Gruppi di Matrici

Roberto Catenacci e Diego Giovannini.

Versione del 9 Aprile 2004

Argomenti di Teoria dei Gruppi di Matrici svolti nel corso di Teoria dei Gruppi e utilizzati, in parte, per il corso di Fisica Matematica 1.

Indice

1 Gruppi di Matrici

In questa sezione iniziamo lo studio dei principali gruppi di matrici (reali o complesse), come introduzione alla teoria dei gruppi di Lie; daremo per noti i principali risultati di algebra lineare utilizzati. Indichiamo con $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$ rispettivamente gli insiemi delle matrici $n \times n$ reali o complesse (se non importa indicare esplicitamente il campo di numeri considerato, useremo semplicemente il simbolo M_n). E' noto che $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$ sono spazi vettoriali *reali* di dimensione n^2 e $2n^2$ rispettivamente; è noto anche che su $M_n(\mathbb{R})$ e $M_n(\mathbb{C})$ si può definire un *prodotto,* il cosiddetto *prodotto righe* $\times$ *colonne*: se $A, B \in M_n$ con elementi $A_{ij}, B_{ij,}$ allora:

$$(AB)_{ij} = \sum_{k=1}^{k=n} A_{ik} B_{kj}$$

La matrice prodotto $C = AB$ è ancora $\in M_n$. Ricordiamo anche che una matrice $A \in M_n$ è *invertibile* se e solo se $\det(A) \neq 0$ e, in questo caso, $\exists$ una *unica* matrice A^{-1} tale che $AA^{-1} = A^{-1}A = I$ (dove I è una matrice con elementi $I_{ij} = 1$ se $i = j$ e $I_{ij} = 0$ se $i \neq j$). Ricordando le seguenti proprietà del determinante:

$$\det(AB) = \det A \det B \text{ e } \det(A)^{-1} = (\det A)^{-1},$$

possiamo ora dare le seguenti definizioni:

Definizione 1.1 *Il gruppo* ***generale lineare reale****, denotato con* $GL(n, \mathbb{R})$ *è l'insieme delle matrici invertibili* $\in M_n(\mathbb{R})$ *con il prodotto righe* $\times$ *colonne. Il gruppo* ***speciale lineare reale****, denotato con* $SL(n, \mathbb{R})$ *è il sottogruppo delle matrici* $A \in GL(n, \mathbb{R})$ *tali che* $\det A = 1$.

Definizione 1.2 *Il gruppo* ***generale lineare complesso****, denotato con* $GL(n, \mathbb{C})$ *è l'insieme delle matrici invertibili* $\in M_n(\mathbb{C})$ *con il prodotto righe* $\times$ *colonne. Il gruppo* ***speciale lineare complesso****, denotato con* $SL(n, \mathbb{C})$ *è il sottogruppo delle matrici* $A \in GL(n, \mathbb{C})$ *tali che* $\det A = 1$.

Teorema 1.1 *I gruppi speciali lineari sono sottogruppi normali dei gruppi generali lineari, inoltre:* $GL(n, \mathbb{R})/SL(n, \mathbb{R}) = \mathbb{R}^*$ *(e analoga per* $\mathbb{C}$*).*

Prova. La dimostrazione è identica per il caso reale e complesso. Dalle proprietà del determinante segue che l'applicazione $\det : GL(n, \mathbb{R}) \to \mathbb{R}^*$ è un omomorfismo suriettivo di nucleo $Ker(\det) = SL(n, \mathbb{R})$. Dal fatto che il nucleo di un omomorfismo è un sottogruppo normale e dal teorema di isomorfismo segue l'asserto. ■

Descriveremo ora alcuni casi particolari per piccoli n.

Esempio 1.1 $GL(1, \mathbb{R}) = R^*$ *e* $GL(1, \mathbb{C}) = \mathbb{C}^*$.

Esempio 1.2 $GL(1, \mathbb{C})$ *è sottogruppo di* $GL(2, \mathbb{R})$. *Infatti si può definire il seguente* ***omorfismo iniettivo****:*

$$\rho(x + iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

Notare che $\det \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = x^2 + y^2$.

Esempio 1.3 *H^* (il gruppo moltiplicativo dei quaternioni non nulli) è sottogruppo di $GL(2,\mathbb{C})$. Infatti si può definire il seguente **omorfismo iniettivo**:*

$$\rho(x+iy+jz+kt) = \begin{pmatrix} x+iy & -z-it \\ z-it & x-iy \end{pmatrix}$$

Notare che $\det \begin{pmatrix} x+iy & -z-it \\ z-it & x-iy \end{pmatrix} = x^2+y^2+z^2+t^2.$

2 Gruppi Ortogonali e Unitari

Studiamo ora i più importanti sottogruppi dei gruppi generali lineari: i gruppi ortogonali e unitari. E' noto che in $\mathbb{R}^n$ si definisce il *prodotto scalare*:

$$(x,y) = x^t y = \sum_{i=1}^{n} x^i y^i$$

Dove $x = \begin{pmatrix} x^1 \\ x^2 \\ . \\ x^n \end{pmatrix}$, $y = \begin{pmatrix} y^1 \\ y^2 \\ . \\ y^n \end{pmatrix}$ e x^t denota la matrice *trasposta* di x. Analogamente, in $\mathbb{C}^n$ si definisce il *prodotto hermitiano*:

$$(x,y) = x^* y = \sum_{i=1}^{n} \bar{x}^i y^i$$

Dove x^* denota *l'aggiunta* della matrice x, cioè $x^* = \bar{x}^t$.

Lemma 2.1 *Una matrice $A \in GL(n,\mathbb{R})$ tale che $A^{-1} = A^t$ preserva il prodotto scalare: $(Ax,Ay) = (x,y)$ per ogni $x,y \in \mathbb{R}^n$; viceversa, se preserva il prodotto scalare per ogni x,y allora $A^{-1} = A^t$. Una matrice $A \in GL(n,\mathbb{C})$ tale che $A^{-1} = A^* = \bar{A}^t$ preserva il prodotto hermitiano: $(Ax,Ay) = (x,y)$ per ogni $x,y \in \mathbb{C}^n$ e viceversa.*

Prova. La dimostrazione è analoga nei due casi: osserviamo che, dalla definizione di prodotto hermitiano, segue che $(Ax,y) = (x,A^*y)$; si ottiene allora $(Ax,Ay) = (x,A^*Ay) = (x,y)$. Viceversa, se $(Ax,Ay) = (x,y)$ allora $(Ax)^*(Ay) = x^*y$ e quindi, (per le proprietà note dell'aggiunzione) $x^*A^*Ay = x^*y$. Essendo verificata per ogni x e y, deve essere $A^*A = I$. ■

