternioni, appunto. Egli fece questa scoperta mentre stava passeggiando lungo un canale a Dublino, quando improvvisamente gli venne in mente la soluzione nella forma dell'equazione $i^2 = j^2 = k^2 = ijk = -1$. Egli incise l'equazione sul lato del ponte Brougham; ora lì è presente una lapide che racconta la scoperta.

Hamilton decise poi, nell'ottobre del 1843, di inviare una lettera al suo amico Graves, da cui ebbe ispirazione per la scoperta dei quaternioni. Poco tempo dopo, nel dicembre del 1843, Graves descrisse gli ottonioni, anche se non pubblicò il suo lavoro fino al 1845, in risposta alla pubblicazione di Cayley della propria scoperta degli ottonioni. Ad entrambi viene quindi riconosciuta questa scoperta, appunto perchè ognuno dei due l'ha fatta in modo indipendente dall'altro.

Si può andare avanti con questo processo, detto di Cayley-Dickson, anche se man mano si procede si costruiscono strutture che hanno sempre meno proprietà delle precedenti.

Dando per noti i numeri complessi, nel primo capitolo andremo a definire i quaternioni e vedremo che l'insieme $\mathbb{H}$, con le opportune operazioni di somma e prodotto, risulta essere un corpo non commutativo. Andremo a descrivere ogni quaternione in forma vettoriale e in forma matriciale, definendo per ognuno di essi i concetti di coniugato, norma e, se il quaternione è non nullo, il concetto di inverso, con le relative proprietà.

Nel secondo capitolo andremo ad introdurre una rappresentazione più geometrica per i quaternioni e la rappresentazione polare (come quella dei numeri complessi). Queste costruzioni ci serviranno per vedere più facilmente che ogni quaternione interpreta una rotazione (attorno ad una retta) dello spazio tridimensionale. Come applicazione di ciò, alla fine del capitolo, si accennerà alla tecnica della slerp, usata per animare la rotazione 3D.

Nel terzo capitolo andremo a definire gli ottonioni e vedremo che l'insieme $\mathbb{O}$, con le opportune operazioni di somma e prodotto, risulta essere un'estensione non associativa dei quaternioni. In particolare è un'algebra di dimensione otto sul campo dei numeri reali, non associativa. Come quanto visto nel primo capitolo per i quaternioni, andremo a descrivere ogni ottonione in forma vettoriale, definendo i concetti di coniugato, norma e, se l'ottonione non è nullo, anche di inverso, con le loro proprietà. Successivamente vedremo gli ottonioni come coppie di quaternioni e quindi verrà introdotto il modello Cayley-Dickson, che sta alla base della costruzione di $\mathbb{C}, \mathbb{H}, \mathbb{O}$ e non solo; infatti, nell'ultima sezione, illustreremo i sedenioni, costruiti appunto sulla base di quel modello.

Infine, nell'ultimo capitolo, verranno enunciati i due principali risultati di Algebra attinenti ai capitoli precedenti con le realtive dimostrazioni: il Teorema di Frobenius e il Teorema di Hurwitz, con la conseguenza che un prodotto vettoriale come quello definito usualmente in $\mathbb{R}^3$ può esistere solo in $\mathbb{R}, \mathbb{R}^3, \mathbb{R}^7$.

Ho scelto di sviluppare questo argomento in quanto volevo approfondire meglio i quaternioni, di cui avevo già sentito parlare in modo superficiale in alcuni corsi durante il mio percorso triennale. Da qui poi ho notato che si può proseguire in avanti con altre strutture e quindi ho cercato di descriverle e di trovarne delle proprietà. Infine ho pensato di inserire dei risultati che accomunano o in qualche modo legano le strutture descritte nella tesi.

Capitolo 1

Quaternioni

In questo capitolo definiremo l'insieme dei quaternioni di Hamilton $\mathbb{H}$. Doteremo $\mathbb{H}$ di una somma e di un prodotto e dimostreremo che con tali operazioni risulta essere un corpo [1] non commutativo.

1.1 Storia

I quaternioni furono scoperti nel 1843 dall'irlandese William Rowan Hamilton (1805-1865). Egli era alla ricerca di un metodo per estendere i numeri complessi su un numero maggiore di dimensioni spaziali. Dopo aver ricercato senza alcun successo un'estensione tridimensionale, ne formulò una con dimensione quattro: i quaternioni.

In seguito Hamilton raccontò di aver fatto questa scoperta mentre passeggiava con la moglie lungo un canale a Dublino, quando improvvisamente gli venne in mente la soluzione nella forma dell'equazione:

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

Eccitato dalla scoperta, incise l'equazione sul lato del vicino ponte Brougham (ora noto come Broom Bridge). Sul Broom Bridge c'è ora una lapide che recita:

[1] Un corpo è un anello commutativo con unità in cui ogni elemento non nullo ha un inverso moltiplicativo.

« Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ and cut it on a stone of this bridge».[2]

I quaternioni fornirono il primo linguaggio naturale con il quale trattare fenomeni fisici, come l'elettromagnetismo. Il linguaggio moderno dell'analisi vettoriale fu introdotto solo dopo la metà del 1880 da Josiah Willard Gibbs, Oliver Heaviside e Hermann von Helmholtz. Dopo varie controversie, si scelse di usare il calcolo vettoriale e, ancora oggi, l'elettromagnetismo viene insegnato quasi esclusivamente con metodi vettoriali.

Oggi, i quaternioni vengono utilizzati principalmente nella rappresentazione delle rotazioni spaziali. Hanno applicazioni in settori che vanno dall'aeronautica e la robotica ai videogiochi. Ad esempio, è comune per i veicoli spaziali un sistema di controllo dell'assetto comandato mediante quaternioni, che sono anche usati per misurare mediante telemetria l'assetto attuale. La ragione è che la combinazione di molte trasformazioni descritte da quaternioni è più stabile numericamente della combinazione di molte trasformazioni matriciali.

[2](Mentre qui passeggiava, il 16 ottobre 1843 Sir William Rowan Hamilton, in un lampo d'ispirazione scoprì la formula fondamentale per la moltiplicazione dei quaternioni, e la incise su una pietra di questo ponte.)

1.2 Forma vettoriale

Definizione 1.1. *Sia $\mathbb{H}$ l'insieme di tutti gli elementi del tipo*

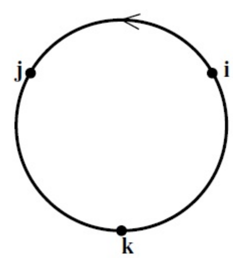
$$a + ib + jc + kd \quad \text{con} \quad a, b, c, d \in \mathbb{R} \quad \text{e} \quad i, j, k \quad \text{simboli}.$$

Definiamo su questo insieme le operazioni di somma e prodotto nel seguente modo:

- *somma:* $(a + ib + jc + kd) + (a' + ib' + jc' + kd') = (a + a') + i(b + b') + j(c + c') + k(d + d')$.
- *prodotto: pretendendo che il prodotto tra numeri reali sia quello di $\mathbb{R}$, basta definire i prodotti tra i simboli i, j, k.*

  Lo facciamo nel seguente modo:

  $i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik$ [3]



(ovvero i quadrati risultano tutti essere -1; i prodotti di due elementi consecutivi nell'ordine ciclico i, j, k dà l'elemento successivo, mentre i prodotti di due elementi consecutivi nell'ordine inverso dà l'opposto del terzo elemento).

Quindi, dati due elementi $z = a + ib + jc + kd$ e $z' = a' + ib' + jc' + kd'$ di $\mathbb{H}$, in base alla Definizione 1.1, si ha:

$zz' = (aa' - bb' - cc' - dd') + i(ab' + ba' + cd' - dc') + j(ac' + ca' + db' - bd') + k(ad' + da' + bc' - cb')$.

Gli elementi di $\mathbb{H}$ sono detti *quaternioni di Hamilton*.

In particolare, preso $r \in \mathbb{R}$ e $z = a + ib + jc + kd \in \mathbb{H}$, il loro prodotto è definito come:

$$rz = ra + irb + jrc + krd.$$

[3] In particolare, da qui si vede che il prodotto in $\mathbb{H}$ non è commutativo.

Le operazioni di somma e di moltiplicazione per scalari reali dotano l'insieme $\mathbb{H}$ di una struttura di *spazio vettoriale reale* di dimensione quattro ed una sua base è $1, i, j, k$.

Il prodotto sopra definito è bilineare.

Inoltre le operazioni di somma e prodotto dotano $\mathbb{H}$ di una struttura di anello.

Dato un quaternione $z = a + ib + jc + kd$, $a = \Re z$ si dirà *parte reale* di z, mentre $ib + jc + kd = \Im z$ si dirà *parte immaginaria* di z.[4] Perciò $z = \Re z + \Im z$.

Un quaternione $z = a + ib + jc + kd$ può essere rappresentato da una 4-upla di numeri reali (a, b, c, d), e quindi è possibile vederlo come un punto o un vettore in $\mathbb{R}^4$.

Vediamo che possiamo inoltre scrivere z nella forma:

$$z = (a + ib) + (c + id)j;$$

perciò un quaternione può essere visto anche come una coppia di numeri complessi $(z_{1_{\mathbb{C}}}, z_{2_{\mathbb{C}}}) = (a + ib, c + id)$, o equivalentemente possiamo scrivere $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$.

I quaternioni contengono in modo naturale:

- i numeri reali ($r = (r, 0, 0, 0)$, $r \in \mathbb{R}$),
- i numeri complessi ($a + ib = (a, b, 0, 0), a, b \in \mathbb{R}$),
- i vettori in $\mathbb{R}^3$ ($\vec{v} = (0, v_1, v_2, v_3), v_i \in \mathbb{R}$, dove i, j, k sono in questo caso i versori di un sistema di riferimento cartesiano destrorso).

Anche per i quaternioni, in analogia con i numeri complessi, si definiscono i concetti di *coniugato* e di *norma*. Inoltre ogni quaternione diverso da zero possiede un *inverso* rispetto al prodotto. Si differenziano però dai complessi per il fatto che il loro prodotto non è commutativo.

Definizione 1.2 (Coniugato)**.** *Dato un elemento $z = a+ib+jc+kd$ di $\mathbb{H}$, il suo coniugato è il quaternione $\overline{z} = a-ib-jc-kd = a+i(-b)+j(-c)+k(-d)$.*

Un quaternione z si dice:

- *puramente reale se $b = c = d = 0$, quindi $z = \Re z$,*
- *puramente immaginario se $a = 0$, quindi $z = \Im z$.*

[4]La notazione differente per la parte immaginaria rispetto a quella usata per i numeri complessi non ha conseguenze ed è dettata dalla tradizione.

Proposizione 1.3. *Il coniugato, come funzione* $\overline{\cdot}\colon \mathbb{H} \to \mathbb{H}$, *soddisfa le seguenti proprietà:*

1. *rispetta la somma:* $\overline{z+z'} = \overline{z} + \overline{z'}$,
2. $\overline{z} = z$ *se e solo se* z *è puramente reale,*

   $\overline{z} = -z$ *se e solo se* z *è puramente immaginario,*
3. *(anti) rispetta il prodotto:* $\overline{zz'} = \overline{z'}\,\overline{z}$,
4. $z\overline{z} = \overline{z}z = a^2 + b^2 + c^2 + d^2$ *è puramente reale per ogni* $z = a + ib + jc + kd \in \mathbb{H}$, *ed è un numero positivo se* $z \neq 0$,
5. $\overline{\overline{z}} = z$ *per ogni* $z \in \mathbb{H}$.

Dimostrazione. Siano $z = a + ib + jc + kd, z' = a' + ib' + jc' + kd' \in \mathbb{H}$.

1. Per la Definizione 1.1, $z+z' = (a+a')+i(b+b')+j(c+c')+k(d+d')$.

$$\begin{aligned}\overline{z+z'} &= (a+a') - i(b+b') - j(c+c') - k(d+d') = \\ &= (a - ib - jc - kd) + (a' - ib' - jc' - kd') = \\ &= \overline{z} + \overline{z'}.\end{aligned}$$

2. $\overline{z} = z$ se e solo se $a = a, b = -b, c = -c, d = -d$ (ma a, b, c, d sono numeri reali perciò questo accade) se e solo se $a \in \mathbb{R}$ e $b = c = d = 0$ se e solo se, dalla Definizione 1.2, z è puramente reale.

   $\overline{z} = -z$ se e solo se $a = -a, b = b, c = c, d = d$ se e solo se $a = 0$ e $b, c, d \in \mathbb{R}$ se e solo se, dalla Definizione 1.2, z è puramente immaginario.

3. Per la Definizione 1.1, $zz' = (aa' - bb' - cc' - dd') + i(ab' + ba' + cd' - dc') + j(ac' + ca' + db' - bd') + k(ad' + da' + bc' - cb')$; quindi si ha che $\overline{zz'} = (aa' - bb' - cc' - dd') - i(ab' + ba' + cd' - dc') - j(ac' + ca' + db' - bd') - k(ad' + da' + bc' - cb')$.

   Poi, essendo $\overline{z'} = a' - ib' - jc' - kd'$ e $\overline{z} = a - ib - jc - kd$, si ha che $\overline{z'}\,\overline{z} = (a'a - b'b - c'c - d'd) + i(-a'b - b'a + c'd - d'c) + j(-a'c - c'a + d'b - b'd) + k(-a'd - d'a + b'c - c'b) = (aa' - bb' - cc' - dd') - i(ab' + ba' + cd' - dc') - j(ac' + ca' + db' - bd') - k(ad' + da' + bc' - cb')$.

4. Si verifica facilmente che $z\overline{z} = \overline{z}z = a^2 + b^2 + c^2 + d^2$, che risulta essere un numero puramente reale (in quanto somma di reali). Ovviamente quel prodotto è sempre positivo tranne quando $a^2 + b^2 + c^2 + d^2 = 0$, ovvero quando $a = b = c = d = 0$, cioè $z = 0$.

5. Dal momento che $\overline{z} = a - ib - jc - kd = a + i(-b) + j(-c) + k(-d)$, allora $\overline{\overline{z}} = a - i(-b) - j(-c) - k(-d) = a + ib + jc + kd = z$.

$\square$

Definizione 1.4 (Norma)**.** *Dato un elemento $z = a + ib + jc + kd$ di $\mathbb{H}$, la sua norma è il numero reale non negativo $\|z\| = \sqrt{z\overline{z}}$. Dunque, per la Proposizione 1.3, in particolare si ha:*

$$\|z\| = \sqrt{a^2 + b^2 + c^2 + d^2} \in \mathbb{R}_{\geq 0}.$$

Proposizione 1.5. *La norma, come funzione $\|\cdot\| \colon \mathbb{H} \to \mathbb{R}_{\geq 0}$, soddisfa le seguenti proprietà:*

1. $\|z\|^2 = z\overline{z} = \overline{z}z = \|\overline{z}\|^2$ *per ogni* $z \in \mathbb{H}$,
2. *positività:* $\|z\| \geq 0$ *per ogni* $z \in \mathbb{H}$ *e* $\|z\| = 0 \iff z = 0$,
3. *moltiplicatività:* $\|zz'\| = \|z\|\|z'\|$,
4. *sub-additività:* $\|z + z'\| \leq \|z\| + \|z'\|$.

Dimostrazione. Siano $z = a + ib + jc + kd, z' = a' + ib' + jc' + kd' \in \mathbb{H}$.

