

Dispense del corso di Teoria delle Rappresentazioni

Matematici e fisici del secondo anno, a.a. 2016/2017

11 luglio 2017

Indice

1	Nozioni di base di teoria dei gruppi	4
1.1	Definizioni e primi risultati	4
1.2	Gruppi ciclici	9
1.3	Gruppi abeliani	9
1.4	Gruppi simmetrici	10
1.5	Gruppi diedrali	11
2	Alcuni risultati di algebra lineare	12
3	Algebra multilineare	14
3.1	Base di uno spazio vettoriale	14
3.2	Prodotto tensoriale	14
3.3	Prodotto esterno e prodotto simmetrico	18
4	Prime proprietà delle rappresentazioni	22
4.1	Definizione e primi esempi	22
4.2	Operazioni con le rappresentazioni	25
4.3	Sottospazi invarianti e scomposizione delle rappresentazioni	27
4.4	Alcuni isomorfismi notevoli	32
5	Teoria dei caratteri	33
5.1	Tabella dei caratteri	38
5.2	Esempi di rappresentazioni di gruppi finiti	38
5.2.1	I problemi della prima lezione visti con i nuovi strumenti	43
6	Rappresentazioni reali, complesse e quaternioniche	46
6.1	Quaternioni	51
7	Rappresentazioni indotte	56
7.1	Formula di aggiunzione	59
7.1.1	Le rappresentazioni dei gruppi diedrali D_n	60
8	Rappresentazioni di gruppi compatti	62
8.1	Le rappresentazioni di \mathbb{S}^1	63
8.2	Le rappresentazioni di $SU(2)$	67
8.2.1	Le rappresentazioni irriducibili di $SO(3)$	73

9	Rappresentazioni di algebre	76
9.1	Prime definizioni e esempi	76
9.2	Ideali e quozienti	78
9.3	Serie di composizione	79
9.4	Teorema di Krull-Schmidt	81
9.5	Semisemplicità	83
9.6	Struttura di $\mathbb{K}[G]$ come algebra	85
9.7	Un teorema di divisibilità	88
10	Rappresentazioni di S_n	91

Introduzione

Qui dovremmo scrivere una introduzione, specificare quali sono le finalità e a chi sono rivolti determinati capitoli, eccetera.

1 Nozioni di base di teoria dei gruppi

1.1 Definizioni e primi risultati

Definizione 1.1 (Gruppo). Un gruppo è un insieme G dotato di un'operazione binaria $\cdot : G \times G \rightarrow G$ che gode delle seguenti proprietà:

1. Associatività: presi comunque $a, b, c \in G$ vale che $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. Esiste $e \in G$, chiamato *unità*, o *identità*, o *elemento neutro*, tale che $\forall a \in G$ vale $e \cdot a = a = a \cdot e$
3. Per ogni $a \in G$ esiste un a' tale che $a' \cdot a$ e $a \cdot a'$ sono unità, ovvero si comportano come l'elemento e al punto precedente. Un tale a' si dice *inverso* di a .

Per comodità di solito si omette il puntino. Se G è finito e ha cardinalità n , si dice che G ha *ordine* n , e si scrive $|G| = n$ oppure $\text{ord}(G) = n$.

Primi esempi di gruppi

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con l'operazione di somma.
2. $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con l'operazione di moltiplicazione (dagli insiemi è stato tolto 0).
3. $GL_n(\mathbb{K})$ dove \mathbb{K} è un campo o in generale $GL(V)$ dove V è uno spazio vettoriale.
4. L'insieme delle funzioni $f : I \rightarrow I$ biunivoche, dove I è un insieme e l'operazione di gruppo è la composizione. Nel caso in cui I sia un insieme finito, tanto vale scegliere $I = \{1, 2, 3, \dots, n\}$. In tal caso questo gruppo si indica con S_n .

Alcune proprietà elementari

1. L'unità e è unica.

Dimostrazione: supponiamo che e ed e' siano entrambe unità. Allora vale

$$e = ee' = e'$$

2. Dato $a \in G$, l'inverso di a è unico (e usualmente si denota con a^{-1}).

Dimostrazione: supponiamo che a', a'' siano entrambi inversi di a . Allora

$$(a'a)a'' = a'(aa'') \implies ea'' = a'e \implies a'' = a'$$

3. Dati a_1, a_2, \dots, a_n , il prodotto $a_1 \cdot a_2 \cdots a_n$ è ben definito senza bisogno di parentesi.

4. Se $ab = e$, allora anche $ba = e$, dunque a e b sono uno l'inverso dell'altro.

Dimostrazione: $ba = bae = babb^{-1} = beb^{-1} = bb^{-1} = e$.

5. Dato un intero positivo k e un elemento $a \in G$, definiamo $a^k = \underbrace{a \cdot a \cdots a}_{k \text{ volte}}$. Inoltre poniamo

$a^0 = e$ e infine $a^{-k} = (a^{-1})^k$, così abbiamo definito le potenze con esponente in \mathbb{Z} . Non è difficile dimostrare che, se k, h sono interi (non necessariamente positivi), valgono le usuali proprietà:

$$a^{k+h} = a^k \cdot a^h \quad (a^k)^h = a^{kh}$$

Però non è vero in generale che $(ab)^k = a^k b^k$ (sarebbe vero se l'operazione fosse commutativa). Osserviamo infine che

$$(ab)^{-1} = b^{-1}a^{-1}$$

infatti $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$.

Definizione 1.2 (Sottogruppo). Sia G un gruppo, $H \subseteq G$ si dice sottogruppo di G se:

- $e \in H$
- $x, y \in H \implies xy \in H$
- $x \in H \implies x^{-1} \in H$

e si indica $H \leq G$. Si verifica facilmente che queste condizioni sono quelle necessarie (e sufficienti) a fare in modo che H sia esso stesso un gruppo con l'operazione ereditata da G .

Esempio 1.1 (Sottogruppo generato da un elemento). Sia G un gruppo e a un suo elemento. L'insieme delle potenze di a , ovvero $\{a^k | k \in \mathbb{Z}\}$, è un sottogruppo di G , che di solito viene denotato con $\langle a \rangle$.

Osservazione. Se G è gruppo, $a \in G$ ed esiste un intero $n > 0$ tale che $a^n = e$, allora tutti gli elementi di $\langle a \rangle$ sono della forma a^k per qualche $0 \leq k < n$. Infatti se si considera un qualsiasi a^s con $s \in \mathbb{Z}$, si può scrivere $s = nq + r$ con $0 \leq r < n$. Allora

$$a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$$

Se n è il minimo intero positivo tale che $a^n = e$, allora si dice che a ha *ordine* n . In tal caso è facile verificare che l'insieme $\langle a \rangle$ contiene esattamente n elementi distinti, ovvero a^0, a^1, \dots, a^{n-1} . Infatti, se fosse $a^i = a^j$ con $0 \leq i < j < n$, allora $a^{j-i} = e$, che sarebbe assurdo siccome $0 < j - i < n$.

Se $\langle a \rangle$ è finito (il che è certo se ad esempio G è finito) allora di sicuro esiste $n > 0$ tale che $a^n = e$. Infatti basta prendere $0 \leq i < j$ tali che $a^i = a^j$ e osservare che $a^{j-i} = e$. Questi i e j esistono per forza perché se tutte le potenze fossero distinte allora $\langle a \rangle$ sarebbe infinito.

Definizione 1.3 (Laterale). Sia G un gruppo e $H < G$ un suo sottogruppo: definiamo *laterale destro* o *classe laterale destra* di H un sottoinsieme di G del tipo

$$gH = \{gh \mid h \in H\}$$

Osservazione. Dato un gruppo G e un sottogruppo $H < G$, tutte le classi laterali di H hanno la stessa cardinalità di H . Consideriamo infatti una classe laterale gH dove g è un certo elemento di G . Allora l'applicazione $\phi_g : H \rightarrow gH$ tale che $\phi_g(h) = gh$ per ogni $h \in H$ è certamente surgettiva. Se fosse $\phi_g(h_1) = \phi_g(h_2)$ allora $gh_1 = gh_2$ e moltiplicando a sinistra per l'inverso di g si otterrebbe $h_1 = h_2$. Quindi ϕ_g è iniettiva e in conclusione è bigettiva.

Definizione 1.4 (Quoziente). Sia G un gruppo e H un suo sottogruppo: chiamiamo *quoziente* di G per H l'insieme delle classi laterali di H , che indicheremo con G/H , ovvero

$$G/H = \{gH \mid g \in G\}$$

Teorema 1.1. *Il quoziente di un gruppo G per un suo sottogruppo H fornisce una partizione di G : per ogni $g \in G$ esiste un unico H -laterale destro $g'H$ tale che $g \in g'H$.*

Dimostrazione. L'esistenza è facile: si osserva che $g \in gH$ visto che $gH = \{gh \mid h \in H\}$ e che $e \in H$. Supponiamo ora che $g \in \alpha H$, dunque $g = \alpha h_1$ per qualche h_1 . Si osserva allora che i due laterali coinciderebbero:

$$\alpha H = \{\alpha h \mid h \in H\} = \{\alpha h_1 h \mid h \in H\} = \{gh \mid h \in H\} = gH$$

□

Da quanto abbiamo visto segue subito il seguente risultato:

Teorema 1.2 (Teorema di Lagrange). *Sia G un gruppo finito, $H < G$, allora $|H|$ divide $|G|$ e, in particolare, $|G/H| = \frac{|G|}{|H|}$; il numero $|G/H|$ viene chiamato indice di H in G .*

Definizione 1.5 (Sottogruppo normale). Sia G un gruppo, $H \leq G$ si dice *normale* in G se

$$\forall h \in H, \forall g \in G \quad ghg^{-1} \in H$$

e si indica $H \trianglelefteq G$.

Definizione 1.6 (Gruppo quoziente). Sia G gruppo, $H \trianglelefteq G$ (osservare che si richiede che il sottogruppo sia *normale*), allora chiameremo *gruppo quoziente* di G su H l'insieme quoziente come l'abbiamo definito (1.4) munito della seguente operazione:

$$(g_1 H) \cdot (g_2 H) = g_1 g_2 H$$

Lasciamo come esercizio la dimostrazione del fatto che tale operazione è ben definita, ovvero non dipende dai “rappresentanti” g_1, g_2 , e che rispetta effettivamente gli assiomi di gruppo. In particolare è essenziale il fatto che H sia normale per dimostrare la buona definizione dell'operazione.

Definizione 1.7 (Classi di coniugio). Sia G un gruppo, $x \in G$, la classe di coniugio di x è l'insieme $\{xgx^{-1} \mid g \in G\}$. Si dimostra facilmente che le classi di coniugio di tutti gli elementi di G formano una partizione del gruppo stesso. Si osserva inoltre che un sottogruppo è normale se e solo se è unione di classi di coniugio (ma in generale non è vero che unendo delle classi di coniugio si ottiene un sottogruppo).

Esempio 1.2 (Le classi di coniugio di $GL_n(\mathbb{C})$). Nel caso del gruppo $GL_n(\mathbb{C})$ due matrici stanno nella stessa classe di coniugio se e solo se sono simili, quindi per ogni classe di coniugio esiste un rappresentante canonico che è la forma di Jordan di una qualsiasi matrice nella classe (con opportune convenzioni sull'ordine dei blocchi e degli autovalori).

Definizione 1.8 (Centro di un gruppo). Sia G un gruppo, il *centro* di G si indica con $Z(G)$ ed è il sottoinsieme degli elementi che commutano con tutto G :

$$Z(G) = \{h \in G \mid hg = gh \forall g \in G\}$$

È immediato verificare che $Z(G)$ è un sottogruppo normale di G .

Definizione 1.9 (Prodotto diretto di gruppi). Siano G e H gruppi. Si definisce prodotto diretto di G e H il gruppo formato dall'insieme $G \times H = \{(g, h) \mid g \in G, h \in H\}$ con l'operazione componente per componente, ovvero separatamente per i due gruppi di partenza.

Definizione 1.10 (Omomorfismo (isomorfismo) di gruppi). Siano G ed H gruppi, un'applicazione $\varphi : G \rightarrow H$ si dice *omomorfismo di gruppi* se

$$\forall g_1, g_2 \in G \quad \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$$

dove la prima moltiplicazione è fatta in G mentre la seconda in H . Se φ è bigettiva, allora si dice *isomorfismo*, e i due gruppi si dicono *isomorfi* (in tal caso si scrive $G \cong H$). Indichiamo con $\text{Hom}(G, H)$ l'insieme degli omomorfismi da G ad H .

Due gruppi isomorfi sono a tutti gli effetti “lo stesso gruppo”, nel senso che dall'uno all'altro cambiano solo i simboli con cui indichiamo gli elementi, e il modo con cui passare da una “scrittura” all'altra è dato dall'isomorfismo.

Esercizio 1.1. Dati G e H due gruppi e $f : G \rightarrow H$ un omomorfismo di gruppi, $f(e_G) = e_H$ dove e_G, e_H sono le unità dei rispettivi gruppi.

Definizione 1.11. Siano G e H gruppi, $f : G \rightarrow H$ un omomorfismo di gruppi, allora definiamo il nucleo (kernel) e l'immagine di f rispettivamente come:

$$\begin{aligned} \text{Ker } f &= \{g \in G \mid f(g) = e_H\} \\ \text{Im } f &= \{h \in H \mid \exists g \in G \text{ tale che } f(g) = h\} \end{aligned}$$

dove e_H è l'unità di H . Non è difficile verificare che sia $\text{Ker } f$ che $\text{Im } f$ sono sempre sottogruppi rispettivamente di G e di H .

Esercizio 1.2. Dati G e H due gruppi e $f : G \rightarrow H$ un omomorfismo di gruppi, $\text{Ker } f$ è un sottogruppo normale di G .

Esercizio 1.3. Dati G e H due gruppi e $f : G \rightarrow H$ un omomorfismo di gruppi, esso è *iniettivo* se e solo se $\text{Ker } f = \{e\}$ dove $e \in G$ è l'elemento neutro.

Teorema 1.3 (Primo teorema di omomorfismo). *Dati due gruppi G e H e un omomorfismo $f : G \rightarrow H$, vale che*

$$G / \text{Ker } f \cong \text{Im } f$$

Cenno di dimostrazione. Considerare l'applicazione $\phi : G / \text{Ker } f \rightarrow \text{Im } f$ definita da

$$\phi(g \text{Ker } f) = f(g)$$

Dimostrare innanzitutto che è ben definita (questo è il punto fondamentale) e poi che è un omomorfismo di gruppi. Infine, mostrare che è bigettiva. \square

Osservazione. Se la f del teorema precedente è iniettiva, allora $G / \text{Ker } f \cong G$ e quindi $G \cong \text{Im } f$. Invece se f è surgettiva, allora $G / \text{Ker } f \cong H$.

Osservazione. Ci si può chiedere se, dato un gruppo G e due sottogruppi normali $H, K \trianglelefteq G$ tali che $H \cong K$, si possa concludere che $G/H \cong G/K$. Questo in generale è falso! Come esempio si può prendere $G = \mathbb{Z}$, $H = 5\mathbb{Z}$ e $K = 7\mathbb{Z}$, dove

$$5\mathbb{Z} = \{5t \mid t \in \mathbb{Z}\} \quad 7\mathbb{Z} = \{7t \mid t \in \mathbb{Z}\}$$

sono i sottogruppi generati rispettivamente da 5 e 7. Infatti è facile esibire degli isomorfismi $H \cong \mathbb{Z} \cong K$, ma G/H ha 5 elementi mentre G/K ne ha 7, quindi non possono essere isomorfi.¹

¹Esistono controesempi anche con gruppi finiti.

Definizione 1.12 (Azione di un gruppo su un insieme). Sia G un gruppo e I un insieme. Chiamiamo azione di G su I una funzione $a : G \times I \rightarrow I$ che rispetti la regola di composizione, ovvero tale che se $h, g \in G$ e $i \in I$, valga

$$a(h, a(g, i)) = a(hg, i)$$

e tale che l'elemento neutro $e \in G$ agisca "banalmente", ovvero $a(e, i) = i$ per ogni $i \in I$. Normalmente si usa una notazione abbreviata in cui invece di scrivere $a(g, i)$ si scrive direttamente $g \cdot i$ o addirittura gi , quindi le condizioni date si riscrivono:

$$\begin{aligned} h \cdot (g \cdot i) &= (hg) \cdot i \\ e \cdot i &= i \end{aligned}$$

In pratica un'azione di un gruppo G su un insieme I ci consente di "interpretare" ogni elemento $g \in G$ come una funzione $g : I \rightarrow I$, e l'operazione di gruppo diventa la composizione delle funzioni.

Esercizio 1.4. Mostrare che in realtà queste funzioni date dagli elementi di G sono bigettive, e che si ha un omomorfismo di gruppi $G \rightarrow \text{Big}(I)$ dove $\text{Big}(I)$ è il gruppo delle funzioni bigettive da I in sé.

Definizione 1.13 (Azione transitiva). Un'azione di un gruppo G su un insieme $I \neq \emptyset$ si dice *transitiva* se dati comunque due elementi $i, j \in I$ esiste un elemento del gruppo $s \in G$ tale che $j = s \cdot i$.

Definizione 1.14 (Orbita di un elemento). Sia G un gruppo che agisce sull'insieme I , dato $x \in I$ si chiama *orbita* di x indotta dall'azione di G l'insieme $\text{Orb}_G(x) = \{g \cdot x \mid g \in G\}$, se il gruppo utilizzato è chiaro si può scrivere semplicemente $\text{Orb}(x)$. Si osserva subito che un'azione è transitiva se e solo se induce una unica orbita.

Esercizio 1.5. Le orbite indotte da un'azione del gruppo G sull'insieme I formano una partizione dell'insieme I .

Esercizio 1.6. Supponiamo di avere un gruppo G che agisce su un insieme I . Se $x \in I$ chiamiamo *stabilizzatore* di x l'insieme $\text{Stab}(x) = \{g \in G \mid g \cdot x = x\}$. Mostrare che per ogni x :

1. $\text{Stab}(x)$ è un sottogruppo di G .
2. $\text{Orb}(x)$ è in corrispondenza biunivoca con l'insieme quoziente $G/\text{Stab}(x)$.

Dedurre che se G è un gruppo finito allora vale la formula $|\text{Orb}(x)| \cdot |\text{Stab}(x)| = |G|$.

Osservazione. Un gruppo G può agire su se stesso per coniugio, ovvero dati $g \in G$ (qui G è pensato come gruppo che agisce) e $x \in G$ (G pensato come insieme che "subisce" l'azione), si pone $g \cdot x = gxg^{-1}$. Non è difficile verificare che si tratta davvero di una azione. Osserviamo che le classi di coniugio sono le orbite degli elementi generate mediante l'azione per coniugio.

Definizione 1.15 (Azione semplicemente transitiva). Un'azione di G su un insieme $I \neq \emptyset$ si dice *semplicemente transitiva* se presi comunque $i, j \in I$ esiste un unico $s \in G$ tale che $j = s \cdot i$.

Definizione 1.16 (Funzione G -equivariante). Dato un gruppo G che agisce su due insiemi I e J , una funzione $\phi : I \rightarrow J$ si dice G equivariante se

$$\phi(s \cdot_I i) = s \cdot_J \phi(i) \quad \forall s \in G, \quad \forall i \in I$$

1.2 Gruppi ciclici

Definizione 1.17 (Gruppo ciclico). Un gruppo G si dice ciclico se esiste un elemento $a \in G$ tale che ogni elemento di G è una potenza di a , ovvero $G = \langle a \rangle$. Si dice che a è un generatore di G .

Esercizio 1.7. Sia G un gruppo ciclico di cardinalità n e generatore a . Allora n è il più piccolo intero positivo tale che $a^n = e$, e ogni elemento di G si scrive in modo unico come a^k con $0 \leq k < n$.

Esempio 1.3 (Radici dell'unità). Dato $n > 0$ intero, l'insieme $\mu_n \subset \mathbb{C}^*$ delle radici n -esime dell'unità è un gruppo ciclico con n elementi.

Osservazione. Se n è un intero positivo esiste (a meno di isomorfismo) un unico gruppo ciclico di cardinalità n . Abbiamo già visto che esiste (basta considerare μ_n), inoltre dati due gruppi ciclici di cardinalità n e generatori rispettivamente a e b è immediato costruire un isomorfismo $f : \langle a \rangle \rightarrow \langle b \rangle$ ponendo $f(a^k) = b^k$ per $0 \leq k < n$.

Proposizione 1.4. Sia C_n un gruppo ciclico di cardinalità n . Allora

$$n = |\text{Hom}(C_n, \mathbb{C}^*)|$$

Dimostrazione. Sia a un generatore di C_n . Fissato $\omega \in \mu_n$ posso definire una funzione $f : C_n \rightarrow \mathbb{C}^*$ ponendo $f(a^k) = \omega^k$ per $0 \leq k < n$. Verifichiamo che $f \in \text{Hom}(C_n, \mathbb{C}^*)$. A tal fine prendiamo due elementi di C_n , che sono della forma a^k, a^h per certi interi $0 \leq k, h < n$.

$$f(a^k \cdot a^h) = f(a^{k+h}) = \omega^{k+h} = \omega^k \omega^h = f(a^k) f(a^h)$$

Dunque f è omomorfismo. Variando la scelta di $\omega \in \mu_n$ si producono effettivamente n omomorfismi differenti (infatti se ω cambia allora cambia anche $f(a)$). Mostriamo che non ci sono altri omomorfismi oltre a questi. Sia $f \in \text{Hom}(C_n, \mathbb{C}^*)$. Visto che $a^n = e$, deve valere $f(a)^n = f(a^n) = 1$. Allora $f(a)$ deve essere una radice n -esima dell'unità, che chiamiamo ω . A questo punto il fatto che f è omomorfismo implica che $f(a^k) = \omega^k$ per ogni intero k . \square

1.3 Gruppi abeliani

Definizione 1.18 (Gruppo abeliano). Un gruppo G si dice abeliano se l'operazione di gruppo è commutativa, cioè $\forall a, b \in G \quad ab = ba$.

Esercizio 1.8. Un gruppo ciclico è sempre abeliano.

Potrebbe essere utile (ma non è strettamente necessario ai fini di questo corso) conoscere il seguente risultato, la cui dimostrazione richiederebbe una conoscenza più approfondita della teoria dei gruppi.

Teorema 1.5. Ogni gruppo abeliano finito è isomorfo al prodotto diretto di gruppi ciclici.

Sia G un gruppo abeliano. Allora usando il fatto che G è isomorfo al prodotto diretto di alcuni gruppi ciclici e facendo un ragionamento simile a quello della proposizione analoga per gruppi ciclici si ottiene che

$$|G| = |\text{Hom}(G, \mathbb{C}^*)|$$

Se invece G non è abeliano allora nella formula precedente all'uguale va sostituito un $>$. Vedremo comunque come questi risultati seguono facilmente dalla teoria delle rappresentazioni che svilupperemo.

1.4 Gruppi simmetrici

Il gruppo simmetrico S_n è stato introdotto come l'insieme delle funzioni bigettive da $\{1, 2, \dots, n\}$ in sé, dotato dell'operazione di composizione. Dunque S_n agisce in modo naturale su $\{1, 2, \dots, n\}$, permutandone gli elementi. Per descrivere un elemento $\sigma \in S_n$ è spesso conveniente usare la notazione di prodotto di cicli disgiunti, che ora descriviamo informalmente.

Si comincia a costruire la lista $(1, \sigma(1), \sigma^2(1), \dots)$. Visto che abbiamo a disposizione un numero finito di elementi, ci si convince facilmente (ma non è neanche del tutto banale) che ad un certo punto sarà $\sigma^k(1) = 1$. Allora se scriviamo $(1, \sigma(1), \sigma^2(1), \dots, \sigma^{k-1}(1))$ tutti i numeri nella lista saranno diversi tra loro (questo segue dal fatto che σ è bigettiva). Inoltre ognuno dei numeri scritti viene mandato da σ nel numero immediatamente successivo nella lista, e l'ultimo numero viene mandato nel primo. Quello che abbiamo appena scritto è un *ciclo*. È anche possibile che la lista sia semplicemente (1) , il che vorrebbe dire che 1 viene lasciato fisso da σ . Se avessimo cominciato il procedimento con $\sigma(1)$ al posto di 1 avremmo ottenuto $(\sigma(1), \sigma^2(1), \dots, \sigma^{k-1}(1), 1)$, che descrive ugualmente bene il modo in cui σ sposta gli elementi scritti. Anche se la scrittura è diversa, per noi $(1, \sigma(1), \sigma^2(1), \dots, \sigma^{k-1}(1))$ e $(\sigma(1), \sigma^2(1), \dots, \sigma^{k-1}(1), 1)$ sono esattamente lo stesso ciclo, e un ragionamento analogo vale per gli altri numeri facenti parte della lista: non importa da quale si parte. Può darsi che non tutti i numeri da 1 a n compaiano nel ciclo appena scritto: in tal caso si prende un numero ancora non scritto e si ricomincia da capo da lui, creando un nuovo ciclo, e si continua così finché non sono stati scritti tutti i numeri. Alla fine ci ritroviamo con un elenco di cicli che sono necessariamente disgiunti per via della bigettività di σ . È facile convincersi che in questo modo si descrive completamente σ . Inoltre a meno di variare l'ordine con cui sono scritti i cicli e di cambiare i “punti di partenza” dei singoli cicli questa scrittura come cicli disgiunti è unica. Riassumiamo quanto detto nel seguente teorema:

Teorema 1.6. *Ogni elemento $\sigma \in S_n$ si scrive in modo unico come prodotto di cicli disgiunti a meno dell'ordine dei fattori e a meno di cambiare il modo in cui i singoli cicli sono presentati.*

Spesso nella scrittura in cicli disgiunti si tralasciano i cicli di lunghezza uno. Ad esempio $(3, 5, 7)(4, 1) \in S_{12}$ ha perfettamente senso: i numeri 1, 3, 4, 5, 7 vengono “spostati” da σ nel modo descritto e tutti gli altri vengono lasciati fissi.

I cicli, più che essere delle liste, vanno pensati come elementi di S_n , ovvero come funzioni bigettive da $\{1, \dots, n\}$ in sé. In quanto tali possono essere moltiplicati, nel senso di composizione delle funzioni. Ad esempio

$$(1, 2, 3) \cdot (3, 5)$$

chiaramente non è la scrittura come prodotto di cicli disgiunti di un elemento di S_n , in quanto appunto i due cicli scritti non sono disgiunti. Ma il loro prodotto ha perfettamente senso, e usando la stessa convenzione che si usa di solito per la composizione di funzioni vanno fatti “agire” da destra a sinistra. Ad esempio il prodotto scritto manda il numero 5 nel numero 1 (infatti il ciclo a destra manda 5 in 3, il quale viene mandato in 1 dal ciclo a sinistra). Se lo volessimo scrivere come prodotto di cicli disgiunti otterremmo:

$$(1, 2, 3, 5)$$

Teorema 1.7. *Ogni elemento $\sigma \in S_n$ si può scrivere come prodotto di trasposizioni, ovvero cicli di lunghezza 2, non necessariamente disgiunti.*

Dimostrazione. Considerato il teorema sulla decomposizione in cicli, basta mostrare la tesi nel caso in cui σ è un ciclo. Supponiamo $\sigma = (a_1, a_2, \dots, a_k)$. Allora è facile verificare che

$$\sigma = (a_1, a_k) \cdot (a_1, a_{k-1}) \cdots (a_1, a_2)$$

Qualcuno potrebbe essere turbato dal caso in cui il ciclo ha lunghezza 1, ossia σ è l'identità. In tal caso possiamo dire che σ è il prodotto di un insieme vuoto di trasposizioni. Chi fosse ancora turbato potrebbe scrivere, almeno nel caso $n \geq 2$, $\sigma = (1, 2)(1, 2)$. \square

Osserviamo che il teorema precedente assicura solo l'esistenza di una scrittura come prodotto di trasposizioni ma non l'unicità. In effetti questa non sussiste, infatti se in fondo ad un prodotto di trasposizioni si aggiunge $(1, 2)(1, 2)$ allora il risultato non cambia. Per avere un esempio leggermente più sofisticato:

$$(2, 1)(2, 3) = (1, 3)(1, 2)$$

Tuttavia quello che non cambia è la parità del numero di trasposizioni, come precisato dal seguente teorema.

Teorema 1.8. *Siano $\tau_1, \tau_2, \dots, \tau_t, \sigma_1, \sigma_2, \dots, \sigma_s$ trasposizioni in S_n . Supponiamo che*

$$\tau_1 \tau_2 \dots \tau_t = \sigma_1 \sigma_2 \dots \sigma_s$$

Allora $s \equiv t \pmod{2}$.

Cenno di dimostrazione. Definiamo la seguente funzione $f : S_n \rightarrow \mathbb{N}$:

$$f(\rho) = |\{ (a, b) \in \{1, \dots, n\}^2 \mid a < b, \rho(a) > \rho(b) \}|$$

Non è difficile verificare che se $\tau \in S_n$ è una trasposizione allora $f(\rho)$ e $f(\tau\rho)$ hanno parità diversa. Il risultato segue immediatamente visto che $f(\tau_1 \tau_2 \dots \tau_t) = f(\sigma_1 \sigma_2 \dots \sigma_s)$. \square

Definizione 1.19 (Segno di una permutazione). Il teorema appena visto permette di definire il *segno* di ogni elemento $\sigma \in S_n$, che si pone uguale a 1 se σ si scrive come prodotto di un numero pari di trasposizioni, si pone uguale a -1 altrimenti.

Proposizione 1.9. *Il segno di un ciclo di lunghezza k è esattamente $(-1)^{k-1}$*

Dimostrazione. Abbiamo già visto un modo in cui un ciclo di lunghezza k si può scrivere come prodotto di trasposizioni:

$$(a_1, a_2, \dots, a_k) = (a_1, a_k) \cdot (a_1, a_{k-1}) \cdot \dots \cdot (a_1, a_2)$$

Dunque la tesi segue immediatamente. \square

Definizione 1.20. L'insieme degli elementi di S_n aventi segno $+1$ è un sottogruppo di S_n , chiamato *gruppo alterno* e indicato con A_n .

1.5 Gruppi diedrali

Definizione 1.21 (Gruppo diedrale). Consideriamo in \mathbb{R}^2 un poligono regolare di n lati con centro nell'origine. L'insieme D_n delle isometrie di \mathbb{R}^2 che mandano il poligono in sé è un gruppo con l'operazione di composizione. Si verifica che questo gruppo ha $2n$ elementi, di cui n rotazioni (ovvero elementi di $O_2(\mathbb{R})$ con determinante 1) e n riflessioni (ovvero elementi di $O_2(\mathbb{R})$ con determinante -1). Inoltre, detta ρ una rotazione di $2\pi/n$ (che ha ordine n , e per inverso ha ρ^{n-1}) e σ una qualunque riflessione (che ha ordine 2), esse generano il gruppo D_n , che si può presentare nel seguente modo:

$$D_n = \langle \rho, \sigma \mid \rho^n = \sigma^2 = id, \sigma\rho\sigma = \rho^{-1} \rangle$$

Osservazione. Le n potenze distinte di ρ sono tutte e sole le rotazioni di D_n , mentre gli elementi della forma $\sigma\rho^i$, $i = 0, 1, \dots, n-1$ sono tutte e sole le riflessioni.

