Talete e la logica quantistica

Autore: Renato Nobili
Dipartimento di Fisica dell'Università di Padova

1. Le logiche della fisica

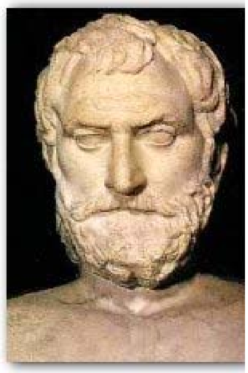
Sia nella fisica classica sia in quella quantistica le proprietà dei sistemi fisici sono descritte da proposizioni logiche che dichiarano la possibile appartenenza dello stato del sistema a certe regioni dello spazio degli stati. Nella fisica classica, dove gli stati fisici sono concepiti come *un insieme di possibilità reciprocamente esclusive*, lo spazio degli stati è rappresentato da un *insieme di punti* S e la proposizione che descrive una proprietà fisica dichiara semplicemente che lo stato appartiene ad un certo *sottoinsieme* di S. Pertanto, le operazioni logiche AND, OR e NOT, che di solito si indicano coi simboli $\wedge$, $\vee$ e $\sim$, denotano rispettivamente le ben note operazioni sugli insiemi: *intersezione*, *unione* e *passaggio al complementare*.

Nella meccanica quantistica gli stati di un sistema fisico formano *un insieme di possibilità che possono interferire in modo costruttivo o distruttivo* secondo un *principio di sovrapposizione* e sono rappresentati dai raggi vettori di lunghezza 1 di uno spazio geometrico infinito H (spazio di Hilbert complesso). In questo caso la proposizione logica indica l'appartenenza del raggio vettore rappresentativo dello stato ad un *sottospazio* di H. L'operazione logica $A\wedge B$ denota ancora, come nel caso classico, l'intersezione insiemistica dei sottospazi A e B, ma ora l'operazione logica $A\vee B$ denota l'*unione geometrica* di A e B, cioè il più piccolo sottospazio vettoriale di H che contiene A e B come sottospazi. La negazione $\sim$ acquista invece il significato di *passaggio allo spazio di raggi vettori ortogonali*. Operazioni simili a queste sono ben note anche nella geometria elementare del piano. Esse sono eseguibili su un foglio di carta mediante riga e matita. Se r ed s sono due rette del piano, l'intersezione geometrica $r\wedge s$ è il punto in cui le rette si intersecano (se le rette sono parallele, il punto si trova all'infinito). Se P, Q sono due punti distinti del piano, $P\vee Q$ non è l'insieme dei due punti ma la retta passante per P e Q. L'operazione di ortogonalizzazione $\sim$ può essere realizzata mediante un squadra per tracciare rette ortogonali ad una retta data.

Nel 1936, Garrett Birkhoff e John von Neumann dimostrarono che la logica quantistica riconosce solo tre tipi di spazi degli stati: lo spazio dei vettori che hanno componenti *reali*, quello dei vettori che hanno come componenti i numeri *complessi* ordinari e quello in cui hanno come componenti i *quaternioni*, di cui ci occuperemo più avanti. In questo scritto mostreremo che le operazioni della logica quantistica $\wedge$ e $\vee$ da sole bastano a determinare le proprietà algebriche dei tre tipi elencati.

2. L'origine della geometria

Per quanto le formalizzazioni simboliche della logica classica e di quella quantistica siano apparse in epoca recente, le operazioni $\wedge$, $\vee$ e $\sim$, intese nel senso geometrico su precisato, furono introdotte circa tre secoli prima che Aristotele (384-322 a.C.) desse inizio alla logica classica. Infatti, esse furono implicite nella *teoria della misura e delle proporzioni* di Talete di Mileto (634-548 a.C.). Il metodo inventato da questo celebre filosofo, più di due millenni prima che i numeri reali venissero concepiti in forma algebrica, non è altro che *l'aritmetica dei numeri reali* espressa con un algoritmo geometrico.