Il lemma 2.1 e le note proprietà dell'aggiunzione:

$$(A^*)^* = A, (AB)^* = B^*A^*, (A^{-1})^* = (A^*)^{-1}, \det A^* = \det A$$

consentono di dare le seguenti definizioni:

Definizione 2.1 ***Il gruppo ortogonale*** *$O(n)$ è il sottogruppo delle matrici di $GL(n,\mathbb{R})$ che preservano il prodotto scalare: $O(n) = \{A \in GL(n,\mathbb{R}) | A^{-1} = A^t\}$.*

Definizione 2.2 ***Il gruppo unitario*** *$U(n)$ è il sottogruppo delle matrici di $GL(n,\mathbb{C})$ che preservano il prodotto hermitiano: $U(n) = \{A \in GL(n,\mathbb{C}) | A^{-1} = A^*\}$.*

Definizione 2.3 ***Il gruppo delle rotazioni*** *(detto anche gruppo speciale ortogonale) $SO(n)$ è dato da $SO(n) = O(n) \cap SL(n,\mathbb{R})$.*

Definizione 2.4 ***Il gruppo speciale unitario*** *$SU(n)$ è dato da $U(n) \cap SL(n,\mathbb{C})$.*

Definizione 2.5 ***La sfera*** $n-1$ ***dimensionale*** *è l'insieme $S^{n-1} = \{x \in \mathbb{R}^n | (x,x) = 1\}$*

Osservazione 2.1 *Dalla relazione $A^*A = I$ segue che se $A \in O(n)$, $\det A = \pm 1$; se $A \in U(n)$, $\det A = z$ con $z\bar{z} = 1$ e quindi $\det A \in S^1$.(Naturalmente non è vero il viceversa).*

Teorema 2.1 *I gruppi speciali ortogonale e unitario sono sottogruppi normali rispettivamente dei gruppi ortogonali e unitari (con lo stesso n). Si ha inoltre:*

$$O(n)/SO(n) = \mathbb{Z}_2 \text{ e } U(n)/SU(n) = S^1$$

In particolare, $O(1) = \mathbb{Z}_2 = S^0$ e $U(1) = S^1$.

Prova. Dalle proprietà del determinante e dall'osservazione 2.1 segue che l'applicazione $\det : O(n) \to \mathbb{Z}_2$ è un omomorfismo suriettivo di nucleo $Ker(\det) = SO(n)$. Dal fatto che il nucleo di un omomorfismo è un sottogruppo normale e dal teorema di isomorfismo segue l'asserto. Per $U(n)$ si procede analogamente. ∎

Osservazione 2.2 *Segue dal teorema precedente che ci sono solo due laterali di $SO(n)$ in $O(n)$: il laterale $SO(n)$ che contiene I e il laterale $O(n) - SO(n)$ che contiene la matrice C tale che $C_{ij} = -1$ e $C_{ij} = \delta_{ij}$ se $i \neq 1$ e $j \neq 1$; per tale matrice, $\det C = -1$. Segue immediatamente che ogni matrice $B \in O(n) - SO(n)$ può essere scritta come $B = AC$ con $A \in SO(n)$ $(A = BC^{-1})$*

Esempio 2.1 *$O(2), SO(2)$ e $U(1)$.*

Una matrice A di $O(2)$ deve verificare:

$$A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} \frac{d}{\det A} & -\frac{b}{\det A} \\ -\frac{c}{\det A} & \frac{a}{\det A} \end{pmatrix} = A^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Si distinguono ora due casi:

i) $\det A = 1$, allora $A \in SO(2)$ e $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ con $a^2 + b^2 = 1$ e quindi possiamo porre $a = \cos\theta, b = \sin\theta$. La matrice A rappresenta una *rotazione* (nel piano cartesiano x, y) in senso antiorario di un angolo θ (cfr. l'esempio **??**). Prendendo l'omomorfismo ρ dell'esempio 1.2 si ottiene $\rho(\cos\theta + i\sin\theta) = A$; è anche chiaro che, in questo caso, ρ è suriettivo, e quindi si ha un isomorfismo:

$$SO(2) = U(1) = S^1$$

ii) $\det A = -1$, allora $A \in O(2) - SO(2)$ e $A = \begin{pmatrix} -a & -b \\ -b & a \end{pmatrix}$ con $a^2 + b^2 = 1$ e quindi possiamo porre $a = \cos\theta, b = \sin\theta$. Si ottiene

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

La matrice $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ rappresenta una riflessione (nel piano cartesiano x, y) rispetto all'asse delle y e la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ una rotazione di angolo θ. Segue che ogni $A \in O(2) - SO(2)$ rappresenta una *riflessione* nel piano x, y rispetto a una retta passante per l'origine. Si noti che la composizione di due riflessioni risulta sempre essere una rotazione (il determinante vale 1).

Esempio 2.2 $SU(2) = S^3 = Sp(1)$ *(il gruppo moltiplicativo dei quaternioni di norma* 1*).*

Le matrici di $SU(2)$ devono verificare la relazione:

$$A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = A^* = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$$

Segue che una matrice di $SU(2)$ si può scrivere:

$$A = \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix} \text{ con } a\bar{a} + b\bar{b} = 1$$

Se poniamo $a = x + iy$ e $b = z + it$ si ottiene che $(x, y, z, t) \in S^3$. La sfera S^3 può essere identificata col gruppo dei quaternioni di norma uno: $Sp(1) = \{q \in \mathbb{H} | q\bar{q} = 1\}$. E' facile verificare che l'immagine dell'omomorfismo ρ dell'esempio 1.3 è proprio $SU(2)$. Infatti, posto $q = x + iy + jz + kt$ si ottiene $\rho(q)(\rho(q))^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Per la suriettività basta ricordare la rappresentazione trovata sopra delle matrici di $SU(2)$ e osservare che $\rho(x + iy + jz + kt) = \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix}$. Si conclude osservando che un omomorfismo iniettivo è un isomorfismo sulla sua immagine.

Osservazione 2.3 S^0, S^1 *e* S^3 *sono le* ***uniche*** *sfere a cui si può dare una struttura di gruppo.*

3 Spazio tangente all'identità

Iniziamo in questa sezione lo studio delle proprietà geometriche e topologiche dei gruppi ortogonali e unitari.

Definizione 3.1 *Sia* V *uno spazio vettoriale* ***reale*** *di dimensione finita, una curva in* V *è una funzione differenziabile* $\gamma : (a, b) \to V$*, dove* $(a, b) \subset \mathbb{R}$ *è un intervallo aperto contenente* 0*.*

Definizione 3.2 *Sia $u = \gamma(c)$ con $c \in (a,b)$. Un vettore v tangente in u a V è $v = \lim_{h\to 0} \frac{\gamma(c+h)-\gamma(c)}{h}$*

Se $(e_1, e_2, ..., e_n)$ è una base di V, si ottiene subito che $v = \gamma'(c) = (\gamma_1'(c)...\gamma_n'(c))$. Come V considereremo d'ora in avanti M_n.