1. Segue immediatamente dalla Proposizione 1.3.
2. $\|z\| = \sqrt{a^2 + b^2 + c^2 + d^2} \geq 0$ per ogni $z \in \mathbb{H}$ (in quanto radice reale di una somma di quadrati reali) e $\|z\| = 0 \iff \sqrt{a^2 + b^2 + c^2 + d^2} = 0 \iff a^2 + b^2 + c^2 + d^2 = 0 \iff a = b = c = d = 0 \iff z = 0$.
3. Al quaternione $z = a + ib + jc + kd$, facciamo corrispondere la matrice $Z = \mathbf{1}a + Ib + Jc + Kd = \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix}$,

   dove le matrici $\mathbf{1}, I, J, K \in M_2(\mathbb{C})$ sono le seguenti:

   $$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

   Si osservi che si ha:

   $I^2 = J^2 = K^2 = -\mathbf{1}, \quad IJ = K = -JI, \quad JK = I = -KJ, \quad KI = J = -IK.$

   Si ha quindi che $det(Z) = (a + ib)(a - ib) - (-c + id)(c + id) = a^2 - iab + iba + b^2 - (-c^2 - icd + idc - d^2) = a^2 + b^2 + c^2 + d^2 = \|z\|^2$. Se Z'

è la matrice associata al quaternione z', per il Teorema di Binet [5] si ha che $det(ZZ') = det(Z)det(Z')$, dunque $\|zz'\|^2 = \|z\|^2\|z'\|^2$. Essendo questi numeri reali non negativi, la conclusione si ottiene eliminando i quadrati.

4. Essendo $\mathbb{H}$ uno spazio vettoriale su $\mathbb{R}$, sappiamo che esiste un isomorfismo $\varphi\colon \mathbb{R}^4 \to \mathbb{H}$ di $\mathbb{R}$-spazi vettoriali, che manda un vettore $v = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \mathbb{R}^4$, nell'elemento $\varphi(v) = a + ib + jc + kd \in \mathbb{H}$.

   Abbiamo poi che:

$$\|v\|_{\mathbb{R}^4} = \| \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \|_{\mathbb{R}^4} = \sqrt{a^2 + b^2 + c^2 + d^2} = \|a+ib+jc+kd\|_{\mathbb{H}} = \|\varphi(v)\|_{\mathbb{H}},$$

   quindi φ rispetta le norme (perché la norma in $\mathbb{R}^4$ è definita come $\|z\| = \sqrt{z \cdot z}$). Inoltre, in $\mathbb{R}^4$ vale la disuguaglianza di Cauchy-Schwarz[6], quindi si ha che:

$$\|v + w\|_{\mathbb{R}^4} \leq \|v\|_{\mathbb{R}^4} + \|w\|_{\mathbb{R}^4}, \quad v, w \in \mathbb{R}^4,$$

   e quindi

$$\|\varphi(v + w)\|_{\mathbb{H}} \leq \|\varphi(v)\|_{\mathbb{H}} + \|\varphi(w)\|_{\mathbb{H}},$$

   ma $\varphi(v + w) = \varphi(v) + \varphi(w)$, e dunque si ottiene:

$$\|\varphi(v) + \varphi(w)\|_{\mathbb{H}} \leq \|\varphi(v)\|_{\mathbb{H}} + \|\varphi(w)\|_{\mathbb{H}}.$$

   Chiamando infine $\varphi(v) = z, \varphi(w) = z'$, si ottiene proprio che

$$\|z + z'\|_{\mathbb{H}} \leq \|z\|_{\mathbb{H}} + \|z'\|_{\mathbb{H}}.$$

□

[5] Il teorema di Binet afferma che, data una matrice quadrata A a coefficienti nel campo C, la matrice è invertibile se e solo se $det(A) \neq 0$ e, date A,B matrici in $M_n(C), det(AB) = det(A)det(B)$.

[6] La disuguaglianza di Cauchy-Schwarz afferma che per ogni coppia di vettori $v, w \in \mathbb{R}^n$, si ha $|v \cdot w| \leq \|v\|\|w\|$ e vale l'uguaglianza se, e solo se, v e w sono linearmente dipendenti. In particolare, implica la disuguaglianza triangolare:
$\|v + w\|^2 = (v + w) \cdot (v + w) = v \cdot v + 2v \cdot w + w \cdot w \leq v \cdot v + 2|v \cdot w| + w \cdot w \leq \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 = (\|v\| + \|w\|)^2$.

Proposizione 1.6 (Identità dei quattro quadrati)**.** *Il prodotto di due somme di quattro quadrati è ancora una somma di quattro quadrati:*

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2) =\\ &(aa'-bb'-cc'-dd')^2+(ab'+ba'+cd'-dc')^2+\\ &(ac'+ca'+db'-bd')^2+(ad'+da'+bc'-cb')^2.\end{aligned}$$

Dimostrazione. Segue dalla moltiplicatività della norma: $\|zz'\| = \|z\|\|z'\|$; quindi, sostituendo in $\|z\|^2\|z'\|^2 = \|zz'\|^2$ i quaternioni $z = a+ib+jc+kd, z' = a'+ib'+jc'+kd'$, si ottiene l'identità voluta. □

Ricordando che l'inverso di un elemento non nullo z in un anello è l'*unico* elemento z' tale che $zz' = z'z = 1$, si ha:

Proposizione 1.7. *Dato un elemento $z = a+ib+jc+kd$ non nullo di $\mathbb{H}$, il suo inverso è $z^{-1} = \frac{\overline{z}}{\|z\|^2}$.*[7]

Inoltre l'inverso soddisfa le seguenti proprietà:

- $\|z^{-1}\| = \frac{1}{\|z\|}$,
- $\overline{z^{-1}} = \overline{z}^{-1}$,
- $(zz')^{-1} = z'^{-1}z^{-1}$.

Dimostrazione. Dalla Proposizione 1.5, abbiamo che $z\overline{z} = \overline{z}z = \|z\|^2$. Se $z \neq 0$, allora anche $\|z\| \neq 0$ e quindi possiamo dividere i membri per $\|z\|^2$. Si ottiene:

$$z\frac{\overline{z}}{\|z\|^2} = \frac{\overline{z}}{\|z\|^2}z = 1.$$

Le proprietà dell'inverso si deducono dalle Proposizioni 1.3 e 1.5. □

1.3 Forma matriciale

Nella dimostrazione della Proposizione 1.5, abbiamo utilizzato la possibilità di esprimere un quaternione tramite matrici 2×2 a coefficienti complessi.

Definizione 1.8. *Il quaternione $z = a+ib+jc+kd = (a+ib)+(c+id)j$, con $z_1 = a+ib, z_2 = c+id$, può essere rappresentato dalla matrice 2×2 a coefficienti complessi:*

$$Z = \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1}\end{pmatrix}, \quad \textit{con} \quad z_1, z_2 \in \mathbb{C},$$

[7] Una volta dimostrato questo, abbiamo che $\mathbb{H}$ è un corpo (non commutativo).

ovvero dalla matrice

$$Z = \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}.$$

Proposizione 1.9. *La forma matriciale dei quaternioni permette di definire una funzione*

$$\begin{array}{rccc} \alpha: & \mathbb{H} & \longrightarrow & M_2(\mathbb{C}) \\ & z & \longmapsto & Z \end{array}$$

che risulta essere un omomorfismo iniettivo di anelli.

Dimostrazione. Siano $z = a + ib + jc + kd, z' = a' + ib' + jc' + kd' \in \mathbb{H}$.

1. $\alpha(0) = \mathbf{0}$;

   $\alpha(z) = \mathbf{0}$ implica $z = 0$ (questo dimostra che l'omomorfismo è iniettivo).

2. $\alpha(z + z') = \alpha(z) + \alpha(z')$:
   Dalla Definizione 1.1, $z+z' = (a+a')+i(b+b')+j(c+c')+k(d+d') = ((a + a') + i(b + b')) + ((c + c') + i(d + d'))j$;

$$\begin{aligned}\alpha(z+z') &= \begin{pmatrix} (a+a')+i(b+b') & (c+c')+i(d+d') \\ -(c+c')+i(d+d') & (a+a')-i(b+b') \end{pmatrix} = \\ &= \begin{pmatrix} (a+ib)+(a'+ib') & (c+id)+(c'+id') \\ (-c+id)+(-c'+id') & (a-ib)+(a'-ib') \end{pmatrix} = \\ &= \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} + \begin{pmatrix} a'+ib' & c'+id' \\ -c'+id' & a'-ib' \end{pmatrix} = \\ &= \alpha(z) + \alpha(z').\end{aligned}$$

3. $\alpha(-z) = -\alpha(z)$:
   se $\alpha(z) = \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$, allora

$$\alpha(-z) = \begin{pmatrix} -a-ib & -c-id \\ c-id & -a+ib \end{pmatrix} = -\alpha(z),$$

   in quanto

$$\alpha(z)+\alpha(-z) = \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} + \begin{pmatrix} -a-ib & -c-id \\ c-id & -a+ib \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

4. $\alpha(1) = \begin{pmatrix} 1 & 0 \\ \overline{0} & \overline{1} \end{pmatrix} = \mathbf{1}$.

5. $\alpha(zz') = \alpha(z)\alpha(z')$:

   Dalla Definizione 1.1, $zz' = (aa' - bb' - cc' - dd') + i(ab' + ba' + cd' - dc') + j(ac' + ca' + db' - bd') + k(ad' + da' + bc' - cb') = (aa' - bb' - cc' - dd') + i(ab' + ba' + cd' - dc') + ((ac' + ca' + db' - bd') + i(ad' + da' + bc' - cb'))j$.

   Siano ora $\beta = (aa' - bb' - cc' - dd'), \gamma = (ab' + ba' + cd' - dc'), \delta = (ac' + ca' + db' - bd'), \eta = (ad' + da' + bc' - cb')$ e siano $z = z_1 + z_2 j,\ z' = z'_1 + z'_2 j$. Allora abbiamo:

$$\begin{aligned} \alpha(zz') &= \begin{pmatrix} \beta + i\gamma & \delta + i\eta \\ -\delta + i\eta & \beta - i\gamma \end{pmatrix} = \\ &= \begin{pmatrix} z_1 z'_1 + z_2(-\overline{z'_2}) & z_1 z'_2 + z_2 \overline{z'_1} \\ -\overline{z_2} z'_1 + \overline{z_1}(-\overline{z'_2}) & -\overline{z_2} z'_2 + \overline{z_1}\overline{z'_1} \end{pmatrix} = \\ &= \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix} \begin{pmatrix} a' + ib' & c' + id' \\ -c' + id' & a' - ib' \end{pmatrix} = \\ &= \alpha(z)\alpha(z'). \end{aligned}$$

6. Dimostriamo che $\alpha(z^{-1}) = \alpha(z)^{-1}$.

   Noto che $det(\alpha(z)) = det \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix} = a^2 + b^2 + c^2 + d^2 = \|z\|^2_{\mathbb{H}}$, quindi tutti gli elementi di $\mathbb{H}$ non nulli sono invertibili e si ha che:

   $\alpha(z)^{-1} = \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix}^{-1} = \frac{1}{\|z\|^2} \begin{pmatrix} a - ib & -c - id \\ c - id & a + ib \end{pmatrix} = \alpha(z^{-1})$.
   Pertanto l'inverso di un elemento non nullo di $\mathbb{H}$ è ancora un elemento non nullo di $\mathbb{H}$.

□

Quindi, dato $z \in \mathbb{H}$, z corrisponderà alla matrice $Z = \mathbf{1}a + Ib + Jc + Kd$, dove $a = \Re Z$, $Ib + Jc + Kd = \Im Z$. In notazione matriciale, risulterà dunque

$$Z = \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix}.$$

Il coniugato $\overline{z}$ di z, corrisponde alla matrice coniugata trasposta di Z, ovvero alla matrice aggiunta di Z, ovvero a $Z^* = {}^t\overline{Z}$, che è anche la matrice dei complementi algebrici.[8]

Dunque,

$$Z^* = \begin{pmatrix} a - ib & -c - id \\ c - id & a + ib \end{pmatrix},$$

cioè $\alpha(\overline{z}) = {}^t\overline{Z}$.

[8]Data una matrice $A = (a_{ij})_{1 \leq i,j \leq n}$ di ordine n a coefficienti nel campo C, la *matrice dei complementi algebrici di* A è la matrice $A^c = (a^c_{ij})_{1 \leq i,j \leq n}$ ove $a^c_{ij} = (-1)^{i+j} det(A_{ji})$ con A_{ji} la matrice di ordine n-1 che si ottiene da A cancellando la riga j-esima e la colonna i-esima.

Se poi la matrice $A = (a_{ij})_{1 \leq i,j \leq n} \in M_n(C)$ è invertibile, allora $A^{-1} = \frac{1}{det(A)} A^c$, ossia l'elemento di posto (i, j) di A^{-1} è uguale a $\frac{(-1)^{i+j} det(A_{ji})}{det(A)}$.

Capitolo 2

Relazioni fra quaternioni e rotazioni nello spazio

In questo capitolo introdurremo una notazione più geometrica per descrivere i quaternioni e le loro operazioni. In particolare vedremo che essi interpretano l'insieme delle rotazioni (attorno a rette) di uno spazio vettoriale reale di dimensione tre.

2.1 Rappresentazione polare

Denotiamo

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{I} = \langle 1 \rangle \oplus \langle i, j, k \rangle,$$

dove gli elementi appartenenti a $\mathbb{R}$ sono i numeri reali e quelli appartenenti a $\mathbb{I}$ si dicono *quaternioni speciali o puramente immaginari*.

Identificando $\mathbb{I}$ con $\mathbb{R}^3$, possiamo introdurre in $\mathbb{I}$ le operazioni di *prodotto scalare* e *prodotto vettoriale*:

dati $v = ib + jc + kd, v' = ib' + jc' + kd' \in \mathbb{I}$, abbiamo che:

- prodotto scalare:
$$v \cdot v' = bb' + cc' + dd' \in \mathbb{R}, \tag{2.1}$$

- prodotto vettoriale:
$$\begin{aligned} v \times v' &= i(cd' - dc') - j(bd' - db') + k(bc' - cb') = \\ &= i(cd' - dc') + j(db' - bd') + k(bc' - cb') \in \mathbb{I}. \end{aligned} \tag{2.2}$$

Quindi il sottocorpo dei quaternioni puramente reali è isomorfo a $\mathbb{R}$ e il sottoinsieme $\mathbb{I}$ dei quaternioni puramente immaginari è uno spazio vettoriale reale di dimensione tre, in cui l'operazione di prodotto corrisponde all'operazione di prodotto vettoriale tra vettori in $\mathbb{R}^3$. Inoltre $\{i, j, k\}$ risulta essere una base *ortonormale* di $\mathbb{I}$.

Definizione 2.1. *Il quaternione $z = a + ib + jc + kd \in \mathbb{H}$ può essere anche rappresentato dalla coppia*

$$z = (a, v),$$

ove $a \in \mathbb{R}$ è la componente scalare di z e $v = ib+jc+kd \in \mathbb{I}$ è la componente vettoriale (o puramente immaginaria) di z.

In particolare, dati $z = (a, v), z' = (a', v') \in \mathbb{H}$, possiamo riscrivere le operazioni di *somma* e di *prodotto* nel seguente modo:

- somma: $z + z' = (a, v) + (a', v') = (a + a', v + v')$,
- prodotto: $zz' = (a, v)(a', v') = (aa' - v \cdot v', av' + a'v + v \times v')$. [1]

Definizione 2.2 (Coniugato)**.** *Il coniugato del quaternione $z = (a, v)$ è:*

$$\overline{z} = (a, -v).$$

Definizione 2.3 (Norma)**.** *La norma del quaternione $z = (a, v)$ è:*

$$\|(a, v)\| = \sqrt{a^2 + v \cdot v}.$$

Un quaternione si dice unitario se ha norma 1*.*
L'insieme dei quaternioni unitari si indica con $\mathbb{H}^1$:

$$\mathbb{H}^1 = \{u \in \mathbb{H} \mid \|u\| = 1\}.$$

I quaternioni hanno una *rappresentazione polare* analoga a quella dei numeri complessi.[2] Per ricavarla, osserviamo che dato $z \in \mathbb{H}$, $z = a + ib + jc + kd$ tale che $\Im z = ib + jc + kd \neq 0$, il vettore $\frac{\Im z}{\|\Im z\|} \in \mathbb{S}^2$(sfera) $\subset \mathbb{I}$ ed è unitario.