Osservazione. Si dimostra facilmente che la relazione $\sigma\rho\sigma = \rho^{-1}$ è verificata da qualsiasi rotazione ρ e qualsiasi riflessione σ .

2 Alcuni risultati di algebra lineare

In questa sezione diamo alcune definizioni e teoremi di algebra lineare che sono stati utilizzati nel corso o che sono utili per avere una visione d'insieme di certi argomenti. Non saranno presenti le dimostrazioni che possono essere trovate su molti libri di algebra lineare.

Definizione 2.1 (Spazio vettoriale duale). Se V è un \mathbb{K} -spazio vettoriale, indichiamo con V^* lo spazio duale dei funzionali lineari $f : V \rightarrow \mathbb{K}$.

Se V è finitamente generato con base $\{v_i\}_{i=1}^n$, allora V^* ammette come base $\{v_i^*\}_{i=1}^n$ (detta *base duale*), dove gli elementi $v_i^* \in V^*$ sono definiti da $v_i^*(v_j) = \delta_{i,j}$.

Teorema 2.1 (Diagonalizzazione simultanea). *Date due matrici $M, N \in \mathcal{M}_n(\mathbb{K})$, diremo che sono simultaneamente diagonalizzabili se esiste una base comune di autovettori per entrambe.*

Date $M, N \in \mathcal{M}_n(\mathbb{K})$, se esse commutano e sono entrambe diagonalizzabili allora sono simultaneamente diagonalizzabili.

Corollario. *Date $M_1, \dots, M_k \in \mathcal{M}_n(\mathbb{K})$, se $M_i M_j = M_j M_i \forall i, j$ e ogni M_i è diagonalizzabile, allora esiste una base comune di autovettori per tutte quante.*

Definizione 2.2 (Ideale di un endomorfismo). Se $p(x) = a_n x^n + \dots + a_0$, allora scriviamo $p(f)$ per intendere $a_n f^n + \dots + a_0 f^0$ dove $f^0 = \text{Id}$ e $f^k = \underbrace{f \circ \dots \circ f}_{k \text{ volte}}$.

Sia V un \mathbb{K} -spazio vettoriale, $f : V \rightarrow V$ un endomorfismo di V . Definiamo *ideale di f* l'insieme

$$I(f) = \{p(x) \in \mathbb{K}[x] \mid p(f) = 0\}$$

Teorema 2.2 (Teorema di decomposizione primaria). *Siano V un \mathbb{K} -spazio vettoriale, $f : V \rightarrow V$ un endomorfismo di V e $q(x) \in I(f)$. Sia $q = q_1 \cdot \dots \cdot q_k$ tale che $\text{MCD}(q_i, q_j) = 1 \forall i \neq j$, allora $V = \text{Ker}(q_1(f)) \oplus \dots \oplus \text{Ker}(q_k(f))$ e gli addendi sono f -invarianti.*

In particolare se f è triangolabile e $\lambda_1, \dots, \lambda_k$ sono gli autovalori di f con molteplicità algebrica rispettivamente $\alpha_1, \dots, \alpha_k$, allora $V = \text{Ker}((f - \lambda_1 \text{Id})^{\alpha_1}) \oplus \dots \oplus \text{Ker}((f - \lambda_k \text{Id})^{\alpha_k})$.

Teorema 2.3 (Forma canonica di Jordan). *Sia $M \in \mathcal{M}_n(\mathbb{K})$ una matrice triangolabile, siano $\lambda_1, \dots, \lambda_k$ i suoi autovalori, allora M è simile alla sua forma canonica di Jordan che è nella forma*

$$\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_t \end{pmatrix} \quad \text{dove } J_i = \begin{pmatrix} \lambda & 1 & & \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix} \quad \text{per qualche } \lambda \in \{\lambda_1, \dots, \lambda_k\}$$

La dimensione e il numero di blocchi di ciascun tipo sono univocamente determinati dalla matrice M , ne segue che la forma canonica di Jordan è unica a meno di permutazione dei blocchi e dunque, scelta una convenzione sull'ordine dei blocchi, essa è un sistema completo di invarianti per similitudine: due matrici sono simili se e solo se hanno la stessa forma di Jordan.

Definizione 2.3 (Forma hermitiana). Siano V, W due \mathbb{C} -spazi vettoriali, una funzione $h : V \times V \rightarrow \mathbb{C}$ si dice *forma hermitiana* se $\forall v, w, z \in V, \forall \alpha \in \mathbb{C}$ vale che

$$\begin{aligned} h(v, w) &= \overline{h(w, v)} \\ h(\alpha v, w) &= \alpha h(v, w) \\ h(v + z, w) &= h(v, w) + h(z, w) \end{aligned}$$

Definizione 2.4. Una forma hermitiana $\phi : V \times V \rightarrow \mathbb{C}$ è *definita positiva* (rispettivamente *negativa*) se $\forall v \in V, v \neq 0$ si ha che $\phi(v, v) > 0$ (rispettivamente $\phi(v, v) < 0$), osservare che $\phi(v, v) \in \mathbb{R} \forall v \in V$, dunque ha senso chiedere che sia maggiore o minore di 0.

Una forma hermitiana $\phi : V \times V \rightarrow \mathbb{C}$ è *semidefinita positiva* (rispettivamente *negativa*) se $\forall v \in V$ si ha che $\phi(v, v) \geq 0$ (rispettivamente $\phi(v, v) \leq 0$)

Teorema 2.4. Ogni forma hermitiana definita positiva su uno spazio vettoriale V di dimensione finita ammette una base ortonormale, ovvero esiste una base $\{v_1, \dots, v_n\}$ di V tale che $\phi(v_i, v_j) = \delta_{ij}$.

3 Algebra multilineare

3.1 Base di uno spazio vettoriale

Definizione 3.1 (Base di uno spazio vettoriale). Sia V un \mathbb{K} –spazio vettoriale e I un insieme; una base di V è una funzione $e : I \rightarrow V$ tale che per ogni $v \in V$ esiste un'unica funzione $a : I \rightarrow \mathbb{K}$ a supporto finito per cui vale $v = \sum_{i \in I} a_i e_i$. Questa definizione è compatibile con la definizione di base come insieme di vettori generatori linearmente indipendenti.

Spesso useremo una notazione del tipo $\{e_i\}_{i \in I}$ per indicare una base di uno spazio vettoriale V . Ciò sottintende una funzione $e : I \rightarrow V$ che manda $i \rightarrow e_i$, in accordo con la definizione che abbiamo appena dato.

Alcuni dei risultati a cui arriveremo sono validi anche per I infiniti, ma per semplicità consideriamo solo spazi vettoriali finitamente generati (per cui esiste una base $e : I \rightarrow V$ con I insieme finito).

Questo primo lemma dovrebbe essere noto a chiunque abbia un minimo di familiarità con l'algebra lineare:

Lemma 3.1. Siano V, W degli spazi vettoriali, sia $e : I \rightarrow V$ una base di V e $f : I \rightarrow W$ una funzione. Allora esiste un'unica $\phi : V \rightarrow W$ lineare tale che

$$\phi(e_i) = f_i$$

Inoltre ϕ è un isomorfismo se e solo se f è una base.

Lemma 3.2. Dato I insieme, esiste uno spazio vettoriale V con base una certa $e : I \rightarrow V$.

Dimostrazione. Definisco il seguente insieme, che è in modo naturale un \mathbb{K} –spazio vettoriale:

$$\mathbb{K}^I = \{v : I \rightarrow \mathbb{K} \mid v \text{ ha supporto finito}\}$$

Ora è facile osservare che $e : I \rightarrow \mathbb{K}^I$ definita da $e_i(j) = \delta_{i,j}$ è una base. □

3.2 Prodotto tensoriale

Definizione 3.2 (Prodotto tensoriale). Siano V, W due \mathbb{K} –spazi vettoriali. Si dice prodotto tensore di V e W , e si indica come $V \otimes W$, uno spazio vettoriale con una funzione bilineare $\otimes : V \times W \rightarrow V \otimes W$ tale che per ogni data funzione bilineare $h : V \times W \rightarrow Z$, esiste unica $\phi : V \otimes W \rightarrow Z$ lineare per cui $\phi(v \otimes w) = h(v, w)$. Ovvero questa ϕ fa commutare il diagramma:

$$\begin{array}{ccc} V \times W & \xrightarrow{\otimes} & V \otimes W \\ & \searrow h & \downarrow \phi \\ & & Z \end{array}$$

Questa proprietà viene detta proprietà universale del prodotto tensoriale e la funzione $\otimes : V \times W \rightarrow V \otimes W$ viene detta funzione universale.

Esempio 3.1. $V = W = V \otimes W = \mathbb{C}$ e come \otimes prendo il prodotto ovvero $v \otimes w = vw$.

Esempio 3.2. W un qualsiasi \mathbb{K} –spazio vettoriale, $V = \mathbb{K}$. Allora posso prendere $\mathbb{K} \otimes W = W$ e come \otimes prendo il prodotto per scalari $\alpha \otimes w = \alpha w$.

Infatti se $h : \mathbb{K} \times W \rightarrow Z$ è una funzione bilineare, allora mi basta definire $\phi : W \rightarrow Z$ ponendo $\phi(w) = h(1, w)$. Si vede facilmente che così il diagramma commuta e non esiste nessun'altra ϕ che fa commutare il diagramma.

Proposizione 3.3. *Se ho due prodotti tensoriali $V \otimes W$ e $V \overline{\otimes} W$, allora esiste un unico isomorfismo $\phi : V \otimes W \rightarrow V \overline{\otimes} W$ tale che, fissati comunque $v \in V, w \in W$, valga $\phi(v \otimes w) = v \overline{\otimes} w$.*

Dimostrazione. Considero i seguenti due diagrammi:

$$\begin{array}{ccc} V \times W & \xrightarrow{\otimes} & V \otimes W \\ & \searrow \overline{\otimes} & \downarrow \\ & & V \overline{\otimes} W \end{array} \quad \begin{array}{ccc} V \times W & \xrightarrow{\overline{\otimes}} & V \overline{\otimes} W \\ & \searrow \otimes & \downarrow \\ & & V \otimes W \end{array}$$

La proprietà universale per il prodotto tensore \otimes dice che $\exists! \phi : V \otimes W \rightarrow V \overline{\otimes} W$ lineare che fa commutare il primo diagramma: analogamente $\exists! \psi : V \overline{\otimes} W \rightarrow V \otimes W$ lineare che fa commutare il secondo diagramma. Ora consideriamo i seguenti due diagrammi:

$$\begin{array}{ccc} & V \otimes W & \\ \otimes \nearrow & \downarrow \phi & \\ V \times W & \xrightarrow{\overline{\otimes}} & V \overline{\otimes} W \\ \searrow \otimes & \downarrow \psi & \\ & V \otimes W & \end{array} \quad \begin{array}{ccc} & V \overline{\otimes} W & \\ \overline{\otimes} \nearrow & \downarrow \psi & \\ V \times W & \xrightarrow{\otimes} & V \otimes W \\ \searrow \overline{\otimes} & \downarrow \phi & \\ & V \overline{\otimes} W & \end{array}$$

Ma noi conosciamo già delle applicazioni lineari che fanno commutare i due diagrammi “più grandi”: le identità sui rispettivi spazi vettoriali. Quindi per unicità possiamo concludere che $\phi\psi = \text{Id}_{V \overline{\otimes} W}$, $\psi\phi = \text{Id}_{V \otimes W}$, ovvero ϕ e ψ sono una l'inversa dell'altra e in particolare ϕ è un isomorfismo. \square

Si può dimostrare inoltre che dati due spazi vettoriali V e W esiste sempre un loro prodotto tensoriale, dunque abbiamo il seguente risultato:

Teorema 3.4. *$V \otimes W$ esiste ed è unico a meno di isomorfismo.*

Nota. È importante notare che non tutti gli elementi $z \in V \otimes W$ si scrivono come $z = v \otimes w$. In particolare, per fare un esempio concreto che mostra che questa cosa non funziona, prendiamo $W = V^*$. Vedremo fra poco che $V \otimes V^*$ è canonicamente isomorfo allo spazio degli endomorfismi di V , i cui elementi si possono rappresentare con matrici $n \times n$. Tuttavia gli elementi del tipo $z = v \otimes w$ avranno matrice associata di rango minore o uguale a 1: è chiaro che questi elementi non bastano a “coprire” tutto lo spazio.

Proposizione 3.5. *L'insieme degli elementi di $V \otimes W$ della forma $v \otimes w$ con $v \in V, w \in W$ genera tutto lo spazio $V \otimes W$.*

Dimostrazione. Consideriamo il sottospazio generato dagli elementi della forma $v \otimes w$:

$$\langle \{v \otimes w : v \in V, w \in W\} \rangle = A$$

Vogliamo quindi dimostrare che $A = V \otimes W$. Consideriamo il diagramma:

$$\begin{array}{ccc} V \times W & \xrightarrow{\otimes} & V \otimes W \\ & \searrow h & \downarrow \\ & & A \end{array}$$

dove $h(v, w) = v \otimes w$ è ovviamente un'applicazione bilineare. Quindi $\exists! \psi : V \otimes W \rightarrow A$ che fa commutare il diagramma. Detta $i : A \rightarrow V \otimes W$ l'inclusione consideriamo il seguente diagramma:

$$\begin{array}{ccc} & V \otimes W & \\ \otimes \nearrow & \downarrow \psi & \\ V \times W & \xrightarrow{h} & A \\ \searrow i \circ h & \downarrow i & \\ & V \otimes W & \end{array}$$

tuttavia il diagramma grande commuta anche con $\text{Id}_{V \otimes W}$ e quindi $i \circ \psi = \text{Id}_{V \otimes W}$ dunque i è surgettiva e pertanto $A = V \otimes W$. \square

Definizione 3.3 (Prodotto tensoriale di mappe lineari). Date $f : V \rightarrow V'$ e $g : W \rightarrow W'$ funzioni lineari, si definisce prodotto tensoriale tra f e g l'unica funzione lineare $f \otimes g : V \otimes W \rightarrow V' \otimes W'$ tale che $(f \otimes g)(v \otimes w) = f(v) \otimes g(w) \forall v \in V, w \in W$.

Una funzione con tale proprietà esiste ed è unica poiché l'applicazione $V \times W \rightarrow V' \otimes W'$ che manda (v, w) in $f(v) \otimes g(w)$ è bilineare.

Osservazione. $\text{Id}_V \otimes \text{Id}_W = \text{Id}_{V \otimes W}$, poiché coincidono su un insieme di generatori.

Proposizione 3.6. Siano V e W \mathbb{K} -spazi vettoriali e sia $\{e_i\}_{i \in I}$ una base di V . Allora ogni elemento di $V \otimes W$ si scrive in modo unico come:

$$\sum_{i \in I} e_i \otimes w_i$$

con $w_i \in W$ tutti nulli tranne al più una quantità finita di essi.

Dimostrazione. Sia x un elemento di $V \otimes W$. Visto che gli elementi della forma $v \otimes w$ generano l'intero spazio $V \otimes W$, possiamo scrivere

$$x = \sum_{j=1}^N v_j \otimes w_j$$

scegliendo opportunamente $N \in \mathbb{N}$, $v_j \in V$, $w_j \in W$ per $j = 1 \dots N$. Visto che $\{e_i\}_{i \in I}$ è base di V :

$$x = \sum_{j=1}^N v_j \otimes w_j = \sum_{j=1}^N \left(\sum_{i \in I} a_{i,j} e_i \right) \otimes w_j = \sum_{i,j} a_{i,j} (e_i \otimes w_j) = \sum_{i \in I} e_i \otimes \tilde{w}_i$$

dove si è posto $\tilde{w}_i = \sum_j a_{i,j} w_j$. Quindi siamo riusciti ad ottenere una scrittura del tipo che volevamo. Resta da mostrare che questa scrittura è unica, ovvero che gli elementi \tilde{w}_i sono univocamente determinati.

Consideriamo la base $\{e_i^*\}_{i \in I}$ di V^* duale rispetto a $\{e_i\}_{i \in I}$. Fissato un $k \in I$ possiamo considerare l'applicazione lineare $e_k^* \otimes \text{Id}_W : V \otimes W \rightarrow \mathbb{K} \otimes W$. Valutandola in x otteniamo:

$$(e_k^* \otimes \text{Id}_W) \left(\sum_{i \in I} e_i \otimes \tilde{w}_i \right) = \sum_{i \in I} e_k^*(e_i) \otimes \tilde{w}_i = 1 \otimes \tilde{w}_k$$

Ma $\mathbb{K} \otimes W$ è isomorfo in modo naturale a W , e questo isomorfismo porta l'elemento $1 \otimes \tilde{w}_k$ in \tilde{w}_k . Quest'ultimo, pertanto, è univocamente determinato. \square

Proposizione 3.7. Se $\{e_i\}_{i \in I}$ è una base di V e $\{f_j\}_{j \in J}$ è una base di W allora $\{e_i \otimes f_j\}_{(i,j) \in I \times J}$ è una base di $V \otimes W$.

Dimostrazione. Dato $x \in V \otimes W$ sappiamo che si può scrivere in modo unico $x = \sum_{i \in I} e_i \otimes w_i$. Ora, per ogni $i \in I$, il vettore w_i si scrive in modo unico come $w_i = \sum_{j \in J} a_{i,j} f_j$. Da questo segue abbastanza facilmente che x si scrive in modo unico come $\sum_{i,j} a_{i,j} (e_i \otimes f_j)$. \square

Corollario. $\dim(V \otimes W) = \dim V \cdot \dim W$

Proposizione 3.8. Siano V e W spazi vettoriali. Allora $V^* \otimes W$ è isomorfo allo spazio vettoriale $\text{Hom}(V, W)$ delle applicazioni lineari da V a W .

Dimostrazione. Definiamo $\theta : V^* \times W \rightarrow \text{Hom}(V, W)$ come la funzione che manda la coppia $(f, w) \in V^* \times W$ nella funzione $h_{f,w}$ definita da: $h_{f,w}(v) = f(v)w$ per ogni $v \in V$. Non è difficile osservare che θ è bilineare, quindi induce una funzione lineare $\phi : V^* \otimes W \rightarrow \text{Hom}(V, W)$ tale che, dati comunque $f \in V^*, w \in W, v \in V$, soddisfa $\phi(f \otimes w)(v) = f(v)w$. Mostriamo che ϕ è un isomorfismo di spazi vettoriali.

Fissiamo $\{v_i\}_{i \in I}$ una base di V , $\{v_i^*\}_{i \in I}$ la base duale, $\{w_j\}_{j \in J}$ una base di W . Ora abbiamo

$$\phi(v_i^* \otimes w_j)(v_k) = \delta_{i,k} w_j$$

Ciò vuol dire che, se scriviamo la matrice dell'applicazione $\phi(v_i^* \otimes w_j) : V \rightarrow W$ secondo le basi date, questa presenta un 1 all'incrocio tra l' i -esima colonna e la j -esima riga, mentre è nulla altrove. Dunque ϕ manda la base $\{v_i^* \otimes w_j\}_{(i,j) \in I \times J}$ dello spazio $V^* \otimes W$ in una base dello spazio $\text{Hom}(V, W)$, quindi è un isomorfismo. \square

Osservazione. In particolare, ponendo $W = V$, otteniamo che $\text{End}(V)$ è isomorfo a $V^* \otimes V$.

Esiste un'applicazione in un certo senso “naturale” $t : V^* \otimes V \rightarrow \mathbb{K}$, dove \mathbb{K} è il campo degli scalari, definita da $t(f \otimes v) = f(v)$. Se indichiamo con ϕ l'isomorfismo $V^* \otimes V \rightarrow \text{End}(V)$ che abbiamo definito nel corso della precedente dimostrazione, otteniamo una funzione lineare $\text{tr} = t \circ \phi^{-1} : \text{End}(V) \rightarrow \mathbb{K}$. Non è difficile vedere che questa tr che abbiamo appena definito coincide con la classica funzione “traccia”. Il modo in cui l'abbiamo definita noi rende evidente il fatto che la traccia non dipende dalla base scelta per scrivere la matrice di un endomorfismo.

Teorema 3.9. Se $f : V \rightarrow V$ e $g : W \rightarrow W$ sono endomorfismi di spazi vettoriali, allora vale la formula $\text{tr}(f \otimes g) = \text{tr}(f) \text{tr}(g)$

Dimostrazione. Sia $\{v_i\}_{i \in I}$ una base di V , $\{w_j\}_{j \in J}$ una base di W , e come al solito indichiamo gli elementi delle basi duali aggiungendo un asterisco.

$$\begin{aligned} \text{tr}(f \otimes g) &= \sum_{(i,j) \in I \times J} (v_i^* \otimes w_j^*)(f \otimes g)(v_i \otimes w_j) = \\ &= \sum_{(i,j) \in I \times J} v_i^*(f(v_i)) \cdot w_j^*(g(w_j)) = \\ &= \left(\sum_{i \in I} v_i^*(f(v_i)) \right) \cdot \left(\sum_{j \in J} w_j^*(g(w_j)) \right) = \\ &= \text{tr}(f) \cdot \text{tr}(g) \end{aligned}$$

\square

Dimostrazione alternativa per \mathbb{C} -spazi vettoriali. Iniziamo a considerare il caso in cui sia f che g siano diagonalizzabili: prendendo due basi $a : I \rightarrow V$, $b : J \rightarrow W$ di autovettori rispettivamente per f e per g , si verifica facilmente la verità della proposizione nella base indotta su $V \otimes W$ (ovvero in quella formata dagli $a_i \otimes b_j$).

Ora, essendo la traccia una funzione continua e le matrici diagonalizzabili dense nello spazio delle matrici, la proprietà affermata dal lemma si estende al caso generale per continuità. \square

Esercizio 3.1. Se V, U, W sono spazi vettoriali sul campo \mathbb{K} dimostrare che esistono (unici) i seguenti isomorfismi:

1. $V \otimes U \cong U \otimes V$, in modo tale che i vettori $v \otimes u$ vengano mandati in $u \otimes v$;
2. $(V \otimes U) \otimes W \cong V \otimes (U \otimes W)$ con $(v \otimes u) \otimes w$ che viene mandato in $v \otimes (u \otimes w)$;
3. $(V \oplus U) \otimes W \cong (V \otimes W) \oplus (U \otimes W)$ con $(v, u) \otimes w$ che viene mandato in $(v \otimes w, u \otimes w)$.

In particolare il punto 2 ci dice che possiamo parlare senza ambiguità dello spazio $V \otimes U \otimes W$, senza bisogno di specificare le parentesi. In realtà potevamo definire questo spazio in modo diretto con una proprietà universale che fa corrispondere alle forme trilineari che partono da $U \times U \times W$ applicazioni lineari da $U \otimes U \otimes W$. Come esercizio è utile formulare per bene questa proprietà universale e dimostrare che $(V \otimes U) \otimes W$ la soddisfa. Allo stesso modo si possono trattare prodotti tensoriali di un numero arbitrario di spazi vettoriali.

Esercizio 3.2. Sia V uno spazio vettoriale. Allora $V^* \otimes V^*$ è isomorfo allo spazio vettoriale delle forme bilineari $V \times V \rightarrow \mathbb{K}$.

3.3 Prodotto esterno e prodotto simmetrico

In questa sezione supponiamo che il campo degli scalari di ogni spazio vettoriale sia \mathbb{C} , o comunque un campo a caratteristica 0.

Definizione 3.4 (Applicazione n -lineare simmetrica/alternante). Una applicazione $\phi : V^n \rightarrow Z$ si dice n -lineare se è lineare in ogni componente dopo aver fissato le altre $n - 1$.

Inoltre ϕ si dice simmetrica se $\phi(v_{s(1)}, \dots, v_{s(n)}) = \phi(v_1, \dots, v_n)$ per ogni permutazione $s \in S_n$, mentre si dice alternante se $\phi(v_{s(1)}, \dots, v_{s(n)}) = \text{sgn}(s)\phi(v_1, \dots, v_n)$ per ogni permutazione $s \in S_n$.

Esercizio 3.3. Un'applicazione n -lineare $h : V^n \rightarrow W$ è alternante se e solo se, presi comunque $v_1, \dots, v_n \in V$ non tutti distinti tra loro, si ha che $h(v_1, \dots, v_n) = 0$.

Esercizio 3.4. Sia $h : V^n \rightarrow W$ un'applicazione n -lineare alternante. Se i vettori v_1, \dots, v_n sono linearmente dipendenti allora $h(v_1, \dots, v_n) = 0$.

Definizione 3.5 (Prodotto esterno). Sia n un intero positivo, V uno spazio vettoriale. Un prodotto esterno è uno spazio vettoriale indicato con $\bigwedge^n V$ dotato di una funzione n -lineare alternante $\wedge : V^n \rightarrow \bigwedge^n V$ che manda le n -uple (v_1, \dots, v_n) in elementi di $\bigwedge^n V$ che indichiamo con $v_1 \wedge v_2 \wedge \dots \wedge v_n$, tale che presa comunque una funzione $h : V^n \rightarrow Z$ n -lineare alternante, esiste un'unica $\phi : \bigwedge^n V \rightarrow Z$ lineare per cui vale $\phi(v_1 \wedge v_2 \wedge \dots \wedge v_n) = h(v_1, \dots, v_n)$ per ogni n -upla di vettori di V .

Definizione 3.6 (Prodotto simmetrico). Sia n un intero positivo, V uno spazio vettoriale. Un prodotto simmetrico è uno spazio vettoriale indicato con $S^n V$ dotato di una funzione n -lineare simmetrica $V^n \rightarrow S^n V$ che manda (v_1, \dots, v_n) in $v_1 v_2 \dots v_n \in S^n V$, tale che presa comunque una funzione $h : V^n \rightarrow Z$ n -lineare simmetrica, esiste un'unica $\phi : S^n V \rightarrow Z$ lineare per cui vale $\phi(v_1 v_2 \dots v_n) = h(v_1, \dots, v_n)$.

Proposizione 3.10 (Proprietà dei prodotti esterni e simmetrici). *Sia V uno spazio vettoriale e n un numero naturale.*

- $\bigwedge^n V$ e $S^n V$ esistono.
- $\bigwedge^n V$ e $S^n V$ sono unici a meno di un unico isomorfismo.
- $\bigwedge^n V$ è generato dai vettori del tipo $v_1 \wedge \dots \wedge v_n$, e analogamente $S^n V$ è generato dai vettori del tipo $v_1 \dots v_n$.

Dimostrazione. Le dimostrazioni sono del tutto analoghe a quelle viste per il prodotto tensore, e vengono lasciate per esercizio. \square

Definizione 3.7 (Potenza simmetrica e potenza esterna di un'applicazione lineare). Sia $f : V \rightarrow V$ un endomorfismo di uno spazio vettoriale. Definiamo $\bigwedge^k f : \bigwedge^k V \rightarrow \bigwedge^k V$ la funzione che manda $v_1 \wedge \dots \wedge v_n$ in $f(v_1) \wedge \dots \wedge f(v_n)$.

In modo analogo si definisce la potenza simmetrica (verificare, tramite le proprietà universali, che queste definizioni hanno senso).

È facile osservare che se V è uno spazio vettoriale allora $\bigwedge^k \text{Id}_V = \text{Id}_{\bigwedge^k V}$, e che date due applicazioni lineari $f : V \rightarrow W$ e $g : W \rightarrow Z$ si ha che $\bigwedge^k (g \circ f) = \bigwedge^k g \circ \bigwedge^k f$. Chiaramente valgono osservazioni analoghe per i prodotti simmetrici.

Teorema 3.11 (Base del prodotto esterno). *Sia V uno spazio vettoriale di dimensione n , $\{e_i\}_{i=1}^n$ una base di V e k un intero positivo. Allora l'insieme*

$$E = \{e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_k} \mid 1 \leq i_1 < i_2 < \dots < i_k \leq n\}$$

è una base di $\bigwedge^k V$ di cardinalità $|E| = \binom{n}{k}$.

Dimostrazione. È facile osservare che l'insieme E genera lo spazio $\bigwedge^k V$. Mostriamo ora che gli elementi di E sono indipendenti. Fissiamo degli indici $1 \leq i_1 < i_2 < \dots < i_k \leq n$. Per prima cosa osserviamo che la funzione $h : V^k \rightarrow \mathbb{C}$ definita da

$$h(v_1, \dots, v_k) = e_{i_1}^*(v_1) \dots e_{i_k}^*(v_k)$$

è k -lineare. Vorremmo in qualche modo renderla alternante, e per farlo usiamo lo stratagemma seguente. Presa una qualsiasi permutazione $s \in S_k$ abbiamo che $h_s(v_1, \dots, v_k) = \text{sgn}(s)h(v_{s(1)}, \dots, v_{s(k)})$ è una funzione k -lineare. Consideriamo la somma

$$H(v_1, \dots, v_k) = \sum_{s \in S_k} h_s(v_1, \dots, v_k)$$

Non è difficile convincersi che H è alternante. Inoltre, se prendiamo $1 \leq j_1 < j_2 < \dots < j_k \leq n$ vale la seguente proprietà:

$$H(e_{j_1}, \dots, e_{j_k}) = \begin{cases} 1 & \text{se } (j_1, \dots, j_k) = (i_1, \dots, i_k) \\ 0 & \text{altrimenti} \end{cases}$$

Con la proprietà universale del prodotto alternante troviamo un funzionale che vale 1 su $e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_k}$ e 0 su gli altri elementi di E . Questo dimostra che gli elementi di E sono indipendenti. \square

Osserviamo a questo punto che se V è uno spazio vettoriale con base $\{e_i\}_{i=1}^n$, allora $\bigwedge^k V = 0$ se $k > n$, mentre $\bigwedge^n V \neq 0$. Questo fatto può essere usato come dimostrazione dell'invarianza della cardinalità di una base per uno spazio vettoriale.

La potenza esterna permette di dare una definizione di determinante di un endomorfismo in un certo senso più intrinseca di quella che si vede di solito nei corsi di algebra lineare. Supponiamo infatti di avere un endomorfismo $f : V \rightarrow V$. Se V ha dimensione 1 allora f non è altro che la moltiplicazione per uno scalare, che chiamiamo $\det f$. Se invece V ha dimensione n , sappiamo che $\dim \bigwedge^n V = 1$, quindi poniamo $\det f = \det(\bigwedge^n f)$. Come si vede, questa definizione non dipende da nessuna base fissata per lo spazio V . Con la definizione tramite potenza esterna risulta immediata la formula di Binet $\det(f \circ g) = \det f \cdot \det g$, in quanto sappiamo che $\bigwedge^n(f \circ g) = \bigwedge^n f \circ \bigwedge^n g$.

Esercizio 3.5. $v_1 \wedge \cdots \wedge v_k \neq 0$ se e solo se v_1, \dots, v_k sono linearmente indipendenti. Dedurre che per un endomorfismo $f : V \rightarrow V$ si ha che $\det f \neq 0$ se e solo se f è isomorfismo.

Esercizio 3.6. Dimostrare l'equivalenza tra la classica definizione di determinante e la definizione tramite potenza esterna.

