Elementi di Teoria dei Gruppi e Applicazioni alla Meccanica Quantistica

Dario Capasso

16 dicembre 2005

Indice

Capitolo 1

Fondamenti

1.1 I Gruppi

Definizione 1 *Un insieme G possiede una struttura di gruppo se è assegnata una legge di composizione, cioé un'operazione binaria interna* $\cdot : (g_1, g_2) \in G \times G \to g_1 \cdot g_2 \in G$ *per cui valgano le seguenti proprietà:*

1. $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ ***Proprietá associativa***[1]
2. $\exists e \in G : e \cdot g = g \cdot e = g \qquad \forall g \in G$ ***Elemento neutro***
3. $\forall g \in G \qquad \exists g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$ ***Inverso***

Le richieste per definire un gruppo possono essere ulteriormente generalizzate modificando i punti 2 e 3, cioé richiedendo solo l'esistenza di un elemento neutro ed un inverso destro (o sinistro); questo modo di assiomatizzare il gruppo è comunque equivalente a quello dato.

Proposizione 1 *L'elemento neutro è unico.*

Dimostrazione. Indicano con e ed e' due distinti elementi neutri abbiamo che $e = ee' = e'$, contro l'ipotesi. ■

Proposizione 2 *L'inverso è unico.*

Dimostrazione. Indicando con h e h' due inversi di g abbiamo che $h' = h'(gh) = (h'g)h = h$, contro l'ipotesi (si noti che nella dimostrazione è stata essenziale l'associatività della moltiplicazione). ■

Il gruppo è detto **commutativo** o **abeliano** se $g_1 \cdot g_2 = g_2 \cdot g_1$ $\forall g_1, g_2 \in G$; nel caso di un gruppo abeliano si suole usare la notazione additiva, dove l'operazione interna $+$ è denominata addizione e l'elemento neutro è indicato col simbolo 0, mentre nel caso generale si usa la notazione moltiplicativa, dove l'operazione interna $\cdot$ è detta moltiplicazione e l'elemento neutro è indicato col simbolo 1.

In seguito ometteremo il simbolo $\cdot$ usando la notazione $g_1 g_2$.

Il numero di elementi (cioé la cardinalità[2] di G) che formano il gruppo è detto **ordine** del gruppo; quindi è possibile distinguere fra gruppi di ordine finito

[1] Se è valida solo la proprietà associativa la coppia $(G, \cdot)$ è detta **semigruppo**.

[2] La cardinalità di un insieme X sarà indicata con $|X|$.

(**gruppi finiti**) e di ordine infinito (**gruppi infiniti**); inoltre se è possibile identificare un elemento del gruppo con un insieme di parametri continui il gruppo è detto **gruppo continuo**. I gruppi finiti possono essere rappresentati tramite le **Tabelle di Cayley** che riportano il valore di tutti i possibili prodotti fra gli elementi del gruppo.

Esempio 1
1. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ formano un gruppo abeliano rispetto all'usuale addizione;*
2. *$\mathbb{Q}^*$ [3], $\mathbb{R}^*$ e $\mathbb{C}^*$ formano un gruppo abeliano rispetto all'usuale moltiplicazione;*
3. *L'insieme delle matrici quadrate $n \times n$ su un campo $F(+, \cdot)$ con determinante diverso da 0 è un gruppo rispetto all'usuale moltiplicazione fra matrici, denominato gruppo generale lineare ($GL(n, F)$); il gruppo è abeliano per $n = 1$, in quanto si riduce al gruppo moltiplicativo del campo (F^*), e non abeliano per $n > 1$;*
4. *L'insieme (di ordine 4) $G = \{1, i, -1, -i\} \subseteq \mathbb{C}^*$ è un gruppo rispetto all'usuale moltiplicazione fra numeri complessi con la seguente tabella di Cayley:*

$$\begin{array}{c|cccc} & 1 & i & -1 & -i \\ \hline 1 & 1 & i & -1 & -i \\ i & i & -1 & -i & 1 \\ -1 & -1 & -i & 1 & i \\ -i & -i & 1 & i & -1 \end{array} \tag{1.1}$$

Questo gruppo è, come vedremo, un gruppo ciclico generato dall'elemento i o dall'elemento $-i$.

Proposizione 3 *Presi x, a, b appartenenti al gruppo G si ha che $ax = b$ se e solo se $x = a^{-1}b$.*

Dimostrazione.
$$x = a^{-1}(ax) = a^{-1}b$$

■

Proposizione 4 *Presi x, y appartenenti al gruppo G si ha che $(xy)^{-1} = y^{-1}x^{-1}$ e $(x^{-1})^{-1} = x$.*

Dimostrazione.

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

■

Si definisce induttivamente la **potenza** $n-$esima x^n, con $n \in \mathbb{Z}$, dell'elemento x appartenente al gruppo G come segue:

- $x^0 = 1, \qquad x^1 = x$
- $x^{-1} : x^{-1}x = 1$

[3] Con l'apice $*$ indichiamo il campo privato dell'elemento neutro 0 dell'addizione.

- $x^n = x^{n-1}x$ se $n > 0$ e $x^n = (x^{-1})^{-n}$ se $n < 0$.

Proposizione 5 $x^{n+m} = x^n x^m$

Dimostrazione.

$$x^{n+m} = \prod_{i=1}^{n+m} x = \prod_{i=1}^{n} x \prod_{j=n+1}^{n+m} x = x^n x^m$$

■

Proposizione 6 $(x^n)^m = x^{nm}$

Dimostrazione.

$$(x^n)^m = \prod_{j=1}^{m} \left[\prod_{i=1}^{n} x \right] = \prod_{i=1}^{nm} x = x^{nm}$$

■

1.2 Sottogruppi

Definizione 2 *Un sottogruppo di un gruppo $G(\cdot)$è un sottoinsieme $H \subseteq G$ che è chiuso per $\cdot$ ($\forall x, y \in H \Rightarrow x \cdot y \in H$) e tale che la struttura indotta $H(\cdot)$ sia un gruppo.*

Per indicare che H è un sottogruppo del gruppo G si usa la notazione $H \leq G$. È facile verificare che l'elemento neutro del sottogruppo H di G coincide con l'elemento neutro di G.

Esempio 2

1. *$\mathbb{Z}$ è un sottogruppo del gruppo additivo $\mathbb{Q}$ che a sua volta è un sottogruppo additivo di $\mathbb{R}$ ed $\mathbb{R}$ è un sottogruppo di $\mathbb{C}$;*

2. *l'insieme singleton costituito dall'elemento neutro 1 ed il gruppo G stesso sono sottogruppi del gruppo G e sono detti **sottogruppi banali**, mentre gli altri eventuali sottogruppi sono detti **sottogruppi non banali**; un **sottogruppo proprio** di G ($\neq \{1\}$) è un sottogruppo distinto da G;*

3. *l'insieme $U(1) = \{x \in \mathbb{C} : x = e^{i\phi}, \phi \in \mathbb{R}\}$ è un sottogruppo di $\mathbb{C}^*(\cdot)$ rispetto all'usuale moltiplicazione; un suo sottogruppo proprio è l'insieme $C_\infty = \{x \in \mathbb{C} : x = e^{ik\theta}\}$[4], dove si è posto $\theta = 2\pi/n$ e dove $n \in \mathbb{N}$ e $k \in \mathbb{Z}$.*

La proprietà di essere un sottogruppo è transitiva, cioè dato un sottogruppo H del gruppo G ed un sottogruppo K di H allora K è un sottogruppo di G.

Proposizione 7 *Dato H sottoinsieme del gruppo G, allora H è un sottogruppo di G se e solo se H non è vuoto e $\forall x, y \in H$ si ha che $xy^{-1} \in H$.*

[4] $U(1)$ indica il gruppo unitario di dimensione 1, vedi il paragrafo 6.3.

Dimostrazione. L'elemento neutro appartiene ad H ($xx^{-1} = 1$) come l'inverso (basta porre $x = 1$). ■

L'intersezione di una famiglia di sottogruppi $H_i \leq G$ è ancora un sottogruppo in quanto, come conseguenza della struttura di gruppo degli H_i, all'intersezione appartiene l'elemento neutro 1 e dati $g_1, g_2 \in \cap_i H_i$ allora avremo anche che $g_1 g_2 = g_3 \in \cap_i H_i$. L'intersezione di tutti i sottogruppi di G contenenti un dato insieme $S \subseteq G$ è il più piccolo sottogruppo contenente S ed è indicato con $< S >$ [5]ed è detto **sottogruppo generato dall'insieme** S. Nel caso di un insieme S formato dal solo elemento g_0, il sottogruppo $< g_0 >$ è formato da tutti gli elementi esprimibili come potenze di g_0 ed è detto **gruppo ciclico**; più in generale un gruppo si dice **finitamente generato** se esiste un insieme finito di elementi X del gruppo che lo genera, cioé $G =< X >$.

Un gruppo ciclico $< x >$ è *finito* se esiste un intero positivo $n \in \mathbb{N}$ tale che $x^n = 1$; è facile verificare che il più piccolo n che verifica la precedente relazione è l'**ordine** del gruppo ed è detto **ordine** o **periodo** dell'elemento x in quanto coincide proprio con il numero di elementi del gruppo ($< x >= \{1, x^1, ..., x^{n-1}\}$)[6]; se non esiste un n che verifica la precedente condizioni allora il gruppo ciclico è *infinito*.

Proposizione 8 *Tutti i gruppi ciclici di ordine infinito sono isomorfi; tutti i gruppi ciclici di ordine n sono isomorfi.*

Dimostrazione. I gruppi ciclici di ordine infinito sono isomorfi al gruppo additivo $\mathbb{Z}$ tramite l'isomorfismo che associa ad ogni elemento $k \in \mathbb{Z}$ l'elemento $a^k \in< a >$; i gruppi ciclici di ordine n sono isomorfi al gruppo delle radici n-esime dell'unità nel campo complesso od anche al gruppo additivo degli interi modulo n. ■

Proposizione 9 *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Dimostrazione. Consideriamo un gruppo ciclico $< a >$ di ordine n ed un suo sottogruppo H non identico; sia k il minimo intero positivo tale che $a^k \in H - \{1\}$ e sia $l \in \mathbb{Z}$ tale che $a^l \in H$. Applicando alla coppia (l, k) l'algoritmo della divisione euclidea in $\mathbb{Z}$ si ha $l = kq + r$, con $q, r \in \mathbb{Z}$ e $0 \leq r < k$. Si ha allora

$$a^l = (a^k)^q a^r$$

e quindi

$$a^r = a^l (a^{-k})^q \in H$$

Ne segue che $r = 0$ per definizione di k. Abbiamo dimostrato che l deve essere un multiplo di k e quindi che $H =< a^k >$. ■

Tutti gli elementi di un gruppo finito hanno ordine finito; esistono anche gruppi di ordine infinito i cui elementi hanno ordine finito. I gruppi i cui elementi hanno tutti ordine finito sono detti **periodici** o di **torsione**; i gruppi i cui elementi, esclusa l'unità, hanno tutti ordine infinito sono detti **liberi da torsione**, mentre i restanti sono detti **misti**.

[5]$< S >$ contiene tutti prodotti di potenze di elementi di S ed è pertanto costituito da essi.

[6]Sia m un divisore di n allora l'elemento $x^{n/m}$ del gruppo è una radice $m-$esima dell'unità ed ha periodo m.

Possiamo introdurre un **prodotto fra sottoinsiemi** nel seguente modo: dati due sottoinsiemi X e Y del gruppo G, costruiamo i seguenti insiemi:

$$XY = \{xy \in G : x \in X, y \in Y\}$$

$$X^{-1} = \{x^{-1} \in G : x \in X\}$$

Due sottogruppi H e K del gruppo G sono detti **sottogruppi permutabili** se $HK = KH$, cioé se per ogni $h_1 \in H$ e per ogni $k_1 \in K$ esistono $h_2 \in H$ e $k_2 \in K$ tali che $h_1k_1 = k_2h_2$.

Proposizione 10 *Dati due sottogruppi H e K permutabili allora l'insieme HK é un sottogruppo.*

Dimostrazione. Per la proposizione 7 dobbiamo dimostrare che presi gli elementi $h_1k_1, h_2k_2 \in HK$ allora $h_1k_1(h_2k_2)^{-1} \in HK$

$$h_1k_1(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = h_1k_3h_2^{-1} = h_1h_3k_4 \in HK$$

dove

$$k_3 = k_1k_2^{-1}$$

e h_3 e k_4 sono elementi di H e K rispettivamente tali che

$$k_3h_2^{-1} = h_3k_4$$

■

In generale, dati due sottogruppi A e B di G, il sottogruppo generato dai due sottogruppi contiene l'insieme prodotto, cioé:

$$AB \subseteq < A, B >$$

e vale l'uguaglianza se e solo se A e B sono permutabili.

1.3 Omomorfismi

Un'applicazione f dal gruppo G al gruppo H è detta **omomorfismo** se conserva le leggi di composizione, cioé se:

$$f(g_1g_2) = f(g_1)f(g_2) \qquad \forall g_1, g_2 \in G,$$

inoltre se f è iniettiva, suriettiva o biettiva è detta, rispettivamente *monomorfismo*, *epimorfismo* od *isomorfismo*. L'insieme degli omomorfismi fra G eH si indica con $Hom(G, H)$.

Due gruppi G e H si dicono **isomorfi** se esiste un isomorfismo $\phi : G \to H$, indicheremo ciò con la scrittura $G \simeq H$. Nella classe di tutti i gruppi l'isomorfismo è una relazione di equivalenza[7] sicché si possono considerare le *classi di isomorfismo dei gruppi* invece di considerare tutti i possibili gruppi[8].

Un omomorfismo possiede le seguenti proprietà:

1. $f(1) = 1$ dove 1 al primo membro e 1 al secondo membro sono gli elementi neutri, rispettivamente, di G e H;
2. $f(g^{-1}) = (f(g))^{-1}$;
3. f trasforma sottogruppi in sottogruppi;
4. $Im(f) = \{h \in H : h = f(g), g \in G\}$ è un sottogruppo di H.
5. $Ker(f) = \{g \in G : f(g) = 1\}$ è un sottogruppo di G.

Dimostrazione.

1. $h = f(g) = f(g1) = f(g)f(1) = hf(1)$;
2. $f(g)f(g)^{-1} = 1 = f(1) = f(gg^{-1}) = f(g)f(g^{-1})$;
3. detto K il sottoinsieme di H immagine del sottogruppo F di G, per dimostrare che K è un sottogruppo adoperiamo la proposizione 7, cioé, dati $h_1, h_2 \in K$ e $g_1, g_2 \in F$ tali che e $h_1 = f(g_1)$ e $h_2 = f(g_2)$, si ha:
$$h_1(h_2)^{-1} = f(g_1)f(g_2)^{-1} = f(g_1)f[(g_2)^{-1}] = f[g_1(g_2)^{-1}]$$
ma $g_1(g_2)^{-1} \in F$, quindi $h_1(h_2)^{-1} \in K$;
4. segue dalla 3., perché G è un sottogruppo di G;
5. dati $g_1, g_2 \in Ker(f)$ allora $1 = 1(1)^{-1} = f(g_1)f(g_2)^{-1} = f(g_1)f[(g_2)^{-1}] = f[g_1(g_2)^{-1}]$, cioé $g_1(g_2)^{-1} \in Ker(f)$; l'asserto segue dalla proposizione 7.

■

Esempio 3 *1. L'omomorfismo $f : x \in \mathbb{R} \to e^{ix} \in U(1)$ è un epimorfismo dal gruppo additivo $\mathbb{R}$ sul gruppo moltiplicativo $U(1)$ dei numeri complessi con modulo uguale ad uno; il nucleo di questo omomorfismo è il sottogruppo additivo $2\pi\mathbb{Z}$ generato da 2π;*

2. l'omomorfismo $f : x \in \mathbb{R} \to e^x \in \mathbb{R}^*$ è un monomorfismo dal gruppo additivo $\mathbb{R}$ al gruppo moltiplicativo $\mathbb{R}^*$ e $Im(f) = \mathbb{R}^+(\cdot)$ (gruppo moltiplicativo dei numeri reali positivi).

---

[7] Una relazione di equivalenza $\mathcal{R}$ in una classe (in un insieme) è una relazione binaria che soddisfa le seguenti proprietà:

1. transitiva: se $a\mathcal{R}b$ e $b\mathcal{R}c$ allora $a\mathcal{R}c$
2. simmetrica: se $a\mathcal{R}b$ allora $b\mathcal{R}a$
3. riflessiva: $a\mathcal{R}a$

[8] Dato un gruppo con una legge di composizione che presenti difficoltà di calcolo ed un gruppo ad esso isomorfo con una legge di composizione più maneggevole, allora è possibile effettuare il calcolo nel gruppo più semplice da trattare e, successivamente, usare l'isomorfismo per ottenere il risultato relativo al gruppo di partenza.

Ci sono gruppi che possono essere isomorfi ad un loro sottogruppo proprio, naturalmente la condizione necessaria perché questo sia possibile è che il gruppo sia infinito; un esempio è l'isomorfismo che associa ad ogni elemento di $k \in \mathbb{Z}$ l'elemento $2k$ appartenente al gruppo additivo degli interi pari.

Un omomorfismo nel gruppo G induce un omomorfismo anche sui suoi sottogruppi.

Dato un gruppo K isomorfo ad un sottogruppo H del gruppo G questo può essere *embedded* nel gruppo G, cioè può essere immerso nel gruppo G. Precisamente, se $\sigma : K \to H$ è un isomorfismo e

$$\imath : h \in H \to h \in G$$

è l'omomorfismo di immersione di H in G, allora

$$\imath \circ \sigma : K \to G$$

è un monomorfismo che immerge K in G.

Esempio 4 *Il gruppo simmetrico di grado $n-1$ può essere immerso nel gruppo simmetrico di grado n.*

1.4 Sistemi di Generatori

Definizione 3 *Un* **sistema di generatori** *del gruppo G è un insieme $M \subseteq G$ tale che*

$$G =< M > .$$

Esiste sempre un sistema di generatori in quanto basta considerare come insieme M tutto il gruppo G.

Un sistema di generatori M è detto **irriducibile** o **minimale** se non esiste nessun sottoinsieme proprio di M che generi tutto il gruppo, mentre il gruppo è detto **finitamente** od **infinitamente generato** a seconda che possieda un sistema di generatori rispettivamente finito od infinito. La finitezza di un sistema di generatori non implica la finitezza dell'ordine del gruppo; il gruppo additivo $\mathbb{Z}$ è generato dal solo elemento 1.

Proposizione 11 *Ogni sistema finito di generatori di un gruppo finitamente generato contiene un sistema irriducibile di generatori.*

Dimostrazione. Dato un sistema di generatori basta escludere da esso gli elementi superflui. ■

Distinti sistemi di generatori irriducibili di gruppi finitamente generati possono contenere un diverso numero di elementi.

Proposizione 12 *Ogni imagine tramite un omomorfismo di un gruppo finitamente generato è un gruppo finitamente generato.*

Dimostrazione. Consideriamo il gruppo finitamente generato

$$G =< a_1, a_2, ..., a_n >$$

ed un omomorfismo $\phi : G \to H$, allora un elemento a' del gruppo H immagine dell'elemento $a \in G$ tramite l'omomorfismo ϕ è esprimibile nel seguente modo

$$a' = \phi(a) = \phi(a_{i_1}^{k_1} a_{i_2}^{k_2} ... a_{i_s}^{k_s}) = \phi(a_{i_1})^{k_1} \phi(a_{i_2})^{k_2} ... \phi(a_{i_s})^{k_s}$$

dove $a = a_{i_1}^{k_1} a_{i_2}^{k_2} ... a_{i_s}^{k_s}$. Quindi $\phi(a_1), \phi(a_2), ..., \phi(a_n)$ è un sistema di generatori per H. ■

1.5 Classi Laterali (Cosets)

Dato un sottogruppo $H \leq G$, definiamo in G la seguente relazione di equivalenza $\mathcal{R}_H^R$: *dati due elementi $g_1, g_2 \in G$, essi sono equivalenti ($g_1 \mathcal{R}_H^R g_2$) se esiste $h \in H$ tale che $g_1 = hg_2$.* L'insieme Hg, formato dagli elementi hg con $h \in H$ e $g \in G$, è detto **classe laterale destra** di H in G; in modo analogo è possibile definire le **classi laterali sinistre** tramite la relazione di equivalenza $\mathcal{R}_H^L$ ($g_1 \mathcal{R}_H^L g_2$ se esiste $h \in H$ tale che $g_1 = g_2 h$)[9]. Ogni classe laterale puó essere indicata fornendo un unico elemento ad essa appartenente, detto **rappresentante**, in quanto, preso g_0 come rappresentante, l'elemento $g_1 \in Hg_0$ si otterrà come $g_1 = h_1 g_0$ con $h_1 \in H$, essendo $Hg_1 = Hh_1 g_0 = Hg_0$; da ciò si ottiene che classi laterali (destre o sinistre) distinte non possiedono elementi in comune. Le classi laterali hanno la stessa cardinalità di H, in quanto l'applicazione $h \in H \to hg \in Hg$ è biettiva. Consideriamo un insieme T costituito dai rappresentanti delle classi laterali destre di H in G; G è uguale all'unione disgiunta delle classi laterali, cioé

$$G = \bigcup_{t \in T} Ht \tag{1.2}$$

l'insieme T è un **trasversale destro**; equivalentemente si può definire un trasversale sinistro.

Possiamo esprimere il concetto di laterale e trasversale utilizzando il prodotto fra insiemi definito nel paragrafo 1.2, cioé la (1.2) può essere riscritta nella seguente forma: $G = HT$ e $|H \cap T| = 1$.

Proposizione 13 *Dato un sottogruppo H del gruppo G e indicando con T un trasversale destro, allora T^{-1} é un trasversale sinistro.*

Dimostrazione.

$$G = G^{-1} = (HT)^{-1} = T^{-1} H^{-1} = T^{-1} H$$

dove si è utilizzato il fatto che H è un sottogruppo. Inoltre si ha che $|H \cap T^{-1}| = |H^{-1} \cap T^{-1}| = 1$. ■

La cardinalità di T, detta **indice** di H in G e indicata con il simbolo $|G : H|$, è uguale alla cardinalità dell'insieme costituito da tutte le classi laterali di G rispetto

[9] D'ora in avanti saranno usati i laterali destri, a meno che non sia esplicitamente dichiarato, in quanto in modo simile si può fare riferimento a quelli sinistri.

ad H. Indichiamo la cardinalità di T con lo stesso simbolo indipendentemente dal fatto che T sia un trasversale destro o sinistro in quanto, per la precedente proposizione, esiste una biezione fra i trasversali destri e quelli sinistri, quindi si ha che $|G/\mathcal{R}_H^R| = |G/\mathcal{R}_H^L|$.

Da quanto detto finora risulta naturale usare come scrittura per indicare i trasversali[10] la seguente

$$T \equiv G/\mathcal{R}_H^R$$

questa scrittura rappresenta in forma grafica anche il seguente teorema:

Teorema 14 (di Lagrange) *Se H è un sottogruppo del gruppo G allora $|G| = |G:H||H|$, e quindi se $|G|$ è finito si ha che $|G:H| = |G|/|H|$.*

Dimostrazione. L'indice di H in G, cioè la cardinalità di $G/\mathcal{R}_H^R$, è il numero di classi laterali di H in G; ogni classe laterale contiene $|H|$ elementi, quindi, essendo $G = H(G/\mathcal{R}_H^R)$, si ha che la cardinalità di G è il prodotto delle cardinalità di H e di $G/\mathcal{R}_H^R$. Inoltre se $|G|$ è finita allora è finita anche $|H|$ e quindi è possibile effettuare la divisione. ■

L'insieme $G/\mathcal{R}_H^R$, dove H è un sottogruppo del gruppo G, assume la struttura di gruppo (**gruppo quoziente**) se e solo se $Hg_1Hg_2 = Hg_1g_2$ cioè se $Hg_1Hg_2 = H(g_1H)g_2 = H(Hg_1)g_2 = Hg_1g_2$, dove $g_1, g_2 \in G$; un tale sottogruppo è detto **normale** od **invariante** ($gH = Hg$ [11]) ed è indicato con $H \trianglelefteq G$; dalla definizione segue che *se G è abeliano ogni sottogruppo è normale.* L'intersezione di sottogruppi normali è ancora un sottogruppo normale. La definizione di sottogruppo normale significa che Hg è sia un laterale destro sia un laterale sinistro, cioé si ha che $\mathcal{R}_H^R = \mathcal{R}_H^L$, quindi il gruppo quoziente si può denotare, senza ambiguità, con

$$G/H$$

Se $H \trianglelefteq G$ allora la proiezione canonica

$$\phi : g \in G \to Hg \in G/H$$

è un epimorfismo detto *epimorfismo canonico.* Dalla definizione di sottogruppo normale abbiamo che

$$g^{-1}Hg = H \qquad \forall g \in G$$

I sottogruppi normali sono un caso particolare di sottogruppi permutabili con ogni sottogruppo, come provato nella seguente proposizione.

Proposizione 15 *Il sottogruppo $< H, K >$ generato da un sottogruppo normale H e da un sottogruppo K coincide con HK.*

Dimostrazione. Poiché H è un gruppo normale allora si ha

$$h_1k = kh_2 \in KH$$

dove $h_1, h_2 \in H$ e $k \in K$. Quindi $HK = KH$ cioé $HK =< H, K >$. ■

La proprietà di essere un sottogruppo normale non è transitiva, cioé dato un sottogruppo normale F del sottogruppo normale H di G, allora non è detto che

[10] Un'altra dicitura che useremo è quella di **insieme quoziente**.

[11] $gh_1 = h_2g$ dove $h_1, h_2 \in H$.

F sia un sottogruppo normale di G ($F \lhd H \lhd G$ non implica che $F \lhd G$); invece se F è un sottogruppo normale di G ed è contenuto nel sottogruppo H ($F \subseteq H$), allora $F \lhd H$.

Il gruppo G è detto **semplice** se non possiede sottogruppi normali, escludendo i sottogruppi banali G e $\{1\}$; G è detto **semisemplice** se non possiede sottogruppi normali abeliani, escludendo il sottogruppo banale $\{1\}$.

L'insieme C di tutti gli elementi del gruppo G che commutano con tutti gli elementi di G ($C = \{c : cg = gc \ \forall g \in G\}$) è detto **centro** di G; gli elementi di C formano un sottogruppo abeliano di G che, per la definizione, è anche invariante.