Definizione 3.3 *Sia G un sottogruppo di $GL(n,\mathbb{R})$ (o $GL(n,\mathbb{C})$). Una curva in G passante per l'identità è una curva in $GL(n,\mathbb{R})$ (o $GL(n,\mathbb{C})$ tale che, $\forall c \in (a,b), \gamma(c) \in G$ e $\gamma(0) = I$.*

Definizione 3.4 *Siano α e β due curve in G passanti per l'identità, la curva prodotto è la curva (in G e passante per l'identità) $\eta(c) = (\alpha\beta)(c) = \alpha(c)\beta(c)$*

Osservazione 3.1 *Si ottiene subito (facendo attenzione all'ordine in cui si moltiplicano gli elementi di G):*

$$(\alpha\beta)'(c) = \alpha(c)\beta'(c) + \alpha'(c)\beta(c)$$

Definizione 3.5 *Lo spazio tangente a G nell'identità è l'insieme $T(G) = \{v \in M_n | v = \gamma'(0)\}$, essendo γ una curva in G passante per l'identità.*

Lemma 3.1 *$T(G)$ è un sottospazio vettoriale di M_n.*

Prova. Siano $\alpha'(0), \beta'(0) \in T(G)$, allora

$$(\alpha\beta)'(0) = \alpha(0)\beta'(0) + \alpha'(0)\beta(0) = \alpha'(0) + \beta'(0)$$

e quindi, dato che $(\alpha\beta)'(0) \in T(G)$ per la definizione di curva prodotto, anche $\alpha'(0) + \beta'(0) \in T(G)$. Sia ora $\alpha'(0) \in T(G)$ e sia u un numero reale; posto $\sigma(t) = \alpha(ut)$ si trova immediatamente che σ è una curva in G passante per l'identità e che $\sigma'(0) = u\gamma'(0)$ e quindi $u\gamma'(0) \in T(G)$. ■

Esempio 3.1 *$T(GL(1,\mathbb{C})) = \mathbb{C} = \mathbb{R}^2$, $T(GL(2,\mathbb{R})) = M_2(\mathbb{R}) = \mathbb{R}^4$. Basta infatti osservare che i valori delle derivate in zero di funzioni reali sono arbitrari numeri reali.*

Esempio 3.2 *$T(SO(2)) = \mathbb{R}$. Sia (vedi esempio 2.1)*

$$\alpha(t) = \begin{pmatrix} \cos f(t) & -\sin f(t) \\ \sin f(t) & \cos f(t) \end{pmatrix} \quad \textit{con } f(0) = 0$$

una curva in $SO(2)$ passante per I. Essendo $f'(0)$ un arbitrario numero reale, si vede subito che:

$$T(SO(2)) = \{\textit{matrici } 2 \times 2 \textit{ di tipo } \alpha'(0)\} = \left\{ \begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}, a \in \mathbb{R} \right\}$$

E quindi $T(SO(2))$ è, come spazio vettoriale reale, isomorfo a $\mathbb{R}$. Il lettore farebbe bene a verificare in tutti i dettagli che $\left\{ \begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}, a \in \mathbb{R} \right\}$ è uno spazio vettoriale reale di dimensione 1.

Definizione 3.6 *La dimensione di* G *(*$\dim(G)$*) è la dimensione di* $T(G)$ *come spazio vettoriale* ***reale****.*

Definizione 3.7 *Un omomorfismo differenziabile* $\varphi : H \to G$ *è un omomorfismo tale che* $\beta(t) = \varphi(\alpha(t)) = (\varphi \circ \alpha)(t)$ *è una curva in* G *per ogni* α *curva in* H.

Osservazione 3.2 *Si noti che se* α *passa per l'identità di* H *necessariamente* $(\varphi \circ \alpha)$ *passa per l'identità di* G *in virtù del fatto che un omomorfismo manda l'identità nell'identità. Il punto chiave della definizione è la differenziabilità della funzione composta. Tutti gli omomorfismi considerati in questa sezione sono differenziabili perchè si ottengono da prodotti e somme tra numeri reali, numeri complessi (visti come coppie di numeri reali) e quaternioni (visti come quaterne di numeri reali).*

Definizione 3.8 *Il differenziale* $d\varphi$ *di un omomorfismo differenziabile è l'applicazione* $d\varphi : T(H) \to T(G)$*:*

$$d\varphi(\alpha'(0)) = \beta'(0) = (\varphi \circ \alpha)'(0)$$

In particolare, il differenziale dell'omomorfismo identità è l'applicazione identità tra $T(H)$ e $T(G)$.

Esempio 3.3 *Consideriamo il caso dell'omomorfismo* ρ *dell'esempio 1.2. Sia* $\alpha(t) = x(t) + iy(t)$ *una curva in* $GL(1, \mathbb{C})$ *passante per* I*. Si ottiene subito che*

$$(\rho \circ \alpha)(t) = \begin{pmatrix} x(t) & -y(t) \\ y(t) & x(t) \end{pmatrix}$$

e quindi:

$$(\rho \circ \alpha)'(0) = \begin{pmatrix} x'(0) & -y'(0) \\ y'(0) & x'(0) \end{pmatrix}$$

Ora $x'(0)$ *e* $y'(0)$ *sono due arbitrari numeri reali, diciamo* a *e* b; *risulta quindi dalla definizione 3.8 e dall'esempio 3.1 che* $d\rho : \mathbb{R}^2 \to M_2(\mathbb{R})$

$$d\rho : \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2 \to \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R})$$

Si osservi che $d\rho$ *è una applicazione lineare iniettiva di rango* 2, *la sua immagine è il sottospazio bidimensionale di* $M_2(\mathbb{R})$ *generato da* $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *e* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Esempio 3.4 *Se restringiamo* ρ *alle matrici di* $U(1)$ *cioè ai numeri complessi di norma* 1, $x'(0)$ *non può più essere arbitrario. Infatti, se* $x(t)^2 + y(t)^2 = 1$ *si ottiene*

$$2x(t)x'(t) + 2y(t)y'(t) = 0,$$

ma $x(0) + iy(0) = 1$ *e quindi deve essere* $x'(0) = 0$. *Ne segue che:*

$$d\rho : b \in \mathbb{R} \to \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix} \in T(SO(2)) \subset M_2(\mathbb{R})$$