Talete

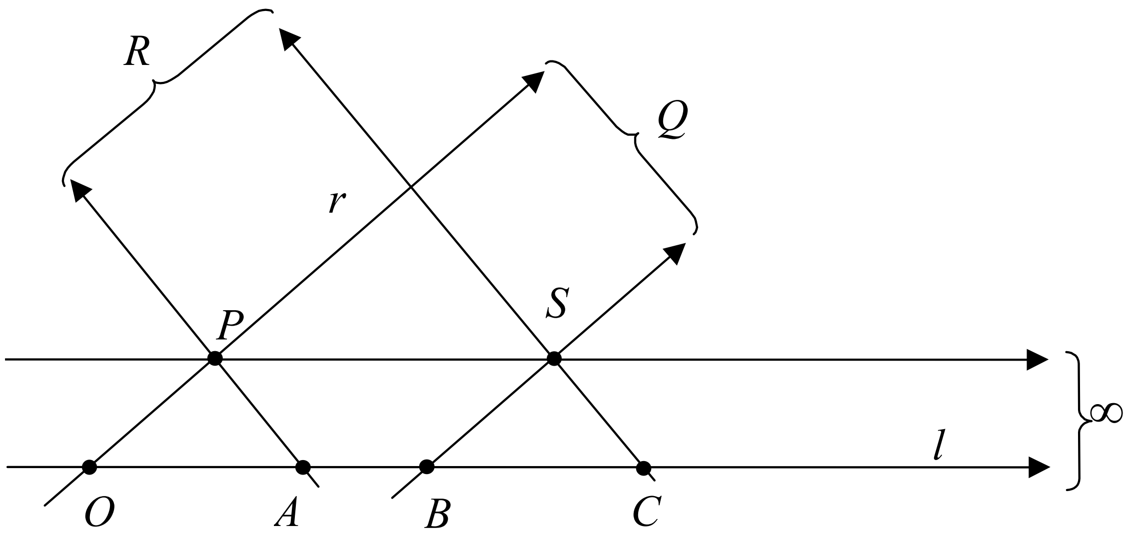
Non è un caso che la teoria geometrica della misura sia stata contemporanea dell'invenzione del *denaro*, "misura di tutte le cose". Infatti, come racconta Erodoto, la circolazione della moneta fu introdotta per la prima volta nel commercio tra i popoli del mediterraneo da Creso, re di Lidia dal 560 al 546 a.C., di cui Talete fu consigliere militare.

3. L'addizione di Talete

Sia data la retta l e su di essa i punti O, A, B e il punto all'infinito ∞ (*punto improprio*). Sia data inoltre un'altra retta r diversa da l e passante per O, e su di essa un punto arbitrario P distinto da O e il punto improprio Q, che equivale alla direzione di r. I punti impropri del piano formano la retta all'infinito, detta anche *retta impropria*. Questa è individuata come la retta che passa per ∞ e Q.

Il metodo di Talete permette di trovare su r il punto di C tale che $OC = OA + OB$. In modo analogo, dati O, A, C e il punto improprio ∞, si può trovare un quinto punto B tale che $OB = OC - OA$. Si ottengono in questo modo l'*addizione* e la *sottrazione* di numeri rappresentati da segmenti.

Per effettuare queste operazioni dobbiamo combinare le operazioni geometriche $\vee$, $\wedge$ e $\sim$, dove $A\vee B$ significa "retta che unisce i punti A e B", mentre $r\wedge l$ significa "punto d'intersezione delle rette r e l". L'operazione $\sim$, che si esegue con riga e squadra, serve a tracciare tutte le rette parallele ortogonali ad una retta data che servono per la costruzione.



Possiamo rappresentare simbolicamente la costruzione che individua il punto-addizione nella forma:

$$C = (O\vee\infty)\wedge(R\vee S), \quad \text{dove } R = (A\vee P)\wedge(Q\vee\infty), \; S = (B\vee Q)\wedge(P\vee\infty).$$