Esistono gruppi non commutativi in cui ogni sottogruppo è normale e sono detti *Hamiltoniani*.

1.6 Teoremi sugli Omomorfismi ed altre Proprietà

Sia

$$f : G \to H$$

un omomorfismo, allora sono valide le seguenti proprietà:

1. f trasforma sottogruppi normali di G in sottogruppi normali di $Im(f)$;
2. $Ker(f) = \{g \in G : f(g) = 1\}$ è un sottogruppo normale del gruppo G.

Dimostrazione.

1. Dato un sottogruppo normale K del gruppo G allora si ha che $gKg^{-1} = K$ cioé che $f(gKg^{-1}) = f(K)$, allora sviluppando il termine sinistro si ottiene che $f(g)f(K)f(g^{-1}) = f(K)$, cioé il sottogruppo $f(K)$ immagine del sottogruppo K è normale in $Im(f)$;
2. poniamo $N = Ker(f)$, allora $f(gNg^{-1}) = f(g)f(N)f(g^{-1}) = f(g)1f(g^{-1}) = 1 = f(N)$. Poiché ogni sottogruppo normale N di un gruppo G è il nucleo dell'omomorfismo canonico $\phi : G \to G/N$, possiamo affermare che tutti i sottogruppi normali di G sono i nuclei ($Ker(f)$) di tutti i possibili omomorfismi di G.

■

Teorema 16 (primo teorema degli omomorfismi) *Sia $f : G \to H$ un omomorfismo. Denotato con $\phi : G \to G/Ker(f)$* ***l'epimorfismo canonico****, l'unica applicazione iniettiva $\psi : G/Ker(f) \to H$ tale che $f = \psi \circ \phi$ è un monomorfismo e quindi $G/Ker(f)$ è isomorfo a $Im(f)$.*

Dimostrazione. L'applicazione ψ è definita come segue

$$\psi[gKer(f)] = f(g) \qquad (g \in G)$$

ed è un omomorfismo in quanto lo è f. Poiché $Im(\psi) = Im(f)$ si ha ovviamente che la corestrizione di ψ a $Im(f)$ è un isomorfismo $G/Ker(f) \to Im(\psi) = Im(f)$.
■

Teorema 17 (secondo teorema degli omomorfismi) *Dati un sottogruppo H ed un sottogruppo normale N in G, allora $N \cap H \trianglelefteq H$ e i gruppi quoziente $H/(N \cap H)$ e $(NH)/N$ sono isomorfismi.*

Dimostrazione. Sia $f : H \to G/N$ l'applicazione definita come segue

$$f(h) = Nh \qquad (h \in H).$$

f è la restrizione a H dell'epimorfismo canonico $G \to G/N$ e quindi f è un omomorfismo. D'altronde si ha, con $h \in H$:

$$h \in Ker(f) \Leftrightarrow Nh = h \Leftrightarrow h \in H \cap N$$

cioé $Ker(f) = H \cap N$. Allora il teorema 16 assicura che $H/(H \cap N)$ è isomorfo a $Im(f) = \{Nh : h \in H\} = NH/N$, da cui si ha l'asserto. ■

Teorema 18 (terzo teorema degli omomorfismi) *Dati due sottogruppi normali M, N di G con $N \leq M$, allora $M/N \triangleleft G/N$ e $(G/N)/(M/N)$ è isomorfo a G/M.*

Dimostrazione. Per dimostrare il teorema basta mostrare che M/N è il nucleo di un epimorfismo f dal gruppo G/N nel gruppo G/M; sia $f : G/N \to G/M$ l'applicazione definita come segue

$$f(Ng) = Mg \qquad (g \in G).$$

f è ben definita poiché $N \leq M$ e quindi

$$Ng_1 = Ng_2 \Rightarrow Mg_1 = Mg_2,$$

inoltre, da quanto appena detto, è ovvio che f sia un epimorfismo. Infine si ha che

$$Ker(f) = \{Ng \in G/N : Mg = M\} = M/N.$$

■

1.7 Endomorfismi ed Automorfismi

Definizione 4 *Un applicazione di un gruppo G in sé è detta **endomorfismo** se è un omomorfismo del gruppo G in se stesso; in particolare se l'applicazione è biettiva allora si dice **automorfismo**.*

Esistono gruppi isomorfi ad un loro sottogruppo proprio (ciò è possibile solo nel caso di gruppi infiniti), in questo caso un isomorfismo è un endomorfismo iniettivo in quanto, dato un elemento del gruppo, non è detto che la controimmagine sia non vuota.

Fra gli endomorfismi è definita l'operazione di composizione (non commutativa) che corrisponde ad applicare in successione gli endomorfismi; ciò è possibile in quanto il dominio di ogni endomorfismo è l'intero gruppo e quindi contiene il codominio di un qualsiasi endomorfismo.

Proposizione 19 *Un endomorfismo ϕ di un gruppo $G =< a_1, a_2, ... >$ è completamente determinato una volta che siano note le immagini, tramite ϕ, del sistema di generatori.*

Dimostrazione.

$$\phi(a) = \phi(a_{i_1}^{k_1} a_{i_2}^{k_2} ...) = \phi(a_{i_1})^{k_1} \phi(a_{i_2})^{k_2} ...$$

dove $a = a_{i_1}^{k_1} a_{i_2}^{k_2} ....$ ■

Proposizione 20 *La composizioni di due endomorfismi è un endomorfismo.*

Dimostrazione.

$$[\psi \circ \phi](ab) = \psi[\phi(ab)] = \psi[\phi(a)\phi(b)] = \psi[\phi(a)]\psi[\phi(b)] = [\psi \circ \phi](a)[\psi \circ \phi](b)$$

■

In particolare la composizione di due automorfismi è un automorfismo.

Da quanto detto si deduce che l'insieme degli endomorfismi di un gruppo rispetto all'operazione di composizione non è un gruppo, dato che non esistono le applicazioni inverse[12], a differenza degli automorfismi che formano un gruppo che si denota di solito con $Aut(G)$.

Proposizione 21 *L'applicazione $\phi_a : x \in G \to axa^{-1} \in G$, dove $a \in G$, è un automorfismo del gruppo G detto **coniugio** mediante l'elemento a.*

Dimostrazione. L'applicazione ϕ_a definisce un omomorfismo in quanto

$$\phi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \phi_a(x)\phi_a(y).$$

L'applicazione è, inoltre, un isomorfismo in quanto esiste la sua applicazione inversa

$$\phi_a^{-1} : x \in G \to a^{-1}xa \in G$$
$$[\phi_a \circ \phi_a^{-1}](x) = \phi_a(a^{-1}xa) = aa^{-1}xaa^{-1} = x$$

■

Gli automorfismi che si possono identificare con l'operazione di coniugio rispetto ad un elemento del gruppo formano un sottoinsieme del gruppo degli automorfismi e tali automorfismi sono detti **inner**, mentre tutti gli altri automorfismi sono detti **outer**.

Proposizione 22 *Gli automorfismi inner di un gruppo G sono un sottogruppo del gruppo degli automorfismi, denotato di solito con $Inn(G)$.*

Dimostrazione. Consideriamo gli automorfismi ϕ_a e ϕ_b corrispondenti rispettivamente agli elementi $a, b \in G$, allora, utilizzando la (7) si ha

$$[\phi_a \circ \phi_b^{-1}](x) = \phi_a[\phi_b^{-1}(x)] = \phi_a(b^{-1}xb) = ab^{-1}xba^{-1} = (ab^{-1})x(ab^{-1})^{-1} = \phi_{ab^{-1}}(x)$$

cioé $\phi_{ab^{-1}}$ è l'automorfismo generato dall'elemento $ab^{-1} \in G$, cioé il coniugio mediante ab^{-1}. ■

Nel caso di un gruppo abeliano il sottogruppo degli automorfismi di tipo inner si riduce all'automorfismo identico; più in generale è vera la seguente affermazione:

[12] Tra gli endomorfismi esiste **l'endomorfismo nullo** che associa ad ogni elemento del gruppo l'elemento neutro, che ovviamente non è invertibile, salvo il caso banale che G sia identico.

Proposizione 23 *Dato un gruppo G ed il suo centro C, allora si ha che il sottogruppo $Inn(G)$ degli automorfismi di tipo inner è isomorfo al gruppo quoziente*

$$G/C.$$

Dimostrazione. Basta notare che C è il nucleo dell'omomorfismo

$$\phi : a \in G \to \phi_a \in Inn(G)$$

ed utilizzare il teorema 16 degli omomorfismi. ■

Proposizione 24 *Il sottogruppo $Inn(G)$ degli automorfismi di tipo inner è normale in $Aut(G)$.*

Dimostrazione. Consideriamo l'automorfismo ψ e l'automorfismo di tipo inner ϕ_a, ciò che dobbiamo dimostrare è che l'automorfismo $\psi \circ \phi_a \circ \psi^{-1}$ è di tipo inner.

$$[\psi \circ \phi_a \circ \psi^{-1}](x) = \psi\{\phi_a[\psi^{-1}(x)]\} =$$

$$= \psi[a\psi^{-1}(x)a^{-1}] = \psi(a)x\psi(a^{-1}) = \psi(a)x\psi^{-1}(a) = \phi_{\psi(a)}(x)$$

■

La definizione di sottogruppo normale data nel paragrafo 1.5 può essere riscritta nella seguente forma:

Definizione 5 *Un **sottogruppo normale** N del gruppo G è un sottogruppo tale che ogni elemento coniugato di $x \in N$ mediante qualsiasi elemento $a \in G$ è un elemento di N, cioé $axa^{-1} \in N$.*

1.8 Sottogruppi Caratteristici e Pienamente invarianti

I sottogruppi normali vengono trasformati in se stessi sotto l'azione degli automorfismi di tipo inner; questa condizione si può generalizzare considerando il caso di sottogruppi invarianti sotto l'applicazione di tutti gli automorfismi, detti **sottogruppi caratteristici**, o sottogruppi invarianti rispetto a tutti gli endomorfismi, detti **sottogruppi pienamente invarianti**.

Esempio 5

1. *Il centro C di un gruppo G è un sottogruppo caratteristico in quanto, preso $a \in C$ ed un automorfismo ϕ, si ha*

$$\phi(a)\phi(x) = \phi(ax) = \phi(xa) = \phi(x)\phi(a) \qquad \forall x \in G,$$

cioé $\phi(a) \in C$;

2. *tutti i sottogruppi di un gruppo ciclico sono pienamente invarianti in quanto, detto a un generatore del sottogruppo e ϕ un qualsiasi endomorfismo ($\phi(a) = a^k$ per un certo $k \in \mathbb{N}$), si ha che $\phi(a^s) = (a^s)^k = a^{sk} \in < a >$.*

1.8.1 I Commutatori ed il Gruppo Derivato

Definizione 6 *Dati due elementi a e b del gruppo G si definisce* ***commutatore*** *della coppia (a, b) il seguente elemento del gruppo G*

$$[a, b] = (ba)^{-1}ab$$

Il nome commutatore deriva dal fatto che

$$ab = ba[a, b]$$

e quindi $[a, b]$ è uguale all'unità del gruppo solo se a e b sono permutabili, cioé se commutano fra di loro.

Sono verificate le seguenti proprietà:

1. $$[a, b][b, a] = [(ba)^{-1}(ab)][(ab)^{-1}(ba)] = 1$$

   da cui
   $$[a, b]^{-1} = [b, a]$$

2. $$[a, b^{-1}] = (b^{-1}a)^{-1}ab^{-1} = a^{-1}bab^{-1} = a^{-1}(ab)(ab)^{-1}bab^{-1} = b[b, a]b^{-1}$$

3. $$[ab, c] = b^{-1}a^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}a(cb)(cb)^{-1}bc = b^{-1}[a, c]b[b, c]$$

Il commutatore in generale non è associativo

$$[a, [b, c]] \neq [[a, b], c]$$

Definizione 7 *Il sottogruppo G' del gruppo G generato dall'insieme dei commutatori di ogni coppia di elementi di G è detto* ***derivato*** *di G.*

$$G' =< \{g \in G : g = [a, b], \forall a, b \in G\} >$$

Il gruppo derivato è pienamente invariante in quanto, detto ϕ un endomorfismo del gruppo G, si ha

$$\phi([a, b]) = \phi(a^{-1}b^{-1}ab) = \phi^{-1}(a)\phi^{-1}(b)\phi(a)\phi(b) = [\phi(a), \phi(b)]$$

1.8.2 Gruppi con Operatori

Possiamo generalizzare quanto affermato nel paragrafo precedente assegnando un insieme Σ di operatori, cioé un $\Sigma \subseteq End(G)$, al gruppo G; un sottogruppo che è trasformato in se stesso da tutti gli endomorfismi di Σ è detto **sottogruppo ammissibile** di G rispetto a Σ o **Σ-sottogruppo** di G.

Per l'insieme Σ contenete tutti gli automorfismi di tipo inner otterremo che i sottogruppi ammissibili corrispondono ad i sottogruppi normali, per $\Sigma = Aut(G)$ avremo che i sottogruppi ammissibili corrispondono ad i sottogruppi caratteristici ed, infine, per $\Sigma = End(G)$ i sottogruppi ammissibili saranno i sottogruppi pienamente invarianti.

1.9 Prodotti fra Gruppi

Presi n gruppi G_i definiamo un nuovo gruppo $G = G_1 \times G_2 \times ... \times G_n$ dove $g = (g_1, g_2, ..., g_n) \in G$ con $g_i \in G_i$; la moltiplicazione fra due elementi $g = (g_1, g_2, ..., g_n), h = (h_1, h_2, ..., h_n) \in G$ è definita come $gh = (g_1h_1, g_2h_2, ..., g_nh_n) \in G$; un prodotto fra gruppi così definito è detto **prodotto diretto**[13] (o **somma diretta** se il prodotto definito su tutti i G_n è commutativo).

Definiamo l'applicazione proiezione p_i che agisce nel seguente modo

$$p_i : (g_1, ..., g_i, ..., g_n) \in G \to g_i \in G_i$$

e l'applicazione di immersione $\imath_i$ tale che

$$\imath_i : g_i \in G_i \to (1_{G_1}, ..., g_i, ..., 1_{G_n}) \in \overline{G_i}$$

Proposizione 25 *Dato $G = G_1 \times ... \times G_i \times ... \times G_n$ si ha che gli elementi di $\overline{G_i}$ formano un sottogruppo normale di G isomorfo a G_i.*

Dimostrazione. $\overline{G_i}$ è isomorfo a G_i facendo corrispondere a $\{1_{G_1}, ..., h_i, ..., 1_{G_n}\}$ l'elemento $h_i \in G_i$; inoltre $\overline{G_i}$ è normale in quanto

$$G\overline{G_i} \ni (g_1, ..., g_i, ..., g_n) \cdot (1_{G_1}, ..., h_i, ..., 1_{G_n}) = (g_1 1_{G_1}, ..., g_ih_i, ..., g_n 1_{G_n}) =$$

$$= (g_1 1_{G_1}, ..., k_ig_i, ..., g_n 1_{G_n}) = (1_{G_1}, ..., k_i, ..., 1_{G_n}) \cdot (g_1, ..., g_i, ..., g_n) \in \overline{G_i}G$$

dove $k_ig_i = g_ih_i$ cioé $k_i = g_ih_i(g_i)^{-1}$. ■

Proposizione 26 *Siano G, G_1, G_2 dei gruppi, un omomorfismo $\phi : G \to G_1 \times G_2$ è in corrispondenza biettiva con le coppie ordinate di omomorfismi (ϕ_1, ϕ_2) dove:*

$$\phi_1 : G \to G_1 \qquad \phi_2 : G \to G_2$$

Il nucleo di ϕ è $Ker(\phi) = Ker(\phi_1) \cap Ker(\phi_2)$.

Dimostrazione. La coppia (ϕ_1, ϕ_2) corrispondente a ϕ è

$$\phi_1 = p_1(\phi) \qquad \phi_2 = p_2(\phi)$$

Essendo $(1_{G_1}, 1_{G_2})$ l'elemento neutro del gruppo $G_1 \otimes G_2$, si ha che un elemento $h \in G$ appartiene al nucleo di ϕ se e solo se sono verificate entrambe le relazioni $\phi_1(h) = 1_{G_1}$ e $\phi_2(h) = 1_{G_2}$, ne segue $Ker(\phi) = Ker(\phi_1) \cap Ker(\phi_2)$. ■

Preso un gruppo G ed un sottogruppo $A \leq Aut(G)$ si definisce **prodotto semidiretto** di G per A, indicato con $G \rtimes A$, il gruppo avente come insieme sostegno il prodotto cartesiano $G \times A$ e munito della seguente moltiplicazione:

$$(g, \Lambda)(g', \Lambda') = (g\Lambda(g'), \Lambda\Lambda') \tag{1.3}$$

dove $(g, \Lambda) \in G \rtimes A$ e $\Lambda(g')$ è l'immagine di g' mediante l'automorfismo Λ.

L'elemento neutro del gruppo è la coppia $(1, id_G)$, dove id_G è l'automorfismo identico, e l'inverso di un elemento è dato da $(g, \Lambda)^{-1} = (\Lambda^{-1}(g^{-1}), \Lambda^{-1})$. L'applicazione $g \in G \to (g, id_G) \in G \rtimes A$ è un monomorfismo (G è canonicamente embedded in $G \rtimes A$); è pertanto lecito adottare l'identificazione $G \rtimes A$):

$$g = (g, id_G) \qquad g \in G$$

[13] Nel caso in cui tutti i gruppi G_i siano commutativi si ha che il gruppo G è commutativo; in questo caso si adotta la notazione additiva e quindi si parla di **somma diretta** e $G = G_1 + G_2 + ... + G_n$.

Proposizione 27 *G è un sottogruppo invariante di $G \rtimes A$.*

Dimostrazione.

$$(g, \Lambda)(g', id_G)(g, \Lambda)^{-1} = (g\Lambda(g'), \Lambda)(\Lambda^{-1}(g^{-1}), \Lambda^{-1}) = (g\Lambda(g')g^{-1}, id_G)$$

■

Proposizione 28 *$G \rtimes A/G$ è isomorfo a A.*

Dimostrazione. Basta notare che l'applicazione $\phi : (G, \Lambda) \in G \rtimes A \to \Lambda \in A$ è un epimorfismo da $G \rtimes A$ in A il cui nucleo è G. ■

1.10 Il Gruppo delle Permutazioni su un Insieme

Definizione 8 *Una **permutazione** di un insieme X è un'applicazione biettiva di X in X.*

Per un'applicazione g (in particolare per una permutazione) possiamo utilizzare sia la notazione sinistra

$$g : x \in X \to gx \in X$$

sia la notazione destra

$$x \in X \to xg \in X$$

Le permutazioni formano gruppo rispetto al prodotto fra applicazioni, in quanto il prodotto di due permutazioni è ancora una permutazione e l'elemento neutro è la permutazione identica ($x \to x$).

Il gruppo delle permutazioni è detto **gruppo simmetrico** ed è indicato con $Sym(X)$; se $|X| = n$ l'ordine di $Sym(X)$ è $n!$.

Dato un insieme X costituito da n elementi un elemento del gruppo delle permutazioni è indicato schematicamente con una matrice $2 \times n$; prendiamo per esempio il gruppo delle permutazioni sull'insieme $X = \{1, 2, 3\}$. Presi $a, b \in Sym(X)$

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

allora il prodotto ab si costruisce riscrivendo la prima riga di a e scrivendo nella seconda riga la sequenza ottenuta sostituendo ogni elemento x_i della seconda riga di a con l'elemento che si trova nella seconda riga di b corrispondente alla'elemento x_i nella prima riga di b.

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Il gruppo delle permutazioni su di un insieme X non è commutativo per $n = |X| \geq 3$, come si può verificare facilmente.

Una **trasposizione** è una permutazione che scambia solo due elementi (e fissa i rimanenti); ad esempio l'elemento del gruppo delle permutazioni che trasforma la sequenza $(3, 1, 2)$ nella sequenza $(3, 2, 1)$ è una trasposizione. Ogni permutazione di un insieme finito si può ottenere come prodotto di trasposizioni: se il numero di trasposizioni è pari la permutazione è detta **pari**, altrimenti è detta **dispari**. Non è difficile provare che la parità del numero di trasposizioni in cui si decompone una permutazione non varia.

Esempio 6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (12)(13)(14)(15) = (34)(35)(13)(23)$$

Il prodotto di due permutazioni pari è ovviamente una permutazione pari, mentre il prodotto di due permutazioni dispari è una permutazione pari; l'identità è una permutazione pari in quanto è il quadrato di una qualsiasi trasposizione, essendo le trasposizioni involutorie (l'inversa di una trasposizione è la trasposizione stessa); quindi le permutazioni pari formano un sottogruppo del gruppo delle permutazioni chiamato *gruppo alterante*, indicato con A_n, dove $n = |X|$. A_n è un gruppo di ordine $n!/2$, non commutativo per $n \geq 4$.

1.11 Azioni di un Gruppo

Un'**azione sinistra di un gruppo** G su di un insieme S è un'applicazione che associa ad un elemento del gruppo e ad uno dell'insieme S un elemento di S, cioé è un'applicazione $(g, s) \in G \times S \mapsto (gs) \in S$, che soddisfa le seguenti proprietà

1. $1s = s \qquad \forall s \in S$
2. $g(g's) = (gg')s \qquad \forall g, g' \in G$ e $\forall s \in S$

È facile osservare che l'applicazione

$$w : g \in G \to (s \to gs) \in Sym(S)$$

è un omomorfismo. Viceversa ogni omomorfismo

$$w : G \to Sym(S)$$

da luogo ad un'azione sinistra di G su S:

$$(g, s) \in G \times S \to gs := w(g)(s) \in S.$$

Un insieme con un'azione del gruppo G è detto G-insieme; allo stesso modo si può definire un'**azione destra**. Si osservi che, se $(g, s) \in G \times S \to sg \in S$ è un'azione destra di G su S, allora l'omomorfismo $w : G \to Sym(S)$ ad essa associato è definito come segue:

$$w : g \in G \to (s \to sg^{-1}) \in Sym(S).$$

Definizione 9 *Si definisce* ***orbita*** *di s, con $s \in S$, sotto l'azione del gruppo G il sottoinsieme*

$$O_s = \{s' \in S : s' = gs \qquad g \in G\} \subset S$$

L'orbita di un elemento dell'insieme sotto l'azione del gruppo ci dice come viene trasformato l'elemento sotto l'azione del gruppo.

Le orbite di un insieme S sotto l'azione di un gruppo G sono classi di equivalenza di S: $s' \sim s$ se $s' = gs$ per un certo $g \in G$. Il gruppo G opera indipendentemente su ciascuna orbita, non trasportando elementi di un orbita in una distinta, quindi le orbite di S formano una partizione di S, cioé S è l'unione disgiunta di tutte le sue orbite.

Se S contiene una sola orbita allora si dice che G *agisce transitivamente* su S.

Definizione 10 *Si definisce* ***stabilizzatore*** *di $s \in S$ il sottogruppo G_s di G che lascia invariato s, cioé*

$$G_s = \{g \in G : gs = s\}$$

Per verificare che lo stabilizzatore è un sottogruppo basta utilizzare la proposizione 7, cioé dati $x, y \in G_s$ bisogna verificare che $xy^{-1}s = s$, si ha infatti

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

Consideriamo ora l'azione destra del gruppo G sui propri laterali destri rispetto al sottogruppo H, cioé sull'insieme $G/\mathcal{R}_H^R$. Preso un laterale Ha, dove $a \in G$, l'azione del gruppo G è definita come segue:

$$(Ha)g = H(ag) \qquad g \in G$$

Il gruppo agisce transitivamente su $G/\mathcal{R}_H^R$, cioé $G/\mathcal{R}_H^R$ è formato da una sola orbita.

Proposizione 29 *Dato un G-insieme S ed un elemento $s \in S$, sia G_s lo stabilizzatore e O_s l'orbita di s; allora esiste un'applicazione biettiva $\phi : G_s a \in G/\mathcal{R}_{G_s}^R \to sa \in O_s$. Questa applicazione è compatibile con l'azione di G, cioé $\phi((G_s a)g) = \phi(G_s a)g$.*

Dimostrazione. Verifichiamo innanzitutto se l'applicazione è ben definita cioé se è indipendente dall'elemento che rappresenta il laterale di $G_s := H$ in G. Dati due elementi a, b appartenenti alla stessa classe laterale ($b = ha$ dove $h \in H$) allora deve verificarsi $sa = sb$, infatti

$$sb = s(ha) = (sh)a = sa$$

dove nell'ultimo passaggio si è usato il fatto che h appartiene allo stabilizzatore di s.

L'applicazione è suriettiva in quanto $\forall g \in G$ abbiamo che $sg \in O_s$ per definizione di orbita. L'applicazione è anche iniettiva in quanto, supponendo per assurdo che presi due elementi a, b appartenenti a due classi differenti ($Ha \neq Hb$), si ha che $sa = sb$, si ottiene che $sab^{-1} = s$ cioé che $ab^{-1} \in H$ il che comporta $Ha = Hb$, contro l'ipotesi. ■

Da questa proposizione si ottiene che l'indice $[G : G_s]$ coincide con la cardinalità $|O_s|$ dell'orbita di s. Così, se G è finito, l'ordine del gruppo G è uguale al prodotto fra l'ordine dello stabilizzatore e l'ordine dell'orbita

$$|G| = |G_s||O_s|$$

Proposizione 30 *Dato un G-insieme S, $s \in S$ e $s' \in O_s$, cioé tale che $s' = as$ con $a \in G$, allora si ha la seguente relazioni tra gli stabilizzatori di s e di s'*

$$G_{s'} = aG_s a^{-1}$$

Dimostrazione. Se $a \in G$ allora $aG_s a^{-1} = G_s$; infatti, essendo $s' = G_{s'}s' = G_{s'}as$, si ha $as = G_{s'}as$ da cui la tesi. ■

1.12 Azioni di un Gruppo su se stesso

Tra le azioni di un gruppo G sono di particolare interesse le seguenti azioni di G sul proprio insieme sostegno (su se stesso).

Definizione 11 *Si definisce* ***traslazione sinistra*** *associata all'elemento $g \in G$ la seguente applicazione:*

$$L_g : x \in G \rightarrow gx \in G$$

Analogamente si definisce l'azione destra.