Proposizione 2.4 (Rappresentazione polare)**.** *Dato $z \in \mathbb{H}$ tale che $\Im z \neq 0$, esiste $\theta \in \mathbb{R}, \theta \in [0, \pi)$ tale che*

$$z = \|z\|(\cos\theta + \frac{\Im z}{\|\Im z\|} \sin\theta).$$

[1] Ove $v \cdot v'$ e $v \times v'$ indicano il prodotto scalare e il prodotto vettoriale in $\mathbb{I}$ definiti in 2.1 e 2.2.

[2] Dato un numero complesso $z = a+ib \neq 0$, la rappresentazione polare è: $z = |z|(\cos\theta + i\sin\theta)$, dove $|z|$ è il modulo (numero reale non negativo) del numero complesso, mentre θ è l'argomento del numero complesso.

Se poi u è quaternione unitario, allora:

$$u = \cos\theta + \frac{\Im u}{\|\Im u\|}\sin\theta,$$

ovvero si può scrivere nella forma:

$$u = (\cos\theta, \sin\theta v),^{3}$$

con $v \in \mathbb{S}^2 \subset \mathbb{I}$ *unitario (ovvero* $v = \frac{\Im u}{\|\Im u\|}$*).*

Dimostrazione. Possiamo supporre che il quaternione sia unitario (altrimenti basta dividere per la sua norma, che per ipotesi è diversa da zero dal momento che $\Im z \neq 0$).

Posto ora $u = \alpha+\beta = a+ib+jc+kd$, $\alpha = a = \Re u$, $\beta = ib+jc+kd = \Im u$, abbiamo che $\overline{\alpha} = \alpha$ e $\overline{\beta} = -\beta$ (poiché α è puramente reale e β è puramente immaginario) e $\|\alpha\|^2 + \|\beta\|^2 = (\alpha)^2 + \|\beta\|^2 = a^2 + (b^2+c^2+d^2) = \|u\|^2 = 1$. Dunque basta scegliere θ tale che $\cos\theta = \alpha$ e $\sin\theta = \|\beta\|$. Ed essendo poi che $\sin\theta \geq 0$ (perché, per definizione, la norma è sempre non negativa), si può scegliere $\theta \in [0,\pi)$. □

Perciò un quaternione unitario u individua un *versore* v nello spazio tridimensionale e un *angolo* $\theta \in [0,\pi)$.

Proposizione 2.5. *Siano* $v, v' \in \mathbb{I}$. *Allora esiste una formula che lega il prodotto tra quaternioni puramente immaginari con il prodotto scalare e quello vettoriale definiti in 2.1 e 2.2:*

$$vv' = -v \cdot v' + v \times v' \in \mathbb{H}.$$

Dimostrazione. Siano $v = ib + jc + kd, v' = ib' + jc' + kd' \in \mathbb{I} \subset \mathbb{H}$. Allora, per la Definizione 1.1, a sinistra abbiamo:

$vv' = (-bb' - cc' - dd') + i(cd' - dc') + j(db' - bd') + k(bc' - cb')$.

A destra abbiamo:

$$\begin{aligned} -v \cdot v' + v \times v' &= -(bb' + cc' + dd') + i(cd' - dc') + j(db' - bd') + k(bc' - cb') \\ &= (-bb' - cc' - dd') + i(cd' - dc') + j(db' - bd') + k(bc' - cb'). \end{aligned}$$

□

[3] È unitario perché, dalla Definizione 2.3, si ha che:

$$\begin{aligned} \|u\| &= \|(\cos\theta, \sin\theta v)\| = \\ &= \sqrt{(\cos\theta)^2 + (\sin\theta v)\cdot(\sin\theta v)} = \\ &= \sqrt{(\cos\theta)^2 + (\sin\theta)^2 (v \cdot v)} = \\ &= \sqrt{(\cos\theta)^2 + (\sin\theta)^2} = 1. \end{aligned}$$

2.2 Relazione tra $\mathbb{H}^1$ e $SO_3(\mathbb{R})$

Vogliamo vedere che ogni quaternione unitario rappresenta un elemento di $SO_3(\mathbb{R})$ [4] e vogliamo determinare quando due quaternioni unitari rappresentano la stessa rotazione dello spazio euclideo.

Consideriamo ora il sottoinsieme $\mathbb{H}^1$ di $\mathbb{H}$ dei quaternioni unitari:

$$\mathbb{H}^1 = \{u \in \mathbb{H} | \|u\| = 1\}.$$

Per dimostrare la prossima Proposizione (la più importante di tutto il capitolo), abbiamo bisogno del seguente lemma:

Lemma 2.6. *Siano v e x due vettori dello spazio euclideo $\mathbb{R}^3$, con $\|v\| = 1$. Allora:*

1. *$x = (v \times x) \times v + (v \cdot x)v$.*
2. *$\|v \times x\| = \|(v \times x) \times v\|$ e i vettori $(v \times x) \times v, v \times x, v$ formano una base ortogonale concorde con la base canonica se $x \notin \langle v \rangle$.*
3. *$\varrho(x) = \cos\theta(v \times x) \times v + \sin\theta v \times x + (v \cdot x)v$ è il vettore che si ottiene ruotando x attorno alla retta $\langle v \rangle$ di un angolo θ in senso antiorario (con l'asse orientato col vettore v).*

Dimostrazione. 1. Al secondo membro dell'uguaglianza abbiamo (usando la formula del doppio prodotto vettore [5]):

$$\begin{aligned}(v \times x) \times v + (v \cdot x)v &= -v \times (v \times x) + (v \cdot x)v = \\ &= v(x \cdot (-v)) - x(-v \cdot v) + (v \cdot x)v = \\ &= -v(x \cdot v) + x(v \cdot v) + (v \cdot x)v = \\ &= -v(x \cdot v) + x + (v \cdot x)v \\ &= x.\end{aligned}$$

[4] Il gruppo ortogonale, ossia il gruppo delle trasformazioni ortogonali su C^n, viene identificato con il gruppo delle matrici ortogonali:

$$O_n(C) = \{P \in GL_n(C) | {}^tPP = 1_n\}$$

(ad ogni trasformazione ortogonale viene associata la sua matrice rispetto alla base canonica). Il sottogruppo delle trasformazioni ortogonali *speciali*, cioè quelle di determinante 1, viene indicato con $SO_n(C)$.

[5] Il doppio prodotto vettoriale $a \times (b \times c) = b(c \cdot a) - c(a \cdot b)$.

2. Mostriamo che le due norme coincidono, applicando l'identità di Lagrange[6] al prodotto vettore $(v \times x) \times v$:

$$\|(v \times x) \times v\|^2 = \|v \times x\|^2 \|v\|^2 - ((v \times x) \cdot v)^2 = \|v \times x\|^2$$

perché, per ipotesi, $\|v\| = 1$ e inoltre il prodotto scalare tra $v \times x$ e v è nullo. Essendo poi numeri reali non negativi, si conclude togliendo i quadrati.

Ricordiamo poi che, dati due vettori w_1, w_2, il prodotto vettoriale $w_1 \times w_2$ è ortogonale sia a w_1 che a w_2. Quindi:

- $v \times x \perp v$,
- $(v \times x) \times v \perp v \times x$,
- $(v \times x) \times v \perp v$.

Inoltre $v \neq 0$ perché $\|v\| = 1$, $v \times x \neq 0$ perché $x \notin \langle v \rangle$ e infine $(v \times x) \times v \neq 0$ perchè $v \times x$ e v non sono paralleli. Dunque, se $x \notin \langle v \rangle$, i tre vettori sono non nulli e ortogonali a due a due.

Dobbiamo infine verificare che formano una base concorde con la base canonica.[7] Ma il loro prodotto misto è uguale a $((v \times x) \times v) \cdot ((v \times x) \times v) = \|(v \times x) \times v\|^2 = \|v \times x\|^2 > 0$ perché $x \notin \langle v \rangle$.

3. Fissiamo in $\mathbb{R}^3$ la base ortogonale $B = \{(v \times x) \times v, v \times x, v\}$.

   In base a quanto visto nei punti precedenti, possiamo dire che x e $\varrho(x)$ hanno la stessa componente lungo la semiretta generata da v e le proiezioni sul piano ortogonale, $\langle (v \times x) \times v, v \times x \rangle$, risultano ruotate di un angolo θ [8].

$\square$

[6] L'identità di Lagrange: $\|v \times w\|^2 = \|v\|^2 \|w\|^2 - (v \cdot w)^2$.

[7] Una base (ordinata) u, v, w di $\mathbb{R}^3$ si dice *concorde* con la base canonica se $u \cdot (v \times w) > 0$.

[8] Per il punto 1 del Lemma 2.6, il vettore x rappresentato nella base B è:

$$(x)_B = \begin{pmatrix} 1 \\ 0 \\ v \cdot x \end{pmatrix}.$$

Se ruotiamo attorno al terzo asse di un angolo θ in senso antiorario (con l'asse orientato col vettore v), la matrice della rotazione nella base B è :

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Proposizione 2.7. *Fissato un quaternione unitario $u = (\cos\theta, \sin\theta v)$, la funzione*

$$\varphi_u \colon \mathbb{I} \to \mathbb{I}, \quad x \mapsto ux\overline{u}.$$

corrisponde a ruotare i vettori di $\mathbb{I}$ attorno all'asse $\langle v\rangle$ orientato con v di un angolo 2θ (in senso antiorario).

Inoltre, la funzione

$$\varphi \colon \mathbb{H}^1 \to SO_3(\mathbb{R}), \quad u \mapsto \varphi_u$$

risulta essere un omomorfismo suriettivo di gruppi per le strutture moltiplicative e, fissati due quaternioni unitari u, u', questi inducono la stessa rotazione su $\mathbb{I}$ se, e solo se, $u = \pm u'$.

Dimostrazione. Fissiamo $u = (\cos\theta, \sin\theta v) \in \mathbb{H}^1$.

Osserviamo che $ux\overline{u} \in \mathbb{I}$, qualunque sia $x \in \mathbb{I}$, infatti dalla Definizione 2.1, si ha:

$$\begin{aligned} ux\overline{u} &= (\cos\theta, \sin\theta v)(0, x)(\cos\theta, -\sin\theta v) = \\ &= (-\sin\theta v\cdot x, \cos\theta x + \sin\theta v \times x)(\cos\theta, -\sin\theta v) = \\ &= (-\sin\theta\cos\theta v\cdot x + \sin\theta\cos\theta v\cdot x + (\sin\theta)^2(v\times x)\cdot v, \dots). \end{aligned}$$

Quindi, essendo nulla la componente scalare del prodotto, $ux\overline{u}$ risulta essere puramente immaginario, ovvero $ux\overline{u} \in \mathbb{I}$.

Terminando il calcolo precedente si ottiene che la componente vettoriale del prodotto $ux\overline{u}$ risulta essere:

$$(\sin\theta)^2(v\cdot x)v + (\cos\theta)^2 x + 2\sin\theta\cos\theta(v\times x) - (\sin\theta)^2(v\times x)\times v.$$

Per il punto 1 del Lemma 2.6, possiamo scrivere:

$$(\cos\theta)^2 x = (\cos\theta)^2[(v\times x)\times v + (v\cdot x)v],$$

quindi otteniamo:

$(\sin\theta)^2(v\cdot x)v + (\cos\theta)^2[(v\times x)\times v + (v\cdot x)v] + 2\sin\theta\cos\theta(v\times x) - (\sin\theta)^2(v\times x)\times v = (\sin\theta)^2(v\cdot x)v + (\cos\theta)^2(v\times x)\times v + (\cos\theta)^2(v\cdot x)v + 2\sin\theta\cos\theta(v\times x) - (\sin\theta)^2(v\times x)\times v = \cos(2\theta)(v\times x)\times v + \sin(2\theta)(v\times x) +$

Dunque il vettore che si ottiene è:

$$\varrho_v(x) = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ v\cdot x \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \\ v\cdot x \end{pmatrix}.$$

$(v \cdot x)v$,[9] che risulta essere, per il punto 3 del Lemma 2.6, il vettore che si ottiene ruotando x attorno all'asse $\langle v \rangle$ di un angolo 2θ, in senso antiorario attorno a v.

Consideriamo ora la funzione $\varphi\colon \mathbb{H}^1 \to SO_3(\mathbb{R})$, definita da $\varphi(u) = \varphi_u$.

Si verifica facilmente (dalle proprietà del coniugato della Proposizione 1.3) che è un omomorfismo di gruppi [10], infatti:

$\varphi(uu')(x) = \varphi_{uu'}(x) = uu'x\overline{uu'} = uu'x\overline{u'}\,\overline{u} = \varphi_u(u'x\overline{u'}) = \varphi_u(\varphi_{u'}(x)) = \varphi(u)\varphi(u')(x)$.[11]

Chiaramente l'omomorfismo è suriettivo, poiché ogni elemento di $SO_3(\mathbb{R})$ è una rotazione attorno ad un fissato asse, e quindi si rappresenta tramite un quaternione.

Infine, consideriamo $u = (\cos\theta, \sin\theta v), u' = (\cos\theta', \sin\theta' v')$. Ricordando che $\theta \in [0, \pi)$, si ha che u ed u' inducono la stessa rotazione se, e solo se:

- $v = v'$ e $2\theta = 2\theta' + 2k\pi, k \in \mathbb{Z} \iff v = v'$ e $\theta = \theta' + k\pi \iff v = v'$ e $\theta = \theta'$ (essendo $\theta \in [0, \pi)$), cioè $u = u'$, oppure

- $v = -v'$ e $2\theta = 2k\pi - 2\theta', k \in \mathbb{Z} \iff v = -v'$ e $\theta = k\pi - \theta' \iff v = -v'$ e $\theta = \pi - \theta'$ (essendo $\theta \in [0, \pi)$), cioè $u = -u'$.

$\square$

2.3 Relazione tra $SU_2(\mathbb{C})$ e $SO_3(\mathbb{R})$

La Proposizione 2.7 generalizza l'osservazione che il gruppo $SO_2(\mathbb{R})$ delle rotazioni (attorno all'origine) del piano coincide con il gruppo $U_1(\mathbb{C})$ [12] delle trasformazioni unitarie di $\mathbb{C}$, ovvero con il gruppo formato dai numeri complessi di modulo 1.

Nel caso che più ci interessa,

Proposizione 2.8. *Il gruppo $SO_3(\mathbb{R})$ delle rotazioni nello spazio è immagine omomorfa del gruppo $SU_2(\mathbb{C})$ delle trasformazioni unitarie speciali di $\mathbb{C}^2$, ovvero del gruppo dei quaternioni di modulo 1.*

[9] In questi ultimi passaggi sono state usate le identità trigonometriche: $(\sin\theta)^2 + (\cos\theta)^2 = 1, (\cos\theta)^2 - (\sin\theta)^2 = \cos(2\theta), 2\sin\theta\cos\theta = \sin(2\theta)$.

[10] Il prodotto uu' è quello tra quaternioni della Definizione 2.1, mentre quello tra $\varphi(u)$ e $\varphi(u')$ è quello usuale tra matrici.

[11] La formula $\varphi(uu') = \varphi(u)\varphi(u')$ dà un modo quasi immediato per capire che la composizione di due rotazioni nello spazio è ancora una rotazione.

