Capitolo 5

GRUPPI, ALGEBRE E RAPPRESENTAZIONI

In questo capitolo collezioniamo alcune definizioni, teoremi ed esempi relativi alle strutture algebriche più pervasive nella matematica: i gruppi, le algebre e le loro rappresentazioni. Diamo solo alcune conseguenze quasi immediate della definizione di gruppo (nella III parte studieremo a fondo le strutture di gruppo che intervengono in meccanica quantistica: i gruppi topologici e di Lie), mentre per le algebre ci limitiamo alle definizioni ed agli esempi di dimensione finita, dato che una classe importante di algebre a dimensione infinita, le algebre di operatori, saranno esaminate dettagliatamente nella II parte. Le rappresentazioni sono pure introdotte nel caso di dimensione finita: in appendice 5.6 è data una trattazione elementare dei prodotti tensoriali per rendere autosufficiente l'esposizione di questi concetti.

5.1 Gruppi

5.1.1 Definizione *Un insieme G dotato di una operazione $\cdot : G \times G \longrightarrow G$ si dice un* gruppo *se l'operazione $\cdot$ (che si indicherà semplicemente per giustapposizione dei suoi operandi) è:*

(1) *associativa, cioè $g(g'g'') = (gg')g''$;*

(2) *possiede identità $e \in G$, cioè $ge = eg = g$;*

(3) *ogni elemento g possiede un inverso, cioè esiste $g^{-1} \in G$ tale che $gg^{-1} = g^{-1}g = e$.*

5.1.2 Definizione *Un gruppo si dice* abeliano *(o* commutativo*) se l'operazione è commutativa (i.e. $gg' = g'g$). Se un gruppo è finito, la sua cardinalità si dice* ordine *del gruppo.*

5.1.3 Esempio

(1) *Uno spazio vettoriale rispetto alla somma di vettori è un gruppo abeliano.*

(2) *L'insieme S_X delle funzioni biunivoche di un insieme X in sé è un gruppo (non abeliano a meno che* $\operatorname{Card} X \leq 2$*).*

(3) *L'insieme degli interi $\mathbb{Z}$ è un gruppo rispetto alla somma, come pure il "reticolo" $\mathbb{Z}^n$ dei vettori in $\mathbb{R}^n$ a coordinate intere.*

(4) *Se V è uno spazio vettoriale reale di dimensione finita, l'insieme delle applicazioni lineari invertibili (isomorfismi lineari) di V n sé è un gruppo $GL(V)$ rispetto alla composizione, che si dice* gruppo lineare generale*; se fissiamo una base in V, i.e. un isomorfismo $V \cong \mathbb{R}^n$ allora $GL(V) = GL_n(\mathbb{R})$ è il* gruppo delle matrici invertibili di ordine *n: l'operazione di gruppo è in questo caso il prodotto di matrici (righe per colonne).*

Se G e H sono gruppi e $f : G \longrightarrow H$ è una funzione, si dice che f è un *omomorfismo*[1] se $f(gg') = f(g)f(g')$. Se inoltre f è iniettiva (risp. suriettiva, biunivoca) si dice che è un *monomorfismo* (risp. *epimorfismo, isomorfismo*) del gruppo G nel gruppo H. Gruppi isomorfi sono da considerarsi equivalenti ed ovviamente la classe dei gruppi rispetto agli omomorfismi forma una categoria.

5.1.4 Esempio *Se G è il gruppo dei numeri reali rispetto alla somma e H il gruppo dei numeri reali positivi rispetto al prodotto, allora la funzione esponenziale $x \in G \longmapsto e^x \in H$ è un isomorfismo.*

Se G è un gruppo e $S, T \subset G$ sono sottoinsiemi, definiamo

$$ST := \{s \cdot t \,|\, s \in S, t \in T\}$$

Se $f : G \longrightarrow H$ è un omomorfismo allora la sua immagine $\operatorname{im} f = f(G)$ è un sottoinsieme di H tale che $(\operatorname{im} f)(\operatorname{im} f) \subset \operatorname{im} f$ dato che $f(g)f(g') = f(gg')$.

5.1.5 Definizione *Un sottoinsieme H di un gruppo G tale che $HH \subset H$ si dice* sottogruppo *di G e si scrive in questo caso $H < G$.*

Anche il *nucleo* del morfismo f

$$\ker f := \{g \in G \,|\, f(g) = e\}$$

è un sottogruppo, che gode anche della proprietà $(\ker f)G = G(\ker f)$ (infatti se $k \in \ker f$ e $g \in G$: $f(kg) = f(k)f(g) = f(g) = f(g)f(k) = f(gk)$). In altri termini, se $g \in G$ e $k \in \ker f$ allora $gkg^{-1} \in \ker f$.

[1] Si tratta della nozione analoga a quella di applicazione lineare nel caso degli spazi vettoriali: molte definizioni che si danno per gli spazi vettoriali (funzioni lineari, sottospazi, quozienti, prodotti) si generalizzano ai gruppi..

5.1.6 Definizione *Un sottogruppo $H < G$ tale che $HG = GH$ si dice* normale *e si scrive $H \lhd G$.*

5.1.7 Esempio *Se G è abeliano, ogni sottogruppo è automaticamente normale: in particolare nel caso di uno spazio vettoriale rispetto alla somma.*

Come nel caso degli spazi vettoriali, un omomorfismo $f : G \longrightarrow H$ è iniettivo se e solo se $\ker f = \{e\}$; in generale $i : \ker f \hookrightarrow G$; ovviamente $f : G \longrightarrow \operatorname{im} f$ è un epimorfismo, e la composizione $i \circ f$ è identicamente e. Si esprime questo dicendo che la successione

$$(*) \qquad \{e\} \longrightarrow \ker f \longrightarrow G \longrightarrow \operatorname{im} f \longrightarrow \{e\}$$

è *esatta*. Nel caso degli spazi vettoriali esiste una nozione analoga: se V, W e Z sono spazi vettoriali e $f : V \longrightarrow W$, $g : Z \longrightarrow V$ sono mappe lineari, la successione

$$Z \xrightarrow{g} V \xrightarrow{f} W$$

è esatta se $\ker f = \operatorname{im} g$; quindi se $Z = 0$ l'esattezza vuol dire l'iniettività di f e se $W = 0$ vuol dire la suriettività di g. La stessa cosa nel caso di gruppi qualsiasi.

Un modo diverso di esprimere la (*) è dire che il gruppo $\operatorname{im} f$ è *quoziente del gruppo G modulo il sottogruppo* $\ker f$.

In generale, se G è un gruppo e $K \lhd G$ è un sottogruppo normale allora l'insieme

$$G/K := \{gK \mid g \in G\}$$

dei sottoinsiemi di G della forma gK è un gruppo rispetto al prodotto

$$(gK)(g'K) = (gg')K$$

e si dice *gruppo quoziente modulo K*. Gli elementi gK di G/K si dicono *classi laterali* (sinistre) di G modulo K.

5.1.8 Proposizione *I sottogruppi normali di G sono esattamente i nuclei dei possibili omomorfismi di G in un altro gruppo.*

DIMOSTRAZIONE: Che se $f : G \longrightarrow H$ è un omomorfismo allora $\ker f \lhd G$ già lo sappiamo; viceversa, se $K \lhd G$ allora la proiezione $p : G \longrightarrow G/K$ è un epimorfismo di nucleo K.

QED

Nel caso della (*) $G/\ker f$ è isomorfo, tramite l'isomorfismo $G/\ker f \longmapsto \operatorname{im} f$, a $\operatorname{im} f$. Si noti che, se H non è normale, G/H non è un gruppo.

Se G e H sono gruppi il prodotto $G \times H$ è un gruppo rispetto a

$$(g,h)(g',h') := (gg',hh')$$

Evidentemente questa definizione si generalizza al prodotto di una famiglia qualsiasi di gruppi; il gruppo $G \times H$ si dice *prodotto diretto* dei gruppi G e H: i fattori si immergono nel prodotto con due immersioni

$$\begin{array}{rccc} i_G: & G & \hookrightarrow & G \times H \\ & g & \longmapsto & (g,e) \end{array} \qquad \begin{array}{rccc} i_H: & H & \hookrightarrow & G \times H \\ & h & \longmapsto & (e,h) \end{array}$$

che sono monomorfismi: quindi $G < G \times H$ e $H < G \times H$. Inoltre i sottogruppi G e H sono normali, e si ha

$$G \times H/G \cong H \qquad \text{e} \qquad G \times H/H \cong G$$

(un isomorfismo fra i gruppi G e G' si indica con $G \cong G'$). Quindi la struttura di $G \times H$ è in un certo senso determinata da quella di G e H: ogni volta che un gruppo ha sottogruppi normali, passando ai quozienti si trovano gruppi "meno complicati" del gruppo di partenza. Questo motiva la seguente

5.1.9 Definizione *Un gruppo G è* semplice *se non ha sottogruppi normali non banali.*

"Non banali" vuol dire diversi da $\{e\}$ e G stesso, che sono ovviamente sottogruppi normali di G.

Se $H, H' < G$ sono sottogruppi, anche $H \cap H'$ lo è, ovviamente; se $S \subset G$ è un sottoinsieme qualsiasi, il *sottogruppo generato da S* è

$$\langle S \rangle := \bigcap_{S \subset H < G} H$$

l'intersezione di tutti i sottogruppi che contengono S. In particolare, per $S = \{s\}$ si scrive $\langle g \rangle$ per il sottogruppo generato dall'elemento $g \in G$.

Naturalmente g è formato da e, g, gg,... Usiamo la notazione esponenziale scrivendo g^n in luogo di $g \cdots g$ (n volte): allora è ovvio che $g^n g^m = g^{n+m}$ e quindi che $\langle g \rangle$ è abeliano.

5.1.10 Esempio *Consideriamo il gruppo $\mathbb{Z}$ rispetto alla somma: l'identità è $e = 0$; se consideriamo $1 \in \mathbb{Z}$ allora ogni elemento di $\mathbb{Z}$ è della forma $1 + \cdots + 1$ (n volte) e quindi $\mathbb{Z} = \langle 1 \rangle$.*

5.1.11 Definizione *Se un gruppo G è generato da un suo elemento $g \in G$, i.e. se $G = \langle g \rangle$, si dice* ciclico.

Quindi $\mathbb{Z}$ è ciclico. Notiamo che possiamo definire un gruppo ciclico finito per ogni numero naturale n: basta considerare un insieme $C_n = \{c_0, ..., c_{n-1}\}$ e definire il prodotto ponendo

$$c_1^k := c_k$$

($k = 0, ..., n-1$.) Otteniamo così un gruppo ciclico generato da c_1 con n elementi, il cui elemento unità è $c_0 = e$.

Un modo familiare di rappresentare questo gruppo è considerare le classi di congruenza di numeri interi modulo n: $\mathbb{Z}_n$. Rispetto alla somma (modulo n) si tratta esattamente di C_n (l'isomorfismo è la mappa $c : \mathbb{Z}_n \longrightarrow C_n$ data da $c(n) = c_n$).

Notiamo che, *se n è un numero primo allora C_n è un gruppo semplice*: in effetti, dato che è abeliano, bisogna mostrare che non ha sottogruppi non banali; sia $C < C_n$ un sottogruppo e sia $c_k \in C$; se $c_1 = c_k$ allora $C = C_n$; altrimenti, C contiene di certo il sottogruppo (ciclico) generato da c_k; ma dato che $c_k^m = e$ per un certo m e $c_k \in C_n$, deve essere $m|n$; se n è primo questo non è possibile a meno che $m = n$ (col che $c_k = c_1$) oppure $m = 1$ (col che $c_k = e$); quindi $C = \{e\}$ oppure $C = C_n$.

Il gruppo $\mathbb{Z}$ lo consideriamo come C_∞; non esistono in effetti gruppi ciclico di cardinalità maggiore al numerabile:

5.1.12 Teorema *Un gruppo ciclico è finito o numerabile e due gruppi ciclici C_n e C_m sono isomorfi se e solo se $n = m$ ($n, m \in \mathbb{N} \cup \{\infty\}$).*

DIMOSTRAZIONE: Sia $\langle g \rangle$ un gruppo ciclico infinito: allora, per definizione, le potenze g^n sono tutte distinte fra loro, e quindi la mappa

$$g^n \longmapsto n$$

è un isomorfismo fra $\langle g \rangle$ e $\mathbb{Z}$: è ovviamente biunivoca, ed è un omomorfismo perché $g^n g^m = g^{n+m}$.

Se invece $\langle g \rangle$ è un gruppo ciclico finito, esiste un n tale che $g^n = e$; sia n minimo rispetto a questa proprietà; allora la mappa $c : g^n \longmapsto c_n$ è un isomorfismo di $\langle g \rangle$ in C_n.

QED

Nei gruppi, a differenza che negli spazi vettoriali, può manifestarsi il fenomeno della torsione, vale a dire, un elemento $g \in G$ può avere una potenza pari all'unità e: $\exists n > 0 \; g^n = e$. Il minimo intero che soddisfa questa relazione si dice *ordine*

dell'elemento g. Ad esempio nel caso di un gruppo ciclico finito, il suo generatore ha ordine pari all'ordine del gruppo.

Esiste, nel caso dei gruppi, una nozione analoga a quella di base per gli spazi vettoriali. Se ogni elemento di G si esprime come prodotto di numero finito di elementi di un certo sottoinsieme fissato $S \subset G$, si dice che gli elementi di S *generano il gruppo*. In altri termini, S è un insieme di generatori di G se

$$G = \langle S \rangle$$

In generale la cardinalità di un sistema di generatori potrà variare, non si può cioè parlare di "dimensione" di un gruppo. Tuttavia un gruppo può essere *finitamente generato*, cioè può avere un insieme finito di generatori. Un teorema fondamentale, per il quale si rimanda ai testi specialistici, afferma che *un gruppo abeliano finitamente generato è il prodotto diretto di un gruppo ciclico finito C_n e di un reticolo $\mathbb{Z}^m$ di interi.*

5.2 Azioni di gruppi

Abbiamo visto che se X è un insieme, possiamo considerare l'insieme di tutte le funzioni biunivoche di X in sé: si tratta di un gruppo rispetto alla composizione di applicazioni (l'elemento unità è la funzione identità $x \longmapsto x$ e l'inverso è la funzione inversa).

In particolare, se X è un insieme finito, otteniamo il *gruppo S_n delle permutazioni* di n oggetti:

$$i = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ i(1) & i(2) & i(3) & ... & i(n) \end{pmatrix}$$

Possiamo infatti vedere S_n come l'insieme delle funzioni biunivoche $i : \{1, .., n\} \longrightarrow \{1, .., n\}$.

Questo gruppo è di fondamentale importanza, specie nelle applicazioni in Fisica e Chimica; osserviamo che contiene tutte le permutazioni possibili di n oggetti, quindi ha ordine[2] $n!$.

5.2.1 Teorema (CAYLEY) *Ogni gruppo finito di ordine n è (isomorfo a) un sottogruppo del gruppo simmetrico S_n.*

[2]In effetti per costruire una permutazione i su n oggetti $\{1, 2, ..., n\}$ cominciamo a stabilire quale sia il suo valore $i(1)$ su 1; abbiamo n scelte possibili per questo, e ne restano $(n-1)$ per il valore $i(2)$; una volta assegnato anche questo valore, restano $(n-2)$ scelte possibili per $i(3)$ e così via fino a $i(n)$ che risulterà una scelta obbligata. In definitiva abbiamo $n(n-1)(n-2)...2$ possibili permutazioni.

DIMOSTRAZIONE: Sia G un gruppo finito di ordine n: possiamo supporre che S_n sia l'insieme delle funzioni biunivoche di G in sé (nella definizione di gruppo simmetrico non conta affatto la natura degli elementi che permuta: tutti gli insiemi finiti della stessa cardinalità sono equivalenti da questo punto di vista). Allora, se $g \in G$ definiamo

$$L_g : G \longrightarrow G$$

come

$$L_g(g') := gg'$$

Fissato $g \in G$, L_g è una funzione biunivoca: infatti

$$L_g(g') = L_g(g'') \iff gg' = gg'' \iff g' = g''$$

(poiché esistono gli inversi in un gruppo vale la legge di cancellazione). Quindi $L_g \in S_n$, ed abbiamo quindi definito una funzione

$$L : G \longrightarrow S_n$$

Dimostriamo che si tratta di un monomorfismo di gruppi. Intanto è iniettiva: se $g, g' \in G$ allora

$$\forall h \in G \quad L_g(h) = L_{g'}(h) \iff gh = g'h \iff g = g'$$

(di nuovo per cancellazione), e quindi $L : g \longmapsto L_g$ è iniettiva; infine è un omomorfismo di gruppi:

$$Lgg'(h) = gg'h = g(g'h) = L_g(g'h) = L_gL_{g'}(h)$$

QED

L'idea usata in questa dimostrazione è di fondamentale importanza: la funzione L_g si dice *rappresentazione regolare*, ed è un caso particolare del concetto generale di *rappresentazione*.