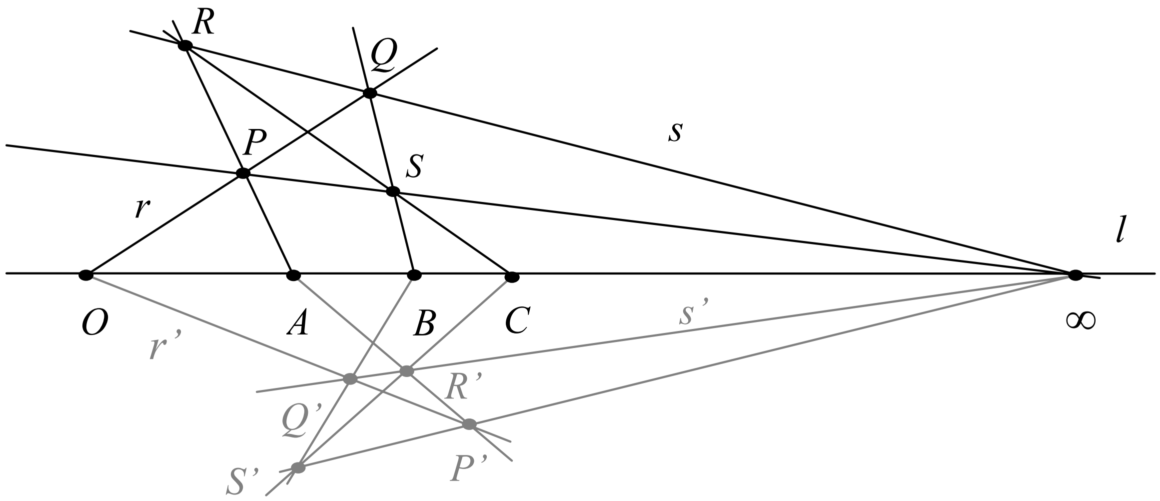
Viceversa, dati A e C, la costruzione che individua il punto-differenza B è rappresentata da:

$$B = (O\vee\infty)\wedge(Q\vee S), \quad \text{dove } R = (A\vee P)\wedge(Q\vee\infty), \; S = (C\vee R)\wedge(P\vee\infty).$$

È abbastanza evidente che le operazioni geometriche così definite sono formalmente commutative e invertibili. Esse dimostrano come si possa implementare l'addizione di Talete utilizzando gli operatori $\vee$ e $\wedge$.

4. La generalizzazione proiettiva dell'addizione di Talete

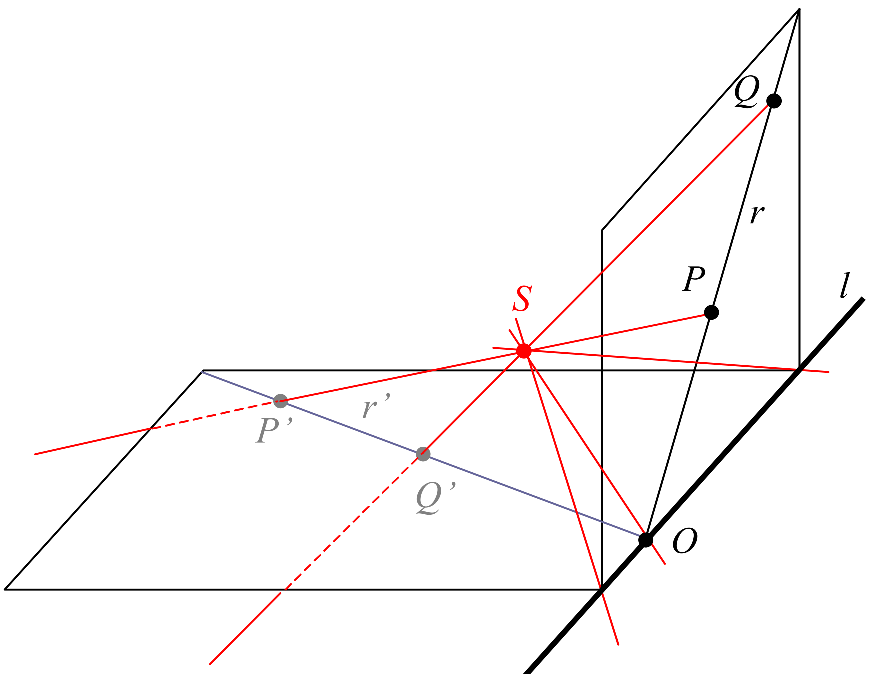
Immaginiamo ora di vedere la figura "in prospettiva" in modo che i punti impropri ∞, Q cadano al finito su una retta s che funge da "linea d'orizzonte". Questa trasformazione prospettica conserva le operazioni logiche $\vee$ e $\wedge$ ma non $\sim$; in questo modo, ci liberiamo dalla necessità di tracciare rette parallele. Il risultato non dipende dal modo con cui si esegue la trasformazione prospettica. Infatti, come dimostreremo nel prossimo paragrafo, esistono infinite altre trasformazioni prospettiche che, lasciando invariata l, proiettano la retta impropria su un'arbitraria retta s' passante per ∞, mentre R e Q sono proiettati su due punti arbitrari e distinti R', Q' di s' (di conseguenza r è proiettata in r' e P su P').