[12] Il gruppo unitario è il gruppo delle matrici unitarie $U_n(\mathbb{C}) = \{P \in GL_n(\mathbb{C}) | {}^t\overline{P}P = 1_n\}$. Il sottogruppo delle matrici unitarie *speciali*, cioè quelle di determinante 1, viene indicato con $SU_n(\mathbb{C})$.

Dimostrazione. Per quanto visto nella Definizione 1.8 e nella Proposizione 1.9, l'applicazione α ristretta ad $\mathbb{H}^1$ induce un isomorfismo:

$$\begin{array}{rccc} \alpha_{\mathbb{H}^1}: & \mathbb{H}^1 & \longrightarrow & SU_2(\mathbb{C}) \\ & z = z_1 + z_2 j & \longmapsto & \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix}. \end{array}$$

Essendo $1 = \|z\|^2_{\mathbb{H}} = \|z_1\|^2 + \|z_2\|^2 = det(\alpha(z))$, abbiamo che

$$\alpha(\mathbb{H}^1) = SU_2(\mathbb{C}).$$

Consideriamo un elemento di $SU_2(\mathbb{C})$ [13]:

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = x_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_1 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = x_0 \mathbf{1} + x_1 I + x_2 J + x_3 K,$$

con $\alpha = x_0 + ix_1, \beta = x_2 + ix_3 \in \mathbb{C}$.

Quindi, considerando il prodotto tra matrici, si ha che lo spazio vettoriale reale di dimensione quattro generato da $\mathbf{1}, I, J, K$ in $GL_2(\mathbb{C})$ è un corpo isomorfo a quello dei quaternioni. Infatti si ha che $I^2 = J^2 = K^2 = -\mathbf{1}$, $\quad IJ = K = -JI$, $\quad JK = I = -KJ$, $\quad KI = J = -IK$; il quadrato della norma dei quaternioni corrisponde al determinante delle matrici, quindi *i quaternioni unitari corrispondono alle matrici unitarie speciali.* Di conseguenza, possiamo dire che $SU_2(\mathbb{C})$ sta a $\mathbb{H}^1$ (sfera tridimensionale in $\mathbb{R}^4$), come $SO_2(\mathbb{R})$ sta a $\mathbb{S}^1$ (sfera unidimensionale in $\mathbb{R}^2$). Dunque esiste un omomorfismo *suriettivo* canonico: $SU_2(\mathbb{C}) \rightarrow SO_3(\mathbb{R})$, che manda $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$ nella matrice corrispondente al quaternione unitario (x_0, x_1, x_2, x_3). $\square$

È uso comune dire che i due elementi di $SU_2(\mathbb{C})$ che danno luogo ad una stessa rotazione (e che sono uno l'opposto dell'altro) differiscono per lo *spin*. Per questo motivo $SU_2(\mathbb{C})$ viene anche detto *gruppo degli spin*.

2.4 Slerp

È abbastanza naturale utilizzare i quaternioni unitari per descrivere le singole rotazioni, anche perché, a differenza delle corrispondenti matrici in

[13] Si dimostra che le matrici in $SU_2(\mathbb{C})$ sono tutte e sole le matrici complesse della forma $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$, con $|\alpha|^2 + |\beta|^2 = 1$ (lo si vede esplicitando la condizione ${}^t\overline{A}A = 1_2$ e $detA = 1$).

$SO_3(\mathbb{R})$, è facile scrivere un quaternione unitario che la produca conoscendo l'asse e l'angolo di rotazione. In più, per passare da una rotazione ad un'altra, ci si sposta tra due punti della sfera unitaria di $\mathbb{H}$.

La tecnica che ora spiegheremo è detta *slerp*[14] ed è utilizzata nell'animazione computerizzata.

Consideriamo p, q due quaternioni unitari con $p \neq \pm q$, quindi linearmente indipendenti come vettori in $\mathbb{R}^4$ [15].

Per la disuguaglianza di Schwarz in $\mathbb{R}^4$, si ha che $0 \leq \frac{|p \cdot q|}{\|p\|\|q\|} \leq 1$. Dunque, essendo $\|p\| = \|q\| = 1$, possiamo scrivere

$$p \cdot q = \cos\theta, \quad con \quad \theta \in (0, \pi)^{16}.$$

Osserviamo ora che $\|q - (p \cdot q)p\| \neq 0$, infatti: se per assurdo fosse $\|q - (p \cdot q)p\| = 0$, allora $q - (p \cdot q)p = 0$ ma quindi $q = (p \cdot q)p$, il che è impossibile perché riuscirei a scrivere $q = \alpha p$ con $\alpha = p \cdot q \in \mathbb{R}$ contro l'ipotesi.

Possiamo quindi considerare il quaternione unitario $n = \frac{q-(p \cdot q)p}{\|q-(p \cdot q)p\|}$.

Vediamo che p ed n sono ortogonali, infatti:

$$\begin{aligned} p \cdot n &= p \cdot \frac{q-(p \cdot q)p}{\|q-(p \cdot q)p\|} = \\ &= p \cdot \left(\frac{q}{\|q-(p \cdot q)p\|} - \frac{(p \cdot q)p}{\|q-(p \cdot q)p\|}\right) = \\ &= \frac{p \cdot q}{\|q-(p \cdot q)p\|} - \frac{(p \cdot p)(p \cdot q)}{\|q-(p \cdot q)p\|} = 0. \end{aligned}$$

Quindi risulta $\langle p, q\rangle = \langle p, n\rangle$ e $q = (\cos\theta)p + (\sin\theta)n$. Perciò l'arco di cerchio massimo che congiunge p e q nella sfera unitaria è formato dai quaternioni:

$$p(t) = (\cos t)p + (\sin t)n, \quad per \quad t \in [0, \theta].$$

Osserviamo poi che $\|q-(p \cdot q)p\|^2 = 1+(p \cdot q)^2-2(p \cdot q)^2 = 1-(\cos\theta)^2 = (\sin\theta)^2$ ($\neq 0$ perché $\theta \neq 0, \pi$) e dunque la forma che viene utilizzata per la slerp è:

$$\begin{aligned} p(t) &= \frac{(\sin\theta)(\cos t)p}{\sin\theta} + \sin t \frac{[q-(\cos\theta)p]}{\sin\theta} = \\ &= \frac{\sin t}{\sin\theta} q - \frac{\sin t \cos\theta}{\sin\theta} p + \frac{\cos t \sin\theta}{\sin\theta} p = \\ &= \frac{\sin t}{\sin\theta} q + \frac{\sin\theta\cos t - \sin t \cos\theta}{\sin\theta} p = \\ &= \frac{\sin t}{\sin\theta} q + \frac{\sin(\theta - t)}{\sin\theta} p, \quad per \quad t \in [0, \theta]. \end{aligned}$$

[14]spherical linear interpolation. È stata introdotta da Ken Shoemake con lo scopo di animare la rotazione $3D$. Si riferisce al movimento a velocità costante lungo un arco di cerchio, date le estremità e un parametro di interpolazione tra 0 e 1.

[15]Infatti, se per assurdo p e q fossero lineramente dipendenti come vettori in $\mathbb{R}^4$, allora esisterebbe $\alpha \in \mathbb{R}$ tale che $p = \alpha q$. Ma p e q sono presi unitari per ipotesi, dunque $1 = \|p\| = \|\alpha q\| = |\alpha|\|q\|$. Dunque deve risultare $|\alpha| = 1$, ovvero $\alpha = \pm 1$. Ma quindi si avrebbe $p = \pm q$, assurdo.

[16]θ è angolo non orientato tra p, q.

Capitolo 3

Ottonioni

In questo capitolo definiremo l'insieme degli ottonioni $\mathbb{O}$. Doteremo $\mathbb{O}$ di una somma e di un prodotto e vedremo che con queste operazioni risulta essere un'algebra [1] di dimensione 8 sui reali, non associativa.

3.1 Storia

Hamilton decise, nell'ottobre del 1843, di inviare una lettera ad uno suo caro amico, John T. Graves (1806-1870), da cui ebbe ispirazione per la scoperta dei quaternioni.

Poco dopo, il 26 dicembre 1843, Graves descrisse gli *ottonioni* (o *ottetti*), che lui chiamò *ottave*, un nome che a volte viene ancora oggi utilizzato. Ma Graves non pubblicò questo suo lavoro fino al 1845, poco dopo e in risposta alla pubblicazione di Arthur Cayley (1821-1895) della propria scoperta degli ottonioni. Per questo motivo gli ottetti sono anche meglio conosciuti come *numeri di Cayley.* Ad entrambi viene riconosciuta questa scoperta, appunto perché ciascuno dei due l'ha fatta in modo indipendente dall'altro.

3.2 Forma vettoriale

Verrebbe naturale proseguire la catena

$$\mathbb{R} \subset \mathbb{C} \subset \mathbb{H},$$

[1] Si dice che $\mathbb{O}$ è una $\mathbb{R}$-algebra o un'algebra sul campo dei numeri reali se $\mathbb{O}$ è uno spazio vettoriale su $\mathbb{R}$ munito di un'operazione binaria $\cdot \colon \mathbb{O} \times \mathbb{O} \to \mathbb{O}$ che sia bilineare.

introducendo l'insieme formato dalle matrici della forma:

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}, \quad \text{con} \quad z, w \in \mathbb{H}.$$

Dobbiamo però fare attenzione perché l'insieme sopra definito non è chiuso rispetto al prodotto usuale tra matrici, infatti: se $z, w, h, k \in \mathbb{H}$ e

$$A = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}, \quad B = \begin{pmatrix} h & k \\ -\overline{k} & \overline{h} \end{pmatrix}, \quad \text{allora} \quad AB = \begin{pmatrix} zh - w\overline{k} & zk + w\overline{h} \\ -\overline{w}h - \overline{z}\overline{k} & -\overline{w}k + \overline{z}\overline{h} \end{pmatrix},$$

che non risulta più essere della forma di partenza perché, ad esempio, $\overline{zh - w\overline{k}} = \overline{h}\overline{z} - k\overline{w} \neq \overline{z}\overline{h} - \overline{w}k$, perché il prodotto in $\mathbb{H}$ abbiamo visto essere non commutativo.

Procediamo quindi con una definizione vettoriale, come avevamo fatto anche per i quaternioni.

Definizione 3.1. *Sia $\mathbb{O}$ l'insieme di tutti gli elementi del tipo*

$$x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8{}^2,$$

con $x_m \in \mathbb{R}$ $\quad \forall m = 1, \ldots, 8 \quad$ e $\quad i, j, k, l, kl, jl, il \quad$ simboli.

Definiamo su questo insieme le operazioni di somma e prodotto nel seguente modo:

- *somma: $(x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8) + (y_1 + iy_2 + jy_3 + ky_4 + kly_5 + jly_6 + ily_7 + ly_8) = (x_1 + y_1) + i(x_2 + y_2) + j(x_3 + y_3) + k(x_4 + y_4) + kl(x_5 + y_5) + jl(x_6 + y_6) + il(x_7 + y_7) + l(x_8 + y_8)$.*

- *prodotto: pretendendo che il prodotto tra numeri reali sia quello di $\mathbb{R}$, basta definire i prodotti tra i simboli i, j, k, l, kl, jl, il.*

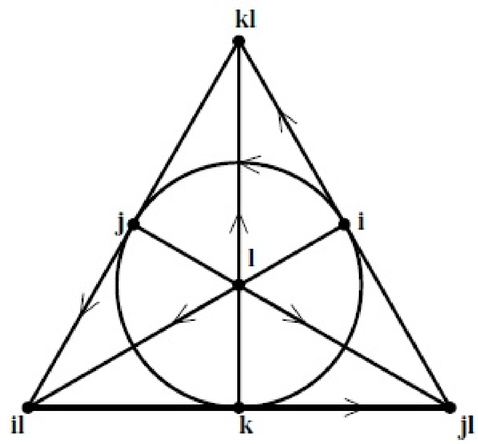
  Lo facciamo nel seguente modo:

  $i^2 = j^2 = k^2 = l^2 = (kl)^2 = (jl)^2 = (il)^2 = -1$;

  La tabella completa di moltiplicazione è illustrata qui sotto [3]:

[2] Indichiamo i volte l con il e così anche per j, k.

[3] Il diagramma che rappresenta la tabella di moltiplicazione degli ottetti unitari prende il nome di *piano di Fano*. Esso è composto da sette punti e sette linee (il cerchio tra i, j, k è considerato una linea). Le linee si devono considerare orientate e i sette punti corrispondono alle sette unità immaginarie. Presi arbitrariamente due punti distinti, questi giacciono su un' unica linea e ogni linea passa esattamente per tre punti.



(ovvero i quadrati risultano tutti essere -1; se (a, b, c) è una tripla ordinata di punti giacenti su una data linea con ordine specificato dalla direzione della freccia, la moltiplicazione è data da $ab = c$ e $ba = -c$, soggetta a permutazione ciclica).

Per esempio, $(k)(l) = kl$, $(l)(kl) = k$, $(kl)(k) = l$.

Ognuno di quei prodotti è anticommutativo, ovvero invertendo l'ordine del prodotto (rispetto alla freccia) contribuisce un segno meno.

Gli elementi di $\mathbb{O}$ sono detti *ottonioni*. In particolare, preso $r \in \mathbb{R}$ e $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8 \in \mathbb{O}$, il loro prodotto è definito come:

$$rx = rx_1 + irx_2 + jrx_3 + krx_4 + klrx_5 + jlrx_6 + ilrx_7 + lrx_8.$$

Le operazioni di somma e prodotto per scalari reali dotano l'insieme $\mathbb{O}$ di una struttura di *spazio vettoriale reale* di dimensione otto ed una sua base è $1, i, j, k, l, kl, jl, il$.

Dato un ottonione $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8$,

$x_1 = \Re x$ si dirà *parte reale* di x, mentre $ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8 = \Im x$ si dirà *parte immaginaria* di x. Perciò $x = \Re x + \Im x$. Algebricamente possiamo quindi definire $\Re x = \frac{x+\overline{x}}{2}, \Im x = \frac{x-\overline{x}}{2}$. [4]

[4] Si vada a vedere nelle pagine seguenti come è definito il coniugato di un ottonione.
È importante notare che la parte immaginaria è proprio immaginaria.
Questo differisce, come avevamo anche visto per i quaternioni, dalla notazione usata per i numeri complessi, dove $\Im z$ si riferiva normalmente ad un numero reale, ovvero il coefficiente di i. Questa convenzione non è possibile qui, dal momento che la parte immaginaria ha sette gradi di libertà e può essere pensata come un vettore in $\mathbb{R}^7$.

Un ottonione $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8$ può essere rappresentato da una 8-upla di numeri reali $(x_1, \dots, x_8)$, e quindi è possibile vederlo come un punto o un vettore in $\mathbb{R}^8$.

Vediamo che possiamo inoltre scrivere x nella forma: $x = (x_1 + ix_2 + jx_3 + kx_4) + (x_8 + ix_7 + jx_6 + kx_5)l$. Perciò un ottonione può essere visto anche come una coppia di quaternioni $(z_{1_{\mathbb{H}}}, z_{2_{\mathbb{H}}}) = (x_1 + ix_2 + jx_3 + kx_4, x_8 + ix_7 + jx_6 + kx_5)$, o equivalentemente possiamo scrivere $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}l$.

Gli ottonioni contengono in modo naturale:

- i numeri reali $(r = (r, 0, 0, 0, 0, 0, 0, 0), r \in \mathbb{R})$,
- i numeri complessi $(a + ib = (a, b, 0, 0, 0, 0, 0, 0), a, b \in \mathbb{R})$,
- i quaternioni $(a + ib + jc + kd = (a, b, c, d, 0, 0, 0, 0), a, b, c, d \in \mathbb{R})$.

Anche per gli ottonioni, in analogia con i complessi e i quaternioni, si definiscono i concetti di *coniugato* e di *norma*. Inoltre ogni ottonione diverso da zero possiede un *inverso* rispetto al prodotto. Si differenziano però dai quaternioni per il fatto che il loro prodotto non è associativo (oltre a non essere commutativo).