In altri termini (vedi l'esempio 3.2), $d\rho$ *è un* ***isomorfismo di spazi vettoriali reali*** *tra* $T(U(1))$ *e* $T(SO(2))$*. Sappiamo anche (vedi l'esempio 2.1) che* ρ *è un* ***isomorfismo di gruppi*** *tra* $U(1)$ *e* $SO(2)$*. La situazione descritta in questo esempio si generalizza nel seguente lemma:*

Lemma 3.2 *Il differenziale* $d\varphi$ *di un omomorfismo differenziabile* φ *è una applicazione lineare. Se* φ *è un isomorfismo di gruppi* $H \to G$*, allora* $d\varphi$ *è un isomorfismo di spazi vettoriali reali* $T(H) \to T(G)$*.*

Prova. Diamo solo un accenno di dimostrazione, sorvolando su alcuni particolari di carattere analitico. Siano $\alpha'(0), \gamma'(0) \in T(H)$, e a, b numeri reali; allora:

$$d\varphi(a\alpha'(0) + b\gamma'(0)) = [\varphi \circ (a\alpha + b\gamma)]'(0) = \{[\varphi \circ a\alpha]' + [\varphi \circ b\gamma)]'\}(0)$$

Osserviamo ora che, dalla definizione di differenziale, si ha proprio:

$$ad\varphi(\alpha'(0)) + bd\varphi(\gamma'(0)) = a[\varphi \circ \alpha]'(0) + b[\varphi \circ \gamma]'(0) = \{[\varphi \circ a\alpha]' + [\varphi \circ b\gamma)]'\}(0)$$

e quindi la linearità è provata.

La seconda parte segue dal fatto che la composizione di funzioni differenziabili è differenziabile e dalla regola di Leibniz. Se φ e ψ sono omomorfismi differenziabili

$$H \xrightarrow{\psi} G \xrightarrow{\varphi} K$$

anche $\varphi \circ \psi$ lo è e, inoltre, si verifica che $d(\varphi \circ \psi) = d\varphi \circ d\psi$. Se φ è un isomorfismo differenziabile, anche φ^{-1} lo è e quindi segue che:

$$d(\varphi \circ \varphi^{-1}) = d(Id) = Id = d\varphi \circ d\varphi^{-1}.$$

Analogamente:

$$d(\varphi^{-1} \circ \varphi) = d(Id) = Id = d\varphi^{-1} \circ d\varphi.$$

Dove abbiamo indicato con Id l'applicazione identità. Ne consegue che $(d\varphi)^{-1} = d\varphi^{-1}$ e quindi $d\varphi$ è una applicazione lineare invertibile e quindi un isomorfismo. ■

Teorema 3.1 *Due gruppi differenziabilmente isomorfi hanno la stessa dimensione.*

Prova. Segue banalmente dal lemma 3.2. ■

Teorema 3.2

$$\dim(SO(2)) = \dim(U(1)) = \dim(S^1) = 1$$

e

$$\dim(SU(2)) = \dim(S^3) = 3.$$

(questo enunciato suggerisce che debba esistere una definizione di dimensione (applicabile anche alle sfere che non sono gruppi) per cui $\dim(S^n) = n$*)*

Prova. Abbiamo già visto nell'esempio 3.4 che $\dim(SO(2)) = \dim(U(1)) = 1$. Ne vediamo ora un'altra dimostrazione: $SO(2), U(1)$ e S^1 sono differenziabilmente isomorfi (vedi l'esempio 2.1 ed il teorema 2.1) e quindi, (vedi teorema 3.1), possiamo calcolare solo $\dim(S^1)$. Sia ora $\gamma(t) = e^{if(t)}$ con $f(t)$ reale, differenziabile e tale che $f(0) = 0$ una curva in S^1 passante per 1. Si ha $T(S^1) = \{\gamma'(0) = if'(0)|\}$. Essendo ogni numero reale a la derivata in 0 della funzione (reale, differenziabile e passante per 0) $f(t) = at$ segue che $T(S^1)$ è tutto l'asse immaginario e quindi è isomorfo, come spazio vettoriale reale, a $\mathbb{R}$. Dimostriamo ora la seconda parte. $SU(2), S^3$ e $Sp(1)$ sono differenziabilmente isomorfi (vedi esempio 2.2). Sia ora $\gamma(t) = x(t) + y(t)i + z(t)j + w(t)k$ con $x(t)^2 + y(t)^2 + z(t)^2 + w(t)^2 = 1$ e $x(0) = 1$, $y(0) = z(0) = w(0) = 0$ una curva passante per l'identità in $Sp(1)$. Si nota che in $x(0) = 1$ la funzione $x(t)$ ha un massimo e quindi $x'(0) = 0$ (vedi anche l'esempio 3.4). Ne segue che $\gamma'(0) = y'(0)i + z'(0)j + w'(0)k$. Allora $T(Sp(1)) = \{\gamma'(0)|\gamma(0) = 1\} \subset \mathbb{R}^3$ (dove $\mathbb{R}^3$ è visto come lo spazio vettoriale reale generato da i, j, k). Viceversa, $\mathbb{R}^3 \subset T(Sp(1)) = \{\gamma'(0)|\gamma(0) = 1\}$ perchè, per ogni a, b, c reali, basta considerare la curva (in $Sp(1)$,con dominio di definizione un piccolo intervallo attorno a 0 dipendente da a, b, c in modo che $1 - a^2t^2 - b^2t^2 - c^2t^2 > 0$, differenziabile e passante per 1):

$$\gamma(t) = \sqrt{1 - a^2t^2 - b^2t^2 - c^2t^2} + ati + btj + ctk$$

e si ottiene proprio $ai + bj + ck = \gamma'(0)$. ■

Il seguente teorema fornisce un'altra giustificazione per l'uso del termine *dimensione* nella definizione 3.6.

Teorema 3.3 $\dim GL(n, \mathbb{R}) = n^2$ *e* $\dim GL(n, \mathbb{C}) = 2n^2$

Prova. Siccome (come spazi vettoriali reali) $\dim M_n(\mathbb{R}) = n^2$ e $\dim M_n(\mathbb{C}) = 2n^2$, basta dimostrare che ogni matrice di M_n può essere vista come la derivata in 0 di una curva in $GL(n, \mathbb{R})$ (oppure $GL(n, \mathbb{C})$) passante per l'identità. Sia allora $v \in M_n$ e si consideri, in un intervallo contenente lo zero, la curva $\sigma : (a, b) \to M_n$ definita da $\sigma(t) = tv + I$. Tale curva verifica $\sigma(0) = I$ e $\sigma'(0) = v$. Il determinante è una funzione continua (si calcola solo con somme e prodotti) e quindi prendendo l'intervallo di definizione di σ abbastanza piccolo, possiamo essere certi che $\det \sigma(t) \neq 0$ in quanto $\det \sigma(0) = 1$. In altre parole una matrice che differisce di poco dall'identità è invertibile. Ci si può convincere di ciò anche dimostrando la formula seguente (ad esempio nel caso semplice di $M_2(\mathbb{R})$):

$$\det(I + \varepsilon A) = 1 + \varepsilon tr(A) + O(\varepsilon^2)$$

Si ricorda che $tr(A)$ è la traccia della matrice A cioè la somma degli elementi presenti sulla diagonale principale. ■

La dimostrazione del teorema 3.2, tutta basata su calcoli e costruzioni *ad hoc* non è per niente illuminante sulla struttura degli spazi tangenti, ma, a questo punto della trattazione non era forse possibile fare di meglio...