Abbiamo allora, esattamente come per le costruzioni di Talete, $C = (O\vee\infty)\wedge(R\vee S) = (O\vee\infty)\wedge(R'\vee S')$, dove $R = (A\vee P)\wedge(Q\vee\infty)$ e $S = (B\vee Q)\wedge(P\vee\infty)$; oppure, dove $R' = (A\vee P')\wedge(Q\vee\infty)$ e $S' = (B\vee Q')\wedge(P'\vee\infty)$. È evidente che queste equazioni sono *formalmente invarianti* per scambio di A con B e nello stesso tempo di P con Q, oppure di P' con Q'. Poiché, come ora dimostreremo, la costruzione non dipende dalle posizioni di P e Q su r, l'*addizione proiettiva* così definita è formalmente commutativa e invertibile.

5. Insiemi prospettici e invarianza delle relazioni proiettive

La figura sottostante esemplifica come si possa trovare una proiezione prospettica da un punto S che lascia invariata la retta l, mentre proietta una retta r passante per O su un'altra arbitraria retta r' passante per O in modo che una coppia arbitraria di punti P, Q di r (distinti tra loro e da O) sia proiettata su una coppia arbitraria di punti distinti P', Q' di r' (distinti tra loro e da O).

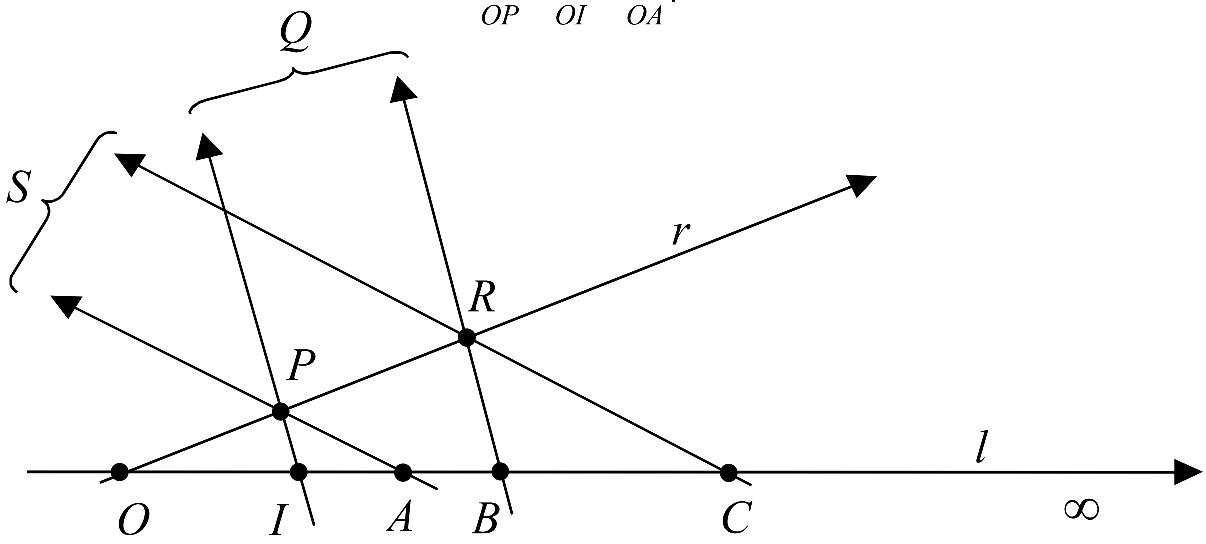


Questo spiega perché tutte le relazioni proiettive tra i punti di l che dipendono da r, P e Q rimangono invariate rispetto alla trasformazione prospettica $r \to r'$, $P \to P'$ e $Q \to Q'$.