Definizione 3.2 (Coniugato)**.** *Dato un elemento $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8$ di $\mathbb{O}$, il suo coniugato è l'ottonione $\overline{x} = x_1 - ix_2 - jx_3 - kx_4 - klx_5 - jlx_6 - ilx_7 - lx_8$.*

Un ottonione x si dice:

- *puramente reale se $x_m = 0 \quad \forall m = 2, \dots, 8$, quindi $x = \Re x$,*
- *puramente immaginario se $x_1 = 0$, quindi $x = \Im x$.*

Proposizione 3.3. *Il coniugato, come funzione $\bar{\cdot} : \mathbb{O} \to \mathbb{O}$, soddisfa le seguenti proprietà:*

1. *rispetta la somma: $\overline{x + y} = \overline{x} + \overline{y}$,*
2. *$\overline{x} = x$ se e solo se x è puramente reale,*

   $\overline{x} = -x$ se e solo se x è puramente immaginario,
3. *(anti) rispetta il prodotto: $\overline{xy} = \overline{y}\ \overline{x}$,*
4. *$x\overline{x} = \overline{x}x = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2$ è puramente reale per ogni $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8 \in \mathbb{O}$, ed è un numero positivo se $x \neq 0$,*

5. $\overline{\overline{x}} = x$ *per ogni* $x \in \mathbb{O}$.

Dimostrazione. Siano $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8$ e $y = y_1 + iy_2 + jy_3 + ky_4 + kly_5 + jly_6 + ily_7 + ly_8$ due elementi di $\mathbb{O}$.

1. Per la Definizione 3.1, $x + y = (x_1 + y_1) + i(x_2 + y_2) + j(x_3 + y_3) + k(x_4 + y_4) + kl(x_5 + y_5) + jl(x_6 + y_6) + il(x_7 + y_7) + l(x_8 + y_8)$.

   $\overline{x+y} = (x_1 + y_1) - i(x_2 + y_2) - j(x_3 + y_3) - k(x_4 + y_4) - kl(x_5 + y_5) - jl(x_6 + y_6) - il(x_7 + y_7) - l(x_8 + y_8) = (x_1 - ix_2 - jx_3 - kx_4 - klx_5 - jlx_6 - ilx_7 - lx_8) + (y_1 - iy_2 - jy_3 - ky_4 - kly_5 - jly_6 - ily_7 - ly_8) = \overline{x} + \overline{y}$.

2. $\overline{x} = x$ se e solo se $x_1 = x_1$ e $x_m = -x_m \quad \forall m = 2, \ldots, 8$ (ma x_m $\forall m = 2, \ldots, 8$ sono tutti numeri reali perciò questo accade) se e solo se $x_1 \in \mathbb{R}$ e $x_m = 0 \quad \forall m = 2, \ldots, 8$ se e solo se, dalla Definizione 3.2, x è puramente reale.

   $\overline{x} = -x$ se e solo se $x_1 = -x_1$ e $x_m = x_m$ $\forall m = 2, \ldots, 8$ se e solo se $x_1 = 0$ e $x_m \in \mathbb{R} \quad \forall m = 2, \ldots, 8$ se e solo se, dalla Definizione 3.2, x è puramente immaginario.

3. Possiamo dimostrarlo senza sviluppare tutti i conti (molto lunghi), ma osservando che, come già visto all'inizio di questo capitolo, gli ottonioni possono essere visti come coppie di quaternioni [5], ovvero che un ottonione x si può scrivere anche come:

   $$x = (z, w), \quad \textit{con} \quad z, w \in \mathbb{H}.$$

   Sull'insieme $\mathbb{O} \simeq \mathbb{H} \times \mathbb{H}$ formato dalle coppie descritte sopra, definiamo le operazioni di somma e prodotto nel seguente modo:

   - somma: $(z, w) + (h, k) = (z + h, w + k)$,
   - prodotto: $(z, w)(h, k) = (zh - \overline{k}w, kz + w\overline{h})$.

   $\mathbb{O}$ risulta essere un'algebra non associativa con dimensione otto sul campo dei numeri reali. Inoltre $\mathbb{O}$ contiene la sottoalgebra $\mathbb{H}$ formata dagli elementi della forma $(z, 0)$.[6]

[5] $\mathbb{O} \simeq \mathbb{H}^2 \simeq \mathbb{R}^8$. Si vede che $\mathbb{O}$ è un $\mathbb{R}$-spazio vettoriale. Inoltre, preso $r \in \mathbb{R}$, si ha che :

$$r(z, w) = (r, 0)(z, w) = (rz, rw) = (z, w)(r, 0),$$

ricordando che $rz = zr$ e $\overline{r} = r$.

[6] Abbiamo che $\mathbb{R} \to \mathbb{C} \to \mathbb{H} \to \mathbb{O}, r \mapsto (r, 0) \mapsto (r, 0, 0, 0) \mapsto (r, 0, 0, 0, 0, 0, 0, 0)$.

A questo punto, il coniugato di $x = (z, w) \in \mathbb{O}$ è l'ottonione

$$\overline{x} = \overline{(z, w)} = (\overline{z}, -w),$$

e la sua norma è il numero reale non negativo

$$\|(z, w)\| = \sqrt{\|z\|_{\mathbb{H}}^2 + \|w\|_{\mathbb{H}}^2}.$$

In particolare si ha:

$$\|(z, w)\| = \sqrt{(z, w)\overline{(z, w)}} \in \mathbb{R}_{\geq 0}.$$

Dunque, per dimostrare che il coniugato (anti) rispetta il prodotto, basta far vedere che $\overline{(z, w)(h, k)} = \overline{(h, k)}\ \overline{(z, w)}$.

Per la definizione di prodotto tra coppie di quaternioni data sopra, abbiamo che $(z, w)(h, k) = (zh - \overline{k}w, kz + w\overline{h})$.

$$\begin{aligned}
\overline{(z, w)(h, k)} &= (\overline{zh - \overline{k}w}, -(kz + w\overline{h})) = \\
&= (\overline{h}\overline{z} - \overline{w}k, -kz - w\overline{h}) = \\
&= (\overline{h}, -k)(\overline{z}, -w) = \overline{(h, k)}\ \overline{(z, w)}.
\end{aligned}$$

4. Possiamo dimostrarlo ragionando con la costruzione appena descritta. Vediamo dunque che $(z, w)\overline{(z, w)} = \overline{(z, w)}(z, w) = \|z\|_{\mathbb{H}}^2 + \|w\|_{\mathbb{H}}^2$.

$$\begin{aligned}
(z, w)\overline{(z, w)} &= (z, w)(\overline{z}, -w) \\
&= (z\overline{z} + \overline{w}w, -wz + wz) = \\
&= (\|z\|_{\mathbb{H}}^2 + \|w\|_{\mathbb{H}}^2, 0) = \\
&= (\overline{z}z + \overline{w}w, w\overline{z} - w\overline{z}) = \\
&= (\overline{z}, -w)(z, w) = \overline{(z, w)}\ (z, w).
\end{aligned}$$

Per quanto visto riguardo i quaternioni, quel numero (essendo somma di due norme in $\mathbb{H}$) è un numero puramente reale ed è nullo se e solo se sia z che w sono nulli, cioè se e solo se $x = (0, 0)$ è l'ottonione nullo.

5. Dal momento che $\overline{x} = x_1 - ix_2 - jx_3 - kx_4 - klx_5 - jlx_6 - ilx_7 - lx_8 = x_1 + i(-x_2) + j(-x_3) + k(-x_4) + kl(-x_5) + jl(-x_6) + il(-x_7) + l(-x_8)$, allora $\overline{\overline{x}} = x_1 - i(-x_2) - j(-x_3) - k(-x_4) - kl(-x_5) - jl(-x_6) - il(-x_7) - l(-x_8) = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8 = x$.

□

Definizione 3.4 (Norma)**.** *Dato un elemento* $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8$ *di* $\mathbb{O}$*, la sua norma è il numero reale non negativo* $\|x\| = \sqrt{x\overline{x}}$*. Dunque, per la Proposizione 3.3, in particolare si ha:*

$$\|x\| = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2} \in \mathbb{R}_{\geq 0}.$$

Proposizione 3.5. *La norma, come funzione* $\|\cdot\| : \mathbb{O} \to \mathbb{R}_{\geq 0}$*, soddisfa le seguenti proprietà:*

1. $\|x\|^2 = x\overline{x} = \overline{x}x = \|\overline{x}\|^2$ *per ogni* $x \in \mathbb{O}$*,*
2. *positività:* $\|x\| \geq 0$ *per ogni* $x \in \mathbb{O}$ *e* $\|x\| = 0 \iff x = 0$*,*
3. *moltiplicatività:* $\|xy\| = \|x\|\|y\|$*,*
4. *sub-additività:* $\|x + y\| \leq \|x\| + \|y\|$*.*

Dimostrazione. Siano $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8$ e $y = y_1 + iy_2 + jy_3 + ky_4 + kly_5 + jly_6 + ily_7 + ly_8$ due elementi di $\mathbb{O}$.

1. Segue immediatamente dalla Proposizione 3.3.
2. $\|x\| = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2} \geq 0$ per ogni $x \in \mathbb{O}$ (in quanto radice reale di una somma di quadrati reali) e $\|x\| = 0 \iff \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2} = 0 \iff x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2 = 0 \iff x_m = 0 \quad \forall m = 1, \ldots, 8 \iff x = 0$.
3. Considerando ancora $\mathbb{O} \simeq \mathbb{H} \times \mathbb{H}$, dimostriamo che $\|(z,w)(h,k)\| = \|(z,w)\|\|(h,k)\|$.

   Abbiamo che: $\|(z,w)\|^2\|(h,k)\|^2 = (\|z\|_{\mathbb{H}}^2 + \|w\|_{\mathbb{H}}^2)(\|h\|_{\mathbb{H}}^2 + \|k\|_{\mathbb{H}}^2)$.

   Poi, $\|(z,w)(h,k)\|^2 = (z,w)(h,k)\overline{(z,w)(h,k)} = (zh - \overline{k}w, kz + w\overline{h})(\overline{h}\overline{z} - \overline{w}k, -kz - w\overline{h})$.

   Ora, la seconda componente di quel prodotto è: $(-kz - w\overline{h})(zh - \overline{k}w) + (kz + w\overline{h})(zh - \overline{k}w) = 0$,

   mentre la prima componente risulta:

   $$\begin{aligned}
   &(zh - \overline{k}w)(\overline{h}\overline{z} - \overline{w}k) - (-\overline{z}\overline{k} - h\overline{w})(kz + w\overline{h}) = \\
   &zh\overline{h}\overline{z} - zh\overline{w}k - \overline{k}w\overline{h}\overline{z} + \overline{k}w\overline{w}k + \overline{z}\overline{k}kz + \overline{z}\overline{k}w\overline{h} + h\overline{w}kz + h\overline{w}w\overline{h} = \\
   &\|h\|_{\mathbb{H}}^2\|z\|_{\mathbb{H}}^2 + \|k\|_{\mathbb{H}}^2\|w\|_{\mathbb{H}}^2 + \|z\|_{\mathbb{H}}^2\|k\|_{\mathbb{H}}^2 + \|h\|_{\mathbb{H}}^2\|w\|_{\mathbb{H}}^2 - \\
   &- zh\overline{w}k - \overline{k}w\overline{h}\overline{z} + \overline{z}\overline{k}w\overline{h} + h\overline{w}kz = \\
   &(\|z\|_{\mathbb{H}}^2 + \|w\|_{\mathbb{H}}^2)(\|h\|_{\mathbb{H}}^2 + \|k\|_{\mathbb{H}}^2) - zh\overline{w}k - \overline{k}w\overline{h}\overline{z} + \overline{z}\overline{k}w\overline{h} + h\overline{w}kz.
   \end{aligned}$$

Poi osserviamo che $\overline{z}\overline{k}w\overline{h} = \overline{h\overline{w}kz}$ e $\overline{k}w\overline{h}\overline{z} = \overline{zh\overline{w}k}$. Dunque,

$$\begin{aligned} -zh\overline{w}k - \overline{k}w\overline{h}\overline{z} + \overline{z}\overline{k}w\overline{h} + h\overline{w}kz &= -zh\overline{w}k - \overline{zh\overline{w}k} + h\overline{w}kz + \overline{h\overline{w}kz} = \\ &= -2\Re(zh\overline{w}k) + 2\Re(h\overline{w}kz), \end{aligned}$$

quindi risulta essere un quaternione puramente reale. Ricordiamo poi che, dalla Definizione 2.1, la parte reale del prodotto di due quaternioni $(r, v)(s, w)$ è $rs - v \cdot w$ e ciò non dipende dall'ordine dei termini (in quanto il prodotto tra numeri reali e il prodotto scalare sono commutativi). Quindi si ha che $\Re(zh\overline{w}k) = \Re(z(h\overline{w}k)) = \Re((h\overline{w}k)z) = \Re(h\overline{w}kz)$. Perciò si ha che $-2\Re(zh\overline{w}k) + 2\Re(h\overline{w}kz) = 0$.

Quindi si ha che $\|(z, w)(h, k)\|^2 = \|(z, w)\|^2\|(h, k)\|^2$ e, togliendo i quadrati (lo possiamo fare perché sono numeri reali non negativi) si ottiene quanto si voleva dimostrare.

4. Se vediamo un ottonione come coppia di quaternioni, abbiamo facilmente che:

$$\begin{aligned} \|(z_1, w_1) + (z_2, w_2)\|^2 &= \|(z_1 + z_2, w_1 + w_2)\|^2 = \\ &= \|z_1 + z_2\|^2_{\mathbb{H}} + \|w_1 + w_2\|^2_{\mathbb{H}} \leq \\ &\leq \|z_1\|^2_{\mathbb{H}} + \|z_2\|^2_{\mathbb{H}} + \|w_1\|^2_{\mathbb{H}} + \|w_2\|^2_{\mathbb{H}} = \\ &= \|(z_1, w_1)\|^2 + \|(z_2, w_2)\|^2. \end{aligned}$$

Essendo la norma un numero reale non negativo, la conclusione si ottiene togliendo i quadrati.

Oppure, un'altra dimostrazione è la seguente:

essendo $\mathbb{O}$ uno spazio vettoriale su $\mathbb{R}$, sappiamo che esiste un isomorfismo $\varphi\colon \mathbb{R}^8 \to \mathbb{O}$ di $\mathbb{R}$-spazi vettoriali, che manda un vettore $v = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} \in \mathbb{R}^8$, nell'elemento $\varphi(v) = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8 \in \mathbb{O}$.

Abbiamo poi che

$$\|v\|_{\mathbb{R}^8} = \| \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} \|_{\mathbb{R}^8} =$$
$$\sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2} =$$
$$\|x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6 + ilx_7 + lx_8\|_{\mathbb{O}} = \|\varphi(v)\|_{\mathbb{O}},$$

quindi φ rispetta le norme (perché la norma in $\mathbb{R}^8$ è definita come $\|x\| = \sqrt{x \cdot x}$).

Inoltre, in $\mathbb{R}^8$ vale la disuguaglianza di Cauchy-Schwarz, quindi vale anche:

$\|v + w\|_{\mathbb{R}^8} \leq \|v\|_{\mathbb{R}^8} + \|w\|_{\mathbb{R}^8}$ per $v, w \in \mathbb{R}^8$,

e quindi vale che $\|\varphi(v + w)\|_{\mathbb{O}} \leq \|\varphi(v)\|_{\mathbb{O}} + \|\varphi(w)\|_{\mathbb{O}}$, ma $\varphi(v + w) = \varphi(v) + \varphi(w)$, e dunque si ottiene:

$\|\varphi(v) + \varphi(w)\|_{\mathbb{O}} \leq \|\varphi(v)\|_{\mathbb{O}} + \|\varphi(w)\|_{\mathbb{O}}$. Chiamando infine $\varphi(v) = x, \varphi(w) = y$, si ottiene proprio che $\|x + y\|_{\mathbb{O}} \leq \|x\|_{\mathbb{O}} + \|y\|_{\mathbb{O}}$.