Definizione 3.9 *Una matrice* $A \in M_n(\mathbb{R})$ *è detta antisimmetrica se* $A + A^t = 0$ *(dove* 0 *è la matrice con tutti gli elementi nulli.*

Definizione 3.10 *Una matrice $A \in M_n(\mathbb{C})$ è detta antihermitiana se $A + A^* = 0$.*

Definizione 3.11 $so(n) = \{A \in M_n(\mathbb{R}) | A + A^t = 0\}$ *(notare che risulta sempre $tr(A) = 0$)*

Definizione 3.12 $u(n) = \{A \in M_n(\mathbb{C}) | A + A^* = 0\}$

Definizione 3.13 $su(n) = \{A \in M_n(\mathbb{C}) | A + A^* = 0$ ***e*** $tr(A) = 0\}$

Lemma 3.3 *$so(n)$ è un sottospazio vettoriale di $M_n(\mathbb{R})$ di dimensione $\frac{n(n-1)}{2}$.*

Prova. Se $A, B \in so(n)$ segue che $(A + B) + (A + B)^t = (A + A^t) + (B + B^t) = 0$. Se $a \in \mathbb{R}$ e $A \in so(n)$ segue che $aA + (aA)^t = a(A + A^t) = 0$. Per il calcolo della dimensione, basta osservare che ogni matrice antisimmetrica ha la diagonale tutta nulla e che gli elementi sotto la diagonale sono gli opposti di quelli sopra la diagonale (infatti $A + A^t = 0$ implica che $A_{ij} = -A_{ji}$ e $A_{ii} = 0$). Gli elementi indipendenti di una matrice con diagonale tutta nulla sono $n^2 - n$, di cui $\frac{n^2-n}{2}$ stanno sopra la diagonale e $\frac{n^2-n}{2}$ sotto. L'osservazione precedente mostra però che in una matrice antisimmetrica gli elementi sopra la diagonale determinano anche quelli sotto la diagonale e quindi ne restano solo $\frac{n^2-n}{2}$ indipendenti. ∎

Lemma 3.4 *$u(n)$ è un sottospazio vettoriale* ***reale*** *di $M_n(\mathbb{C})$ di dimensione n^2 e $su(n)$ è un sottospazio vettoriale* ***reale*** *di $M_n(\mathbb{C})$ di dimensione $n^2 - 1$.*

Prova. Se $A, B \in u(n)$ segue che $(A + B) + (A + B)^* = (A + A^*) + (B + B^*) = 0$. Se $a \in \mathbb{R}$ e $A \in u(n)$ segue che $aA + (aA)^* = aA + \bar{a}A^* = a(A + A^*) = 0$ (Notare che $u(n)$ **non** è uno spazio vettoriale su $\mathbb{C}$, perchè se $a \in \mathbb{C} - \mathbb{R}$ si ha $a \neq \bar{a}$). Il caso di $su(n)$ è totalmente analogo essendo la traccia una operazione lineare. Per il calcolo della dimensione, basta osservare che ogni matrice antihermitiana ha la diagonale tutta puramente immaginaria e che gli elementi sotto la diagonale sono gli opposti dei coniugati di quelli sopra la diagonale (infatti $A + A^* = 0$ implica che $A_{ij} = -\bar{A}_{ji}$ e $\bar{A}_{ii} = 0$). Osserviamo ora che gli $n^2 - n$ *numeri complessi* che individuano gli elementi indipendenti di una matrice complessa con diagonale tutta nulla, sono determinati da $2(n^2 - n)$ *numeri reali*, di cui $n^2 - n$ stanno sopra la diagonale e $n^2 - n$ sotto. Sappiamo però che in una matrice antihermitiana gli elementi sopra la diagonale determinano anche quelli sotto la diagonale; agli $n^2 - n$ *numeri reali* rimasti indipendenti vanno però ancora aggiunti gli n *numeri reali* che individuano gli elementi puramente immaginari della diagonale. Nel caso di $su(n)$ la traccia è nulla, e quindi gli elementi puramente immaginari sulla diagonale non sono tutti indipendenti, ma uno tra loro deve essere l'opposto della somma dei rimanenti, e questo fa calare di uno la dimensione reale. ∎

Possiamo ora enunciare un risultato preliminare che però inizia a mostrare l'importanza degli spazi vettoriali sopra definiti che appaiono in modo naturale in molte altre situazioni.

Lemma 3.5

1. *Se γ è una curva passante per l'identità in $O(n)$ oppure in $SO(n)$ allora $\gamma'(0) \in so(n)$.*

2. *Se γ è una curva passante per l'identità in $U(n)$ allora $\gamma'(0) \in u(n)$.*

3. *In particolare,* $\dim O(n) \le \frac{n^2-n}{2}, \dim SO(n) \le \frac{n^2-n}{2}, \dim U(n) \le n^2$,

Prova. In tutti i casi abbiamo $(\gamma\gamma^*)(t) = \gamma(t)\gamma^*(t) = I$, per cui $(\gamma\gamma^*)'(t) = 0$. Dalla osservazione 3.1 si ottiene subito:

$$(\gamma\gamma^*)'(0) = \gamma(0)\gamma^{*\prime}(0) + \gamma'(0)\gamma^*(0) = \gamma^{*\prime}(0) + \gamma'(0) = 0$$

Il punto 3 segue dai lemmi 3.3 e 3.4. ■

Osservazione 3.3 *Si noti che non abbiamo detto nulla su $SU(n)$ (perchè ?)Per dimostrare che le disuguaglianze del punto* 3 *sono, in realtà, uguaglianze e trattare anche il caso di $SU(n)$, avremo bisogno di altri concetti e risultati, la cui importanza va tuttavia molto oltre questo scopo.*

4 Esponenziale e Algebre di Lie

Ad un gruppo di matrici G abbiamo associato, nel paragrafo precedente, uno spazio vettoriale: il suo spazio tangente $T(G)$. In questa parte del corso ci occuperemo di un metodo per costruire un gruppo a partire da uno spazio vettoriale con particolari proprietà.