6. La moltiplicazione di Talete

Sia data la retta l e su di essa i punti O, I, A, B e il punto improprio ∞. È data inoltre la retta r passante per O e su di essa il punto P e il punto improprio Q. Utilizzando il teorema di Talete sui triangoli simili si trova che i segmenti OR, OP, OI, OC, OA e OB soddisfano alle proporzioni:

$$\frac{OR}{OP} = \frac{OB}{OI} = \frac{OC}{OA}.$$



Pertanto, posto $OI = 1$ (unità di misura) si ottiene:

$$OC = OA \cdot OB; \ \ OB = \frac{OC}{OA}.$$

Vale a dire si trova che il punto C soddisfa all'equazione $OC = OA{\cdot}OB$. Per A arbitrario e $B = O$ si hanno i casi degeneri:

$$OA \cdot OO; \qquad \frac{OA}{OO} = O\,\infty.$$

Queste relazioni mostrano che $OO = 0$ (*zero*) e $O\,\infty$ (*infinito*) e sono uno l'inverso dell'altro. Essi sono tuttavia dei punti eccezionali perché $O\,\infty \cdot OO$ è indeterminato.

È facile verificare che il punto C, che rappresenta la moltiplicazione, è individuato dall'equazione:

$$C = (O \vee \infty) \wedge (R \vee S), \text{ dove } R = (O \vee P) \wedge (B \vee Q), \ S = (\infty \vee Q) \wedge (A \vee P),$$

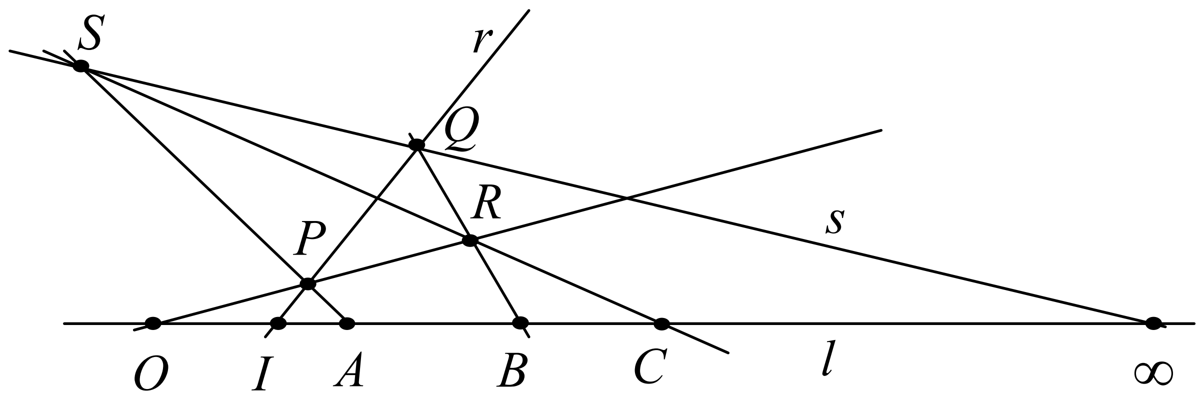
mentre il punto B, che rappresenta la divisione, è individuato dall'equazione:

$$B = (O \vee \infty) \wedge (R \vee Q), \text{ dove } R = (O \vee P) \wedge (C \vee S), \ \ Q = (\infty \vee S) \wedge (I \vee P).$$

Queste equazioni dimostrano come si possa implementare la moltiplicazione di Talete utilizzando gli operatori $\vee$ e $\wedge$.

7. Generalizzazione proiettiva della moltiplicazione di Talete

Consideriamo una trasformata prospettica non degenere della figura precedente. Ora i punti fissi O, I e ∞ di l sono tutti al finito, mentre A e B sono punti generici variabili su l. La retta r passante per I è arbitraria e così pure i punti P e Q (non appartenenti a l).



Ancora, i punti ∞ e Q, e di conseguenza S, non si trovano più sulla retta impropria ma su una retta al finito s. La *moltiplicazione proiettiva* è allora definita dalle equazioni:

$$C = (O\vee\infty)\wedge(R\vee S), \text{ dove } R = (O\vee P)\wedge(B\vee Q), \ S = (\infty\vee Q)\wedge(A\vee P). \qquad (*)$$

Per l'invarianza delle operazioni $\vee$ e $\wedge$, la relazione tra i punti OA, OB e OD è una deformazione prospettica della moltiplicazione di Talete. Possiamo pertanto definire OC come il prodotto proiettivo di OA e OB e scrivere anche in questo caso $OC = OA{\cdot}OB$. Viceversa, dato C, il punto B, che permette di ottenere l'operazione inversa $OB = OC/OA$, è definito dalle equazioni:

$$B = (O\vee\infty)\wedge(R\vee Q), \text{ dove } R = (O\vee P)\wedge(C\vee S), \ Q = (\infty\vee S)\wedge(I\vee P). \qquad (**)$$

È perciò ben definita anche la divisione proiettiva (tranne, naturalmente, quella per zero).