Osserviamo intanto che, chiaramente, la dimostrazione si estende al caso di cardinalità qualsiasi: *ogni gruppo G è un sottogruppo del gruppo S_X delle trasformazioni biunivoche di un insieme X, della stessa cardinalità di G, in sé.*

Ovviamente l'insieme S_G è in generale molto misterioso; tuttavia possiamo sempre ridurci a particolari classi di trasformazioni biunivoche, e precisamente a quelle lineari.

Per il momento studiamo comunque il concetto di rappresentazione più in generale.

5.2.2 Definizione *Se G è un gruppo e X un insieme, si dice che G* agisce su X *se esiste un omomorfismo di gruppi $A : G \longrightarrow S_X$ (che si dice* azione del gruppo sull'insieme*).*

Esplicitamente, una azione A soddisfa le

$$\forall g, g' \in G \; \forall x \in X \quad A_{gg'}x = A_g A_{g'} x \tag{5.1}$$

$$\forall x \in X' \quad A_e x = x \tag{5.2}$$

Si scrive più semplicemente gx in luogo di $A_g x$ (o, ancora peggio, di $A(g)x$ che sarebbe la scrittura più pedantemente corretta).

Ad esempio, la rappresentazione regolare L_g è una azione di G su sé stesso; bisognerebbe chiamarla "rappresentazione regolare sinistra", dato che, se il gruppo non è commutativo, $L_g h \neq L_h g$, e si può definire una *rappresentazione regolare destra* come

$$R_g h := hg$$

Un'altra rappresentazione di G in sé è la *rappresentazione coniugata*:

$$A_g h := ghg^{-1}$$

Si noti che $A_g = L_g R_{g^{-1}}$. Un elemento della forma ghg^{-1} si dice *coniugato* di h rispetto a g; il coniugio è una relazione di equivalenza, come è facile verificare (vedremo questo fatto più in generale fra breve).

5.2.3 Definizione *Se G agisce su un insieme X e sia $x \in X$; allora*

(1) *Lo* stabilizzatore *dell'elemento x è il sottogruppo G_x di G definito come*

$$G_x := \{g \in G \,|\, gx = x\}$$

(2) *L'*orbita *di x in X è il sottoinsieme Gx di X definito come*

$$Gx := \{y \in X \,|\, \exists g \in G \; gy = x\}$$

Quindi lo stabilizzatore di un elemento è il sottogruppo (che lo sia segue dalle definizioni) formato dagli elementi del gruppo che "fissano" un punto dell'insieme X, mentre l'orbita di un elemento è l'insieme degli altri punti di X che possono "essere spostati" su x agendo con elementi di G. Intuitivamente pensiamo a X come ad uno spazio e a G come ad un gruppo di trasformazioni di quello spazio.

5.2.4 Esempio *Se $X = \mathbb{R}^n$ e $G = GL_n(\mathbb{R})$ allora la moltiplicazione di una matrice per un vettore fornisce una azione di G su $\mathbb{R}^n$.*

5.2.5 Teorema *Le orbite dell'azione di un gruppo G su un insieme X formano la partizione di X in classi rispetto alla relazione di equivalenza*

$$x \approx y \iff \exists g \in G \; gx = y$$

Questo segue dalle definizioni; quindi possiamo sempre decomporre X in unione di sottoinsiemi disgiunti:

$$X = \bigcup_{x \in X} Gx$$

che si chiamano *orbite* dell'azione.

Osserviamo che la rappresentazione regolare può definirsi da G sull'insieme dei sotto-gruppi di G: se $H < G$:

$$gH = \{gh \,|\, h \in H\}$$

i.e. g manda H nella sua classe laterale sinistra gH: evidentemente lo stabilizzatore di H è H stesso

$$G_H = \{g \in G \,|\, gH = H\} = H$$

e l'orbita

$$GH = \{H' < G \,|\, \exists g \in G \; gH' = H\}$$

è in corrispondenza biiunivoca con l'insieme dei laterali sinistri G/H. In particolare, se il gruppo G è finito, abbiamo, per il teorema precedente:

$$\operatorname{Card} G = \sum_{gH \in G/H} \operatorname{Card} gH$$

Ma gH è in corrispondenza biunivoca con H, quindi le classi hanno tutte la stessa cardinalità $\operatorname{Card} H$:

$$\operatorname{Card} G = \operatorname{Card} H \cdots \operatorname{Card} H = [G : H] \operatorname{Card} H$$

ove $[G : H]$ è l'intero che moltiplicato per $\operatorname{Card} H$ dà $\operatorname{Card} G$: si dice *indice del sottogruppo* H in G.

In particolare

5.2.6 Teorema (Lagrange) *Un sottogruppo H di un gruppo finito G ha ordine che divide l'ordine di G.*

Questo teorema è un criterio notevole per determinare la struttura di un gruppo (e.g: se l'ordine di un gruppo è un numero primo, non possiede sottogruppi non banali).

5.2.7 Definizione *Se un'azione di G su X ha come unica orbita X stesso, si dice* transitiva.

Quindi un'azione è transitiva se ogni elemento di X può essere trasformato in qualsiasi altro per mezzo di qualche $g \in G$.

5.2.8 Lemma *Se G agisce su X e $x, y \in X$ stanno nella stessa orbita allora gli stabilizzatori G_x e G_y sono coniugati.*

DIMOSTRAZIONE: Se $y \in Gx$ allora esiste $g \in G$ con $gx = y$; consideriamo dunque l'azione di coniugio in g $A_g : h \longmapsto ghg^{-1}$; allora

$$gG_xg^{-1} = G_y$$

dato che se $h \in Gx$ se e solo se $ghg^{-1}y = ghx = gx = y$.

QED

Quindi se $y \in Gx$ esiste $g \in G$ tale che $gx = y$ e questo g è unico a meno di elementi di G_x: infatti $gx = y$ e $g'x = y$ implicano che $gx = g'x$ i.e. $g^{-1}g' \in G_x$. Quindi ogni classe gG_x corrisponde in modo unico ad un elemento $y \in Gx$ tramite la $gG_x \longmapsto gx$. Ne segue il

5.2.9 Teorema *Se G agisce su X e $x \in X$ allora esiste una corrispondenza biunivoca fra Gx e G/G_x.*

Importante è il caso transitivo:

5.2.10 Corollario *Se G agisce transitivamente su un insieme X allora, per ogni $x \in X$, esiste una corrispondenza biunivoca*

$$G/G_x \longleftrightarrow X$$

Ad esempio, consideriamo l'azione di G su se stesso data dal coniugio:

$$g \cdot h = ghg^{-1}$$

Osserviamo che, per ogni gruppo, è definito il suo *centro*

$$Z(G) := \{g \in G \,|\, \forall g' \in G \; gg' = g'g\}$$

Si tratta cioè del sottoinsieme degli elementi di G che commutano con tutti gli altri. Si tratta evidentemente di un sottogruppo normale, e notiamo che, se $z \in Z(G)$:

$$zhz^{-1} = zz^{-1}h = h$$

Viceversa, se $ghg^{-1} = h$ allora $g \in Z(G)$; quindi $Z(G)$ è il *nucleo* dell'azione di coniugio, secondo la

5.2.11 Definizione *Se G agisce su X, il* nucleo dell'azione *è il sottogruppo normale*

$$Z := \{g \in G \,|\, \forall x \in X \;\; gx = x\}$$

In altri termini il nucleo di un'azione è l'intersezione degli stabilizzatori di tutti gli elementi di X:

$$Z = \bigcap_{x \in X} G_x$$

Un'azione che abbia nucleo banale ($Z = \{e\}$) si dice *fedele*: ad esempio la rappresentazione regolare sinistra (o destra) è fedele.

Tornando all'esempio dell'azione di coniugio, chiediamoci come sono fatte le orbite e gli stabilizzatori. Se $h \in G$ allora

$$G_h = \{g \in G \,|\, gh = hg\} =: Z_h(G)$$

è il *centralizzante* dell'elemento h in G, i.e. il sottogruppo degli elementi che commutano con un elemento fissato h. Le orbite dell'azione coniugata sono

$$Gh = \{h' \in G \,|\, \exists g \in G \;\; gh'g^{-1} = h\}$$

e si dicono *classi coniugate* di G contenenti h.

Se il gruppo è finito, allora la decomposizione in orbite

$$G = \bigcup_{g \in G} Gh$$

decompone il gruppo nelle sue classi coniugate: dato che $Ge = Z(G)$ (la classe coniugata dell'identità è il centro), e dato che ogni singola classe è l'orbita, per i teoremi precedenti:

$$\operatorname{Card} G = \operatorname{Card} Z(G) + \sum_g [G : G_g]$$

(g varia in G modulo l'appartenenza ad uno stesso stabilizzatore) ove $[G : H]$ denota l'*indice* del sottogruppo H; questa si chiama *equazione delle classi*, ed è fondamentale in teoria dei gruppi finiti.

Ad esempio deduciamo da essa un lemma della teoria dei *p-gruppi*, importante nell'ambito della teoria dei gruppi finiti.

5.2.12 Teorema *Se G è un p-*gruppo *(i.e. è finito ed ha ordine p^N ove p è un numero primo) allora $Z(G)$ non è banale.*

DIMOSTRAZIONE: Se G è abeliano, si ha per definizione $G = Z(G)$ e quindi il teorema è banale; altrimenti l'equazione delle classi è

$$p^n = \operatorname{Card} Z(G) + \sum [G : G_h]$$

Ma se $\operatorname{Card} G = p^n$, la cardinalità di un suo sottogruppo è della forma p^m con $m < n$ e quindi $\operatorname{Card}[G : H] = p^{n-m}$. Quindi p divide l'ordine di $Z(G)$.

QED

Osserviamo che l'azione di coniugio non solo opera sull'insieme G, ma anche sull'insieme dei sottogruppi di G: se $H < G$ allora

$$A_g H := gHg^{-1}$$

Rispetto a questa azione, lo stabilizzatore di un punto è

$$G_H = \{g < G \,|\, gHg^{-1} = H\} =: N(H)$$

il *normalizzante* del sottogruppo H: per definizione si tratta del più piccolo sottogruppo di G che contenga H come sottogruppo normale (in particolare, $H \lhd G \iff N(H) = G$). L'orbita di un punto è

$$G \cdot H = \{H' < G \,|\, \exists g \in G \; gH'g^{-1} = H\}$$

Si noti che la mappa $h \longmapsto ghg^{-1}$ è un isomorfismo del gruppo in sé: quindi gli elementi di GH sono sottogruppi fra loro isomorfi. In particolare, al variare di $g \in G$, l'insieme dei coniugati gHg^{-1} di H è esattamente l'insieme G/H:

$$G \cdot H = G/H$$

5.3 Rappresentazioni di gruppi

Rappresentare un gruppo vuol dire realizzarlo come il gruppo delle trasformazioni di un opportuno insieme X: in realtà, spesso X sarà un insieme dotato di qualche struttura, ad esempio uno spazio topologico, ed in questo caso si richiederà che le trasformazioni del gruppo preservino questa struttura, ad esempio che siano degli omeomorfismi.

5.3.1 Definizione *Se V è uno spazio vettoriale, una* rappresentazione lineare *di G è un omomorfismo del gruppo nel gruppo $GL(V)$ delle applicazioni lineari ed invertibili di V in sé.*

Spesso si dice semplicemente che lo spazio V è la rappresentazione del gruppo, qualora sia chiara l'azione di G su $GL(V)$.

Sono possibili altri tipi di rappresentazioni: ad esempio, se X è uno spazio proiettivo, una *rappresentazione proiettiva* di G è un omomorfismo del gruppo nel gruppo $PGL(X)$ delle trasformazioni proiettive invertibili di X in sé.

Tuttavia, nella discussione sulle rappresentazioni di un gruppo ci si limita al caso lineare, ed alle particolarizzazioni di questo (ad esempio le rappresentazioni unitarie, se X non solo è uno spazio vettoriale ma ha anche una struttura euclidea o hermitiana). Questa non è una limitazione troppo forte: se infatti è data una rappresentazione ρ di un gruppo G nel gruppo S_X di tutte le applicazioni (invertibili) di un insieme X in se stesso, possiamo sempre associargli una rappresentazione π lineare ponendo

$$(\pi(g)f)(x) = f(\rho(g^{-1})(x))$$

ove f appartiene allo spazio vettoriale di tutte le funzioni definite su X.

Quindi per noi una rappresentazione di un gruppo G sarà un omomorfismo di G nel gruppo $GL(V)$ di un certo spazio vettoriale *complesso*: potremmo considerare spazi vettoriali su campi qualsiasi, ma la teoria classicamente si sviluppa su $\mathbb{C}$, che ha proprietà notevoli come l'essere algebricamente chiuso e di caratteristica zero; inoltre nel caso di rappresentazioni di dimensione infinita, si usa l'Analisi Funzionale (cfr. capitolo **??**) che essenzialmente ha luogo negli spazi complessi. Per ora limiteremo la discussione al caso di rappresentazioni di dimensione finita, ove la *dimensione di una rappresentazione* è la dimensione dello spazio V. In altri termini, siamo interessati a vedere quanto un gruppo possa considerarsi un gruppo di matrici...

Ad esempio consideriamo un gruppo che già è un gruppo di matrici, $GL(V)$; esiste una rappresentazione ovvia di questo gruppo in V:

$$A \cdot v := Av$$

che si dice *rappresentazione identica*.

In generale gli elementi del gruppo verranno fatti corrispondere a matrici, i cui coefficienti saranno i *coefficienti della rappresentazione*; naturalmente questi coefficienti dipendono dalla scelta della base; tuttavia, il cambiamento di base in V avviene per coniugio rispetto ad elementi di $GL(V)$, così che, se $\pi : G \longrightarrow GL(V)$ è una rappresentazione e $A \in GL(V)$ una matrice di cambiamento di base, allora $\pi(g)v = \pi(g)(Av'A^{-1})$ e quindi la rappresentazione non deve dipendere dalla coniugazione per una matrice:

$$A\pi(g) = \pi(g)A$$

5.3.2 Definizione *Due rappresentazioni $\pi : G \longrightarrow GL(V)$ e $\pi' : G \longrightarrow GL(V')$ si dicono* equivalenti *se esiste un isomorfismo $A : V \longrightarrow V'$ tale che*

$$A\pi(g) = \pi'(g)A$$

Dato che una rappresentazione agisce su uno spazio vettoriale, possiamo provare ad estendere le nozioni dell'Algebra Lineare alla teoria delle rappresentazioni: in particolare considereremo i concetti di sottospazio, quoziente, morfismi, dualità, somma diretta, prodotto tensoriale e prodotto scalare.

Se $\pi : G \longrightarrow GL(V)$ è una rappresentazione del gruppo G, un sottospazio W di V si dice *invariante* se

$$\forall g \in G \quad \pi(g)W \subset W$$

Evidentemente, in questo caso, la restrizione $\pi|_W$ è una rappresentazione $\pi|_W : G \longrightarrow GL(W)$ che si dice *sottorappresentazione* di π.

In modo analogo, sul quoziente V/W di uno spazio per un sottospazio invariante è definita una rappresentazione $\widetilde{\pi} : G \longrightarrow GL(V/W)$ che si dice *quoziente* della rappresentazione π.

5.3.3 Definizione *Se V è una rappresentazione di G e W una sottorappresentazione, V si dice* riducibile *se il complemento di W in V è pure un sottospazio invariante: in questo caso la rappresentazione π si decompone in somma diretta delle rappresentazioni $\pi|_W$ e $\pi|_{W^\perp}$.*

Se $W \subset V$ è una sottorappresentazione, allora la matrice che rappresenta V sarà a blocchi della forma

$$\pi(g) = \begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}$$

ove $A(g) = \pi|_W(g)$ e $C(g)$ è la matrice della rappresentazione quoziente; se V è riducibile, allora possiamo trovare una base in cui la matrice B è zero.

5.3.4 Definizione *Una rappresentazione V che non abbia sottorappresentazioni non banali (cioè diverse da V stesso e dalla rappresentazione nulla) si dice irriducibile.*

5.3.5 Esempio *Una rappresentazione di dimensione 1 è irriducibile: si tratta semplicemente di un omomorfismo di gruppi*

$$\pi : G \longrightarrow \mathbb{C} \setminus 0 = GL_1(\mathbb{C})$$

ed uno spazio di dimensione 1 non ha sottospazi non banali.

5.3.6 Definizione *Se una rappresentazione V è tale che ogni sua sottorappresentazione ammetta una sottorappresentazione complementare, si dice che V è completamente riducibile.*

Non è affatto detto che una rappresentazione di dimensione finita sia completamente riducibile.