Definizione 4.1 *Sia $A \in M_n$ l'esponenziale della matrice A è la serie:*

$$e^A = I + A + A^2/2 + A^3/3! + ...$$

La serie va interpretata nel senso che $\forall i, j$ la matrice e^A (quando esiste) ha componenti:

$$\left(e^A\right)_{ij} = I_{ij} + A_{ij} + \left(A^2/2\right)_{ij} + \left(A^3/3!\right)_{ij} + ...$$

Fortunatamente, la matrice e^A **esiste sempre**:

Lemma 4.1 *La serie $e^A = I + A + A^2/2 + A^3/3! + ...$ converge ad un elemento di M_n.*

Prova. Sia $a = \max\{|A_{ij}|\}$. Pensando di sostituire ogni elemento di A con a si ottiene:

$$|A_{ij}| \le a, \left|\left(A^2/2\right)_{ij}\right| \le na^2/2, ..., \left|\left(A^k/k!\right)_{ij}\right| \le n^{k-1}a^k/k!.$$

Essendo n e a numeri fissati, il criterio del rapporto dice che la serie converge in modulo elemento per elemento. ■

Teorema 4.1

1. Se $AB = BA$ allora $e^{A+B} = e^A e^B$.

2. $e^A \in GL(n, \mathbb{R})$.

3. $e^{BAB^{-1}} = Be^AB^{-1}$.

Prova. I punti 1 e 3 sono solo lunghe verifiche. Il punto 2 segue dal punto 1: $I = e^0 = e^{A-A} = e^A e^{-A}$, e quindi e^A è invertibile. ■

Esempio 4.1 *$SO(2) = \{e^A$ con $A \in so(2)\}$. Se $A \in so(2)$ allora $e^A \in SO(2)$. Cioè:*

$$e^{\begin{pmatrix} 0 & -x \\ x & 0 \end{pmatrix}} = \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$$

Basta calcolare $\begin{pmatrix} 0 & -x \\ x & 0 \end{pmatrix}^2 = \begin{pmatrix} -x^2 & 0 \\ 0 & -x^2 \end{pmatrix}$, $\begin{pmatrix} 0 & -x \\ x & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & x^3 \\ -x^3 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & -x \\ x & 0 \end{pmatrix}^4 = \begin{pmatrix} x^4 & 0 \\ 0 & x^4 \end{pmatrix}$, $\begin{pmatrix} 0 & -x \\ x & 0 \end{pmatrix}^5 = \begin{pmatrix} 0 & -x^5 \\ x^5 & 0 \end{pmatrix}$, ... , *applicare la definizione di esponenziale e ricordare gli sviluppi delle funzioni* $\cos x$ *e* $\sin x$. *Si osservi anche che ciò mostra esplicitamente che* ***tutte*** *le matrici di $SO(2)$ (vedi esempio 2.1) si ottengono in questo modo.*

Esempio 4.2 *Se $A \in so(n)$ allora $e^A \in O(n)$. Abbiamo infatti:*

$$I = e^0 = e^{A+A^t} = e^A e^{A^t} = e^A (e^A)^t$$

E' bene notare esplicitamente cosa l'esempio ***non*** *dice;* ***non è vero*** *che ogni matrice ortogonale è esponenziale di una matrice antisimmetrica (infatti l'esempio 4.1 mostra che* $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *non si otterrà mai per esponenziazione).*

Dimostremo ora alcune importanti formule:

Teorema 4.2 *Sia $A(t)$ una curva passante per l'identità in un gruppo di matrici. Allora:*

$$\frac{d}{dt} \det A = \det A \cdot tr(A^{-1} \frac{dA}{dt})$$

Prova. Indichiamo con A_{ij} gli elementi di A, e con a_{ij} i loro complementi algebrici (i determinanti moltiplicati per $(-1)^{i+j}$ del minore ottenuto da A eliminando la riga i e la colonna j). E' noto che: $\forall i$, $\det A = \sum_{j=1}^{j=n} A_{ij} a_{ij}$ e che $(A)^{-1}_{ij} = \frac{a_{ji}}{\det A}$ (notare lo scambio $i \longleftrightarrow j$). Si ottiene quindi: $\frac{\partial \det A}{\partial A_{ij}} = a_{ij} = (A)^{-1}_{ji} \det A$. Allora:

$$\frac{d}{dt} \det A = \sum_{i,j=1}^{i,j=n} \frac{\partial \det A}{\partial A_{ij}} \cdot \frac{dA_{ij}}{dt} = \sum_{i,j=1}^{i,j=n} \det A \cdot (A)^{-1}_{ji} \frac{dA_{ij}}{dt} = \det A \cdot tr(A^{-1} \frac{dA(t)}{dt})$$

■

Lemma 4.2 *Sia $A \in M_n$ e t un numero reale. Allora $\det e^{tA} = 1$ $\forall t$ se e solo se $trA = 0$.*

Prova. Siccome $\frac{d}{dt}e^{tA} = e^{tA}A$, segue dal teorema 4.2 applicato alla curva e^{tA}: (il punto 2 del teorema 4.1 ci assicura che ciò si può fare)

$$\frac{d}{dt}\det e^{tA} = \det e^{tA} \cdot tr(e^{-tA}\frac{de^{tA}}{dt}) = \det e^{tA} \cdot tr(e^{-tA}e^{tA}A) = \det e^{tA} \cdot trA$$

Allora se $trA = 0, \det e^{tA}$ è una costante e, essendo uguale a 1 in $t = 0$, è sempre uguale a 1. Viceversa se $\det e^{tA} = 1$ la stessa formula fornisce $trA = 0$. ■

Teorema 4.3 *Per ogni matrice $A \in M_n$ e per ogni numero reale t si ha:* $\det e^{tA} = e^{t(trA)}$. *In particolare,* $\det e^A = e^{trA}$.

Prova. La formula ricavata per la dimostrazione del lemma 4.2:

$$\frac{d}{dt}\det e^{tA} = \det e^{tA} \cdot trA,$$

può essere interpretata come una equazione differenziale: $\frac{dx}{dt} = trA \cdot x$ con la condizione iniziale $x(0) = 1$. Integrandola si ottiene $x(t) = e^{t(trA)}$, cioè $\det e^{tA} = e^{t(trA)}$ ■

Possiamo ora concludere il calcolo dello spazio tangente ai gruppi ortogonali e unitari.

Lemma 4.3

1. *Se $A \in so(n)$ allora $\gamma(t) = e^{tA}$ è una curva passante per l'identità in $SO(n)$* e $\gamma'(0) = A$.
2. *Se $A \in u(n)$ allora $\gamma(t) = e^{tA}$ è una curva passante per l'identità in $U(n)$ e $\gamma'(0) = A$.*
3. *Se $A \in su(n)$ allora $\gamma(t) = e^{tA}$ è una curva passante per l'identità in $SU(n)$ e $\gamma'(0) = A$.*
4. *In particolare,* $\dim O(n) \geq \frac{n^2-n}{2}, \dim SO(n) \geq \frac{n^2-n}{2}, \dim U(n) \geq n^2, \dim SU(n) \geq n^2 - 1$.