Nonostante il fatto che la costruzione geometrica di Talete e la sua generalizzazione proiettiva siano commutative rispetto allo scambio di A con B, i sistemi di equazioni (*) e (**) *non sono formalmente invarianti* per scambio di A con B e nello stesso tempo di P con Q. Così, in linea di principio, non rimane esclusa la possibilità che la moltiplicazione proiettiva sia *non commutativa*. Si può tuttavia dimostrare che la moltiplicazione proiettiva è distributiva rispetto all'addizione proiettiva. Questa dimostrazione riesce più facile utilizzando prima le costruzioni di Talete e poi applicando delle trasformazioni prospettiche.

8. I campi numerici *R*, *C* e *Q*

Le costruzioni geometriche di Talete richiedono riga e squadra, ma per eseguire le operazioni $\vee$, $\wedge$ proiettive illustrate nei paragrafi precedenti basta la riga. Entrambi i metodi permettono di implementare il calcolo *aritmetico* sui punti di una retta dove tre punti distinti arbitrari giocano il ruolo di 0, 1 e ∞. Si ottengono in questo modo le rappresentazioni proiettive del *campo numerico reale* ***R***.

Con maggiore generalità, una retta proiettiva può riguardarsi in astratto come un *campo* ***F*** di entità numeriche nel quale sono definite un'*addizione* associativa e commutativa e una *moltiplicazione* associativa, distributiva rispetto l'addizione, ma generalmente non commutativa. ***F*** deve inoltre contenere i punti 0, 1, ∞ in modo da assicurare che le operazioni siano invertibili e che esistono multipli infiniti di ogni numero. Applicando le addizioni e le loro inverse ai numeri 0 e 1 possiamo generare tutti gli interi; applicando le moltiplicazioni e le loro inverse agli interi possiamo generare tutti i razionali; i numeri reali possono essere definiti mediante sequenze infinite di numeri razionali. Pertanto, ogni possibile campo numerico deve contenere i reali come sottocampo.


Frobenius

Ci si chiede se siano concepibili campi numerici più generali di quello reale. La risposta è che esistono solo altri due campi numerici: quello dei *numeri complessi* ***C*** e quello dei *quaternioni* ***Q***. Il fatto che i numeri complessi formino un campo è abbastanza evidente. L'esistenza del campo quaternionico è meno banale, e lo è ancor meno che non ne esistano altri. Questo notevole fatto fu dimostrato da Ferdinand Georg Frobenius (1849-1917) nella seconda metà dell'800 mediante l'algebra delle matrici, come è brevemente descritto nel seguente paragrafo.

9. La dimostrazione di Frobenius

Le proprietà associative dell'addizione e della moltiplicazione, e quella distributiva della seconda rispetto la prima, permettono di fornire rappresentazioni fedeli dei numeri ***F*** mediante matrici. Per semplicità, assumeremo che le matrici siano definite nel campo complesso (anche se la dimostrazione può ottenersi usando solo matrici reali). Assumeremo inoltre che le matrici operino transitivamente sui vettori di uno spazio finito (cioè che la rappresentazione sia irriducibile). Nel seguito chiameremo numeri del campo le matrici stesse. Identificheremo con 0 la matrice nulla, con 1 la matrice identica M_0 e con ∞ il multiplo infinito di M_0. Se M_1, M_2, M_3, … sono numeri di ***F***, allora, poiché ***F*** contiene ***R***, ogni combinazione lineare *a coefficienti reali* di M_1, M_2, M_3,… e di M_0=1 è un numero di ***F***. Diremo che gli $n + 1$ numeri 1, $M_1, M_2, M_3,\ldots,M_n$ sono linearmente indipendenti se non si possono trovare $n + 1$ numeri reali $a_0, a_1,\ldots, a_n$ in modo da aversi $a_0 + a_1M_1 +\ldots+ a_nM_n = 0$.