Lemma 3.12. Sia $f : V \rightarrow W$ un'applicazione lineare e k un intero positivo. Allora:

1. se f è surgettiva allora $\bigwedge^k f : \bigwedge^k V \rightarrow \bigwedge^k W$ è surgettiva;
2. se f è iniettiva allora $\bigwedge^k f : \bigwedge^k V \rightarrow \bigwedge^k W$ è iniettiva.

Dimostrazione. Dimostriamo separatamente i due punti.

1. Sia $w_1 \wedge \cdots \wedge w_k \in \bigwedge^k W$ e supponiamo $f(v_i) = w_i$ (tali v_i esistono per surgettività di f). Allora $\bigwedge^k f(v_1 \wedge \cdots \wedge v_k) = w_1 \wedge \cdots \wedge w_k$. Visto che l'immagine contiene un insieme di generatori, allora $\bigwedge^k f$ è surgettiva.
2. Sia $\{e_i\}_{i=1}^n$ base di V . Allora $f(e_1), \dots, f(e_n)$ sono indipendenti in W e dunque si possono completare ad una base di W . Ora si vede chiaramente che la base di $\bigwedge^k V$ introdotta nel teorema 3.11 viene mandata iniettivamente in una parte della base di $\bigwedge^k W$.

□

Proposizione 3.13. Sia $f : V \rightarrow W$ lineare e consideriamo una sua potenza esterna $\bigwedge^k f$. Allora $\bigwedge^k f = 0$ se e solo se $k > \text{rango}(f)$.

Dimostrazione. Sia $Z \subseteq W$ l'immagine di f . Allora posso scrivere $f = h \circ g$, dove $g : V \rightarrow Z$ è surgettiva (non è altro che f , con codominio ristretto) e $h : Z \rightarrow W$ è l'inclusione (quindi iniettiva). Passando alle potenze esterne abbiamo $\bigwedge^k f = \bigwedge^k h \circ \bigwedge^k g$ e per il lemma precedente $\bigwedge^k g$ è surgettiva mentre $\bigwedge^k h$ è iniettiva. Dunque $\bigwedge^k f = 0$ se e solo se $\bigwedge^k Z = 0$ da cui si conclude. □

Teorema 3.14 (Base del prodotto simmetrico). Sia V uno spazio vettoriale di dimensione n , $\{e_i\}_{i=1}^n$ una base di V e k un intero positivo. Allora l'insieme

$$E = \{e_{i_1} e_{i_2} \cdots e_{i_k} \mid 1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n\}$$

è una base di $S^k V$ di cardinalità $|E| = \binom{n+k-1}{k}$.

Dimostrazione. È simile a quella per il prodotto esterno, quindi viene lasciata per esercizio. □

Sia V uno spazio vettoriale di dimensione n . Allora sappiamo che:

- $\dim V \otimes V = n^2$

- $\dim S^2V = \frac{n(n+1)}{2}$
- $\dim \bigwedge^2 V = \frac{n(n-1)}{2}$

Possiamo definire in modo abbastanza naturale un'applicazione lineare $V \otimes V \rightarrow \bigwedge^2 V \oplus S^2V$, mandando il vettore $v \otimes w$ nella coppia $(v \wedge w, vw)$. In effetti questa applicazione è un isomorfismo.

Dimostrazione. Per uguaglianza delle dimensioni degli spazi di partenza e di arrivo, basta dimostrare che è surgettiva. Per ogni coppia $v \in V$, $w \in W$ abbiamo che:

$$\begin{aligned}\frac{v \otimes w + w \otimes v}{2} &\rightarrow (0, vw) \\ \frac{v \otimes w - w \otimes v}{2} &\rightarrow (v \wedge w, 0)\end{aligned}$$

Quindi $\bigwedge^2 V$ e S^2V sono contenuti nell'immagine. Ma da questo segue subito la tesi. \square

Esercizio 3.7. Sia V un \mathbb{C} -spazio vettoriale. Allora S^2V^* è isomorfo allo spazio vettoriale delle forme bilineari simmetriche $V \times V \rightarrow \mathbb{C}$.

Esercizio 3.8. Sia V un \mathbb{C} -spazio vettoriale. Allora $\bigwedge^2 V^*$ è isomorfo allo spazio vettoriale delle forme bilineari antisimmetriche $V \times V \rightarrow \mathbb{C}$.

Proposizione 3.15. Sia $f : V \rightarrow V$ un endomorfismo di uno spazio vettoriale. Allora vale

$$\begin{cases} \text{tr}(\bigwedge^2 f) = \frac{(\text{tr}(f))^2 - \text{tr}(f^2)}{2} \\ \text{tr}(S^2 f) = \frac{(\text{tr}(f))^2 + \text{tr}(f^2)}{2} \end{cases}$$

Dimostrazione. Sia $\{e_1, \dots, e_n\}$ una base di V , allora $\exists a_{ij} : f(e_j) = \sum_i a_{ij} e_i$. Se $i < j$

$$\begin{aligned}\bigwedge^2 f(e_i \wedge e_j) &= f(e_i) \wedge f(e_j) = \left(\sum_k a_{ki} e_k \right) \wedge \left(\sum_l a_{lj} e_l \right) = \\ &= \sum_{k,l} a_{ki} a_{lj} (e_k \wedge e_l) = \sum_{k < l} (a_{ki} a_{lj} - a_{li} a_{kj}) (e_k \wedge e_l) \\ \Rightarrow \text{tr}(\bigwedge^2 f) &= \sum_{i < j} (a_{ii} a_{jj} - a_{ij} a_{ji}) = \frac{1}{2} \sum_{i,j} (a_{ii} a_{jj} - a_{ij} a_{ji}) = \frac{(\text{tr}(f))^2 - \text{tr}(f^2)}{2}\end{aligned}$$

Per $S^2 f$ si dimostra in maniera analoga. \square

4 Prime proprietà delle rappresentazioni

4.1 Definizione e primi esempi

Definizione 4.1 (Rappresentazione). Sia G un gruppo e V uno spazio vettoriale. Una funzione $\rho : G \rightarrow GL(V)$ che manda ciascun elemento del gruppo in un'applicazione lineare invertibile di V si dice rappresentazione di G se è un omomorfismo di gruppi. Quindi deve valere

$$\rho(st)v = \rho(s)\rho(t)v \quad \forall v \in V, \quad \forall s, t \in G$$

La dimensione di V (che supporremo sempre finita) viene detta grado della rappresentazione. Per il momento consideriamo solo rappresentazioni su spazi vettoriali complessi, ovvero supponiamo che V sia \mathbb{C} -spazio vettoriale.

Con un piccolo abuso di linguaggio, spesso indicheremo con il nome di “rappresentazione” direttamente V , se è chiaro quale sia la rappresentazione ρ che stiamo considerando. Spesso indicheremo gli spazi vettoriali su cui è definita una rappresentazione ρ con nomi del tipo V_ρ , dove il pedice ci ricorda la rappresentazione che stiamo considerando.

Detto in altri termini, una rappresentazione di un gruppo G è un'azione lineare di G su uno spazio vettoriale V . Se non c'è ambiguità (cioè se è chiaro quale rappresentazione stiamo considerando) possiamo scrivere semplicemente $g \cdot v$ in luogo di $\rho(g)v$ per alleggerire la notazione. In pratica stiamo “interpretando” gli elementi di G come endomorfismi di uno spazio vettoriale.

Osservazione. $\rho(G)$ è evidentemente un sottogruppo di $GL(V)$, quindi esistono sempre inversi, potenze e valgono tutte le cose che sono vere per i gruppi.

Esempio 4.1. La rappresentazione banale, di grado qualsiasi, che manda qualsiasi elemento di g nell'identità di $GL(V)$, ovvero

$$\rho(s) = \text{Id}_{V_{\rho_1}} \quad \forall s \in G$$

Esempio 4.2. Dato S_n , il segno di un elemento $s \in S_n$ è una rappresentazione di grado 1. Infatti si ha $\text{sgn}(st) = \text{sgn}(s)\text{sgn}(t)$.

Esempio 4.3. L'azione naturale di S_n sui vettori della base. Prendiamo quindi $G = S_n$ e uno spazio vettoriale di dimensione n , che quindi è isomorfo a \mathbb{C}^n . Prendiamo la base canonica di \mathbb{C}^n e la indichiamo con $\{e_i\}_{i=1}^n$. Descriviamo la rappresentazione $\rho : S_n \rightarrow GL(\mathbb{C}^n)$ dicendo cosa fa agli elementi della base: per linearità si estenderà a tutto lo spazio.

$$\rho(s)e_i = e_{s(i)}$$

Notare che in questo caso $\deg(\rho) = n$. Notiamo inoltre che se rappresentiamo nella base canonica le matrici associate a $\rho(s)$ queste matrici sono unitarie. Inoltre, ogni colonna (e anche ogni riga) contiene esattamente un 1 e tutti gli altri sono 0.

Prendiamo come esempio S_3 che agisce su \mathbb{C}^3 e vediamo cosa succede. Una prima cosa a cui siamo interessati è capire se per caso ci sono dei sottospazi di \mathbb{C}^3 che sono invarianti rispetto all'azione del gruppo. La risposta in questo caso è semplice: c'è il sottospazio di dimensione 1 generato da $(1, 1, 1)$ che viene lasciato “indisturbato” dall'azione di S_3 , perché il gruppo non fa altro che scambiare le coordinate degli elementi, che però sono tutte uguali e quindi non cambia nulla. Riusciamo per caso a scrivere $\mathbb{C}^3 = \langle (1, 1, 1) \rangle \oplus W$ in modo che anche W sia invariante? La risposta è sì: basta considerare il sottospazio di dimensione 2 dei vettori la cui somma delle coordinate è nulla: è chiaro che la somma rimane 0 anche dopo aver permutato le coordinate a causa dell'azione di qualche permutazione di S_3 . In questo modo abbiamo “scomposto” la nostra rappresentazione di grado 3 in due rappresentazioni di grado 1 e 2 rispettivamente. In pratica

abbiamo “diagonalizzato a blocchi” gli endomorfismi dati dagli elementi di S_3 . Osserviamo che non si può ottenere una scomposizione più fine di quella che abbiamo appena trovato, perché questo corrisponderebbe a diagonalizzare simultaneamente tutti gli endomorfismi dati dagli elementi di S_3 : ciò non è possibile perché tali endomorfismi non commutano tutti tra di loro (invece matrici diagonali commutano).

Proposizione 4.1. *Sia G un gruppo finito e $\rho : G \rightarrow GL(V_\rho)$ una sua rappresentazione. Allora $\forall g \in G$ la matrice $\rho(g)$ ammette una base di autovettori in V_ρ , ovvero è diagonalizzabile. Inoltre, tutti gli autovalori di $\rho(g)$ sono radici n -esime dell’unità.*

Nota. Per ogni matrice in generale la base è diversa, quindi le varie matrici in generale *non* sono simultaneamente diagonalizzabili. Però se G è abeliano tutte le matrici $\rho(s)$ sono simultaneamente diagonalizzabili.

Dimostrazione. Se G è un gruppo finito, allora se $g \in G$ esiste un intero positivo k tale che $g^k = e$. Dato che $\rho : G \rightarrow GL(V_\rho)$ è un omomorfismo, dovrà essere $\rho(g)^k = \text{Id}$.

Visto che il polinomio minimo di $\rho(g)$ non ha radici multiple, con il teorema di decomposizione primaria (2.2) si mostra facilmente che $\rho(g)$ è diagonalizzabile. Inoltre da questa formula è anche evidente che tutti gli autovalori di $\rho(g)$ hanno modulo 1 e in particolare saranno radici k -esime dell’unità.

Ricordiamo un teorema di algebra lineare per mostrare che se G è abeliano allora tutte le matrici $\rho(g)$ sono simultaneamente diagonalizzabili: degli endomorfismi di uno spazio vettoriale diagonalizzabili sono simultaneamente diagonalizzabili se e solo se commutano tra loro. \square

Definizione 4.2 (Omomorfismo di rappresentazioni). Siano ρ e σ due rappresentazioni di G su V_ρ e V_σ rispettivamente. Un omomorfismo di spazi vettoriali $\varphi : V_\rho \rightarrow V_\sigma$ si dice *omomorfismo di rappresentazioni* se

$$\forall a \in G, \forall v \in V_\rho \quad \varphi(\rho(a)(v)) = \sigma(a)(\varphi(v))$$

oppure equivalentemente

$$\forall a \in G \quad \varphi \circ \rho(a) = \sigma(a) \circ \varphi$$

Ovvero se si fa prima agire un elemento del gruppo e poi si applica φ si ottiene la stessa cosa che si sarebbe ottenuta applicando prima φ e poi facendo agire lo stesso elemento del gruppo.

Indicheremo l’insieme degli omomorfismi tra due rappresentazioni di un gruppo G con $\text{Hom}_G(V_\rho, V_\sigma)$ oppure con $\text{Hom}(\rho, \sigma)$.

Definizione 4.3 (Rappresentazioni isomorfe). Due rappresentazioni si dicono *isomorfe* se esiste un omomorfismo di rappresentazioni tra di loro che è anche bigettivo.

Dato un gruppo G , le sue rappresentazioni di grado 1 sono per definizione omomorfismi che vanno da G all’insieme degli isomorfismi di \mathbb{C} -spazi vettoriali di dimensione 1. Senza perdere di generalità possiamo supporre che lo spazio vettoriale sia proprio \mathbb{C} . Dunque le rappresentazioni di grado 1 non sono altro che omomorfismi $G \rightarrow \mathbb{C}^*$.

Teorema 4.2. *Gli omomorfismi $G \rightarrow \mathbb{C}^*$ sono rappresentazioni di G tra loro non isomorfe.*

Dimostrazione. Siano $\rho : G \rightarrow \mathbb{C}^*$ e $\sigma : G \rightarrow \mathbb{C}^*$ rappresentazioni isomorfe. Allora esiste $\varphi : \mathbb{C} \rightarrow \mathbb{C}$ isomorfismo di \mathbb{C} (ovvero $\varphi \in \mathbb{C}^*$) tale che per ogni $g \in G$ vale $\varphi\rho(g) = \sigma(g)\varphi$. Visto che \mathbb{C}^* è commutativo abbiamo allora che $\rho(g) = \sigma(g)$ per ogni $g \in G$, il che vuol dire che in realtà ρ e σ sono proprio la stessa rappresentazione. \square

Nel tentativo di trovare le possibili rappresentazioni di un gruppo G (che qui supporremo finito), un buon punto di partenza è cercare per prima cosa le rappresentazioni di grado 1. Per fare questo c'è un metodo generale (indicheremo con ρ la rappresentazione cercata e con μ_m il sottoinsieme di \mathbb{C} che contiene le radici m -esime dell'unità):²

1. cercare dei generatori per il gruppo G : g_1, \dots, g_k
2. per ogni generatore g_i trovare il suo ordine n_i (ovvero il minimo intero n_i tale che $g_i^{n_i} = e$)
3. imporre che $\rho(g_i) \in \mu_{n_i}$ per ogni $i = 1, \dots, k$
4. imporre infine che $\rho : G \rightarrow GL(\mathbb{C})$ sia veramente un omomorfismo di gruppi (per ora abbiamo solo posto delle condizioni necessarie): per fare ciò bisogna controllare che le *relazioni* che intercorrono tra i generatori siano rispettate nell'immagine.³ In effetti già le condizioni imposte al punto 3 possono essere considerate come relazioni imposte dai generatori.

Questo definisce un omomorfismo da G a \mathbb{C}^* : dato $h \in G$ tale che $h = g_{i_1}^{a_1} \dots g_{i_t}^{a_t}$, allora $\rho(h) = \rho(g_{i_1})^{a_1} \dots \rho(g_{i_t})^{a_t}$.

Osservazione. Non è detto che tutte le rappresentazioni che si ottengono siano non isomorfe, questo metodo solamente le produce tutte.

Esempio 4.4 (Rappresentazioni di grado 1 di C_n). Dato $G = C_n$, prendiamo un suo generatore g (un qualsiasi elemento di ordine n), imponiamo che $\rho(g) \in \mu_n$ (ovvero $\rho(g) = e^{2k\pi i/n}$ per qualche $k \in \{0, \dots, n-1\}$). Visto che per ogni $h \in G$ esiste un $k \in \mathbb{N}$ tale che $h = g^k$, ho già definito ρ su ogni elemento di G . Ora abbiamo definito tutte le rappresentazioni di C_n di grado 1, ma sono tutte distinte? In effetti mostriamo che in questo caso il processo che abbiamo operato ha prodotto tutte rappresentazioni non isomorfe. Supponiamo di avere due rappresentazioni ρ_1, ρ_2 trovate con il metodo descritto sopra e supponiamo inoltre di avere $\varphi : \rho_1 \rightarrow \rho_2$ un isomorfismo di rappresentazioni. Allora deve valere che $\forall x \in \mathbb{C}, \forall g \in G \varphi(\rho_1(g)x) = \rho_2(g)\varphi(x)$, ma $\rho_1(g)$ è la moltiplicazione per uno scalare e φ è lineare, quindi vorrebbe dire che $\rho_1(g)\varphi(x) = \rho_2(g)\varphi(x)$. Preso $x \neq 0$ si ottiene che $\rho_1(g) = \rho_2(g)$ per ogni $g \in G$.

Questo esempio era particolarmente semplice quindi non abbiamo dovuto faticare troppo, però il procedimento descritto è abbastanza laborioso con gruppi più complicati: vediamo un altro metodo che permette di trovare alcune rappresentazioni di grado 1 a patto di conoscere un quoziente ciclico di G e le sue rappresentazioni di grado 1.

Sia G un gruppo, H un suo sottogruppo normale tale che G/H sia ciclico. Allora trovando le rappresentazioni di G/H di grado 1 siamo capaci di ricostruire delle rappresentazioni di grado 1 di G : consideriamo $\pi : G \rightarrow G/H$ la proiezione al quoziente, ovvero $\pi(g) = gH$, e un omomorfismo di gruppi $\rho : G/H \rightarrow \mathbb{C}^*$ (la rappresentazione di G/H), allora come omomorfismo $\sigma : G \rightarrow GL(\mathbb{C})$ (ovvero una rappresentazione di G) prendiamo l'omomorfismo che fa commutare il seguente diagramma:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ & \searrow \sigma & \downarrow \rho \\ & & GL(\mathbb{C}) \end{array}$$

²stiamo cercando un omomorfismo di gruppi da G a $GL(\mathbb{C}) = \mathbb{C}^*$.

³questo in parole povere significa che tutte le regole con cui vengono moltiplicati gli elementi devono essere rispettate, per dare una spiegazione formale servirebbero i prodotti liberi che però non sono necessari per questo corso.

ovvero $\sigma(g) = \rho(\pi(g))$.

Questo metodo è particolarmente potente perché, per ogni rappresentazione $\sigma : G \rightarrow GL(\mathbb{C})$, l'immagine è un gruppo ciclico⁴, quindi, in virtù del primo teorema di omomorfismo(1.3), l'immagine di una qualsiasi rappresentazione σ di grado 1 è un quoziente ciclico di G . Questo implica che in realtà il metodo esposto è in grado di trovare *tutte* le rappresentazioni di G di grado 1 (a patto di esaminare tutti i quozienti ciclici le loro rappresentazioni di grado 1).

Osservazione. È possibile generalizzare il procedimento descritto. Sia G un gruppo, $H \trianglelefteq G$ tale che conosciamo alcune rappresentazioni di G/H , allora riusciamo a ricostruire delle rappresentazioni di G allo stesso modo: sia $\rho : G/H \rightarrow GL(V)$ rappresentazione di G/H , $\pi : G \rightarrow G/H$ la proiezione al quoziente, si considera lo stesso omomorfismo σ di prima: $\sigma(g) = \rho(\pi(g))$.

Esempio 4.5 (Rappresentazioni di grado 1 di S_3). Conosciamo già due rappresentazioni di S_3 di grado 1 (ovvero omomorfismi $G \rightarrow \mathbb{C}^*$): quella banale, in cui ogni elemento viene mandato in 1, e la rappresentazione segno, che in questo caso manda le trasposizioni in -1 e gli altri elementi in 1. Mostriamo che non ce ne sono delle altre. Sia $\rho : S_3 \rightarrow \mathbb{C}^*$ omomorfismo di gruppi.

$$\rho((1, 2, 3))^{-1} = \rho((1, 3, 2)) = \rho((1, 2))\rho((1, 3)) = \rho((1, 3))\rho((1, 2)) = \rho((1, 2, 3))$$

Quindi $\rho((1, 2, 3))$ vale 1 oppure -1 . Però $(1, 2, 3)^3 = (1)$, quindi necessariamente $\rho((1, 2, 3)) = 1$. Visto che $\rho((1, 2))^2 = \rho((1)) = 1$, deve essere $\rho((1, 2)) = \pm 1$. Distinguendo i due casi si conclude che ρ è la rappresentazione banale oppure è la rappresentazione segno.

4.2 Operazioni con le rappresentazioni

Definizione 4.4 (Somma di rappresentazioni). Date due diverse rappresentazioni dello stesso gruppo G , $\rho : G \rightarrow GL(V)$, $\sigma : G \rightarrow GL(W)$ si può definire la rappresentazione somma $\rho + \sigma$ sullo spazio vettoriale $V \oplus W$ nel modo ovvio

$$(\rho + \sigma)_g(v, w) = \rho_g(v) + \sigma_g(w) \quad \forall (v, w) \in V \oplus W$$

Matricialmente $(\rho + \sigma)_g$ si rappresenta come

$$[(\rho + \sigma)_g] = \begin{bmatrix} [\rho_g] & 0 \\ 0 & [\sigma_g] \end{bmatrix}$$

Osservazione. Abbiamo le seguenti proprietà della somma di rappresentazioni:

1. $\deg(\rho + \sigma) = \deg(\rho) + \deg(\sigma)$
2. $\rho + \sigma \cong \sigma + \rho$
3. $\rho + (\sigma + \tau) \cong (\rho + \sigma) + \tau$
4. Esiste l'elemento neutro che è la rappresentazione di grado 0 ma non esiste l'inverso.

Definizione 4.5 (Prodotto di rappresentazioni). Date due rappresentazioni dello stesso gruppo G , $\rho : G \rightarrow GL(V_\rho)$, $\sigma : G \rightarrow GL(V_\sigma)$ possiamo definire il prodotto di rappresentazioni che si indica con $\rho \otimes \sigma$ ma anche con $\rho\sigma$ ⁵ definito sullo spazio $V_\rho \otimes V_\sigma$ tale che

$$\rho \otimes \sigma(g)(v \otimes w) = \rho(g)v \otimes \sigma(g)w \quad \forall v \in V_\rho, w \in V_\sigma$$

⁴È abbastanza facile convincersene ricordando che ogni elemento di G deve essere mandato in una radice dell'unità.

⁵Quest'ultima notazione può portare a confusione in quanto può essere scambiata con la composizione se le due rappresentazioni sono definite sullo stesso spazio, quindi cercheremo di evitarla.

Il seguente esercizio è molto importante e dovrebbe essere svolto con calma, prestando attenzione al fatto che si devono esibire degli isomorfismi di rappresentazioni, non semplicemente degli isomorfismi di spazi vettoriali.

Esercizio 4.1. Abbiamo le seguenti proprietà del prodotto di rappresentazioni:

1. $\deg(\rho \otimes \sigma) = \deg \rho \cdot \deg \sigma$
2. $1 \otimes \rho \cong \rho$
3. $\rho \otimes \sigma \cong \sigma \otimes \rho$
4. $0 \otimes \rho \cong 0$
5. $\rho \otimes (\sigma \otimes \tau) \cong (\rho \otimes \sigma) \otimes \tau$
6. $\rho \otimes (\sigma_1 + \sigma_2) \cong \rho \otimes \sigma_1 + \rho \otimes \sigma_2$

Definizione 4.6 (Rappresentazione duale). Sia ρ una rappresentazione di G su V_ρ . Allora la rappresentazione duale ρ^* è la rappresentazione di G su V_ρ^* definita da:

$$\rho^*(s)f = f \circ \rho(s^{-1})$$

La verifica che si tratti effettivamente di una rappresentazione è molto semplice e viene lasciata per esercizio.

Definizione 4.7 (Definizione equivalente di duale). Sia ρ una rappresentazione di G su V . Definiamo la rappresentazione duale ρ^* come l'unica rappresentazione tale che

$$\rho_g^*(f)(\rho_g(v)) = f(v) \quad \forall g \in G, \forall v \in V, \forall f \in V^*$$

Nota. Se la matrice di $\rho(s)$ rispetto ad una fissata base di V è una certa $A \in \mathcal{M}_n(\mathbb{C})$, allora la matrice di $\rho^*(s)$ rispetto alla base duale è $(A^t)^{-1}$.

Proposizione 4.3. $(\rho + \sigma)^* \cong \rho^* + \sigma^*$

Dimostrazione. Consideriamo la funzione $\Theta : (V_\rho \oplus V_\sigma)^* \rightarrow V_\rho^* \oplus V_\sigma^*$ definita da

$$\Theta(f) = (f \circ \iota_{V_\rho}, f \circ \iota_{V_\sigma})$$

per ogni funzionale $f \in (V_\rho \oplus V_\sigma)^*$, dove ι_{V_ρ} e ι_{V_σ} sono le immersioni di V_ρ e V_σ dentro la loro somma diretta. È facile osservare che si tratta di un'applicazione lineare. Consideriamo anche la funzione $\Xi : V_\rho^* \oplus V_\sigma^* \rightarrow (V_\rho \oplus V_\sigma)^*$ definita da

$$\Xi(h, k) = h \circ \pi_{V_\rho} + k \circ \pi_{V_\sigma}$$

per ogni coppia di funzionali $h \in V_\rho^*$, $k \in V_\sigma^*$, dove π_{V_ρ} e π_{V_σ} indicano come al solito le proiezioni sui sottospazi. Anche Ξ è lineare, inoltre è facile osservare che Θ e Ξ sono una l'inversa dell'altra. Dunque sono degli isomorfismi. Resta da mostrare che Θ è omomorfismo di rappresentazioni. Prendiamo $g \in G$: dobbiamo mostrare che

$$(\rho^* + \sigma^*)(g) \circ \Theta = \Theta \circ (\rho + \sigma)^*(g)$$

ovvero che per ogni funzionale $f \in (V_\rho \oplus V_\sigma)^*$ vale

$$[(\rho^* + \sigma^*)(g)](f \circ \iota_{V_\rho}, f \circ \iota_{V_\sigma}) = [(\rho + \sigma)^*(g)f] \circ \iota_{V_\rho}, [(\rho + \sigma)^*(g)f] \circ \iota_{V_\sigma}$$

che si riscrive:

$$([\rho^*(g)](f \circ \iota_{V_\rho}), [\sigma^*(g)](f \circ \iota_{V_\sigma})) = ([(\rho + \sigma)^*(g)f] \circ \iota_{V_\rho}, [(\rho + \sigma)^*(g)f] \circ \iota_{V_\sigma})$$

che è equivalente a:

$$(f \circ \iota_{V_\rho} \circ [\rho(g^{-1})], f \circ \iota_{V_\sigma} \circ [\sigma(g^{-1})]) = (f \circ [(\rho + \sigma)(g^{-1})] \circ \iota_{V_\rho}, f \circ [(\rho + \sigma)(g^{-1})] \circ \iota_{V_\sigma})$$

Per ottenere la tesi basta osservare che valgono

$$\iota_{V_\rho} \circ [\rho(g^{-1})] = [(\rho + \sigma)(g^{-1})] \circ \iota_{V_\rho}$$

$$\iota_{V_\sigma} \circ [\sigma(g^{-1})] = [(\rho + \sigma)(g^{-1})] \circ \iota_{V_\sigma}$$

Notiamo infine che l'isomorfismo trovato è canonico, ovvero non dipende da alcuna scelta delle basi. \square

4.3 Sottospazi invarianti e scomposizione delle rappresentazioni

Definizione 4.8 (Sottorappresentazione). Sia ρ una rappresentazione di G su V_ρ . Una sottorappresentazione di ρ è un sottospazio vettoriale $W \subseteq V_\rho$ tale che $\rho(s)(W) \subseteq W$ per ogni $s \in G$. Infatti su tale sottospazio c'è in modo naturale una rappresentazione $\sigma : G \rightarrow GL(W)$ con $\sigma(s) = \rho(s)|_W$ (potremo scrivere $\sigma \subseteq \rho$).

Notazione: $V_\rho^G = \{v \in V_\rho : \rho(s)v = v \ \forall s \in G\}$, il sottospazio dei vettori invarianti.

Definizione 4.9 (Rappresentazione irriducibile). Una rappresentazione ρ di G è *irriducibile* se

1. $\rho \neq 0$ (ovvero $\deg(\rho) \geq 1$)
2. ρ non ha sottorappresentazioni non banali (diverse da 0 e V_ρ).

Definizione 4.10 (Rappresentazione completamente riducibile). Una rappresentazione si dice completamente riducibile se si può scrivere come somma di rappresentazioni irriducibili.

Osservazione. Attenzione al gioco di parole in italiano: una rappresentazione irriducibile è completamente riducibile. Il nome della definizione può in effetti portare a confusione.

Osservazione. Una cosa che vorremmo saper fare è scomporre la rappresentazione di un gruppo come somma di rappresentazioni irriducibili. Vedremo diversi teoremi che ci aiuteranno in questo tipo di problema.

Definizione 4.11 (Rappresentazione regolare). Consideriamo un gruppo finito G e uno spazio vettoriale V_ρ di dimensione $|G|$ su \mathbb{C} . Possiamo indicare gli elementi della base con e_g al variare di $g \in G$. Un generico vettore di questo spazio si scrive quindi come

$$v = \sum_{g \in G} a_g e_g$$

dove a_g sono dei numeri complessi. Possiamo definire una rappresentazione di G su questo spazio nel modo seguente:

$$\rho(h)v = \rho(h) \sum_{g \in G} a_g e_g = \sum_{g \in G} a_g \rho(h)e_g := \sum_{g \in G} a_g e_{hg}$$

Notare che questa definizione ha senso in quanto essendo G un gruppo, $gh \in G$ e quindi sicuramente e_{gh} è un elemento della base. Questa particolare rappresentazione di G si chiama *rappresentazione regolare* di G .

Esempio 4.6 (Rappresentazione regolare di S_3).

Teorema 4.4 (Le rappresentazioni di un gruppo finito sono completamente riducibili). *Sia G un gruppo finito e $\rho : G \rightarrow GL(V_\rho)$ una sua rappresentazione. Allora ρ è completamente riducibile.*

Per dimostrare questo teorema ci servono diversi lemmi che enunciamo e andiamo a dimostrare. Finiti i lemmi seguirà la dimostrazione.