$\square$

Proposizione 3.6 (Identità degli otto quadrati)**.** *Il prodotto di due somme di otto quadrati è ancora una somma di otto quadrati:*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) =$$
$$(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 +$$
$$(x_1x_2 + x_2y_1 + x_3y_4 - x_4y_3 + x_5y_6 - x_6y_5 - x_7y_8 + x_8y_7)^2 +$$
$$(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 - x_5y_7 - x_6y_8 + x_7y_5 + x_8y_6)^2 +$$
$$(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 - x_5y_8 + x_6y_7 - x_7y_6 + x_8y_5)^2 +$$
$$(x_1y_5 - x_2y_6 + x_3y_7 + x_4y_8 + x_5y_1 + x_6y_2 - x_7y_3 - x_8y_4)^2 +$$
$$(x_1y_6 + x_2y_5 + x_3y_8 - x_4y_7 - x_5y_2 + x_6y_1 + x_7y_4 - x_8y_3)^2 +$$
$$(x_1y_7 + x_2y_8 - x_3y_5 + x_4y_6 + x_5y_3 - x_6y_4 + x_7y_1 - x_8y_2)^2 +$$
$$(x_1y_8 - x_2y_7 - x_3y_6 - x_4y_5 + x_5y_4 + x_6y_3 + x_7y_2 + x_8y_1)^2.$$

Dimostrazione. Segue dalla moltiplicatività della norma: $\|xy\| = \|x\|\|y\|$; quindi, sostituendo in $\|x\|^2\|y\|^2 = \|xy\|^2$ gli ottonioni $x = x_1 + ix_2 + jx_3 +$

$kx_4+klx_5+jlx_6+ilx_7+lx_8$ e $y = y_1+iy_2+jy_3+ky_4+kly_5+jly_6+ily_7+ly_8$, si ottiene l'identità voluta.[7] $\square$

Proposizione 3.7. *Dato un elemento* $x = x_1 + ix_2 + jx_3 + kx_4 + klx_5 + jlx_6+ilx_7+lx_8$ *non nullo di* $\mathbb{O}$, *il suo inverso è* $x^{-1} = \frac{\overline{x}}{\|x\|^2}$. *Inoltre l'inverso soddisfa le seguenti proprietà:*

- $\|x^{-1}\| = \frac{1}{\|x\|}$,
- $\overline{x^{-1}} = \overline{x}^{-1}$,
- $(xy)^{-1} = y^{-1}x^{-1}$.[8]

Dimostrazione. Dalla Proposizione 3.5, abbiamo che $x\overline{x} = \overline{x}x = \|x\|^2$. Se $x \neq 0$, allora anche $\|x\| \neq 0$ e quindi possiamo dividere per $\|x\|^2$. Si ottiene:

$$x\frac{\overline{x}}{\|x\|^2} = \frac{\overline{x}}{\|x\|^2}x = 1.$$

Le proprietà dell'inverso si deducono dalle Proposizioni 3.3 e 3.5. $\square$

Abbiamo detto che il prodotto di ottonioni non è associativo. Diamone ora un esempio:

Esempio 3.8. *Consideriamo il prodotto dei tre ottonioni* i, j, k*:*

$$(i \quad j)(l) = +(k)(l) = +kl, \quad \textit{mentre} \quad (i)(j \quad l) = (i)(jl) = -kl$$

Comunque, l'associatività vale per i prodotti che coinvolgono non più di due ottonioni indipendenti;

[7] Per verificarlo basta eseguire un pò di conti, si ha:
$xy = (x_1y_1-x_2y_2-x_3y_3-x_4y_4-x_5y_5-x_6y_6-x_7y_7-x_8y_8)+i(x_1x_2+x_2y_1+x_3y_4-x_4y_3+x_5y_6-x_6y_5-x_7y_8+x_8y_7)+j(x_1y_3-x_2y_4+x_3y_1+x_4y_2-x_5y_7-x_6y_8+x_7y_5+x_8y_6)+k(x_1y_4+x_2y_3-x_3y_2+x_4y_1-x_5y_8+x_6y_7-x_7y_6+x_8y_5)+kl(x_1y_5-x_2y_6+x_3y_7+x_4y_8+x_5y_1+x_6y_2-x_7y_3-x_8y_4)+jl(x_1y_6+x_2y_5+x_3y_8-x_4y_7-x_5y_2+x_6y_1+x_7y_4-x_8y_3)+il(x_1y_7+x_2y_8-x_3y_5+x_4y_6+x_5y_3-x_6y_4+x_7y_1-x_8y_2)+l(x_1y_8-x_2y_7-x_3y_6-x_4y_5+x_5y_4+x_6y_3+x_7y_2+x_8y_1)$.

[8] È sempre vero in un'algebra associativa, infatti:

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = 1.$$

Ma qui siamo in un'algebra non associativa, per cui dobbiamo dimostrarlo:

$$(xy)^{-1} = \frac{\overline{xy}}{\|xy\|^2} = \frac{\overline{y}\overline{x}}{\|y\|^2\|x\|^2} = \frac{\overline{y}}{\|y\|^2}\frac{\overline{x}}{\|x\|^2} = y^{-1}x^{-1}.$$

si può infatti vedere, con un pò di conti che:

$$(xy)y = xy^2, \quad (xy)x = x(yx).$$

Inoltre, questo si può estendere al prodotto con i coniugati:

$$(xy)\overline{y} = x\|y\|^2, \quad (xy)\overline{x} = x(y\overline{x}).$$

3.3 La costruzione di Cayley-Dickson

La costruzione di Cayley-Dickson produce una sequenza di algebre sopra il campo dei numeri reali, ognuna delle quali ha dimensione doppia della precedente. Le algebre prodotte da questo processo sono note come *algebre di Cayley-Dickson* e sono tutte dotate di una norma e di un'operazione di coniugazione. In tutte le algebre il prodotto di un elemento per il suo coniugato è pari al quadrato della sua norma. I primi tre passaggi (quaternioni, ottetti, sedenioni) hanno la sorprendente caratteristica di perdere ad una ad una tre proprietà che invece soddisfano i numeri reali e i complessi: ovvero la *commutatività* per i quaternioni, l'*associatività* per gli ottonioni e infine le proprietà dell'*algebra alternativa*[9] per i sedenioni.

Tutte le algebre di Cayley-Dickson mantengono l'associatività della potenza. L'operazione di somma rimane sempre commutativa e associativa.

Nelle sezioni precedenti abbiamo costruito i quaternioni e gli ottonioni "raddoppiando" un'algebra più piccola (e in questo modo si costruiscono anche i numeri complessi):

$$\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i,$$
$$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j,$$
$$\mathbb{O} = \mathbb{H} \oplus \mathbb{H}l.$$

Utilizzando una notazione leggermente diversa, abbiamo che:

NUMERI COMPLESSI Un numero complesso z si può scrivere come una coppia di numeri reali, la sua *parte reale* e la sua *parte immaginaria*. Dunque possiamo scrivere:

$$z = (x, y),$$

che corrisponde, nel linguaggio vettoriale, a $z = x + yi$. Abbiamo che:

- $\overline{(x, y)} = (x, -y)$,

[9] Per *algebra alternativa* si intende un'algebra su campo per la quale valgono le identità $(xx)y = x(xy)$ e $y(xx) = (yx)x$ per ogni elemento x e y dell'algebra.

- $(x, y)(h, k) = (xh - ky, kx + yh)$,[10]
- $(x, y)\overline{(x, y)} = (x^2 + y^2, 0)$.

QUATERNIONI Un quaternione q si può scrivere come una coppia di numeri complessi. Dunque possiamo scrivere:

$$q = (z, w),$$

che corrisponde, nel linguaggio vettoriale, a $q = z + wj$. Abbiamo che:

- $\overline{(z, w)} = (\overline{z}, -w)$,
- $(z, w)(h, k) = (zh - \overline{k}w, kz + w\overline{h})$,
- $(z, w)\overline{(z, w)} = (|z|^2 + |w|^2, 0)$.

OTTONIONI Un ottonione p si può scrivere come una coppia di quaternioni. Dunque possiamo scrivere:

$$p = (q, r),$$

che corrisponde, nel linguaggio vettoriale, a $p = q + rl$. Abbiamo che:

- $\overline{(q, r)} = (\overline{q}, -r)$,
- $(q, r)(s, t) = (qs - \overline{t}r, tq + r\overline{s})$,
- $(q, r)\overline{(q, r)} = (\|q\|_{\mathbb{H}}^2 + \|r\|_{\mathbb{H}}^2, 0)$.

Tutte queste costruzioni sono casi speciali del processo di Cayley-Dickson, per cui:

- $\overline{(a, b)} = (\overline{a}, -b)$,
- $(a, b)(c, d) = (ac - \epsilon\overline{d}b, da + b\overline{c})$,
- $(a, b)\overline{(a, b)} = (\|a\|^2 + \epsilon\|b\|^2, 0)$,

dove $\epsilon = \pm 1$.

Possiamo quindi usare questa costruzione per generare algebre più grandi a partire da algebre più piccole facendo, ad ogni step, una scelta per ϵ.

[10] La definizione di prodotto tra numeri complessi coincide con quella data più in generale successivamente perché ricordiamo che nei reali si ha $\alpha = \overline{\alpha}$.

3.4 Sedenioni

Cosa succede se continuiamo questo processo?

Definiamo i *sedenioni* considerando coppie di ottonioni:

$$s = (x, y), \quad x, y \in \mathbb{O}.$$

Tramite il processo di Cayley-Dickson, con $\epsilon = 1$, definiamo:

le operazioni di *somma* e di *prodotto*:

- $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$,
- $(x_1, y_1)(x_2, y_2) = (x_1x_2 - \overline{y_2}y_1, y_2x_1 + y_1\overline{x_2})$.

Dato un sedenione $s = (x, y)$, il suo coniugato è il sedenione $\overline{s} = (\overline{x}, -y)$.

Si ha che $(x, y)\overline{(x, y)} = (\|x\|^2_{\mathbb{O}} + \|y\|^2_{\mathbb{O}}, 0)$.

Se definiamo l'elemento $e = (0, 1)$, allora possiamo anche scrivere:

$$s = x + ye,$$

dal momento che $(x, 0)(1, 0) = (x, 0)$ e $(y, 0)(0, 1) = (0, y)$.

Per i sedenioni non valgono nè la proprietà commutativa, nè quella associativa (in quanto sono coppie di ottonioni). Come per le altre algebre definite in precedenza, la norma di un sedenione non nullo è strettamente positiva.

Tuttavia i sedenioni contengono i divisori dello zero, ovvero elementi non nulli il cui prodotto fa zero:

$$\begin{aligned}(il + je)(jl + ie) &= (il, j)(jl, i) = ((il)(jl) - \bar{i}j, i(il) + j(\overline{jl})) = \\ &= ((il)(jl) + ij, i(il) - j(jl)) = (-k + k, -l + l) = (0, 0).\end{aligned}$$

I sedenioni non sono un'algebra di composizione, ovvero non soddisfano l'identità $\|s_1s_2\| = \|s_1\|\|s_2\|$.

Capitolo 4

Teoremi di Frobenius e Hurwitz

In quest'ultimo capitolo presentiamo due importanti risultati di Algebra.

Il primo è dovuto al matematico tedesco Ferdinand Georg Frobenius (1849-1917) e mostra che qualunque spazio vettoriale reale di dimensione finita, dotato di un prodotto che lo renda un corpo (anche non commutativo), dev'essere isomorfo a $\mathbb{R}$ oppure a $\mathbb{C}$ oppure a $\mathbb{H}$.

Il secondo è stato dimostrato dal matematico tedesco Adolf Hurwitz (1859-1919) e afferma che i numeri reali, i numeri complessi, i quaternioni e gli ottonioni sono le uniche $\mathbb{R}$-*algebre di composizione* [1] con una norma definita positiva, ed anche le uniche senza divisori dello zero.

Infine, come applicazione del Teorema di Hurwitz, vediamo che gli unici spazi euclidei che possono ammettere un prodotto simile a quello vettoriale sono $\mathbb{R}, \mathbb{R}^3, \mathbb{R}^7$ (il caso $\mathbb{R}$ è degenere).

4.1 Teorema di Frobenius

Teorema 4.1 (Ferdinand Georg Frobenius, 1878)**.** *Sia V uno spazio vettoriale di dimensione finita su $\mathbb{R}$ dotato di un prodotto che lo renda un corpo (non necessariamente commutativo). Allora V è isomorfo a $\mathbb{R}$, oppure a $\mathbb{C}$ oppure ad $\mathbb{H}$.*

[1] Un'algebra di composizione è un'algebra in cui vale la moltiplicatività delle lunghezze (o delle norme), ovvero:
data A algebra, A è algebra di composizione se, presi $z_1, z_2 \in A$, vale $\|z_1 z_2\| = \|z_1\| \|z_2\|$.

Dimostrazione. [2]

Essendo per ipotesi V un corpo, $1 \in V$ (è l'elemento neutro per il prodotto) e quindi abbiamo che $\mathbb{R} \subseteq V$ (perché $\mathbb{R}$ si identifica con il sottospazio generato da 1).

Se $V = \mathbb{R}$ abbiamo finito.

Altrimenti, consideriamo un elemento $v \in V \setminus \mathbb{R}$. Dal momento che $dim_{\mathbb{R}} V < \infty$, possiamo supporre che $dim_{\mathbb{R}} V = n$. Allora gli elementi $1 = v^0, v, v^2, \ldots, v^n$ sono linearmente dipendenti (essendo $n+1$). Quindi esiste un polinomio $P(x)$ [3] a coefficienti in $\mathbb{R}$ tale che $P(v) = 0_V$. Per il teorema fondamentale dell'algebra, P si può fattorizzare in termini lineari e quadratici[4], cioè:

$$P_1(v)P_2(v)\ldots P_k(v) = 0.$$

Essendo ora quel prodotto nullo (un corpo è privo di divisori dello zero), dev'essere che uno di quei termini (almeno uno) è nullo. Se v soddisfasse un'equazione lineare, allora $v \in \mathbb{R}$, contro l'ipotesi. Dunque possiamo assumere che valga l'equazione:

$$av^2 + bv + c = 0, \quad \text{con} \quad a \neq 0.$$

Allora

$$v = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Da qui si ha che $\sqrt{b^2 - 4ac} \in V$.

Se $\sqrt{b^2 - 4ac} \in \mathbb{R}$, allora anche $v \in \mathbb{R}$, assurdo.

Perciò dev'essere $b^2 - 4ac < 0$ e $\sqrt{b^2 - 4ac} = \sqrt{-(4ac - b^2)}$. Chiamiamo allora $i = \frac{\sqrt{b^2-4ac}}{\sqrt{4ac-b^2}}$, quindi $i \in V$ è tale che $i^2 = -1$.

(Useremo ancora questo argomento notando che, se w è un altro elemento non appartenente a $\mathbb{R}$, allora possiamo ancora scriverlo come $w = r_1 + r_2 j$, con j un altro elemento tale che $j^2 = -1$).

Questa scelta di $i \in V$ ci permette di definire un morfismo (iniettivo)[5] di $\mathbb{R}$-algebre

$$\begin{array}{rccc} \alpha : & \mathbb{C} & \longrightarrow & V \\ & a + ib & \longmapsto & a + ib. \end{array}$$

[2] La dimostrazione riportata è quella di Richard Sheldon Palais, pubblicata nel mensile americano *The American Mathematical Monthly* nell'aprile del 1968.