Diremo che ***F*** ha dimensione N+1 se non si possono trovare più di N+1 numeri linearmente indipendenti. In tal caso 1, $M_1,\ldots, M_N$ sarà chiamata un base di ***F***. Dimostriamo i seguente teoremi:

Teorema 1. *Ogni matrice* $M\in \boldsymbol{F}$ *soddisfa ad un'equazione dei secondo grado del tipo* $(M-a)^2+b^2=0$*, dove a e b sono numeri reali. Pertanto M possiede o un solo autovalore (generalmente non reale) oppure due autovalori complessi coniugati.*

Questo teorema segue dal fatto che M, essendo invertibile, è necessariamente quadrata con determinante $|M|$ diverso da zero. Ciò significa che nessuna matrice non nulla di ***F*** può avere zero come autovalore, oppure, ciò che è lo stesso, se M ha un autovalore nullo allora $M = 0$. Supponiamo ora che $a+ib$, con a e b reali, sia un autovalore non nullo di M. Allora $M-a$ possiede ib come autovalore e $(M-a)^2 + b^2$ possiede un autovalore nullo. Ne segue $(M-a)^2 + b^2 = 0$. Questo è possibile solo se M possiede, al più, gli autovalori $a+ib$ e $a-ib$ (o solo uno di essi).

È chiaro che se la base 1, $M_1,\ldots, M_N$ possiede autovalori 1, $a_1 \pm ib_1$, ..., $a_n \pm ib_n$ allora, posto $V_i= (M_i-a_i)/b_i$, anche le matrici 1, $V_1,\ldots,V_N$ formano una base di ***F*** e inoltre $V_i^2 = -1$. Chiameremo 1 e V_i un sistema di unità di ***F***.

Teorema 2. *Sia* 1 *e* V_i *un sistema di unità di* ***F***. *Allora, se* N=1, *si può porre* $V=V_1 = \pm\, i$. *Se invece è* $N > 1$ *si ha* $ViVj \neq VjVi$, *in altri termini se* ***F*** *possiede più di due unità la moltiplicazione non è commutativa.*

Chiaramente, se $N = 1$, le sole rappresentazioni irriducibili di V sono matrici 1×1, precisamente i o $-i$.

Se invece $N > 1$, da $(V_i+V_j)(V_i-V_j)= -1+1+ (V_iV_j-V_jV_i)$ segue che V_i, V_j non commutano, altrimenti sarebbe $V_i=V_j$.

Teorema 3. *Si può trovare una base* $1, U_1,\dots,U_N$ *in modo che* $U_iU_j + U_jU_i = -2\delta_{ij}$, $i, j = 1,\dots, N$, *dove* δ_{ij} *è la delta di Kronecker.*

Sia $N > 1$ e V_1, V_2 due unità di $\boldsymbol{F}$. Allora esistono quattro numeri reali a, b, c, d tali che $(V_1V_2-a)^2+b^2=0$ e $(V_2V_1-c)^2+d^2=0$, vale a dire

$$V_1V_2\,V_1V_2 -2aV_1V_2 + a^2+b^2 = 0 \quad \text{e} \quad V_2V_1\,V_2V_1 -2cV_2V_1 + c^2+d^2 = 0.$$

Moltiplicando la prima a sinistra per V_1 e a destra per V_2, e la seconda a sinistra per V_2 e a destra per V_1, si ottengono le equazioni $V_2\,V_1 - 2a + (a^2+b^2\,)V_1V_2 = 0$, $\quad V_1\,V_2 -2c + (c^2+d^2)V_2\,V_1 = 0$, dalle quali si ricava $a^2+b^2 = c^2+d^2 = 1$, $a = c$. È dunque chiaro che nel caso generale potremo scrivere

$$V_iV_j + V_jV_i = -2g_{ij} = -2g_{ij}\,,\; i, j = 1,\dots,N, \text{ dove } g_{ii} = 1.$$

Dunque la matrice G di elementi g_{ij} ha le caratteristiche di un tensore metrico definito positivo. Potremo pertanto eseguire una rotazione dello spazio mediante una matrice ortogonale R, che come è noto possiede coefficienti R_{ij} reali, in modo da aversi $RGR^{-1} = D$, dove D è una matrice diagonale con elementi diagonali $D_i > 0$. È chiaro allora che gli elementi di $\boldsymbol{F}$ definiti dalle equazioni

$$U_i = \frac{1}{\sqrt{D_i}}\sum_j R_{ij}V_j\,,$$

che chiameremo *unità immaginarie*, soddisfano alle relazioni di *anticommutazione* $U_iU_j + U_jU_i = -2\delta_{ij}$.