Proposizione 4.5 (Prodotto hermitiano invariante). *Sia G un gruppo finito e $\rho : G \rightarrow V_\rho$ una sua rappresentazione. Allora lo spazio vettoriale V_ρ ammette una forma hermitiana invariante sotto l'azione di G , ovvero un prodotto tale che $h(v, w) = h(\rho(g)v, \rho(g)w) \forall v, w \in V_\rho, \forall g \in G$*

Dimostrazione. Lo spazio V_ρ ammette sicuramente una forma hermitiana, che chiamiamo h . Ora andiamo a fare una sorta di media per trasformare questa forma in una invariante. Consideriamo quindi

$$h_G(v, w) := \frac{1}{|G|} \sum_{g \in G} h(\rho(g)v, \rho(g)w)$$

È abbastanza facile mostrare adesso che effettivamente h_G è invariante sotto l'azione di G . Infatti,

$$h_G(\rho(h)v, \rho(h)w) = \sum_{g \in G} h(\rho(gh)v, \rho(gh)w)$$

Ma dato che G è un gruppo, questo vuol dire solo *eseguire la somma in un ordine diverso*. Di conseguenza h_G è G -invariante. \square

Lemma 4.6. *Sia $h : V_\rho \times V_\rho \rightarrow \mathbb{C}$ una forma hermitiana definita positiva e invariante per $\rho : G \rightarrow GL(V_\rho)$ e sia $\rho|_W : G \rightarrow GL(W)$ una sottorappresentazione di ρ . Allora se W^\perp è l'ortogonale di W , $\rho|_{W^\perp} : G \rightarrow GL(W^\perp)$ è una sottorappresentazione.*

Dimostrazione. Per noti teoremi di algebra lineare sappiamo che

$$V_\rho = W \oplus W^\perp$$

Di conseguenza un generico vettore di V_ρ si potrà scrivere come somma di $w_1 + w_2$, con $w_1 \in W$ e $w_2 \in W^\perp$. Inoltre sappiamo che $\rho|_W$ è una sottorappresentazione. Mostriamo che anche $\rho|_{W^\perp}$ è una sottorappresentazione: quello che dobbiamo mostrare è che $\rho(g)w_2 \in W^\perp \forall g \in G$. Dato che abbiamo un prodotto hermitiano la cosa più facile da verificare è che $\rho(g)w_2$ sia ortogonale a W . Consideriamo quindi l'espressione

$$0 = h(w_1, w_2) \quad \forall w_1 \in W, \forall w_2 \in W^\perp$$

Ma noi sappiamo che h è G -invariante, quindi

$$0 = h(w_1, w_2) = h(\rho(g)w_1, \rho(g)w_2) \quad \forall w_1 \in W, \forall w_2 \in W^\perp$$

E dato che $\rho(g)W = W$ per ipotesi, abbiamo mostrato che $\rho(w_2) \in W^\perp$. \square

Lemma 4.7. *Sia $\rho : G \rightarrow GL(V_\rho)$ una rappresentazione di un gruppo finito G . Sia $\rho|_W : G \rightarrow GL(W)$ una sottorappresentazione di ρ . Allora esiste una sottorappresentazione $\sigma : G \rightarrow GL(W')$ tale che*

$$\rho = \rho|_W + \sigma$$

Dimostrazione. La tesi segue dai due lemmi precedenti. L'ipotesi di gruppo finito si usa per l'esistenza della forma hermitiana invariante. \square

Osservazione. Notare che il teorema precedente è falso per gruppi infiniti. Un esempio si può costruire prendendo $G = \mathbb{Z}$, $V = \mathbb{C}^2$, e come rappresentazione

$$\begin{aligned}\rho : \mathbb{Z} &\rightarrow GL(\mathbb{C}^2) \\ k &\rightarrow M^k\end{aligned}$$

dove $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ è scritta nella base canonica.

Si vede subito che una sottorappresentazione è $\text{Span}(e_1)$ essendo e_1 autovettore per ogni $\rho(k)$, ma non esiste un suo complementare G -invariante: se esistesse avrebbe dimensione 1, quindi avremmo diagonalizzato $\rho(k) \forall k \in \mathbb{Z}$, ma sappiamo che tali endomorfismi non sono diagonalizzabili.

Dimostrazione del teorema 4.4. Sia $\rho : G \rightarrow GL(V_\rho)$ una rappresentazione di G . Se ρ è irriducibile, allora è completamente riducibile e quindi segue la tesi. Se invece esiste un sottospazio invariante W , allora per i lemmi precedenti esiste $Z \subset V_\rho$ tale che $V_\rho = W \oplus Z$ e tale che Z sia una sottorappresentazione. Per induzione si procede fino ad ottenere la tesi. \square

Teorema 4.8. Se $\rho : G \rightarrow GL(V_\rho)$ e $\sigma : G \rightarrow GL(V_\sigma)$ sono rappresentazioni di G e $f : V_\rho \rightarrow V_\sigma$ è un omomorfismo di rappresentazioni, allora $\text{Im}(f)$ è una sottorappresentazione di σ e $\text{Ker}(f)$ è una sottorappresentazione di V_ρ .

Dimostrazione. Se $v \in \text{Ker}(f)$ allora per la definizione di omomorfismo di rappresentazioni ho che $\forall s \in G \ f(\rho(s)v) = \sigma(s)f(v) = 0$ e quindi $\rho(s)v \in \text{Ker}(f)$. Allo stesso modo, se $w \in \text{Im}(f)$ allora $w = f(v)$ per qualche $v \in V_\rho$ e quindi sempre per la definizione di omomorfismo di rappresentazione $\sigma(s)w = \sigma(s)f(v) = f(\rho(s)v) \in \text{Im}(f)$. \square

Teorema 4.9. Sia G un gruppo abeliano finito. Allora ogni rappresentazione di G è isomorfa alla somma di rappresentazioni di grado 1.

Dimostrazione. È una conseguenza immediata della proposizione (4.1): sia $\rho : G \rightarrow GL(V_\rho)$, con $\dim V_\rho = n$, dato che G è finito $\forall g \in G \ \rho(g)$ è diagonalizzabile inoltre, visto che è abeliano, si sfrutta l'osservazione alla fine della proposizione per dedurre che le $\rho(g)$ sono simultaneamente diagonalizzabili. A questo punto il teorema è dimostrato: sia $\{v_1, \dots, v_n\}$ una base comune di autovettori, per ogni $1 \leq i \leq n$ $\text{Span}(v_i)$ è una sottorappresentazione di grado 1 di G (perché invariante per G), visto che $V_\rho = \text{Span}(v_1) \oplus \dots \oplus \text{Span}(v_n)$, allora $\rho \cong \rho_1 + \dots + \rho_n$, dove $\rho_i : G \rightarrow GL(\text{Span}(v_i))$. \square

Proposizione 4.10. La rappresentazione regolare \mathcal{R} di C_n è isomorfa alla somma delle n rappresentazioni irriducibili di grado 1 di C_n .

Lemma 4.11. Date ρ_1, ρ_2, σ rappresentazioni di G , allora

$$\text{Hom}(\rho_1 + \rho_2, \sigma) \cong \text{Hom}(\rho_1, \sigma) \oplus \text{Hom}(\rho_2, \sigma)$$

Dimostrazione. Consideriamo il lato destro dell'uguaglianza. Un elemento $\phi_i \in \text{Hom}(\rho_i, \sigma)$ si potrà scrivere

$$\phi_i : V_{\rho_i} \rightarrow V_\sigma \mid \phi_i(\rho_i(g)v) = \sigma(g)\phi_i(v) \quad \forall v \in V_{\rho_i}, \forall g \in G$$

Esibiamo ora una mappa

$$\begin{aligned}\Xi : \text{Hom}(\rho_1, \sigma) \oplus \text{Hom}(\rho_2, \sigma) &\rightarrow \text{Hom}(\rho_1 + \rho_2, \sigma) \\ \phi_1, \phi_2 &\rightarrow \phi_1 + \phi_2\end{aligned}$$

in modo ovvio e mostriamo che è un isomorfismo.

$$\Xi(\phi_1(v) + \phi_2(v)) = (\phi_1 + \phi_2)(v)$$

Innanzitutto la funzione $\phi_1 + \phi_2 : V_{\rho_1} \oplus V_{\rho_2} \rightarrow V_{\sigma}$ è effettivamente un omomorfismo di rappresentazioni e il motivo è che le due rappresentazioni in un certo senso agiscono separatamente sui due spazi senza interferire, quindi la verifica è immediata.

Ξ è iniettiva in quanto per l'appunto le due rappresentazioni agiscono in modo separato sui due spazi e quindi affinché due coppie di ϕ_i diano lo stesso risultato, devono essere uguali le coppie.

Ξ inoltre è suriettiva in quanto è un'applicazione lineare iniettiva fra spazi vettoriali che hanno la stessa dimensione.

□

Teorema 4.12 (Lemma di Schur). *Siano $\rho : G \rightarrow GL(V_{\rho})$ e $\sigma : G \rightarrow GL(V_{\sigma})$ due rappresentazioni irriducibili di G gruppo finito e $\phi : V_{\rho} \rightarrow V_{\sigma}$ un omomorfismo di rappresentazioni, allora ϕ è un isomorfismo oppure è identicamente nullo. Se poi $f : V_{\rho} \rightarrow V_{\rho}$ è un omomorfismo di rappresentazioni e lo spazio vettoriale V_{ρ} è su \mathbb{C} o su un campo algebricamente chiuso \mathbb{K} , allora f è una moltiplicazione per scalare.*

Dimostrazione. Supponiamo che $\phi \neq 0$, allora sappiamo che $\text{Ker}(\phi) \subseteq V_{\rho}$ è una sottorappresentazione di ρ , ma ρ è irriducibile e quindi $\text{Ker}(\phi) = 0 \Rightarrow \phi$ iniettiva. Ma anche $\text{Im}(\phi) \subseteq V_{\sigma}$ è una sottorappresentazione di σ e, non essendo nulla ed essendo σ irriducibile, coincide con tutto $V_{\sigma} \Rightarrow \phi$ suriettiva, da cui ϕ è un isomorfismo. Consideriamo ora f : sia λ un autovalore di f , che esiste perché G è finito e stiamo lavorando su \mathbb{C} , allora $f - \lambda \text{Id} : V_{\rho} \rightarrow V_{\rho}$ è un omomorfismo di rappresentazioni. Ma non è iniettivo, perché c'è almeno un autovettore relativo a λ , e quindi per la prima parte del lemma di Schur ho che $f - \lambda \text{Id}$ è identicamente nullo, da cui ricaviamo che f è la moltiplicazione per uno scalare (λ). □

Come immediato corollario, notiamo che, prese due rappresentazioni irriducibili ρ e σ , si ha che $\dim(\text{Hom}(\rho, \sigma))$ è uguale a 1 se $\rho \simeq \sigma$, ed è uguale a 0 se $\rho \not\simeq \sigma$. Generalizzando, se ρ si scompone in somma di rappresentazioni irriducibili come $\rho = \sum n_i \rho_i$, allora $\dim(\text{Hom}(\rho, \rho_i)) = n_i$.

Teorema 4.13. *Sia $\rho : G \rightarrow GL(V_{\rho})$ una rappresentazione e*

$$\rho = \sum_{i=1}^N n_i \rho_i$$

una sua scomposizione come somma di rappresentazioni irriducibili a due a due non isomorfe. Allora la scomposizione è unica.

Teorema 4.14. *Sia \mathcal{R} la rappresentazione regolare di G , un gruppo finito, e sia*

$$\mathcal{R} = \sum_{i=1}^N n_i \rho_i,$$

con ρ_i irriducibili e a due a due non isomorfe. Allora ogni rappresentazione irriducibile di G è isomorfa ad una ρ_i . Inoltre $n_i = \deg(\rho_i)$.

Dimostrazione. Per il corollario del Lemma di Schur, la tesi è equivalente al seguente fatto: se ρ è una rappresentazione irriducibile di G , allora $\dim(\text{Hom}(\mathcal{R}, \rho)) = \deg \rho$ (in realtà non useremo l'ipotesi di irriducibilità di ρ). Costruiamo dunque un isomorfismo tra gli spazi vettoriali $\text{Hom}(\mathcal{R}, \rho)$ e V_ρ .

Chiamando e_g l'elemento della base di $V_\mathcal{R}$ associato a $g \in G$, notiamo preliminarmente che, presa $\varphi \in \text{Hom}(\mathcal{R}, \rho)$, vale $\varphi(e_g) = \varphi(\mathcal{R}(g)e_1) = \rho(g)\varphi(e_1)$, dove con 1 si indica l'elemento neutro di G . Quindi, il valore di $\varphi(e_1)$ determina completamente $\varphi(e_g)$ per ogni g , e quindi determina completamente φ .

Sia allora $\Phi: \text{Hom}(\mathcal{R}, \rho) \rightarrow V_\rho$ tale che $\Phi(\varphi) = \varphi(e_1)$. Per quanto appena visto, Φ è iniettiva. D'altra parte, lo stesso ragionamento ci permette anche di dimostrare facilmente che Φ è suriettiva: per ogni $v \in V_\rho$, la funzione φ_v tale che $\varphi_v(e_g) = \rho(g)v$ è tale che $\Phi(\varphi_v) = \varphi_v(e_1) = \rho(1)v = v$. La linearità di Φ consente di concludere. \square

Corollario. *Se G è abeliano allora ha $|G|$ rappresentazioni irriducibili di grado 1 e \mathcal{R} è la somma di queste.*

Corollario. *Sia G un gruppo finito. G ha un numero finito di rappresentazioni irriducibili, a meno di isomorfismi. Inoltre*

$$|G| = \sum n_i^2$$

4.4 Alcuni isomorfismi notevoli

Sia G un gruppo e siano $\rho : G \rightarrow GL(V)$ e $\sigma : G \rightarrow GL(W)$ sue rappresentazioni. Sappiamo bene che l'insieme delle applicazioni lineari da V in W , che denotiamo con $\text{Hom}(V, W)$, è uno spazio vettoriale. Quello che vogliamo fare ora è rendere tale spazio vettoriale una rappresentazione di G , ovvero vogliamo definire un'azione lineare di G su $\text{Hom}(V, W)$. Il modo naturale di farlo è il seguente: sia $\varphi \in \text{Hom}(V, W)$. Definiamo $g \cdot \varphi \in \text{Hom}(V, W)$ come la funzione che fa commutare il diagramma:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \rho(g) \downarrow & & \downarrow \sigma(g) \\ V & \xrightarrow{g \cdot \varphi} & W \end{array}$$

Ovvero esplicitamente: $g \cdot \varphi = \sigma(g) \circ \varphi \circ \rho(g^{-1})$

La verifica che si tratti di un'azione di gruppo è molto semplice, inoltre è evidente dalla definizione che l'azione è lineare: dunque abbiamo davvero dotato $\text{Hom}(V, W)$ di una struttura di G -rappresentazione.

Sappiamo già che $\text{Hom}(V, W)$ e $V^* \otimes W$ sono isomorfi come spazi vettoriali. Quello che vogliamo vedere è che sono isomorfi anche come G -rappresentazioni. Ovviamente la rappresentazione che si considera su $V^* \otimes W$ è la rappresentazione $\rho^* \otimes \sigma$, che per semplicità indichiamo con τ .

Teorema 4.15. *$\text{Hom}(V, W)$ e $V^* \otimes W$ sono isomorfi come G -rappresentazioni.*

Dimostrazione. Conosciamo già un isomorfismo di spazi vettoriali $\Psi : V^* \otimes W \rightarrow \text{Hom}(V, W)$, costruito in maniera tale che per ogni $f \in V^*, w \in W, v \in V$ si abbia $\Psi(f \otimes w)(v) = f(v)w$. Mostriamo che Ψ è omomorfismo di rappresentazioni, ovvero che fissato $g \in G$ il seguente diagramma commuta:

$$\begin{array}{ccc} V^* \otimes W & \xrightarrow{\Psi} & \text{Hom}(V, W) \\ \tau(g) \downarrow & & \downarrow g \\ V^* \otimes W & \xrightarrow{\Psi} & \text{Hom}(V, W) \end{array}$$

Ovvero dobbiamo controllare se

$$g \circ \Psi = \Psi \circ \tau(g)$$

Possiamo limitarci a fare le verifiche sugli elementi decomponibili di $V^* \otimes W$, in quanto essi generano tutto lo spazio. Prendiamo dunque $f \in V^*, w \in W$ e consideriamo $f \otimes w$. Vogliamo mostrare che

$$g(\Psi(f \otimes w)) = \Psi(\tau(g)(f \otimes w))$$

Quindi prendiamo $v \in V$ e vediamo dove viene mandato dalla funzione a sinistra:

$$\begin{aligned} & g(\Psi(f \otimes w))(v) \\ = & \sigma(g) \Psi(f \otimes w) (\rho(g^{-1}) v) \\ = & \sigma(g) f(\rho(g^{-1}) v) w \\ = & f(\rho(g^{-1}) v) \sigma(g) w \end{aligned}$$

Mentre dalla funzione a destra viene mandato in:

$$\begin{aligned} & \Psi(\tau(g)(f \otimes w))(v) \\ = & \Psi([f \circ \rho(g^{-1})] \otimes [\sigma(g)w])(v) \\ = & f(\rho(g^{-1})v) \sigma(g) w \end{aligned}$$

Avendo ottenuto lo stesso risultato in entrambi i casi, si ha la tesi. \square

5 Teoria dei caratteri

Definizione 5.1. Sia $\rho : G \rightarrow GL(V_\rho)$ una rappresentazione di un gruppo G . Definiamo carattere di ρ la funzione che associa ad ogni elemento del gruppo G la traccia della matrice associata all'elemento, ovvero

$$\chi_\rho(s) := \text{tr}(\rho(s)) \quad \forall s \in G$$

Notare che χ_ρ è una funzione che va dal gruppo in \mathbb{C} , ovvero $\chi_\rho : G \rightarrow \mathbb{C}$

Vediamo delle proprietà elementari del carattere

1. Se $\deg(\rho) = 1$ allora il carattere di s è uguale a $\rho(s)$
2. $\chi_{\rho_1} = \deg(\rho)$.⁶
Questo è vero poichè $[\rho_1] = \text{Id}_n \Rightarrow \text{tr}(\rho_1) = n$ ed $n = \deg(\rho)$.
3. $\chi_{\rho+\sigma}(s) = \chi_\rho(s) + \chi_\sigma(s)$.
Questo è dovuto al fatto che la somma di rappresentazioni si può scrivere come matrice a blocchi. Una volta scritto così è evidente il risultato.
4. $\chi_{\rho\sigma}(s) = \chi_\rho(s)\chi_\sigma(s)$. In particolare dunque $\chi_{\rho^2} = (\chi_\rho)^2$.
Questo deriva immediatamente dal teorema 3.9.
5. $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$
Essendo G un gruppo finito, $\forall s \in G$ $\rho(s)^n = \text{id}$ dove $n = |G|$: dunque tutti gli autovalori di $\rho(s)$ sono radici ennesime dell'unità e $\rho(s)$ è diagonalizzabile⁷. In tale base è evidente che:

$$\chi_\rho(s^{-1}) = \text{tr}(\rho(s^{-1})) = \text{tr}(\rho(s)^{-1}) = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda_i} = \overline{\text{tr}(\rho(s))} = \overline{\chi_\rho(s)}$$

in quanto, avendo gli autovalori modulo 1, l'inverso coincide con il coniugio.

6. $\chi_{\rho^*}(s)^8 = \overline{\chi_\rho(s)}$.

Per l'osservazione precedente vale che

$$\chi_{\rho^*}(s) = \text{tr}({}^t \rho(s^{-1})) = \text{tr}(\rho(s^{-1})) = \overline{\text{tr}(\rho(s))} = \overline{\chi_\rho(s)}$$

7. $\chi_\rho(hsh^{-1}) = \chi_\rho(s)$ ovvero χ_ρ è costante sulle classi di coniugio di G . La motivazione è semplice: se due elementi sono coniugati tra loro questo significa che le matrici corrispondenti saranno simili e la traccia è un invariante di similitudine.

Di conseguenza, non sarà necessario calcolare il carattere per ogni elemento del gruppo ma basterà farlo per le classi di coniugio di G .

Le funzioni che costanti sulle classi di coniugio di un gruppo vengono dette *funzioni di classe*. L'insieme delle funzioni di classe di un gruppo viene normalmente indicato con $Cl(G)$ e si verifica che esso è un sottospazio di \mathbb{C}^G .

8. Supponiamo di avere una rappresentazione per permutazioni. Sia I un insieme finito e G un gruppo allora

$$\chi_{\rho_I}(s) = \#\{\text{punti fissi di } \rho_I(s)\} = |I^s|$$

dove $I^s := \{i \in I | s \circ i = i\}$. La veridicità di questo fatto si vede scrivendo esplicitamente la matrice che rappresenta $\rho_I(s)$.

⁶Al solito ρ_1 è la rappresentazione che manda ogni elemento nell'identità di V_ρ

⁷Si veda la proposizione 4.1

⁸Ricordiamo che $\rho^*(s) = (\rho(s)^{-1})^*$

9. Consideriamo la rappresentazione per permutazioni regolare R . Calcoliamone il carattere:

$$\chi_R(s) = \begin{cases} |G| & \text{se } s = e \\ 0 & \text{se } s \neq e \end{cases}$$

semplicemente perchè $s \circ g = g \Leftrightarrow s = e$.

Esempio 5.1. $G = S_3$, $I = \{1, 2, 3\}$. Allora

$$\chi_{\rho_I}(s) = \begin{cases} 3 & \text{se } s = e \\ 1 & \text{se } s \text{ è una trasposizione} \\ 0 & \text{se } s \text{ è un treciclo} \end{cases}$$

Ricordandoci che $\chi_{\rho_I} = \chi_{1+\rho}$ si ha che

$$\chi_{\rho}(s) = \begin{cases} 2 & \text{se } s = e \\ 0 & \text{se } s \text{ è una trasposizione} \\ -1 & \text{se } s \text{ è un 3-ciclo} \end{cases}$$

Definizione 5.2 (Prodotto hermitiano dei caratteri).

$$\langle f|g \rangle = \frac{1}{|G|} \sum_{s \in G} f(s) \overline{g(s)}$$

Teorema 5.1 (Relazioni di ortogonalità). *Se ρ e σ sono rappresentazioni irriducibili di G , allora vale*

$$\langle \chi_{\rho} | \chi_{\sigma} \rangle = \begin{cases} 1 & \text{se } \rho \cong \sigma \\ 0 & \text{altrimenti} \end{cases}$$

Per dimostrare questo teorema abbiamo bisogno di un lemma che ora enunciamo e dimostriamo.

Lemma 5.2. *Se (ρ, V_{ρ}) e (σ, V_{σ}) sono rappresentazioni⁹ di G , allora vale*

$$\langle \chi_{\sigma} | \chi_{\rho} \rangle = \dim(\text{Hom}(\rho, \sigma))$$

Dimostrazione. L'idea principale per dimostrare questo lemma è di ridurci al caso più facile in cui una delle due rappresentazioni è quella banale. Per farlo notiamo un paio di cose

$$\langle \chi_{\sigma} | \chi_{\rho} \rangle = \frac{1}{|G|} \sum_{s \in G} \chi_{\sigma}(s) \overline{\chi_{\rho}(s)} = \frac{1}{|G|} \sum_{s \in G} \chi_{\rho^* \sigma}(s) = \frac{1}{|G|} \sum_{s \in G} \chi_{\rho^* \sigma}(s) = \langle \chi_{\rho^* \sigma} | 1 \rangle$$

Siamo passati da due rappresentazioni ad una sola. In particolare lo spazio vettoriale su cui agisce questa rappresentazione è

$$V_{\rho^* \sigma} = V_{\rho}^* \otimes V_{\sigma} \cong \text{Hom}(V_{\rho}, V_{\sigma})$$

dove l'isomorfismo di rappresentazioni è quello dimostrato nel teorema 4.15. In particolare abbiamo che

$$(V_{\rho^* \sigma})^G \cong \text{Hom}(V_{\rho}, V_{\sigma})^G \cong \text{Hom}(\rho, \sigma)$$

Per cui dato che noi stiamo cercando $\dim(\text{Hom}(\rho, \sigma))$, basterà trovare $\dim(V_{\rho^* \sigma})^G$.

⁹Non necessariamente irriducibili

Lemma 5.3. Sia ρ una rappresentazione di un gruppo finito G . Allora $\dim(V_\rho)^G = \text{tr}(T)$ dove

$$T = \frac{1}{|G|} \sum_{s \in G} \rho(s).$$

Prima di iniziare la dimostrazione diamo una giustificazione della scelta della applicazione lineare T : questa è stata dettata dal fatto che

$$\text{tr}(T) = \text{tr} \left(\frac{1}{|G|} \sum_{s \in G} \rho(s) \right) = \frac{1}{|G|} \sum_{s \in G} \text{tr}(\rho(s)) = \langle \chi_\rho | 1 \rangle$$

Si nota anzitutto che

$$\rho(t)T(v) = \frac{1}{|G|} \sum_{s \in G} \rho(t)\rho(s)v = \frac{1}{|G|} \sum_{s \in G} \rho(s)v = T(v)$$

ovvero $\text{Im } T \subseteq V_\rho^G$. D'altra parte se $v \in V_\rho^G$ allora è chiaro che $Tv = v$ (basta applicare la definizione). Per cui $\text{Im } T = V_\rho^G$.

Inoltre

$$T(Tv) = \dots = Tv \quad \text{verifica banale}$$

Per cui T è un proiettore. A questo punto sappiamo dall'algebra lineare che

$$V_\rho = \text{Ker } T \oplus \text{Im } T = \text{Ker } T \oplus V_\rho^G$$

Per cui $\text{tr } T = \dim \text{Im } T = \dim V_\rho^G$. Ma dalla catena di deduzioni che abbiamo fatto

$$\dim(\text{Hom}(V_\rho, V_\sigma)) = \dim(V_{\rho^* \sigma}^G) = \text{tr } T = \langle \chi_{\rho^* \sigma} | 1 \rangle = \langle \chi_\sigma | \chi_\rho \rangle$$

□

Osservazione.

$$\langle \chi_\sigma | \chi_\rho \rangle = \overline{\langle \chi_\rho | \chi_\sigma \rangle}$$

ovvero per quanto appena dimostrato

$$\dim(\text{Hom}(V_\rho, V_\sigma)) = \overline{\dim(\text{Hom}(V_\sigma, V_\rho))}$$

tuttavia essendo dei numeri naturali deduciamo che le eguaglianze sussistono anche senza il coniugio.

Dimostrazione del teorema 5.1. A questo punto la tesi del teorema 5.1 segue dal lemma precedente applicato insieme al lemma di Schur. □

Osservazione. • Ricordiamo che se ρ è una rappresentazione di G , allora ρ si può scrivere in modo unico come

$$\rho = \sum_i n_i \rho_i$$

Dove le ρ_i sono le rappresentazioni irriducibili di G e gli n_i sono numeri naturali ≥ 0 . Dall'equazione scritta sopra segue subito che

$$\chi_\rho = \sum_i n_i \chi_{\rho_i}$$

E possiamo ottenere un'informazione utile prendendo il prodotto scalare dell'equazione precedente con il carattere di una delle rappresentazioni ρ_i

$$\langle \chi_\rho | \chi_{\rho_j} \rangle = \sum_i n_i \langle \chi_{\rho_i} | \chi_{\rho_j} \rangle \Rightarrow n_i \delta_{ij} = \langle \chi_\rho | \chi_{\rho_j} \rangle \Rightarrow n_i = \langle \chi_\rho | \chi_{\rho_i} \rangle$$

- Caso particolare interessante del fatto precedente riguarda la rappresentazione regolare di un gruppo. Difatti come sappiamo,

$$\chi_{\mathcal{R}}(s) = \begin{cases} |G| & \text{se } s = e \\ 0 & \text{altrimenti} \end{cases}$$

Quindi considerando una sottorappresentazione si ha che

$$\langle \chi_{\mathcal{R}} | \chi_\rho \rangle = \frac{1}{|G|} |G| \chi_\rho(e) = \chi_\rho(e) = \deg(\rho)$$

In particolare se ρ è una sottorappresentazione irriducibile allora

$$\deg(\rho) = \dim(\text{Hom}(\mathcal{R}, \rho))$$

Quindi ottengo una conferma del teorema precedente

$$\langle \chi_{\mathcal{R}} | \chi_\rho \rangle = \dim(\text{Hom}(\mathcal{R}, \rho))$$

- Se ρ e σ sono 2 rappresentazioni irriducibili allora

$$\rho \cong \sigma \Leftrightarrow \chi_\rho = \chi_\sigma$$

- $\langle \chi_\rho | \chi_\rho \rangle = |\chi_\rho|^2 = \sum_i n_i^2$.
- Conseguenza dell'ultima osservazione è che una rappresentazione di un gruppo ρ è irriducibile $\Leftrightarrow \langle \chi_\rho | \chi_\rho \rangle = |\chi_\rho|^2 = 1$

Corollario (Corollario del lemma 5.2: Lemma di Burnside). *Sia I un insieme finito e G un gruppo finito che agisce su di esso. Vale allora la formula*

$$|I/G| = \frac{1}{|G|} \sum_{s \in G} |I^s|$$

Dimostrazione. Consideriamo la rappresentazione per permutazioni corrispondente all'azione di G sull'insieme I , (ρ_I, V_{ρ_I}) . Consideriamo

$$\langle \chi_{\rho_I} | 1 \rangle = \frac{1}{|G|} \sum_{s \in G} \text{tr } \rho_I(s)$$

Ma è ovvio che

$$\text{tr } \rho_I(s) = |I^s| \quad I^s = \{i \in I | s \cdot i = i\}$$

Per cui lo spazio

$$\begin{aligned} V_{\rho_I}^G &= \{v \in V_{\rho_I} : \rho_I(s)v = v \ \forall s \in G\} = \left\{ \sum_i a_i e_i : \rho_I \left(\sum_i a_i e_i \right) = \sum_i a_i e_i \ \forall s \in G \right\} \\ &= \left\{ \sum_i a_i e_i : \sum_i a_i e_{s o i} = \sum_i a_i e_i \ \forall s \in G \right\} = \left\{ \sum_i a_i e_i : \sum_i (a_{s^{-1} o i} - a_i) e_i = 0 \ \forall s \in G \right\} \end{aligned}$$

sarà composto da i vettori che hanno i coefficienti a_i costanti su ciascuna orbita di G su I , proprio per lasciarlo invariante. Perciò

$$\dim V_{\rho_I}^G = \text{numero delle orbite} = |I/G|$$

E con l'affermazione precedente si ottiene appunto il lemma di Burnside \square

Teorema 5.4. *Sia G un gruppo finito e siano ρ_1, \dots, ρ_r le sue rappresentazioni irriducibili. Sia inoltre $\mathbb{C}(G)^\#$ lo spazio delle funzioni da G in \mathbb{C} costanti sulle classi di coniugio di G .*

Chiaramente $\dim \mathbb{C}(G)^\# = \text{numero di classi di coniugio di } G := s$. La tesi del teorema è che $r = s$ dove r è il numero di rappresentazioni irriducibili.

Osservazione. Per questo motivo la tabella dei caratteri sarà una tabella quadrata.

Dimostrazione. Mostriamo intanto che $r \leq s$: i caratteri di ρ_1, \dots, ρ_r sono infatti ortonormali rispetto alla forma hermitiana definita positiva $\langle \cdot, \cdot \rangle$, e quindi sono indipendenti (non posso avere più di s vettori linearmente indipendenti in uno spazio vettoriale di dimensione s).