5.3.7 Esempio *Consideriamo $G = \mathbb{R}$ (gruppo additivo dei numeri reali) e la sua rappresentazione bidimensionale*

$$t \longmapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$$

Allora $V = \mathbb{R}^2$, e $t(x, y) = (x + ty, y)$; il sottospazio $\{(x, 0)\}$ è invariante, mentre $\{(0, y)\}$ non lo è, quindi la rappresentazione non è completamente riducibile.

5.3.8 Esempio *Se $G = \mathbb{R}$ è ancora il gruppo additivo dei numeri reali e $V = \mathbb{R}[x]$ lo spazio dei polinomi su $\mathbb{R}$, possiamo considerare la rappresentazione di G in V (che ha dimensione infinita):*

$$(\pi(t)p)(x) := p(x + t)$$

Se V_k è il sottospazio di V dei polinomi di grado al più k, evidentemente è un sottospazio invariante per π. Le rappresentazioni V_k sono tutte riducibili (per $k \geq 1$) me non completamente riducibili, dato che in esse i sottospazi invarianti V_{k-1} non hanno complementi invarianti.

Gli elementi di $\hom_G(V_k, V_h)$ sono operatori differenziali a coefficienti costanti: da questo segue che

$$\dim \hom_G(V_k, V_h) = 1 + \min(h, k)$$

per ogni k, h, e quindi anche $\dim \hom_G(V_k, V) = 1 + k$.

D'altra parte si trova che $\dim \hom_G(V, V_k) = 0$: infatti ogni polinomio f può scriversi come derivata $(k+1)$-ma di un altro polinomio F e se $A \in \hom_G(V_k, V)$ allora deve commutare con le traslazioni, e quindi anche con le derivate, sicché

$$Af = A\frac{d^{k+1}f}{dx^{k+1}} = \frac{d^{k+1}Af}{dx^{k+1}} = 0$$

(dato che $Af \in V_k$).

5.3.9 Definizione *Se* $\pi_1 : G \longrightarrow GL(V_1)$ *e* $\pi_2 : G \longrightarrow GL(V_2)$ *sono rappresentazioni di un gruppo* G *negli spazi vettoriali* V_1 *e* V_2*, l'insieme degli operatori* di allacciamento *è*

$$(\pi_1, \pi_2) := \{A \in \hom(V_1, V_2) \mid A\pi_1 = \pi_2 A\}$$

Questo insieme si denota anche $\hom_G(V_1, V_2)$ *ed i suoi elementi si dicono anche* morfismi *fra le rappresentazioni* π_1 *e* π_2*.*

L'insieme delle rappresentazioni di un gruppo forma una categoria rispetto ai morfismi di rappresentazioni, come è immediato verificare.

Evidentemente A è un morfismo fra la rappresentazione $\pi_1 : G \longrightarrow GL(V_1)$ e la rappresentazione $\pi_2 : G \longrightarrow GL(V_2)$ se e solo se il seguente diagramma

$$\begin{array}{ccc} V_1 & \xrightarrow{A} & V_2 \\ {\scriptstyle \pi_1(g)}\downarrow & & \downarrow{\scriptstyle \pi_2(g)} \\ V_1 & \xrightarrow[A]{} & V_2 \end{array}$$

è commutativo per ogni $g \in G$.

La dimensione dello spazio vettoriale $\hom_G(V_1, V_2)$ si dice *numero di allacciamento* delle rappresentazioni π_1 e π_2.

Per rappresentazioni di dimensione finita, si ha che

$$\dim \hom_G(V_1, V_2) = \dim \hom_G(V_2, V_1)$$

5.3.10 Definizione *Se* $\dim \hom_G(V_1, V_2) = 0$ *le rappresentazioni si dicono* disgiunte.

Ovviamente

5.3.11 Proposizione *Le rappresentazioni sono equivalenti se e solo se l'insieme dei morfismi* $\hom_G(V_1, V_2)$ *contiene un isomorfismo.*

Osserviamo che se due rappresentazioni di dimensione finita sono equivalenti, allora le loro dimensioni coincidono, ed è possibile trovare basi in questi spazi vettoriali tali che le matrici che rappresentano gli operatori della rappresentazione coincidano. Il risultato fondamentale sulle rappresentazioni irriducibili è il

5.3.12 Lemma (SCHUR) *Se* V_1 *e* V_2 *sono rappresentazioni irriducibili di un gruppo* G *allora ogni elemento (non nullo) di* $\hom_G(V_1, V_2)$ *è invertibile.*

Dimostrazione: Sia $A \in \hom_G(V_1, V_2)$ non nullo: allora il nucleo di A è un sottospazio di V_1:

$$\ker A = \{v \in V_1 \,|\, Av = 0\}$$

Dato che $g \cdot Av = Ag \cdot v$ allora se $v \in \ker A$: $Ag \cdot v = gAv = 0$, quindi $gv \in \ker A$. Dunque $\ker A$ è una sottorappresentazione di V_1, che però è irriducibile. Ne segue che $\ker A = 0$ oppure $\ker A = V_1$.

Se $\ker A = V_1$ allora $A = 0$ per definizione; se $\ker A = 0$ allora A è invertibile. Ma l'immagine di A è un sottospazio di V_2

$$\operatorname{im} A = \{w \in V_2 \,|\, \exists v \in V_1 \;\; Av = w\}$$

ed è una sottorappresentazione di V_2: infatti se $w \in \operatorname{im} A$ allora $gw = gAv = Agv$, quindi gw è immagine di gv tramite A i.e. $gw \in \operatorname{im} A$. Per irriducibilità di V_2 segue che $\operatorname{im} A = 0$ oppure $\operatorname{im} A = V_2$; ma A era invertibile, quindi $\operatorname{im} A \neq 0$, i.e. $\operatorname{im} A = V_2$ sicché A è un isomorfismo.

QED

In altri termini, un morfismo fra due rappresentazioni irriducibili è zero oppure è un isomorfismo: in particolare due rappresentazioni irriducibili distinte non possono essere contenute l'una nell'altra. Questo ci dice che le rappresentazioni irriducibili sono le più semplici possibili: in effetti una rappresentazione irriducibile si chiama anche *semplice*.

Consideriamo ora una rappresentazione $\pi : G \longrightarrow GL(V)$ di un gruppo; osserviamo che, se $\dim V = 1$ allora $V = \mathbb{K}$ e quindi

$$\forall g \in G \quad \pi(g) = id_{\mathbb{K}}$$

(infatti $\pi(g)(k) = k\pi(g)(1) = k$: cioè $\operatorname{im} \pi = \{id_V\}$ è il sottogruppo banale formato dal solo isomorfismo $v \longmapsto v$). Una rappresentazione la cui immagine si riduca al solo elemento id_V si dice *banale*; abbiamo appena visto che su uno spazio vettoriale di dimensione 1 esiste solo la rappresentazione banale π_0. Se $\pi : G \longrightarrow GL(V)$ è una rappresentazione allora gli operatori di (π, π_0) sono quindi funzionali lineari $f \in V^*$ tali che $f\pi = f$.

5.3.13 Definizione *Gli elementi di* (π, π_0) *si dicono* invarianti *della rappresentazione.*

In realtà è significativo considerare come invarianti non solo le funzioni lineari su V, ma anche i polinomi su V, che possono esser visti come gli elementi dell'algebra simmetrica $\operatorname{Sym}(V^*)$.

Se $\pi : G \longrightarrow GL(V)$ è una rappresentazione, possiamo considerare sullo spazio duale V^* una rappresentazione $\pi^* : G \longrightarrow GL(V^*)$ definita come:

$$\langle \pi^*(g)(A), v \rangle = \langle f, \pi(g^{-1})v \rangle$$

($\langle , \rangle$ è la dualità fra V e V^*). è immediato verificare che si tratta in effetti di una rappresentazione, che viene detta *duale* (o *contrograduiente*) di π: in coordinate, la matrice di $\pi^*(g)$ è la trasposta di $\pi(g^{-1})$.

Torniamo ora alle sottorappresentazioni: se V è una rappresentazione (di dimensione finita) e $V_1 \subset V$ una sottorappresentazione che ammette un complementare, questo vuol dire che il sottospazio vettoriale $V_2^{\perp} \subset V$ (i.e. lo spazio tale che $V_1 \oplus V_2 = V$) è pure una sottorappresentazione: in questo caso V di decompone in *somma diretta di sottorappresentazioni*. La matrice che rappresenta un elemento di G in $GL(V)$ è della forma

$$\pi(g) = \begin{pmatrix} A_1(g) & 0 \\ 0 & A_2(g) \end{pmatrix}$$

ove A_1 è la matrice che rappresenta G in $GL(V_1)$ e A_2 è la matrice che rappresenta G in $GL(V_1)$.

Una rappresentazione che si decompone in somma diretta di sottorappresentazioni irriducibili si dice talvolta *semisemplice*: dimostriamo ora che le rappresentazioni semisemplici sono esattamente quelle completamente riducibili: lo faremo per rappresentazioni di dimensione qualsiasi.

5.3.14 Lemma *Se V è una rappresentazione completamente riducibile allora ogni sua sottorappresentazione è completamente riducibile.*

DIMOSTRAZIONE: Sia V una rappresentazione completamente riducibile, e W una sottorappresentazione di V: allora ogni sottorappresentazione Z di W è anche una sottorappresentazione di V, quindi esiste una sottorappresentazione Z' di V tale che $Z' \oplus Z = V$; dato che $Z \subset W \subset V$ allora

$$Z' \cap W = (0)$$

Inoltre $W = Z + (Z' \cap W)$ e questa somma è diretta; quindi $Z' \cap W$ è una sottorappresentazione complementare di Z in W.

QED

5.3.15 Lemma *Se V è una rappresentazione completamente riducibile allora possiede una sottorappresentazione irriducibile.*

DIMOSTRAZIONE: Se V ha dimensione finita questo si vede facilmente per induzione; dimostriamolo tuttavia in generale: se $V \neq 0$ esisterà $v \in V \setminus 0$; sia $\mathcal{R}(v)$ l'insieme delle sottorappresentazioni di V che non contengono v. $\mathcal{R}(v)$ è non vuoto, dato che 0 è una sottorappresentazione che non contiene v, ed è un insieme parzialmente ordinato dall'inclusione: dimostriamo che soddisfa le ipotesi del

Lemma di Zorn. Se $\{R_i\}$ è un sottoinsieme totalmente ordinato di $\mathcal{R}(v)$ l'unione $\bigcup_i R_i$ è chiaramente una sottorappresentazione di V che non contiene v, ed è un confine superiore per gli $\{R_i\}$: quindi possiamo applicare il lemma di Zorn e dedurre l'esistenza di un massimale $R \subset V$ che non contenga v. Ora, dato che V è completamente riducibile, esiste una sottorappresentazione Q complementare a R, che contiene v. Dimostriamo che è irriducibile.

Supponiamo che Q contenga una sottorappresentazione Q_1: allora (essendo Q completamente riducibile per il lemma precedente) esiste una sottorappresentazione Q_2 di Q tale che $Q = Q_1 \oplus Q_2$; supponiamo che $v \notin Q_1$. Allora $Q_1 + R$ è una sottorappresentazione di V che non contiene v e contiene R, il che contraddice la massimalità di R. Quindi una tale decomposizione di Q non esiste e Q è irriducibile.

QED

5.3.16 Teorema *Una rappresentazione è completamente irriducibile se e solo se si decompone in somma diretta di rappresentazioni irriducibili.*

Dimostrazione: Dimostriamo che se V è somma diretta di sottorappresentazioni irriducibili allora è completamente riducibile: sia W una sottorappresentazione di V; dobbiamo mostrare che ammette una sottorappresentazione complementare. Sia $\mathcal{R}$ l'insieme di tutte le sottorappresentazioni irriducibili S tali che $S \cap W = 0$ e consideriamo la famiglia $\mathcal{S}$ degli elementi della forma $\oplus_i S_i$ con $S_i \in \mathcal{R}$; $\mathcal{S}$ è non vuota (non lo è $\mathcal{R}$: contiene 0) ed è ordinata dall'inclusione: dimostriamo che soddisfa le ipotesi del lemma di Zorn. Se $\{R_j\}$ è una sottofamiglia di $\mathcal{S}$ totalmente ordinata, basta porre $R = \bigoplus_j R_j$ per avere un confine superiore in questa famiglia. Quindi per il lemma di Zorn esiste un elemento massimale in $\mathcal{S}$, i.e. una somma diretta $\bigoplus_i S_i$ di sottorappresentazioni irriducibili di V tali che $S_i \cap W = 0$. Dimostriamo che $V = \bigoplus_i S_i \oplus W$. Sappiamo per ipotesi che V è

$$V = \bigoplus_j V_j$$

ove le V_j sono irriducibili e quindi, per ogni i, $S_i = \bigoplus S_i \cap V_j$ i.e. $S_i = V_{j_i}$ per qualche j_i (per irriducibilità delle S_i e V_j ed il lemma di Schur). Quindi

$$V = \bigoplus_i S_i \oplus \bigoplus_{j \neq j_i} V_j$$

Ci basta quindi dimostrare che $W = \bigoplus_{j \neq j_i} V_j$. Ora certamente $W \subset \bigoplus_{j \neq j_i} V_j$; se l'inclusione fosse stretta, esisterebbe $j \neq j_i$ tale che $W \cap V_j = 0$ (infatti V_j è irriducibile); ma allora $V_j \oplus \bigoplus_i S_i$ sarebbe un elemento di $\mathcal{S}$ il che contraddice la massimalità di $\oplus_i S_i$. Quindi $W = \bigoplus_{j \neq j_i} V_j$.

Viceversa, se V è completamente riducibile consideriamo la somma diretta W di tutte le sottorappresentazioni irriducibili di V (si tratta di un sottospazio $\neq 0$ per il lemma 5.3.15): vogliamo dimostrare che $W = V$. In effetti, se $W \subset V$, allora, per completa riducibilità di V, W avrebbe una sottorappresentazione complementare $W^\perp$; ma questa sottorappresentazione è completamente riducibile per il lemma 5.3.14 e quindi deve possedere una sottorappresentazione irriducibile Z (per il lemma 5.3.15) quindi Z è una sottorappresentazione irriducibile di V, e, per definizione, $Z \subset W$. Il che è assurdo ($W \cap W^\perp = 0$) a meno che $W^\perp = 0$ e quindi $W = V$.

QED

Assieme alla somma diretta, la costruzione più importante dell'Algebra Lineare è il prodotto tensoriale (cfr. 5.6): ci limitiamo nella discussione seguente al caso di dimensione finita.

Se $\pi_i : G \longrightarrow GL(V_i)$ $(i = 1, 2)$ sono rappresentazioni di un gruppo G, definiamo una funzione $\pi_1 \otimes \pi_2 : G \longrightarrow GL(V_1 \otimes V_2)$

$$\pi_1 \otimes \pi_2(g)(v_1 \otimes v_2) := (\pi_1(g)v_1) \otimes (\pi_2(g)v_2)$$

che di dice *prodotto tensoriale delle rappresentazioni*.

5.3.17 Proposizione *Se V_1 e V_2 sono rappresentazioni di un gruppo allora il prodotto tensoriale $V_1 \otimes V_2$ è una rappresentazione del gruppo.*

DIMOSTRAZIONE: Ovviamente $\pi_1 \otimes \pi_2(e)(v_1 \otimes v_2) = v_1 \otimes v_2$. Inoltre

$$\begin{aligned}\pi_1 \otimes \pi_2(gh)(v_1 \otimes v_2) =& \pi_1(gh)v_1 \otimes \pi_2(gh)v_2 \\ =& \pi_1(g)\pi_1(h)v_1 \otimes \pi_2(g)\pi_2(h)v_2 \\ =& \pi_1 \otimes \pi_2(g)\pi_1 \otimes \pi_2(h)(v_1 \otimes v_2)\end{aligned}$$

QED

Il prodotto tensoriale di rappresentazioni è legato al prodotto diretto di gruppi:

5.3.18 Teorema *Ogni rappresentazione irriducibile (di dimensione finita) V del prodotto diretto $G = G_1 \times G_2$ è equivalente al prodotto tensoriale di rappresentazioni irriducibili V_i dei gruppi G_i.*

DIMOSTRAZIONE: V_1 e V_2 sono rappresentazioni irriducibili di G_i se e solo se $V_1 \otimes V_2$ è una rappresentazione irriducibile di G: infatti ogni rappresentazione $V_1 \otimes V_2$ induce due rappresentazioni ottenute considerando gli operatori $id_{V_1} \otimes \pi_2(g)$ e $\pi_1(g) \otimes id_{V_2}$.

L'unica cosa che dobbiamo verificare è che ogni rappresentazione di $G_1 \times G_2$ sia della forma $V_1 \otimes V_2$; sia π una rappresentazione in V di $G_1 \times G_2$, e siano

$$V_1 = \pi(g, e)(V) \qquad \text{e} \qquad V_2 = \pi(e, g)(V)$$

Si tratta di rappresentazioni, rispetto alle restrizioni di π sul primo e sul secondo fattore diretto di $G_1 \times G_2$; ovviamente

$$\pi(g, h)(v_1, v_2) = (\pi(g, e)(v_1), \pi(e, h)v_2)$$

e quindi abbiamo una famiglia di funzioni bilineare $V_1 \times V_2 \longrightarrow V$ data da

$$\pi(g, h)(v_1, v_2) = \pi(g, h)(v_1, v_2)$$

Per la proprietà del prodotto tensoriale abbiamo quindi $V = V_1 \otimes V_2$.