[3] Il polinomio $P(x)$ è del tipo $\sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$; e si ha che $\sum_{i=0}^{n} a_i v^i = 0_V$, con $a_i \in \mathbb{R}$ non tutti nulli.

[4] Sono quadratici quando la radice è complessa (accoppiando il complesso e il suo coniugato); sono lineari quando la radice è reale.

[5] Il morfismo α induce una struttura di $\mathbb{C}$-spazio vettoriale su V.

Se è anche suriettivo, ovvero se $dim_{\mathbb{R}}V = 2$, allora $V \simeq \mathbb{C}$ e quindi abbiamo finito; altrimenti sia $dim_{\mathbb{R}}V > 2$.

Se ignoriamo la moltiplicazione in V e notiamo che gli elementi di V possono essere moltiplicati scalarmente per elementi di $\mathbb{C}$ a sinistra, vediamo che V risulta essere anche uno spazio vettoriale su $\mathbb{C}$.

Definiamo ora l'endomorfismo di $\mathbb{C}$[6]:

$$\begin{array}{cccc} I: & V & \longrightarrow & V \\ & x & \longmapsto & xi. \end{array}$$

Dunque se calcoliamo:

$$(I^2 + id_V)(x) = I^2(x) + id_V(x) = I^2(x) + x =$$
$$I(xi) + x = (xi)i + x = x(i^2) + x = -x + x = 0.$$

Siano poi:

$$V_+ = \{x \mid I(x) = ix\} = \{x \mid xi = ix\},$$
$$V_- = \{x \mid I(x) = -ix\} = \{x \mid xi = -ix\}.$$

$V_+ \oplus V_- = V$.

Ogni elemento di $\mathbb{C}$ appartiene a V_+. Viceversa, se $y \in V_+$, allora commuta con tutti i numeri complessi. Gli elementi $1, y, y^2, \ldots$ sono linearmente dipendenti su $\mathbb{C}$ (essendo V di dimensione finita su $\mathbb{R}$), perciò y soddisfa un polinomio $P(x)$. Fattorizzando $P = P_1(x) \ldots P_k(x)$, notiamo che su $\mathbb{C}$, ogni fattore irriducibile è lineare. Dunque, per un opportuno indice j, si ha che $P_j(y) = 0$, da cui si ottiene che $y \in \mathbb{C}$. Quindi $V_+ \simeq \mathbb{C}$.

Notiamo poi che il prodotto di due elementi x e y in V_- sta in V_+, infatti:

$$se \quad ix = -xi \quad e \quad iy = -yi, \quad allora \quad ixy = -xiy = +xyi.$$

Sia poi z un elemento non nullo di V_-[7]. Dall'osservazione fatta all'inizio della dimostrazione, possiamo scrivere $z = r_1 + r_2 j$ con j un elemento che soddisfa $j^2 = -1$. Quindi $z^2 \in V_+$ e $z^2 = r_1^2 + 2r_1r_2j - r_2^2$. Questo elemento appartiene a $\mathbb{C}$, quindi o $r_1r_2 = 0$ oppure $j \in \mathbb{C}$. Ma se $j \in \mathbb{C}$, allora anche $z \in \mathbb{C}$, assurdo. Perciò dev'essere $r_1r_2 = 0$, ovvero $r_1 = 0$ oppure $r_2 = 0$. Se $r_2 = 0$, allora $z \in \mathbb{R}$, il che è impossibile. Quindi dev'essere $r_1 = 0$ e $j \in V_-$.

Inoltre per ogni $z' \in V$ si ha che il prodotto $z'j \in \mathbb{C}$. Quindi se $z'j = c$, allora essendo $j^2 = -1$, si ha che $(z'j)j = z'(jj) = -z' = cj$, cioè $z' = -cj$,

[6]I è applicazione $\mathbb{C}$-lineare di V in V, infatti:

$$I(c_1x_1 + c_2x_2) = (c_1x_1 + c_2x_2)i = c_1(x_1i) + c_2(x_2i) = c_1(I(x_1)) + c_2(I(x_2)).$$

[7]Quindi $z \notin \mathbb{C}$ perché si ha che $V_+ \cap V_- = \{0\}$.

ovvero j genera V_- sul campo $\mathbb{C}$. Definiamo $k = ij$. Notiamo poi che $ij = -ji$ dalla definizione di V_-. Troviamo poi che $k^2 = (ij)^2 = ijij = -ijji = -1$. Allora si ha che $i^2 = j^2 = k^2 = -1$. Poi $ij = k = -ji$, $jk = jij = -ijj = i$ e $kj = ijj = -i$. In conclusione, $ki = iji = -jii = j$ e $ik = iij = -j$. Perciò $V \simeq \mathbb{H}$. □

4.2 Teorema di Hurwitz

Quando la moltiplicazione è *commutativa*, un prodotto di due quadrati è ancora un quadrato:

$$x^2y^2 = (xy)^2.$$

Procedendo, sappiamo che esiste un'*identità dei due quadrati*, che esprime il prodotto di due somme di due quadrati come una somma di due quadrati:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2,^8 \tag{4.1}$$

Inoltre, come abbiamo visto nella Proposizione 1.6, vale l'*identità dei quattro quadrati*, ovvero il prodotto di due somme di quattro quadrati è una somma di quattro quadrati:

$$\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\
&(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\
&(x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2.
\end{aligned}$$

Tutte le identità sopra descritte sono *identità polinomiali*, perciò sono valide anche quando andiamo a sostituire al posto delle variabili x_i, y_j elementi di un qualsiasi campo.

In queste identità, i termini sono tutti espressioni bilineari nella x e nella y; ad esempio, in 4.1, $x_1y_2 + x_2y_1$ è combinazione lineare della x quando la y è fissata ed è combinazione lineare della y quando la x è fissata.

Nel XIX secolo, dopo che Hamilton rese popolare l'identità dei quattro quadrati nel suo lavoro sui quaternioni (era già stata trovata da Eulero nel XVIII secolo, ma poi dimenticata), Cayley scoprì una simile identità, quella

[8] Segue dalla proprietà del modulo dei numeri complessi: $|z_1z_2| = |z_1||z_2|$. Quindi sostituendo in $|z_1|^2|z_2|^2 = |z_1z_2|^2$ i numeri complessi $z_1 = x_1 + ix_2, z_2 = y_1 + iy_2$, si ottiene l'identità cercata.

degli otto quadrati, già vista nella Proposizione 3.6:

$$(x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2)(y_1^2+y_2^2+y_3^2+y_4^2+y_5^2+y_6^2+y_7^2+y_8^2)=$$
$$(x_1y_1-x_2y_2-x_3y_3-x_4y_4-x_5y_5-x_6y_6-x_7y_7-x_8y_8)^2+$$
$$(x_1x_2+x_2y_1+x_3y_4-x_4y_3+x_5y_6-x_6y_5-x_7y_8+x_8y_7)^2+$$
$$(x_1y_3-x_2y_4+x_3y_1+x_4y_2-x_5y_7-x_6y_8+x_7y_5+x_8y_6)^2+$$
$$(x_1y_4+x_2y_3-x_3y_2+x_4y_1-x_5y_8+x_6y_7-x_7y_6+x_8y_5)^2+$$
$$(x_1y_5-x_2y_6+x_3y_7+x_4y_8+x_5y_1+x_6y_2-x_7y_3-x_8y_4)^2+$$
$$(x_1y_6+x_2y_5+x_3y_8-x_4y_7-x_5y_2+x_6y_1+x_7y_4-x_8y_3)^2+$$
$$(x_1y_7+x_2y_8-x_3y_5+x_4y_6+x_5y_3-x_6y_4+x_7y_1-x_8y_2)^2+$$
$$(x_1y_8-x_2y_7-x_3y_6-x_4y_5+x_5y_4+x_6y_3+x_7y_2+x_8y_1)^2.$$

Era quindi naturale per i matematici del tempo cercare un'identità simile che valesse per i sedici quadrati, ma non ci si riuscì. Alla fine dei XIX secolo, Hurwitz dimostrò il suo celebre teorema "1,2,4,8 Teorema" che affermava che altre identità del tipo sopra descritto non esistono.

Fu così che il matematico tedesco Adolf Hurwitz (1859-1919) provò, nel 1898, il seguente teorema:

Teorema 4.2 (Hurwitz, 1898)**.** *Sia K un campo di caratteristica $\neq 2$.* [9] *Se*

$$(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_n^2)=z_1^2+\cdots+z_n^2, \tag{4.2}$$

per ogni $x_1,\ldots,x_n,y_1,\ldots,y_n$ in K, dove ogni z_k è bilineare nella x e nella y, allora:

$$n=1,2,4 \quad \textit{oppure} \quad 8.$$

La dimostrazione originale di Hurwitz era stata fatta per $K=\mathbb{C}$, campo di caratteristica zero. Mentre Hurwitz ha dimostrato soltanto che quell'identità vale per i vincoli dimensionali $n=1,2,4,8$, in realtà si può far vedere che le uniche identità di quel tipo sono quelle associate alla moltiplicazione nelle quattro classiche algebre di divisione, di dimensione $1,2,4$ e 8, ovvero: i numeri reali, i numeri complessi, i quaternioni e gli ottonioni.

Lemma 4.3. *Sia V uno spazio vettoriale di dimensione finita su K, con K campo di caratteristica diversa da 2. Se c'è una coppia di endomorfismi di V che siano lineari, invertibili e anticommutativi, allora $dimV$ è pari.*

---

[9] Se infatti considero un campo K di caratteristica 2, abbiamo che l'identità del teorema vale per qualsiasi n, in quanto una somma di quadrati in caratteristica 2 è ancora un quadrato.

Ricordiamo infatti che per un campo K di caratteristica un numero primo p, si ha che: $(x+y)^p=x^p+y^p$.

Dimostrazione. Supponiamo esistano $L, L' \colon V \to V$ lineari, invertibili e tali che $LL' = -L'L$. Allora $(detL)(detL') = (-1)^{dimV}(detL')(detL)$. Essendo L, L' invertibili, si ha che $detL \neq 0$, $detL' \neq 0$, dunque dev'essere $1 = (-1)^{dimV}$ in K; perciò anche $dimV$ è pari (dal momento che K ha caratteristica diversa da 2). □

La dimostrazione del Teorema di Hurwitz. Torniamo ora a 4.2. Che le z_k siano funzioni bilineari nella x e nella y significa che

$$z_k = \sum_{i,j=1}^{n} a_{ijk} x_i y_j, \quad \text{per qualche} \quad a_{ijk} \in K. \tag{4.3}$$

Ad esempio, nel caso $n = 2$, possiamo vedere da 4.1 che possiamo porre

$$\begin{aligned} z_1 &= x_1 y_1 - x_2 y_2, \\ z_2 &= x_1 y_2 + x_2 y_1. \end{aligned}$$

Possiamo raccogliere le due equazioni sopra in:

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} x_1 y_1 - x_2 y_2 \\ x_1 y_2 + x_2 y_1 \end{pmatrix} = \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = (x_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Dall'identità dei quattro quadrati, ovvero per $n = 4$, possiamo porre:

$$\begin{aligned} z_1 &= x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4 \\ z_2 &= x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3 \\ z_3 &= x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2 \\ z_4 &= x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2. \end{aligned}$$

Perciò

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = (x_1 A_1 + x_2 A_2 + x_3 A_3 + x_4 A_4) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix},$$

dove A_1, A_2, A_3, A_4 sono matrici 4×4 con entrate tutte uguali a $0, 1, -1$. Sviluppando i conti, troviamo:

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4 \\ x_1 y_2 + x_2 y_1 + x_3 y_4 - x_4 y_3 \\ x_1 y_3 + x_3 y_1 - x_2 y_4 + x_4 y_2 \\ x_1 y_4 + x_4 y_1 + x_2 y_3 - x_3 y_2 \end{pmatrix} = \begin{pmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & -x_4 & x_3 \\ x_3 & x_4 & x_1 & -x_2 \\ x_4 & -x_3 & x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}.$$

Dunque risulta

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$
$$A_3 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Tali equazioni matriciali possono essere sviluppate anche nel caso $n \times n$. Le n equazioni 4.3 per $k = 1, \dots, n$ si possono raggruppare in un'unica equazione:

$$\begin{aligned} \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} &= \begin{pmatrix} \sum_{i,j} a_{ij1} x_i y_j \\ \vdots \\ \sum_{i,j} a_{ijn} x_i y_j \end{pmatrix} = \\ &= \begin{pmatrix} \sum_j (\sum_i a_{ij1} x_i) y_j \\ \vdots \\ \sum_j (\sum_i a_{ijn} x_i) y_j \end{pmatrix} = \\ &= \begin{pmatrix} \sum_i a_{i11} x_i & \dots & \sum_i a_{in1} x_i \\ \vdots & \ddots & \vdots \\ \sum_i a_{i1n} x_i & \dots & \sum_i a_{inn} x_i \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned} \tag{4.4}$$

La matrice $n \times n$ dell'ultima espressione può essere espressa come somma di n matrici $n \times n$, ognuna delle quali contiene una sola delle x_i che può essere portata fuori come coefficiente:

$$x_1 \begin{pmatrix} a_{111} & \dots & a_{1n1} \\ \vdots & \ddots & \vdots \\ a_{11n} & \dots & a_{1nn} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{n11} & \dots & a_{nn1} \\ \vdots & \ddots & \vdots \\ a_{n1n} & \dots & a_{nnn} \end{pmatrix}.$$

Questa somma può essere scritta come

$$x_1 A_1 + \dots + x_n A_n,$$

dove A_i è una matrice $n \times n$ con a_{ikj} nell'entrata (j, k). Quindi 4.4 si può anche scrivere come:

$$z = (x_1 A_1 + \dots + x_n A_n) y = A_x y,$$

dove $A_x = x_1A_1 + \cdots + x_nA_n$.

Con questa notazione, il membro di destra di 4.2 diventa

$$z_1^2+\cdots+z_n^2 = z\cdot z = (A_xy)\cdot(A_xy) = {}^t y({}^t A_xA_xy) = y\cdot({}^t A_xA_xy) = ({}^t A_xA_xy)\cdot y,$$

mentre il membro di sinistra di 4.2 risulta essere

$$(\sum_i x_i^2)y \cdot y = ((\sum_i x_i^2)y) \cdot y.$$

Pertanto,

$$({}^t A_xA_xy) \cdot y = ((\sum_i x_i^2)y) \cdot y.$$

Confrontando i due membri (dal momento che il campo K ha più di due elementi), si ottiene

$$ {}^t A_xA_x = (\sum_i x_i^2)\mathbf{1}_n; \tag{4.5}$$

Espandendo il membro di sinistra di 4.5 usando $A_x = x_1A_1 + \cdots + x_nA_n$, abbiamo che

$$ {}^t A_xA_x = \sum_i^n ({}^t A_iA_i)x_i^2 + \sum_{1\leq i<j\leq n} ({}^t A_iA_j + {}^t A_jA_i)x_ix_j,$$

perciò 4.5 è equivalente al sistema di equazioni matriciali:

$$ {}^t A_iA_i = \mathbf{1}_n, \tag{4.6}$$
$$ {}^t A_iA_j + {}^t A_jA_i = \mathbf{0}_n, \quad \text{per} \quad i < j. \tag{4.7}$$

Queste sono le *equazioni matriciali di Hurwitz*. (Le entrate delle matrici A_i non ci interessano più.)

Il resto della dimostrazione del Teorema di Hurwitz serve per mostrare che quel sistema (4.6 +4.7) fatto da matrici di ordine $n\times n$ ammette soluzioni solo se $n = 1, 2, 4$ oppure 8.