Verifichiamo ora che $\langle \chi_{\rho_1}, \dots, \chi_{\rho_r} \rangle^\perp = 0$. Sia $f \in \mathbb{C}(G)^\#$ e ρ una rappresentazione, definiamo $T_f = \frac{1}{|G|} \sum_s f(s) \rho(s)$ e verifichiamo che è un omomorfismo di rappresentazioni:

$$\begin{aligned} T_f \circ \rho(t) &= \frac{1}{|G|} \sum_s f(s) \rho(s) \rho(t) = \frac{1}{|G|} \sum_s \rho(t) \rho(t^{-1}) f(s) \rho(s) \rho(t) = \\ &= \frac{1}{|G|} \rho(t) \sum_s f(s) \rho(t^{-1}) \rho(s) \rho(t) = \frac{1}{|G|} \rho(t) \sum_s f(s) \rho(t^{-1} s t) = \\ &= \frac{1}{|G|} \rho(t) \sum_{s'} f(s') \rho(s') = \rho(t) \circ T_f \end{aligned}$$

Abbiamo usato il fatto che $f(s) \in \mathbb{C}$, quindi commuta con $\rho(g)$, e che f è una funzione di classe nella sostituzione di s con $s' = t^{-1} s t$ (essendo il coniugio un automorfismo, cambia solo l'ordine della somma).

Se ρ è irriducibile, $T_f = \alpha I$ è uno scalare per il lemma di Schur, $\alpha = \frac{\text{tr}(T_f)}{\deg(\rho)}$. Si ha

$$\alpha = \frac{1}{\deg(\rho)} \text{tr}(T_f) = \frac{1}{\deg(\rho)|G|} \sum_s f(s) \chi_\rho(s) = \frac{1}{\deg(\rho)} \langle f | \chi_{\rho^*} \rangle = 0$$

se $f \in \langle \chi_{\rho_1}, \dots, \chi_{\rho_r} \rangle^\perp$.

Generalizziamo a quando ρ non è irriducibile, ossia $\rho = \sigma_1 + \dots + \sigma_n$, con σ_i irriducibili. Allora si ha $V_\rho = V_{\sigma_1} \oplus \dots \oplus V_{\sigma_n}$, ed essendo $T_f = 0$ su ogni V_{σ_i} , è nullo anche su V_ρ .

Mostriamo che questo implica $f = 0$: sia \mathcal{R} la rappresentazione regolare di G ; si ha:

$$0 = |G| T_f(e_1) = \sum_s f(s) \mathcal{R}(s)(e_1) = \sum_s f(s) e_s$$

Di conseguenza $f(s) = 0 \ \forall s \in G$ essendo gli e_s una base di V_R . In questo modo abbiamo mostrato che $\langle \chi_{\rho_1}, \dots, \chi_{\rho_r} \rangle^\perp = \{0\}$, quindi $r = s$. \square

5.1 Tabella dei caratteri

Dato un gruppo G , possiamo costruire la *tabella dei caratteri* nel seguente modo:

- su ogni colonna mettiamo un rappresentante della classe di coniugio con sotto la cardinalità dell'orbita ovvero

G	e	$\text{Orb}(g_1)$	$\text{Orb}(g_2)$	
	1	$ \text{Orb}(g_1) $	$ \text{Orb}(g_2) $	

- su ogni riga mettiamo una rappresentazione irriducibile del gruppo
- all'incrocio tra la rappresentazione ρ_i e la classe di coniugio di g_j inseriamo il valore di $\chi_{\rho_i}(g_j)$.

5.2 Esempi di rappresentazioni di gruppi finiti

Esempio 5.2 (Tabella dei caratteri di S_3). La prima cosa da fare per costruire la tabella dei caratteri è vedere quanti elementi ha S_3 , suddividerli in classi di coniugio e poi cercare le rappresentazioni irriducibili solo dopo aver fatto tutto questo. Notiamo subito che S_3 ha esattamente 3 classi di coniugio. La prima è ovviamente quella banale, composta solo dall'identità e . Poi c'è la classe delle trasposizioni $\{(12), (23), (13)\}$ che ha 3 elementi e poi ci sono i 3cicli, ovvero (123) e (132) . Possiamo cominciare a scrivere una tabella vuota 3×3

S_3	e	(12)	$(1\ 2\ 3)$
	1	3	2

Una rappresentazione irriducibile che c'è sempre è la rappresentazione banale di grado 1, ovvero quella che manda ogni elemento nell'identità. La tabella con questa informazione diventa

S_3	e	(12)	$(1\ 2\ 3)$
	1	3	2
ρ_1	1	1	1

Un'altra rappresentazione che già conosciamo è il segno, ϵ , che ricordiamo vale $(-1)^{n-1}$ dove n è la lunghezza del ciclo. La tabella diventa

S_3	e	(12)	$(1\ 2\ 3)$
	1	3	2
ρ_1	1	1	1
ϵ	1	-1	1

A questo punto ci sono due motivi per dire che l'ultima rappresentazione ha grado 2: il primo è che è l'unico modo di ottenere la relazione

$$|G| = \sum_i n_i^2$$

Il secondo è che se fossero due rappresentazioni di grado 1 allora il gruppo avrebbe solo rappresentazioni irriducibili di grado 1 e un teorema che abbiamo fatto implicherebbe che S_3 sia abeliano, cosa palesemente falsa.

Per trovare il carattere dell'ultima rappresentazione possiamo agire in più modi. Innanzitutto la tabella ora ha la forma

S_3	e	(12)	$(1\ 2\ 3)$
	1	3	2
ρ_1	1	1	1
ϵ	1	-1	1
ρ	2		

In generale ci saranno due numeri complessi a, b nelle due caselle che mancano. Tuttavia noi sappiamo un sacco di teoremi che ci permettono di restringere il campo dei valori che possono avere. Per esempio noi sappiamo che

$$\langle \rho_i | \rho_j \rangle = \delta_{ij}$$

Per cui imponendo che il prodotto scalare con entrambe le precedenti faccia 0 abbiamo due equazioni e due incognite, ovvero un problema risolvibile. L'altro modo è dire che

$$\mathcal{R} = 1 + \epsilon + 2\rho$$

E dato che il carattere si comporta bene con la somma di rappresentazioni,

$$\chi_{\mathcal{R}} = \chi_1 + \chi_{\epsilon} + 2\chi_{\rho}$$

Ma sappiamo anche che

$$\chi_{\mathcal{R}}(s) = \begin{cases} |G| & \text{se } s = e \\ 0 & \text{altrimenti} \end{cases}$$

Per cui con agili conti riusciamo a completare la tabella

S_3	e	(12)	$(1\ 2\ 3)$
	1	3	2
ρ_1	1	1	1
ϵ	1	-1	1
ρ	2	0	-1

Tabella 1: Tabella dei caratteri di S_3

L'ultimo modo è cercare di scomporre un'altra rappresentazione a caso di S_3 , cercando di trovare la rappresentazione che ci manca. Per esempio ricordiamo l'azione di S_3 sui vettori di base di \mathbb{R}^3

$$\tau(s)e_i = e_{s(i)}$$

Ricordiamo che il sottospazio di dimensione 1 fatto dallo $Span$ del vettore $v = e_1 + e_2 + e_3$ è un sottospazio invariante in cui $\tau(s)$ è sostanzialmente l'identità. Il suo ortogonale è un altro sottospazio invariante su cui ρ è irriducibile. Di conseguenza potremo scrivere

$$\tau = 1 + \rho$$

E siamo sicuri che l'altra rappresentazione di grado 2 sia esattamente quella che stiamo cercando proprio grazie al teorema che ci dice che tutte le rappresentazioni irriducibili di un gruppo compaiono nella sua rappresentazione regolare. (Teorema 4.14)

Dato che è facile calcolare il carattere di $\tau(s)$ in quanto è uguale a $\text{Fix}(s)$, possiamo scrivere

$$\text{Fix}(s) = 1 + \chi_\rho$$

Da cui si ricava subito il carattere della rappresentazione ρ

Esempio 5.3 (Tabella dei caratteri di S_4). Facciamo la prima cosa importante: dividiamo S_4 in classi di coniugio. Per i soliti teoremi sugli S_n , le classi di coniugio saranno

$$\{e\}, \{(ab)\}, \{(abc)\}, \{(abcd)\}, \{(ab)(cd)\}$$

E notiamo che sono 5. Possiamo quindi cominciare a compilare la tabella dei caratteri vuota

S_4	e	(12)	(1 2 3)	(1234)	(12)(34)
	1	6	8	6	3
ρ_1	1	1	1	1	1

dove ho già messo la rappresentazione banale. Anche per S_4 , essendo un gruppo simmetrico c'è la rappresentazione segno di grado 1.

S_4	e	(12)	(1 2 3)	(1234)	(12)(34)
	1	6	8	6	3
ρ_1	1	1	1	1	1
ϵ	1	-1	1	-1	1

A questo punto bisogna fare cose a caso cercando le rappresentazioni irriducibili. Per esempio possiamo di nuovo considerare la rappresentazione per permutazioni

$$\tau(s)e_i = e_{s(i)}$$

Che si scompone anche questa come

$$\tau = 1 + \rho$$

Vorremmo sapere se ρ è irriducibile. Potremmo invocare qualche teorema ma lo faremo con le mani calcolando il carattere di ρ

$$\chi_\rho(s) = \text{Fix}(s) - 1 = \begin{cases} 3 & \text{Se } s = e \\ 1 & \text{Se } s = (ab) \\ 0 & \text{Se } s = (abc) \\ -1 & \text{Se } s = (abcd), (ab)(cd) \end{cases}$$

E andando a calcolare

$$\langle \chi_\rho | \chi_\rho \rangle = \frac{1}{24} (3^2 + 6 \cdot 1^2 + 0 + (-1)^2 \cdot (3 + 6)) = 1$$

Per cui è effettivamente irriducibile. Aggiungiamola alla tabella.

S_4	e	(12)	(1 2 3)	(1234)	(12)(34)
	1	6	8	6	3
ρ_1	1	1	1	1	1
ϵ	1	-1	1	-1	1
ρ	3	1	0	-1	-1

Abbiamo appena terminato le rappresentazioni che conoscevamo di S_4 .

Ottimo consiglio: Quando non vengono in mente altre rappresentazioni, considera due già presenti nella tabella e fanne il prodotto. Risulta utile il seguente lemma.

Lemma 5.5. *Se ρ e σ sono due rappresentazioni e $\deg(\rho) = 1$ (ovvero $\rho : G \rightarrow \mathbb{C}^*$), allora σ è irriducibile $\Leftrightarrow \rho\sigma$ lo è. Inoltre hanno lo stesso grado.*

Dimostrazione. Che sia ancora a tutti gli effetti una rappresentazione si verifica esplicitamente sapendo che

$$\forall s \in G \quad \rho\sigma(s) = \rho(s)\sigma(s)$$

Per dimostrare che è irriducibile si considera il fatto che

$$\sigma \text{ irriducibile} \Leftrightarrow 1 = \langle \chi_\sigma | \chi_\sigma \rangle = \frac{1}{|G|} \sum_{s \in G} |\chi_{\sigma(s)}|^2$$

Quindi

$$\langle \chi_{\rho\sigma} | \chi_{\rho\sigma} \rangle = \frac{1}{|G|} \sum_{s \in G} |\chi_{\rho\sigma(s)}|^2 = \frac{1}{|G|} \sum_{s \in G} |\chi_{\rho(s)} \chi_{\sigma(s)}|^2 = \frac{1}{|G|} \sum_{s \in G} |\rho(s) \chi_{\sigma(s)}|^2 = \frac{1}{|G|} \sum_{s \in G} |\rho(s)|^2 |\chi_{\sigma(s)}|^2$$

ed essendo $\rho(s)$ una radice n -esima dell'unità dove n è l'ordine di G si ha che

$$\langle \chi_{\rho\sigma} | \chi_{\rho\sigma} \rangle = \frac{1}{|G|} \sum_{s \in G} |\chi_{\sigma(s)}|^2 = \langle \chi_\sigma | \chi_\sigma \rangle$$

Che abbiano lo stesso grado deriva dal fatto che

$$\chi_{\rho\sigma} = \chi_\rho \chi_\sigma \Rightarrow \deg(\rho\sigma) = \chi_{\rho\sigma}(e) = \chi_\rho(e) \chi_\sigma(e) = \deg(\rho) \deg(\sigma) = \deg(\sigma).$$

□

S_4	e	(12)	$(1\ 2\ 3)$	(1234)	$(12)(34)$
	1	6	8	6	3
ρ_1	1	1	1	1	1
ϵ	1	-1	1	-1	1
ρ	3	1	0	-1	-1
$\rho\epsilon$	3	-1	0	1	-1

Essendo ϵ di grado 1 e ρ irriducibile allora anche $\rho\epsilon$ è un'altra rappresentazione irriducibile. A questo punto dato che $|S_4| = 24$ e che $1 + 1 + 3^2 + 3^2 = 20$ si possono avere due situazioni: S_4 potrebbe avere ancora 4 rappresentazioni irriducibili di grado 1 oppure solo più una di grado 2. Tuttavia abbiamo visto come S_n ammetta solo due rappresentazioni irriducibili di grado 1 quindi siamo nel secondo caso.

Dato che ce ne manca solo una possiamo usare il trucco di prima (differenza dalla rappresentazione \mathcal{R}) e concludere:

S_4	e	(12)	$(1\ 2\ 3)$	(1234)	$(12)(34)$
	1	6	8	6	3
ρ_1	1	1	1	1	1
ϵ	1	-1	1	-1	1
ρ	3	1	0	-1	-1
$\rho\epsilon$	3	-1	0	1	-1
σ	2	0	-1	0	2

Tabella 2: Tabella dei caratteri di S_4

Osservazione. Guardiamo la tabella, in particolare il "minore" ottenuto considerando le prime due e l'ultima riga e le prime 3 colonne.

S_4	e	(12)	$(1\ 2\ 3)$
	1	6	8
ρ_1	1	1	1
ϵ	1	-1	1
σ	2	0	-1

Se la confrontiamo con la tabella dei caratteri di S_3 vediamo che sono analoghe. Intuitivamente ρ in S_3 deriva dalla rappresentazione σ di S_4 mediante un omomorfismo

$$S_4 \rightarrow S_3$$

che corrisponde ad una azione di S_4 su un insieme di 3 elementi. Tale insieme è il sottogruppo di Klein privato dell'unità ovvero

$$\{(12)(34), (13)(24), (14)(23)\}$$

In questo caso non è servito ma possono risultare utili i prossimi lemmi.

Lemma 5.6. ρ^* è irriducibile $\Leftrightarrow \rho$ è irriducibile.

Infatti $\chi_{\rho^*} = \overline{\chi_\rho}$ e quindi analogamente al lemma precedente si vede che

$$1 = \langle \chi_\rho | \chi_\rho \rangle \Leftrightarrow 1 = \langle \chi_{\rho^*} | \chi_{\rho^*} \rangle$$

Lemma 5.7. Se ρ è una rappresentazione di grado d di G , come sempre gruppo finito, allora:

(a) $|\chi_\rho(s)| \leq d$

(b) Direttamente dal punto (a) si deduce che,

$$\chi_\rho(s) = d \Leftrightarrow \lambda_1, \dots, \lambda_d = 1 \Leftrightarrow \rho(s) = \text{Id}$$

dove $\lambda_1, \dots, \lambda_d$ sono gli autovalori della matrice $[\rho(s)]$.

Dimostrazione. Se $\lambda_1, \dots, \lambda_d$ sono gli autovalori della matrice $[\rho(s)]$ allora $\chi_\rho(s) = \sum_{i=1}^d \lambda_i$. Inoltre essendo G finito $|\lambda_i| = 1 \forall i \in \{1, \dots, d\}$. Se ne deduce che

$$|\chi_\rho(s)| \leq \sum_{i=1}^d |\lambda_i| = d$$

□

Esempio 5.4 (Tabella dei caratteri di D_5). La prima cosa da fare è dividere D_5 in classi di coniugio
FINIRE

5.2.1 I problemi della prima lezione visti con i nuovi strumenti

Esempio 5.5 (Problema 1 prima lezione).

Esempio 5.6 (Problema 2 prima lezione).

Esempio 5.7 (Problema 3 prima lezione). Consideriamo un cubo. Scriviamo un numero su ciascuna delle facce e consideriamo l'operazione T che per ogni faccia sostituisce al numero presente la media dei numeri presenti sulle 4 facce del cubo adiacenti. Vogliamo studiare il comportamento dei numeri del cubo quando questa iterazione viene compiuta molte volte.

Cerchiamo di formalizzare il problema usando la teoria della rappresentazione. Possiamo considerare l'insieme F delle facce del cubo¹⁰. Una generica configurazione del cubo sarà esprimibile come

$$v = \sum_{f \in F} a_f e_f$$

Dove $a_f \in \mathbb{C}$ e e_f sono una base. L'operatore che sostituisce la media è lineare ma soprattutto commuta con le simmetrie del problema. Ora spiegherò meglio questo concetto.

Consideriamo il gruppo G delle rotazioni del cubo, ovvero

$$G = \{g \in SO(3) | g(\text{Cubo}) \subset \text{Cubo}\}$$

É ovvio che il problema è invariante per simmetria, ovvero se $g \in G$, allora vale

$$Tv = g^{-1}Tgv$$

Che è la formula di un cambio di base. Questo si può scrivere come

$$gT = Tg$$

Ovvero ci dice che $\forall g \in G$ le due operazioni commutano. Le due frasi precedenti sono state dette un po' alla garibaldina in quanto non è g ad agire sul cubo ma è una sua rappresentazione

¹⁰Che ha quindi 6 elementi

di grado $|F| = 6$. Di conseguenza è bene scrivere in modo formale che $\tau : G \rightarrow GL(V_\tau)$ è una rappresentazione del gruppo di rotazioni del cubo in \mathbb{C}^6 e questa rappresentazione commuta con un operatore T , ovvero

$$T\tau(g) = \tau(g)T \quad \forall g \in G$$

L'obiettivo che ci poniamo ora è quello di riuscire a scomporre τ come somma di rappresentazioni irriducibili in quanto una volta trovata una scomposizione

$$V_\tau = \bigoplus_{i=1}^n V_{\rho_i}$$

Allora potremo usare il lemma di Schur per dire che su ogni V_{ρ_i} l'operatore T si comporta come scalare ovvero è *più che diagonalizzato*. Per riuscire a capire qualcosa di come sono fatte le rappresentazioni di questo gruppo è opportuno prima cercare di dare una struttura più chiara a questo gruppo.

È possibile mostrare che QUALCUNO CHE HA VOGLIA DI FARLO LO FACCIA PLS $G \cong S_4$. A questo punto noi abbiamo una rappresentazione di grado 6 di S_4 che cerchiamo di scomporre come somma di rappresentazioni irriducibili. Tuttavia grazie al teorema 4.14 sappiamo che tutte le sottorappresentazioni di τ saranno isomorfe alle sottorappresentazioni della rappresentazione regolare $\mathcal{R}(S_4)$, di cui abbiamo preventivamente calcolato la tabella dei caratteri 2. Dato che

$$\tau = \sum_i n_i \rho_i \Rightarrow \chi_\tau = \sum_i n_i \chi_{\rho_i}$$

Andiamo a calcolare i prodotti scalari dei caratteri delle rappresentazioni irriducibili di S_4 con il carattere di τ per trovare quali rappresentazioni compaiono. Per farlo calcoliamo prima il carattere di τ

SCRIVI CHE NON HO VOGLIA

Per cui si ottiene

$$\tau = 1 + \epsilon\rho + \sigma$$

Ovvero

$$V_\tau = V_1 \oplus V_{\epsilon\rho} \oplus V_\sigma$$

Cerchiamo quindi di capire come sono fatti questi tre spazi che hanno rispettivamente dimensione 1,3,2.

SCRIVI PIÙ DETTAGLIATO CHE DEVO ANDARE A LEZIONE

$$V_1 = \text{Span}(e_1 + e_2 + \dots + e_6)$$

$$V_{\epsilon\rho} = \text{Le facce opposte hanno numeri opposti}$$

$$V_\sigma = \text{Le facce opposte hanno numeri uguali e la somma di tutti è 0}$$

Su questi spazi è facile vedere che effettivamente T è scalare. In particolare

$$\begin{cases} T|_{V_1} = 1 \\ T|_{V_{\epsilon\rho}} = 0 \\ T|_{V_\sigma} = -\frac{1}{2} \end{cases}$$

E quindi è evidente che $T^n \rightarrow$ su ogni faccia viene la media dei numeri che c'erano all'inizio.

6 Rappresentazioni reali, complesse e quaternioniche

Sono di un certo interesse le rappresentazioni su \mathbb{C} che possono essere espresse con matrici a coefficienti reali. Diamo una definizione precisa:

Definizione 6.1. Diciamo che una rappresentazione $\rho : G \rightarrow GL(V_\rho)$ del gruppo G è reale se esiste una base di V_ρ secondo la quale le matrici di $\rho(g)$, al variare di g nel gruppo, sono tutte a coefficienti reali.

Sia V un \mathbb{C} –spazio vettoriale di dimensione n . Denotiamo con $V^\mathbb{R}$ lo spazio vettoriale su \mathbb{R} che ha per “insieme di vettori” lo stesso di V , con la stessa somma ma chiaramente con prodotto per scalari ristretto ad \mathbb{R} . Osserviamo che se $\{v_1, \dots, v_n\}$ è una base di V allora $\{v_1, w_1, v_2, w_2, \dots, v_n, w_n\}$ è una base di $V^\mathbb{R}$, il quale di conseguenza ha dimensione $2n$. Se $\rho : G \rightarrow GL(V)$ è una rappresentazione del gruppo G , allora è definita in modo naturale una rappresentazione $\rho^\mathbb{R} : G \rightarrow GL(V^\mathbb{R})$, in cui gli il gruppo G agisce sullo spazio vettoriale esattamente come nella rappresentazione ρ (se G agisce in modo \mathbb{C} –lineare, a maggior ragione l’azione è \mathbb{R} –lineare).

Il fatto che ρ sia una rappresentazione reale è equivalente a chiedere l’esistenza di un sottospazio reale $V_0 \subset V^\mathbb{R}$ che sia stabile sotto l’azione di G e che abbia dimensione n . Cioè è possibile scomporre $V^\mathbb{R}$ come somma di sottorappresentazioni:

$$V^\mathbb{R} = V_0 \oplus iV_0$$

Esempio 6.1. Prendiamo come gruppo un gruppo ciclico, per esempio $\mathbb{Z}/3\mathbb{Z}$ ¹¹. Evidentemente tutte le rappresentazioni non banali di G non sono reali, in quanto sono di grado 1 e sono le radici dell’unità.

Non è difficile osservare che se indichiamo con $\alpha_{i,j}$ i coefficienti della matrice $\rho(g)$ rispetto alla base $\{v_1, \dots, v_n\}$, allora la matrice di $\rho^\mathbb{R}(g)$ rispetto alla base $\{v_1, w_1, \dots, v_n, w_n\}$ si ottiene ponendo al posto di $\alpha_{i,j}$ il blocchetto 2×2 :

$$\begin{pmatrix} \Re \alpha_{i,j} & -\Im \alpha_{i,j} \\ \Im \alpha_{i,j} & \Re \alpha_{i,j} \end{pmatrix}$$

dove \Re e \Im indicano parte reale e immaginaria. Dunque abbiamo il seguente risultato:

Proposizione 6.1. $\chi_{\rho^\mathbb{R}}(g) = \chi_\rho(g) + \chi_{\rho^*}(g)$

Dimostrazione. Basta ricordare che χ_{ρ^*} è il complesso coniugato di χ_ρ , dunque $\chi_\rho(g) + \chi_{\rho^*}(g) = 2\Re \chi_\rho(g)$ è evidentemente la traccia di $\rho^\mathbb{R}(g)$ per quanto detto sopra. \square

Proposizione 6.2. Se $\rho : G \rightarrow GL(V)$ è irriducibile (V è un \mathbb{C} –spazio vettoriale), allora ρ è reale se e solo se $\rho^\mathbb{R}$ è riducibile.

Dimostrazione. Se ρ è rappresentazione reale, sia $\{v_1, \dots, v_n\}$ una base di V tale che le matrici di $\rho(g)$ rispetto a tale base siano a coefficienti reali. Ora, $V^\mathbb{R}$ ha per base $\{v_1, w_1, \dots, v_n, w_n\}$. Indico con V_0 il sottospazio di $V^\mathbb{R}$ generato da $\{v_1, \dots, v_n\}$, che ha dimensione n . Ora, V_0 è G –invariante, dunque $\rho^\mathbb{R}$ è riducibile.

Viceversa, supponiamo che $V^\mathbb{R} = U \oplus W$ sia scomposizione di rappresentazioni con U e W diversi da $\{0\}$. A meno di scambiare U e W posso supporre $\dim U \leq n$. Il sottospazio di V generato dai vettori di U (con combinazioni lineari complesse) è G –invariante, dunque essendo ρ irriducibile tale sottospazio deve coincidere con V . Tutto ciò si traduce nel fatto che $V^\mathbb{R} = U + iU$,

¹¹Che per i fisici è isomorfo a C_3

e siccome $\dim \iota U = \dim U \leq n$ deve essere necessariamente che U e ιU sono in somma diretta e hanno entrambi dimensione n . Ora basta prendere una qualsiasi base di U , la quale è anche base di V (essendo costituita da n vettori che generano V) ed è tale che la matrice di $\rho(g)$ è a coefficienti reali per ogni $g \in G$, ovvero ρ è reale secondo la definizione 6.1. \square

Ora andremo a fare una classificazione delle rappresentazioni in 3 tipi diversi:

- Reali
- Complesse
- Quaternioniche

La classificazione verrà fatta in base all'esistenza o meno di forme bilineari di un certo tipo invarianti sotto G . Iniziamo con alcune proprietà soddisfatte dalle rappresentazioni reali:

Teorema 6.3. *Prendiamo una $\rho : G \rightarrow GL(V)$ rappresentazione $/\mathbb{C}$ che sia reale. Allora:*

1. $\chi_\rho(g) \in \mathbb{R} \ \forall g \in G$
2. V possiede una forma bilineare simmetrica G -invariante non nulla. Ovvero lo spazio delle forme bilineari simmetriche $S^2 V^* \subset V^* \otimes V^*$ è tale che $(S^2 V^*)^G \neq 0$.

Dimostrazione. Abbiamo supposto la rappresentazione reale. Quindi la matrice è reale ed in particolare lo sarà anche la sua traccia. Quindi il primo punto è vero. Ora veniamo al secondo punto: esisterà un V_0 spazio vettoriale reale G -invariante che tensorizzato con \mathbb{C} dia $V^\mathbb{R}$. Consideriamo ora una forma bilineare simmetrica B_0 non degenera $/\mathbb{R}$

$$B_0 \in S^2 V_0^*$$

Possiamo ora renderla invariante sotto l'azione di G con il solito metodo del fare la media. Consideriamo quindi \tilde{B}_0 definito come

$$\tilde{B}_0(v_1, v_2) = \frac{1}{|G|} \sum_{g \in G} B_0(\rho(g)v_1, \rho(g)v_2)$$

Questo ha le caratteristiche precedenti ed è anche invariante sotto G , ovvero $\tilde{B}_0 \in (S^2 V_0^*)^G$. Possiamo a questo punto estenderla a forma bilineare su V complessificandola in modo ovvio. Costruiamo quindi $B \in (S^2 V^*)^G$ definendola nel seguente modo:

$$B(v_1 + iv'_1, v_2 + iv'_2) = \left(\tilde{B}_0(v_1, v_2) - \tilde{B}_0(v'_1, v'_2) \right) + i \left(\tilde{B}_0(v'_1, v_2) + \tilde{B}_0(v_1, v'_2) \right)$$

È una banale verifica controllare che rispetta le caratteristiche richieste. \square

Osservazione. Supponiamo che $\rho : G \rightarrow GL(V)$ sia una rappresentazione irriducibile. Allora il fatto che esiste una forma bilineare G -invariante non nulla equivale a $(V^* \otimes V^*)^G \neq 0$. Ma ricordando che $(V^* \otimes V^*)^G \cong \text{Hom}(V, V^*)^G$ (che è l'insieme degli omomorfismi di rappresentazioni) ciò vuol dire che ρ e ρ^* sono isomorfi, il che si traduce in $\chi_\rho = \chi_{\rho^*}$. Ma questo avviene esattamente quando χ_ρ assume solo valori reali. Ciò significa che la seconda condizione trovata (che prevede l'esistenza di una forma bilineare simmetrica invariante) è strettamente più forte della prima (che è soddisfatta anche nel caso in cui esista una forma bilineare invariante non necessariamente simmetrica).

Vediamo ora un lemma che ci servirà per la classificazione.

Lemma 6.4. *Sia V una G -rappresentazione irriducibile $/\mathbb{C}$. Allora ogni forma bilineare non nulla G -invariante è non degenere. Inoltre, se esiste, è unica a meno di scalari, ovvero $\dim(V^* \otimes V^*)^G \leq 1$.*

Dimostrazione. Prendiamo un elemento $B \in (V^* \otimes V^*)^G$.

Ricordiamo che $V^* \otimes V^*$ e $\text{Hom}(V, V^*)$ sono G -rappresentazioni isomorfe. In particolare:

$$(V^* \otimes V^*)^G \cong \text{Hom}(V, V^*)^G$$

A questo punto, se esiste una forma bilineare non nulla invariante, questa corrisponde ad un omomorfismo di rappresentazioni $\phi : V \rightarrow V^*$. Per il lemma di Schur o ϕ è nullo o ϕ è un isomorfismo. Dato che la forma è non nulla, allora $\phi = \lambda \text{Id}$ con $\lambda \in \mathbb{C} \setminus \{0\}$. \square

Teorema 6.5. *Sia $\rho : G \rightarrow GL(V_\rho)$ una rappresentazione irriducibile $/\mathbb{C}$.*

Definiamo $m_\rho = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g^2)$ detto "indicatore di Frobenius-Schur". Allora

1. *Se $B \in (V^* \otimes V^*)^G$ allora $B \in S^2 V^*$ oppure $B \in \bigwedge^2 V^*$*
2. *$m_\rho \in \{-1, 0, 1\}$*
3.
 - *se $m_\rho = 0$ allora $(V^* \otimes V^*)^G = 0$*
 - *se $m_\rho = 1$ allora $(S^2 V^*)^G \neq 0$*
 - *se $m_\rho = -1$ allora $(\bigwedge^2 V^*)^G \neq 0$*

Dimostrazione. Indichiamo $W = (V^* \otimes V^*)^G$ lo spazio delle forme bilineari G -invarianti, che è sottorappresentazione di $V^* \otimes V^*$. Vogliamo dimostrare che $W \subseteq S^2 V^*$ oppure $W \subseteq \bigwedge^2 V^*$. Dal lemma precedente sappiamo che $\dim W \leq 1$. Se $\dim W = 0$ allora si ha automaticamente la tesi. Supponiamo ora $\dim W = 1$.

Ricordando che $V^* \otimes V^* \cong S^2 V^* \oplus \bigwedge^2 V^*$ è scomposizione in somma di rappresentazioni, consideriamo le proiezioni $p_{\text{sym}} : V^* \otimes V^* \rightarrow S^2 V^*$ e $p_{\text{alt}} : V^* \otimes V^* \rightarrow \bigwedge^2 V^*$ che in particolare sono omomorfismi di rappresentazioni (la verifica è facile, comunque questo accade ogni volta che si ha una somma di rappresentazioni).