QED

Si noti che se V e W sono rappresentazioni irriducibili di G non è affatto vero che $V \otimes W$ sia irriducibile per G: lo è solo per $G \times G$. In generale decomporre un prodotto tensoriale in somma di rappresentazioni irriducibili è un problema fondamentale (teoria di Clebsh–Gordan) per il quale si rimanda ai testi specialistici.

Infine consideriamo ancora una costruzione degli spazi vettoriali che ha un significativo riverbero in teoria delle rappresentazioni: supponiamo infatti che lo spazio V sia unitario, i.e. che (sia complesso e) possegga un prodotto hermitiano (v, w) definito positivo (i.e. quella che si dice una *forma sesquilineare*: $(av+bw) = a\bar{b}(v, w)$). Ricordiamo che una trasformazione lineare $A : V \longrightarrow V$ è *unitaria* se

$$\forall v, w \in V \quad (Av, Aw) = (v, w)$$

In termini di matrici questo significa, ovviamente, che

$$\overline{A^T} A = I$$

In particolare $|\det A| = 1$ i.e. $\det A \in \mathbb{T} = \{|z| = 1\}$ e quindi una matrice unitaria è invertibile, cioè determina necessariamente un isomorfismo di V in sé. Dunque le matrici unitarie formano un sottogruppo del gruppo lineare generale (complesso[3])

$$U(V) = \{A : V \longrightarrow V \,|\, \overline{A^T} A = I\} \subset GL(V)$$

[3]Si noti che $GL_n(\mathbb{C}) \subset GL_{2n}(\mathbb{R})$: infatti una struttura complessa su uno spazio vettoriale è sempre una struttura di spazio vettoriale reale $2n$-dimensionale, mentre non ogni matrice reale $2n \times 2n$ preserva la struttura complessa, i.e. la moltiplicazione per i numeri complessi.

5.3.19 Definizione *Una rappresentazione $\pi_G \longrightarrow GL(V)$ è* unitaria *se V è uno spazio unitario e* $\operatorname{im}\pi \subset U(V)$.

In altri termini, π è unitaria se G agisce per operatori unitari su V. Scriveremo A^* in luogo di $\overline{A^T}$.

Le rappresentazioni unitarie sono le più importanti, perché vige il seguente

5.3.20 Teorema *Una rappresentazione unitaria (di dimensione finita) è completamente riducibile.*

DIMOSTRAZIONE: Consideriamo una rappresentazione unitaria V di un gruppo G; se $W \subset V$ è un sottospazio invariante per G basta costruire un complementare invariante per avere la completa riducibilità. Consideriamo quindi il complemento ortogonale $W^\perp$ rispetto al prodotto hermitiano di V. Allora

$$\forall v \in W \ \forall w \in W^\perp \quad (\pi(g)w, v) = (\pi(g)^{-1}\pi(g)w, \pi(g)^{-1}v) = (w, \pi(g)^{-1}v) = 0$$

dato che $\pi(g) \in U(V)$ e v è invariante; quindi $\pi(g)w \in W^\perp$ e $W^\perp$ è invariante.

QED

Abbiamo quindi una condizione sufficiente per la completa riducibilità di una rappresentazione: che sia equivalente ad una rappresentazione unitaria.

5.3.21 Definizione *Due rappresentazioni π_1, π_2 qualsiasi di un gruppo G in uno stesso spazio unitario V sono* unitariamente equivalenti *se esiste un operatore unitario $A \in (\pi_1, \pi_2)$.*

Questa condizione, per rappresentazioni unitarie, non è più restrittiva della semplice equivalenza:

5.3.22 Proposizione *Se due rappresentazioni unitarie sono equivalenti allora sono unitariamente equivalenti.*

DIMOSTRAZIONE: Utilizziamo un fatto ben noto dall'Algebra Lineare: la decomposizione polare di un operatore: supponiamo che A sia un isomorfismo di V in sé appartenente a (π_1, π_2); allora

$$A = U|A|$$

ove $|A|$ è un operatore hermitiano (i.e. $|A| + |A|^* = 0$) e U è unitario. Quindi la $\pi_1(g)A = A\pi_2(g)$ diviene

$$\pi_1(g)U|A| = U|A|\pi_2(g)$$

Sostituendo g^{-1} e tenendo conto che $\pi(g^{-1}) = \pi(g)^*$ abbiamo che $\pi_1(g)^* U|A| = U|A|\pi_2(g)^*$ i.e. applicando * e tenendo conto che $A^*B^*) = (BA)^*$:

$$|A|^* U \pi_1(g) = \pi_2(g)|A|^* U$$

i.e. $(U^*U = I)$

$$\begin{aligned} |A|^2\pi_2(g) =& |A|^* U^* U|A|\pi_2(g) = |A|U^* A\pi_2(g) \\ =& |A|U^*\pi_1(g)U|A| = |A|^* U\pi_1(g)U|A| = \\ =& \pi_2(g)|A|^* UU|A| = \pi_2(g)|A|^2 \end{aligned}$$

quindi $|A|^2$ (e dunque anche $|A|$) commuta con $\pi_2(g)$. Allora

$$U\pi_2(g)|A| = U|A|\pi_2(g) = \pi_1(g)U|A|$$

e, dato che $|A|$ è invertibile

$$\pi_1(g)U = U\pi_2(g)$$

i.e. $U \in (\pi_1, \pi_2)$ e quindi le rappresentazioni sono unitariamente equivalenti.

QED

Concludiamo con un risultato cruciale per la teoria dei gruppi finiti:

5.3.23 Teorema *Ogni rappresentazione di dimensione finita di un gruppo finito è equivalente ad una rappresentazione unitaria.*

Dimostrazione: Sia V una rappresentazione di G: possiamo considerare su V un prodotto hermitiano qualsiasi, ad esempio fissando una base $(e_1, ..., e_n)$ di V e ponendo, se $v = \sum_i v_i e_i$ e $w = \sum_i w_i e_i$:

$$(v, w) = \sum_{i=1}^{n} v_i \overline{w_i}$$

Ovviamente rispetto a questo prodotto non è affatto detto che la rappresentazione sia unitaria: possiamo comunque definire un nuovo prodotto hermitiano per il quale lo è: basta considerare[4] (il gruppo è finito)

$$(v, w)' := \frac{1}{\operatorname{Card} G} \sum_{g \in G} (\pi(g)v, \pi(g)w)$$

[4]Stiamo sommando sul gruppo, cioè "integrando": in effetti questo ragionamento si estende a tutti i gruppi sui quali esista una misura invariante, e.g. i gruppi compatti.

$(.)'$ è un prodotto hermitiano: è lineare perché lo sono π, $(.)$ e la somma; inoltre è definito positivo perché lo è $(.)$; infine la rappresentazione è unitaria rispetto ad esso:

$$\begin{aligned}(\pi(h)v, \pi(h)w)' =& \frac{1}{\operatorname{Card} G} \sum_{g\in G} (\pi(g)\pi(h)v, \pi(g)\pi(h)w) \\ =& \frac{1}{\operatorname{Card} G} \sum_{g\in G} (\pi(gh)v, \pi(gh)w) \\ =& \frac{1}{\operatorname{Card} G} \sum_{k\in G} (\pi(k)v, \pi(k)w) = (v, w)'\end{aligned}$$

ove $k = gh$; se g descrive G anche gh descrive G con h costante.

QED

5.3.24 Corollario *Ogni rappresentazione di dimensione finita un gruppo finito è completamente riducibile.*

5.4 Algebra di gruppo

Approfondiamo ora la teoria delle rappresentazioni dei gruppi finiti: G sarà sempre un gruppo finito con elemento neutro e.

Molti concetti che svilupperemo sono validi in generale, come la nozione di *carattere*. Ricordiamo dall'Algebra Lineare le proprietà della traccia

$$\operatorname{tr} A = \sum_{i=1}^{n} a_{ii}$$

di una matrice $A \in M_n(\mathbb{K})$ su un campo $\mathbb{K}$ (ad esempio sui numeri complessi):

5.4.1 Proposizione

(1) $\operatorname{tr}(aA + bB) = a \operatorname{tr} A + b \operatorname{tr} B$ *se* $a, b \in \mathbb{C}$ *e* $A, B \in M_n(\mathbb{C})$

(2) $\operatorname{tr} AB = \operatorname{tr} BA$

(3) $\operatorname{tr} I = n$

(4) $\operatorname{tr} ABA^{-1} = \operatorname{tr} B$

(5) *La traccia di A è la somma degli autovalori di A contati con le loro molteplicità.*

Consideriamo ora una rappresentazione $\pi : G \longrightarrow GL(V)$ di un gruppo finito: per la (4) della proposizione, per ogni operatore $F \in End(V)$ è ben definita la sua traccia, come la traccia di una qualsiasi matrice che rappresenti F in qualche base di V.

5.4.2 Definizione *Il* carattere *della rappresentazione π è la funzione $\chi_\pi : G \longrightarrow \mathbb{C}$ data da*

$$\chi_\pi(g) = \operatorname{tr} \pi(g)$$

Evidentemente il carattere di una rappresentazione ha valori in $GL(\mathbb{C}) = \mathbb{C}\backslash 0$, ed è un invariante nel senso seguente

5.4.3 Proposizione *I caratteri di due rappresentazioni equivalenti coincidono.*

(Questo segue direttamente da $\operatorname{tr} ABA^{-1} = \operatorname{tr} B$). Inoltre

$$\chi\pi^*(g) = \chi_\pi(g^{-1})^*$$

e quindi, se π è unitaria

$$\chi(g^{-1}) = \overline{\chi(g)}$$

Notiamo anche che

$$\chi_{\pi_1 \oplus \pi_2} = \chi_{\pi_1} + \chi_{\pi_2}$$

Per il prodotto vale la

5.4.4 Proposizione $\chi_{\pi_1 \otimes \pi_2} = \chi_{\pi_1}\chi_{\pi_2}$.

DIMOSTRAZIONE: Basta fissare due basi $(e_1, ..., e_n)$ di V_1 e $(f_1, ..., f_m)$ di V_2; allora

$$\pi_1(g) = ((a_{ij})) \qquad \pi_2(g) = ((b_{rs}))$$

e quindi $\pi_1 \otimes \pi_2(g)$ è una matrice i cui indici sono coppie di indici: $((c_{irjs})) = ((a_{ij}b_{rs}))$; ne segue che

$$\chi_{\pi_1 \otimes \pi_2} = \sum_{i,r=1}^{n} c_{irir} = \sum_{i,r=1}^{n} a_{ii}b_{rr} = \sum_{i=1}^{n} a_{ii} \sum_{i=1}^{n} b_{rr} = \chi\pi_1\chi_{\pi_2}$$

QED

La traccia si dice essere una "funzione di classe", perché è invariante rispetto alla coniugazione di matrici: il riverbero di questo fatto a livello di caratteri è il

5.4.5 Teorema *Il carattere di una rappresentazione è costante sulle classi coniugate del gruppo.*

Ricordiamo ora che ogni rappresentazione finito-dimensionale di un gruppo finito G è completamente riducibile: vogliamo trovare una tale decomposizione per ogni rappresentazione: i caratteri giocano un ruolo in questa ricerca.

Consideriamo la *rappresentazione regolare sinistra* del gruppo, che già ci è venuta in soccorso, ad esempio nel dimostrare che il gruppo è un sottogruppo di S_n:

$$L_g(h) = gh$$

Questa rappresentazione ne induce una sullo spazio di tutte le funzioni del gruppo:

$$\mathbb{C}[G] = \mathbb{C}^G = \{F : G \longrightarrow \mathbb{C}\}$$

come

$$(L_g(F))(h) = F(gh)$$

Lo spazio $\mathbb{C}[G]$ è uno spazio vettoriale di dimensione $\operatorname{Card} G$ rispetto alla somma di funzioni, e quindi è una rappresentazione, ed è unitaria rispetto al prodotto hermitiano

$$(F, G)_F = \frac{1}{\operatorname{Card} G} \sum_{g \in G} F(g)\overline{G(g)}$$

dato che $\sum_{g\in G} H(hg) = \sum_{g\in G} H(g)$ (invarianza per traslazioni). Vedremo che tutte le rappresentazioni irriducibili del gruppo sono sottorappresentazioni di $\mathbb{C}[G]$.

Sia $\pi : G \longrightarrow GL(V)$ una rappresentazione (di dimensione finita) di G, e consideriamo lo spazio degli invarianti di V

$$V^G := \{v \in V \mid \forall g \in G\ \pi(g)v = v\}$$

e la funzione di *media*

$$I(v) := \frac{1}{\operatorname{Card} G} \sum_{g \in G} \pi(g)(v)$$

Ora, $I : V \longrightarrow V^G$ è un epimorfismo di spazi vettoriali: infatti è per definizione lineare, e se $v \in V^G$ allora, sempre per definizione

$$v = \pi(g)v = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \pi(g)v$$

quindi I è una proiezione sul sottospazio V^G:

$$I(I(v)) = I(v) = v$$

Rammentiamo che V può supporsi unitaria (il gruppo è finito) e quindi completamente riducibile: il metodo della media ci dà uno spunto per tentare di decomporre V nelle sue sottorappresentazioni irriducibili.

Dato che $I^2 = I$ su V^G:

$$\dim V^G = \dim \operatorname{im} I = \operatorname{tr} I = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \operatorname{tr} \pi(g) = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \chi(g)$$

Osserviamo che, se V è irriducibile, dato che V^G è una sottorappresentazione, si ha $V^G = V$ oppure $V^G = 0$: nel primo caso V è la rappresentazione banale $\pi(g) = id_V$, nel secondo

$$\sum_{g \in G} \chi(g) = 0$$

Ora consideriamo due rappresentazioni irriducibili $\pi : G \longrightarrow GL(V)$ e $\rho : G \longrightarrow GL(W)$, e la loro rappresentazione associata $\hom(V, W)$ (si noti che è $\hom(V, W) = V^* \otimes W$); dato che è il prodotto tensoriale di W per la rappresentazione duale di V abbiamo che

$$\chi_{\hom(\pi,\rho)} = \overline{\chi_\pi} \chi_\rho$$

Osserviamo inoltre che

$$\hom(V, W)^G = (\pi, \rho)$$

e quindi, per il lemma di Schur, $\dim \hom(V, W)^G = \delta_{VW}$ è zero se le rappresentazioni non sono equivalenti e 1 se lo sono. Dalla formula precedente per la dimensione di V^G segue che

5.4.6 Teorema (Ortogonalità dei caratteri) *Se V e W sono rappresentazioni irriducibili di dimensione finita di un gruppo finito allora*

$$\frac{1}{\operatorname{Card} G} \sum_{g \in G} \chi_W(g) \overline{\chi_V(g)} = \begin{cases} 1 & \text{se } V \cong W \\ 0 & \text{altrimenti} \end{cases}$$

Dato che $\chi \in \mathbb{C}[G]$, questo si scrive anche

$$(\chi_W, \chi_W)_F = \delta_{VW}$$

Quindi i caratteri sono un insieme ortonormale in $\mathbb{C}[G]$: di più, sono una base ortonormale nel sottospazio delle funzioni costanti sulle classi coniugate.

5.4.7 Corollario *Il numero di rappresentazioni irriducibili di un gruppo finito G è minore o uguale al numero di classi coniugate di G.*

Infatti, due rappresentazioni irriducibili sono equivalenti se e solo se i loro caratteri coincidono, la corrispondenza che assegna ad una rappresentazione il suo carattere è iniettiva.

5.4.8 Esempio *Se il gruppo è abeliano, le classi coniugate coincidono con gli elementi del gruppo: in questo caso i caratteri delle rappresentazioni irriducibili sono una base ortonormale di $\mathbb{C}[G]$ e le rappresentazioni irriducibili sono di dimensione 1; in definitiva coincidono con i loro caratteri, e questi sono in corrispondenza biunivoca con gli elementi del gruppo.*

5.4.9 Corollario *Una rappresentazione qualsiasi è determinata dal suo carattere*

DIMOSTRAZIONE: Se V è irriducibile questo è l'ortogonalità; altrimenti V sarà somma diretta di rappresentazioni irriducibili

$$V = \oplus_{i=1}^{k} V_i^{\oplus m_i}$$

ove V_i è irriducibile e m_i è la molteplicità con la quale figura nella decomposizione di V; ma allora

$$\chi_V = \sum_{i=1}^{k} m_i \chi_{V_i}$$

e le χ_{V_i} sono linearmente indipendenti.