Teorema 31 (di Cayley) *Ogni gruppo è isomorfo ad un sottogruppo del gruppo simmetrico $Sym(G)$.*

Dimostrazione. L'omomorfismo

$$L : G \rightarrow Sym(G)$$

è iniettivo e quindi

$$G \simeq Im(L)$$

■

Un'altra azione del gruppo su se stesso è il coniugio

$$(g, x) \in G \times G \mapsto gxg^{-1} \in G$$

Lo stabilizzatore in G rispetto all'azione per coniugio sull'elemento $x \in G$ è detto **centralizzante** di x in G e si denota con $C_G(x)$; esso è formato da tutti gli elementi di G che commutano con x

$$C_G(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G : gx = xg\}$$

Proposizione 32 *L'intersezione di tutti i centralizzanti è il centro del gruppo.*

1.13 I Teoremi di Sylow

I teoremi di Sylow riguardano i sottogruppi di un gruppo finito aventi come ordine una potenza di un numero primo. Indichiamo con n l'ordine del gruppo finito G ($n = |G|$), con p un primo divisore di n e con r il massimo esponente tale che p^r sia un divisore di n ($n = p^r m$ e p non è un divisore di m).

Teorema 33 (Primo Teorema di Sylow) *Esiste un sottogruppo di G di ordine p^r.*

I sottogruppi di G di ordine p^r sono detti **p-sottogruppi** (o **sottogruppi**) **di Sylow** di G.

Teorema 34 (Secondo Teorema di Sylow) *Sia P un sottogruppo di Sylow di G e sia H un p-sottogruppo di G, allora esiste $g \in G$ tale che H è un sottogruppo di gPg^{-1} (o anche: esiste $g \in G$ tale che gHg^{-1} è un sottogruppo di P).*

Teorema 35 (Terzo Teorema di Sylow) *Sia s il numero dei p-sottogruppi di Sylow di G, allora s divide $m = n/p^r$ ed è tale che $s = ap + 1$, dove $a \in \mathbb{Z}$, cioé $s \equiv 1$ (modulo p).*

Capitolo 2

Gruppi

2.1 I Gruppi Liberi

Consideriamo un insieme non vuoto M, finito o infinito, ed indichiamo con $x_1, x_2, ..., x_i, ...$ i suoi elementi; costruiamo gli elementi $x_1^{-1}, x_2^{-1}, ..., x_i^{-1}, ...$ che siano in corrispondenza biunivoca con gli elementi di M e che non appartengano ad M. Denotato con M^{-1} l'insieme degli elementi $x_1^{-1}, x_2^{-1}, ..., x_i^{-1}, ...$, gli elementi di M potranno anche essere indicati con la notazione x_i^{+1}. Possiamo costruire la potenza positiva di un elemento di M come un nuovo elemento x_i^s che corrisponde a considerare la sequenza $x_i x_i ... x_i$ costituita da s volte l'elemento x_i; ovviamente le potenze negative si definiscono nel medesimo modo utilizzando però gli elementi $x_1^{-1}, x_2^{-1}, ..., x_i^{-1}, ...$. Definiamo **parola** w su M una sequenza ordinata (cioé tale che non sia possibile scambiare il posto di due elementi) di elementi

$$w = x_{i_1}^{s_1} x_{i_2}^{s_2} ... x_{i_l}^{s_l}$$

dove $s_p \in \mathbb{Z} - \{0\}$ e i_q indica uno degli indici degli elementi di M il quale può apparire nell'espressione della parola anche più volte; l'insieme delle parole su M sarà denotato con $W(M)$. Definiamo anche una nozione di prodotto (giustapposizione) fra due parole w_1, w_2 che corrisponde a costruire una nuova parola come la sequenza degli elementi della prima seguita dalla sequenza di elementi della seconda, cioé posto

$$w_1 = x_{i_1}^{s_1} x_{i_2}^{s_2} ... x_{i_l}^{s_l}$$

$$w_2 = x_{q_1}^{p_1} x_{q_2}^{p_2} ... x_{q_l}^{p_l}$$

si definisce $w_1 w_2$ come segue:

$$w_1 w_2 = x_{i_1}^{s_1} x_{i_2}^{s_2} ... x_{i_l}^{s_l} x_{q_1}^{p_1} x_{q_2}^{p_2} ... x_{q_l}^{p_l}.$$

Il prodotto così definito nell'insieme delle parole su M non è commutativo però è associativo.

Le parole possono avere lunghezze arbitrarie e le parole di lunghezza 1 sono gli elementi di M e gli elementi $x_1^{-1}, x_2^{-1}, ..., x_i^{-1}, ...$ di M^{-1}. Costruiamo un ulteriore elemento che corrisponde alla **parola vuota**, w_0, il quale risulta essere l'unico elemento ad avere lunghezza 0; la parola vuota è tale che data una parola w si ha $ww_0 = w_0 w = w$.

Infine una parola è detta **ridotta** se non compaiono al suo interno termini del tipo $x_i^{-1}x_i^{+1}$ o del tipo $x_i^{+1}x_i^{-1}$. Si definisce in $W(M)$ la seguente relazione di equivalenza $\sim$: $w \sim v$ se w si ottiene da v mediante un numero finito di inserimenti o cancellazioni di parole del tipo $x_i^{+1}x_i^{-1}$ o $x_i^{-1}x_i^{+1}$. È facile provare che in ciascuna classe di equivalenza $[w]_\sim$ c'è un'unica parola ridotta e che la relazione $\sim$ è una congruenza del semigruppo $W(M)(\cdot)$. Allora $W(M)/\sim(\cdot)$ è un gruppo con l'operazione quoziente. L'elemento neutro di $W(M)/\sim(\cdot)$ è la classe $[w_0]_\sim$; se

$$w = x_{i_1}^{s_1}x_{i_2}^{s_2}...x_{i_l}^{s_l}$$

e

$$w^{-1} = x_{i_1}^{-s_1}x_{i_2}^{-s_2}...x_{i_l}^{-s_l}$$

sono una parola e la sua inversa su M, si ha

$$[w]_\sim \cdot [w^{-1}]_\sim = [w_0]_\sim$$

cioé $[w^{-1}]_\sim = [w]_\sim^{-1}$.

Si può quindi scegliere come modello del gruppo $W(M)/\sim(\cdot)$ l'insieme delle parole ridotte con la moltiplicazione che consiste nella cancellazione delle parole $x_i^{-1}x_i^{+1}$ e $x_i^{+1}x_i^{-1}$ ($\in [w_0]_\sim$) dopo la giustapposizione delle parole ridotte da moltiplicare.

In questo modo l'insieme costituito da tutte le parole ridotte su un qualsiasi insieme M soddisfa gli assiomi di gruppo. Tale gruppo prende il nome di gruppo libero sull'insieme M e solitamente si denota con F_M. Questa procedura è la maniera più generale per costruire un gruppo astratto, cioé senza precisare la natura dei suoi elementi, e che non abbia altre proprietà se non quella di essere generato da un insieme di assegnata (ma arbitraria) cardinalità. Ogni gruppo si può costruire a partire da un gruppo libero, nel senso precisato nella proposizione 36.

Il **rango** di un gruppo libero è la cardinalità di M, quindi un gruppo libero di rango finito è numerabile. Per la non commutatività del prodotto fra parole si ha che solo i gruppi liberi di rango 1 sono commutativi. Escludendo l'identità, cioé la parola vuota, ogni elemento del gruppo ha ordine infinito.

Definizione 12 *L'insieme M è detto sistema di generatori liberi "standard" del gruppo libero F_M.*

Proposizione 36 *Ogni gruppo è isomorfo ad un gruppo quoziente di un gruppo libero.*

Dimostrazione. Dato un sistema di generatori (irriducibile) $M = \{x_1, x_2, ...\}$ del gruppo G possiamo costruire il gruppo libero F_M ad esso associato. L'applicazione che associa ad ogni elemento

$$x_{i_1}^{s_1}x_{i_2}^{s_2}...x_{i_l}^{s_l} \in F_M$$

l'elemento

$$x_{i_1}^{s_1}x_{i_2}^{s_2}...x_{i_l}^{s_l} \in G$$

è un omomorfismo il cui Kernel K è costituito dagli elementi di F_M che rappresentano l'unità 1 di G. Quindi, utilizzando il primo teorema degli omomorfismi 16, si ha che

$$G \simeq F_M/K$$

■

Dalla precedente proposizione segue che ogni gruppo con n generatori è isomorfo ad un gruppo quoziente di un gruppo libero di rango n. I prodotti degli elementi del gruppo che sono uguali all'unità, cioé

$$x_{i_1}^{s_1} x_{i_2}^{s_2} ... x_{i_l}^{s_l} = 1$$

definiscono il Kernel dell'omomorfismo della precedente proposizione e quindi individuano il gruppo stesso e sono dette **relazioni di definizione** o anche **relazioni generatrici**; un gruppo è completamente determinato una volta note le sue relazioni di definizione.

Esempio 7 *1. Un gruppo abeliano si può costruire utilizzando la seguente relazione di definizione:*

$$[x_i, x_j] = 1$$

2.2 I gruppi Abeliani

In questo paragrafo useremo la notazione additiva per indicare l'operazione interna del gruppo, 0 per indicare l'elemento neutro ed il segno $-$ preposto all'elemento del gruppo indicherà l'inverso dell'elemento, in modo da sottolineare la proprietà di commutatività del gruppo. Inoltre la notazione esponenziale x^n, nella notazione additiva, sarà scritto in modo moltiplicativo come nx ($n \in \mathbb{Z}$).

Un gruppo abeliano è detto **periodico** o di **torsione** se i suoi elementi sono periodici, cioé di ordine finito, **libero da torsione** se tutti gli elementi, escluso l'elemento nullo, hanno ordine infinito, e **misto** se alcuni elementi hanno ordine finito ed altri ordine infinito.

Se G è un gruppo abeliano il sottoinsieme T di G costituito da tutti gli elementi di ordine finito di G forma un sottogruppo detto **sottogruppo di torsione**. Il gruppo G/T [1] è libero da torsione.

Teorema 37 *In un gruppo abeliano G il sottogruppo di torsione T è la somma diretta delle componenti primarie G_p [2] di G.*

Un elemento $g \in G$ è detto **divisibile** da un intero positivo m se esiste un elemento $g' \in G$ tale che $g = mg'$; un gruppo abeliano G è detto divisibile se ciascun elemento di G è divisibile da ogni intero positivo. È facile vedere che somme di sottogruppi divisibili sono ancora sottogruppi divisibili[3].

[1] Ha senso considerare il gruppo quoziente G/T perché G è abeliano e quindi $T \trianglelefteq G$.

[2] Il sottogruppo G_p è formato da tutti gli elementi di G aventi ordine una potenza del numero primo p.

[3] Da ciò discende che esiste il massimo sottogruppo divisibile di un gruppo abeliano G, dato dalla somma di tutti i sottogruppi divisibili di G.

Teorema 38 *Se D è un sottogruppo divisibile di G allora $G = D \oplus E$, dove E è un certo sottogruppo di G.*

Un gruppo abeliano R è detto **ridotto** se non possiede sottogruppi divisibili escluso il sottogruppo nullo. Un gruppo abeliano G è decomponibile (decomposizione di Baer) nella somma diretta del massimo sottogruppo divisibile D di G e di un sottogruppo ridotto R di G ($G = D \oplus R$).

Consideriamo un sottoinsieme S del gruppo abeliano G, allora si dice che S è **linearmente indipendente** o **indipendente** se, dati r elementi distinti di S, $s_1, s_2, ..., s_r$, e gli interi $m_1, m_2, ..., m_r$, la relazione

$$m_1 s_1 + m_2 s_2 + ... + m_r s_r = 0$$

implica che $m_i s_i = 0$ per ogni i; da ciò si deduce che un gruppo abeliano G è somma diretta di gruppi ciclici se e solo se è generato da un sottoinsieme indipendente (detto **base**). Il lemma di Zorn mostra che ogni sottoinsieme indipendente di G è contenuto in un sottoinsieme indipendente massimale di G.

Dato un numero primo p definiamo **p-rango** del gruppo abeliano G, che indichiamo con $r_p(G)$, la cardinalità di un sottoinsieme indipendente massimale di elementi di G aventi ordine una potenza del primo p; similmente si definisce lo **0-rango** o **rango libero da torsione** $r_0(G)$ la cardinalità di un sottoinsieme indipendente massimale di G costituito da elementi di ordine infinito. Si può dimostrare che i numeri cardinali $r_0(G)$ e $r_p(G)$ non dipendono dai sistemi massimali scelti ma solo dal gruppo G.

Un gruppo abeliano G è detto **abeliano libero** se è generato da una parte indipendente massimale S costituita da elementi di ordine infinito, cioé se è somma diretta di gruppi ciclici di ordine infinito.

Proposizione 39 *Dato un gruppo abeliano libero G ed assegnata una base S, allora ogni elemento del gruppo è rappresentato da un unica famiglia di elementi di S a supporto finito*[4].

Dimostrazione. Consideriamo che l'elemento $y \in G$ sia esprimibile tramite le seguenti combinazioni[5]

$$y = \sum_{s \in S} n_s x_s = \sum_{s \in S} n'_s x_s$$

allora

$$\sum_{s \in S} (n_s - n'_s) x_s = 0$$

da cui, per l'indipendenza, si ottiene $n_s = n'_s$. ■

Proposizione 40 *Ogni gruppo abeliano G è isomorfo ad un gruppo quoziente di un gruppo abeliano libero.*

[4] $supp(m_s)_{s \in S} = \{s \in S : m_s \neq 0\}$.

[5] Le somme sono intese su tutti gli elementi a supporto finito.

Dimostrazione. Dato un sistema di generatori $S = \{s_1, s_2, ...\}$ del gruppo G possiamo costruire il gruppo abeliano libero F_S ad esso associato. L'applicazione che associa ad ogni elemento

$$s_{i_1}^{j_1} + s_{i_2}^{j_2} + ... + s_{i_l}^{j_l} \in F_S$$

l'elemento

$$s_{i_1}^{j_1} + s_{i_2}^{j_2} + ... + s_{i_l}^{j_l} \in G$$

è un omomorfismo il cui Kernel K è costituito dagli elementi di F_S che rappresentano lo 0 di G. Quindi, utilizzando il primo teorema degli omomorfismi 16, si ha che

$$G \simeq F_S/K$$

■

2.3 Gruppi Risolubili

Definizione 13 *Un gruppo G è detto* ***risolubile*** *se possiede una serie finita di sottogruppi ciascuno normale nel successivo*

$$1 = G_0 \lhd G_1 \lhd ... \lhd G_n = G,$$

detta ***serie risolubile****, tale che tutti i gruppi quoziente G_{i+1}/G_i siano abeliani.*

Questa classe di gruppi contiene i gruppi abeliani in quanto ogni sottogruppo di un gruppo abeliano è normale ed ogni gruppo quoziente è ovviamente abeliano.

Proposizione 41 *Se G è un gruppo risolubile allora ogni sottogruppo H è risolubile.*

Dimostrazione. Essendo il gruppo G risolubile allora esiste una serie risolubile $G_0, G_1, ..., G_n$; poniamo

$$H_i = H \cap G_i$$

dove $i = 0, 1, ..., n$. Dimostriamo che la serie $H_0, H_1, ..., H_n$ è una serie risolubile di sottogruppi di H.

$$H_0 = H \cap G_0 = H \cap 1_G = 1_G$$

$$H_n = H \cap G_n = H \cap G = H$$

Preso $u \in H_i$ e $v \in H_{i-1}$ allora si ha che $uvu^{-1} \in H_{i-1}$ in quanto, dato che $H_i \subseteq G_i$ e $H_{i-1} \subseteq G_{i-1}$, si ha che $uvu^{-1} \in G_{i-1}$, essendo G_{i-1} normale in G_i, e,essendo H un sottogruppo, l'elemento uvu^{-1} deve appartenere anche ad H.

Infine utilizzando il secondo teorema degli omomorfismi (17) si ha che il gruppo quoziente

$$\frac{H_i}{H_{i-1}} = \frac{(G_i \cap H)}{G_{i-1} \cap H} = \frac{(G_i \cap H)}{G_{i-1} \cap (G_i \cap H)}$$

è isomorfo a

$$\frac{G_{i-1}(G_i \cap H)}{G_{i-1}}$$

che è un sottogruppo del gruppo abeliano G_i/G_{i-1}. ■

Proposizione 42 *Se G è un gruppo risolubile allora, dato H un suo sottogruppo normale, il gruppo G/H è risolubile.*

Proposizione 43 *Dato un sottogruppo normale e risolubile H di G allora, se il gruppo G/H è risolubile, lo è anche G.*

Proposizione 44 *I gruppi ciclici che abbiano come ordine un numero primo p sono tutti e soli i gruppi risolubili semplici.*

2.4 Gruppi Nilpotenti

Definizione 14 *Una serie finita di sottogruppi di G*

$$1_G = A_0 \subset A_1 \subset ... \subset A_n = G$$

*è detta **serie centrale** se il gruppo quoziente A_{i+1}/A_i è contenuto nel centro di G/A_i, cioé se*

$$[A_{i+1}, G] \subseteq A_i$$

Un gruppo G che possiede una serie centrale è detto **gruppo nilpotente**. Naturalmente i gruppi abeliani sono gruppi nilpotenti ed i gruppi nilpotenti sono gruppi risolubili in quanto

$$[A_{i+1}, G] \subseteq A_i \Rightarrow [A_i, G] \subseteq A_i$$

essendo $A_i \subset A_{i+1}$, cioé $A_i \lhd G$, e A_{i+1}/A_i è abeliano perché è contenuto nel centro di G/A_i.

Capitolo 3

I Gruppi di Lie

3.1 Le Algebre di Lie

Definizione 15 *Uno spazio vettoriale* $\mathbf{V}$ *sul campo* K *possiede una struttura di* ***algebra di Lie*** *se è assegnata un'operazione (moltiplicazione di Lie o* ***commutatore*** *o crochet) interna allo spazio* $\mathbf{V}$ *con le seguenti proprietà:*

1. $\begin{array}{l}[\alpha\mathbf{x}+\beta\mathbf{y},\mathbf{z}]=\alpha[\mathbf{x},\mathbf{z}]+\beta[\mathbf{y},\mathbf{z}]\\ [\mathbf{z},\alpha\mathbf{x}+\beta\mathbf{y}]=\alpha[\mathbf{z},\mathbf{x}]+\beta[\mathbf{z},\mathbf{y}]\end{array}$ *con* $\alpha,\beta\in K$ *(Bilinearità)*

2. $[\mathbf{x},\mathbf{x}]=0$ *(Nilpotenza)*

3. $[\mathbf{x},[\mathbf{y},\mathbf{z}]]+[\mathbf{y},[\mathbf{z},\mathbf{x}]]+[\mathbf{z},[\mathbf{x},\mathbf{y}]]=0$ *(Identità di Jacobi o Associatività di Jacobi)*

Sfruttando la prorietà di nilpotenza e la proprietà di bilinerità di un'algebra di Lie possiamo sviluppare il seguente commutatore

$$0=[\mathbf{x}+\mathbf{y},\mathbf{x}+\mathbf{y}]=[\mathbf{x},\mathbf{x}]+[\mathbf{x},\mathbf{y}]+[\mathbf{y},\mathbf{x}]+[\mathbf{y},\mathbf{y}]=[\mathbf{x},\mathbf{y}]+[\mathbf{y},\mathbf{x}]$$

da cui ricaviamo la sua antisimmetria

$$[\mathbf{x},\mathbf{y}]=-[\mathbf{y},\mathbf{x}]$$

È facile osservare che, se il campo K ha caratteristica 2, allora ogni K-algebra di Lie è commutativa; mentre, se la caratteristica del campo è diversa da 2, una K-algebra di Lie V è commutativa se e solo se il commutatore è nullo, cioé $[\mathbf{x},\mathbf{y}]=\mathbf{0}$ $\forall\mathbf{x},\mathbf{y}\in\mathbf{V}$.

Data un'algebra associativa $\mathbf{A}$, possiamo costruire un'algebra di Lie tramite la seguente posizione:

$$[\mathbf{x},\mathbf{y}]=\mathbf{xy}-\mathbf{yx}$$

dove $\mathbf{x},\mathbf{y}\in\mathbf{A}$. È facile verificare che il precedente commutatore soddisfa tutte le proprietà di un prodotto di Lie.

Un sottospazio $\mathbf{H}$ di $\mathbf{V}$ che sia stabile per la moltiplicazione di Lie indotta da $\mathbf{V}$ è una sottoalgebra di Lie di $\mathbf{V}$; un **ideale** è una sottoalgebra tale che $[\mathbf{V},\mathbf{H}]\subset\mathbf{H}$; si definisce **centro** di $\mathbf{V}$ la massima sottoalgebra $\mathbf{C}$ tale che $[\mathbf{V},\mathbf{C}]=\mathbf{0}$, la quale è evidentemente una sottoalgebra commutativa.

Assegnata una base $\mathbf{e_1}, \mathbf{e_2}, ..., \mathbf{e_n}$ nello spazio $\mathbf{V}$, sfruttando la bilinearità del commutatore otteniamo:

$$\mathbf{z} = z^i \mathbf{e_i} = [\mathbf{x}, \mathbf{y}] = [x^j \mathbf{e_j}, y^k \mathbf{e_k}] = x^j y^k [\mathbf{e_j}, \mathbf{e_k}]$$

cioé

$$z^i = [\mathbf{x}, \mathbf{y}]^i = c^i_{jk} x^j y^k \tag{3.1}$$

Resta così definito un tensore di rango 3 e di tipo $(1, 2)$; le c^i_{jk} sono dette **costanti di struttura**

$$c^i_{jk} \mathbf{e_i} = [\mathbf{e_j}, \mathbf{e_k}]. \tag{3.2}$$

Dalla proprietà di antisimmetria e dall'identità di Jacobi si ha

$$c^i_{jk} = -c^i_{kj}$$

$$c^p_{is} c^s_{jk} + c^p_{js} c^s_{ki} + c^p_{ks} c^s_{ij} = 0$$

Dati due spazi $\mathbf{V_1}, \mathbf{V_2}$ con una struttura di algebra di Lie, un'applicazione lineare $f : \mathbf{v} \in \mathbf{V_1} \to f(\mathbf{v}) \in \mathbf{V_2}$ è detta **omomorfismo** se

$$[f(\mathbf{v_1}), f(\mathbf{v_1'})] = f([\mathbf{v_1}, \mathbf{v_1'}])$$

dove $\mathbf{v_1}, \mathbf{v_1'} \in \mathbf{V_1}$. Un omomorfismo biettivo è detto isomorfismo; due algebre sono isomorfe se esiste un isomorfismo tra loro.

Il kernel di un omomorfismo è un ideale del dominio in quanto, preso $\mathbf{y} \in Ker(f)$ e $\mathbf{x} \in \mathbf{L}$, avremo $f([\mathbf{x}, \mathbf{y}]) = [f(\mathbf{x}), \mathbf{0}] = \mathbf{0}$ cioé $[\mathbf{x}, \mathbf{y}] \in Ker(f)$.

Sia $\mathbf{L}$ un'algebra di Lie ed $\mathbf{M}$ un suo ideale, allora definiamo le seguente relazione di equivalenza: $\mathbf{v_1} \sim \mathbf{v_2}$ se $\mathbf{v_1} = \mathbf{v_2} + \mathbf{m}$ con $m \in \mathbf{M}$. La relazione di equivalenza è una congruenza di $\mathbf{L}$, cioé se $\mathbf{v_1} \sim \mathbf{v_2}$ e $\mathbf{w_1} \sim \mathbf{w_2}$ allora $[\mathbf{v_1}, \mathbf{w_1}] \sim [\mathbf{v_2}, \mathbf{v_2}]$, sicché l'operazione di commutazione è indipendente dalla scelta del rappresentante della classe di equivalenza

$$[\mathbf{v_1}, \mathbf{v}] = [\mathbf{v_2} + \mathbf{m}, \mathbf{v}] = [\mathbf{v_2}, \mathbf{v}] + [\mathbf{m}, \mathbf{v}] = [\mathbf{v_2}, \mathbf{v}] + \mathbf{m'}.$$

Lo spazio quoziente $\mathbf{H} = \mathbf{L}/\mathbf{M}$ è quindi un'algebra di Lie che chiameremo **algebra quoziente di Lie**.

Siano $\mathbf{L_1}, \mathbf{L_2}, ..., \mathbf{L_n}$ n algebre di Lie sullo stesso campo K; nello spazio vettoriale $\mathbf{L} = \bigoplus_i \mathbf{L_i}$, **somma diretta** dei singoli spazi, definiamo il commutatore nel seguente modo:

$$[(\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}), (\mathbf{y_1}, \mathbf{y_2}, ..., \mathbf{y_n})] = ([\mathbf{x_1}, \mathbf{y_1}], [\mathbf{x_2}, \mathbf{y_2}], ..., [\mathbf{x_n}, \mathbf{y_n}]) \tag{3.3}$$

dove $\mathbf{x_i}, \mathbf{y_i} \in \mathbf{L_i}$; è facile verificare che $\mathbf{L}$ resta munita di una struttura di algebra di Lie.