Prova. Chiaramente $\gamma(0) = e^0 = I$ e $\gamma'(0) = \lim_{t\to 0} \frac{e^{tA}-I}{t} = A$. Inoltre:

$$\gamma(t)\gamma(t)^* = e^{tA}e^{tA^*} = e^{t(A+A^*)} = I$$

E quindi $\gamma(t)$ è una curva passante per l'identità in un gruppo ortogonale o unitario. Ricordando inoltre (vedi teorema 4.3) che $\det e^{tA} = e^{t(trA)}$, si trova che nei casi 1 e 3, (dove $trA = 0$), la curva è tutta in $SO(n)$ e $SU(n)$ rispettivamente. ■

Teorema 4.4 *(Le seguenti uguaglianze rappresentano isomorfismi di spazi vettoriali reali).*

1. $T(O(n)) = T(SO(n)) = so(n)$.
2. $T(U(n)) = u(n)$.
3. $T(SU(n)) = su(n)$.
4. *In particolare,* $\dim SO(n) = \dim O(n) = \frac{n(n-1)}{2}, \dim U(n) = n^2$ *e* $\dim SU(n) = n^2 - 1$.

Prova. I lemmi 3.5 e 4.3 forniscono immediatamente i punti 1 e 2. Per il punto 3, si deve prima di tutto osservare che se $\gamma(t)$ è una curva passante per l'identità in $SU(n)$ allora $\gamma'(0) \in su(n)$. Infatti $\det \gamma(t) = 1$ per cui (vedi teorema 4.2): $\frac{d}{dt} \det \gamma = tr(\gamma^{-1} \frac{d\gamma}{dt}) = 0$, e quindi per $t = 0$ si ottiene $tr\gamma'(0) = 0$, e quindi $T(SU(n)) \subset su(n)$ e allora $\dim SU(n) \leq n^2 - 1$. Questo permette di concludere la dimostrazione, perchè per il lemma 4.3 $\dim SU(n) \geq n^2 - 1$. ■

Osservazione 4.1 *Si noti che* $\dim SO(3) = \dim SU(2) = 3$ *($so(3)$ e $su(2)$ sono infatti spazi vettoriali isomorfi). Per quanto ne sappiamo fino ad ora $SO(3)$ e $SU(2)$ potrebbero quindi essere gruppi isomorfi. In realtà non lo sono (hanno il centro diverso) ma questo fatto suggerisce che si debba approfondire lo studio delle relazioni tra i gruppi di matrici e i loro spazi tangenti.*

Osservazione 4.2 *Gli spazi vettoriali reali $so(n)$ e $su(n)$ non sono chiusi rispetto al prodotto righe $\times$ colonne dei loro elementi. Si può tuttavia introdurre in essi una operazione interna, chiamata commutatore, che gode di tutte le proprietà sensate del prodotto salvo l'associatività.*

Definizione 4.2 *Indicando come al solito con $T(G)$ lo spazio tangente di un gruppo ortogonale o unitario G, siano A e B due suoi elementi. Si definisce commutatore di A e B la matrice:*

$$[A, B] = AB - BA$$

Lemma 4.4 *Siano $A, B, C \in T(G)$, il commutatore gode delle seguenti proprietà:*

1. $[A, B] \in T(G)$
2. $[A, B] = -[B, A]$
3. $[A, B + C] = [A, B] + [A, C]$
4. $[A + B, C] = [A, C] + [B, C]$
5. $\forall a \in \mathbb{R}$, $[aA, B] = [A, aB] = a[A, B]$
6. $[A, [B, C]] + [C, [A, B]] + [B, [C, A]] = 0$

Prova. Sono tutte noiose e banali verifiche basate solo sull'uso della definizione. Per il punto 1, nel caso di $su(n)$ occorre anche ricordarsi che, per ogni matrice, $tr(AB) = tr(BA)$. ■

Osservazione 4.3 *la formula del punto 6 è detta* ***identità di Jacobi****, e sostituisce l'associatività per il prodotto $A \circ B = [A, B]$:*

$$A \circ (B \circ C) - (A \circ B) \circ C = (A \circ C) \circ B \text{ e non } = 0$$

Definizione 4.3 *Un qualsiasi spazio vettoriale reale V, dotato di un prodotto interno (denotato con $[\ ,\ ]_V$ anche nel caso astratto in cui lo spazio vettoriale non sia un sottospazio di M_n) che soddisfa le proprietà da 2 a 5 del lemma 4.4 è detto* ***Algebra di Lie.***

Definizione 4.4 *Un omomorfismo di algebre di Lie è una applicazione lineare φ tra i corrispondenti spazi vettoriali:*

$$\varphi : V \to W$$

*che, **inoltre**, verifica:*

$$\varphi[A, B]_V = [\varphi(A), \varphi(B)]_W$$

Osservazione 4.4 *Spazi vettoriali isomorfi possono benissimo non essere isomorfi come Algebre di Lie. In altre parole, non tutti gli isomorfismi di spazi vettoriali sono isomorfismi di Algebre di Lie. (vedi l'esempio 4.4)*

4.1 Algebra del gruppo delle rotazioni in $\mathbb{R}^3$

Esempio 4.3 *$so(3)$ e $su(2)$. Una base dello spazio vettoriale reale $so(3)$ è:*

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

E' facile verificare che la sua struttura di Algebra di Lie è data da:

$$[A_1, A_2] = A_3, [A_2, A_3] = A_1, [A_3, A_1] = A_2.$$

*Una base dello spazio vettoriale **reale** $su(2)$ è:*

$$U_1 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, U_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, U_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

E' facile verificare che la sua struttura di Algebra di Lie è data da:

$$[U_1, U_2] = 2U_3, [U_2, U_3] = 2U_1, [U_3, U_1] = 2U_2.$$

*Un **isomorfismo di Algebre di Lie** (e non solo di spazi vettoriali) è dato da:*

$$\varphi(U_i) = 2A_i.$$

Infatti, ad esempio,

$$\begin{aligned} \varphi[U_1, U_2]_{su(2)} &= \varphi(2U_3) = 2\varphi(U_3) = 4A_3 \\ \varphi[U_3, U_1]_{su(2)} &= \varphi(2U_2) = 2\varphi(U_2) = 4A_2 \\ \varphi[U_2, U_3]_{su(2)} &= \varphi(2U_1) = 2\varphi(U_1) = 4A_1 \end{aligned}$$

ed anche:

$$[\varphi(U_1), \varphi(U_2)]_{so(3)} = [2A_1, 2A_2]_{so(3)} = 4[A_1, A_2]_{so(3)} = 4A_3 \text{ ed analoghe.}$$