QED

Si noti in particolare, che se $V_i = V_j$ allora $1 = (\chi_{V_i}, \chi_{V_j})_F = \sum_i m_i^2$ e quindi

5.4.10 Corollario *V è irriducibile se e solo se $(\chi_V, \chi_V)_F = 1$.*

Evidentemente

$$m_i = (\chi_V, \chi_{V_i})_F$$

Dimostriamo ora un teorema fondamentale:

5.4.11 Teorema *Se $V_1, ..., V_n$ sono tutte le rappresentazioni irriducibili di G (a meno di equivalenza) allora i coefficienti a_{ij}^k delle matrici $\pi_k(g)$ sono una base ortogonale dello spazio $\mathbb{C}[G]$.*

DIMOSTRAZIONE: L'ortogonalità degli elementi segue dall'ortonormalità dei caratteri delle rappresentazioni V_i: dato che il carattere è la traccia, se $\dim V_i = n_i$ allora

$$(a_{ij}^k, a_{rs}^h) = \begin{cases} 0 & \text{se } k \neq h \text{ o } i \neq r \text{ o } j \neq s \\ \frac{1}{n_k} & \text{se } k = n, i = r, j = s \end{cases}$$

Dimostriamo ora che le funzioni $a^k_{ij} : G \longrightarrow \mathbb{C}$ sono una base di $\mathbb{C}[G]$; consideriamo la rappresentazione regolare sinistra: sappiamo che è completamente riducibile, dato che è unitaria (per definizione del prodotto hermitiano $(.)_F$) e quindi

$$\mathbb{C}[G] = X_1 \oplus ... \oplus X_p$$

ove X_j sono sottorappresentazioni tali che la restrizione L_j della rappresentazione regolare ad esse è irriducibile: quindi, poiché le V_i esauriscono le rappresentazioni irriducibili di G, L_j è equivalente ad una certa V_{i_j}: allora esiste una base $(e^j_1, ..., e^j_{n_{i_j}})$ di X_j nella quale la matrice che rappresenta L_j ha come coefficienti $a^{i_j}_{rs}$, quindi

$$e^j_s(gh) = L(g)e^j_s(h) = L_j(g)e^j_s(h) = \sum_r a^{i_j}_{rs}(h)e_r(g)$$

Per $g = e$ e $c_{sj} = e^j_s(e)$ si ha

$$e^j_s(h) = \sum_r c_{sj}a^{i_j}_{rs}(h)$$

Dunque ciascuna funzione e^j_s appartiene ad una base di X_j (e quindi ciascuna funzione su X_j) è combinazione lineare delle $a^{i_j}_{rs}$. Dato che $\mathbb{C}[G]$ è somma diretta degli X_j si ottiene la tesi.

QED

Definiamo ora sullo spazio vettoriale $\mathbb{C}[G]$ una operazione, la *convoluzione di funzioni*:

$$F * G(g) = \frac{1}{\operatorname{Card} G} \sum_{h \in G} F(h)G(gh^{-1})$$

5.4.12 Teorema *L'operazione $*$ è associativa, possiede un elemento neutro ed è commutativa se e solo se lo è il prodotto del gruppo.*

DIMOSTRAZIONE: Basta osservare che una base dello spazio vettoriale $\mathbb{C}[G]$ sono gli elementi del gruppo G, e che la convoluzione su essi coincide con il prodotto del gruppo. L'elemento neutro è lo stesso del gruppo.

QED

Dato che $\mathbb{C}[G]$ è lo spazio della rappresentazione regolare, si decompone in sottorappresentazioni irriducibili di G: questa decomposizione rispetta la struttura algebrica di $\mathbb{C}[G]$. Per formulare correttamente questi risultati, dobbiamo introdurre alcuni concetti algebrici generali.

5.5 Algebre associative

Gli esempi fondamentali di gruppi che abbiamo considerato erano il gruppo delle trasformazioni biunivoche di uno spazio in sé, in particolare i gruppi simmetrici S_n, ed il gruppo degli isomorfismi lineari di uno spazio vettoriale $GL(V)$.

In generale ha interesse considerare trasformazioni che non siano necessariamente biunivoche: ad esempio, nel caso degli spazi vettoriali, ha interesse considerare lo spazio $End(V)$ di tutte le funzioni lineari di V in sé che, nel caso di dimensione finita, corrisponde allo spazio di tutte le matrici $M_n(\mathbb{C})$. Questo non è semplicemente uno spazio vettoriale, ma i suoi elementi possono essere moltiplicati fra loro, componendo le mappe lineari o (equivalentemente) moltiplicando le matrici righe per colonne.

Motivati da questi esempi diamo la

5.5.1 Definizione *Uno spazio vettoriale $\mathcal{A}$ su un campo $\mathbb{K}$ (che per noi sarà sempre $\mathbb{C}$ o al più $\mathbb{R}$) si dice un'*algebra *se è data una funzione*

$$\mu : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$$

bilineare (il prodotto *dell'algebra). Si scrive ab in luogo di $\mu(a, b)$.*

Questo concetto è estremamente generale: notiamo che, per bilinearità del prodotto μ, possiamo scrivere

$$\mu : A \otimes A \longrightarrow A$$

5.5.2 Esempio

(1) *I numeri complessi, le matrici complesse e gli endomorfismi di uno spazio vettoriale sono esempi di algebre complesse.*

(2) *Se X è un insieme, lo spazio vettoriale $F(X)$ delle funzioni $X \longrightarrow \mathbb{C}$ possiede un prodotto, definito come segue: se $f, g \in F(X)$ allora*

$$fg(x) = f(x)g(x)$$

(prodotto di numeri complessi).

(3) *$\mathcal{A} = M_n(\mathbb{C})$ non è un'algebra solo per il prodotto AB di matrici; ponendo*

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

otteniamo un nuovo prodotto [.] *su* $\mathcal{A}$*, che si dice* prodotto di Lie*. Una ulteriore struttura di algebra sulle matrici è data dal* prodotto di Jordan*:*

$$(A, B) = AB + BA$$

(4) *Lo spazio dei polinomi complessi* $\mathbb{C}[x_1, ..., x_n]$ *è un'algebra rispetto al prodotto:*

$$PQ(x_1, ..., x_n) := P(x_1, ..., x_n)Q(x_1, ..., x_n)$$

come si verifica immediatamente.

(5) *Più in generale, lo spazio delle funzioni continue su uno spazio topologico è un'algebra rispetto alla stessa moltiplicazione (punto per punto).*

Notiamo che in questi esempi, i prodotti godono di proprietà differenti: ad esempio il prodotto di funzioni è commutativo: $fg = gf$, mentre il prodotto di matrici non lo è; il prodotto di matrici verifica tuttavia l'*identità associativa*

$$A(BC) = (AB)C$$

mentre il prodotto di Lie di matrici non lo è, ma verifica invece la

$$[A, [B, C]] + [C, [A, B]] + [B, [C, A]] = 0$$

(*identità di Jacobi*) e la *anticommutatività*:

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

Il prodotto di Jordan verifica invece l'*identità di Jordan*:

$$((A, B), (A, A)) = (A, (B, (A, A)))$$

5.5.3 Esempio *Si consideri* $\mathcal{A} = C^\infty(\mathbb{R}^{2n})$ *(algebra delle funzioni differenziabili) e si definisca il prodotto*

$$\{f, g\}(x_1, ..., x_{2n}) = \sum_{i=1}^{n} \left(\frac{\partial f}{\partial x_i} \frac{\partial g}{\partial x_{i+n}} - \frac{\partial g}{\partial x_i} \frac{\partial f}{\partial x_{i+n}} \right)$$

(parentesi di Poisson). Il classico teorema di Jacobi afferma che queste parentesi verificano l'identità di Jacobi.

5.5.4 Definizione *Un'algebra* $\mathcal{A}$ *si dice*

(1) associativa *se il prodotto verifica la proprietà associativa;*

(2) commutativa *se il prodotto verifica la proprietà commutativa;*

(3) di Lie *se il prodotto verifica le proprietà anticommutativa e di Jacobi;*

(4) di Jordan *se il prodotto verifica le proprietà commutativa e di Jordan.*

Questi assiomi sono indipendenti fra loro, ma si possono utilmente combinare: ad esempio l'algebra dei polinomi è associativa e commutativa.

5.5.5 Definizione *Un'algebra (associativa) si dice* con identità *o* con unità *se possiede un* elemento neutro $e \in \mathcal{A}$ *tale che*

$$\forall a \in \mathcal{A} \quad ea = ae = a$$

Ad esempio le algebre delle matrici e dei polinomi posseggono gli elementi neutri I e 1. Un'algebra anticommutativa (e.g. un'algebra di Lie) non può possedere un elemento neutro e, dato che $a = ae = ea = -ae$ implica $a = ae = 0$.

Se un'algebra associativa non possiede elemento neutro è sempre possibile aggiungerglielo, considerando $\widetilde{\mathcal{A}} = \mathcal{A} \oplus \mathbb{K}$ col prodotto

$$(a, k)(a', k') = (aa' + ka' + k'a, kk')$$

Si vede facilmente che $(0, 1)$ è un elemento neutro per $\widetilde{\mathcal{A}}$ e che $\mathcal{A}$ è la sottoalgebra di $\widetilde{\mathcal{A}}$ degli elementi $(a, 0)$.

Convenzione. *Supporremo nel seguito che le nostre algebre, se non altrimenti specificato, siano algebre associative con elemento neutro e di dimensione finita.*

5.5.6 Esempio *Lo spazio $\mathbb{C}[G]$ della rappresentazione regolare di un gruppo finito è un'algebra rispetto al prodotto di convoluzione; sappiamo che si tratta di un'algebra associativa con elemento neutro, commutativa se e solo se lo è il gruppo.*

5.5.7 Definizione *Un elemento a di un'algebra con unità $\mathcal{A}$ si dice* invertibile *se esiste un $b \in \mathcal{A}$ tale che $ab = ba = e$. Si scrive $b = a^{-1}$.*

Ovviamente in un'algebra (associativa, con unità) l'insieme $\mathcal{A}^{-1}$ degli elementi invertibili forma un gruppo rispetto al prodotto dell'algebra: ad esempio se $\mathcal{A} = End(V)$ allora $\mathcal{A}^{-1} = GL(V)$.

5.5.8 Definizione *Se in un'algebra $\mathcal{A}$ ogni elemento è invertibile, $\mathcal{A}$ si dice un* corpo.

Ad esempio $\mathbb{C}$ è un corpo commutativo, cioè un campo (notiamo che si tratta di una $\mathbb{R}$-algebra oltre che di una $\mathbb{C}$-algebra).

5.5.9 Esempio *Consideriamo il* corpo dei quaternioni*: partiamo dallo spazio vettoriale reale* $\mathcal{H} = \mathbb{R}^4$ *con la base* $(1, i, j, k)$*:*

$$1 = (1,0,0,0) \quad i = (0,1,0,0) \quad j = (0,0,1,0) \quad k = (0,0,0,1)$$

Per definire un prodotto basta definirlo sui generatori ed estenderlo per bilinearità: sia

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

e 1 *l'elemento neutro. Un elemento* $a1 + bi + cj + dk \in \mathcal{H}$ $(a, b, c, d \in \mathbb{R})$ *si dice* quaternione *e può essere rappresentato con una matrice (come spazi vettoriali* $\mathbb{R}^4 \cong M_2(\mathbb{C})$*)*

$$(Q) \qquad \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$$

ove $a, b \in \mathbb{C}$*; allora il prodotto di quaternioni è il prodotto di queste matrici. Non ogni matrice* 2×2 *(ovviamente) è un quaternione, ed infatti la sottoalgebra di* $M_2(\mathbb{C})$ *dei quaternioni è un corpo: infatti ogni matrice della forma (Q) ammette come inversa la*

$$\frac{1}{|a|^2 + |b|^2} \begin{pmatrix} \overline{a} & -b \\ \overline{b} & \overline{a} \end{pmatrix}$$

(ove $|a|^2 = a\overline{a}$ *è il modulo del numero complesso* a*).*

Dato che il prodotto in un'algebra qualsiasi $\mathcal{A}$ è bilineare, resta completamente determinato una volta che lo si sia definito su una base dello spazio vettoriale $\mathcal{A}$. Ad esempio, se $\dim \mathcal{A} < \infty$ e se $(e_1, ..., e_n)$ ne è una base, i coefficienti del sistema di equazioni

$$e_i e_j = \sum_k c_{ij}^k e_k$$

si dicono *costanti di struttura* dell'algebra e la determinano completamente.

In analogia con i gruppi, avremo i concetti di *sottoalgebra*, *morfismo* e *quoziente* di algebre. Una sottoalgebra $\mathcal{B} \subset \mathcal{A}$ è un sottospazio vettoriale tale che $\mathcal{B}\mathcal{B} \subset \mathcal{B}$ (se $S, T \subset \mathcal{A}$ sono sottoinsiemi di un'algebra scriviamo ST per l'insieme $\{st \,|\, s \in S, t \in T\}$), un morfismo fra algebre è una mappa lineare

$$f : \mathcal{A} \longrightarrow \mathcal{B}$$

tale che

$$f(ab) = f(a)f(b)$$

Sia il nucleo

$$\ker f = \{a \in \mathcal{A} \,|\, f(a) = 0\}$$

che l'immagine $\operatorname{im} f$ di un morfismo sono sottoalgebre di $\mathcal{A}$ e $\mathcal{B}$ rispettivamente. Inoltre il nucleo è un ideale nel senso della

5.5.10 Definizione *Una sottoalgebra $\mathcal{B}$ di un'algebra $\mathcal{A}$ è un* ideale destro *se $\mathcal{BA} \subset \mathcal{B}$ e un* ideale sinistro *se $\mathcal{AB} \subset \mathcal{B}$; se è un ideale sia destro che sinistro si dice* bilatero.

Dato che $\mathcal{B}$ è un ideale sinistro se per ogni $a \in \mathcal{A}$ e $b \in \mathcal{B}$: $ba \in \mathcal{B}$. Quindi se $\mathcal{B}$ è un ideale di $\mathcal{A}$ sullo spazio vettoriale quoziente $\mathcal{A}/\mathcal{B}$ il prodotto di $\mathcal{A}$ induce un prodotto e quindi una struttura di algebra.

È inoltre ovvio che il quoziente è un'algebra associativa.

5.5.11 Teorema *Un'algebra commutativa è un campo se e solo se è priva di ideali non banali.*

DIMOSTRAZIONE: Osserviamo che un ideale $\mathcal{I}$ non può contenere e altrimenti per ogni $a \in \mathcal{A}$ $ea \in \mathcal{I}$ i.e. $\mathcal{I} = \mathcal{A}$. Per lo stesso motivo non può contenere un elemento invertibile, dato che in questo caso $a^{-1}a \in \mathcal{I}$ i.e. $e \in \mathcal{I}$.

Ora, se $\mathcal{A}$ è un corpo, ogni elemento non nullo è invertibile e quindi un ideale non può contenere elementi non nulli, i.e. non può che essere 0. Viceversa, se $\mathcal{I}$ è un ideale non banale, un suo elemento non nullo non può essere invertibile, quindi $\mathcal{A}$ non è un corpo.

QED

A differenza del caso dei gruppi, in un'algebra associativa commutativa non è vero che le sottoalgebre sono ideali; ad esempio, in ogni algebra esiste il *centro*:

$$\mathcal{Z}(\mathcal{A}) = \{z \in \mathcal{A} \,|\, \forall a \in \mathcal{A} az = za\}$$

In generale non si tratta di un ideale: se $z \in \mathcal{Z}(\mathcal{A})$ e $a, b \in \mathcal{A}$ allora $a(bz) = azb \neq bza$. Se l'algebra è commutativa allora $\mathcal{A} = \mathcal{Z}(\mathcal{A})$.

All'opposto abbiamo il concetto di algebra semplice, motivato anche dal teorema precedente, che è falso nel caso non commutativo: mostreremo fra breve, ad esempio, che l'algebra delle matrici non possiede ideali non banali (ma ovviamente non è un campo).

5.5.12 Definizione *Un'algebra $\mathcal{A}$ si dice* semplice *se non possiede ideali bilateri non banali.*

Le algebre semplici, come suggerisce il nome, sono "prive di struttura interna" e sono usate per produrre nuove algebre per mezzo della somma diretta, ad esempio.

Se $\{\mathcal{A}_\alpha\}$ è una famiglia di algebre (sullo stesso campo e dello stesso tipo) sul prodotto diretto di spazi vettoriali $\bigoplus_\alpha \mathcal{A}_\alpha$ v'è un ovvia struttura di algebra:

$$ab(\alpha) = a(\beta)b(\beta)$$

(si rammenti che il prodotto è l'insieme delle applicazioni dall'insieme degli indici alla totalità degli addendi diretti). Ad esempio, su $\mathcal{A} \oplus \mathcal{B}$ abbiamo

$$(a \oplus b)(a' \oplus b') = (aa') \oplus (bb')$$

Ogni addendo diretto è un ideale del prodotto.