Prendiamo ora $B \in W$ forma bilineare invariante non nulla. Allora almeno uno tra $p_{\text{sym}}(B)$ e $p_{\text{alt}}(B)$ è non nullo. Se fossero entrambi non nulli allora avremmo $\dim(V^* \otimes V^*)^G = \dim(S^2 V^*)^G + \dim(\bigwedge^2 V^*)^G \geq 2$, assurdo. Dunque B deve essere simmetrica oppure alternante, e ciò dimostra il punto 1.

Passiamo ora agli altri due punti. Ricordando il teorema 3.15 abbiamo che:

- $\dim(S^2 V^*)^G = \langle 1 | \chi_{S^2 \rho^*} \rangle = \frac{1}{|G|} \sum_{g \in G} \frac{\chi_\rho(g)^2 + \chi_\rho(g^2)}{2}$
- $\dim(\bigwedge^2 V^*)^G = \langle 1 | \chi_{\bigwedge^2 \rho^*} \rangle = \frac{1}{|G|} \sum_{g \in G} \frac{\chi_\rho(g)^2 - \chi_\rho(g^2)}{2}$
- $\dim(V^* \otimes V^*)^G = \langle 1 | \chi_{\rho^* \otimes \rho^*} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)^2$

dunque possiamo scrivere $\dim(S^2 V^*)^G = \frac{\dim(V^* \otimes V^*)^G + m_\rho}{2}$; $\dim(\bigwedge^2 V^*)^G = \frac{\dim(V^* \otimes V^*)^G - m_\rho}{2}$.

Ora, usando quanto ottenuto al punto 1 e distinguendo i casi in cui V ammetta una forma simmetrica invariante, una forma antisimmetrica invariante, oppure non ammetta forme invarianti, si ottiene facilmente quanto affermato ai punti 2 e 3. \square

Definizione 6.2 (Classificazione tramite l'indice di Frobenius). Sia $\rho : G \rightarrow GL(V)$ una rappresentazione irriducibile $/\mathbb{C}$: essa è detta

- **reale** se $m_\rho = 1$
- **complessa** se $m_\rho = 0$
- **quaternionica** se $m_\rho = -1$

Ma la nuova definizione che abbiamo dato è compatibile con la 6.1 data inizialmente? La rassicurante risposta è data dal seguente lemma.

Lemma 6.6. Sia $\rho : G \rightarrow GL(V_\rho)$ una rappresentazione irriducibile su \mathbb{C} . Allora ρ è reale secondo la definizione 6.1 se e solo se $m_\rho = 1$.

Dimostrazione. Sappiamo già che se ρ è reale nel senso 6.1 allora $m_\rho = 1$, in quanto V_ρ ammette una forma simmetrica invariante non nulla. Mostriamo il viceversa.

Sia $B \in (S^2 V_\rho^*)^G$, con $\dim_{\mathbb{C}} V_\rho = n$. Noi stiamo cercando un certo $V_0 \subset V_\rho$ spazio vettoriale su \mathbb{R} tale che $V_\rho^{\mathbb{R}} = V_0 \oplus iV_0$.

Prendiamo ora una certa forma $h : V_\rho \times V_\rho \rightarrow \mathbb{C}$ hermitiana, definita positiva e G -invariante. Questa sicuramente esiste, è stato dimostrato nel teorema 4.5. Definiamo a questo punto un endomorfismo di spazi vettoriali reali $\phi : V_\rho \rightarrow V_\rho$ imponendo che soddisfi $B(x, y) = h(x, \phi(y))$. La bontà di tale definizione è garantita dal teorema di Riesz.

Che proprietà ha ϕ ? Possiamo notare che ϕ è G -equivariante, ovvero vale $\phi(\rho(g)x) = \rho(g)\phi(x)$. Mostriamolo rapidamente

$$h(\phi(\rho(g)x), y) = B(\rho(g)x, y) = B(x, \rho(g^{-1})y) = h(\phi(x), \rho(g^{-1})y) = h(\rho(g)x, y)$$

Questo non è male, in quanto se ϕ fosse lineare avremmo subito che ϕ è un omomorfismo di rappresentazioni irriducibili e potremmo usare Schur. Tuttavia

$$\phi(z_1x_1 + z_2x_2) = \overline{z_1}\phi(x_1) + \overline{z_2}\phi(x_2) \quad \forall z_1, z_2 \in \mathbb{C}, \forall x_1, x_2 \in V_\rho$$

La linearità rispetto ai vettori è abbastanza evidente. L'antilinearità rispetto agli scalari deriva essenzialmente dal fatto che stiamo usando un prodotto hermitiano invece di un prodotto scalare. Infatti

$$h(\phi(zx), y) = B(zx, y) = B(x, zy) = h(\phi(x), zy) = \overline{z}h(\phi(x), y)$$

E quindi purtroppo ϕ non è davvero lineare come applicazione tra spazi vettoriali sul campo \mathbb{C} . Vediamo però che ϕ^2 si comporta meglio:

$$\phi^2(z_1x_1 + z_2x_2) = \phi(\overline{z_1}\phi(x_1) + \overline{z_2}\phi(x_2)) = z_1\phi^2(x_1) + z_2\phi^2(x_2) \quad \forall z_1, z_2 \in \mathbb{C}, \forall x_1, x_2 \in V_\rho$$

E quindi effettivamente ϕ^2 è un omomorfismo di rappresentazioni irriducibili. Per questo motivo possiamo applicare Schur e concludere che $\phi^2 = \lambda \text{Id}_{V_\rho}$ per un certo $\lambda \in \mathbb{C}$.

Cosa possiamo dire su λ ? Il claim è che sia $\lambda \in \mathbb{R}$ e $\lambda > 0$. Vediamo come si mostra

$$h(\phi(x), y) = B(x, y) = B(y, x) = h(\phi(y), x) = \overline{h(x, \phi(y))}$$

usando questo fatto possiamo considerare

$$\lambda h(x, y) = h(\phi^2(x), y) = \overline{h(\phi(x), \phi(y))} = h(x, \phi^2(y)) = \overline{\lambda} h(x, y) \quad \forall x, y \in V_\rho$$

E questo ci dice ovviamente che $\lambda \in \mathbb{R}$. Per mostrare ora che $\lambda > 0$ dobbiamo sfruttare il fatto che la nostra forma hermitiana sia definita positiva. Per questo motivo andiamo a considerare

$$\lambda h(x, x) = h(\phi^2(x), x) = \overline{h(\phi(x), \phi(x))} \Rightarrow \lambda = \frac{\overline{h(\phi(x), \phi(x))}}{h(x, x)} \quad \forall x \neq 0 \in V_\rho$$

E dato che h è definita positiva si ha anche $\lambda > 0$

A questo punto possiamo (a meno di riscalarlo) scegliere $\lambda = 1$, ovvero $\phi^2 = \text{Id}$. A questo punto ci piacerebbe tornare a fare cose con ϕ e non ϕ^2 . Notiamo che se ci restringiamo a spazi vettoriali su \mathbb{R} , allora anche ϕ è lineare in quanto il coniugio non ci dà fastidio. Dato che quindi ϕ è un endomorfismo di uno spazio vettoriale reale tale che $\phi^2 = 1$, allora ϕ è diagonalizzabile e ha solo gli autovalori ± 1 . Per questo motivo possiamo scomporre lo spazio di partenza $V_\rho = V_+ \oplus V_-$, con ovvia notazione per gli autospazi.

A questo punto ci manca poco. V_+ e V_- sono sottospazi reali del nostro spazio di partenza. Se mostriamo che sono isomorfi, abbiamo trovato la nostra scomposizione dello spazio V_ρ in due spazi $V_\rho = V_0 \oplus iV_0$. Proprio per questo motivo è intelligente notare che vale $iV_+ = V_-$. Mostriamo perché con il solito trucco della doppia inclusione. Prendiamo per esempio $x \in V_+$. Allora

$$\phi(ix) = -i\phi(x) = -ix$$

Ovvero il vettore ix è autovettore di ϕ con autovalore -1 . Applicando due volte questo ragionamento si ottiene facilmente

$$V_+ \cong V_- \quad (iV_+ = V_-)$$

Per cui a questo punto abbiamo finito □

Lemma 6.7. Sia $\rho : G \rightarrow GL(V)$ rappresentazione di un gruppo finito G . Allora $\dim V^G = \langle \chi_\rho | \chi_1 \rangle$

Dimostrazione. Definiamo un'applicazione lineare $R : V \rightarrow V$ nel seguente modo:

$$R = \frac{1}{|G|} \sum_{g \in G} \rho(g)$$

Se prendiamo $v \in V$ e $s \in G$ allora

$$\rho(s)R(v) = \rho(s) \frac{1}{|G|} \sum_{g \in G} \rho(g)v = \frac{1}{|G|} \sum_{g \in G} \rho(sg)v = R(v)$$

ovvero $R(v) \in V^G$. Inoltre se $w \in V^G$ allora $R(w) = w$. Di conseguenza $R^2 = R$ (cioè R è una cosiddetta *proiezione*) e quindi R si diagonalizza con autovalori 0 e 1. Inoltre l'autospazio relativo a 1 è proprio V^G . Ciò implica che

$$\dim V^G = \text{tr}(R) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) = \langle \chi_\rho | \chi_1 \rangle$$

□

Nota. Il proiettore R sopra trovato si chiama *proiettore di Reynolds*.

Lemma 6.8. $\rho : G \rightarrow GL(V)$ rappresentazione irriducibile $/\mathbb{C}$: allora χ_ρ è reale $\Leftrightarrow \rho$ è una rappresentazione reale o quaternionica.

Dimostrazione. Abbiamo visto prima che $(V^* \otimes V^*)^G \neq 0 \Rightarrow \chi_\rho = \chi_{\rho^*} \Rightarrow \chi_\rho$ è reale, e se ρ è reale o quaternionica ha proprio $(V^* \otimes V^*)^G$ diverso da 0. Viceversa χ_ρ reale implica $\chi_\rho = \chi_{\rho^*}$. D'altra parte dato che ρ e ρ^* sono entrambe rappresentazioni irriducibili allora $\rho \cong \rho^* \Leftrightarrow \chi_\rho = \chi_{\rho^*}$. Ciò significa che $\text{Hom}_G(V, V^*) \neq 0 \Rightarrow \exists B \in (V^* \otimes V^*)^G \Rightarrow \rho$ può essere solo reale o quaternionica. \square

Esercizio 6.1. Mostrare che tutte le rappresentazioni irriducibili $/_{\mathbb{C}}$ su S_4 sono reali.

Esercizio 6.2. Sia G gruppo ciclico di ordine dispari, allora le rappresentazioni non banali sono complesse.

Teorema 6.9. Sia $\rho : G \rightarrow GL(V)$ rappresentazione irriducibile $/_{\mathbb{R}}$: allora $\exists \sigma : G \rightarrow GL(V_\sigma)$ rappresentazione irriducibile $/_{\mathbb{C}}$ tale che è vera una delle seguenti affermazioni:

1. $\chi_\rho = \chi_\sigma$;
2. $\chi_\rho = \chi_\sigma + \chi_{\sigma^*}$;
3. $\chi_\rho = 2\chi_\sigma$.

Dimostrazione. Definisco $V^{\mathbb{C}} = \mathbb{C} \otimes V$ la complessificazione di V (è semplicemente V visto però come spazio vettoriale su \mathbb{C}). Vi sono due casi:

1. $\rho : G \rightarrow GL(V^{\mathbb{C}})$ (che chiamiamo $\rho^{\mathbb{C}}$ solo per ricordarci che V è visto come spazio vettoriale sui complessi) è una rappresentazione irriducibile $/_{\mathbb{C}}$;
2. $\rho^{\mathbb{C}} : G \rightarrow GL(V^{\mathbb{C}})$ è una rappresentazione riducibile $/_{\mathbb{C}}$.

Se siamo nel primo caso $\sigma = \rho^{\mathbb{C}}$ è irriducibile $/_{\mathbb{C}}$ e ovviamente $\chi_\rho = \chi_{\rho^{\mathbb{C}}}$.

Se siamo nel secondo caso allora $V^{\mathbb{C}} = U \oplus W$ con U e W sottospazi G -invarianti. Quindi $\rho^{\mathbb{C}} = \rho_U + \rho_W$. Passiamo ora alla loro realificazione: $(\rho_{\mathbb{C}})^{\mathbb{R}} = (\rho_U)^{\mathbb{R}} + (\rho_W)^{\mathbb{R}}$. Tuttavia sapendo che $\rho_{\mathbb{C}}$ derivava da una rappresentazione reale allora $\rho_{\mathbb{C}}^{\mathbb{R}} = \rho + \rho$ derivante dalla scomposizione $V^{\mathbb{R}} = V + iV$ dunque si ha

$$\rho + \rho = \rho_U^{\mathbb{R}} + \rho_W^{\mathbb{R}} \Rightarrow \rho = \rho_U^{\mathbb{R}}$$

poichè le ρ sono irriducibili e non si possono ulteriormente spezzare quindi devono essere contenute interamente in un sottospazio invariante. Analogamente se ρ_U fosse ancora riducibile avrei una scrittura di ρ come somma di due rappresentazioni più piccole, il che è assurdo. Quindi la σ irriducibile su \mathbb{C} cercata è ρ_U . Da questo deduciamo che $\dim(U) = \dim(W) = \frac{n}{2}$ e quindi deduciamo che se la dimensione di V è dispari allora ρ su \mathbb{C} è irriducibile. Dato che $\sigma^{\mathbb{R}} = \rho \Rightarrow \chi_\rho = \chi_\sigma + \chi_{\sigma^*}$ per la proposizione 6.1. Se $\sigma \cong \sigma^*$ allora si è nel terzo caso (ovvero quando il carattere di σ è reale). \square

6.1 Quaternioni

Ovviamente le rappresentazioni quaternioniche hanno a che fare con il corpo dei quaternioni. Vediamo un po' di caratteristiche interessanti di questo oggetto.

Il corpo \mathbb{H} si può vedere come

$$\mathbb{H} = \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$$

Con i, j, k unità immaginarie che rispettano le seguenti regole

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = -ji = k \\ jk = -kj = i \\ ki = -ik = j \end{cases}$$

Vediamo un po' di proprietà interessanti. Per esempio se consideriamo

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

allora questo insieme è un gruppo se munito della moltiplicazione. Possiamo andare a vedere la tabella dei caratteri di questo gruppo.

Per farlo possiamo utilizziamo il secondo metodo descritto nel paragrafo (??). Consideriamo i seguenti sottogruppi di Q_8

$$H_1 = \{\pm 1, \pm i\}$$

$$H_2 = \{\pm 1, \pm j\}$$

$$H_3 = \{\pm 1, \pm k\}$$

È semplice verificare che H_i è normale in Q_8 per $i = 1, 2, 3$ e che $Q_8/H_i \cong \mathbb{Z}_2$ ¹². Di \mathbb{Z}_2 conosciamo le rappresentazioni di grado 1: c'è la rappresentazione banale (che induce su G la rappresentazione banale appunto) e $\rho : \mathbb{Z}_2 \rightarrow \mathbb{C}^*$ che manda $[1]_2 \rightarrow -1$. Da quest'ultima otteniamo le rappresentazioni che indicheremo con ρ_i, ρ_j, ρ_k rispettivamente nel caso in cui quozientiamo per H_1, H_2, H_3 ; vediamo ora come calcolare una di queste, per esempio ρ_i , riportando il diagramma degli omomorfismi.

$$\begin{array}{ccc} Q_8 & \xrightarrow{\pi_1} & Q_8/H_1 \\ & \searrow \rho_i & \downarrow \rho \\ & & \mathbb{C}^* \end{array}$$

Sia $g \in Q_8$, vogliamo capire quanto fa $\rho_i(g)$, ci sono due casi da considerare:

1. se $g \in H_1$, allora $\pi(g) = eH_1$ dunque, visto che eH_1 è l'identità nel quoziente, $\rho_i(g) = 1$
2. se $g \notin H_1$, allora $\pi(g) = gH_1 \neq eH_1$, quindi, per la definizione di ρ , $\rho_i(g) = -1$

L'ultima rappresentazione che si trova deve avere dimensione 2 perché abbiamo già trovato 4 rappresentazioni di grado 1 (quella banale più le tre ρ_i, ρ_j, ρ_k essendo tutte non isomorfe¹³), abbiamo inoltre esaurito le rappresentazioni di grado 1: potremmo ancora quozientare per $H = \{1, -1\}$, ma si vede abbastanza facilmente che $Q_8/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, mentre avevamo detto che cercavamo quozienti ciclici; dalla formula $\sum n_i^2 = |Q_8| = 8$ si deduce quindi che l'ultima rappresentazione deve avere grado 2. Quest'ultima si ottiene dalla rappresentazione matriciale dei quaternioni: è noto che i quaternioni possono essere presentati come un sottoinsieme delle matrici complesse 2×2 :

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}$$

La rappresentazione è determinata dall'omomorfismo $\rho_{\mathbb{H}} : Q_8 \rightarrow GL(\mathbb{C}^2)$ definito sui generatori:

$$\rho_{\mathbb{H}}(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \rho_{\mathbb{H}}(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Quindi vediamo che gli elementi di Q_8 possono essere visti come matrici 2×2 complesse:

$$1_{\mathbb{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i_{\mathbb{H}} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad j_{\mathbb{H}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad k_{\mathbb{H}} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Queste 4 matrici prendono il nome di matrici di spin di Pauli in quanto hanno alcune applicazioni in Fisica. Possiamo infine ricostruire quindi la tabella dei caratteri di Q_8

¹²Visto che gli H_i sono normali, Q_8/H_i è un gruppo, avendo solo due elementi è necessariamente \mathbb{Z}_2 .

¹³La verifica è immediata

	1	1	2	2	2
Q_8	1	-1	$\pm i$	$\pm j$	$\pm k$
ρ_1	1	1	1	1	1
ρ_i	1	1	1	-1	-1
ρ_j	1	1	-1	1	-1
ρ_k	1	1	-1	-1	1
$\rho_{\mathbb{H}}$	2	-2	0	0	0

Tabella 3: Tabella dei caratteri di Q_8

É interessante notare che la tabella dei caratteri di Q_8 è uguale a quella di D_4 , ma i due gruppi non sono isomorfi. Questo ci ricorda che la tabella dei caratteri dice tanto di un gruppo ma non tutto.

Ora vorremmo effettivamente capire il perché dei nomi dati nella classificazione delle rappresentazioni come reali, complesse e quaternioniche. Per questo motivo ci servono un paio di concetti di algebra.

Definizione 6.3 (Algebra). Un'algebra su \mathbb{R} è uno spazio vettoriale reale A dotato di una moltiplicazione $\cdot : A \times A \rightarrow A$ che sia associativa e bilineare. Inoltre imponiamo che vi sia un elemento neutro rispetto a questa moltiplicazione. Quest'ultima richiesta non fa parte della più generale definizione di algebra (le algebre che la soddisfano si dicono *unitarie*), ma noi la inseriamo nella definizione poiché in questo corso non tratteremo mai algebre non unitarie.

Definizione 6.4 (Algebra di divisione). Un'algebra di divisione è un'algebra in cui ogni elemento escluso lo 0 possiede un inverso moltiplicativo.

Esempio 6.2. Gli esempi più standard di algebra di divisione su \mathbb{R} di dimensione finita sono i campi \mathbb{R} e \mathbb{C} come spazi vettoriali reali. Un esempio più sofisticato è dato dal corpo dei quaternioni \mathbb{H} (ovviamente visto come spazio vettoriale su \mathbb{R}).

Osservazione. Consideriamo una rappresentazione irriducibile $\rho : G \rightarrow GL(V_\rho)$ con V_ρ spazio vettoriale su \mathbb{R} . Allora l'insieme degli endomorfismi di ρ

$$\text{End}_G(V_\rho)$$

è un'algebra di divisione su \mathbb{R} se dotato della composizione. Infatti per lemma di Schur (in particolare la prima parte dell'enunciato, che vale su ogni campo) ogni elemento di $\text{End}_G(V_\rho)$ o è la funzione nulla oppure è un isomorfismo, quindi ammette inverso. Se $\dim V_\rho = n$ allora $\text{End}_G(V_\rho)$, essendo contenuto in $\text{End}(V_\rho)$, ha dimensione finita, in particolare $\dim \text{End}_G(V_\rho) \leq n^2$. Vedremo tuttavia che vale una limitazione molto più forte.

Presentiamo ora un sorprendente teorema che afferma che non ci sono altre algebre di divisione di dimensione finita su \mathbb{R} oltre a quelle che abbiamo elencato come esempi, ovvero $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

Teorema 6.10 (di Frobenius). *Sia A un'algebra di divisione su \mathbb{R} di dimensione finita. Allora si ha*

$$A \cong \mathbb{R} \quad \vee \quad A \cong \mathbb{C} \quad \vee \quad A \cong \mathbb{H}$$

Dimostrazione. Indichiamo con $\mathbf{1} \in A$ l'elemento neutro rispetto alla moltiplicazione di A (occhio: è un vettore di A , non un numero reale). Il sottospazio vettoriale generato da $\mathbf{1}$ è chiaramente isomorfo ad \mathbb{R} come \mathbb{R} -spazio vettoriale, ma in realtà lo è anche come sottoalgebra: infatti se $a, b \in \mathbb{R}$ allora

$$a\mathbf{1} \cdot b\mathbf{1} = ab(\mathbf{1} \cdot \mathbf{1}) = ab\mathbf{1}$$

dove nel primo passaggio abbiamo usato la bilinearità e nel secondo il fatto che $\mathbf{1}$ è elemento neutro. Dunque, con un lieve abuso di notazione, possiamo scrivere $\mathbb{R} \subseteq A$, intendendo per \mathbb{R} proprio il sottospazio generato da $\mathbf{1}$. Se $\dim A = 1$ allora sarebbe $A = \mathbb{R}$. D'ora in poi supponiamo $\dim A > 1$.

Vogliamo ora mostrare che esiste una sottoalgebra di A isomorfa a \mathbb{C} . Sia $\alpha \in A \setminus \mathbb{R}$ e indichiamo con $A[\alpha]$ la sottoalgebra generata da α , ovvero consideriamo l'insieme

$$A[\alpha] = \left\{ \sum_{n=0}^N a_n \alpha^n \mid N \in \mathbb{N}, a_i \in \mathbb{R}, \alpha \in A \right\}$$

L'algebra $A[\alpha]$, essendo contenuta in A , ha necessariamente dimensione finita, quindi esisterà un certo N per cui gli elementi $\alpha^0, \alpha^1, \dots, \alpha^N$ sono linearmente dipendenti. Più precisamente prendiamo il minimo N per cui questo avviene. Allora esistono dei coefficienti a_n reali tali che

$$\sum_{n=0}^N a_n \alpha^n = 0$$

Ovvero il polinomio a coefficienti reali

$$p(x) = \sum_{n=0}^N a_n x^n$$

è annullato da α . Se potessimo scomporre in modo non banale $p(x) = p_1(x)p_2(x)$ allora avremmo che $0 = p_1(\alpha)p_2(\alpha)$, dunque α annullerebbe uno dei due fattori (qui stiamo usando che A è un'algebra unitaria), il che sarebbe assurdo vista l'ipotesi di minimalità di N . Dunque $p(x)$ deve essere irriducibile. Ma su \mathbb{R} i polinomi irriducibili possono solo avere grado 1 o 2. Vediamo rapidamente perché non può avere grado 1. Supponiamo per assurdo che sia

$$p(x) = a_0 + a_1 x$$

Ma ciò vorrebbe dire che $a_0 + a_1 \cdot \alpha = 0$, ovvero $\alpha = -a_0/a_1 \in \mathbb{R}$, ma noi avevamo assunto $\alpha \notin \mathbb{R}$. Di conseguenza $p(x)$ ha grado esattamente 2. Non è difficile mostrare che $A[\alpha]$ ha esattamente dimensione 2: se α^2 si scrive in termini di potenze inferiori lo faranno anche tutte le potenze successive, dunque ogni elemento di $A[\alpha]$ si può scrivere nella forma $x + \alpha y$ con x, y reali e $\{1, \alpha\}$ è base di $A[\alpha]$, essendo i due elementi indipendenti. A meno di moltiplicare $p(x)$ per una costante per renderlo monico, possiamo scrivere

$$p(x) = (x - s)^2 + t^2$$

con s, t reali, $t \neq 0$. Se definiamo

$$i = \frac{\alpha - s}{t}$$

è facile osservare che $i^2 = -1$. Ora $\{1, i\}$ è base di $A[\alpha]$ (essendo 1 e i linearmente indipendenti) e il nostro i gioca esattamente lo stesso ruolo dell'unità immaginaria in \mathbb{C} . A questo punto è immediato esibire un isomorfismo

$$A[\alpha] \cong \mathbb{C}$$

Se $\dim A = 2$ abbiamo finito. Supponiamo d'ora in poi $\dim A > 2$ e scriviamo $\mathbb{C} \subset A$ identificando \mathbb{C} con la sottoalgebra $A[\alpha]$. Definiamo ora un'applicazione $\varphi : A \rightarrow A$ nel modo seguente:

$$\varphi(x) = -ixi = x i^{-1}$$

Osserviamo che φ è \mathbb{R} -lineare, infatti presi $a, b \in \mathbb{R}$ e $x, y \in A$ si ha:

$$\varphi(ax + by) = i(ax + by)i^{-1} = i(ax)i^{-1} + i(by)i^{-1} = a\varphi(x) + b\varphi(y)$$

Inoltre osserviamo che φ^2 è l'identità. Questo implica che possiamo decomporre

$$A = A_+ \oplus A_-$$

dove A_+ e A_- sono gli autospazi relativi rispettivamente agli autovalori 1 e -1 . In particolare gli elementi di A_+ sono esattamente quelli che commutano con i . Vogliamo ora mostrare che $A_+ = \mathbb{C}$. Sia $\beta \in A_+$. Imitando il ragionamento fatto prima con α , possiamo considerare il polinomio a coefficienti complessi di minimo grado che si annulla in β . Come fatto prima osserviamo che deve essere irriducibile (questo passaggio richiede in realtà qualche cautela, ma tutto funziona come deve poiché β commuta con tutti gli elementi di \mathbb{C} . Se avessimo preso $\beta \in A_-$ il ragionamento sarebbe errato). Ma gli unici polinomi irriducibili a coefficienti in \mathbb{C} sono quelli di grado 1, quindi $\beta \in \mathbb{C}$.

Abbiamo dunque stabilito che $A_+ = \mathbb{C}$. Dato che $\dim A > 2$ possiamo prendere $z \in A_-$ non nullo. Consideriamo l'applicazione $\psi_z : A \rightarrow A$ definita da $\psi_z(x) = zx$. Osserviamo che valgono le seguenti implicazioni:

$$x \in A_+ \implies \varphi(\psi_z(x)) = \varphi(zx) = izxi^{-1} = izi^{-1}ixi^{-1} = -zx = -\psi_z(x)$$

$$x \in A_- \implies \varphi(\psi_z(x)) = \varphi(zx) = izxi^{-1} = izi^{-1}ixi^{-1} = (-z)(-x) = \psi_z(x)$$

ovvero ψ_z scambia A_+ e A_- . Inoltre ψ_z è bigettiva e lineare, dunque concludiamo che $A_+ \cong A_-$ come \mathbb{R} -spazi vettoriali e in particolare $\dim A = 4$.

Con un ragionamento simile a quello che avevamo fatto per α , osserviamo che z^2 è nel sottospazio generato da 1 e z . Inoltre $z^2 = \psi_z(z) \in A_+$. Visto che $\text{Span}(1, z) \cap A_+ = \mathbb{R}$ deve essere per forza $z^2 \in \mathbb{R}$.

Se fosse $z^2 \geq 0$ allora potremmo scrivere $z^2 = r^2$ per qualche $r \in \mathbb{R}$. Visto che r e z commutano sarebbe allora $(z - r)(z + r) = 0$, dunque uno dei due fattori sarebbe 0, assurdo perché $z \notin \mathbb{R}$. Pertanto $z^2 < 0$ e possiamo definire

$$j = \frac{z}{\sqrt{-z^2}}$$

così $j^2 = -1$. Infine definiamo $k = ij$.

Ora k e j sono indipendenti e sono in A_- , dunque formano una base di A_- . Allora $\{1, i, j, k\}$ è base per A ed è facile verificare che questi quattro elementi rispettano le stesse regole di moltiplicazione dei quaternioni, pertanto si conclude che $A \cong \mathbb{H}$ e la tesi è dimostrata. \square

Dal teorema precedente si ha immediatamente che se $G \rightarrow GL(V)$ è una rappresentazione irriducibile su \mathbb{R} allora $\text{End}_G(V)$ è isomorfo a uno tra $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

Proposizione 6.11. *Sia $\rho : G \rightarrow GL(V)$ rappresentazione irriducibile su \mathbb{R} . Allora:*

- $\text{End}_G(V) \cong \mathbb{R}$ se e solo se $\langle \chi_\rho | \chi_\rho \rangle = 1$
- $\text{End}_G(V) \cong \mathbb{C}$ se e solo se $\langle \chi_\rho | \chi_\rho \rangle = 2$
- $\text{End}_G(V) \cong \mathbb{H}$ se e solo se $\langle \chi_\rho | \chi_\rho \rangle = 4$

Dimostrazione. Basta ricordare che $\dim \text{End}_G(V) = \langle \chi_\rho | \chi_\rho \rangle$ e la tesi segue subito dal teorema di Frobenius. \square

7 Rappresentazioni indotte

Supponiamo di avere $\rho : H \rightarrow GL(V)$ una rappresentazione di $H < G$ con G gruppo. Il nostro obiettivo è quello di definire una $\tilde{\rho} : G \rightarrow GL(V)$ rappresentazione di G che estende ρ .

Definizione 7.1. Indichiamo con *induzione da H in G di W* il seguente spazio vettoriale:

$$\text{Ind}_H^G(W) = \{f : G \rightarrow W : \rho(h) \circ f(gh) = f(g) \ \forall (g, h) \in G \times H\}$$

Osservazione. $\text{Ind}_H^G(W)$ è lo spazio vettoriale di una rappresentazione di G . Si consideri $N = \{f : G \rightarrow W\}$: definisco

$$\rho_N : G \rightarrow GL(N) \text{ tale che } (\rho_N(g)f)(g') = f(g^{-1}g')$$

Si verifica che ρ_N è una rappresentazione di G su N . Notiamo innanzitutto che $\text{Ind}_H^G(W) \subseteq N$ e che tale sottospazio è ρ_N -invariante poichè detta $f \in \text{Ind}_H^G(W)$ si ha che

$$\rho_N(g)(f)(g') = f(g^{-1}g') = \rho(h)f(g^{-1}g'h) = \rho(h)\rho_N(g)(f)(g'h)$$

ovvero $\rho_N(g)f \in \text{Ind}_H^G(W)$. Questo ci dice che $\text{Ind}_H^G(W)$ è una sottorappresentazione di ρ_N che chiamiamo $\rho_{ind} : G \rightarrow GL(\text{Ind}_H^G(W))$.