Per cui:

$$\varphi[U_i, U_j]_{su(2)} = [\varphi(U_i), \varphi(U_j)]_{so(3)}.$$

Esempio 4.4 ***(Un non esempio)*** *L'isomorfismo ovvio $\varphi(U_i) = A_i$* ***non è*** *un isomorfismo di Algebre di Lie (perchè?).*

Esempio 4.5 *Esponenziale degli elementi della base di $so(3)$ e sottogruppi abeliani di $SO(3)$. Posto (vedi lemma 4.3 ed esempio 4.1):*

$$R_i(t) = e^{tA_i},$$

si verifica facilmente che:

$$R_1(t) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & -\sin t \\ 0 & \sin t & \cos t \end{pmatrix}, R_2(t) = \begin{pmatrix} \cos t & 0 & \sin t \\ 0 & 1 & 0 \\ -\sin t & 0 & \cos t \end{pmatrix}, R_3(t) = \begin{pmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

e che gli $R_i = \{R_i(t), t \in \mathbb{R}\}$ sono sottogruppi ***abeliani*** *di $SO(3)$ (isomorfi a $SO(2)$). Le matrici di R_i operano sui vettori di $\mathbb{R}^3$, rappresentati da $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ come* ***rotazioni in senso antiorario*** *attorno, rispettivamente, R_1 all'asse x, R_2 all'asse y, R_3 all'asse z. E' noto dall'algebra lineare (vedi anche l'esempio 4.7) che per ogni matrice R di $SO(3)$ esiste in $\mathbb{R}^3$ una base ortonormale in cui $R = BAB^{-1}$, con $A \in R_3$ e $B \in O(3)$. Ricordando che $A \in R_3$ significa che $A = e^{tA_3}$ per un certo t, ed il punto 3 del teorema 4.1, si ottiene $R = Be^{tA_3}B^{-1} = e^{tBA_3B^{-1}}$. Essendo $B^{-1} = B^t$ si verifica facilmente che $BA_3B^{-1} \in so(3)$, cioè* ***l'esponenziale è suriettivo:*** *ogni matrice di $SO(3)$ è ottenuta esponenziando una matrice di $so(3)$. Questo fatto importante si generalizza come segue:*

Definizione 4.5 *Sia G un gruppo di matrici, la componente connessa con l'identità, (indicata con G_0) è l'insieme degli elementi di G che possono essere connessi all'identità tramite una curva (differenziabile e contenuta in G). In altre parole, $g \in G_0$ se e solo se esiste una curva γ tale che: $\gamma(t) \in G$, $\gamma(0) = I$, $\gamma(1) = g$.*

Definizione 4.6 *G è connesso se $G_0 = G$.*

Esempio 4.6 *$GL(n,\mathbb{R})$ non è connesso. Il determinante è una applicazione differenziabile e suriettiva da $GL(n,\mathbb{R})$ a $\mathbb{R}^*$, per cui se $GL(n,\mathbb{R})$ fosse connesso, lo sarebbe anche $\mathbb{R}^*$, che però, ovviamente, non lo è. Si ha, evidentemente, $GL_0(n,\mathbb{R}) = \{A | \det A > 0\}$.*

Esempio 4.7 *$SO(3)$ è connesso. (Vedi anche esempio 4.5)*

Prova. Vogliamo mostrare che ogni elemento di $SO(3)$ è connesso all'identità da una curva tutta contenuta in $SO(3)$. Dimostriamo prima di tutto che per ogni matrice R di $SO(3)$ esiste in $\mathbb{R}^3$ una base ortonormale in cui $R = BAB^{-1}$, con $A \in R_3$ e $B \in O(3)$.

- $R \in SO(n)$ con n **dispari**, ammette sempre l'autovalore 1; basta calcolare:

  $$\det(R - I) = \det(R - RR^t) = \det R \det(I - R^t) = \det(I - R) = (-1)^n \det(R - I)$$

  Si ottiene quindi $\det(R - I) = 0$.

- V , l'autospazio dell'autovalore 1, non può avere dimensione 2. Infatti se ha dimensione 2, siano $u, v \in V$ di lunghezza 1 e ortogonali tra loro, e sia $w \in V'$ (il complemento ortogonale di V) anch'esso di lunghezza 1. Si ottiene: $(Rw, u) = (Rw, Ru) = (w, u) = 0$ e $(Rw, v) = (Rw, Rv) = (w, v) = 0$. Ne segue allora $Rw \in V'$, (cioè il sottospazio V' è invariante sotto R) ma la dimensione di V' è 1 e quindi $Rw = \pm w$ (si ricordi che gli autovalori possibili per R sono solo ± 1). Il caso -1 è impossibile perchè allora la matrice R avrebbe come autovalori $1, 1, -1$ e quindi il suo determinante non potrebbe essere uguale a 1. Nel caso $+1$, seguirebbe che V ha dimensione 3, e quindi V' sarebbe ridotto al solo vettore nullo.

- Se V ha dimensione 3 non c'è nulla da dimostrare: nella base u, v, w si ha $R = I$.

- Nel caso in cui V ha dimensione 1, V' ha dimensione 2. Sia u, v, w una base ortonormale di $\mathbb{R}^3 = V' \oplus V$. In questa base, essendo V' è invariante sotto R, la matrice R assume la forma (abbiamo indicato con $B \in O(3)$ la matrice di passaggio dalla base canonica di $\mathbb{R}^3$ alla base u, v, w):
$$A = B^{-1}RB = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
Essendo A ortogonale e di determinante 1, deve essere $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ (con $\alpha \neq 0$) e quindi:
$$R = BAB^{-1} = Be^{\alpha A_3}B^{-1}$$

- Il gruppo $SO(3)$ è quindi connesso perchè la curva: (vedi esempio 4.5)
$$\gamma(t) = Be^{\alpha t A_3}B^{-1} \in SO(3)$$
verifica $\gamma(0) = I$ e $\gamma(1) = R$.

■

Teorema 4.5 *Sia G un qualsiasi gruppo di matrici, l'applicazione esponenziale:*
$$\exp : T(G) \to G$$
è suriettiva su G_0.

Il corso termina qui e, provvisoriamente, anche le dispense. Altri argomenti sui Gruppi di Matrici e sulle Algebre di Lie di interesse in Meccanica Analitica verranno visti nel corso di Fisica Matematica 1; altri argomenti sui Gruppi di Matrici (calcolo di centri, ulteriori considerazioni topologiche, tori massimali e rango di un gruppo di matrici, elementi di teoria delle rappresentazioni) sono rimandati ad un eventuale secondo corso di Teoria dei Gruppi.