5.5.13 Definizione *Un'algebra si dice* semisemplice *se è somma diretta di algebre semplici.*

Diamo ora qualche esempio.

5.5.14 Teorema *L'algebra associativa delle matrici $M_n(\mathbb{K})$ è semplice.*

DIMOSTRAZIONE: Sia J in ideale in $M_n(\mathbb{K})$ non nullo e sia $A \in J$ una matrice non nulla, che possiamo esprimere in termini di matrici "elementari" E_{ij} (ove E_{ij} è la matrice $((\delta_{ij}))$ che ha zero in ogni entrata, tranne che nell'elemento della riga i e della colonna j ove ha 1):

$$A = \sum_{i,j} a_{ij} E_{ij}$$

Se h, k sono tali che $a_{hk} \neq 0$ ($A \neq 0$) allora

$$\forall r, s \in \{1, ..., n\} \quad E_{rs} = a_{hk}^{-1} E_{rh} A E_{ks} \in J$$

e quindi ogni matrice $E_{rs} \in J$ cioè $J = M_n(\mathbb{K})$.

QED

Si noti che la dimostrazione funziona per l'algebra delle matrici a coefficienti in un corpo $\mathbb{K}$ qualsiasi. Notiamo inoltre che $M_n(\mathbb{K})$ possiede centro non banale:

$$\mathcal{Z}(M_n(\mathbb{K})) = \{kI \mid k \in \mathbb{K}\}$$

(di dimensione 1) formato dai multipli costanti della matrice I.

Dal teorema segue che le somme dirette di algebre di matrici sono semisemplici.

5.5.15 Esempio *Consideriamo le matrici triangolari superiori:*

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ 0 & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & ... & a_{nn} \end{pmatrix}$$

Quest'algebra non è semisemplice, dato che possiede molti ideali: ad esempio quello delle matrici triangolari i cui elementi diagonali siano tutti nulli (il quoziente è l'algebra delle matrici diagonali).

Il fatto che i nostri esempi siano tutti basati sulle matrici non è un caso:

5.5.16 Teorema *Ogni algebra associativa di dimensione n su un campo $\mathbb{K}$ è isomorfa ad una sottoalgebra di $M_k(\mathbb{K})$ con $k \leq n+1$.*

DIMOSTRAZIONE: Sia $\mathcal{A}$ un'algebra associativa con unità 1 e consideriamo la rappresentazione regolare sinistra

$$L : \mathcal{A} \longrightarrow End(\mathcal{A}) = M_n(\mathbb{K})$$

definita da $L(a)(b) = ab$; si tratta evidentemente di un omomorfismo di $\mathcal{A}$ nell'algebra associativa $End(\mathcal{A})$: dimostriamo che è iniettivo, il che ci fornisce la tesi. Se $L(a)(b) = 0$ per ogni $b \in \mathcal{A}$ allora $ab = 0$ per ogno b e quindi per $b = 1$, da cui $a = 0$; cioè il nucleo di L è banale.

Se $\mathcal{A}$ non possiede l'unità, possiamo considerare lo spazio vettoriale $\widetilde{\mathcal{A}} = \mathcal{A} \oplus \mathbb{K}$, e definire su di esso un prodotto

$$(a + k, b + h) = (ab + kb + ha, kh)$$

associativo; evidentemente l'algebra $\widetilde{\mathcal{A}}$ possiede un elemento neutro: $(0, 1)$. Ma allora $\widetilde{\mathcal{A}}$ (e quindi anche $\mathcal{A}$, per restrizione) si immerge in $M_k(\mathbb{K})$.

QED

Questo teorema è analogo al teorema di Cayley per i gruppi: l'idea è la stessa e ci dà lo spunto per parlare di rappresentazioni di algebre; prima facciamo un'ulteriore convenzione:

Convenzione. *D'ora in avanti un'algebra sarà un'algebra associativa con elemento neutro di dimensione finita sui numeri complessi:* $\mathbb{K} = \mathbb{C}$.

5.5.17 Definizione *Una funzione $a \longmapsto A^*$ in un'algebra A si dice una* involuzione *se*

(1) $a^{**} = a$

(2) $(\lambda a)^* = \overline{\lambda} a^*$ *se* $\lambda \in \mathbb{C}$.

(3) $(a + b)^* = a^* + b^*$

(4) $(ab)^* = b^* a^*$

5.5.18 Definizione *Un'algebra dotata di involuzione $*$ si dice una* *-algebra.

L'esempio ispiratore è l'algebra delle matrici complesse: l'involuzione è semplicemente la coniugazione della trasposta:

$$A^* = \overline{A^T}$$

Si noti che, sebbene ogni algebra sia una sottoalgebra delle matrici, non è detto che sia una sotto-*-algebra. Anche le matrici reali rispetto alla semplice trasposizione sono una *-algebra.

5.5.19 Definizione *Un elemento $a \in A$ si dice* autoaggiunto *se $a^* = a$ e si dice* normale *se $a^*a = aa^*$.*

Ovviamente ogni elemento $a \in \mathcal{A}$ si scrive in modo unico come

$$a = a_1 + ia_2$$

ove a_1, a_2 sono autoaggiunti: basta porre

$$a_1 = \frac{1}{2}(a + a^*) \qquad \text{e} \qquad a_2 = \frac{1}{2i}(a - a^*)$$

Inoltre per ogni a, a^*a e aa^* sono autoaggiunti, come pure autoaggiunto è e.

Ora vogliamo dare per una *-algebra il concetto di rappresentazione: ovviamente un omomorfismo di *-algebre è un omomorfismo φ tale che

$$\varphi(a^*) = \varphi(a)^*$$

e si dice anche **-omomorfismo*.

5.5.20 Definizione *Un* modulo *su una *-algebra $\mathcal{A}$ è uno *-omomorfismo di *-algebre*

$$\varphi : \mathcal{A} \longrightarrow End(M)$$

ove M è uno spazio vettoriale complesso.

In altri termini, se scriviamo

$$am := \varphi(a)(m)$$

allora

(1) $(\lambda a + \mu b)m = \lambda(am) + \mu(bm)$ se $\lambda, \mu \in \mathbb{C}$, $a, b \in \mathcal{A}$ e $m \in M$;

(2) $(ab)m = a(bm)$

(3) $1m = m$

Il concetto è del tutto analogo a quello di rappresentazione, ed infatti, come nel caso delle rappresentazioni abbiamo i concetti di

(1) *sottomodulo*, cioè di $\mathcal{A}$-modulo N che sia un sottospazio di M;

(2) *modulo irriducibile*, cioè di $\mathcal{A}$-modulo M che non possiede sottomoduli diversi da 0 e M;

(3) *morfismo di moduli*, cioè di applicazione lineare $A : M \longrightarrow N$ fra due sottomoduli tale che $A(am) = a(Am)$ per ogni $a \in \mathcal{A}$ e $m \in M$; l'insieme dei morfismi si denota con $\hom_{\mathcal{A}}(M, N)$;

(4) *somma diretta di moduli*, del tutto ovvia;

(5) *completa riducibilità di moduli*, cioè un modulo è completamente riducibile se è somma diretta di sottomoduli irriducibili.

Esattamente come nel caso delle rappresentazioni dei gruppi abbiamo il

5.5.21 Lemma (SCHUR) *Se M e N sono $\mathcal{A}$-moduli irriducibile allora ogni morfismo di moduli $F : M \longrightarrow N$ è un isomorfismo oppure è zero.*

5.5.22 Corollario *Se M è un $\mathcal{A}$-modulo irriducibile allora* $\hom_{\mathcal{A}}(M, M) = \mathbb{C}$.

Osserviamo che se lo spazio M possiede una struttura hermitiana $(.)$, si dice uno **-modulo* se

$$(am, m') = (m, a^* m')$$

ovvero $a^* m = (am)^*$. Esattamente come per le rappresentazioni unitarie, si dimostra il seguente

5.5.23 Teorema *Uno *-modulo su una *-algebra $\mathcal{A}$ è completamente riducibile.*

Ad esempio l'algebra di gruppo di un gruppo finito è completamente riducibile, dato che

5.5.24 Teorema *Se G è un gruppo, esiste una corrispondenza biunivoca fra $\mathbb{C}[G]$-moduli e rappresentazioni di G: ai moduli irriducibili corrispondono rappresentazioni irriducibili.*

DIMOSTRAZIONE: Se $\pi : G \longrightarrow GL(V)$ è una rappresentazione di G possiamo estenderla per linearità ad una funzione

$$\varphi(\sum_g a_g g) = \sum_g a_g \varphi(g)$$

su $\mathbb{C}[G]$ ottenendo così una funzione $\mathbb{C} \longrightarrow End(V)$

$$(\sum_g a_a g)(v) := \sum_g a_g \varphi(g)(v)$$

che si verifica facilmente essere una struttura di $\mathbb{C}[G]$-modulo su V.

Per ricostruire la rappresentazione del gruppo a partire dall'algebra basta restringere la rappresentazione di $\mathbb{C}[G]$ a $G \subset \mathbb{C}[G]$.

QED

Dimostriamo ora che l'algebra di gruppo è semisemplice: in effetti vale molto di più: ogni rappresentazione di un'algebra semisemplice è completamente riducibile (teorema di Wedderburn) ed è somma diretta di algebre di matrici, che ne costituiscono i "fattori"; ogni tale fattore $\mathcal{F}$ verifica la relazione $\mathcal{F} \cap \mathcal{F}' = \mathbb{C}$ ove $\mathcal{F}' = \{A \in \mathcal{A} \,|\, \forall F \in \mathcal{F}\ AF = FA\}$ è il *commutante* del fattore $\mathcal{F}$. La teoria ammette una vastissima generalizzazione al caso di dimensione infinita, generalizzazione dovuta a von Neumann e Murray.

5.5.25 Teorema *Se G è un gruppo finito, l'algebra $\mathbb{C}[G]$ è somma diretta delle algebre*

$$M_{n_1}(\mathbb{C}) \oplus ... \oplus M_{n_k}(\mathbb{C})$$

ove n_i sono le dimensioni delle rappresentazioni irriducibili di G e k è il loro numero.

Dimostrazione: Siano $\pi_1 : G \longrightarrow GL(V_1), ..., \pi_k : G \longrightarrow GL(V_k)$ le rappresentazioni irriducibili non equivalenti di G e supponiamo che sia $\dim V_i = n_i$; allora, se poniamo

$$\begin{aligned} \Phi : \mathbb{C}[G] &\longrightarrow M_{n_1}(\mathbb{C}) \oplus ... \oplus M_{n_k}(\mathbb{C}) \\ g &\longmapsto (\pi_1(g), ..., \pi_k(g)) \end{aligned}$$

(definendola su G, che è una base di $\mathbb{C}[G]$ ed estendendola per linearità) abbiamo un omomorfismo di algebre: si tratta di uno *-omomorfismo, dato che le rappresentazioni V_i sono unitarie.

Per vedere che è un isomorfismo ci basta dunque mostrare che è iniettivo e suriettivo. è iniettivo perché se $\ker \Phi \neq 0$ allora

$$\pi_i(a) = 0$$

e quindi tutti i coefficienti delle matrici $\pi_i(g)$ sono nulli; ma questi sono una base dello spazio $\mathbb{C}[G]$ e quindi $a = 0$.

Dimostriamo infine che è suriettivo: abbiamo che, se $a = \sum_g a(g)g$:

$$\pi_i(a) = \sum_{g \in G} a(g)\pi_i(g)$$

Se quindi $A_1 \oplus ... \oplus A_k$ è un generico elemento di $\bigoplus M_{n_i}(\mathbb{C})$ allora vogliamo mostrare che esiste $a \in \mathbb{C}[G]$ tale che $\Phi(a) = A_1 \oplus ... \oplus A_k$.

Sia perciò $A_1 \oplus ... \oplus A_k$ un elemento di $\bigoplus M_{n_i}(\mathbb{C})$; le matrici A_i sono matrici delle rappresentazioni $\pi_i(g)$ rispetto a certe basi di V_i; sappiamo che questi elementi generano come spazio vettoriale $\mathbb{C}[G]$, dato che ne costituiscono una base

ortogonale, quindi ogni elemento a di $\mathbb{C}[G]$ è, in una certa base, combinazione lineare di queste funzioni, da cui

$$\Phi(a) = \Phi\left(\sum_{g\in G} a(g)g\right) = \sum_{g\in G} a(g)(\pi_1(g) \oplus ... \oplus \pi_k(g)) = \sum_{g\in G} a(g)A_1 \oplus ... \oplus A_k$$

QED

5.6 Appendice: Cenni di algebra tensoriale

In questa appendice supporremo di avere a che fare con spazi vettoriali di dimensione finita su un campo $\mathbb{K}$, che potremo limitarci a pensare come i numeri reali $\mathbb{R}$ o complessi $\mathbb{C}$.

5.6.1 Algebra tensoriale

Consideriamo quindi due spazi vettoriali V e W. Vogliamo costruire a partire da questi due un nuovo spazio vettoriale di dimensione finita che abba il diritto di dirsi "prodotto" dei due dati. L'idea è che i suoi elementi, che saranno formati a partire dagli elementi di V e W non dovranno soddisfare altre relazioni se non quelle di bilinearità.

Ricordiamo che una mappa bilineare fra gli spazi vettoriali V, W e Z è una applicazione

$$f : V \times W \longrightarrow Z$$

tale che, fissato un qualsiasi $v \in V$ la mappa $w \longmapsto f(v, w)$ sia lineare da W a Z e, fissato un qualsiasi $w \in W$ la mappa $v \longmapsto f(v, w)$ sia lineare da V a Z.

Quando $Z = \mathbb{K}$, f si dice *forma bilineare*. Ad esempio un prodotto scalare su uno spazio vettoriale reale è una forma bilineare.

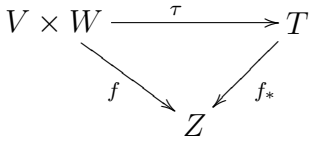
Il problema che ora ci poniamo è di trovare uno spazio vettoriale "universale" rispetto al concetto di bilinearità, e la risposta è fornita dal seguente

5.6.1 Teorema *Se V e W sono spazi vettoriali su $\mathbb{K}$ allora esiste uno spazio vettoriale T su $\mathbb{K}$ ed una mappa bilineare*

$$\tau : V \times W \longrightarrow T$$

tale che

(1) *Per ogni mappa bilineare* $f : V \times W \longrightarrow Z$ *esiste un'unica mappa lineare* $f_* : T \longrightarrow Z$ *tale che* $f = f_* \circ \tau$*, i.e. che il seguente diagramma*



(2) *Se* $(v_1, ..., v_n)$ *è una base di* V *e* $(w_1, ..., w_m)$ *è una base di* W *allora* $\{\tau(v_i, w_j)\}_{i,j}$ *è una base di* T*.*

Dimostrazione: Questa dimostrazione non è la più raffinata ma ha il pregio della concretezza: consideriamo la base $(v_1, ..., v_n)$ di V e la base $(w_1, ..., w_m)$ di W, ed associamo ad ogni coppia (v_i, w_j) un simbolo τ_{ij}. Allora lo spazio vettoriale T generato su $\mathbb{K}$ dai simboli τ_{ij} ha dimensione nm, ed è formato da tutti le combinazioni lineari formali

$$\sum_{i,j} a_{ij}\tau_{ij}$$

con $a_{ij} \in \mathbb{K}$. In altri termini le $\{\tau_{ij}\}$ sono per definizione una base di T.

Definiamo ora la mappa τ su una coppia qualsiasi di vettori di V e W, espressi in termini delle loro basi come $v = \sum_i x_i v_i$ e $w = \sum_j y_j w_j$, nel modo seguente:

$$\tau(v, w) := \sum_{i,j} x_i y_j \tau_{ij}$$

Per definizione questa mappa è bilineare. Verifichiamo ora i due enunciati del teorema.

Sia dunque f la nostra mappa bilineare. Se definiamo

$$f_*(\tau_{ij}) := f(v_i, w_j)$$

questo determina un'unica mappa lineare su T (infatti l'abbiamo definita sulla sua base $\{\tau_{ij}\}$) e per definizione si ha $f = f_* \circ \tau$.

Per dimostrare il secondo enunciato, basta considerare due altre basi di V e W: $(v'_1, ..., v'_n)$ e $(w'_1, ..., w'_n)$. Dobbiamo dimostrare che gli elementi $\{\tau(v'_i, w'_j)\}$ costituiscono una base di T. Ma di certo questi elementi generano T, in quanto, per ogni coppia $(v, w) \in V \times W$ esistono dei coefficienti in $\mathbb{K}$ tali che

$$v = \sum x_i v'_i \qquad \text{e} \qquad w = \sum y_i w'_i$$

Sicché, per bilinearità di τ:

$$\tau(v, w) = \sum_{i,j} x_i y_j \tau(v'_i, w'_j)$$

e quindi ogni elemento di T si esprime come combinazione lineare degli $\{\tau(v'_i, w'_j)\}$. Inoltre, dato che questi elementi sono nm e che la dimensione di T pure è nm, devono necessariamente costituirne una base.