Esempio 7.1. $H = \{e\}$ e $W = \mathbb{C}$ con $\rho : H \rightarrow GL(\mathbb{C})$: allora

$$\text{Ind}_H^G(W) = \{f : G \rightarrow \mathbb{C} : \rho(e)f(ge) = f(g)\} = \{f : G \rightarrow \mathbb{C}\}$$

Notazione: Spesso indicheremo lo spazio vettoriale $\{f : G \rightarrow \mathbb{C}\}$ con $\mathbb{C}[G] = \bigoplus_{g \in G} \mathbb{C}e_g$ dove gli $\{e_g\}_{g \in G}$ sono una base di $\{f : G \rightarrow \mathbb{C}\}$. In tal modo risulta che

$$\{f : G \rightarrow W\} = \mathbb{C}[G] \otimes W$$

sempre nel senso che se prendo $\{e_g\}_{g \in G}$ una base di $\mathbb{C}[G]$ e $\{w_i\} \in W$ una base di W allora

$$e_g \otimes w_i : G \rightarrow W \text{ tale che } g \mapsto w_i \text{ e } g' \mapsto 0 \ \forall g' \neq g$$

Torniamo a ρ_{ind} : ricapitolando $\rho_{ind} : G \mapsto GL(\text{Ind}_H^G(W))$ tale che $g \mapsto \rho_{ind}(g)$ dove $\rho_{ind}(g)f(g') = f(g^{-1}g')$. Vediamo ora un po' delle sue caratteristiche. Poniamo per snellire la scrittura $V = \text{Ind}_H^G(W)$. Ricordandoci il nostro aim, di certo vogliamo che W sia un sottospazio di V .

Definizione 7.2. Data $f \in \{f : G \rightarrow W\}$ (che contiene V) definiamo il supporto di f

$$\text{Supp}(f) = \{g \in G : f(g) \neq 0\}.$$

Definizione 7.3. Dato $g \in G$ definiamo $V_g = \{f \in V : \text{Supp}(f) \subseteq gH\}$.

Osservazione. se $g' \in gH$, allora $g'H = gH \Rightarrow V_g = V_{g'}$. Quindi più che dipendere dagli elementi di G , gli insiemi sopra definiti dipendono dalle classi laterali di H in G . Perciò ora parleremo non più di V_g bensì di V_{gH} .

Osservazione. dato che le classi laterali di H sono una partizione di G , dette $\{g_iH\}_{i \in |G/H|}$ i rappresentanti delle classi laterali gH al variare di g in G allora

$$G = \bigsqcup_{i=1}^{|G/H|} g_iH$$

e quindi ogni funzione la posso scrivere come combinazione lineare di $f_i \in V_{g_iH}$.

$$\Rightarrow V = \bigoplus_{i=1}^{|G/H|} V_{g_iH}$$

Voglio ora rintracciare W , in quanto sono interessato a trovare un sottospazio isomorfo a W dentro V . Notiamo innanzitutto che la scrittura precedente non è detto che sia una decomposizione di rappresentazioni, ma possiamo vedere subito che si comporta bene sotto l'azione di ρ_{ind} .

Lemma 7.1. ρ_{ind} permuta le varie V_{gH} nel senso che $\rho_{ind}(g)V_{g'H} = V_{gg'H}$.

Dimostrazione. Data $f \in V$, definisco

$$f_i(g) = \begin{cases} f(g) & \text{se } g \in g_i H \\ 0 & \text{altrimenti} \end{cases} \Rightarrow f = \sum_{i=1}^{|G/H|} f_i \quad \text{e per come le ho definite } f_i \in V_{g_i H}$$

Sia ora $f \in V_{g'H}$ e fissiamo un $g \in G$ allora

$$\rho_{ind}(g)(f)(x) = f(g^{-1}x) \Rightarrow \rho_{ind}(g)(f)(x) \neq 0 \Leftrightarrow g^{-1}x \in \text{Supp}(f) \subseteq g'H \Leftrightarrow x \in g \text{Supp}(f) \subseteq gg'H$$

Ovvero $x \in \text{Supp}(\rho_{ind}(g)(f)) \Leftrightarrow x \in g \text{Supp}(f)$. Ciò implica che

$$\begin{array}{ccc} & \xrightarrow{\rho_{ind}(g)} & \\ V_{g'H} & & V_{gg'H} \\ & \xleftarrow{\rho_{ind}(g^{-1})} & \end{array}$$

Essendo $\rho_{ind}(g), \rho_{ind}(g^{-1}) \in GL(V)$ allora seguono i seguenti fatti:

1. $\rho_{ind}(g)V_{g'H} \subseteq V_{gg'H}$;
2. $\rho_{ind}(g^{-1})V_{gg'H} \subseteq V_{g'H}$;
3. $V_{g'H} \cong V_{gg'H}$, ovvero sono due spazi vettoriali isomorfi;
4. $\rho_{ind}(g)^{-1} = \rho_{ind}(g^{-1})$;

Quindi $\rho_{ind}(g)V_{g'H} = V_{gg'H}$. □

Corollario.

$$\forall i, j \in |G/H| \quad V_{g_i H} \cong V_{g_j H}.$$

In particolare hanno tutti la stessa dimensione e quindi

$$\dim(V) = |G/H| \dim(V_{eH}) = \dim(\text{Ind}_H^G(W))$$

Concentriamoci ora su $V_{eH} = \{f \in V : \text{supp}(f) \subseteq H\}$. Sia $h \in H$: allora $\rho_{ind}(h) : V_{eH} \rightarrow V_{eH}$ in quanto $eH = hH$. Ciò significa che $\rho_{ind}|_H$ definisce una rappresentazione di H in V_{eH} .

Lemma 7.2. La rappresentazione appena trovata di H su V_{eH} è naturalmente isomorfa a $\rho : H \rightarrow GL(W)$.

Dimostrazione. Considero la seguente funzione:

$$\Phi : V_{eH} \rightarrow W \quad \text{tale che } f \mapsto f(e)$$

ovvero la funzione che associa ad un f la valutazione della stessa nell'elemento neutro. Verifichiamo innanzitutto che si tratta di un omomorfismo di rappresentazione. Ricordiamo chi è V_{eH} :

$$V_{eH} = \{f : G \rightarrow W : \rho(h)f(gh) = f(g) \quad \forall h, g \quad \text{e} \quad \text{Supp}(f) \subseteq H\}$$

Φ è un omomorfismo di rappresentazioni se e solo se $\Phi(\rho_{ind}(h)f) = \rho(h)\Phi(f) \forall h \in H$.

$$\Phi(\rho_{ind}(h)f) = \rho(h)\Phi(f) \Leftrightarrow (\rho_{ind}(h)f)(e) = \rho(h)(f(e)) \Leftrightarrow f(h^{-1}e) = f(h^{-1}) = \rho(h)f(e)$$

ma ciò è vero in quanto $f \in \text{Ind}_H^G(W)$.

Verifichiamo che Φ è iniettiva. $\text{Supp}(f) \subseteq H$ e $\forall h \in H f(h) = \rho(h^{-1}f(e))$: questo mi dice che una volta che si è fissato il valore di $f(e)$ allora la funzione è univocamente determinata su H . D'altra parte so che in $G \setminus H$ la funzione è identicamente nulla \Rightarrow quindi è univocamente determinata su tutto G . Allora detti Φ è iniettiva.

Vediamo ora che è anche surgettiva. Sia $w \in W$ vogliamo $f \in V_{eH}$ che valutata in e dia w . Definiamo $f_w : G \rightarrow W$ nel seguente modo:

$$f_w := \begin{cases} \rho(h^{-1})(w) & \text{se } h \in H \\ 0 & \forall g \in G \setminus H \end{cases}$$

Si verifica che tale funzione soddisfa le proprietà richieste. □

Dunque possiamo ora concludere il seguente teorema

Teorema 7.3. *Detto $g_1H, \dots, g_{|G/H|}H$ i rappresentanti delle classi laterali allora*

$$\text{Ind}_H^G(W) = \bigoplus_{i=1}^{|G/H|} \rho_{ind}(g_i)V_{eH} (= \bigoplus_{i=1}^{|G/H|} V_{g_iH})$$

Inoltre $\rho_{ind}|_H$ definisce una rappresentazione di H su V_{eH} isomorfa a ρ . In particolare quindi

$$\dim(\text{Ind}_H^G(W)) = |G/H| \dim(W)$$

Vediamo ora degli esempi.

1. Abbiamo visto prima $H = \{e\}$ $W = \mathbb{C}$ allora $\text{Ind}_H^G(W) = \mathbb{C}[G]$ è la rappresentazione regolare di G .
2. $H \neq \{e\}, \subseteq G$ e $\rho : H \rightarrow GL(W)$ la rappresentazione banale con $W = \mathbb{C}$. Allora

$$\text{Ind}_H^G(\mathbb{C}) = \{f : G \rightarrow \mathbb{C} : \rho(h)f(gh) = f(gh) = f(g) \forall g, h\}$$

allora $f \in \text{Ind}_H^G(\mathbb{C})$ se e solo se è costante sulle classi laterali di H

quindi $\text{Ind}_H^G(\mathbb{C}) = \{f : G \rightarrow \mathbb{C} : f \text{ è costante sulle classi laterali di } H\} = \mathbb{C}[G/H]$

$$\begin{array}{ccc} G & \xrightarrow{f} & \mathbb{C} \\ \pi \downarrow & \nearrow f \circ \pi & \\ G/H & & \end{array}$$

G/H è un insieme finito dove G agisce per moltiplicazione a sinistra ($g(g'H) = gg'H$). Quindi $\text{Ind}_H^G(W)$ è la rappresentazione per permutazione associata all'azione di G in G/H .

Recall: X è un G -insieme, sia $X = \bigsqcup X_i$ la decomposizione in G -orbite: allora

$$\mathbb{C}[X] = \bigoplus_{i=1}^{\#-orbite} \mathbb{C}[X_i]$$

3. $H \subseteq G$ e $\rho : H \rightarrow GL(W) : \rho(h) = id \ \forall h \in H$. Nel caso in cui W avesse dimensione 1 si torna all'esempio 1. Tuttavia anche se $\dim(W) > 1$, $\text{Ind}_H^G(W) = \{f : G \rightarrow \mathbb{C} : f \text{ è costante sulle classi laterali di } H\} = \mathbb{C}[G/H] \otimes W$

Esercizio 7.1. Supponiamo che $W = W_1 \oplus W_2$ una rappresentazione di H non riducibile: allora

$$\text{Ind}_H^G(W) = \text{Ind}_H^G(W_1) \oplus \text{Ind}_H^G(W_2)$$

7.1 Formula di aggiunzione

Vediamo ora una proprietà universale di queste rappresentazioni indotte. Prima abbiamo definito passando da ρ a ρ_{ind} sostanzialmente una applicazione

$$\text{Ind} : \text{Rappr}(H) \rightarrow \text{Rappr}(G)$$

e abbiamo anche "l'inversa" ovvero la restrizione della rappresentazione ad H

$$\text{Res} : \text{Rappr}(G) \rightarrow \text{Rappr}(H)$$

e risulta che $\text{Res}_H^G(V) = V$ visto però come una rappresentazione di H ($\rho_{res} = \rho|_H$). Che legame c'è tra queste due applicazioni?

Teorema 7.4. Sia $\rho : H \rightarrow GL(W)$ una rappresentazione di H e sia $\sigma : G \rightarrow GL(U)$ una rappresentazione di G . Allora

$$\text{Hom}_H(W, \text{Res}_H^G(U)) \cong \text{Hom}_G(\text{Ind}_H^G(W), U)$$

ovvero che ogni $\phi : W \rightarrow \text{Res}_H^G(U)$ omomorfismo di H -rappresentazione si estende in modo unico a un $\hat{\phi} : \text{Ind}_H^G(W) \rightarrow U$ omomorfismo di G -rappresentazione

Dimostrazione. sia $\phi : W \rightarrow \text{Res}_H^G(U)$ un omomorfismo di H -rappresentazione e sia $V := \text{Ind}_H^G(W) = \bigoplus_{i=1}^{\#-orbite} \rho_{ind}(g_i)V_{eH}$. Essendo $V_{eH} \cong W$ come H -rappresentazioni, allora $\phi : V_{eH} \rightarrow \text{Res}_H^G(U)$: voglio estenderlo a V . Essendo V definito come una somma diretta è sufficiente definire l'omomorfismo sui blocchi e per questo considero V_{g_iH} : ho che

$$V_{g_iH} \xrightarrow{\rho_{g_i}^{-1}} V_{eH} \xrightarrow{\phi} \text{Res}_H^G(U) \xrightarrow{\sigma(g)} U \Rightarrow \sigma(g)\phi\rho_{ind}(g_i^{-1}) : V_{g_iH} \rightarrow U$$

Incollando tutte queste applicazioni ottengo $\hat{\phi} : \text{Ind}_H^G(W) \rightarrow U$ dove $\hat{\phi}(v) = \sigma_g \circ \phi \circ \rho_{ind}(g^{-1})(v)$ con $v \in V_{gH}$. Si verifica che $\hat{\phi} \in \text{Hom}_G(\text{Ind}_H^G(W), U)$.

Vediamo ora che questa estensione è unica. Siano $\hat{\phi}_1$ e $\hat{\phi}_2$ due estensioni di ϕ : valutiamole nello stesso elemento $v \in V_{gH}$.

$$\hat{\phi}_1(\rho_{ind}(g^{-1})v) = \phi(\rho_{ind}(g^{-1})(v)) = \hat{\phi}_2(\rho_{ind}(g^{-1})v)$$

dove l'uguaglianza è vera perchè $\rho_{ind}(g^{-1})(v) \in V_{eH}$. Quindi coincidendo sui singoli blocchi le due estensioni coincidono anche su V . E quindi l'estensione è unica. □

7.1.1 Le rappresentazioni dei gruppi diedrali D_n

Per fare un esempio di come si possano usare le rappresentazioni indotte, studiamo le rappresentazioni dei gruppi diedrali. Ricordiamo che i gruppi diedrali hanno due generatori, che in accordo con quello che è stato fatto all'inizio del corso chiameremo σ e τ . Il gruppo $G = D_n$ si scrive quindi

$$D_n = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1} \mid \tau^2 = \sigma^n = 1, \sigma\tau = \tau\sigma^{n-1}\}$$

Consideriamo l'ovvio sottogruppo H generato da σ , che è evidentemente un gruppo ciclico, isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Le rappresentazioni di questo gruppo, dato che è abeliano, sono decisamente banali, in quanto sono di grado 1 e sono le radici ennesime dell'unità. In particolare la rappresentazione ρ_k è univocamente determinata dal suo valore sul generatore. Indicheremo in modo naturale

$$\rho_k(\sigma) = \omega^k \quad \omega = e^{\frac{2\pi i}{n}}$$

Studiamo ora la rappresentazione che induce ρ_k , ovvero studiamo $\text{Ind}_G^H \rho_k$, che per amore di brevità indicheremo con $\text{Ind } \rho_k$. È abbastanza utile notare che noi conosciamo la dimensione della rappresentazione indotta, in quanto conosciamo la formula

$$\dim \text{Ind}_G^H \rho_k = |G/H| \deg \rho_k = 2 \cdot 1 = 2$$

Per andare avanti è intelligente ricordare la definizione di questo spazio. Indicheremo con W lo spazio su cui agisce $\text{Ind } \rho_k$ (che è ovviamente isomorfo a \mathbb{C}^2)

$$\text{Ind } \rho_k = \{f : G \rightarrow W \mid f(gh) = \rho(h)^{-1}f(g) \quad \forall g \in G, \forall h \in H\}$$

Possiamo prendere una base di questo spazio per scrivere la matrice che le rappresenta e calcolarne poi il carattere, per esempio. Scegliamo questa base: prendiamo le funzioni $f_H, f_{\tau H}$ definite da

$$\begin{cases} f_H(e) = 1 \\ f_H(\tau) = 0 \end{cases} \quad \begin{cases} f_{\tau H}(e) = 0 \\ f_{\tau H}(\tau) = 1 \end{cases}$$

Evidentemente questa è una base e, data la definizione dello spazio, è anche sufficiente a determinare il comportamento delle funzioni su tutto il gruppo G .

In particolare una generica funzione $f \in \text{Ind } \rho_k$ si potrà scrivere come \mathbb{C} combinazione lineare delle due funzioni appena definite, ovvero

$$f = af_H + bf_{\tau H} \quad a, b \in \mathbb{C}$$

Possiamo ovviamente esprimere la funzione in modo diretto come

$$f(g) = f(1)f_H(g) + f(\tau)f_{\tau H}(g)$$

Ora che abbiamo lo spazio dove agiscono le rappresentazioni indotte, dobbiamo trovare esplicitamente le rappresentazioni. Per ogni ρ_k , indicheremo con $\hat{\rho}_k$ la sua indotta. Per vedere come è fatta, facciamola agire sulla base dello spazio. In questo modo potremo scriverla come matrice.

Dobbiamo quindi calcolare

$$\begin{pmatrix} \hat{\rho}_k(\sigma)f_H \\ \hat{\rho}_k(\sigma)f_{\tau H} \end{pmatrix} \quad \begin{pmatrix} \hat{\rho}_k(\tau)f_H \\ \hat{\rho}_k(\tau)f_{\tau H} \end{pmatrix}$$

Facciamo questa cosa in quanto in realtà dovremmo calcolare su ogni elemento del gruppo la matrice, ma sappiamo che σ e τ generano il gruppo, ed è più facile moltiplicare matrici piuttosto che fare conti di questo tipo. Per esempio

$$\hat{\rho}_k(\sigma)f_H(1) = f_H(\sigma^{-1}) = \rho_k(\sigma)f_H(1) = \omega^k f_H(1)$$

Con conti analoghi si ottiene

$$\hat{\rho}_k(\sigma) = \begin{pmatrix} \omega^k & 0 \\ 0 & \omega^{-k} \end{pmatrix} \quad \hat{\rho}_k(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

A questo punto abbiamo un sacco di rappresentazioni di D_n . Se vogliamo costruire tutte le rappresentazioni del gruppo dobbiamo domandarci se sono irriducibili o meno e in caso decomporle. Alcuni casi particolari si vedono abbastanza facilmente. Per esempio, per $k = 0$, $\hat{\rho}_k(\sigma) = \text{Id}$. Di conseguenza, tutte le $\hat{\rho}_0$ sono simultaneamente diagonalizzabili e quindi in realtà la rappresentazione non sarà irriducibile in quanto il gruppo diventa abeliano.

BISOGNA FINIRE CHE DEVO ANDARE A LEZIONE.

8 Rappresentazioni di gruppi compatti

Ci piacerebbe in qualche modo estendere quello che abbiamo fatto per i gruppi finiti ad una categoria particolare di gruppi infiniti, in particolare i gruppi compatti. Per farlo, abbiamo bisogno di un po' di definizioni che generalizzino quello che abbiamo fatto.

Definizione 8.1 (Gruppo topologico). Dato un insieme G , una funzione $\cdot : G \times G \rightarrow G$ e un sottoinsieme delle parti di G , τ , la terna (G, \cdot, τ) si dice gruppo topologico se valgono le seguenti proprietà:

- (G, \cdot) è un gruppo.
- (G, τ) è uno spazio topologico.
- Le due operazioni $\cdot : G \times G \rightarrow G$ e $i : G \rightarrow G$, la seconda definita come la mappa che manda g in g^{-1} , sono continue secondo la topologia indotta da τ .

La definizione che abbiamo dato sopra è in un certo senso l'unica che si poteva dare per mettere insieme topologia e gruppi, in quanto le prime due sono obbligate e la terza dice che in qualche modo vogliamo che le due operazioni di gruppo e di topologia si parlino fra di loro e che non siano indipendenti. Si possono fare diversi esempi, come

- G finito, con la topologia discreta
- G qualsiasi, con la topologia discreta
- Il gruppo additivo dei numeri reali $(\mathbb{R}, +)$ con la topologia euclidea
- Il gruppo $GL_n(\mathbb{R})$ (o anche su \mathbb{C}), con la topologia indotta da quella di $M_n(\mathbb{R})$

In questo corso non parleremo di rappresentazioni di gruppi topologici in generale, ma solo di alcuni, ovvero quelli compatti. Per cui diamo la definizione

Definizione 8.2. (G, \cdot, τ) si dice compatto se (G, τ) è compatto.

Facciamo un po' di esempi di gruppi compatti che andremo a trattare

- I gruppi finiti, con la topologia discreta.
- I gruppi O_n, SO_n, U_n, SU_n : dimostriamo che effettivamente lo sono (lo dimostriamo per O_n perchè per U_n la dimostrazione è analoga e gli altri sono sottogruppi). Se $G \subseteq \mathbb{R}^m$ dotato della topologia euclidea indotta allora

$$G \text{ compatto} \Leftrightarrow G \text{ è chiuso in } \mathbb{R}^m \text{ e limitato}$$

Considero $O_n(\mathbb{R}) \subseteq \mathbb{R}^{n^2}$: esso è così descritto

$$O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : A^t A = I\} = \{A \in M_n(\mathbb{R}) : \sum_{h=1}^n a_{ih} a_{jh} = \delta_{ij} \forall i, j = 1, \dots, n\}$$

$\Rightarrow O_n$ è chiuso poichè descritto da equazioni (risulta essere l'intersezione finita di cotroimmagini di chiusi $\{1\}, \{0\}$). Inoltre per $i = j \Rightarrow \sum_{h=1}^n a_{ih}^2 = 1 \Rightarrow |a_{ij}| \leq 1 \forall i, j \Rightarrow O_n$ è limitato.

In particolare può essere utile notare alcuni fatti noti che possono aiutare, cioè

$$\begin{aligned} SO_2(\mathbb{R}) &\cong \mathbb{S}^1 \\ SU_2(\mathbb{C}) &\cong \mathbb{S}^3 \end{aligned}$$

A questo punto sarà opportuno dare una nozione di rappresentazione in cui entra in gioco la topologia di G , oltre alla sua struttura di gruppo.

Definizione 8.3 (Rappresentazione continua). Consideriamo una rappresentazione del gruppo topologico G , $\rho : G \rightarrow GL(V_\rho)$. Diciamo che la rappresentazione è continua se la mappa

$$\rho : G \rightarrow GL(V_\rho)$$

è continua. Per il primo termine bisogna considerare la topologia su G , che è definita in quanto il gruppo è topologico, mentre su $GL(V_\rho)$ si usa la topologia euclidea.

Facciamo alcuni esempi

- Se G è finito, ovviamente con la topologia discreta ogni rappresentazione è continua. In un certo senso questo non è così banale, in quanto ci dice che quello che andremo a fare sarà una generalizzazione di quello che abbiamo fatto per gruppi finiti.
- Un'altra rappresentazione del tutto ovvia: la rappresentazione del gruppo $GL(V)$ in $GL(V)$ tramite l'identità, che è evidentemente continua
- La mappa esponenziale $e^x : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$ che associa x a e^x

8.1 Le rappresentazioni di \mathbb{S}^1

Per chiarirci le idee, andremo a studiare nel dettaglio un gruppo particolare, ovvero \mathbb{S}^1 , che è ovviamente isomorfo a $SO_2(\mathbb{R})$. Cerchiamo quindi innanzitutto le sue rappresentazioni irriducibili su spazi di dimensione finita sui complessi.

Lemma 8.1. *Tutte le rappresentazioni irriducibili $/_{\mathbb{C}}$ di un gruppo compatto abeliano G hanno dimensione 1. Di conseguenza, essendo \mathbb{S}^1 un gruppo compatto abeliano, tutte le rappresentazioni di \mathbb{S}^1 irriducibili su uno spazio vettoriale complesso hanno dimensione 1.*

Dimostrazione. G è un gruppo compatto abeliano e sia $\rho : G \rightarrow GL(V)$ con V \mathbb{C} -sp. vettoriale: quindi

$$gh = hg \quad \forall g, h \in G \Rightarrow \rho(g)\rho(h) = \rho(h)\rho(g) \quad \forall g, h \in G$$

Il che vuol dire che, fissato h , $\rho(h)$ è un'omomorfismo di rappresentazioni irriducibili su \mathbb{C} , ovvero appartiene a $\text{End}_{\mathbb{S}^1}(V)$ proprio perchè commuta con $\rho(g)$ per tutte le g . Sia λ un autovalore di $\rho(h)$ (esiste perchè siamo su \mathbb{C}): allora $\rho(g) - \lambda \text{Id} \in \text{End}_{\mathbb{S}^1}(V)$ e ha un nucleo \Rightarrow per Schur il nucleo coincide con V essendo V irriducibile. Allora $\rho(h) \equiv \lambda(h) \text{Id}$. Quello che abbiamo fatto vale per ogni $h \in G$, per cui tutti i $\rho(g)$ sono in realtà scalari. Questo ci dice che ogni base di V è una base di autovettori per $\rho(g) \forall g \in G$ e quindi ogni autospazio è G -invariante. Dunque le rappresentazioni irriducibili di G sono tutte di grado 1. \square

Proposizione 8.2. *Le rappresentazioni irriducibili di \mathbb{S}^1 sono tutte e sole le $\rho_n : \mathbb{S}^1 \rightarrow \mathbb{C}^*$ definite, al variare di n in \mathbb{Z} , nel seguente modo:*

$$\rho_n(z) = z^n$$

Dimostrazione. Innanzitutto notiamo che le ρ_n definite nell'enunciato sono effettivamente delle rappresentazioni irriducibili di \mathbb{S}^1 , quindi bisogna solo verificare che non ce ne sono altre.

Sappiamo che le rappresentazioni irriducibili dovranno avere dimensione 1, per cui saranno omomorfismi $\rho : \mathbb{S}^1 \rightarrow \mathbb{C}^*$. Inoltre dovrà per forza essere $|\rho(z)| = 1 \quad \forall z \in \mathbb{S}^1$. Questo si dimostra abbastanza facilmente. Supponiamo per assurdo infatti che si abbia

$$|\rho(x)| > 1$$

per qualche x . Allora anche $\rho(x)^n$ farebbe parte di $\rho(G)$. Tuttavia qui c'è un assurdo in quanto $\rho(G)$ è compatto perché la rappresentazione è continua (compatti vanno in compatti), mentre $\rho(x)^n$ non è limitato. Se invece per assurdo fosse $|\rho(x)| < 1$ si potrebbe usare lo stesso argomento notando che $|\rho(x^{-1})| > 1$. Di conseguenza sappiamo che $\rho(\mathbb{S}^1) \subseteq \mathbb{S}^1$. Consideriamo ora la mappa

$$\begin{aligned} \phi : (\mathbb{R}, +) &\rightarrow \mathbb{S}^1 \\ x &\rightarrow e^{ix} \end{aligned}$$

che è evidentemente continua ed è omomorfismo di gruppi (è un rivestimento). Sia $\hat{\rho}$ l'applicazione che fa commutare il seguente diagramma:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\phi} & \mathbb{S}^1 \\ & \searrow \hat{\rho} & \downarrow \rho \\ & & \mathbb{S}^1 \end{array}$$

Essendo composizione di omomorfismi continui, anche $\hat{\rho}$ è omomorfismo continuo. Si può dimostrare (ma non lo facciamo in questa sede) che esiste un'applicazione continua $\theta : \mathbb{R} \rightarrow \mathbb{R}$ che fa commutare il diagramma:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\phi} & \mathbb{S}^1 \\ \theta \downarrow & \searrow \hat{\rho} & \downarrow \rho \\ \mathbb{R} & \xrightarrow{\phi} & \mathbb{S}^1 \end{array}$$

Ovvero che fattorizza $\hat{\rho} = \phi\theta$. A questo punto $\theta(0)$ deve essere un multiplo intero di 2π , visto che deve risultare $e^{i\theta(0)} = \hat{\rho}(0) = 1$. Quindi, a meno di traslare θ di un multiplo intero di 2π (il che non interferisce con la commutatività del diagramma), possiamo assumere $\theta(0) = 0$. Dati x, y reali deve valere

$$e^{i\theta(x+y)} = \hat{\rho}(x+y) = \hat{\rho}(x) \cdot \hat{\rho}(y) = e^{i\theta(x)+i\theta(y)}$$

per cui deve essere

$$\theta(x+y) - \theta(x) - \theta(y) \in 2\pi\mathbb{Z} \quad \forall x, y \in \mathbb{R}$$

Ma visto che θ è continua l'espressione sopra deve essere necessariamente costante al variare di x e y . Ponendo $x = y = 0$ ricaviamo che tale costante è $-\theta(0) = 0$, dunque

$$\theta(x+y) = \theta(x) + \theta(y) \quad \forall x, y \in \mathbb{R}$$

A questo punto si osserva (sfruttando la continuità di θ) che deve essere $\theta(x) = \theta(1)x$, con $\alpha \in \mathbb{R}$. Non solo, possiamo dare delle informazioni a riguardo di $\theta(1)$. Infatti, dato che $\hat{\rho}$ è "periodico", deve essere

$$1 = \hat{\rho}(0) = \hat{\rho}(2\pi) = e^{i\theta(1)2\pi}$$

per cui in realtà si ha $\theta(1) \in \mathbb{Z}$. Ricapitolando, abbiamo mostrato che per ogni $x \in \mathbb{R}$ vale che

$$e^{i\theta(1)x} = \rho(e^{ix})$$

dove $\theta(1)$ è un intero fissato. Ovvero per ogni $z \in \mathbb{S}^1$ vale

$$\rho_{\theta(1)}(z) = z^{\theta(1)} = \rho(z)$$

che è quello che volevamo mostrare. □

A questo punto il nostro obiettivo sarebbe quello di cercare la stessa cosa che abbiamo fatto per i gruppi finiti, ovvero scomporre una rappresentazione generica come somme di rappresentazioni irriducibili. Per farlo in sostanza abbiamo inventato quel prodotto hermitiano invariante che da solo ci ha permesso praticamente di fare tutto. Sarebbe molto bello avere una cosa simile anche per questi gruppi topologici. In particolare per i gruppi compatti possiamo andare a cercare di definire qualcosa di molto simile.

Definizione 8.4 (Integrazione su un gruppo). Sia G un gruppo topologico. Consideriamo un'applicazione $I : C_{\mathbb{R}}(G) \rightarrow \mathbb{R}$ dove con $C_{\mathbb{R}}$ si intendono le funzioni continue da G in \mathbb{R} ¹⁴. La mappa I si dice integrazione se rispetta le seguenti proprietà.

- È lineare: $I(af + bg) = aI(f) + bI(g)$.
- Se la funzione f è positiva (> 0), allora anche l'integrale deve essere positivo (> 0).

A questo punto, in analogia con quello che abbiamo fatto con i prodotti finiti, cerchiamo di trovare quello invariante.

Definizione 8.5. Sia G un gruppo compatto e I una integrazione su G . Si dice che I è G -invariante se $\forall f \in C_{\mathbb{R}}(G), \forall g \in G$ vale che

$$I(f) = I(L_g(f)) = I(R_g(f))$$

dove $(L_g(f))(x) = f(g^{-1}x)$ e $(R_g(f))(x) = f(xg)$.

Se questa integrazione esiste, allora in analogia a quanto fatto per i gruppi finiti possiamo sperare che le rappresentazioni di un gruppo compatto siano completamente irriducibili.