Senza perdità di generalità, supponiamo $n > 2$.

Da 4.6, abbiamo che A_i è una matrice invertibile con inversa ${}^t A_i$.

Sia ora $B_i = A_i\, {}^t A_n$.

È facile vedere che 4.6 e 4.7 sono equivalenti a:

$$B_n = \mathbf{1}_n,$$
$$ {}^t B_iB_i = \mathbf{1}_n,$$
$$ {}^t B_iB_j + {}^t B_jB_i = \mathbf{0}_n, \quad \text{per} \quad i < j.$$

(Scriveremo $i \neq j$ piuttosto che $i < j$ per rendere le cose più simmetriche, ma non cambia nulla.)

Prendendo $j = n$ nella terza equazione, si ha che

$$^tB_i = -B_i, \quad \text{per} \quad i \neq n.$$

Pertanto le $n-1$ matrici $B_1, \ldots, B_{n-1}$ soddisfano:

$$^tB_i = -B_i, \quad B_i^2 = -\mathbf{1}_n, \quad B_iB_j = -B_jB_i \quad \text{per} \quad i \neq j. \tag{4.8}$$

Quindi vediamo necessariamente dal Lemma 4.3 che n dev'essere pari (quindi il caso n=3 è escluso). A questo punto possiamo prendere $n \geq 4$ (e n pari). Ignoriamo la matrice B_{n-1} perché abbiamo detto che ci serve un numero pari di B_i. Consideriamo quindi l'insieme formato dalle matrici $B_1^{\delta_1}, \ldots, B_{n-2}^{\delta_{n-2}} \in M_{n\times n}(K)$, dove $\delta_i \in \{0, 1\}$. Si dimostra che queste matrici sono linearmente indipendenti. Ma le matrici di ordine $n \times n$ vivono in uno spazio di dimensione n^2. Quindi dev'essere soddisfatta

$$2^{n-2} \leq n^2.$$

E si vede che quella disuguaglianza è vera per $n = 2, 4, 6, 8$ e nessun'altro n. $\square$

4.3 I prodotti vettoriali

Usiamo il Teorema di Hurwitz per rispondere alla seguente domanda:

Il prodotto vettoriale in $\mathbb{R}^3$ può avere un analogo in $\mathbb{R}^n$, con $n > 3$? Dopo aver specificato quali proprietà vogliamo che soddisfi questo prodotto, vedremo che le scelte sono alquanto limitate.

- La moltiplicazione in $\mathbb{R}^n$ deve assegnare, ad ogni v, w in $\mathbb{R}^n$, un terzo vettore in $\mathbb{R}^n$, che denoteremo con $v \times w$.

- Il prodotto dev'essere $\mathbb{R}$-bilineare in v e in w:

$$(v_1+v_2)\times w = v_1\times w+v_2\times w, \quad v\times(w_1+w_2) = v\times w_1+v\times w_2. \tag{4.9}$$

  e

$$(cv) \times w = c(v \times w), \quad v \times (cw) = c(v \times w), \quad c \in \mathbb{R}. \tag{4.10}$$

- Una conseguenza della bilinearità è che:

$$v \times 0 = 0, \quad 0 \times w = 0. \tag{4.11}$$

- Il prodotto dev'essere ortogonale ad entrambi i fattori:

  per ogni $v, w \in \mathbb{R}^n$,

  $$v \cdot (v \times w) = 0, \quad w \cdot (v \times w) = 0. \tag{4.12}$$

  Questa proprietà è soddisfatta dal prodotto vettoriale in $\mathbb{R}^3$, ma non vale per altri tipi di prodotti nell'algebra lineare. Ad esempio, la moltiplicazione di matrici in $M_n(\mathbb{R})$ è un prodotto $\mathbb{R}$-bilineare ma non soddisfa 4.12 quando v e w sono matrici, $\times$ indica l'usuale prodotto tra matrici e $\cdot$ è dato da $(a_{ij}) \cdot (b_{ij}) = \sum_{ij} a_{ij} b_{ij}$.

- Il modulo $\|v \times w\|$ dev'essere determinato dalla stessa formula che vale per il prodotto vettoriale in $\mathbb{R}^3$:

  $$\|v \times w\|^2 = \|v\|^2 \|w\|^2 - (v \cdot w)^2, \text{[10]} \tag{4.13}$$

  Osserviamo che quando $n = 1$, un prodotto in $\mathbb{R}^n = \mathbb{R}$ dev'essere identicamente nullo, infatti, essendo che il prodotto scalare su $\mathbb{R}$ è il prodotto usuale, si ha che 4.13 diventa:

  $$|x \times y|^2 = x^2 y^2 - (xy)^2 = 0, \quad \text{perciò} \quad x \times y = 0.$$

  Quindi risulta interessante studiare solo i casi per $n > 1$.

Il seguente risultato esprime 4.13 in termini più semplici:

Lemma 4.4. *Sia $\times$ un prodotto in $\mathbb{R}^n$ che soddisfi 4.9, 4.10 e 4.12. Allora 4.13 è equivalente alle seguenti due condizioni (prese insieme):*

1. *Per ogni $v \in \mathbb{R}^n$, $v \times v = 0$.*
2. *Se $\|v\| = 1, \|w\| = 1$ e $v \perp w$, allora $\|v \times w\| = 1$.*

Dimostrazione. È facile vedere che 4.13 implica le due condizioni del Lemma, infatti:

1. Sostituendo in 4.13 $w \in \mathbb{R}^n$ con $v \in \mathbb{R}^n$ si ha:

   $$\|v \times v\|^2 = \|v\|^2 \|v\|^2 - (v \cdot v)^2 = \|v\|^4 - \|v\|^4 = 0,$$

   dunque $\|v \times v\| = 0$, cioè $v \times v = 0$ per ogni $v \in \mathbb{R}^n$.

[10]È l'identità di Lagrange.

2. Sostituendo in 4.13, $\|v\| = 1, \|w\| = 1, v \perp w$, si ha:
$$\|v \times w\|^2 = 1 - 0 = 1,$$
dunque $\|v \times w\| = 1$, essendo la norma un numero reale non negativo.

Ora mostriamo il viceversa, cioè deriviamo 4.13 assumendo le due condizioni del Lemma.

- Supponiamo dapprima che v e w siano linearmente dipendenti, ovvero che esista un $c \in \mathbb{R}$ per cui valga $w = cv$. Allora:

  $\|v \times w\|^2 = \|v \times (cv)\|^2 = \|c(v \times v)\|^2 = |c|^2 \|v \times v\|^2 = c^2 \|v \times v\|^2 = 0,$ [11]

  $\|v\|^2\|w\|^2 - (v \cdot w)^2 = \|v\|^2\|cv\|^2 - (v \cdot cv)^2 = \|v\|^2|c|^2\|v\|^2 - c^2(v \cdot v)^2 = c^2\|v\|^4 - c^2\|v\|^4 = 0,$

  dunque entrambi i membri dell'equazione 4.13 sono nulli.

- Supponiamo che v e w siano linearmente indipendenti.

  Quindi essendo $w \neq 0_{\mathbb{R}^3}$, si ha $w \cdot w = \|w\|^2 \neq 0$, dunque possiamo considerare il vettore $u \in \mathbb{R}^n$ dato da:
$$u = v - \frac{v \cdot w}{w \cdot w} w.$$
  Abbiamo che $u \perp w$, infatti:
$$u \cdot w = (v - \frac{v \cdot w}{w \cdot w} w) \cdot w = v \cdot w - (\frac{v \cdot w}{w \cdot w}) w \cdot w = v \cdot w - v \cdot w = 0.$$
  Dunque $\frac{u}{\|u\|}$ e $\frac{w}{\|w\|}$ sono versori perpendicolari; quindi, dalla seconda condizione del Lemma:
$$\|\frac{u}{\|u\|} \times \frac{w}{\|w\|}\| = 1.$$
  Per bilinearità:
$$1 = \|\frac{u}{\|u\|} \times \frac{w}{\|w\|}\| = \frac{\|u \times w\|}{\|u\|\|w\|},$$
  dunque
$$\|u \times w\| = \|u\|\|w\| \tag{4.14}$$

[11] Dove la seconda uguaglianza segue da 4.10 e l'ultima segue dalla prima condizione del Lemma.

Dal momento che $w \times w = 0$ (dalla prima condizione del Lemma), per bilinearità e per 4.11, si ha che:

$$u \times w = (v - \frac{v \cdot w}{w \cdot w}w) \times w = v \times w - (\frac{v \cdot w}{w \cdot w})(w \times w) = v \times w.$$

Quindi l'equazione 4.14 diventa:

$$\|u \times w\| = \|v \times w\| = \|u\|\|w\|,$$

ed elevando al quadrato si ha:

$$\|v \times w\|^2 = \|u\|^2\|w\|^2.$$

Andiamo ora a calcolare $\|u\|^2$:

$$\begin{aligned} \|u\|^2 &= u \cdot u = \\ &= (v - \tfrac{v \cdot w}{w \cdot w}w)(v - \tfrac{v \cdot w}{w \cdot w}w) = \\ &= v \cdot v - 2\tfrac{v \cdot w}{w \cdot w}v \cdot w + \tfrac{(v \cdot w)^2}{(w \cdot w)^2}w \cdot w = \\ &= \|v\|^2 - 2\tfrac{(v \cdot w)^2}{w \cdot w} + \tfrac{(v \cdot w)^2}{w \cdot w} = \\ &= \|v\|^2 - \tfrac{(v \cdot w)^2}{w \cdot w} = \\ &= \|v\|^2 - \tfrac{(v \cdot w)^2}{\|w\|^2}, \end{aligned}$$

quindi si ha che:

$$\|v \times w\|^2 = (\|v\|^2 - \frac{(v \cdot w)^2}{\|w\|^2})\|w\|^2 = \|v\|^2\|w\|^2 - (v \cdot w)^2.$$

□

Teorema 4.5. *Per $n \geq 1$, supponiamo esista un prodotto $\times : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ soddisfacente le condizioni 4.9, 4.10, 4.12 e 4.13. Allora $n = 1, 3$ oppure 7.*

Dimostrazione. Usiamo il prodotto $\times$ in $\mathbb{R}^n$ per definire un prodotto, detto $\odot$, in $\mathbb{R}^{n+1}$. Scriviamo i vettori in $\mathbb{R}^{n+1}$ nella forma (x, v), dove $x \in \mathbb{R}$, $v \in \mathbb{R}^{n+1}$.

Notiamo che il prodotto scalare di due vettori in $\mathbb{R}^{n+1}$ può essere espresso in termini dei prodotti scalari delle componenti:

$$(x, v) \cdot (y, w) = xy + v \cdot w.$$

Per $(x, v), (y, w) \in \mathbb{R}^{n+1}$, definiamo:

$$(x, v) \odot (y, w) = (xy - v \cdot w, xw + yv + v \times w). \tag{4.15}$$

Questa formula ha un senso dal momento che $xy - v \cdot w \in \mathbb{R}$ e $xw + yv + v \times w \in \mathbb{R}^{n+1}$.

Questo prodotto $\odot$ in $\mathbb{R}^{n+1}$ ha due proprietà chiavi:

1. È bilineare in (x, v) e in (y, w). Cioè, fissando una coppia di questi vettori in $\mathbb{R}^{n+1}$, il membro di destra dell'equazione 4.15 è una funzione lineare dell'altra coppia.

2. È moltiplicativo per le lunghezze, cioè vale:
$$\|(x, v) \odot (y, w)\|^2 = \|(x, v)\|^2 \|(y, w)\|^2. \tag{4.16}$$

Verifichiamo ora 4.16. A sinistra, abbiamo che:

$$\begin{aligned}
&\|(x, v) \odot (y, w)\|^2 = \\
&(xy - v \cdot w, xw + yv + v \times w) \cdot (xy - v \cdot w, xw + yv + v \times w) = \\
&(xy - v \cdot w)^2 + (xw + yv + v \times w) \cdot (xw + yv + v \times w).
\end{aligned}$$

Da 4.12 abiamo che $v \times w$ è ortogonale a $xw + yv$.

Pertanto,

$$\begin{aligned}
&(xw + yv + v \times w) \cdot (xw + yv + v \times w) = \\
&(xw + yv) \cdot (xw + yv) + (v \times w) \cdot (v \times w) = \\
&x^2(w \cdot w) + 2xy(v \cdot w) + y^2(v \cdot v) + \|v \times w\|^2 = \\
&x^2\|w\|^2 + 2xy(v \cdot w) + y^2\|v\|^2 + \|v \times w\|^2.
\end{aligned}$$

Aggiungendo a questo anche $(xy - v \cdot w)^2 = x^2y^2 - 2xy(v \cdot w) + (v \cdot w)^2$, otteniamo che:

$$\begin{aligned}
&\|(x, v) \odot (y, w)\|^2 = \\
&x^2y^2 - 2xy(v \cdot w) + (v \cdot w)^2 + x^2\|w\|^2 + 2xy(v \cdot w) + y^2\|v\|^2 + \|v \times w\|^2 = \\
&x^2y^2 + (v \cdot w)^2 + x^2\|w\|^2 + y^2\|v\|^2 + \|v \times w\|^2 = \\
&x^2y^2 + x^2\|w\|^2 + y^2\|v\|^2 + \|v\|^2\|w\|^2 = \\
&(x^2 + \|v\|^2)(y^2 + \|w\|^2) = \\
&\|(x, v)\|^2\|(y, w)\|^2,
\end{aligned}$$

e così abbiamo provato 4.16.

Mostriamo ora la connessione tra $\odot$ e il Teorema di Hurwitz.

Consideriamo due vettori $(x_1, \ldots, x_{n+1}), (y_1, \ldots, y_{n+1}) \in \mathbb{R}^{n+1}$. Il loro prodotto $\odot$ è un terzo vettore $(z_1, \ldots, z_{n+1}) \in \mathbb{R}^{n+1}$, le cui componenti sono calcolate in accordo a 4.15.

Invertendo i termini di destra con quelli di sinistra in 4.16, otteniamo:

$$(x_1^2 + \cdots + x_{n+1}^2)(y_1^2 + \cdots + y_{n+1}^2) = z_1^2 + \cdots + z_{n+1}^2. \tag{4.17}$$

Questa identità vale per qualsiasi valore dato alle variabili. Dalla prima proprietà di $\odot$, gli z_k sono funzioni bilineari nelle x_i e y_j.

Dunque, 4.17 e il Teorema di Hurwitz ci dicono che $n+1 = 1, 2, 4$ oppure 8, dunque $n = 0, 1, 3$ oppure 7. (Il caso $n = 0$ viene scartato). $\square$

Bibliografia

[1] M.Candilera, A.Bertapelle, (2011), *Algebra lineare e primi elementi di Geometria*, McGraw-Hill, Milano

[2] M.Cailotto, (2006), *Algebra e Geometria Lineari e Quadratiche*, http://www.math.unipd.it/ maurizio/m2m/AGLQ910pp.pdf

[3] K.Conrad, *The Hurwitz Theorem on sums of squares*, http://www.math.uconn.edu/ kconrad/blurbs/linmultialg/hurwitzlinear.pdf

[4] R.Koch, (2015), *Frobenius' Theorem*, http://pages.uoregon.edu/koch/Frobenius.pdf

[5] R.Koch, (2015), *The Octonions*, http://pages.uoregon.edu/koch/Octonions.pdf

[6] G.Ottaviani, *Introduzione alla geometria dei quaternioni*, http://web.math.unifi.it/users/ottavian/quaternion.pdf

[7] R.Koch, (2015), *Hurwitz's Theorem*, http://pages.uoregon.edu/koch/Hurwitz.pdf

[8] T. Dray, A. Manogue, (2015), *The Geometry of the Octonions*, Lai Fun Kwong/V. Vishnu Mohan, Singapore