Definizione 16 *Una **derivazione** D di un'algebra è un'applicazione lineare dell'algebra in se stessa tale che:*

$$D(\mathbf{xy}) = D(\mathbf{x})\mathbf{y} + \mathbf{x}D(\mathbf{y})$$

Nel caso di un'algebra di Lie la precedente relazione si può riscrivere nel modo seguente:

$$D([\mathbf{x},\mathbf{y}]) = [D(\mathbf{x}),\mathbf{y}] + [\mathbf{x}, D(\mathbf{y})]$$

Prese $D_1, D_2 \in \mathcal{D}(\mathbf{L})$, dove $\mathcal{D}(\mathbf{L})$ è l'insieme delle derivazioni nell'algebra di Lie $\mathbf{L}$, abbiamo che

$$(D_1 + D_2)([\mathbf{x},\mathbf{y}]) = D_1([\mathbf{x},\mathbf{y}]) + D_2([\mathbf{x},\mathbf{y}]) =$$

$$= [D_1(\mathbf{x}),\mathbf{y}] + [\mathbf{x}, D_1(\mathbf{y})] + [D_2(\mathbf{x}),\mathbf{y}] + [\mathbf{x}, D_2(\mathbf{y})] =$$

$$= [(D_1 + D_2)(\mathbf{x}),\mathbf{y}] + [\mathbf{x},(D_1 + D_2)(\mathbf{y})]$$

e che

$$(\alpha D)([\mathbf{x},\mathbf{y}]) = \alpha[D(\mathbf{x}),\mathbf{y}] + \alpha[\mathbf{x}, D(\mathbf{y})] = \alpha D([\mathbf{x},\mathbf{y}])$$

per la bilinearità del commutatore e la linearità delle derivazioni; inoltre si ha anche che

$$[D_1, D_2]([\mathbf{x},\mathbf{y}]) = (D_1D_2)[\mathbf{x},\mathbf{y}] - (D_2D_1)[\mathbf{x},\mathbf{y}] =$$

$$= (D_1)([D_2(\mathbf{x}),\mathbf{y}] + [\mathbf{x}, D_2(\mathbf{y})]) - (D_2)([D_1(\mathbf{x}),\mathbf{y}] + [\mathbf{x}, D_1(\mathbf{y})]) =$$

$$= [D_1D_2(\mathbf{x}),\mathbf{y}] + [D_2(\mathbf{x}), D_1(\mathbf{y})] + [D_1(\mathbf{x}), D_2(\mathbf{y})] + [\mathbf{x}, D_1D_2(\mathbf{y})]+$$

$$-[D_2D_1(\mathbf{x}),\mathbf{y}] - [D_1(\mathbf{x}), D_2(\mathbf{y})] - [D_2(\mathbf{x}), D_1(\mathbf{y})] - [\mathbf{x}, D_2D_1(\mathbf{y})] =$$

$$= [[D_1, D_2](\mathbf{x}),\mathbf{y}] + [\mathbf{x}, [D_1, D_2](\mathbf{y})]$$

Quindi $\mathcal{D}(\mathbf{L})$ è un'algebra di Lie.

Siano $\mathbf{T}$ e $\mathbf{M}$ due K-algebre di Lie e sia D un omomorfismo di $\mathbf{M}$ in $\mathcal{D}(\mathbf{T})$; nello spazio vettoriale $\mathbf{M} \oplus \mathbf{T}$ definiamo il seguente commutatore:

$$[(\mathbf{x_1},\mathbf{y_1}),(\mathbf{x_2},\mathbf{y_2})] = ([\mathbf{x_1},\mathbf{x_2}], \mathbf{x_2}D(\mathbf{y_1}) - \mathbf{x_1}D(\mathbf{y_2}) + [\mathbf{y_1},\mathbf{y_2}])$$

dove $(\mathbf{x_1},\mathbf{y_1}),(\mathbf{x_2},\mathbf{y_2}) \in \mathbf{M} \oplus \mathbf{T}$. Tale operazione definisce l'algebra **somma semidiretta** delle algebre $\mathbf{M}$ e $\mathbf{T}$, indicata con $\mathbf{T} \rtimes \mathbf{M}$.

Nel caso particolare in cui consideriamo i vettori $\mathbf{x} \equiv (\mathbf{x}, \mathbf{0})$ e $\mathbf{y} \equiv (\mathbf{0}, \mathbf{y})$, otteniamo

$$[(\mathbf{0},\mathbf{y}),(\mathbf{x},\mathbf{0})] = (\mathbf{0}, \mathbf{x}D(\mathbf{y}))$$

cioé

$$[\mathbf{y},\mathbf{x}] = \mathbf{y}D(\mathbf{x})$$

Esempio 8 *1. Nell'insieme delle matrici quadrate su un campo K possiamo introdurre un commutatore nel seguente modo:*

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

dove $A, B \in M_n$. Il centro di questa algebra è la sottoalgebra delle matrici scalari λI.

2. *Una base, sul campo complesso, dello spazio delle matrici* 2×2 *complesse* $M(2, \mathbb{C})$ *è data dalle matrici:*
$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{3.4}$$
Utilizzando il commutatore fra matrici sulle le matrici di Pauli σ_i *otteniamo:*
$$[\sigma_i, \sigma_j] = 2i\varepsilon^i_{jk}\sigma_k.$$
Le matrici di Pauli sono una base di una sottoalgebra dell'algebra di Lie $M(2, \mathbb{C})$ *con costanti di struttura* $c^i_{jk} = 2i\varepsilon^i_{jk}$.

3.2 Spazi Topologici

Definizione 17 *Un insieme* X *è detto* ***spazio topologico*** *se esiste una famiglia di sottoinsiemi* $\mathcal{U}$ *tale che:*

1. $\emptyset \in \mathcal{U}$, $X \in \mathcal{U}$;
2. *l'unione di insiemi appartenenti ad* $\mathcal{U}$ *appartiene ancora ad* $\mathcal{U}$;
3. *l'intersezione di un numero finito di insiemi appartenenti ad* $\mathcal{U}$ *appartiene ancora ad* $\mathcal{U}$.

Gli insiemi $U_i \in \mathcal{U}$ sono detti **aperti** e definiscono la topologia T sull'insieme X; differenti famiglie di aperti $\mathcal{U}$ definiscono differenti topologie; si può definire una struttura topologica su di un insieme arbitrario X considerando come aperti tutti i suoi sottoinsiemi ottenendo in questo modo una topologia detta **discreta**. Una famiglia $\mathcal{V}$ di insiemi aperti definisce una **base** dello spazio topologico se ogni insieme della famiglia $\mathcal{U}$ è esprimibile come unione di insiemi appartenenti alla base, quindi una base è tale se:

1. $\emptyset \in \mathcal{V}$;
2. l'intersezione di un numero finito di insiemi appartenenti a $\mathcal{V}$ è l'unione di insiemi appartenenti a $\mathcal{V}$;
3. l'unione di tutti gli insiemi di $\mathcal{V}$ è X.

Esempio 9 1. *Uno spazio topologico* X *è munito della* ***topologia banale*** *se* $\mathcal{U} = \{\emptyset, X\}$;

2. *Un sottoinsieme* V *di uno spazio topologico* X *è munito della* ***topologia indotta*** *da* X *se si assume come base l'insieme delle intersezioni tra gli insiemi (aperti) di una base di* X *e l'insieme* V*, equivalentemente, assumendo come aperti di* V *le sue intersezioni con gli aperti di* X;

3. *Possiamo strutturare lo spazio vettoriale* $\mathbb{R}^n$ *a spazio topologico utilizzando una topologia detta* ***naturale*** *scegliendo come base la famiglia di parallelepipedi aperti* $a_i < x_i < b_i$ *con* $x = (x_1, x_2, ..., x_n) \in \mathbb{R}^n$ *e l'insieme vuoto. Utilizzando la topologia naturale di* $\mathbb{R}^{2n}$*, possiamo strutturare* $\mathbb{C}^n$ *con la topologia naturale, tenendo presente che* $\mathbb{C}^n$ *e* $\mathbb{R}^{2n}$ *sono* $\mathbb{R}$*-spazi vettoriali isomorfi.*

Negli spazi topologici si possono definire le seguenti nozioni:

1. un **intorno** $U(x)$ è un aperto contenente x;
2. un insieme **chiuso** è un complementare[1] di un insieme aperto;
3. la **chiusura** di un insieme M (indicata con $\overline{M}$) è l'intersezione di tutti gli insiemi chiusi contenenti l'insieme dato;
4. un punto di X è un **punto di aderenza** se ogni suo intorno contiene almeno un punto di X;
5. un insieme M si dice **denso** in X se $\overline{M} = X$;
6. uno spazio X è **separabile** se esiste un sottoinsieme al più numerabile e denso in X.

Una funzione f da uno spazio topologico X in uno spazio topologico Y si dice **continua nel punto** x_0 se l'immagine inversa di ogni intorno $V(y_0)$, dove $y_0 = f(x_0)$, contiene un intorno di x_0; f, inoltre, è detta **continua** se è continua in ogni punto di X. È facile osservare che f è continua se e solo se la controimmagine di ogni aperto di Y è un aperto di X.

Un'applicazione f dallo spazio X allo spazio Y è detta **omeomorfismo** se è biettiva e se f e f^{-1} sono continue. Un omeomorfismo conserva le **proprietà topologiche** di un insieme, cioé manda aperti in aperti, chiusi in chiusi, chiusure in chiusure.

Definizione 18 *Uno spazio topologico X si dice* ***separato*** *o* ***spazio di Hausdorff*** *se, per ogni coppia $(x, y) \in X \times X$, esistono un intorno di x ed un intorno di y che non si intersecano.*

In uno spazio di Hausdorff il limite di una successione di elementi in X, se esiste è unico.

Dati n spazi topologici X_i possiamo definire uno spazio topologico ponendo $X = X_1 \times X_2 \times ... \times X_n$; X si può munire della topologia indotta dagli spazi X_i, considerando come base di X il prodotto cartesiano delle basi delle componenti X_i; X si dice **spazio topologico prodotto**.

3.3 I Gruppi Topologici

Definizione 19 *Un* ***Gruppo Topologico*** *G è uno spazio topologico che possiede una struttura di gruppo ed in cui la funzione $f : (g, h) \in G \times G \to gh^{-1} \in G$ è continua.*

Ponendo $g = e$ si ottiene che $f(e, h) = h^{-1}$, sicché ola funzione $i : h \in G \to h^{-1} \in G$ è continua, ciò significa che un elemento in un intorno di h ha

[1]Dato un insieme F si definisce complementare del sottoinsieme A il sottoinsieme $B = F - A$, intendendo con questa scrittura l'insieme dei punti che appartengono a F e che non appartengono a A.

l'inverso in un intorno di h^{-1}. Inoltre, sfruttando la continuità di i, si ottiene la continuità dell'operazione di moltiplicazione fra gli elementi del gruppo: $f(g, h^{-1}) = f(g, f(e, h)) = f^*(g, h) = gh$.

Ogni gruppo può essere banalmente strutturato a gruppo topologico, munendolo della topologia discreta. Poiché l'applicazione $i : g \in G \to g^{-1}$ è continua abbiamo che se $U(e)$ è un intorno dell'unità allora lo sará anche U^{-1} $(i(e) = e)$.

In un gruppo topologico la **traslazione destra** (**sinistra**) $g \to gg_0$ $(g \to g_0 g)$ è un omeomorfismo di G su G; ciò significa che, se $\mathcal{V}(g)$ è una base di intorni dell'elemento g, allora $\mathcal{V}(g)g_0$ $(g_0\mathcal{V}(g))$ è una base di intorni dell'elemento gg_0 $(g_0 g)$; in particolare avremo che, fornendo una base di intorni dell'elemento neutro, avremmo una base di intorni di un qualsiasi elemento del gruppo cioé la topologia di un gruppo topologico è completamente definita assegnando una base di intorni dell'identità.

Esempio 10 *1.* $GL(n, \mathbb{R})$ *(*$GL(n, \mathbb{C})$*) è il gruppo degli invertibili dell'anello* $\mathbb{M}_n(\mathbb{R})$ *(*$\mathbb{M}_n(\mathbb{C})$*) delle matrici* $n \times n$ *su* $\mathbb{R}$ *(*$\mathbb{C}$*). Poiché* $\mathbb{M}_n(\mathbb{R})$ *(*$\mathbb{M}_n(\mathbb{C})$*) è un* $\mathbb{R}$*-spazio vettoriale di dimensione* n^2 *(*$2n^2$*), esso è isomorfo a* $\mathbb{R}^{n^2}$ *(*$\mathbb{R}^{2n^2}$*) ed è pertanto munito della topologia prodotto indotta dalla topologia naturale di* $\mathbb{R}$ *(*$\mathbb{C}$*). Pertanto* $GL(n, \mathbb{R})$ *(*$GL(n, \mathbb{C})$*) resta munito della topologia indotta di* $\mathbb{M}_n(\mathbb{R})$ *(*$\mathbb{M}_n(\mathbb{C})$*). Infine si può facilmente verificare che* $GL(n, \mathbb{R})$ *(*$GL(n, \mathbb{C})$*) è un gruppo topologico.*

Un sottogruppo è detto **chiuso** se è un sottoinsieme chiuso di G.

Un gruppo topologico è detto **lineare** se è isomorfo ad un sottogruppo di $GL(n, \mathbb{C})$ o di $GL(n, \mathbb{R})$.

Dato un gruppo topologico G ed un sottogruppo H, possiamo strutturare H come sottogruppo topologico attraverso la topologia indotta da G; lo spazio quoziente $G/\mathcal{R}_H^R$ può essere strutturato anch'esso a spazio topologico attraverso l'epimorfismo canonica $\phi : G \to G/\mathcal{R}_H^R$, imponendo che ϕ sia una funzione continua; ciò significa che gli aperti di $G/\mathcal{R}_H^R$ sono le immagini, mediante ϕ, degli aperti di G.

Proposizione 45 *Se* H *è un sottogruppo chiuso allora lo spazio quoziente* $G/\mathcal{R}_H^R$ *è separato.*

Dimostrazione. Presi due laterali destri $\{g_1\} = Hg_1$ e $\{g_2\} = Hg_2$ appartenenti a $G/\mathcal{R}_H^R$ con $\{g_1\} \neq \{g_2\}$ si ha che $g_1^{-1}g_2 \notin H$. Essendo H chiuso esiste un intorno U di $g_1^{-1}g_2$ tale che $U \cap H = \emptyset$; essendo continua la funzione $f(g, h) = g^{-1}h$ esistono due intorni U_1 e U_2, rispettivamente di g_1 e g_2, tali che $U_1^{-1}U_2 \subset U$; $\widetilde{U}_1 = \phi(U_1)$ e $\widetilde{U}_2 = \phi(U_2)$, dove ϕ è l'omomorfismo canonico, sono intorni rispettivamente delle classi $\{g_1\}$ e $\{g_2\}$; per dimostrare la separabilità di $G/\mathcal{R}_H^R$ basta notare che $\widetilde{U}_1 \cap \widetilde{U}_2 = \emptyset$ infatti, se così non fosse, presi $g_0, g_0' \in \{g_0\} \in \widetilde{U}_1 \cap \widetilde{U}_2$, si avrebbe $g_0^{-1}g_0' = g_0^{-1}(g_0 h) = h \in H$ in contraddizione col fatto che $U \cap H = \emptyset$. ■

Proposizione 46 *Se* H *è un sottogruppo normale chiuso allora* G/H *è un sottogruppo topologico di Hausdorff.*

Dimostrazione. Dal fatto che H è normale discende che G/H è un sottogruppo, mentre dalla chiusura segue che è anche separato; imponendo la continuità dell'epimorfismo canonico otteniamo che è possibile strutturare il gruppo quoziente G/H a gruppo topologico. ■

Se G e K sono gruppi topologici, un'applicazione f di G in K è detta **omomorfismo continuo** se:

1. f è continua;
2. f è un omomorfismo di G in K.

Proposizione 47 *Sia f un omomorfismo continuo di G in K e $N = Ker(f)$, allora:*

1. *N è un sottogruppo normale chiuso;*
2. *$f = \psi\phi$ dove ϕ è l'omomorfismo canonico e ψ è un isomorfismo continuo di G/N in K.*

Inoltre, se f è aperta (manda aperti in aperti), ψ è un **isomorfismo topologico** (perché conserva le proprietà topologiche), da cui si ha che G/N e $f(G)$ sono topologicamente isomorfi (omeomorfi).

3.3.1 Gruppi Compatti

Definizione 20 *Sia X uno spazio topologico, allora una famiglia $\mathcal{F}$ di sottoinsiemi di X è detta **ricoprimento aperto (chiuso)** di un sottoinsieme M di X se l'unione di tutti gli insiemi aperti (chiusi) di $\mathcal{F}$ contiene M.*

Definizione 21 *Un sottoinsieme di uno spazio topologico X ,in particolare uno spazio topologico, è detto **compatto** se da ogni suo ricoprimento aperto $\mathcal{F}$ se ne può estrarre uno contenente un numero finito di insiemi.*

Proposizione 48 *Un insieme compatto di uno spazio separato è chiuso.*

Proposizione 49 *Un insieme $M \subset \mathbb{R}^n$ è compatto se e solo se è chiuso e limitato in $\mathbb{R}^n$.*

Proposizione 50 *Un sottospazio chiuso M di uno spazio topologico compatto X è compatto.*

Proposizione 51 *Un'applicazione continua manda insiemi compatti in insiemi compatti.*

Proposizione 52 *Un'applicazione continua da uno spazio compatto in uno separato manda chiusi in chiusi.*

Proposizione 53 *Il prodotto topologico di spazi topologici compatti è uno spazio topologico compatto.*

Definizione 22 *Uno spazio X si dice **localmente compatto** se ogni punto $x \in X$ possiede un intorno, la cui chiusura è compatta.*

Definizione 23 *Un gruppo topologico G è* ***compatto*** *se lo è lo spazio topologico G.*

Proposizione 54 *Ogni sottogruppo chiuso di un gruppo compatto è compatto.*

Un gruppo topologico G è **localmente compatto** se esiste un intorno U dell'elemento neutro la cui chiusura è compatta.

Una funzione f da un gruppo topologico G al gruppo topologico $\mathbb{C}^n$ munito della topologia naturale si dice **uniformemente continua** su G se per ogni $\epsilon > 0$ esiste un intorno U dell'elemento neutro di $\mathbb{C}^n$ tale che: $|f(g_1) - f(g_2)|_{\mathbb{C}^n} < \epsilon$ per $g_2, g_1 \in U$.

Proposizione 55 *Ogni funzione continua su un gruppo localmente compatto è uniformemente continua.*

3.3.2 Gruppi Connessi

Definizione 24 *Due sottoinsiemi $M, N \subset X$ sono una* ***partizione*** *di X se $M \cup N = X$, $M \cap N = \emptyset$ e $M, N \neq \emptyset$.*

Definizione 25 *Uno spazio topologico X è* ***connesso*** *se non esiste una sua partizione fatta da insiemi chiusi.*

Un insieme aperto connesso è detto **dominio**.

Proposizione 56 *Funzioni continue mandano insiemi connessi in insiemi connessi.*

Dimostrazione. Data $Y = f(X)$ una funzione continua e X uno spazio connesso e presa una partizione di Y fatta da F_1 e F_2 chiusi, allora avremo X sarebbe l'unione delle immagini inverse, tramite f, di F_1 e F_2 che sarebbero due insiemi chiusi (funzioni continue mandano chiusi in chiusi) in contraddizione con la connessione di X. ■

Proposizione 57 *L'unione di una famiglia di insiemi connessi aventi un punto in comune è un insieme connesso.*

Il più grande insieme connesso contenente $x \in X$ è detto **componente connessa** di x.

Proposizione 58 *Ogni componente connessa è chiusa.*

Proposizione 59 *Se ogni coppia di punti appartenenti ad X può essere connessa da una curva*[2] *continua contenuta in X, allora X è connesso;*

Proposizione 60 *Il prodotto topologico di spazi connessi è uno spazio topologico connesso.*

[2] Una curva continua su uno spazio topologico X è una funzione continua dallo spazio topologico $\mathbb{R}$, dotato della topologia naturale, e X.

Uno spazio topologico è l'unione disgiunta delle sue componenti connesse.

Definizione 26 *Un gruppo topologico G è* ***connesso*** *se lo è lo spazio topologico.*

Proposizione 61 *La componente connessa dell'identità è un sottogruppo normale chiuso di G.*

Proposizione 62 *La componente connessa di ogni elemento $g \in G$ è il laterale $gK = Kg$ dove K è la componente connessa di g ($K = G$ se e solo se G è connesso).*

3.4 Varietà differenziabili

Ricordiamo che si definisce **omeomorfismo** dallo spazio topologico X allo spazio topologico Y un'applicazione $f : U \to V$ tra due aperti, dove $U \subset X$ e $V \subset Y$, invertibile e continua con la sua inversa.

Definizione 27 *Un'applicazione $f : \mathbb{R}^n \to \mathbb{R}^n$ è detta* ***diffeomorfismo*** *di classe C^k se tutte le sue derivate parziali di ordine l $(0 \leq l \leq k)$ sono omeomorfismi.*

Definizione 28 *Una* ***varietà differenziabile*** n***-dimensionale*** *è uno spazio topologico di Hausdorff X tale che:*

1. *esiste una famiglia di aperti $\mathcal{U}$ che costituiscono un ricoprimento di X;*
2. *esiste un omeomorfismo $\phi_i : U_i \to \mathbb{R}^n$ per ogni $U_i \in \mathcal{U}$;*
3. *per ogni coppia di carte (U_i, ϕ_i) e (U_j, ϕ_j) per cui $U_i \cap U_j \neq \emptyset$, $\phi_i \circ \phi_j^{-1} : \phi_j(U_i \cap U_j) \subset \mathbb{R}^n \to \phi_i(U_i \cap U_j) \subset \mathbb{R}^n$ è un diffeomorfismo di classe C^k.*

La coppia (U_i, ϕ_i) si dice **carta** e ϕ_i **applicazione coordinata**. Una collezione di carte i cui domini costituiscono un ricoprimento aperto di X forma un'**atlante** α. L'applicazione ϕ associa ad ogni punto della varietà un punto su $\mathbb{R}^n$ permettendo così di descrivere localmente una qualsiasi varietà utilizzando coordinate in $\mathbb{R}^n$.

La coppia $V_n = (X, \alpha)$ è una **varietà differenziabile n-dimensionale**.

Su una varietà differenziabile V_n una **funzione** $f : V_n \to \mathbb{R}$ si dice di classe C^h, cioé differenziabile fino all'ordine $h < k$, se è tale l'applicazione $f \circ \phi^{-1} : \phi(U) \subset \mathbb{R}^n \to \mathbb{R}$; inoltre una **curva** di classe C^h sulla varietà è un'applicazione $\gamma : [a, b] \subset \mathbb{R} \to V_n$ tale che $\phi \circ \gamma : [a, b] \to \mathbb{R}^n$ sia di classe C^h.

Un'applicazione $F : V_n \to V_m$ è detta di classe C^h se tale risulta la funzione $\psi \circ F \circ \phi^{-1} : \phi(U) \subset \mathbb{R}^n \to \psi(V) \subset \mathbb{R}^m$, dove (U, ϕ) e $(V \psi)$ sono due carte rispettivamente di V_n e V_m.

Esempio 11 *Una sfera tridimensionale di raggio r è una varietà bidimensionale che, immersa in uno spazio tridimensionale può essere definita dall'equazione*

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - r^2 = 0$$

Con questa descrizione della varietà non è possibile descrivere in modo intrinseco (non considerando lo spazio in cui la varietà è immersa) la sfera, per fare *ciò possiamo descriverla tramite delle coordinate, α e β, sulla superficie stessa e l'applicazione coordinata ϕ*

$$x_1 = rsin\alpha cos\beta$$
$$x_2 = rsin\alpha sin\beta$$
$$x_3 = rcos\alpha$$

introducendo così una carta sull'aperto $U = (0, 2\pi) \times (0, \pi)$. È necessaria una seconda carta definita in un modo simile nella parte della sfera in cui c'è ambiguità nella descrizione (per $\alpha = 0$ β può assumere un qualsiasi valore).

3.4.1 Spazi Vettoriali Tangenti

Indicando con $\mathcal{F}^1(M)$ l'insieme dele funzioni di classe C^1 sulla varietà M, definiamo **vettore tangente** alla curva γ nel punto $x = \gamma(t_0)$ l'applicazione

$$\mathbf{X}_x : \mathcal{F}^1(x) \to \mathbb{R} \tag{3.5}$$

tale che

$$\mathbf{X}_x f = \frac{d}{dt}\left[(f \circ \gamma)(t)\right]_{t_0} \tag{3.6}$$

$\mathbf{X}_x$ è quindi un operatore di *derivazione direzionale*, che possiamo esplicitare nel seguente modo:

$$\mathbf{X}_x f = \frac{d}{dt}\left[(f \circ \phi^{-1} \circ \phi \circ \gamma)(t)\right]_{t_0} = \frac{\partial}{\partial x^i}\left(f \circ \phi^{-1}\right)_{\phi(x)} \left(\frac{dx^i}{dt}\right)_{t_0}. \tag{3.7}$$

Proposizione 63

$$\left(\frac{\partial}{\partial x^i}\right)_x f = \frac{\partial}{\partial x^i}(f \circ \phi^{-1})_{\phi(x)} \tag{3.8}$$

definiscono n vettori indipendenti.

Dimostrazione. Consideriamo una combinazione lineare dei vettori

$$\lambda^i \frac{\partial}{\partial x^i} = \mathbf{0}$$

che applichiamo alla funzione proiezione i-esima che restituisce la componente i-esima del vettore su $\mathbb{R}$ ottenendo

$$0 = \lambda^i \left(\frac{\partial}{\partial x^i}\right)(pr^j \circ \phi) = \lambda^i \left(\frac{\partial x^j}{\partial x^i}\right) = \lambda^j$$

■

Da quanto appena dimostrato si ottiene che possiamo scrivere un generico vettore, in modo unico, come

$$\mathbf{X}_x = X^i \frac{\partial}{\partial x^i} \tag{3.9}$$

con $X^i = \left.\frac{dx^i}{dt}\right|_{t_0}$, definendo così una base detta **base olonoma**.

Gli **spazi vettoriali tangenti** (T_xV_n) sono sempre relativi al punto, in quanto solo nel caso in cui la varietà differenziale sia $\mathbb{R}^n$ potremo definire un unico spazio tangente indipendentemente dal punto [3].

Il duale di T_xV_n, cioé lo **spazio vettoriale cotangente** $T_x^*V_n$, si può dotare di una base definita dalla condizione

$$(\mathbf{\Theta}^i)_x\mathbf{X}_x = X^i \tag{3.10}$$

Definiamo **differenziale** di $f \in \mathcal{F}^1(M)$, che indichiamo con $(df)_x$, l'applicazione $(df)_x : T_xV_n \to \mathbb{R}$ tale che

$$(df)_x(\mathbf{X}_x) = \mathbf{X}_x f = \frac{\partial}{\partial x^i}(f \circ \phi^{-1})_{\phi(x)} \left(\frac{dx^i}{dt}\right)_{t_0} = a_i X^i \tag{3.11}$$

dove $a_i = (\frac{\partial}{\partial x^i}(f \circ \phi^{-1}))_{\phi(x)}$. Essendo $(df)_x = \frac{\partial f \circ \phi^{-1}}{\partial x^i} dx^i = a_i dx^i$ otteniamo che una base di $T_x^*V_n$ è formata dagli n covettori indipendenti dx^i.