Teorema 4. *Non esiste alcun campo numerico con due unità immaginarie o con più di tre unità immaginarie.*

Si supponga, per assurdo, che U_1 e U_2 siano le unità immaginarie di un campo numerico con $N = 3$. Sarà allora $U_1^2 = U_2^2 = -1$, $\quad U_1\,U_2 = -U_1\,U_2$. Con tutta generalità possiamo scrivere $U_1U_2 = a_0+a_1U_1+a_2U_2$, dove a_0, a_1, a_2 sono numeri reali. Moltiplicando questa relazione a destra per U_1 otteniamo $-U_2 = a_0U_1 - a_1+ a_2U_1U_2$. Dovrà pertanto valere l'equazione $a_0a_2+a_1a_2U_1+a_2^2U_2 = a_1- a_0U_1 - U_2$, che nel campo reale ammette soltanto la soluzione $a_0 = a_1 = a_2 = 0$. Si conclude che non può essere $N = 3$.

Si supponga ora che sia $N > 3$. Dalle relazioni di anticommutazione otteniamo $U_1U_2U_k = -U_2U_1U_k = U_2U_kU_1$ per $k = 3, \dots, N$. In altri termini, U_2U_k commuta con U_1 e potremo pertanto scrivere $U_2U_k = a_k+b_kU_1$. D'altronde $(U_2U_k\,)^2 = U_2U_k\,U_2U_k = -\,U_2U_k\,U_kU_2 = -1$, dalla quale si deduce $a_k = 0$, $b_k = \pm 1$. Possiamo allora porre senza perdita di generalità $U_2U_k = U_1$. Chiaramente queste relazioni implicano $U_k = \pm U_3$ per $k = 4, \dots, N$. Ponendo $U_1 = \boldsymbol{i}$, $U_2 = \boldsymbol{j}$, $U_3 = \boldsymbol{k}$ avremo $\boldsymbol{i}^{\,2} = \boldsymbol{j}^{\,2} = \boldsymbol{k}^{\,2} = \boldsymbol{ijk} = -1$. Potremo pertanto scrivere i numeri di questo campo quadridimensionale, che per questa ragione è detto dei *quaternioni*, nella forma scritta per la prima volta da Hamilton $\boldsymbol{q} = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$.

Hamilton

Una rappresentazione matriciale dello stesso quaternione è data da

$$\mathbf{q} = \begin{pmatrix} a+ib, -c+ib \\ c-ib, \ a-ib \end{pmatrix} .$$

In un ponte di Dublino: *Here as he walked by the 16th October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication* $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$ *& cut it on a stone of this bridge.* (Qui passeggiando il 16 ottobre 1843 Sir William Rowan Hamilton in un lampo di genio scoprì la formula fondamentale della moltiplicazione dei quaternioni $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$ e l'incise su una pietra di questo ponte.

Padova 28 ottobre 2006. Ultima revisione 30 settembre 2009.

Bibliografia

1. Birkhoff, G. and von Neumann, J., The Logic of Quantum Mechanics. *Annals of Mathematics*, 37:827-843 (1936).
2. Cartan, E., Nombres Complexes, in *Oevres Complètes*, Partie II, Vol.1, Gauthier-Villars, Paris (1953).
3. Erodoto - *Le Storie*, *Libro I.* Ed. Mondadori, Milano (2000).
4. Frobenius, F.G., Über lineare Substitutionen und bilineare Formen, *J. Reine Angew. Math.*, 84:1-63 (1878).
5. Gigli, D., Aritmetica generale, *Enciclopedia delle Matematiche Elementari*, Vol.I, P.te I, pp. 81 e seg. Hoepli Ed., Milano (1930).
6. Hamilton, W. R., On Quaternions, *Proceedings of the Royal Irish Academy*, 9:1-16 (1847).
7. Veblen, O. and J.W.Young, *Projective Geometry*, *Vol.I*, Ginn & Co. ED., New York (1910).