QED

Osserviamo che la definizione di T è ben posta in virtù del secondo enunciato del teorema, non dipende cioè dalla scelta delle basi fissate in V e W per costruire i generatori di T.

Un altro corollario immediato del teorema è che lo spazio T è unico a meno di isomorfismi: infatti se ne esiste un altro, diciamo T', soddisfacente alla proprietà (1) del teorema, possiamo applicare il teorema a T' con $Z = T$ e $f = \tau$ ed a T con $Z = T'$ e $f = \tau'$, ottenendo così due mappe τ_* e τ'_* che sono ovviamente l'una l'inversa dell'altra e dunque realizzano un isomorfismo di T con T'.

D'ora in poi indicheremo lo spazio T associato a V e W con $V \otimes W$, e lo chiameremo *prodotto tensoriale* di V e W. Inoltre al posto di $\tau(v, w)$ scriveremo $v \otimes w$ e chiameremo gli elementi di $V \otimes W$ *tensori*.

Per costruzione si ha

$$\dim V \otimes W = \dim(V) \dim(W)$$

è ovvia la verifica dell'esistenza dei seguenti isomorfismi canonici (tutto ciò che bisogna usare è il teorema 1):

$$V \otimes W \cong W \otimes V$$
$$V \otimes (W \otimes Z) \cong (V \otimes W) \otimes Z)$$

5.6.2 Proposizione $V^* \otimes W \cong \hom(V, W)$.

DIMOSTRAZIONE: Definiamo esplicitamente:

$$F : V^* \otimes W \longrightarrow \hom(V, W)$$
$$\varphi \otimes w \longmapsto (v \longmapsto \varphi(v)w)$$

Cioè, al tensore $\varphi \otimes w$ (ove $\varphi \in V^*$ e $w \in W$) assegnamo la mappa lineare $F_{\varphi \otimes w} : V \longrightarrow W$ che calcolata su un elemento v dà come risultato $\varphi(v)w$. è un'ovvia verifica che F è ben definita, lineare e iniettiva, dunque un isomorfismo.

QED

Il seguente fatto è banale, ma molto importante, ed esprime la funtorialità del prodotto tensoriale: se $f : V \longrightarrow U$ e $g : W \longrightarrow Z$ sono mappe lineari di spazi vettoriali allora è definita la mappa lineare

$$f \otimes g : V \otimes W \longrightarrow U \otimes Z$$

come

$$(f \otimes g)(v \otimes w) := f(v) \otimes g(w)$$

In altri termini, tensorizzare per uno spazio vettoriale fissato è un funtore nella categoria degli spazi vettoriali: il prodotto tensoriale lo possiamo vedere come un "funtore in due variabili".

5.6.3 Proposizione

(1) $V \otimes \mathbb{K} \cong V$

(2) $V^* \otimes W^* \cong (V \otimes W)^*$

(3) *Se V è uno spazio vettoriale reale, possiamo considerare $V^{\mathbb{C}} := V \otimes \mathbb{C}$ ove $\mathbb{C}$ è visto come spazio reale bidimensionale. Allora $V^{\mathbb{C}}$ è uno spazio vettoriale complesso.*

Dimostrazione: V soddisfa evidentemente la proprietà universale del prodotto tensoriale $V \otimes \mathbb{K}$ rispetto alla mappa $F : V \times \mathbb{K} \longrightarrow V$ data da $F(v, k) = kv$.

La (2) è pure ovvia: se $F : V^* \times W^* \longrightarrow (V \otimes W)^*$ è data da

$$F(\varphi, \psi)(v \otimes w) := \varphi(v)\psi(w)$$

allora la proprietà universale di $V^* \otimes W^*$ è verificata da $(V \otimes W)^*$.

Infine, se $V^{\mathbb{C}} = V \otimes \mathbb{C}$, vediamo che è definita una moltiplicazione fra gli elementi di $V^{\mathbb{C}}$ e quelli di $\mathbb{C}$ che rende $V^{\mathbb{C}}$ uno spazio complesso: basti porre

$$\forall v \in V^{\mathbb{C}} \ \forall z \in \mathbb{C} \quad zv = v \otimes z$$

Le proprietà del prodotto tensoriale dicono esattamente che lo spazio $V^{\mathbb{C}}$ è complesso. Si noti che $\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V^{\mathbb{C}}$: in effetti una $\mathbb{R}$-base $(e_1, ..., e_n)$ di V è anche una $\mathbb{C}$-base di $V^{\mathbb{C}}$.

QED

Per concludere questa discussione del prodotto tensoriale notiamo il motivo per quale lo si può considerare una versione intrinseca del concetto di multilinearità: ha luogo infatti l'isomorfismo

$$(V \otimes W)^* \cong Bil(V, W)$$

ove $Bil(v, W)$ denota lo spazio delle forme bilineari su $V \times W$. Questo isomorfismo è semplicemente un modo differente di esprimere la proprietà (1) del Teorema 1.

In modo del tutto analogo, considerando per uno spazio vettoriale V le sue potenze tensoriali $V^{\otimes 2} := V \otimes V$, $V^{\otimes 3} := V \otimes V \otimes V$,... possiamo identificare le forme multilineari sullo spazio vettoriale V con le forme lineari sui tensori di V.

Introduciamo ora un oggetto molto importante, l'*algebra tensoriale*. Partiamo dal solito spazio vettoriale V su $\mathbb{K}$. Scriviamo $V^{\otimes 2}$ in luogo di $V \otimes V$. Ovviamente possiamo iterare il prodotto tensoriale quante volte vogliamo, e così considerare le potenze tensoriali di V: $V^{\otimes 0} := \mathbb{K}$, $V^{\otimes 1} = V$,...,$V^{\otimes n}$, ...

Lo spazio vettoriale (di dimensione infinita)

$$T(V) := \bigoplus_{n=1}^{\infty} V^{\otimes n}$$

si chiama algebra tensoriale. è infatti un'algebra associativa rispetto ad un ovvio prodotto che possiamo definire nel modo seguente: se $(v_1, ..., v_n)$ è una base di V, allora un tipico elemento di $T(V)$ è della forma

$$\sum_k \sum_{i_1,...,i_k} a_{i_1,...,i_k} v_{i_1} \otimes ... \otimes v_{i_k}$$

ove la somma su k è finita e gli indici possono anche essere ripetuti, ed i coefficienti stanno ovviamente in $\mathbb{K}$. Cioè i tensori che stanno in $T(V)$, che sono tutti i tensori possibili su V, sono una specie di polinomi nelle variabili $\{v_i\}$, con la notevole eccezione di non essere commutativi, in quanto ovviamente $v \otimes w \neq w \otimes v$. Che $T(V)$ sia uno spazio vettoriale è vero per costruzione, mentre la struttura di algebra si ha considerando il prodotto definito come:

$$v_{i_1} \otimes ... \otimes v_{i_k} \cdot v_{j_1} \otimes ... \otimes v_{j_h} := v_{i_1} \otimes ... \otimes v_{i_k} \otimes v_{j_1} \otimes ... \otimes v_{j_h}$$

Questo è ovviamente un prodotto associativo ed ha un'unità che è poi l'1 di $\mathbb{K} \subset T(V)$.

L'algebra tensoriale è ovviamente di dimensione infinita (possiamo pensare i suoi elementi come "polinomi non commutativi" negli elementi di V), e graduata, nel senso che si decompone in somma diretta di sottospazi vettoriali (per costruzione). Ha così senso parlare di grado di un tensore: un elemento $x \in T(V)$ ha grado n se si scrive come somma di elementi di potenze tensoriali di V non maggiori della n-ma (del tutto analogamente al grado dei polinomi: l'algebra $\mathbb{K}[X_1, ..., X_n]$ è infatti graduata ed il grado è quello usuale dei polinomi).

5.6.2 Algebra simmetrica

Mostriamo ora come possiamo considerare i polinomi su V (le funzioni polinomiali $V \longrightarrow \mathbb{K}$) come quoziente dell'algebra tensoriale.

Consideriamo in $T(V)$ l'ideale I(V) generato dagli elementi della forma $v \otimes w - w \otimes v$ con $v, w \in V$, e quindi il quoziente

$$\mathrm{Sym}(V) := T(V)/I(V)$$

Denotiamo l'immagine di un tensore $v_{i_1} \otimes ... \otimes v_{i_k} \in T(V)$ nel quoziente $\wedge(V)$ con la scrittura $v_{i_1} \cdot ... \cdot \wedge v_{i_k}$. Poichè l'ideale $I(V)$ è graduato, nel senso che se $I^k(V) := I(V) \cap V^{\otimes k}$ allora

$$I(V) = \bigoplus_k I^k(V)$$

anche l'algebra $\mathrm{Sym}(V)$ è graduata:

$$\mathrm{Sym}(V) = \bigoplus_k S^k(V)$$

con

$$S^k(V) = V^{\otimes k}/I^k(V)$$

Questa nuova algebra è stata costruita in modo che i suoi elementi, oltre a soddisfare le relazioni multilineari dei tensori qualsiasi, soddisfino anche la commutatività, cioè se v e w sono in V allora

$$vw = wv$$

Gli elementi di $\mathrm{Sym}(V)$ si dicono *tensori simmetrici*, e $\mathrm{Sym}(V)$ si dice *algebra simmetrica* su V.

Si tratta effettivamente di un'algebra associativa con elemento neutro perché l'ideale $I(V)$ è un ideale per la struttura associativa. Inoltr el'algebra simmetrica è per definizione commutativa.

Notiamo che l'algebra simmetrica può ottenersi considerando la rappresentazione di S_n su V^n data da

$$\sigma(v_1 \otimes ... \otimes v_n) = v_{\sigma(1)} \otimes ... \otimes v_{\sigma(n)}$$

e considerando gli invarianti della rappresentazione, i,e, gli elementi v di $V^{\otimes n}$ tali che $\sigma v = v$: si tratta degli elementi di $S^n(V)$.

Ora ci concentreremo sui singoli addendi $S^k(V)$ dell'algebra simmetrica. Consideriamo cioè il solito spazio vettoriale V di dimensione n con la solita base $(v_1, ..., v_n)$, e l'algebra simmetrica di grado k su V: S^kV.

Vogliamo caratterizzare questo spazio in termini di mappe multilineari, come abbiamo fatto per i tensori. Intanto osserviamo che S^kV si ottiene da $V^{\otimes k}$ quozientando per il sottospazio generato dai vettori $v \otimes v - w \otimes v$, e quindi i suoi elementi, che hanno la forma

$$\sum_{i_1,...,i_k} a_{i_1...i_k} v_{i_1} ... v_{i_k}$$

verificano la commutatività, i.e. si può sempre scrivere

$$v_{i_1}...v_{i_k} = v_{j_1}...v_{j_k}$$

se $\{i_1, ..., i_k\} = \{j_1, ..., j_k\}$. Ora consideriamo le applicazioni multilineari simmetriche di V in sé, cioè le funzioni

$$f : V^k \longrightarrow W$$

multilineari e tali che

$$f(v_1, ..., v_k) = f(v_{i_1}, ..., v_{i_k}) = 0$$

per ogni permutazione $i : j \longrightarrow i_j$ degli interi $\{1, ..., n\}$.

Se $W = \mathbb{K}$ abbiamo il concetto di forma multilineare simmetrica in k variabili: ad esempio un prodotto scalare è una forma bilineare simmetrica.

Notiamo ora che

5.6.4 Proposizione *I tensori $S^k(V)$ sono esattamente i polinomi omogenei di grado k negli elementi di V.*

DIMOSTRAZIONE: Basta osservare che, dato che un elemento di $S^k(V)$ è della forma

$$s = \sum_{i_1,...,i_k} a_{i_1...i_k} v_{i_1}...v_{i_k}$$

Quindi se $(e_1, ..., e_n)$ è una base di V allora

$$s = \sum_{j_1,...,j_n} a_{j_1...j_n} e_1^{j_1}...e_n^{j_n}$$

convenendo che j_k possa anche essere zero, ed in tal caso $e_k^{j_k}$ venga omesso.

QED

Dunque l'algebra simmetrica $\mathrm{Sym}(V)$ può vedersi come l'algebra dei polinomi $\mathbb{K}[V]$ ovvero $\mathbb{K}[e_1, ..., e_n]$; in particolare, $\mathrm{Sym}(V^*)$ sono le funzioni polinomiali su V, quindi i polinomi nel senso elementare del termine. Si noti che $\mathbb{K}[V \times W] = \mathbb{K}[V] \otimes \mathbb{K}[W]$.

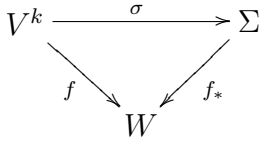
L'algebra simmetrica verifica una proprietà universale:

5.6.5 Teorema *Se V è uno spazio vettoriale di dimensione n su $\mathbb{K}$ e se k è un intero positivo allora esiste un unico spazio vettoriale Σ di dimensione finita su $\mathbb{K}$, ed una mappa multilineare simmetrica*

$$\sigma : V^k \longrightarrow \Sigma$$

tale che

(1) *Se W è uno spazio vettoriale e se $f : V^k \longrightarrow W$ è una mappa multilineare simmetrica, allora esiste un'unica mappa lineare $f_* : \Sigma \longrightarrow W$ tale che $f = f_* \circ \sigma$, i.e. che il seguente diagramma*



(2) *Se $(v_1, ..., v_n)$ è una base di V allora $\{\sigma(v_{i_1}, ..., v_{i_k})\}$ con $1 \leq i_1 \leq ... \leq i_k$ è una base di W.*

Dimostrazione: Procediamo in modo analogo al teorema 5.6.1, considerando per ogni sottoinsieme S di $\{1, ..., n\}$ di k elementi anche ripetuti[5] (ad esempio può essere $S = (1, 1, ..., 1)$ e si noti che $(2, 1, 1, .., 1)$ e $(1, 2, 1, ..., 1)$ corrispondono alla stessa scelta) un simbolo σ_S, e prendendo lo spazio vettoriale generato da questi simboli su $\mathbb{K}$, che ha dimensione $\binom{n+1+k}{k}$, e che denotiamo Σ. Se $\{v_1, ..., v_n\}$ è una base di V, allora S è lo spazio delle combinazioni lineari

$$\sum_{i_1 \leq i_2 \leq ... \leq i_k} a_{i_1 ... i_k} v_{i_1} ... v_{i_k}$$

Sia ora $v \in V^k$ della forma

$$v = \sum_{i_1, ..., i_k} a_{i_1 ... i_k} (v_{i_1}, ..., v_{i_k})$$

e definiamo la mappa σ come

$$\sigma(v) := \sum_{i_1 \leq i_2 \leq ... \leq i_k} a_{i_1 ... i_k} (i_1, ..., i_k)$$

(S è generato da elementi del tipo $(i_1, ..., i_k)$). Che si tratti di una mappa multilineare simmetrica segue dalla definizione, ed è pure un fatto ovvio che

$$\sigma(v_{i_1}, ..., v_{i_k}) = \sigma_S$$

se $S = \{i_1, ..., i_k\}$ con $i_1 \leq ... \leq i_k$.

La dimostrazione della (1) si riduce alla semplice osservazione che se $f : V^k \longrightarrow W$ è multilineare simmetrica, la mappa

$$f_*(\sigma_S) := f(v_{i_1}, ..., v_{i_k})$$

[5] Si tratta sostanzialmente dei monomi di grado k nelle indeterminate $1, .., n$.

è ben definita su una base di Σ e quindi si estende ad un'unica mappa lineare da Σ in W.

Per la dimostrazione della (2) basta notare che gli elementi $\{\sigma(v_{i_1}, ..., v_{i_k})\}$ generano Σ e sono esattamente $\binom{n+k+1}{k}$.

QED

Di nuovo possiamo dedurre l'unicità dello spazio Σ dalla sua proprietà universale, ed è evidente che la potenza simmetrica $S^k(V)$ soddisfa questa proprietà: ne segue che abbiamo una naturale identificazione

$$\Sigma \cong S^k(V)$$

che, a livello di basi, è

$$\sigma(v_{i_1}, ..., v_{i_k}) \longleftrightarrow v_{i_1}...v_{i_k}$$

Osserviamo che il risultato precedente può riformularsi dicendo che lo spazio delle forme multilineari simmetriche è isomorfo allo spazio duale dei tensori simmetrici:

$$\mathrm{Sym}(V^k, \mathbb{K}) \cong (S^k(V))^*$$

Inoltre, è possibile associare ad una mappa $f : V \longrightarrow W$ lineare la sua potenza simmetrica k-sima $S^k f : S^k V \longrightarrow S^k W$ definita come

$$S^k f(u_1, ..., u_k) = f(u_1)...f(u_k)$$

Notiamo che l'algebra simmetrica completa $\bigoplus_k S^k(V)$ è di dimensione infinita e corrisponde all'algebra dei polinomi su V.