Definiamo **campo vettoriale X** sulla varietà differenziabile l'applicazione

$$\mathbf{X} : x \in V_n \to \mathbf{X}_x \in T_xV_n \tag{3.12}$$

che esplicitando è

$$\mathbf{X} = X^i(x)\frac{\partial}{\partial x^i} \tag{3.13}$$

Il campo vettoriale è quindi definito *indipendentemente dal punto* sulla varietà ed è un operatore lineare che agisce nel seguente modo. $(\mathbf{X}f)(x) = \mathbf{X}_x f$. I campi vettoriali formano un'algebra di Lie coll'introduzione del commutatore

$$[\mathbf{X}, \mathbf{Y}] = \mathbf{XY} - \mathbf{YX} = X^j\frac{\partial}{\partial x^j}(Y^i\frac{\partial}{\partial x^i}) - Y^j\frac{\partial}{\partial x^j}(X^i\frac{\partial}{\partial x^i}) =$$

$$= (X^j\frac{\partial Y^i}{\partial x^j} - Y^j\frac{\partial X^i}{\partial x^j})\frac{\partial}{\partial x^i} \tag{3.14}$$

3.5 I Gruppi di Lie

Definizione 29 *Un gruppo astratto G è un gruppo di Lie se*

1. *G è una varietà differenziabile;*

2. *l'applicazione $f(x, y) \to xy^{-1}$ è differenziabile.*

La condizione 2 è equivalente a dire che l'applicazione $x \to x^{-1}$ è differenziabile ed anche che lo è l'applicazione $(x, y) \to xy$, in quanto basta porre $x = e$ nel primo caso, mentre nel secondo basta sfruttare la differenziabilitá dell'applicazione $x \to x^{-1}$.

Un gruppo di Lie è un gruppo topologico rispetto alla struttura topologica indotta dalla sua struttura analitica [4].

[3] L'applicazione coordinata sarebbe $x^i = t^i$, da cui si ottiene $X^i = 1$.

[4] La varietá differenziabile è stata definita come uno spazio topologico di Hausdorff.

Proposizione 64 *Un gruppo di Lie è localmente compatto in quanto la varietà, attraverso l'applicazione coordinata, è localmente euclidea* [5].

Dimostrazione. L'applicazione coordinata è continua, per definizione, e, come tale, manda insiemi compatti in insiemi compatti; un'applicazione continua da uno spazio compatto ($\mathbb{R}^m$) in uno spazio separato (la varietà) manda chiusi in chiusi; dal fatto che un insieme chiuso in uno spazio separato è compatto otteniamo un isomorfismo, tramite l'applicazione canonica, che manda chiusi compatti in chiusi compatti, cioé un isomorfismo tra spazi localmente compatti.[6] ∎

Teorema 65 *Un gruppo topologico localmente euclideo è isomorfo ad un gruppo di Lie.*

Ogni gruppo di Lie complesso di dimensione n può essere trattato come un gruppo di Lie reale $2n-$dimensionale.

Un sottogruppo $H < G$ è un gruppo di Lie se H è una sottovarietà[7].

L'omomorfismo analitico $t \in \mathbb{R} \to x(t) \in G$, dove G è un gruppo di Lie, definisce un **sottogruppo ad un parametro**.

Teorema 66 *Un gruppo topologico localmente compatto è un gruppo di Lie se esiste un'isomorfismo continuo da G in un sottogruppo di $GL(n, \mathbb{R})$.*

Consideriamo una base del campo vettoriale tangente alla varietá differenziale V_n nell'unità, $X_1, X_2, ..., X_n$ (detti **generatori**), avremo allora che ogni vettore del campo sará esprimibile come combinazione lineare della base

$$A = \sum_i^n a^i X_i$$

ed il commutatore di due campi vettoriali sará dato:

$$C = c^i X_i = [A, B] = [a^j X_j, b^k X_k] = a^j b^k [X_j, X_k] \tag{3.15}$$

Da questa relazione si possono definire le costanti di struttura

$$c^i_{jk} X_i = [X_j, X_k]. \tag{3.16}$$

che definiscono un'**algebra di Lie** sui generatori del gruppo di Lie; gruppi di Lie a cui si può associare la medesima algebra di Lie sono detti **localmente isomorfi**.

L'algebra di Lie associata ad un gruppo di Lie è una descrizione del gruppo nelle vicinanze dell'unità.

Lo studio di un gruppo di Lie viene effettuato solo sulla componente connessa all'unità, in quanto si vuole descrivere il gruppo tramite curve continue e differenziabili[8] connesse con l'unità[9].

Se tutti gli elementi di un gruppo sono punti in una regione finita della varietà allora il gruppo è compatto.

---

[5] Lo spazio euclideo $\mathbb{R}^m$ è localmente compatto.

[6] Si sono utilizzate alcune affermazioni che si trovano nel paragrafo sui gruppi compatti.

[7] Una sottovarietà è un sottospazio topologico della varietà strutturato anch'esso a spazio topologico di Hausdorff tramite la topologia indotta.

[8] Da ciò discende la possibilità di utilizzare trasformazioni infinitesime sul gruppo.

[9] Ciò è dovuto al fatto che vogliamo descrivere un gruppo che, quindi, deve possedere l'unità; data una curva $A(t)$ che descriva, ad esempio, un sottogruppo, vi deve essere un $t = t_0$ tale che $A(t_0) = I$, dove I è l'unità.

Teorema 67 *Fra tutti i gruppi aventi la stessa algebra di Lie ce ne è uno solo semplicemente connesso*[10] *detto* ***gruppo di ricoprimento universale****.*

Proposizione 68 *Sia G un gruppo di Lie semplicemente connesso, L la sua algebra di Lie, M un ideale di L e H il sottogruppo relativo a M allora H è un sottogruppo invariante chiuso di G.*

[10] Un varietà è semplicemente connessa se ogni curva chiusa è riducibile con continuità ad un punto.

Capitolo 4

I Gruppi di Trasformazione

4.1 I Gruppi di Trasformazione

Data una varietà differenziabile V_n, una funzione $F : V_n \to V_n$ è un diffeomorfismo di classe C^r [1] se $\phi_i \circ F \circ \phi_j^{-1}$ è un diffeomorfismo di classe C^r, dove ϕ_j e ϕ_i sono le applicazioni coordinate, rispettivamente, di un aperto U_j e dell'aperto U_i immagine, tramite F di U_j. I diffeomorfismi formano un gruppo rispetto alla composizione di applicazioni denotato con $Diff(V_n)$.

Consideriamo un gruppo di Lie G ed un omomorfismo continuo

$$f : \alpha \in G \mapsto f_\alpha \in Diff(V_n)$$

tale che

$$f_1 = id_{V_n} \qquad f_\alpha \circ f_\beta = f_{\alpha\beta} \qquad (\alpha, \beta \in G)$$

cioé un'azione del gruppo G su V_n, allora f è detto **gruppo di trasformazioni**.

Di seguito useremo anche la notazioni $f(\alpha, x) \equiv f_\alpha(x)$, con $x \in V_n$; la composizione con la precedente notazione è esplicitabile nel seguente modo

$$f_\alpha \circ f_\beta(x) = f(f(x, \beta), \alpha) = f(x, \phi(\alpha, \beta)) = f_\phi(x) \tag{4.1}$$

dove l'applicazione

$$\phi : (\alpha, \beta) \in G \times G \to G$$

è la legge di composizione interna del gruppo ($\phi(\alpha, \beta) \equiv \alpha\beta \in G$).

4.2 I Generatori

L'applicazione $\alpha \to f_\alpha(x_0)$ definisce un **orbita** contenuta in V_n e passante per x_0; il campo vettoriale tangente all'orbita del gruppo, equivalentemente al caso di una curva, si dice generatore infinitesimale ed è sempre dato da (3.7)

$$X_x = \left.\frac{\partial F(f(x_0, \alpha))}{\partial \alpha^i}\right|_{\alpha=1} = \left.\frac{\partial f^j(x_0, \alpha)}{\partial \alpha^i}\right|_{\alpha=1} \left.\frac{\partial}{\partial x^j} F\right|_{f(x_0,1)}.$$

[1] Un'applicazione f di classe C^r è un'applicazione differenziabile r volte e tale che la derivata k-esima, con $k \leq r$, sia continua con la sua inversa.

Un punto sulla varietà V_n, facendo uso di un gruppo di trasformazioni, è esprimibile in due modi:

$$x = f(x_0, \alpha) \qquad x = f(x, 1)$$

Poiché siamo interessati al gruppo nelle vicinanze dell'unità, useremo la seconda forma da cui otteniamo che un punto infinitamente vicino ad x è esprimibile come

$$x + dx = f(x, \delta\alpha) \tag{4.2}$$

dove dx rappresenta un incremento infinitesimo rispetto ad un punto $x \neq 0$, $\delta\alpha$ invece rappresenta un incremento infinitesimo rispetto all'unità ($\alpha = 1$).

Dalla (4.2) e dallo sviluppo di Taylor di f al primo ordine rispetto a $\delta\alpha$ ($f(x, \delta\alpha) \to f(x, 1) + \frac{\partial f(x,\alpha)}{\partial \alpha^\sigma}|_{\alpha=1}\delta\alpha^\sigma$) otteniamo

$$dx^i = \left.\frac{\partial f^i(x, \alpha)}{\partial \alpha^\sigma}\right|_{\alpha=1} \delta\alpha^\sigma = u^i_\sigma(x)\delta\alpha^\sigma. \tag{4.3}$$

dove sono stati esplicitati gli indici. Gli $u^i_\sigma(x)$ corrispondono alle componenti dei generatori infinitesimali, quindi avremo che il campo associato al gruppo di trasformazione determinato da f è:

$$X_\sigma = u^i_\sigma(x)\frac{\partial}{\partial x^i} \tag{4.4}$$

Consideriamo ora il gruppo di Lie G.

$$\alpha^\rho + d\alpha^\rho = \phi^\rho(\alpha, \delta\beta) = \phi^\rho(\alpha, 1) + \left.\frac{\partial \phi^\rho(\alpha, \beta)}{\partial \beta^\tau}\right|_{\beta=1} \delta\alpha^\tau \tag{4.5}$$

dove è stato sostituito $\delta\beta$ con $\delta\alpha$ in quanto sono entrambi un incremento infinitesimo su G ed è stata sostituita $\phi(\alpha, \delta\beta)$ con il suo sviluppo al primo ordine rispetto a $\delta\beta$. Dalla (4.5) otteniamo, allo stesso modo del caso precedente, il campo su G

$$X_\sigma(\alpha) = \Theta^\rho_\sigma(\alpha)\frac{\partial}{\partial \alpha^\rho} \tag{4.6}$$

dove $\Theta^\rho_\sigma(\alpha) = \frac{\partial \phi^\rho(\alpha,\beta)}{\partial \beta^\sigma}|_{\beta=1}$.

C'è da notare che il numero di generatori su V_n è determinato dalla dimensione dell'algebra di Lie di G quindi in generale le matrici u^i_σ sono rettangolari a differenza delle matrici Θ^ρ_τ che sono quadrate e, per le proprietá gruppali, invertibili.

Dalla (4.5) otteniamo anche la relazione

$$\delta\alpha^\sigma = \Psi^\sigma_\rho d\alpha^\rho \tag{4.7}$$

dove Ψ^σ_ρ è la matrice inversa di Θ^ρ_τ.

4.3 Dal gruppo all'algebra di Lie

Dalle relazioni (4.3) e (4.7) otteniamo

$$dx^i = u^i_\sigma(x)\Psi^\sigma_\tau(\alpha)d\alpha^\tau$$

cioé il **primo teorema di Lie** esprimibile anche nel seguente modo

$$\frac{\partial x^i}{\partial \alpha^\tau} = u^i_\sigma(x)\Psi^\sigma_\tau(\alpha). \tag{4.8}$$

Perché questo sistema di equazioni lineari abbiano una soluzione unica deve essere verificata la condizione

$$\frac{\partial^2 x^i}{\partial \alpha^\sigma \partial \alpha^\lambda} = \frac{\partial^2 x^i}{\partial \alpha^\lambda \partial \alpha^\sigma}.$$

Questa condizione puó essere riscritta usando la (4.8)

$$\frac{\partial}{\partial \alpha^\sigma}\left(u^i_\rho(x)\Psi^\rho_\lambda(\alpha)\right) = \frac{\partial}{\partial \alpha^\lambda}\left(u^i_\rho(x)\Psi^\rho_\sigma(\alpha)\right) \tag{4.9}$$

usando lo sviluppo

$$\frac{\partial u^i_\rho(x)}{\partial \alpha^\sigma} = \frac{\partial u^i_\rho(x)}{\partial x^j}\frac{\partial x^j}{\partial \alpha^\sigma} = \Psi^\lambda_\sigma(\alpha)u^j_\lambda(x)\frac{\partial u^i_\rho(x)}{\partial x^j}$$

otteniamo

$$\frac{\partial}{\partial \alpha^\sigma}(u^i_\rho \Psi^\rho_\lambda) = \Psi^\tau_\sigma u^j_\tau \frac{\partial u^i_\rho}{\partial x^j}\Psi^\rho_\lambda + u^i_\rho \frac{\partial \Psi^\rho_\lambda}{\partial \alpha^\sigma}$$

e

$$\frac{\partial}{\partial \alpha^\lambda}(u^i_\rho \Psi^\rho_\sigma) = \Psi^\tau_\lambda u^j_\tau \frac{\partial u^i_\rho}{\partial x^j}\Psi^\rho_\sigma + u^i_\rho \frac{\partial \Psi^\rho_\sigma}{\partial \alpha^\lambda} = \Psi^\rho_\lambda u^j_\rho \frac{\partial u^i_\tau}{\partial x^j}\Psi^\tau_\sigma + u^i_\rho \frac{\partial \Psi^\rho_\sigma}{\partial \alpha^\lambda}$$

infine sottraendo la prima alla seconda ricaviamo

$$\Psi^\tau_\sigma \Psi^\rho_\lambda \left[u^j_\tau \frac{\partial u^i_\rho}{\partial x^j} - u^j_\rho \frac{\partial u^i_\tau}{\partial x^j}\right] = \left[\frac{\partial \Psi^\rho_\sigma}{\partial \alpha^\lambda} - \frac{\partial \Psi^\rho_\lambda}{\partial \alpha^\sigma}\right]u^i_\rho. \tag{4.10}$$

Sfruttando l'invertibilitá delle Ψ

$$\left[u^j_\mu \frac{\partial u^i_\nu}{\partial x^j} - u^j_\nu \frac{\partial u^i_\mu}{\partial x^j}\right] = \Theta^\sigma_\mu \Theta^\lambda_\nu \left[\frac{\partial \Psi^\rho_\sigma}{\partial \alpha^\lambda} - \frac{\partial \Psi^\rho_\lambda}{\partial \alpha^\sigma}\right]u^i_\rho. \tag{4.11}$$

Seguendo il medesimo ragionamento, ma partendo dalla relazione $d\beta^i = \Theta^i_\sigma(\beta)\Psi^\sigma_\tau d\alpha^\tau$ ottenuta dalla (4.7) e dalla sua equivalente rispetto a β ($d\beta^i = \Theta^i_\nu \delta\beta^\nu = \Theta^i_\nu \delta\alpha^\nu$), otteniamo

$$\Theta^j_\mu(\beta)\frac{\partial \Theta^i_\nu(\beta)}{\partial \beta^j} - \Theta^j_\nu(\beta)\frac{\partial \Theta^i_\mu(\beta)}{\partial \beta^j} = \Theta^\sigma_\mu(\alpha)\Theta^\lambda_\nu(\alpha)\left[\frac{\partial \Psi^\rho_\sigma(\alpha)}{\partial \alpha^\lambda} - \frac{\partial \Psi^\rho_\lambda(\alpha)}{\partial \alpha^\sigma}\right]\Theta^i_\rho(\beta). \tag{4.12}$$

da cui, sfruttando l'invertibilitá di $\Theta^i_\rho(\beta)$, possiamo separare α da β, quindi è possibile porre il membro in parentesi quadre uguale ad una costante (indipendente anche da x in quanto non compare nell'equazione); otteniamo cosí le due relazioni

$$\left[u^j_\mu \frac{\partial u^i_\nu}{\partial x^j} - u^j_\nu \frac{\partial u^i_\mu}{\partial x^j}\right] = C^\rho_{\mu\nu}u^i_\rho. \tag{4.13}$$

$$\left[\Theta^j_\mu \frac{\partial\Theta^i_\nu}{\partial\alpha^j} - \Theta^j_\nu \frac{\partial\Theta^i_\mu}{\partial\alpha^j}\right] = C^\rho_{\mu\nu}\Theta^i_\rho. \tag{4.14}$$

che, passando dalle componenti dei generatori ai generatori stessi del gruppo, possiamo riscrivere tramite le due seguenti relazioni di commutazione (**secondo teorema di Lie**):

$$[X_\mu(x), X_\nu(x)] = C^\rho_{\mu\nu} X_\rho(x) \tag{4.15}$$

$$[X_\mu(\alpha), X_\nu(\alpha)] = C^\rho_{\mu\nu} X_\rho(\alpha) \tag{4.16}$$

Quindi abbiamo dimostrato che i generatori del gruppo di trasformazioni sulla varietá V_n ed i campi dell'algebra di Lie del gruppo G sono la medesima algebra di Lie.

4.4 Trasformazioni Infinitesime

Consideriamo un operatore unitario

$$U = e^{itX}$$

dove X è un operatore hermitiano in quanto si ha

$$0 = \left.\frac{d(UU^\dagger)}{dt}\right|_{t=0} = iX - iX^\dagger$$

Questo è un gruppo di trasformazioni ad un parametro isomorfo al gruppo additivo su $\mathbb{R}$.

Una trasformazione infinitesima, nell'intorno dell'unità, del gruppo è

$$e^{i\delta tX} = 1 + i\delta tX$$

da cui si deduce che X è il gerneratore infinitesimale del gruppo.

Proposizione 69 *La trasformazione infinitesima è ancora unitaria.*

Dimostrazione.

$$U(\delta t)U^\dagger(\delta t) = (1 + i\delta tX)(1 - i\delta tX^\dagger) = 1 + \delta^2 tXX^\dagger + i\delta t(X - X^\dagger)$$

sfruttando l'hermitianicitá di X ed il fatto che $\delta^2 t$ è un infinitesimo del secondo ordine si ha

$$U(\delta t)U^\dagger(\delta t) = 1$$

■

Una trasformazione finita del gruppo si ottiene applicando una trasformazione infinitesima n volte e poi calcolandone il limite, cioé

$$\lim_{n\to\infty}\left(1 + \frac{itX}{n}\right)^n = e^{itX}.$$

Tramite le trasformazioni infinitesime possiamo ricavare le regole di commutazione dei generatori di due gruppi di trasformazione unitari.

Esempio 12 *Consideriamo le regole di commutazione fra l'operatore posizione e l'operatore di traslazione*[2]

$$[\mathbf{x}, T(dx)]|x\rangle = \mathbf{x}T(dx)|x\rangle - T(dx)\mathbf{x}|x\rangle$$

$$= \mathbf{x}|x + dx\rangle - xT(dx)|x\rangle = [(x + dx) - x]|x + dx\rangle$$

da cui

$$[\mathbf{x}, T(dx)] = dx.$$

Considerando che l'operatore di traslazione ha come generatore l'operatore impulso $\mathbf{p}$ *si ha*

$$[\mathbf{x}, 1 - \frac{i\mathbf{p}dx}{\hbar}] = \frac{-idx}{\hbar}[\mathbf{x}, \mathbf{p}] = dx$$

da cui

$$[\mathbf{x}, \mathbf{p}] = i\hbar.$$

[2]L'operatore di traslazione agisce sull'autostato dell'operatore posizione nel seguente modo: $T(\Delta x')|x\rangle = |x + \Delta x'\rangle$

Capitolo 5

Rappresentazioni

5.1 Le Rappresentazioni

Definizione 30 *Sia G un gruppo topologico localmente compatto, separabile e unimodulare*[1] *e H uno spazio di Hilbert separabile, una* ***rappresentazione lineare*** *del gruppo G sullo spazio degli operatori lineari $L(H)$ in H è un'applicazione $T : x \in G \to T_x \in L(H)$ tale che:*

$$T_{xy} = T_x T_y, \qquad T_e = I.$$

La prima condizione significa che l'applicazione T è un omomorfismo di semigruppo, mentre la seconda corrisponde all'esistenza degli opertori inversi, cioé $Im(T) = \{T_x : x \in G\}$ è un sottogruppo del semigruppo $L(H)$. Inoltre una rappresentazione è detta **fortemente continua** se $\forall u \in H$ l'applicazione $x \to T_x u$ è continua.

Rappresentare un gruppo vuol dire realizzarlo come gruppo di trasformazioni di un dato spazio H, la cui dimensione definisce la **dimensione della rappresentazione**.

Una rappresentazione è detta **limitata** se gli operatori su H sono limitati, in particolare se il gruppo è compatto la rappresentazione è limitata.

Una rappresentazione è **unitaria** se gli operatori sullo spazio di Hilbert sono unitari.

Una rappresentazione è detta **fedele** se l'omomorfismo T è iniettivo, altrimenti la rappresentazione è detta **non fedele**.

Nel caso di gruppi di matrici in cui il prodotto è quello riga per colonna, possiamo rappresentare il gruppo con le matrici stesse, questa è detta **rappresentazione identica**.

Teorema 70 *Data una rappresentazione T non fedele di G e posto $N = Ker(T) \neq I$, allora si ha che T induce una rappresentazione fedele del gruppo quoziente G/N che, con abuso di notazione, indicheremo con T.*

Dimostrazione. L'applicazione $T : x \in G \to T_x \in L(H)$ è un omomorfismo, quindi, utilizzando il teorema 16, si ha che N è un sottogruppo normale e che

$$xN \in G/N \to T_x \in L(H)$$

[1] Un gruppo topologico è unimodulare se esiste una misura invariante a sinistra ed a destra; vedi l'appendice B

è un monomorfismo ben definito in quanto il gruppo G/N è isomorfo ad sottogruppo del semigruppo $L(H)$; infine si può osservare che N è un sottogruppo chiuso e quindi che G/N è un gruppo topologico al pari di G. ■

Data una base ortonormale $|n\rangle$ di H possiamo esprimere gli operatori in forma matriciale come segue

$$D_{i,j}(x) = \langle i|T_x|j\rangle \tag{5.1}$$

in questo modo associamo al sottogruppo $Im(T)$ degli operatori il sottogruppo $GL(n, \mathbb{C})$, dove n è la dimensione dello spazio di Hilbert.

5.2 Rappresentazioni Equivalenti

Definizione 31 *Due rappresentazioni $T : G \to L(H)$ e $T' : G \to L(H')$ si dicono* ***equivalenti*** *se esiste un isomorfismo limitato S tale che $H' = SH$ e tale che si abbia $T'_x = ST_xS^{-1}$ per ogni $x \in G$.*

La relazione definita è una relazione di equivalenza in quanto:

1. ogni rappresentazione è equivalente a se stessa, basta porre $S = I$;
2. se $T'_x = ST_xS^{-1}$ con $H' = SH$, allora si ha $H = S^{-1}H'$ e $T_x = S^{-1}T'_xS$;
3. se $T : G \to L(H)$ è equivalente alla rappresentazione $T' : G \to L(H')$ che a sua volta è equivalente a $T :'' G \to L(H'')$ con $H' = SH$ e $H'' = S'H'$, allora si ha che $T''_x = S'T'_xS'^{-1} = S'ST_x(S'S)^{-1}$.

Si osservi che, essendo S un isomorfismo limitato tale che $H' = SH$ e $T : G \to L(H)$ è una rappresentazione lineare del gruppo G sullo spazio $L(H)$, allora

$$T' : x \in G \to ST_xS^{-1} := T'_x \in L(H)$$

è ancora una rappresentazione in quanto si ha

$$T'_{xy} = ST_{xy}S^{-1} = ST_xS^{-1}ST_yS^{-1} = T'_xT'_y \text{ e } I = SS^{-1} = I'$$

inoltre si ha che

$$\|T'_xu' - T'_yu'\| = \|S(T_xS^{-1}u' - T_yS^{-1}u')\| \leq \|S\|\|T_xu - T_yu\| \to 0 \text{ per } x \to y$$

avendo sfruttato la limitatezza di S ($\|S\| < \infty$).

Definizione 32 *Due rappresentazioni sono* ***unitariamente equivalenti*** *se l'isomorfismo è unitario, cioé se*

$$T'_xU = UT_x \qquad (\forall x \in G). \tag{5.2}$$

Teorema 71 *Due rappresentazioni unitarie equivalenti sono unitariamente equivalenti.*

Dimostrazione. La condizione aggiunta della (5.2) è

$$U^\dagger T'_x = T_x U^\dagger$$

da cui moltiplicando a sinistra per U ed utilizzando di nuovo la (5.2) si ha

$$UU^\dagger T'_x = UT_x U^\dagger = T'_x UU^\dagger$$

cioé $UU^\dagger = I$. ∎

Teorema 72 *Due rappresentazioni unitariamente equivalenti, tramite una opportuna scelta delle basi in H e H' possono essere descritte dalle stesse matrici.*

Dimostrazione.

$$D'_{i,j}(x) = \langle i'|T'_x|j'\rangle = \langle i'|UT_xU^\dagger|j'\rangle = \langle i'|(|i'\rangle\langle i|)T_x(|j\rangle\langle j'|)|j'\rangle = D_{ij}$$

∎

5.3 Rappresentazioni Riducibili ed Irriducibili

Definizione 33 *Presa una rappresentazione T del gruppo G sullo spazio di Hilbert H, un sottospazio $H_1 \subset H$ è detto **invariante** rispetto a T se*

$$T_x H_1 = H_1 \qquad \forall x \in G \tag{5.3}$$

I sottospazi invarianti banali sono l'origine e H stesso; i sottospazi non banali sono detti **propri**.

Definizione 34 *Una rappresentazione è **algebricamente irriducibile** se H non possiede sottospazi invarianti propri.*

Una rappresentazione è quindi detta **riducibile** se H possiede sottospazi invarianti propri. Detto H_1 un sottospazio invariante proprio di H, indichiamo con T_{H_1} la **restrizione** della rappresentazione T al solo sottospazio H_1.

Teorema 73 *Se H_1 è un sottospazio invariante dello spazio H su cui agisce la rappresentazione*

$$T : x \in G \to T_x \in L(H)$$

allora lo spazio quoziente H/H_1 è uno spazio invariante proprio.

Dimostrazione. Per ogni $x \in G$ è ben definita l'applicazione seguente (che, con abuso di notazione, sarà indicata ancora con T_x):

$$T_x : u + H_1 \in H/H_1 \to T_x(u) + H_1 \in H/H_1$$

Infatti, se $u = v + H_1$, cioé $u - v \in H_1$, si ha:

$$T_x(u) - T_x(v) = T_x(u - v) \in T_x(H_1) = H_1$$

e quindi $T_x(u) = T_x(v) + H_1$. Quindi T induce una rappresentazione di G sullo spazio quoziente H/H_1. Se H_1 è un sottospazio proprio allora la dimensione della rappresentazione indotta è minore della dimensione di T e diversa da 0. ■

Se uno spazio H su cui agisce una rappresentazione T è decomponibile nella somma diretta di sottospazi invarianti propri (e non ulteriormente riducibili)

$$H = \bigoplus_i H_i$$

allora potremo scrivere la rappresentazione T come somma diretta delle sottorappresentazioni

$$T = \bigoplus_i T_{H_i}.$$

Teorema 74 *Data una rappresentazione unitaria T del gruppo G sullo spazio di Hilbert H si ha che, se H_1 è un sottospazio invariante proprio, lo è anche il suo complemento ortogonale $H_1^\perp$.*

Dimostrazione. Presi $u \in H_1$ e $v \in H_1^\perp$ abbiamo che per definizione

$$(T_x v, u) = (v, T_x^\dagger u) = (v, T_{x^{-1}} u) = 0$$

dove l'ultima uguaglianza discende dall'invarianza di H_1; $(T_x v, u) = 0$ significa che $T_x v \in H^\perp$, da cui la tesi. ■

Definizione 35 *Una rappresentazione tale che ogni sua sottorappresentazione ammetta una sottorappresentazione complementare è detta* ***completamente riducibile****.*

Quindi dal teorema 35 segue che una rappresentazione unitaria (di dimensione finita) è completamente riducibile; da ciò si può affermare che una condizione sufficiente per la completa riducibilitá per una rappresentazione è quella di essere equivalente ad una rappresentazione unitaria.

Consideriamo una decomposizione dello spazio H in sottospazi invarianti propri H_i ortogonali tra di loro e consideriamo, inoltre, una base ortonormale dei singoli H_i, potremo, quindi, costruire una base di H tramite il prodotto tensoriale delle basi dei singoli sottospazzi: $|n\rangle = |1\rangle \otimes |2\rangle \otimes ... \otimes |i\rangle \otimes ...$; Utilizzando questa base avremo che

$$\langle n'|T|n\rangle = \bigoplus_i \langle i'|T_{H_i}|i\rangle$$

da cui, se $H_i \neq H_{i'}$ l'elemento di matrice è 0, per l'ortogonalitá tra gli spazi, altrimenti se $H_i = H_{i'}$ l'elemento di matrice corrisponde con quello della matrice della sottorappresentazione T_{H_i}; in conclusione avremo che la matrice della rappresentazione è a blocchi:

$$D(x) = \begin{bmatrix} D^1(x) & 0 & ... & 0 & ... \\ 0 & D^2(x) & ... & 0 & ... \\ ... & ... & ... & ... & ... \\ 0 & 0 & ... & D^i(x) & ... \\ ... & ... & ... & ... & ... \end{bmatrix} \tag{5.4}$$

Lemma 75 (di Schur) *Se T_1 e T_2 sono due rappresentazioni irriducibili di un gruppo G su H_1 e H_2 rispettivamente allora ogni G-omomorfismo A non nullo da H_1 a H_2 è invertibile.*

Dimostrazione. Se $A \neq 0$ non fosse invertibile allora avremo che $KerA$ è un sottospazio invariante di H_1; se fosse $KerA \neq 0$, $KerA$ ammetterebbe una sotto-rappresentazione non banale e quindi T_1 sarebbe riducibile, il che contrasta con l'ipotesi. Allora $KerA = 0$. ne segue che ImA è un sottospazio invariante proprio di H_2 e quindi T_2 è riducibile, contro l'ipotesi. ■

5.4 Rappresentazioni di Gruppi Compatti

Teorema 76 *Ogni rappresentazione di dimensione finita di un gruppo topologicamente compatto è equivalente ad una rappresentazione unitaria.*

Dimostrazione. Data una rappresentazione T del gruppo G sullo spazio H su cui è definito un prodotto scalare $\langle , \rangle$ definiamo, utilizzando una **misura di Haar**, la forma

$$(x, y) = \int_G \langle T_g x, \overline{T_g y} \rangle dg$$

che risulta essere hermitiana e tale che

$$(T_h x, T_h y) = \int_G \langle T_h(T_g x), \overline{T_h(T_g y)} \rangle dg = \int_G \langle T_{hg} x, \overline{T_{hg} y} \rangle dg$$

$$= \int_G \langle T_k x, \overline{T_k y} \rangle dk = (x, y)$$

dove si è fatto uso dell'invarianza della misura di Haar per traslazione[2] di un gruppo compatto. Da quanto ricavato si vede che la rappresentazione è unitaria per il prodotto hermitiano $(,)$. ■

L'importanza dei gruppi compatti risiede quindi nel fatto che ogni loro rappresentazione è completamente riducibile.

Teorema 77 (di Stone) *Data una rappresentazione unitaria fortemente continua del gruppo additivo $\mathbb{R}$ allora esiste un unico operatore A hermitiano tale che*

$$U(t) = e^{itA}$$

$U(t)$ è un gruppo di trasformazioni ad un parametro. Il teorema si può generalizzare per il gruppo additivo $\mathbb{R}^n$ (anch'esso localmente compatto) con un gruppo a n parametri.

Tramite il **Teorema di Nelson** è possibile affermare che ad un gruppo compatto è possibile, sotto opportune condizioni, associarvi un'unica rappresentazione unitaria e fortemente continua tramite l'esponenziazione dei suoi generatori, cioé detti J_k dei generatori di un gruppo G si ha la rappresentazione

$$U(t) = e^{itJ_k}$$

[2] $d(hg) = d(g)$

per ogni k.

Queste rappresentazioni sono valide nell'intorno dell'unità ma risultano essere prolungabili a tutta la componente semplicemente connessa all'unità.

In conclusione un gruppo di Lie compatto è rappresentabile tramite l'esponenziazione dei suoi generatori in un intorno dell'unità.

5.4.1 La Quantizzazione

Per mettere in relazione i risultati della teoria dei Gruppi con la Meccanica Quantistica utilizziamo un'osservazione dovuta a Dirac che mette in relazione le parentesi di Poisson con le regole di commutazione fra gli operatori delle rispettive variabili classiche

$$\{,\} \to \frac{[,]}{i\hbar}$$

questa regola va sotto il nome di **quantizzazione secondo Dirac**.

Dati due gruppi di trasformazioni ed i loro integrali primi associati f e g vale la relazione

$$[\mathbf{X}_f, \mathbf{X}_g] = -\mathbf{X}_{\{f,g\}}$$

che lega i generatori del gruppo di trasformazione alla struttura simplettica. In questo modo, dato un gruppo di trasformazione facciamo corrispondere ad una parentesi di Poisson un commutatore fra i generatori del gruppo il quale, diviso per $i\hbar$ (il che corrisponde alla ridefinizione dei generatori $L = i\hbar R$), corrisponde alla commutazione fra gli operatori quantistici.

Il discorso è plausibile in quanto anche le parentesi di Poisson definiscono un algebra di Lie, inoltre l'introduzione del fattore immaginario è dovuto al fatto che le parentesi di Poisson di funzioni reali sono reali mentre i commutatori di operatori hermitiani sono antihermitiani

$$\begin{aligned} iC^\dagger = (-iC)^\dagger = [A,B]^\dagger = (AB)^\dagger - (BA)^\dagger = B^\dagger A^\dagger - A^\dagger B^\dagger \\ = -[A^\dagger, B^\dagger] = -[A,B] = -(-iC). \end{aligned}$$

Capitolo 6

I Gruppi Classici

6.1 Il Gruppo Lineare

Il **gruppo lineare reale** è il sottoinsieme di tutte le matrici quadrate reali $n \times n$ ($M_n(\mathbb{R})$) definito nel seguente modo:

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : detA \neq 0\} \tag{6.1}$$

L'operazione del gruppo è il consueto prodotto riga per colonna fra matrici. Allo stesso modo definiamo il **gruppo lineare complesso** delle matrici quadrate complesse $n \times n$ ($M_n(\mathbb{C})$):

$$GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) : detA \neq 0\} \tag{6.2}$$

Ad ogni matrice complessa di dimensione n possiamo associare una matrice reale di dimensione $2n$, in quanto, potendo scrivere una matrice complessa A come $A = B + iC$ con B e C matrici reali di dimensione n, abbiamo che il prodotto fra matrici complesse si può riottenere come prodotto fra matrici reali del tipo:

$$A_{\mathbb{R}} = \begin{bmatrix} B & -C \\ C & B \end{bmatrix}.$$

In altri termini, l'applicazione

$$A = B + iC \in GL_n(\mathbb{C}) \to A_{\mathbb{R}} \in GL_{2n}(\mathbb{R})$$

è un monomorfismo (immerge $GL_n(\mathbb{C})$ in $GL_{2n}(\mathbb{R})$).

Le matrici $M_n(\mathbb{R})$ possono essere considerate come elementi in uno spazio $\mathbb{R}^{n^2}$ di coordinate x_{ij} (in un ordine arbitrario), in questo modo ad ogni punto dello spazio corrisponde una matrice. Il gruppo lineare è determinato dalla condizione $detA \neq 0$ che, essendo il determinante una funzione differenziabile, descrive una varietá differenziale nello spazio delle matrici.

Il **gruppo lineare speciale** è il sottogruppo di $GL(n, \mathbb{R})$ definito nel seguente modo:

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : detA = 1\} \tag{6.3}$$

allo stesso modo definiamo il gruppo sul campo complesso. Il sottogruppo lineare speciale è un sottogruppo topologico (una varietà di dimensione $n^2 - 1$, in quanto è soggetto alla sola condizione $detA = 1$) chiuso, perché il determinate è una funzione continua. Questo gruppo non è compatto, come si puó vedere dalla seguente matrice

$$\begin{bmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{bmatrix}$$

in cui l'elemento ϵ può assumere un valore arbitrariamente grande (lo spazio è chiuso ma non è limitato).

6.2 Il Gruppo Ortogonale

Il **gruppo ortogonale** $O(n)$ è il sottogruppo del gruppo lineare reale $GL_n(\mathbb{R})$ definito nel seguente modo:

$$O(n) = \{A \in M_n(\mathbb{R}) : AA^T = I\} \tag{6.4}$$

cioé è il gruppo che lascia invariato il prodotto scalare: $(v, w) = (Ov, Ow) = \sum v_i w_i$.

La condizione di definizione ($a_{ij}a_{jk} = \delta_{ik}$) equivale ad $n(n+1)/2$ (n per $i = j$ e $(n^2-n)/2$) per $i > k$) condizioni, da cui il numero di parametri, cioé la dimensione della sottovarietá è $n(n-1)/2$.

Il gruppo topologico ortogonale è compatto in quanto la chiusura discende dalla continuitá della relazione di definizione e la limitatezza dal fatto che

$$|a_{ij}|^2 = a_{ij}a_{ij} \leq \sum_k a_{ik}a_{ik} = 1$$

Il gruppo non è connesso in quanto è composto da due componenti relative alle due condizioni $detA = \pm 1$ ($det(AA^T) = det^2(A) = 1$) non collegabili tramite una curva $A(t)$ continua sulla varietà[1].

Con l'ulteriore condizione $detA = 1$ definiamo il **gruppo ortogonale speciale** $SO(n)$ che definisce la sottovarietà relativa alla componente connessa all'identità. Il gruppo è chiuso e quindi compatto.

Il gruppo ortogonale si può ottenere come:

$$O(n) = \begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix} \times SO(n).$$

Data una curva $A(t)$ tale che $A(0) = I$ abbiamo che il vettore tangente alla curva nell'identità è

$$0 = \left.\frac{dAA^T}{dt}\right|_{t=0} = A^T + A$$

da cui avremo in particolare che ogni elemento del gruppo si ottiene dall'esponenziazione di una matrice antisimmetrica ($A = -A^T$).

[1] Proposizione 59

6.3 Il Gruppo Unitario

Il **gruppo unitario** $U(n)$ è un sottogruppo del gruppo lineare complesso $GL_n(\mathbb{C})$ definito nel seguente modo:

$$U(n) = \{A \in M_n(\mathbb{C}) : AA^\dagger = I\} \tag{6.5}$$

cioé è il gruppo che lascia invariato il prodotto hermitiano: $(v, w) = (Uv, Uw) = \sum v_i \overline{w}_i$.

Le condizioni di definizione ($a_{ij}\overline{a}_{jk} = \delta_{ik}$) sono n^2 (n condizioni reali per $i = k$, $n(n-1)$ condizioni complesse per $i > k$), cioé il numero di parametri del gruppo è $2n^2 - n^2 = n^2$.

Il gruppo topologico unitario è compatto in quanto la chiusura discende dalla continuità della relazione di definizione e la limitatezza dal fatto che

$$|a_{ij}|^2 = a_{ij}\overline{a}_{ij} \leq \sum_k a_{ik}\overline{a}_{ik} = 1$$

Dalla relazione di definizione del gruppo unitario discende che

$$det(UU^\dagger) = |detU|^2 = 1$$

da cui si ottiene che il determinante di una matrice unitaria è una fase. Il **gruppo unitario speciale** $SU(n)$ è il sottogruppo del gruppo unitario definito dall'ulteriore condizione: $detU = 1$, di conseguenza la dimensione del gruppo è $n^2 - 1$.

Inoltre, essendo un sottogruppo chiuso sempre per la continuità del determinante, è un gruppo compatto.

Il gruppo unitario si può ottenere come $U(n) = U(1) \times SU(n)$.

Data una curva $A(t)$ tale che $A(0) = I$ abbiamo che il vettore tangente alla curva nell'identità è

$$0 = \left.\frac{dAA^\dagger}{dt}\right|_{t=0} = A^\dagger + A$$

da cui avremo in particolare che ogni elemento del gruppo si ottiene dall'esponenziazione di una matrice hermitiana antisimmetrica ($A = -A^\dagger$). L'ulteriore condizione a cui è soggetto $SU(n)$ fa sì che le matrici debbano essere anche a traccia nulla

$$1 = det(e^A) = e^{trA} = e^0$$

Esempio 13 *Una rappresentazione bidimensionale su $\mathbb{C}^2$ del gruppo $U(2)$ è fornita da una metrica i cui elementi soddisfino le seguenti condizioni ($UU^\dagger = I$):*

$$|a_{11}|^2 + |a_{12}|^2 = 1 \qquad |a_{21}|^2 + |a_{22}|^2 = 1 \qquad a_{21}\overline{a}_{11} + a_{22}\overline{a}_{12} = 0$$

Il gruppo $SU(2)$ è definito dall'ulteriore condizione $a_{11}a_{22} - a_{12}a_{21} = 1$ ($detSU(2) = 1$). Moltiplicando la precedente relazione per $\overline{a}_{22}$ si ha

$$a_{11}|a_{22}|^2 - a_{12}a_{21}\overline{a}_{22} = \overline{a}_{22}$$

da cui utilizzando la $a_{21}\overline{a}_{11} + a_{22}\overline{a}_{12} = 0$ si ottiene

$$a_{11}|a_{22}|^2 + a_{11}\overline{a}_{21}a_{21} = \overline{a}_{22}$$

cioé $a_{11} = \overline{a}_{22}$ *e* $a_{12} = -\overline{a}_{21}$. *In conclusione si ha che*

$$\begin{bmatrix} a & b \\ -\overline{b} & \overline{a} \end{bmatrix} \tag{6.6}$$

Ponendo $a = x_1 + ix_2$ *e* $b = x_3 + ix_4$ *e calcolando il determinante si ottiene* $\sum_{i=1}^4 x_i^2 = 1$, *da cui si deduce che* $SU(2)$ *è omeomorfo ad una sfera di raggio 1 in* $\mathbb{R}^4$ *(*S^3*).*

$SU(2)$ *è il gruppo di ricoprimento universale di* $O(3)$ *in quanto possiedono la medesima algebra fra i generatori del gruppo ed inoltre* $SU(2)$ *è semplicemente connesso*[2]*; quindi, assegnata la (*6.6*), si ha la corrispondente matrice di* $O(3)$

$$\begin{bmatrix} Re(a^2-b^2) & -Im(a^2+b^2) & -2Re(ab) \\ Im(a^2-b^2) & Re(a^2+b^2) & -2Im(ab) \\ 2Re(a\overline{b}) & -2Im(a\overline{b}) & a\overline{a}-b\overline{b} \end{bmatrix}$$

Considerando che il nucleo della'applicazione è formato dal sottogruppo $\{+I, -I\}$ *da cui abbiamo che* $SO(3) = SU(2)/\{+I, -I\}$.

Illustriamo un'altra procedura per ottenere che $SU(2)$ *è una rappresentazione, detta anche* ***rappresentazione spinoriale*** *del gruppo delle rotazioni.*

Lemma 78 *Ogni automorfismo di un'algebra interna associativa* $M(n, \mathbb{C})$ *è interno*[3]*.*

Consideriamo la seguente base additiva di $M(2, \mathbb{C})$*:*

$$I, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Le relative relazioni di commutazione ed anticommutazione sono:

$$[\sigma_i, \sigma_j] = 2i\varepsilon_{ijk}\sigma_k \qquad \{\sigma_i, \sigma_j\} = 2\delta_{ij} \tag{6.7}$$

Dalla relazione di commutazione si nota che le $i\sigma_j/2$ *sono una rappresentazione dell'algebra di Lie di* $SU(2)$ *e quindi di* $SO(3)$.

Costruiamo uno spazio euclideo utilizzando come base le σ_j*, cioé* $(x^1, x^2, x^3) \to x^j\sigma_j$. *Sia* $\Lambda \in O(3)$ *allora avremo per un vettore* $x'^k = \lambda^k_j x^j$ *da cui*

$$\sigma'_k = \lambda^j_k \sigma_j$$

*Queste trasformazioni lasciano invariata la relazioni di anticommutazione (*6.7*), mentre per la relazione di commutazione otteniamo*

$$[\sigma'_i, \sigma'_j] = \lambda^k_i \lambda^l_j [\sigma_k, \sigma_l] = 2i\varepsilon_{ijk}\sigma'_k$$

solo se $\Lambda \in SO(3)$*; abbiamo cosí definito un automorfismo di* $M(2, \mathbb{C}) \to M(2, \mathbb{C})$*, quindi per il lemma* 78 *avremo una rappresentazione di* $SO(3)$ *in quanto, per ogni matrice* x*, esiste una trasformazione* $g(\Lambda)$ *tale che* $h(x) = gxg^{-1}$*. La rappresentazione è definita a meno di un fattore moltiplicativo che possiamo eliminare se imponiamo che* $g \in SL(2, \mathbb{C})$*; inoltre la rappresentazione è 2 a 1, come abbiamo giá visto precedentemente.*

[2] $SU(2)$ è omeomorfo a S^3 che è semplicemente connesso.

[3] Per automorfismo intendiamo un'applicazione $h : M(n, \mathbb{C}) \to M(n, \mathbb{C})$ tale che $h(x) = gxg^{-1}$ dove $g \in GL(n, \mathbb{C})$.

6.4 Il Gruppo $O(k, n-k)$

Il gruppo $O(k, n-k)$ è definito nel seguente modo:

$$O(k, n-k) = \{A \in GL_n(\mathbb{R}) : A^T G A = G\} \tag{6.8}$$

dove G è la metrica associata alla forma $(,)_k$ che è una forma bilineare simmetrica non degenere che, per il teorema di Sylvester, può essere scritta come $v^T G w = (v, w)_k = \sum_{i=1}^{k} v_i w_i - \sum_{i=k+1}^{n} v_i w_i$.

$$G = \begin{bmatrix} I_k & 0 \\ 0 & -I_{n-k} \end{bmatrix} \tag{6.9}$$

Il gruppo non è compatto perché non è limitato.

Il sottogruppo **speciale** $SO(k, n-k)$ è definito dall'ulteriore condizione $detA = 1$

6.5 Il Gruppo Simplettico

Il **gruppo simplettico** è definito nel seguente modo:

$$Sp = \{A \in M_n(\mathbb{R}) : A^T J A = J\} \tag{6.10}$$

dove la matrice J definisce una forma bilineare antisimmetrica $-(w, v) = (v, w)$, su uno spazio di dimensione pari in quanto è anche non degenere, che può essere ricondotta, per il teorema di Darboux, a $(v, w) = \sum_{i=1}^{k} (v_i w_{i+k} - v_{i+k} w_i)$.

$$J = \begin{bmatrix} 0 & I_k \\ -I_k & 0 \end{bmatrix} \qquad (n = 2k) \tag{6.11}$$

Il gruppo simplettico non è un gruppo compatto.

Capitolo 7

I Gruppi in Meccanica Quantistica

7.1 Teorema di Wigner e descrizioni equivalenti

Consideriamo due osservatori che effettuano misure su due esperimenti simili (con le stesse condizioni iniziali) in sistemi di riferimento differenti O e O' aventi la stessa origine; sia $|jm\rangle$ l'autostato di J^2 e J_z con autovalori $j(j+1)$ e m per l'osservatore O, e $|j,m;R\rangle$ l'autostato di J^2 e $J_{z'}$ col medesimo autovalore m (l'autostato $|j,m;R\rangle$ corrisponde all'autostato $|j,m\rangle$ ruotato); se i due osservatori preparano due particelle con la medesima energia e le fanno viaggiare lungo i rispettivi assi z, indicando con $|\alpha\rangle$ e $|\alpha;R\rangle$ i rispettivi stati delle particelle, dovranno ottenere i medesimi risultati sperimentali dalla misura della probabilità che le particelle abbiano un definito autovalore di J^2 e J_z, cioè che:

$$|\langle\alpha|j,m\rangle| = |\langle R;\alpha|j,m;R\rangle|. \tag{7.1}$$

Questo ragionamento è valido anche nel caso di altre trasformazione, come ad esempio le traslazioni, ed è del tutto indipendente dall'equazione del moto.

Il teorema di Wigner afferma che le uniche trasformazioni che conducono alla (7.1) sono le trasformazioni **unitarie** ($U^\dagger U = 1$)

$$\langle\alpha|\beta\rangle = \langle\alpha U^\dagger|U\beta\rangle = \langle\alpha'|\beta'\rangle \tag{7.2}$$

o le trasformazioni **antiunitarie**

$$\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^* = \langle\beta'|\alpha'\rangle \tag{7.3}$$

Un operatore antiunitario θ

$$|\alpha'\rangle = \theta|\alpha\rangle, \qquad |\beta'\rangle = \theta|\beta\rangle$$

è un operatore antilineare cioè:

$$\langle\beta'|\alpha'\rangle = \langle\beta|\alpha\rangle^* = \langle\alpha|\beta\rangle \tag{7.4}$$

$$\theta(a|\alpha\rangle + b|\beta\rangle) = a^*|\alpha'\rangle + b^*|\beta'\rangle. \tag{7.5}$$

Teorema 79 *Un operatore antiunitario si può decomporre nel prodotto tra un operatore unitario U e l'operatore di coniugazione complessa K ($\theta = UK$).*

Infatti abbiamo:

$$UK(a|\alpha\rangle + b|\beta\rangle) = a^*UK|\alpha\rangle + b^*UK|\beta\rangle = a^*U|\alpha\rangle + b^*U|\beta\rangle, \tag{7.6}$$

$$|\alpha'\rangle = UK\sum_a |a\rangle\langle a|\alpha\rangle = \sum_a \langle a|\alpha\rangle^* UK|a\rangle = \sum_a \langle a|\alpha\rangle^* U|a\rangle \tag{7.7}$$

e, poichè se $|\beta'\rangle = \sum_b \langle b|\beta\rangle^* U|b\rangle$ allora $\langle\beta'| = \sum_b \langle b|\beta\rangle\langle b|U^\dagger$,

$$\langle\beta'|\alpha'\rangle = \sum_{ab} \langle b|\beta\rangle\langle b|U^\dagger U|a\rangle\langle\alpha|a\rangle = \sum_a \langle a|\beta\rangle\langle\alpha|a\rangle = \langle\alpha|\beta\rangle. \tag{7.8}$$

Dimostrazione. Per provare il teorema partiamo dallo stato $|\phi_n\rangle = |a_1\rangle + |a_n\rangle$ e vediemo che è possibile ottenere lo stato $|\phi'_n\rangle = |a'_1\rangle + |a'_n\rangle$. Abbiamo

$$|\phi'\rangle = \sum_m |a'_m\rangle\langle a'_m|(|a_1\rangle + |a_n\rangle)'$$

ed essendo $\langle a'_m|(|a_1\rangle + |a_n\rangle)' = e^{i\tau_m}\langle a_m|(|a_1\rangle + |a_n\rangle) = e^{i\tau_m}(\delta_{m1} + \delta_{mn})$, come si nota dalla (7.1), si ottiene

$$|\phi'\rangle = e^{\tau_1}|a_1\rangle + e^{i\tau_n}|a_n\rangle,$$

cioè, potendo riassorbire il fattore di fase, in quanto $e^{i\tau_n}|a_n\rangle$ e $|a_n\rangle$ rappresentano lo stesso stato fisico, si ha

$$|\phi'_n\rangle = |a'_1\rangle + |a'_n\rangle. \tag{7.9}$$

Ponendo $|\alpha\rangle = \sum_n c_n|a_n\rangle$ e $|\alpha'\rangle = \sum_n c'_n|a'_n\rangle$, si ha

$$|\langle\phi_n|\alpha\rangle| = |c_1 + c_2| = |c'_1 + c'_2| = |\langle\phi'_n|\alpha'\rangle|$$

da cui, scegliendo la fase di $|\alpha'\rangle$ tale che $c_1 = c'_1$ ($|c_n| = |c'_n|$)

$$c_1c_n^* + c_1^*c_n = c_1{c'}_n^* + c_1^*c'_n$$

moltiplicando per c'_n e risolvendo l'equazione di secondo grado per c'_n si ricavano:

$$c'_n = c_n \qquad \text{oppure} \qquad c'_n = \frac{c_1}{c_1^*}c_n^* \tag{7.10}$$

da cui, ridefinendo la fase di $|\alpha\rangle$ in modo che c_1 sia reale, otteniamo:

$$|\alpha'\rangle = \sum_n c_n|a'\rangle \text{ (unitaria)} \qquad |\alpha'\rangle = \sum_n c_n^*|a'\rangle \text{ (antiunitaria)} \tag{7.11}$$

da cui il teorema. ■

Se due descrizioni equivalenti sono ottenute tramite gruppi di trasformazione continui allora la trasformazione è solo unitaria, in quanto il prodotto di due operatori antiunitari è un operatore unitario.