5.6.3 Algebra esterna

Costruiamo ora un'altra algebra tensoriale: l'*algebra esterna*. Consideriamo in $T(V)$ l'ideale I(V) generato dagli elementi della forma $v \otimes v$ per $v \in V$, e quindi il quoziente

$$\wedge(V) := T(V)/I(V)$$

Denotiamo l'immagine di un tensore $v_{i_1} \otimes ... \otimes v_{i_k} \in T(V)$ nel quoziente $\wedge(V)$ con la scrittura $v_{i_1} \wedge ... \wedge v_{i_k}$. Poichè l'ideale $I(V)$ è graduato, nel senso che se $I^k(V) := I(V) \cap V^{\otimes k}$ allora

$$I(V) = \bigoplus_k I^k(V)$$

anche l'algebra $\wedge(V)$ è graduata:

$$\wedge(V) = \bigoplus_k \wedge^k(V)$$

con

$$\wedge^k(V) = V^{\otimes k}/I^k(V)$$

Questa nuova algebra è stata costruita in modo che i suoi elementi, oltre a soddisfare le relazioni multilineari dei tensori qualsiasi, soddisfino anche quelle antisimmetriche, cioè se v e w sono in V allora

$$v \wedge w = -w \wedge v$$

e quindi

$$v \wedge v = 0$$

Da qui per induzione:

$$\forall x \in \wedge^k(V)\ \forall y \in \wedge^h(V) \quad x \wedge y = (-1)^{kh} y \wedge x$$

Gli elementi di $\wedge(V)$ si dicono *tensori antisimmetrici*, e $\wedge(V)$ si dice *algebra esterna* su V. Si tratta di un'algebra associativa, che per definizione è anticommutativa.

Notiamo che $w^k(V)$ può essere costruito considerando la rappresentazione del gruppo A_n su $V^{\otimes n}$ data da

$$\sigma(v_1 \otimes ... \otimes v_n) = v_{\sigma(1)} \otimes ... \otimes v_{\sigma(n)}$$

e considerandone gli invarianti.

Ora ci concentreremo sui singoli addendi $\wedge^k(V)$ dell'algebra esterna. Consideriamo cioè il solito spazio vettoriale V di dimensione n con la solita base $(v_1, ..., v_n)$, e l'algebra esterna di grado k su V: $\wedge^k V$.

Vogliamo caratterizzare questo spazio in termini di mappe multilineari, come abbiamo fatto per i tensori. Intanto osserviamo che $\wedge^k V$ si ottiene da $V^{\otimes k}$ quozientando per il sottospazio generato dai vettori $v \otimes v$, e quindi i suoi elementi, che hanno la forma

$$\sum_{i_1,...,i_k} a_{i_1...i_k} v_{i_1} \wedge ... \wedge v_{i_k}$$

verificano relazioni del tipo:

$$v_{i_1} \wedge ... \wedge v_{i_j} \wedge ... \wedge v_{i_j} \wedge ... \wedge v_{i_k} = 0$$

Ora consideriamo le applicazioni multilineari alterne di V in sé, cioè le funzioni

$$f : V^k \longrightarrow W$$

multilineari e tali che

$$f(v_{i_1}, ..., v, ..., v, ..., v_{i_k}) = 0$$

il che ovviamente implica

$$f(v_{i_1}, ..., v, ..., w, ..., v_{i_k}) = -f(v_{i_1}, ..., w, ..., v, ..., v_{i_k})$$

Se $W = \mathbb{K}$ abbiamo il concetto di forma multilineare alternante in k variabili.

5.6.6 Esempio *Se guardiamo ad una matrice A come alla successione ordinata dei vettori colonna che la compongono, $A = (A^1, ..., A^n)$, il determinante*

$$\det : V^n \longrightarrow \mathbb{K}$$

è multilineare alternante, e si può completamente caratterizzare aggiungendo la condizione

$$\det(1) = 1$$

che il determinante della matrice identica sia 1.

5.6.7 Esempio *Consideriamo i tensori di grado due, i.e. degli elementi di $V \otimes V$: ogni tale tensore è comma di un tensore antisimmetrico e di un tensore simmetrico, in altri termini*

$$V \otimes V = S^2(V) \oplus \wedge^2(V)$$

Il determinante interviene nella dimostrazione del seguente teorema:

5.6.8 Teorema *Se V e W sono spazi vettoriali su $\mathbb{K}$ e se*

$$f : V^k \longrightarrow W$$

è una funzione multilineare alternante, dati qualsiasi $w_1, ..., w_k \in V$ e se $A = ((a_{ij}))$ è una matrice e

$$u_1 = \sum_{i=1}^{k} a_{1i} w_i \,, \qquad ... \qquad u_k = \sum_{i=1}^{k} a_{ki} w_i$$

allora

$$f(u_1, .., u_k) = \det(A) f(w_1, ..., w_k)$$

DIMOSTRAZIONE: Intanto si ha

$$f(u_1, .., u_k) = f(\sum_{i=1}^{k} a_{1i} w_i, ..., \sum_{i=1}^{k} a_{ki} w_i)$$

e, per multilinearità, si ottiene

$$\sum_{\sigma} f(a_{1,\sigma(1)}w_{\sigma(1)}, ..., a_{1,\sigma(k)}w_{\sigma(k)})$$

ove la somma è estesa a tutte le possibili mappe $\sigma : \{1, ..., k\} \longrightarrow \{1, ..., k\}$ che riordinano k elementi. Questa somma è pari a

$$\sum_{\sigma} a_{1,\sigma(1)}...a_{k,\sigma(k)} f(w_{\sigma(1)}, ..., w_{\sigma(k)})$$

sempre per multilinearità. Osserviamo che la somma in realtà non è estesa a tutte le combinazioni possibili di elementi, ma solo alle permutazioni, cioè alle mappe σ biunivoche, perché nel caso di una combinazione di termini che non sia una permutazione, nel termine $f(w_{\sigma(1)}, ..., w_{\sigma(k)})$ due o più argomenti sono uguali e quindi il termine è nullo, per alternanza di f. Otteniamo cioè

$$\sum_{\sigma \in S_k} a_{1,\sigma(1)}...a_{k,\sigma(k)} f(w_{\sigma(1)}, ..., w_{\sigma(k)})$$

ove S_k è il gruppo simmetrico su k elementi. Ora, ogni permutazione $\sigma \in S_k$ si può ottenere come una sequenza di scambi fra coppie di elementi: quando scambiamo due argomenti nel termine $f(w_{\sigma(1)}, ..., w_{\sigma(k)})$ il segno cambia (per alternanza) e quindi una volta effettuata la permutazione, otteniamo un fattore $(-1)^{sgn(\sigma)}$ ove il segno di una permutazione è il numero di scambi che la compongono.

Insomma, trasformare il termine $f(w_{\sigma(1)}, ..., w_{\sigma(k)})$ in $f(w_1, ..., w_k)$ comporta unicamente l'apparizione di un segno $(-1)^{sgn(\sigma)}$, e quindi la somma precedente si trasforma in

$$f(u_1, ..., u_k) = \sum_{\sigma \in S_k} (-1)^{sgn(\sigma)} a_{1,\sigma(1)}...a_{k,\sigma(k)} f(w_1, ..., w_k)$$

che è uguale a

$$\det(A) f(w_1, ..., w_k)$$

QED

Il fatto che il determinante di A sia definito come

$$\det(A) = \sum_{\sigma \in S_k} (-1)^{sgn(\sigma)} a_{1,\sigma(1)}...a_{k,\sigma(k)}$$

segue dal familiare sviluppo di Laplace, e costituisce un esercizio di calcolo combinatorio (nel farlo può essere utile esaminare i casi $k = 2$ e $k = 3$ separatamente...)

La comprensione del teorema precedente è cruciale per capire le forme alternanti. Abbiamo comunque bisogno di una versione più generale di questo teorema, la cui dimostrazione proveremo a lasciare per esercizio, non prima d'aver messo in grado il lettore di risolverlo, per via delle seguenti osservazioni.

Consideriamo una matrice A di dimensioni $k \times n$ e con $k \leq n$ ed un sottoinsieme S dell'insieme di interi $\{1, ..., n\}$ con k elementi. Di tali sottoinsiemi ve ne sono

$$\binom{n}{k}$$

come noto dal calcolo combinatorio. Se questi elementi sono $S = \{i_1, ..., i_k\}$ allora possiamo assumere che siano ordinati: $i_1 < ... < i_k$. Consideriamo una funzione

$$\sigma : \{1, ..., k\} \longrightarrow S$$

cioè un modo di associare ad un numero fra 1 e k un elemento di S e supponiamo che questa funzione sia iniettiva. Allora è biunivoca (perché?) e quindi definisce una permutazione di S.

5.6.9 Esempio *Se $n = 4$ e $k = 3$, e $S = \{1, 3, 4\}$, la permutazione σ definita da*

$$\sigma(1) = 4 \qquad \sigma(3) = 1 \qquad \sigma(4) = 3$$

ha segno +1.

Se chiamiamo $P(S)$ l'insieme delle permutazioni degli elementi di S (che è dire l'insieme delle biiezioni di S in sé, e se torniamo alla nostra matrice $A = ((a_{ij}))$, per ogni insieme S di cardinalità k possiamo considerare il minore $k \times k$ di A costituito dagli elementi a_{ij} tali che $j \in S$. Denotiamo con

$$\det_S(A)$$

il determinante di questo minore. Allora è

$$\det_S(A) = \sum_{\sigma \in P(S)} (-1)^{sgn(\sigma)} a_{1,\sigma(1)} ... a_{k,\sigma(k)}$$

Ora siano $w_1, ..., w_n$ elementi in V, e per ognuno degli insiemi S definiamo

$$w_S = (w_{i_1}, ..., w_{i_k})$$

ove gli elementi di S sono tali che $i_1 < ... < i_k$. A questo punto, usando le notazioni introdotte, il lettore dovrebbe dimostrare il seguente

5.6.10 Teorema *Se V e W sono $\mathbb{K}$-spazi vettoriali, e se*

$$f : V^k \longrightarrow W$$

è una mappa multilineare alternante, se $w_1, ..., w_n$ sono elementi di V e A è una matrice $k \times n$ e se

$$u_1 = \sum_{i=1}^{n} a_{1i} w_i \,, \qquad ... \qquad u_k = \sum_{i=1}^{n} a_{ki} w_i$$

allora

$$f(u_1, .., u_k) = \sum_S \det_S(A) f(w_S)$$

(Come suggerimento si osservi che la dimostrazione è simile a quella del teorema precedente, salvo in un punto nel quale bisogna spezzare la somma $\sum_\sigma$ come $\sum_S \sum_{\sigma \in P(S)}$).

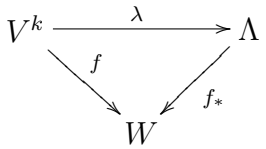
Siamo ora in grado di dimostrare una proprietà universale dei prodotti esterni, analoga al teorema 5.6.1:

5.6.11 Teorema *Se V è uno spazio vettoriale di dimensione n su $\mathbb{K}$ e se k è un intero tale che $1 \leq k \leq n$ allora esiste un unico spazio vettoriale Λ di dimensione finita su $\mathbb{K}$, ed una mappa multilineare alternante*

$$\lambda : V^k \longrightarrow \Lambda$$

tale che

(1) *Se W è uno spazio vettoriale e se $f : V^k \longrightarrow W$ è una mappa multilineare alternante, allora esiste un'unica mappa lineare $f_* : \Lambda \longrightarrow W$ tale che $f = f_* \circ \lambda$, i.e. che il seguente diagramma*



(2) *Se $(v_1, ..., v_n)$ è una base di V allora $\{\lambda(v_{i_1}, ..., v_{i_k})\}$ con $1 \leq i_1 < ... < i_k \leq n$ è una base di W.*

Dimostrazione: Procediamo in modo analogo al teorema 5.6.1, considerando per ogni sottoinsieme S di $\{1, ..., n\}$ di k elementi un simbolo λ_S, e prendendo lo spazio vettoriale generato da questi simboli su $\mathbb{K}$, che ha dimensione $\binom{n}{k}$, e che

denotiamo Λ. Se ora $\{v_1, ..., v_n\}$ è una base di V, se $\{u_1, ..., u_k\}$ sono elementi di V e la matrice A è definita come

$$u_i = \sum_{j=1}^{n} a_{ij} v_j$$

allora la mappa λ si definisce come:

$$\lambda(u_1, ..., u_k) := \sum_S \det_S(A) \lambda_S$$

Che si tratti di una mappa multilineare alternante segue dalle proprietà dei determinanti, ed è pure un fatto ovvio che

$$\lambda(v_{i_1}, ..., v_{i_k}) = \lambda_S$$

se $S = \{i_1, ..., i_k\}$ con $i_1 < ... < i_k$.

La dimostrazione della (1) si riduce alla semplice osservazione che se $f : V^k \longrightarrow W$ è multilineare alternante, la mappa

$$f_*(\lambda_S) := f(v_{i_1}, ..., v_{i_k})$$

è ben definita su una base di Λ e quindi si estende ad un'unica mappa lineare da Λ in W.

Per la dimostrazione della (2) basta notare che gli elementi $\{\lambda(v_{i_1}, ..., v_{i_k})\}$ generano Λ e sono esattamente $\binom{n}{k}$.

QED

Di nuovo possiamo dedurre l'unicità dello spazio Λ dalla sua proprietà universale, ed è evidente che la potenza esterna $\wedge^k(V)$ soddisfa questa proprietà: ne segue che abbiamo una naturale identificazione

$$\Lambda \cong \wedge^k(V)$$

che, a livello di basi, è

$$\lambda(v_{i_1}, ..., v_{i_k}) \longleftrightarrow v_{i_1} \wedge ... \wedge v_{i_k}$$

Osserviamo che il risultato precedente può riformularsi dicendo che lo spazio delle forme multilineari alternanti è isomorfo allo spazio duale dei tensori antisimmetrici:

$$Alt(V^k, \mathbb{K}) \cong (\wedge^k(V))^*$$

Inoltre, è possibile associare ad una mappa $f : V \longrightarrow W$ lineare la sua potenza esterna k-ma $\wedge^k f : \wedge^k V \longrightarrow \wedge^k W$ definita come

$$\wedge^k f(u_1, ..., u_k) = f(u_1) \wedge ... \wedge f(u_k)$$

In particolare, dato che

$$\dim \wedge^k(V) = \binom{\dim V}{k}$$

osserviamo che la massima potenza esterna ($k = n$) di V è unidimensionale: inoltre, dato che $v \wedge v = 0$, non possono esservi potenze esterne $(n+1)$-dimensionali o più, e quindi l'algebra esterna è finito dimensionale! Questa è una profonda differenza rispetto all'algebra simmetrica.

Dato che $\wedge^n(V) \cong \mathbb{K}$, una sua base è data da un qualsiasi scalare non nullo: una scelta naturale è proprio la funzione determinante, che si caratterizza con la condizione $\det(1) = 1$.

5.6.12 Proposizione *Se* $\dim V = n$ *e se* $f : V \longrightarrow V$ *è una mappa lineare, allora la mappa* $\wedge^n f : \wedge^n(V) \longrightarrow \wedge^n(V)$ *è semplicemente una mappa lineare di* $\mathbb{K}$ *in sè, cioè la moltiplicazione per uno scalare, e precisamente*

$$(\wedge^n f)(x) = \det(f)x$$

Si tratta di una riformulazione dello sviluppo di Laplace del determinante.

Per finire vogliamo osservare che un caso particolare di prodotto esterno è certo noto al lettore: si tratta del prodotto vettoriale. Ricordiamo infatti che se V ha dimensione 3, è definito il prodotto vettoriale di due suoi elementi:

$$[v, w] := \begin{pmatrix} v_2w_3 - v_3w_2 \\ v_3w_1 - v_1w_3 \\ v_1w_2 - v_2w_1 \end{pmatrix}$$

se $v = (v_1, v_2, v_3)$ e $w = (w_1, w_2, w_3)$. Ma si ha

$$[v, w] = v \wedge w$$

Infatti $\dim \wedge^2 V = \dim V = 3$ (*in questo caso e solo in questo caso* la dimensione di V coincide con quella della sua seconda potenza esterna), e dato che il prodotto vettoriale è una funzione bilineare alternante, per universalità si ha la formula precedente.

L'algebra $\mathbb{R}^3$ col prodotto $\wedge$ verifica l'identità di Jacobi

$$(v_1 \wedge v_2) \wedge v_3 + (v_3 \wedge v_1) \wedge v_2 + (v_2 \wedge v_3) \wedge v_1 = 0$$

cioè, ponendo

$$[v, w] = v \wedge w$$

$\mathbb{R}^3$ diviene un'algebra di Lie. Si tratta dell'algebra $\mathfrak{so}(3)$ associata al gruppo delle rotazioni del piano.