7.2 Simmetrie

Consideriamo un gruppo di trasformazioni a cui possiamo associare un operatore unitario S; l'operatore S è una **simmetria** del sistema se l'Hamiltoniana è invariante per questo gruppo di trasformazioni, cioé

$$S^\dagger H S = H \text{ oppure } HS = SH, \tag{7.12}$$

che puó essere riscritto come

$$[H, S] = 0. \tag{7.13}$$

Sia G il **generatore infinitesimale** del gruppo di simmetria $S = e^{-\frac{it}{\hbar}G}$; consideriamo una **trasformazione infinitesima** (al primo ordine) $S = 1 - \frac{it}{\hbar}G$, allora la (7.12) diviene

$$H = S^\dagger H S = (1+\frac{it}{\hbar}G)H(1-\frac{it}{\hbar}G) = (H+\frac{it}{\hbar}GH)(1-\frac{it}{\hbar}G) = H+\frac{it}{\hbar}[G,H] \tag{7.14}$$

dove è stato trascurato il termine al secondo ordine in t^2, da cui si ottiene

$$[G, H] = 0 \tag{7.15}$$

analogamente al caso classico; inoltre, utilizzando l'equazione del moto di Heisenberg, si ha che G è una **costante del moto** nel senso che, se il sistema all'istante iniziale è in un autostato di G, negli istanti successivi il vettore di stato evoluto è sempre autostato di G:

$$\frac{dG}{dt} = -\frac{i}{\hbar}[G, H] = 0. \tag{7.16}$$

,,Dalla (7.15) si ha che, se $|n\rangle$ è un autoket di H allora lo sará anche $S|n\rangle$, che in generale rappresenta uno stato diverso, cosiché avremo una degenerazione.

7.3 Traslazioni

L'**operatore di traslazione infinitesimo** $T(\Delta x)$ (trattiamo il caso unidimensionale facilmente generalizzabile al caso tridimensionale) agisce sugli autostati dell'operatore posizione nel seguente modo:

$$T(\Delta x)|x\rangle = |x + \Delta x\rangle \tag{7.17}$$

Indicando con K il generatore infinitesimale delle traslazioni abbiamo che:

$$\begin{aligned}(1 - \frac{i\Delta x'}{\hbar}K)|\alpha\rangle &= \int dx'|x'\rangle\langle x'|T(\Delta x')|\alpha\rangle = \int dx'|x'\rangle\langle x' + \Delta x'|\alpha\rangle \\ &= \int dx'|x'\rangle \left(\langle x'|\alpha\rangle - \Delta x' \frac{\partial}{\partial x'}\langle x'|\alpha\rangle\right) \end{aligned} \tag{7.18}$$

da cui si ottiene che il generatore delle traslazioni è l'operatore momento p (in questo caso p_x).

Una simmetria traslazionale dell'hamiltoniana quindi implica la conservazione del momento.

7.4 Rotazioni

Le rotazioni nello spazio tridimensionale sono implementate tramite una rappresentazione del gruppo in matrici ortogonali su uno spazio di dimensione 3. Queste matrici sono definite come quelle trasformazioni che lasciano invariata la norma di un vettore; il gruppo ha tre parametri che corrispondono alle tre rotazioni attorno ai 3 assi indipendenti dello spazio tridimensionale; le matrici delle rotazioni attorno agli assi x, y, z sono

$$R_z(\theta) = \begin{bmatrix} cos\theta & -sin\theta & 0 \\ sin\theta & cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{7.19}$$

$$R_y(\phi) = \begin{bmatrix} cos\phi & 0 & -sin\phi \\ 0 & 1 & 0 \\ sin\phi & 0 & cos\phi \end{bmatrix} \tag{7.20}$$

$$R_x(\psi) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & cos\psi & -sin\psi \\ 0 & sin\psi & cos\psi \end{bmatrix} \tag{7.21}$$

mentre le matrici

$$L_z = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{7.22}$$

$$L_y = \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \tag{7.23}$$

$$L_x = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix} \tag{7.24}$$

sono le matrici che permettono di esprimere le matrici di rotazione nella seguente forma:

$$R_z = e^{\theta L_z} \qquad R_y = e^{\phi L_y} \qquad R_x = e^{\psi L_x}$$

I generatori infinitesimali del gruppo si ottengono come

$$J_i = L_z \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

che nella base $(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z})$ si esprimono nel seguente modo

$$J_z = -y\frac{\partial}{\partial x} + x\frac{\partial}{\partial y} \qquad J_y = -z\frac{\partial}{\partial x} + x\frac{\partial}{\partial y} \qquad J_x = -z\frac{\partial}{\partial y} + y\frac{\partial}{\partial z} \tag{7.25}$$

Tramite i generatori infinitesimali possiamo ottenere una rappresentazione unitaria infinito dimensionale utilizzando le regole della quantizzazione ($J_i \rightarrow i\hbar[\varepsilon_{ijk}x_j(\partial/\partial x_k)]$) delle rotazioni lungo un asse $\mathbf{n}$ nel seguente modo:

$$D(\mathbf{n},\theta) = e^{-\frac{i\mathbf{J}\cdot\mathbf{n}}{\hbar}\theta} \tag{7.26}$$

Questa rappresentazione soddisfa, per definizione, le regole di commutazione dell'algebra dei generatori infinitesimali

$$[J_i, J_j] = i\hbar\varepsilon_{ijk}J_k \tag{7.27}$$

In questo modo avremo che una rotazione di un ket sará espressa come

$$|\alpha, R\rangle = D(r)|\alpha\rangle \tag{7.28}$$

Una simmetria rotazionale implica la conservazione del momento angolare, cioé di $\mathbf{J}^2$ e di J_z.

7.4.1 Rappresentazioni

Per la costruzione della rappresentazione in n dimensioni utilizziamo i generatori infinitesimali del gruppo introducendo innanzitutto l'**operatore di Casimir**[1] dell'algebra $\mathbf{J}^2 = J_x^2 + J_y^2 + J_z^2$:

$$\begin{aligned}
[\mathbf{J}^2, J_k] &= \sum_{i=1}^{3} J_i[J_i, J_k] + [J_i, J_k]J_i = i\hbar\left(\sum_{i=1}^{3} J_i\varepsilon_{ikj}J_j + \varepsilon_{ikj}J_jJ_i\right) \\
&= i\hbar\left(J_i\varepsilon_{ikj}J_j + \varepsilon_{ikj}J_jJ_i + J_j\varepsilon_{jki}J_i + \varepsilon_{jki}J_iJ_j\right) = 0
\end{aligned}$$

Utilizzando $\mathbf{J}^2$ e J_z potremo costruire una base ortonormale in cui essi sono diagonali.

$$\mathbf{J}^2|a,b\rangle = \hbar^2 a|a,b\rangle \tag{7.29}$$

$$J_z|a,b\rangle = \hbar b|a,b\rangle \tag{7.30}$$

Inoltre, per la costruzione della rappresentazione, risultano utili gli **operatori a scalino**

$$J_\pm = J_x \pm iJ_y,$$

per cui valgono le seguenti regole di commutazione

$$[J_+, J_-] = 2\hbar J_z \tag{7.31}$$

$$[J_z, J_\pm] = \pm\hbar J_\pm \tag{7.32}$$

L'azione di J_z su $J_\pm$ è data da

$$J_zJ_\pm|a,b\rangle = \hbar(b \pm +1)J_\pm|a,b\rangle = cJ_z|a,b\pm 1\rangle$$

dove c è una costante; dalla precedente relazione si deduce che l'azione degli operatori a scala è quella di aumentare o diminuire b che da ora in poi porremo uguale ad m.

[1] Un operatore di Casimir è un operatore che commuta con tutti gli elementi dell'algebra, in particolare commuta con tutti i generatori.

La norma del vettore $J_+|a,m\rangle$ è una quantitá positiva quindi

$$\langle a,m|J_+^\dagger J_+|a,m\rangle = \langle a,m|J_- J_+|a,m\rangle$$

$$= \langle a,m|\mathbf{J}^2 - J_z^2 - \hbar J_z|a,m\rangle = \hbar^2[a - m(m+1)] \geq 0$$

da cui si deduce che m ha un valore limitato e quindi esiste un m_{max} tale che $J_+|a,m_{max}\rangle = 0$, cioé tale che

$$a = m_{max}(m_{max}+1)$$

allo stesso modo, considerando la norma di $J_-|a,m\rangle$, si ricava

$$a = m_{min}(m_{min}-1)$$

da cui si ha anche $m_{max} = -m_{min}$.

Poiché $J_\pm$ varia di una unitá il valore di m deve essere $m_{max} = m_{min} + n$ da cui $j = m_{max} = n/2$; l'autovalore a puó ora essere scritto come $a = j(j+1)$, quindi possiamo scrivere l'autoket utilizzando i valori j e m: $|j,m\rangle$.

j è una quantitá intera o semintera ed è legata alla dimensione dello spazio degli stati dalla relazione $dim(H_j) = 2j+1$.

La rappresentazione su uno spazio di dimensione 2 è ottenibile ponendo $j = 1/2$; in questo modo avremo

$$(\mathbf{J}^{1/2})^2 = \hbar^2 \frac{3}{4} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{7.33}$$

$$J_z^{1/2} = \hbar \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{7.34}$$

La costruzione delle matrici relative a J_x e J_y tramite l'utilizzo degli operatori a scala ci dá le altre matrici di Pauli:

$$J_x^{1/2} = \hbar \frac{1}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{7.35}$$

$$J_y^{1/2} = \hbar \frac{1}{2} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{7.36}$$

Una generica matrice di rotazione (per j fissato) puó essere espressa, utilizzando gli angoli di Eulero nella forma:

$$D^{(j)}_{m'm}(\alpha,\beta,\gamma) = \langle j,m'|e^{\frac{-iJ_z\alpha}{\hbar}} e^{\frac{-iJ_y\beta}{\hbar}} e^{\frac{-iJ_z\gamma}{\hbar}}|j,m\rangle$$

$$= e^{-i(m'\alpha+m\gamma)}\langle j,m'|e^{\frac{-iJ_y\beta}{\hbar}}|j,m\rangle = e^{-i(m'\alpha+m\gamma)} d^{(j)}_{m'm}(\beta) \tag{7.37}$$

$$d^{(1/2)}_{m'm}(\beta) = \langle j,m'|e^{\frac{-iJ_y\beta}{\hbar}}|j,m\rangle = e^{\frac{-iJ_y^{1/2}\beta}{\hbar}} = \begin{bmatrix} cos\frac{\beta}{2} & -sin\frac{\beta}{2} \\ sin\frac{\beta}{2} & cos\frac{\beta}{2} \end{bmatrix}$$

avendo sviluppato la serie dell'esponenziale.

Allo stesso modo in tre dimensioni ($j = 1$) avremo:

$$(\mathbf{J}^1)^2 = \hbar^2 2 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{7.38}$$

$$J_z^1 = \hbar \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix} \tag{7.39}$$

La costruzione di J_y^1, sempre utilizzando gli operatori a scala ci dá

$$J_y^1 = \hbar \frac{i}{2} \begin{bmatrix} 0 & -\sqrt{2} & 0 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 0 & \sqrt{2} & 0 \end{bmatrix} \tag{7.40}$$

da cui

$$d^{(1)}_{m'm}(\beta) = \langle j, m'| e^{\frac{-iJ_y\beta}{\hbar}} |j, m\rangle = e^{\frac{-iJ_y^1\beta}{\hbar}}$$

$$= \begin{bmatrix} \frac{1}{2}(1+cos\beta) & -\frac{1}{\sqrt{2}}sin\beta & \frac{1}{2}(1-cos\beta) \\ \frac{1}{\sqrt{2}}sin\beta & cos\beta & -\frac{1}{\sqrt{2}}sin\beta \\ \frac{1}{2}(1-cos\beta) & \frac{1}{\sqrt{2}}sin\beta & \frac{1}{2}(1+cos\beta) \end{bmatrix}$$

La rappresentazione in uno spazio infinitodimensionale con j variabile è una rappresentazione riducibile a blocchi di cui ognuno agisce su un sottospazio di dimensione $2j+1$; $\mathbf{J}^2$ e J_z sono sempre matrici diagonali mentre il fatto che J_x e J_y sono fatte a blocchi di matrici $(2j+1)\times(2j+1)$ è dovuto al fatto che commutano con $\mathbf{J}^2$ (sono diagonali per diversi j) ma non con J_z (i blocchi non possono quindi essere diagonalizzati).

$$\begin{bmatrix} j=1 & 0 & 0 & ... \\ 0 & j=1/2 & 0 & ... \\ 0 & 0 & j=1 & ... \\ ... & ... & ... & ... \end{bmatrix}$$

7.4.2 Composizione di Momenti Angolari e Rappresentazioni Irriducibili

Consideriamo la somma di due momenti angolari J_1 e J_2 indipendenti che potremo scrivere nel seguente modo

$$J = J_1 \otimes I_2 + I_1 \otimes J_2 \tag{7.41}$$

dove $I_{1,2}$ è l'identitá dello spazio su cui aggisce $J_{1,2}$, da cui si deducono le seguenti regole di commutazione

$$[J_{1i}, J_{1j}] = i\hbar\varepsilon_{ijk}J_{1k} \qquad [J_{2i}, J_{2j}] = i\hbar\varepsilon_{ijk}J_{2k} \qquad [J_{1i}, J_{2j}] = 0$$

L'indipendenza dei momenti angolari discende dall'indipendenza delle rotazioni, $D^1(R)\otimes D^2(R')$, che per rotazioni infinitesime diviene

$$\left(1-\frac{i\mathbf{J}_1\cdot\mathbf{n}d\theta}{\hbar}\right)\otimes\left(1-\frac{i\mathbf{J}_2\cdot\mathbf{n}d\theta}{\hbar}\right)=1-\frac{i(\mathbf{J}_1\otimes I_2+I_1\otimes\mathbf{J}_2)\cdot\mathbf{n}d\theta}{\hbar}$$

Possiamo scegliere due tipi di sistemi massimali di generatori

$$\begin{aligned}
&\mathbf{J}_1^2|j_1,j_2,m_1,m_2\rangle=\hbar^2 j_1(j_1+1)|j_1,j_2,m_1,m_2\rangle\\
&J_{1z}|j_1,j_2,m_1,m_2\rangle=\hbar m_1|j_1,j_2,m_1,m_2\rangle\\
&\mathbf{J}_2^2|j_1,j_2,m_1,m_2\rangle=\hbar^2 j_2(j_2+1)|j_1,j_2,m_1,m_2\rangle\\
&J_{2z}|j_1,j_2,m_1,m_2\rangle=\hbar m_2|j_1,j_2,m_1,m_2\rangle
\end{aligned}$$

oppure

$$\begin{aligned}
&\mathbf{J}_1^2|j_1,j_2,j,m\rangle=\hbar^2 j_1(j_1+1)|j_1,j_2,j,m\rangle\\
&\mathbf{J}_2^2|j_1,j_2,j,m\rangle=\hbar^2 j_2(j_2+1)|j_1,j_2,j,m\rangle\\
&\mathbf{J}^2|j_1,j_2,j,m\rangle=\hbar^2 j(j+1)|j_1,j_2,j,m\rangle\\
&J_z|j_1,j_2,j,m\rangle=\hbar m|j_1,j_2,j,m\rangle
\end{aligned}$$

Nella prima base le matrici sono composte da due blocchi di dimensione $2j_1+1$ e $2j_2+1$, mentre nella seconda abbiamo una rappresentazione irriducibile composta da $j_{max}-j_{min}=(j_1+j_2)-(|j_1-j_2|)$ blocchi, in quanto vale la decomposizione

$$dimH(j_1)\otimes dimH(j_2)=(2j_1+1)(2j_2+1)=\sum_{|j_1-j_2|}^{j_1+j_2}(2j+1)=\bigoplus_{|j_1-j_2|}^{j_1+j_2}dimH(j)$$

$$D^{(j_1)}\otimes D^{(j_2)}=D^{(j_1+j_2)}\oplus D^{(j_1+j_2-1)}\oplus...\oplus D^{(|j_1-j_2|)}\tag{7.42}$$

La matrice nella seconda base è

$$\begin{bmatrix}(j_1+j_2) & 0 & ... & 0\\ 0 & (j_1+j_2-1) & ... & 0\\ ... & ... & ... & ...\\ 0 & 0 & 0 & (|j_1-j_2|)\end{bmatrix}$$

Il passaggio tra le due basi si effettua con i coefficinti di Clebsch-Gordan definiti appunto dalla relazione

$$|j_1,j_2,j,m\rangle=\sum_{m_1}\sum_{m_2}|j_1,j_2,m_1,m_2\rangle\langle j_1,j_2,m_1,m_2|j_1,j_2,j,m\rangle\tag{7.43}$$

$$D^{(j_1)}_{m_1m_1'}\otimes D^{(j_1)}_{m_2m_2'}$$

$$=\bigoplus_{|j_1-j_2|}^{j_1+j_2}\sum_{m}\sum_{m'}\langle j_1,j_2,m_1,m_2|j_1,j_2,j,m\rangle\langle j_1,j_2,m_1',m_2'|j_1,j_2,j,m'\rangle D^{(j)}_{mm'}\tag{7.44}$$

7.5 Paritá

La trasformazione di **paritá** è una simmetria discreta che corrisponde a trasformare un sistema destrorso in uno sinistrorso.

Poiché la trasformazione di paritá corrisponde ad una inversione degli assi $(x, y, z) \to (-x, -y, -z)$, cioé l'operatore di paritá per il vettore posizione corrisponde ad una riflessione

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \tag{7.45}$$

ci aspettiamo che l'azione dell'operatore di paritá P su un autoket dell'operatore posizione sia

$$P|x\rangle = |-x\rangle \tag{7.46}$$

da ció discende che

$$\mathbf{x}P|x\rangle = \mathbf{x}|-x\rangle = -x|-x\rangle = -xP|x\rangle = -Px|x\rangle = -P\mathbf{x}|x\rangle$$

cioé l'operatore posizione anticommuta con P.

Dal fatto che $P^2 = 1$ discende che gli autovalori di P sono ± 1, quindi possiamo distinguere in autoket pari $(+1)$ ed autoket dispari (-1); inoltre è un operatore hermitiano, perché possiede autovalori reali, ed unitario ($P^\dagger = P = P^{-1}$) perché è involutivo.

Uno scalare si distingue da uno pseudoscalare per come si trasforma sotto paritá, lo scalare non cambia di segno mentre lo pseudoscalare si; un vettore è dispari mentre uno pseudovettore è pari.

L'azione dell'operatore paritá sull'operatore di traslazione è la stessa di quella sull'operatore posizione, cioé $PT(dx) = T(-dx)P$ da cui otteniamo

$$P\left(1 - \frac{ip \cdot dx}{\hbar}\right)P^\dagger = PP^\dagger - \frac{iPpP^\dagger \cdot dx}{\hbar} = \left(1 + \frac{ip \cdot dx}{\hbar}\right)$$

essendo dx un parametro, da cui segue che p è dispari.

L'operatore paritá commuta con l'operatore di rotazione in quanto la paritá e l'identitá formano un sottogruppo normale delle rotazioni $(O(3)/SO(3))$ e come tali commutano con ogni rotazione $(SO(3))$; conseguentemente si ha per il generatore delle rotazioni

$$[P, L] = 0 \tag{7.47}$$

Sia $|\alpha\rangle$ un autoket dell'operatore paritá, allora $P|\alpha\rangle = \pm|\alpha\rangle$, ció significa che la funzione d'onda nello spazio delle coordinate sará

$$\langle -x|\alpha\rangle = \langle x|P|\alpha\rangle = \pm\langle x|\alpha\rangle \tag{7.48}$$

cioé le autofunzioni saranno pari o dispari.

Dalla relazione di commutazione fra P e L si deduce che gli autostati di L hanno una parità definita , cioè

$$\langle \mathbf{n}|P|l, m\rangle = \pm\langle \mathbf{n}|l, m\rangle$$

dove **n** rappresenta una direzione nello spazio. Notiamo che è valida anche la

$$\langle \mathbf{n}|P|l,m\rangle = \langle -\mathbf{n}|l,m\rangle = Y_l^m(\pi-\theta,\phi+\pi) = (-1)^l Y_l^m(\theta,\phi) = (-1)^l\langle \mathbf{n}|l,m\rangle$$

dove $Y_l^m(\theta,\phi)$ è l'armonica sferica nella direzione **n**, da cui si ottiene che

$$P|l,m\rangle = (-1)^l|l,m\rangle$$

L'indipendenza della parità da m discende dal fatto che $[L_\pm, P] = 0$.

7.6 Inversione Temporale

La simmetria discreta di **inversione temporale** va vista sotto un altro punto di vista; considerando il moto di una particella avremo che, se è valida la simmetria temporale, allora l'inversione del tempo ($t \to -t$) fara sì che la particella percorra la stessa traiettoria ma nella direzione inversa; ciò permette di interpretare questa simmetria come una **simmetria di inversione del moto** ($p \to -p$).

L'inversione temporale applicata all'equazione di Schrödinger da

$$i\hbar\frac{\partial\psi(x,-t)}{\partial(-t)} = -i\hbar\frac{\partial\psi(x,-t)}{\partial t} = H\psi(x,-t) \tag{7.49}$$

che non è più l'equazione di Schrödinger (per la presenza del segno meno prima della derivata temporale). Per riottenere un'equazione di Schrödinger dobbiamo considerare la sua complessa coniugata

$$i\hbar\frac{\partial\psi^*(x,-t)}{\partial t} = H\psi^*(x,-t) \tag{7.50}$$

Nello spazio dei momenti la funzione d'onda è data da $\phi(p,t) \to \phi^*(-p,-t)$, quindi la forma di Θ dipende dalla rappresentazione della funzione d'onda.

Un operatore che soddisfi queste proprietà è un operatore antiunitario. Indicando con Θ l'operatore antiunitario di inversione temporale avremo

$$\langle x|\Theta e^{-i\frac{Ht}{\hbar}}|\alpha\rangle = \langle x|e^{-i\frac{-Ht}{\hbar}}|\alpha\rangle^* \tag{7.51}$$

Poichè l'inversione temporale è un inversione del moto ci aspettiemo che il propagatore commuti con Θ, in quanto l'applicazione di Θ al propagatore ci dà il moto inverso che corrisponde all'inversione temporale dello stato per $t = t_0$ ($\Theta|\alpha(t_0)\rangle = |\alpha(t_0)\rangle$) ed alla sua propagazione per tempi negativi (inversione);

$$\Theta e^{-i\frac{Ht}{\hbar}} = e^{-i\frac{-Ht}{\hbar}}\Theta$$

Considerando un'evoluzione infinitesima avremo

$$\Theta\left(1-\frac{iH}{\hbar}dt\right)|\alpha\rangle = \left(1+\frac{iH}{\hbar}dt\right)\Theta|\alpha\rangle$$

da cui

$$-\Theta(iH) = (iH)\Theta$$

quindi, utilizzando l'antiunitarietà, si ottiene

$$[\Theta, H] = 0 \tag{7.52}$$

Possiamo distinguere in operatori dispari come p ($\Theta p \Theta^{-1} = -p$, dovuto al fatto che è un inversione del moto) e pari come x ($\Theta x \Theta^{-1} = x$). L'operatore $L = x \wedge p$ risulta essere dispari per definizione, quindi nell'inversione del moto si inverte anche il momento angolare.

L'azione di Θ su gli autostati di L si deduce dlla relazione di coniugazione delle armoniche sferiche ($Y_l^{m*} = (-1)^m Y_l^{-m}$):

$$\Theta|l, m\rangle = (-1)^m |l, -m\rangle \tag{7.53}$$

Nel caso di sistemi a momento semintero la situazione è differente in quanto si ha

$$\Theta^2 |l_{\text{semintero}}\rangle = -|l_{\text{semintero}}\rangle$$

differentemente dal caso di l intero in cui $\Theta^2 = 1$. La (7.53) è generalizzata nel seguente modo:

$$\Theta|l, m\rangle = i^{2m} |l, -m\rangle \tag{7.54}$$

Capitolo 8

I Gruppi Relativistici

8.1 Il Gruppo di Lorentz

Il gruppo delle trasformazioni di Lorentz è il gruppo che lascia invariato il prodotto scalare (lascia invariata la metrica) fra due quadrivettori, $X^T G X = x^\mu x^\nu g_{\mu\nu} = x^\mu x_\nu$ [1], dove G è la metrica di Minkowski che definiamo come

$$G = g_{\mu\nu} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}; \tag{8.1}$$

l'equazione che definisce il gruppo quindi è

$$g_{\mu\nu}\Lambda^\mu_\alpha \Lambda^\nu_\beta = g_{\alpha\beta} \qquad \Lambda^T G \Lambda = G; \tag{8.2}$$

questo è proprio il gruppo $O(1,3)$. Le (8.2) sono 10 equazioni indipendenti (4 per $\alpha = \beta$ e 6 per $\alpha > \beta$) su un totale di 16 elementi di matrice, quindi il gruppo di Lorentz possiede 6 parametri indipendenti.

Il gruppo di Lorentz possiede 4 componenti non connesse (non esiste nessuna curva continua $\Lambda(t)$ che connette queste componenti); dalla (8.2) ricaviamo che $det(\Lambda^T G \Lambda) = det^2(\Lambda) det G = det G$, cioé $det\Lambda = \pm 1$, per cui possiamo innanzitutto distinguere il gruppo **proprio**, che corrisponde alle trasformazioni con determinante uguale a $+1$ indicato, con $SO(1,3)$, da quello **non proprio**, che corrisponde alle trasformazioni con determinante uguale a -1; inoltre, riutilizzando la definizione del gruppo (8.2), riscritta come $g_{\mu\nu}\Lambda^\mu_\alpha \Lambda^\nu_\beta = \Lambda^0_\alpha \Lambda^0_\beta - \sum_{i=1}^3 \Lambda^i_\alpha \Lambda^i_\beta = g_{\alpha\beta}$ e considerata per $\alpha = \beta = 0$ otteniamo $\sqrt{\sum_i (\Lambda^i_0)^2 + 1} = |\Lambda^0_0|$, cioé è possibile distinguere fra trasformazioni **ortocrone**, con $\Lambda^0_0 \geq 1$, e **non ortocrone**, $\Lambda^0_0 \leq -1$ (in cui vi è inversione temporale).

Il gruppo quoziente fra $O(1,3)$ e le trasformazioni proprie ortocrone di Lorentz

[1] Si utilizza la solita convenzione in cui gli indici greci indicano quadrivettori (vanno da 0 a 4) e gli indici latini indicano i vettori (vanno da 1 a 3).

è formato dalle seguenti quattro matrici:

$$
\begin{array}{lcc}
 & det = +1 & det = -1 \\
\Lambda^0_0 \geq 1 & I = \begin{bmatrix} 1 & 0 \\ 0 & I \end{bmatrix} & P = \begin{bmatrix} 1 & 0 \\ 0 & -I \end{bmatrix} \\
\Lambda^0_0 \leq -1 & PT = \begin{bmatrix} -1 & 0 \\ 0 & -I \end{bmatrix} & T = \begin{bmatrix} -1 & 0 \\ 0 & I \end{bmatrix}
\end{array}
\tag{8.3}
$$

dove I è l'identità, P la parità, T l'inversione temporale e PT è l'inversione spazio-temporale. In questo modo un elemento del gruppo di Lorentz è esprimibile tramite il prodotto fra una di queste matrici (che determina a quale componente connessa appartiene l'elemento) e una matrice del gruppo proprio ortocrono di Lorentz; conseguentemente è sufficiente studiare solo il gruppo proprio ortocrono ($L^{\uparrow}_{+}$ [2]).

8.1.1 I Generatori

Il gruppo delle rotazioni proprie $SO(3)$ è un sottogruppo di $L^{\uparrow}_{+}$ con 3 parametri indipendenti (dovuti alla definizione di matrice ortogonale $\Lambda_r^T \Lambda_r = I$).

$$
\Lambda_r(\theta, \phi, \psi) = \begin{bmatrix} 1 & 0 \\ 0 & R \end{bmatrix} \tag{8.4}
$$

Gli altri elementi del gruppo sono i **boost**[3] (simmetriche $A_b^T = A_b$), anch'essi a 3 parametri; un boost lungo l'asse z corrisponde alla seguente matrice:

$$
\Lambda_b^z(\mu) = \begin{bmatrix} cosh\mu & sinh\mu & 0 & 0 \\ sinh\mu & cosh\mu & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{8.5}
$$

Un boost generico lungo la direzione (θ, ϕ) si ottiene con una rotazione dell'asse z, cioè

$$
\Lambda_b(\theta, \phi, \mu) = \Lambda_r(\theta, \phi, 0)\Lambda_b^z(\mu)\Lambda_r^{-1}(\theta, \phi, 0) \tag{8.6}
$$

Il prodotto fra due rotazioni da ancora una rotazione mentre il prodotto fra due boost è decomponibile nel prodotto fra una rotazione ed un altro boost; una generica trasformazione di Lorentz è sempre decomponibile nel prodotto fra una rotazione ed un boost ($\Lambda = \Lambda_r \Lambda_b$)[4], per un totale di 6 parametri; da questa considerazione abbiamo che possiamo utilizzare come generatori del gruppo $L^{\uparrow}_{+}$ i

[2] La freccia verso l'alto indica che è la componente ortocrona (altrimenti si sarebbe usata la $^{\downarrow}$), mentre il pedice indica il segno del determinante.

[3] Cambi di velocità, accelerazioni.

[4] A differenza delle rotazioni i 3 parametri dei boost, che sono legati alla velocitá del sistema di riferimento, possono variare su $\mathbb{R}^3$, da ció segue che ciascuna delle componenti del gruppo di Lorentz è equivalente a $\mathbb{R}^3 \otimes SO(3)$.

3 generatori del gruppo delle rotazioni ed i 3 generatori dei boost:

$$L_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad K_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$L_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \quad K_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{8.7}$$

$$L_3 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad K_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

a cui sono associati i campi

$$L_i = -i\varepsilon_{ijk} x^j \frac{\partial}{\partial x^k} \qquad K_i = -i\left(t\frac{\partial}{\partial x^i} - x^i \frac{\partial}{\partial t}\right) \tag{8.8}$$

con le relazioni di commutazione

$$[L_i, L_j] = i\varepsilon_{ijk} L_k \qquad [L_i, K_j] = i\varepsilon_{ijk} K_k \qquad [K_i, K_j] = -i\varepsilon_{ijk} L_k \tag{8.9}$$

dove sono state usate le solite regole di quantizzazione ed è stato posto $\hbar = 1$[5].

Le precedenti relazioni possono essere riassunte introducendo una matrice 4×4 antisimmetrica (6 parametri indipendenti) definita come

$$L_{\mu\nu} = -i\left(x^\mu \frac{\partial}{\partial x^\nu} - x^\nu \frac{\partial}{\partial x^\mu}\right) \tag{8.10}$$

$$L_{\mu\nu} = \begin{bmatrix} 0 & -K_1 & -K_2 & -K_3 \\ K_1 & 0 & L_3 & -L_2 \\ K_2 & -L_3 & 0 & L_1 \\ K_3 & L_2 & -L_1 & 0 \end{bmatrix}$$

dove

$$L_i = \varepsilon_{ijk} L_{kj} \qquad K_i = L_{0i} \tag{8.11}$$

$L_{\mu\nu}$ si trasforma come un tensore di rango 2.

Le relazioni di commutazione diventano:

$$[L_{\mu\nu}, L_{\rho\sigma}] = i(g_{\nu\rho}L_{\mu\sigma} - g_{\mu\rho}L_{\nu\sigma} + g_{\mu\sigma}L_{\nu\rho} - g_{\nu\sigma}L_{\mu\rho}). \tag{8.12}$$

[5]Per ottenere una rappresentazione completa del gruppo di Lorentz bisogna definire un operatore paritá tale che

$$PL_kP^\dagger = L_k \qquad PK_kP^\dagger = -K_k$$

in quanto PT è multiplo dell'identitá ($PPT = T = -P$).

8.1.2 Orbite e Piccoli Gruppi

Un **piccolo gruppo** consiste nel sottogruppo delle trasformazioni che lascia invariato un sottospazio dello spazio su cui il gruppo è rappresentato

$$\Lambda^p \overline{p} = \overline{p}$$

Data un particella di massa a riposo m tutti i possibili quadrimomenti che la particella puó assumere devono soddisfare la seguente relazione[6]

$$p^\mu p_\mu = m^2; \tag{8.13}$$

che descrive superfici iperboliche, al variare della massa, nello spazio-tempo.

Esiste un isomorfismo tra la superficie e lo spazio quoziente Λ/Λ^p.

I vettori possono essere classificati in:
1) spaziali $p^\mu p_\mu < 0$;
2) isotropi $p^\mu p_\mu = 0$;
3) temporali $p^\mu p_\mu > 0$.

Una particella si muove sempre su un'orbita fissata dalla condizione (8.13) quindi, ad ogni particella, associamo un piccolo gruppo che ne determina l'evoluzione.

Lo spazio puó quindi essere diviso nelle seguenti componenti connesse:
1) cono superiore T^+ ($p_0 > 0$ e $m^2 > 0$);
2) cono inferiore T^- ($p_0 < 0$ e $m^2 > 0$);
3) superficie conica superiore V^+ ($p_0 > 0$ e $m^2 = 0$);
4) superficie conica inferiore V^- ($p_0 < 0$ e $m^2 = 0$);
5) zona esterna al cono S ($m^2 < 0$);
6) l'origine ($p_0 = 0$ e $m^2 = 0$).

Il piccolo gruppo che lascia invariate $T^\pm$ è il sottogruppo delle rotazioni proprie; quello che lascia invariate le $V^\pm$ sono le rotazioni attorno all'asse lungo cui è diretta la parte spaziale di $\overline{p}$; quello che lascia invariata S è formato dal sottogruppo $SO(1,2)$ delle rotazione attorno all'asse lungo cui è diretta la parte spaziale di $\overline{p}$ e dei boost relativi al suo piano perpendicolare; infine vi è il piccolo gruppo banale dell'origine.

8.2 Il Gruppo di Poincarè

Il **gruppo di Poincarè** è formato dal gruppo di Lorentz piú le traslazioni ed è anche detto **gruppo inomogeneo di Lorentz**

$$x^\mu = \Lambda^\mu_\nu x^\nu + b^\mu \tag{8.14}$$

Da ció si vede che il gruppo di Poincarè è definito come il semiprodotto fra il gruppo additivo dello spazio dei quadrivettori e il gruppo delle trasformazioni di Lorentz (che è un sottogruppo degli automorfismi sullo spazio quadrivettoriale), infatti si ha

[6] Si è posto $c = 1$.

$$(b,\Lambda)(b',\Lambda') = (b+\Lambda b', \Lambda\Lambda')$$

Il prodotto fra due elementi del gruppo si puó scrivere in forma piú compatta attraverso il prodotto fra le due seguenti matrici:

$$\begin{bmatrix} \Lambda & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{(sottogruppo di Lorentz)} \tag{8.15}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & b^1 \\ 0 & 1 & 0 & 0 & b^2 \\ 0 & 0 & 1 & 0 & b^3 \\ 0 & 0 & 0 & 1 & b^0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \text{(sottogruppo delle traslazioni)} \tag{8.16}$$

Una trasformazione infinitesima del gruppo di Lorentz è

$$\Lambda = 1 + i\sum(r_i\mathbf{L}_i - b_i\mathbf{K}_i) = 1 - \frac{i}{2}\sum_{\mu\nu}\epsilon_{\mu\nu}\mathbf{L}_{\mu\nu}$$

dove

$$\epsilon_{\mu\nu} = \begin{bmatrix} 0 & b_1 & b_2 & b_3 \\ -b_1 & 0 & -r_3 & r_2 \\ -b_2 & r_3 & 0 & -r_1 \\ -b_3 & -r_2 & r_1 & 0 \end{bmatrix}$$

I Generatori delle traslazioni sono $P_i = p_i$ e $P_0 = H$, dove p_i sono le componenti del momento e H è l'hamiltoniana; le regole di commutazione sono $[P_\mu, P_\nu] = 0$. Una trasformazione infinitesima è data da

$$1 - i\alpha^\mu P_\mu.$$

Per ottenere le regole di commutazione sfruttiamo la relazione (1.3) dove poniamo $g = e$ ottenendo la seguente

$$(1 - \frac{i}{2}\epsilon_{\mu\nu}\mathbf{L}_{\mu\nu})(1 - i\alpha^\lambda P_\lambda)(1 + \frac{i}{2}\epsilon_{\mu\nu}\mathbf{L}_{\mu\nu}) = 1 - iP_\mu(\alpha^\mu + \epsilon^\mu_\nu\alpha^\nu)$$

da cui

$$[L_i, P_0] = 0 \quad [L_i, P_k] = i\varepsilon_{ikl}P_l \quad [K_i, P_0] = iP_i \quad [K_i, P_k] = i\delta_{ik}P_0$$

cioé

$$[L^{\mu\nu}, P^\lambda] = i(g^{\lambda\nu}P^\mu - g^{\lambda\mu}P^\nu).$$

8.3 La rappresentazione Spinoriale del Gruppo di Lorentz

Il gruppo universale di ricoprimento del gruppo di Lorentz si ottiene ponendo

$$\mathbf{L} = \frac{\sigma}{2} \quad \mathbf{K} = -i\frac{\sigma}{2} \tag{8.17}$$

oppure ponendo

$$\mathbf{L} = \frac{\sigma}{2} \quad \mathbf{K} = +i\frac{\sigma}{2} \tag{8.18}$$

Queste due rappresentazioni non sono in effetti una rappresentazione dell'intero gruppo di Lorentz, in quanto non è possibile definire un operatore paritá che dovrebbe commutare con $i\sigma$ e anticommutare con σ [7]; per una rappresentazione completa del gruppo di Lorentz è necessario combinare le due rappresentazioni, ottenendo cosí la rappresentazione quadridimensionale del gruppo attraverso le matrici γ^μ di Dirac.

Possiamo sfruttare il lemma 78 costruendo delle matrici tali che

$$[\gamma^\mu, \gamma^\nu] = 2g^{\mu\nu} \tag{8.19}$$

dove $g^{\mu\nu}$ è la metrica di Minkowski, ottenendo cosí le matrici γ^μ di Dirac:

$$\begin{aligned} \gamma^0 &= \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix} \quad \gamma^1 = \begin{bmatrix} 0 & \sigma_1 \\ \sigma_1 & 0 \end{bmatrix} \\ \gamma^2 &= \begin{bmatrix} 0 & \sigma_2 \\ \sigma_2 & 0 \end{bmatrix} \quad \gamma^3 = \begin{bmatrix} 0 & \sigma_3 \\ \sigma_3 & 0 \end{bmatrix} \end{aligned} \tag{8.20}$$

Notando che, costruendo uno spazio di Minkowski usando come base le γ^μ di Dirac, avremo che data $\Lambda \in O(1,3)$ le matrici si trasformeranno nel seguente modo

$$\gamma'^\mu = \Lambda^\mu_\nu \gamma^\nu$$

mentre la relazione (8.19) rimane invariata; da ció deduciamo che l'applicazione $g(\Lambda)$ è la **rappresentazione spinoriale** di $O(1,3)$; la rappresentazione spinoriale è definita a meno di una costante moltiplicativa eliminabile imponendo ghe $g \in SL(4,\mathbb{C})$, inoltre è bivalente

$$\Lambda \to \pm g(\Lambda) \in SL(4,\mathbb{C}).$$

8.4 Equazioni d'Onda Relativistiche

L'equazione che descrive una meccanica relativistica deve essere invariante per trasformazioni di Lorentz e puó essere ricavata una volta note le proprietá di trasformazione del campo che descrive.

Un primo invariante puó essere costruito dalla norma del quadrivettore impulso

$$p^\mu p_\mu = m^2$$

[7] $[L_i, P] = 0$ e $\{K_i, P\} = 0$ cioé $[\sigma, P] = 0$ e $\{\sigma, P\} = 0$, dove P è l'operatore paritá.

da cui quantizzando nel modo usuale[8] si ottiene l'equazione di Klein-Gordon

$$(\Box + m^2)\psi = 0$$

dove $\Box = g^{\alpha\beta}\partial_\alpha\partial_\beta$.

L'equazione di Klein-Gordon è un'equazione scalare che presenta due problemi di carattere fisico:

1) descrive anche particelle ad energia negativa[9];

2) la densitá di probabilitá dipende linearmente dall'energia per cui puó assumere valori negativi.

Il problema 2) è risolvibile rendendo lineare l'equazione di Klein-Gordon, cioé scomponendola nel seguente modo:

$$-(\Box + m^2) = (i\gamma^\alpha\partial_\alpha + m)(i\gamma^\beta\partial_\beta - m) \tag{8.21}$$

Dalla decomposizione (8.21) si ottiene la relazione (8.19).

L'equazione

$$(i\gamma^\beta\partial_\beta - m)\psi = 0 \tag{8.22}$$

è l'equazione di Dirac, mentre

$$(i\gamma^\beta\partial_\beta + m)\overline{\psi} = 0 \tag{8.23}$$

è l'equazione coniugata di Dirac dove $\overline{\psi} = \gamma^0\psi^*$ è il coniugato di Dirac dello spinore[10] ψ.

È da notare che di nuovo l'equazione è invariante per compensazione degli indici ($\gamma^\mu p_\mu$).

[8]

$$p^0 \to i\partial_t \qquad p^k \to -i\partial_{x_k}$$

[9]La presenza di particelle ad energia negativa è una conseguenza della relazione quadratica $E = \pm\sqrt{p^2 + m^2}$.

[10]Vettore complesso a quattro componenti.

Appendice A

Esponenziale

Le considerazioni fatte in questa sezione sono relative agli esponenziali di matrici di dimensioni finite, ma possono essere generalizzate ad operatori lineari agenti su spazi infinitodimensionali.

Introduciamo una metrica euclidea nello spazio $\mathbb{R}^{n^2}$ per le matrici quadrate $n \times n$ nel seguente modo:

$$|A|^2 = \sum_{ij} |a_{ij}|^2$$

dove $A = a_{ij}$. Una matrice è limitata se la sua norma è finita ($\|A\| < \infty$); per le seguenti dimostrazioni presupporremo che le matrici siano limitate

Definizione 36 *Con esponenziale di una matrice si intende la serie data da*

$$e^X = \sum_n \frac{X^n}{n!} \tag{A.1}$$

che corrisponde ad uno sviluppo in serie classico dell'esponenziale.

Teorema 80 *La serie e^X converge per ogni matrice X.*

Dimostrazione. La condizione di Cauchy per la convergenza dell'esponenziale è

$$\left\| \frac{X^m}{m!} + \frac{X^{m+1}}{(m+1)!} + ... + \frac{X^{m+k-1}}{(m+k-1)!} \right\| < \frac{\|X\|^m}{m!} + \frac{\|X\|^{m+1}}{(m+1)!} + ... + \frac{\|X\|^{m+k-1}}{(m+k-1)!} \tag{A.2}$$

Al secondo membro abbiamo la condizione di Cauchy della serie relativa a $e^{\|X\|}$, dove $\|X\|$ è un numero, che converge. ■

Proposizione 81 $Be^A B^{-1} = e^{BAB^{-1}}$.

Dimostrazione.

$$e^{BAB^{-1}} = \sum_n \frac{(BAB^{-1})^m}{m!} = \sum_n \frac{B(A)^m B^{-1}}{m!} = B \sum_n \frac{(A)^m}{m!} B^{-1} = Be^A B^{-1}$$

■

Proposizione 82 $\forall A \in M_n(\mathbb{R}) \qquad det(e^A) = e^{trA}$.

Dimostrazione. Per ogni matrice A esiste una matrice $B \in GL_n$ tale che BAB^{-1} sia triangolare (anche con elementi complessi); le matrici triangolari formano gruppo, quindi la matrice e^A è una matrice triangolare il cui determinante è dato dal prodotto fra gli elementi diagonali cioé $det(e^A) = e^{a_{11}}e^{a_{22}}...e^{a_{nn}} = e^{a_{11}+a_{22}+...+a_{nn}} = e^{trA}$. ■

Abbiamo visto che ad ogni matrice $A \in M_n(\mathbb{R})$ possiamo far corrisponde una matrice $e^A \in GL_n^+(\mathbb{R})$, in quanto l'esponenziale è positivo ed invertibile ($GL_n^+(\mathbb{R})$ è formato dalla matrici invertibili con determinante maggiore di 0); ció non significa che ad ogni matrice $B \in GL_n^+(\mathbb{R})$ possiamo associare una matrice A tale che $B = e^A$; infatti l'uguaglianza (A è una matrice diagonale)

$$B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = e^A = \begin{bmatrix} e^{a_{11}} & 0 \\ 0 & e^{a_{22}} \end{bmatrix}$$

è impossibile in quanto non esiste il logaritmo di un numero negativo; differentemente nel campo complesso l'applicazione esponenziale è suriettiva per la definizione del logaritmo complesso.

Proposizione 83 *Se due matrici A e B commutano, allora $e^Ae^B = e^{A+B}$.*

Dimostrazione.

$$e^Ae^B = \left(\sum_k \frac{A^k}{k!}\right)\left(\sum_h \frac{B^h}{h!}\right)$$

$$= \sum_m \frac{1}{m!}\left(\sum_{k+h=m} \frac{m!}{h!k!}A^kB^h\right) = \sum_m \frac{(A+B)^m}{m!} = e^{A+B}$$

avendo usato lo sviluppo binomiale possibile solo nel caso in cui le matrici commutino. ■

Teorema 84 (di Weyl) *Se A e B sono matrici tali che*

$$[A,[A,B]] = [B,[A,B]] = 0$$

allora si ha che $e^{A+B} = e^{-\frac{1}{2}[A,B]}e^Ae^B$.

Dimostrazione. (*di Glauber*) Consideriamo la funzione $F(t) = e^{tA}e^{tB}$;

$$\frac{d}{dt}F(t) = (A + e^{tA}Be^{-tA})F(t)$$

dalla condizione $[A,[A,B]] = [B,[A,B]] = 0$ si ricava per ricorrenza la relazione $[B, A^m] = mA^{m-1}[B,A]$, da cui

$$[B, e^{tA}] = \sum_k \frac{(-t)^m}{m!}[B, A^m] = \sum_k \frac{(-t)^m}{(m-1)!}A^{m-1}[B,A] = -te^{-tA}[B,A]$$

cioé

$$\frac{d}{dt}F(t) = (A + B + t[A,B])F(t)$$

da cui integrando (utilizzando la condizione $F(0) = I$) e ponendo $t = 1$ si ottiene la tesi. ■

Proposizione 85 *Se A e B sono matrici tali che*

$$[A,[A,B]] = [B,[A,B]] = 0$$

allora $e^A e^B = e^{[A,B]} e^B e^A$.

Dimostrazione.

$$e^{-\frac{1}{2}[A,B]} e^A e^B = e^{A+B} = e^{B+A} = e^{-\frac{1}{2}[B,A]} e^B e^A$$

sfruttando, inoltre, il fatto che $[A,B]$ e $[B,A]$ commutano (si dimostra utilizzando l'identitá di Jacobi) si ottiene la tesi. ■

Proposizione 86 *Se $A, B \in M_n(\mathbb{R})$ allora*

$$e^{A+B} = \lim_{n\to\infty} \left(e^{\frac{A}{n}} e^{\frac{B}{n}} \right)^n \quad \textit{(Formula di Lie-Trotter)} \tag{A.3}$$

$$e^{[A,B]} = \lim_{n\to\infty} \left(e^{\frac{A}{n}} e^{\frac{B}{n}} e^{-\frac{A}{n}} e^{-\frac{B}{n}} \right)^{n^2} \tag{A.4}$$

Dimostrazione. Innanzitutto sono verificate le due condizioni

$$\lim_{n\to\infty} [\frac{A}{n}, [\frac{A}{n}, \frac{B}{n}]] = \lim_{n\to\infty} [\frac{B}{n}, [\frac{A}{n}, \frac{B}{n}]] = 0$$

dunque è possibile utilizzare il Teorema 84

$$e^{A+B} = \lim_{n\to\infty} \left(e^{\frac{A}{n}+\frac{B}{n}} \right)^n = \lim_{n\to\infty} \left(e^{-\frac{1}{2}[\frac{A}{n},\frac{B}{n}]} e^{\frac{A}{n}} e^{\frac{B}{n}} \right)^n = \lim_{n\to\infty} \left(e^{\frac{A}{n}} e^{\frac{B}{n}} \right)^n$$

avendo utilizzato il fatto che $\frac{[A,B]}{n^2}$ è di ordine superiore rispetto a $\frac{A}{n}, \frac{B}{n}$.

$$e^{[A,B]} = \lim_{n\to\infty} \left(e^{[\frac{A}{n},\frac{B}{n}]} \right)^{n^2} = \lim_{n\to\infty} \left(e^{\frac{A}{n}} e^{\frac{B}{n}} e^{-\frac{A}{n}} e^{-\frac{B}{n}} \right)^{n^2}$$

■

Appendice B

La misura di Haar

Su di un gruppo topologico compatto G possiamo definire una misura μ detta **misura di Haar**.

Data una funzione $f \in L^1(G)$ (ciò significa che f è integrabile su G tramite la misura μ) definiamo una **media invariante** su G nel seguente modo:

$$M(f) = \int_G f(g) d\mu(g). \tag{B.1}$$

Le proprietà della media invariante sono:

1. $M(I) = 1$, dove I è l'applicazione identica e dove si è posto $\int_G d\mu(g) = \mu(G) = 1$;
2. $M(\overline{f}) = \overline{M(f)}$;
3. $M(f) \geq 0$ per $f \geq 0$ e $M(f) > 0$ se f è continua, $f \geq 0$ e $f \neq 0$;
4. $M(f_1 + f_2) = M(f_1) + M(f_2)$;
5. $M(\alpha f) = \alpha M(f)$, dove α è un numero;
6. $M(f(gh)) = M(f(hg)) = M(f(g))$;
7. $M_g(f(g^{-1})) = M_g(f(g))$.

Le proprietà 1)$^{\underline{a}}$5) sono le proprietà dell'integrale, mentre la 6) e la 7) sono relative all'invarianza (a destre ed a sinistra) della misura sul gruppo G (equivalenti all'invarianza del consueto integrale su $\mathbb{R}$ in cui si può sostituire dx con $d(x + a)$, dove a è una costante).

Bibliografia

[1] B. A. Dubrovin, S. P. Novikov, A. T. Fomenko, "Geometria Contemporanea", vol. 1, Editori Riuniti.

[2] M. A. Najmark, A. I. Štern, "Teoria delle Rappresentazioni dei Gruppi", Editori Riuniti.

[3] A. O. Barut, R. Rączka, "Theory of Group Representations and Applications", PWN.

[4] P. Caressa, "Metodi Matematici della Meccanica Quantistica", Roma, 1994, http://www.math.unifi.it/ caressa/math/mec-quan/mmmq.html

[5] A. Romano, G. Starita, "Meccanica Razionale (parte prima)", Liguori Editore.

[6] J. J. Sakurai, "Meccanica Quantistica Moderna", Zanichelli.

[7] K. Gottfried, "Quantum Mechanics", W. A. Benjamin INC..

[8] G. Esposito, G. Marmo e G. Sudarshan, "From Classical to Quantum Mechanics", Cambridge University Press, 2004.

[9] Y. S. Kim, Marilyn E. Noz, "Theory and Applications of Poincaré Group", D. Reidel Publishing Company.

[10] N. Cabibbo, "Relativitá - Teoria di Dirac", 28 gennaio 2003, http://chimera.roma1.infn.it/NICOLA/poincare.pdf

[11] B. Baumslang, B. Chandler, "Theory and Problems of Group Theory", serie Schaum, McGraw-Hill.

[12] M. Artin, "Algebra", Bollati Boringhieri, 1997.

[13] A. G. Kurosh, "The Theory of Groups", vol. I e II, Chelsea Publishing Company, New York, 1955.