Esempio 8.1. Alcuni esempi di integrazioni invarianti sono:

1. Nel caso dei gruppi finiti $I(f) = \frac{1}{|G|} \sum_{g \in G} f(g)$ è una integrazione invariante.
2. Definiamone esplicitamente una su \mathbb{S}^1

$$\int_{\mathbb{S}^1} f(g) dg := \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta$$

Le verifiche che sia una integrazione a tutti gli effetti sono banali: infatti che sia lineare e la positività derivano dalle proprietà dell'integrazione su \mathbb{R} e l'invarianza deriva dal fatto che far agire \mathbb{S}^1 significa solo ruotare di un angolo ovvero riparametrizzare la circonferenza. Il diviso 2π è dovuto al fatto che vogliamo in generale avere una integrazione invariante normalizzata ovvero

$$\int_{\mathbb{S}^1} 1 dg = 1$$

Nel caso dei gruppi finiti dividevamo per la cardinalità del gruppo: ora che si parla di gruppi compatti possiamo immaginare che si divida per la "misura" del gruppo.

¹⁴Tutto funziona allo stesso modo se al posto di \mathbb{R} mettiamo \mathbb{C} . In futuro non si baderà a questa distinzione.

Lemma 8.3. *Se esiste l'integrazione invariante su un gruppo, allora esiste una forma hermitiana definita positiva invariante sotto l'azione del gruppo.*

Dimostrazione. Sia h una forma hermitiana definita positiva su V_ρ . Consideriamo la quantità

$$h_G(v, w) = I(h(\rho(g)v, \rho(g)w))$$

Evidentemente è di nuovo una forma hermitiana definita positiva ed è invariante sotto G . □

Teorema 8.4. *Sia G un gruppo compatto e $\rho : G \rightarrow GL(V_\rho)$ una sua rappresentazione continua, con V_ρ di dimensione finita. Se esiste una integrazione invariante I , allora la rappresentazione è completamente riducibile.*

Dimostrazione. La dimostrazione è identica alla dimostrazione 4.4, usando la forma hermitiana invariante appena definita. □

Teorema 8.5 (Teorema di Haar). *Per ogni gruppo compatto esiste l'integrazione invariante.*

Di questo teorema non daremo la dimostrazione in questo corso.

Definiamo ora in $\mathbb{C}(\mathbb{S}^1)$ un prodotto hermitiano come segue

$$(f_1, f_2) := \int_{\mathbb{S}^1} f_1(g) \overline{f_2(g)} dg$$

È una buona definizione ed è \mathbb{S}^1 invariante.

Osservazione.

$$(\rho_n, \rho_m) = \int_{\mathbb{S}^1} \rho_n(g) \overline{\rho_m(g)} dg = \frac{1}{2\pi} \int_0^{2\pi} e^{in\theta} e^{-im\theta} d\theta = \frac{1}{2\pi} \int_0^{2\pi} e^{i\theta(n-m)} d\theta$$

$$\Rightarrow (\rho_n, \rho_m) = \begin{cases} 1 & n = m \\ 0 & n \neq m \end{cases} \Rightarrow (\rho_n, \rho_m) = \begin{cases} 1 & \rho_n \cong \rho_m \\ 0 & \rho_n \not\cong \rho_m \end{cases}$$

ovvero $\{\rho_n\}_{n \in \mathbb{N}}$ formano un sistema ortonormale.

Corollario. *Sia $\rho : \mathbb{S}^1 \rightarrow GL(V)$ una rappresentazione: allora*

$$\rho \cong \sum_n a_n \rho_n \quad \text{con } n \in \mathbb{N} \text{ ed } a_n \in \mathbb{Z}$$

Più precisamente $a_n = (\rho, \rho_n)$.

MANCA LA PARTE IN CUI PARLAVA DI FOURIER

8.2 Le rappresentazioni di $SU(2)$

Dopo aver studiato in dettaglio S^1 , vediamo come si comporta un suo parente stretto, $SU(2)$. Ricordiamo che $SU(2)$ è definito come un sottoinsieme di $GL(\mathbb{C}^2)$. In particolare ogni matrice di $SU(2)$ si può scrivere come

$$SU(2) = \left\{ \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix} \mid z_1, z_2 \in \mathbb{C}, \quad |z_1|^2 + |z_2|^2 = 1 \right\}$$

È abbastanza naturale considerare $\mathbb{C}^2 \cong \mathbb{R}^4$ e accorgersi che in sostanza $SU(2) \cong S^3$, in quanto tutti gli elementi rispettano l'equazione

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$$

E scrivendo in questo modo ci accorgiamo subito che quindi $SU(2)$ è un gruppo compatto e connesso.

Corollario. *Ogni rappresentazione di $SU(2)$ è scomponibile in una somma di rappresentazioni irriducibili.*

Nella sezione 6.1 abbiamo visto come i quaternioni possono essere visti come un sottoinsieme di $M_2(\mathbb{C})$

$$\mathbb{H} = \left\{ \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix} \in M_2(\mathbb{C}) \right\}$$

Quindi $SU(2)$ può essere immerso in \mathbb{H} avendo le matrici la stessa struttura.

MANCA LA PARTE SU ρ_H MA NON SO QUANTO SERVA.

Come abbiamo fatto per S^1 , vorremmo andare a studiare tutte le sue rappresentazioni irriducibili. Per farlo, innanzitutto sarebbe intelligente farsi un'idea di come può essere fatta l'integrazione invariante su questo gruppo. Se lo immergiamo in \mathbb{R}^4 , possiamo sfruttare l'integrazione lì definita e quindi fare un integrale triplo

$$I(f) = \int_{S^3} f(g) dg = \frac{1}{2\pi^2} \int_0^\pi \int_0^\pi \int_0^{2\pi} f(\theta, \phi, \psi) \sin^2 \theta \sin \phi \, d\theta \, d\phi \, d\psi$$

L'invarianza dell'integrazione sotto l'azione di G deriva sostanzialmente dal fatto che quando si cambia variabili bisogna moltiplicare l'integrando per il determinante dello Jacobiano. Tuttavia $\det(SU(2)) = 1$ e quindi non ci sono problemi.

Rappresentazioni irriducibili Vediamo ora di classificare tutte le rappresentazioni irriducibili di $SU(2)$. Consideriamo l'azione di $SU(2)$ sullo spazio $V_m = \mathbb{C}[x, y]_m$ dei polinomi omogenei su \mathbb{C} di grado m definita in questo modo

$$\rho_m(A)f(x, y) = f(a_{11}x + a_{21}y, a_{12}x + a_{22}y) \quad \forall f \in V_m, \forall A \in SU(2)$$

Proposizione 8.6. ρ_m è una rappresentazione irriducibile di $SU(2)$ $\forall m \in \mathbb{N}$.

Dimostrazione. Cerchiamo di trovare un sottogruppo di $SU(2)$ di cui conosciamo già le rappresentazioni irriducibili e studiamo le ρ_n ristrette a tale sottogruppo. Consideriamo il seguente insieme delle matrici speciali unitarie diagonali

$$T = \left\{ \begin{pmatrix} z & 0 \\ 0 & \bar{z} \end{pmatrix} \in M_2(\mathbb{C}) : |z|^2 = 1 \right\} \subseteq SU(2) \Rightarrow T = \left\{ \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} : 0 \leq \theta \leq 2\pi \right\}$$

É evidente che T sia isomorfo a \mathbb{S}^1 . Dunque $\rho_m|_{\mathbb{S}^1}$ è una rappresentazione di \mathbb{S}^1 su V_m . Come agiscono le matrici in T ? Per vederlo, consideriamo la base "canonica" di V_m , formata dai monomi $\{x^k y^{m-k}\}_{k \in \{0, \dots, m\}}$ e scriviamo

$$V_m = \bigoplus_{k=0}^m \mathbb{C}(x^k y^{m-k})$$

Dato un $\theta \in [0, 2\pi]$ allora

$$\rho_m \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} (x^k y^{m-k}) = (x e^{i\theta})^k (y e^{i\theta})^{m-k} = e^{i(m-2k)} x^k y^{m-k}$$

Ovvero, quello che abbiamo appena scoperto è che la base considerata è formata da autovettori per il sottogruppo T . Quindi, denotando con $\rho_n^{\mathbb{S}^1}$ le rappresentazioni irriducibili di \mathbb{S}^1 , allora $\rho_m|_{\mathbb{S}^1} = \sum_{k=0}^m \rho_{m-2k}^{\mathbb{S}^1}$.

Quindi ora di V_m abbiamo una duplice scrittura:

$$V_m = \bigoplus_{k=0}^m \mathbb{C}(x^k y^{m-k}) = \bigoplus_{k=0}^m V_{\rho_{m-2k}^{\mathbb{S}^1}}$$

dove la seconda scrittura è una somma diretta di rappresentazioni di T irriducibili e a 2 a 2 non isomorfe. Consideriamo $W \neq \emptyset \subseteq V_m$ sottospazio stabile per $SU(2)$: iniziamo con il dimostrare il seguente fatto:

Fatto: Sia $\pi_k : V_m \rightarrow \mathbb{C}[x^{m-k} y^k]$ la proiezione di un vettore sulla sua componente $(m-k)$ -esima. Allora se $\pi_k|_W \neq 0$ allora $V_{m,k} := \mathbb{C}[x^{m-k} y^k] \subseteq W$.

Dato che $\{x^k y^{m-k}\}_{k \in \{0, \dots, m\}}$ sono una base di autovettori per le matrici in T allora $\forall k, \pi_k \in \text{Hom}_T(V_m, V_{m,k}) \Rightarrow \pi_k|_W \in \text{Hom}_T(W, V_{m,k})$. Se $\pi_k|_W \neq 0 \Rightarrow W = \text{Ker}(\pi_k|_W) \oplus W_k$ dove la $\dim(W_k)$ è forzata ad essere 1. Quindi $W_k \cong V_{m,k}$ come rappresentazioni. Tuttavia $V_{m,k}$ è l'unico sottospazio invariante per $\rho_{m-2k}^{\mathbb{S}^1} \Rightarrow V_{m,k} = W_k$.

Quindi dato che abbiamo supposto il nostro W diverso dal vuoto, esiste un k tale che $x^{m-k} y^k \in W$. Se mostriamo che $x^m \in W$ allora abbiamo concluso poichè data la generalità di W avrei dimostrato che $x^m \in$ a tutti i sottospazi di V_m non vuoti e invarianti per $SU(2)$. Quindi se W fosse diverso da V_m avrei $V_m = W \oplus U$ ma con $U \neq \emptyset \Rightarrow x^m \in U \cap W$ il che è assurdo poichè devono essere in somma diretta. Per mostrare che $x^m \in W$ riusciamo il fatto e ci riduciamo a dover dimostrare che $\pi_0|_W \neq 0$. Considero al variare di $g \in SU(2)$ il vettore $\pi_0(\rho_m(g)(x^{m-k} y^k))$ dove $x^{m-k} y^k$ è il monomio che siamo sicuri appartenga a W . Bene, ma allora mi basta scegliere

$$g = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \Rightarrow \rho_m(g)(x^{m-k} y^k) = x^m$$

Quindi $W = V_m$. Le ρ_m sono irriducibili. □

Le classi di coniugio di $SU(2)$ Dato che abbiamo dato tanto peso alla teoria del carattere per i gruppi finiti, probabilmente anche per i gruppi compatti ci saranno applicazioni interessanti. Dato che il carattere è una funzione di classe, è intelligente andare a studiare nel dettaglio le classi di coniugio di $SU(2)$.

Abbiamo già visto che possiamo immergere \mathbb{S}^1 in $SU(2)$. Vediamo come questo abbia a che fare con le classi di coniugio.

Ricordiamo che possiamo scrivere un generico punto di \mathbb{S}^3 come

$$\begin{cases} x_1 = \cos \theta \\ x_2 = \sin \theta \cos \phi \\ x_3 = \sin \theta \sin \phi \cos \psi \\ x_4 = \sin \theta \sin \phi \sin \psi \end{cases}$$

Per cui possiamo scrivere il generico elemento di $SU(2)$ come

$$g(\theta, \phi, \psi) = \begin{pmatrix} \cos \theta + i \sin \theta \cos \phi & \sin \theta \sin \phi (\cos \psi + i \sin \psi) \\ -\sin \theta \sin \phi (\cos \psi - i \sin \psi) & \cos \theta - i \sin \theta \cos \phi \end{pmatrix}$$

Dato che le matrici di $SU(2)$ sono normali, possiamo usare il teorema spettrale normale per dire che sono tutte unitariamente diagonalizzabili, ovvero $\forall g \in SU(2) \exists h \in U(2) \mid hgh^{-1} = m$, con m diagonale. Tuttavia possiamo restringerci ad avere anche h in $SU(2)$ scegliendo $h' = \frac{1}{\sqrt{\det(h)}}h$. Per questo motivo le classi di coniugio saranno tutte matrici di Jordan diagonali, senza 1 sulla sopra-diagonale. Per questo motivo la classe di coniugio sarà univocamente determinata dagli autovalori della matrice. Il polinomio caratteristico di una matrice 2×2 è

$$p(t) = t^2 - \text{tr}(M)t + \det(M)$$

Ma dato che siamo in $SU(2)$ il determinante è 1. La traccia è invece con una banale somma $2 \cos \theta$. I due autovalori hanno modulo 1 e quindi in sostanza sono $e^{i\theta}$ e $e^{-i\theta}$. Per questo motivo un generico elemento di $SU(2)$ è

$$g(\theta, \phi, \psi) \sim \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} = g(\theta, 0, 0)$$

Per questo motivo la funzione $\frac{1}{2} \text{tr}(g) : SU(2) \rightarrow \mathbb{R}$ è una funzione suriettiva in $[-1, 1]$ e le sue fibre sono le classi di coniugio.

Il carattere delle rappresentazioni irriducibili di $SU(2)$ Prendiamo una funzione f

$$f \in \mathbb{C}(SU(2))^\# = \{\text{Funzioni di classe } f : SU(2) \rightarrow \mathbb{C}\}$$

Sappiamo che se questa funzione è di classe, allora non dipende dal rappresentante della classe di coniugio. Per questo motivo possiamo quindi dire che

$$f(g(\theta, \phi, \psi)) = f(g(\theta, 0, 0))$$

Vorremmo andare a studiare come si comporta l'integrazione invariante su questa funzione e poi considerare il caso particolare in cui questa funzione sia per l'appunto il carattere di ρ , una generica rappresentazione di $SU(2)$.

$$\begin{aligned} \int_{\mathbb{S}^3} f(g) dg &= \frac{1}{2\pi^2} \int_0^\pi \int_0^\pi \int_0^{2\pi} f(\theta, \phi, \psi) \sin^2 \theta \sin \phi \, d\theta \, d\phi \, d\psi = \\ &= \frac{1}{2\pi^2} \int_0^\pi \int_0^\pi \int_0^{2\pi} f(\theta, 0, 0) \sin^2 \theta \sin \phi \, d\theta \, d\phi \, d\psi = \\ &= \frac{2}{\pi} \int_0^\pi f(\theta, 0, 0) \sin^2 \theta \, d\theta = \\ &= \frac{1}{\pi} \int_0^{2\pi} f(\theta, 0, 0) \sin^2 \theta \, d\theta \end{aligned}$$

Quindi l'espressione si semplifica parecchio. Prendiamo ora per l'appunto una rappresentazione di ρ e vediamo come si comporta il carattere. In particolare prendiamo una delle ρ_m irriducibili che abbiamo trovato prima. Sappiamo che

$$\rho_m : SU(2) \rightarrow GL(V_m) \quad V_m = \bigoplus_{k=0}^m V_{m,k}$$

In particolare siamo già riusciti a diagonalizzare ρ_m . Avremo che

$$\begin{aligned} \chi_{\rho_m}(\theta, \phi, \psi) &= \chi_{\rho_m}(\theta) = \chi_{\rho_m}(e^{i\theta}) = \\ &= \sum_{k=0}^m \rho_{m-2k}^{\mathbb{S}^1}(e^{i\theta}) = \sum_{k=0}^m e^{i(m-2k)\theta} \\ &= \frac{e^{i(m+1)\theta} - e^{-i(m+1)\theta}}{e^{i\theta} - e^{-i\theta}} = \frac{\sin((m+1)\theta)}{\sin \theta} \end{aligned}$$

Per cui, in analogia a quanto fatto per i gruppi finiti, diamo la definizione di

Definizione 8.6 (Prodotto hermitiano di caratteri).

$$\langle \chi_\rho | \chi_\sigma \rangle = \int_G \chi_\rho(g) \overline{\chi_\sigma(g)} dg$$

Che andiamo prontamente a calcolare in questo caso

$$\langle \chi_{\rho_n} | \chi_{\rho_m} \rangle = \frac{1}{\pi} \int_0^{2\pi} \frac{\sin((n+1)\theta)}{\sin \theta} \frac{\sin((m+1)\theta)}{\sin \theta} \sin^2 \theta d\theta = \delta_{mn}$$

Cosa molto simile a quanto era già successo per i gruppi finiti. A questo punto viene il sospetto che possa esserci qualcosa di più profondo sotto. Vedremo fra poco dei teoremi che generalizzano questi risultati.

Teorema 8.7. *Sia G un gruppo compatto e siano ρ e σ due sue rappresentazioni irriducibili. Allora vale*

$$\langle \chi_\rho | \chi_\sigma \rangle = \begin{cases} 1 & \text{se } \sigma \cong \rho \\ 0 & \text{altrimenti} \end{cases}$$

Per dimostrare il teorema appena enunciato ci servono un paio di lemmi:

Lemma 8.8. *Siano $\rho : G \rightarrow GL(V)$ e $\sigma : G \rightarrow GL(W)$ due rappresentazioni¹⁵ di un gruppo compatto G e sia $\phi \in \text{Hom}(V, W)$ un omomorfismo di spazi vettoriali¹⁶. Allora possiamo definire un $\phi^G \in \text{Hom}_G(V, W)$ nel seguente modo*

$$\langle \phi^G(v) | w \rangle = \int_G \langle \sigma(g)\phi(\rho(g)v) | w \rangle dg$$

Dove $\langle \cdot | \cdot \rangle : W \times W \rightarrow \mathbb{C}$ è una forma hermitiana definita positiva.

¹⁵Non necessariamente irriducibili

¹⁶Per gli amici, un'applicazione lineare.

Dimostrazione. Dobbiamo in sostanza dimostrare che l'omomorfismo che abbiamo definito è anche un omomorfismo di rappresentazioni, ovvero che è G -equivariante, in quanto la linearità è assicurata dal prodotto hermitiano. In formule, dobbiamo mostrare che

$$\phi^G(\rho(g)v) = \sigma(g)\phi^G(v) \quad \forall g \in G, \forall v \in V \Leftrightarrow \phi^G(v) = \sigma(g)^{-1}\phi^G(\rho(g)v) \quad \forall g \in G, \forall v \in V$$

In sostanza la tesi segue dalla definizione sfruttando il fatto che l'integrazione su G sia invariante

$$\langle \sigma(g)^{-1}\phi^G(\rho(g)v) | w \rangle = \int_G \langle \sigma(hg)^{-1}\phi^G(\rho(hg)v) | w \rangle dh = \langle \phi(v) | w \rangle$$

Dove ho saltato un paio di passaggi ma il succo è che essendo l'integrazione invariante per traslazioni di G , è evidente che l'oggetto definito in questo modo diventa invariante sotto G \square

Lemma 8.9. Siano $\rho : G \rightarrow V$ e $\sigma : G \rightarrow W$ rappresentazioni irriducibili di un gruppo compatto G e sia $\phi \in \text{Hom}(V, W)$. Allora

$$\begin{cases} \phi^G = 0 & \text{se } \rho \not\cong \sigma \\ \phi^G = \frac{\text{tr } \phi}{\dim V} \text{Id}_V & \text{altrimenti} \end{cases}$$

Dimostrazione. Nel caso in cui le due rappresentazioni non siano isomorfe, la tesi segue banalmente dal lemma di Schur. Nell'altro caso, possiamo di nuovo usare Schur e dire che $V \cong W$ come spazi vettoriali, ma anche che in un certo senso sono lo stesso spazio, in quanto $\phi = \lambda \text{Id}$, sempre per Schur. L'unica cosa che rimane da mostrare è che vale proprio $\text{tr } \phi^G = \text{tr } \phi$. Per mostrarlo, possiamo fissare una base ortonormale di V , $\{e_n\}_{n \in I}$ e notare che in questa base

$$\text{tr}(\psi) = \sum_{n \in I} \langle \psi e_n | e_n \rangle \quad \forall \psi \in \text{End}(V)$$

Per cui,

$$\begin{aligned} \text{tr } \phi^G &= \sum_{n \in I} \langle \phi^G e_n | e_n \rangle = \sum_{n \in I} \int_G \langle \rho(g)^{-1} \phi(\rho(g)e_n) | e_n \rangle dg = \\ &= \sum_{n \in I} \int_G \langle \phi(\rho(g)e_n) | \rho(g)e_n \rangle dg = \sum_{n \in I} \int_G \langle \phi e_n | e_n \rangle dg = \\ &= \sum_{n \in I} \langle \phi e_n | e_n \rangle = \text{tr } \phi \end{aligned}$$

\square

Dimostrazione del teorema 8.7. Fissiamo una base ortonormale di V , $\{v_n\}$, e una base ortonormale di W , $\{w_n\}$. In base a quanto detto poco fa, avremo che

$$\begin{aligned} \langle \chi_\rho | \chi_\sigma \rangle &= \int_G \chi_\rho(g) \overline{\chi_\sigma(g)} dg = \int_G \text{tr}(\rho(g)) \text{tr}(\sigma(g)^{-1}) dg = \\ &= \int_G \sum_{i \in I} \langle \rho(g)v_i | v_i \rangle \sum_{j \in J} \langle \sigma(g)^{-1}w_j | w_j \rangle dg = \\ &= \sum_{i,j} \int_G \langle \rho(g) \langle \sigma(g)^{-1}w_j | w_j \rangle v_i | v_i \rangle dg \end{aligned}$$

Se definiamo

$$\phi_{ij} \in \text{Hom}(W, V), \quad \phi(w) = \langle w | w_j \rangle v_i$$

e con quello che abbiamo fatto nel lemma poco sopra definiamo anche ϕ_{ij}^G , possiamo notare che in effetti l'espressione poco sopra è proprio ϕ_{ij}^G , ovvero

$$\langle \chi_\rho | \chi_\sigma \rangle = \sum_{i,j} \langle \phi_{ij}^G v_i | w_j \rangle$$

Se ρ e σ non sono isomorfe, allora si ha identicamente $\phi_{ij}^G = 0$ per ogni i e j . Di conseguenza $\langle \chi_\rho | \chi_\sigma \rangle = 0$. Altrimenti, al solito posso identificare $V \cong W$ e possiamo usare l'altra parte del lemma precedente per dire che

$$\langle \chi_\rho | \chi_\sigma \rangle = \sum_{i,j} \langle \phi_{ij}^G v_i | v_j \rangle = \sum_{i,j} \frac{\text{tr } \phi_{ij}}{\dim V} \langle v_i | v_j \rangle = \sum_{i,j} \frac{\text{tr } \phi_{ij}}{\dim V} \delta_{ij}$$

Tuttavia in sostanza la matrice che rappresenta ϕ_{ij} nelle base v_i è evidentemente una matrice che ha tutti zeri tranne uno che è uno, esattamente nella posizione (i, j) , per cui

$$\langle \chi_\rho | \chi_\sigma \rangle = \sum_{i,j} \frac{\text{tr } \phi_{ij}}{\dim V} \delta_{ij} = \sum_{i=j} \frac{1}{\dim V} = 1$$

□

Corollario. *Sia G un gruppo compatto e ρ una sua rappresentazione. Allora ρ è irriducibile se e solo se $\langle \chi_\rho | \chi_\rho \rangle = 1$*

A questo punto possiamo concludere la dimostrazione del fatto che le rappresentazioni che abbiamo trovato prima di $SU(2)$ sono tutte e sole quelle irriducibili.

Teorema 8.10. *Sia ρ una rappresentazione irriducibile di $SU(2)$. Allora $\exists m \in \mathbb{N}$ tale che $\rho \cong \rho_m$. Chiaramente le ρ_m sono quelle definite nella proposizione 8.6*

Dimostrazione. Supponiamo per assurdo che sia $\langle \chi_\rho | \chi_{\rho_m} \rangle = 0 \quad \forall m \in \mathbb{N}$. Vogliamo mostrare che deve essere $\rho = 0$.

$$\begin{aligned} 0 &= \langle \chi_\rho | \chi_{\rho_m} \rangle = \int_G \chi_\rho(g) \overline{\chi_{\rho_m}(g)} dg = \\ &= \frac{1}{\pi} \int_0^{2\pi} \chi_\rho(\theta) \frac{\sin((m+1)\theta)}{\sin \theta} \sin^2 \theta \, d\theta \\ &= \frac{1}{\pi} \int_0^{2\pi} (\chi_\rho(\theta) \sin \theta) \sin((m+1)\theta) \, d\theta \end{aligned}$$

A questo punto possiamo ricordare che in realtà il carattere è una funzione di classe e in particolare si ha $\chi_\rho(\theta) = \chi_\rho(-\theta)$. La funzione $f(\theta) = \chi_\rho(\theta) \sin \theta \in C_{\mathbb{R}}[0, 2\pi]$ è quindi dispari. Inoltre, è evidentemente anche $\mathbb{L}^2[0, 2\pi]$. Ma noi sappiamo dall'analisi che $\{\sin(nx)\}_{n \in \mathbb{N}}$ è una base delle funzioni dispari di $\mathbb{L}^2[0, 2\pi]$. Di conseguenza si ha $f(\theta) = 0$ q.o., ma dato che è continua, $f(\theta) = 0$ identicamente. Per lo stesso motivo, si deve avere $\chi_\rho(\theta) = 0$

□

8.2.1 Le rappresentazioni irriducibili di $SO(3)$

Abbiamo studiato in dettaglio due gruppi importanti, \mathbb{S}^1 e $SU(2)$. Sarebbe bello a questo punto sfruttare quello che abbiamo fatto per trovare le rappresentazioni di $SO(3)$, che ha notevole rilevanza fisica. In particolare, se riuscissimo a trovare un omomorfismo continuo ϕ da $SO(3)$ a $SU(2)$ potremmo notare sul seguente diagramma

$$\begin{array}{ccc} SU(2) & \xrightarrow{\rho_m} & GL(V_m) \\ \phi \uparrow & \nearrow \hat{\rho}_m & \\ SO(3) & & \end{array}$$

che otteniamo gratis un sacco di rappresentazioni continue anche per $SO(3)$. Andiamo quindi a costruire questo omomorfismo.

Definizione 8.7. Definiamo lo spazio vettoriale su \mathbb{R}, \mathbb{E} in questo modo

$$\mathbb{E} = \{ \text{Le matrici autoaggiunte a traccia nulla} \} = \left\{ \begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix} \mid x_i \in \mathbb{R} \right\}$$

Ci piacerebbe far agire in modo sensato $SU(2)$ su \mathbb{E} , sperando di vedere la struttura di $SO(3)$. Il primo tentativo può essere quello di definire

$$\phi(g)x = gx \quad \forall g \in SU(2), x \in \mathbb{E}$$

Tuttavia questa azione non funziona in quanto non è per niente detto che la matrice in arrivo abbia di nuovo traccia nulla. Per mantenere la traccia invariata, la cosa più sensata da fare è agire per coniugio

$$\phi(g)x = gxg^{-1} \quad \forall g \in SU(2), x \in \mathbb{E}$$

In questo caso è evidente che la matrice in arrivo ha traccia nulla. Controlliamo che sia anche autoaggiunta

$$(\phi(g)x)^\dagger = (gxg^{-1})^\dagger = (g^{-1})^\dagger x^\dagger g^\dagger = gxg^{-1} = \phi(g)x$$

In quanto x è autoaggiunta e vale $g^{-1} = g^\dagger \forall g \in SU(2)$. A questo punto se riuscissimo a trovare un prodotto scalare invariante sotto l'azione di $SU(2)$ potremmo dire di aver in qualche modo mappato $SU(2)$ in $O(3)$ e ci staremmo avvicinando all'obiettivo. In particolare notiamo che la funzione

$$f(x) = -\det(x) = x_1^2 + x_2^2 + x_3^2 \quad \forall x \in \mathbb{E}$$

è in effetti una forma quadratica definita positiva su $\mathbb{E} \cong \mathbb{R}^3$ ed è anche invariante sotto $SU(2)$ in sostanza per la formula di Binet. Abbiamo quindi definito $\phi : SU(2) \rightarrow O(3)$ che è in sostanza un omomorfismo continuo di gruppi compatti. Inoltre, dato che $SU(2)$ è connesso, anche $\phi(SU(2))$ sarà connesso e conterrà l'identità. Per questo motivo possiamo quindi dire che

$$\phi(SU(2)) \subseteq SO(3)$$

A questo punto, è decisamente il caso di capire meglio come ϕ mappi un gruppo nell'altro in modo da sfruttare quello che sappiamo per uno anche per l'altro.

Proposizione 8.11. 1. L'omomorfismo $\phi : SU(2) \rightarrow SO(3)$ sopra definito è surgettivo.

2. $\ker \phi = \{\text{Id}, -\text{Id}\} \subseteq SU(2)$
3. $SU(2)/\text{Ker}(\phi) \cong SO(3)$ come gruppi.

Per dimostrare questa proposizione abbiamo bisogno di un lemma.

Lemma 8.12. *Sia $H \subseteq SO(3)$ un sottogruppo. Supponiamo che valgano le due seguenti affermazioni:*

1. H agisce transitivamente su \mathbb{S}^2
2. Esiste un asse $\langle e \rangle \subseteq \mathbb{R}^3$ tale che H contiene tutte le rotazioni intorno a quell'asse.

Allora si ha $H = SO(3)$

Dimostrazione. Consideriamo $|e| = 1$. Dato che H agisce transitivamente su \mathbb{S}^2 , $\forall g \in SO(3) \exists h \in H$ tale che

$$ge = he \Rightarrow e = h^{-1}ge \Rightarrow h^{-1}g \in \text{Stab}(e)$$

Ma lo stabilizzatore di e è una rotazione intorno a quell'asse, quindi è in H , dunque $h^{-1}g \in H \forall g \in SO(3)$, ma allora $\forall g \in SO(3)$ abbiamo che $g \in H$ \square

Dimostrazione della proposizione 8.11. Dimostriamo ora i tre punti della proposizione applicando il lemma appena dimostrato per il primo punto:

1. Dimostriamo che l'azione di $\Phi(SU(2))$ su \mathbb{S}^2 è transitiva. Prendiamo una matrice $x \in \mathbb{E} \cap \mathbb{S}^2$, essendo una matrice autoaggiunta, per il teorema spettrale è unitariamente diagonalizzabile, ovvero $\exists g \in U(2) | gxg^{-1}$ è una matrice diagonale. In particolare, dato che $|\det(g)| = 1$, possiamo considerare $\hat{g} = \frac{g}{\sqrt{\det(g)}}$ per dire che possiamo scegliere una matrice $\hat{g} \in SU(2)$. Nella sua forma diagonale la matrice sarà

$$\hat{g}x\hat{g}^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix} \quad \lambda \in \mathbb{R}$$

e dovrà essere $-\det(m) = \lambda^2 = 1$, per cui $\lambda = \pm 1$. Dato che in $SU(2)$ c'è una matrice che scambia λ con $-\lambda$, possiamo prendere WLOG $\lambda > 0$

$$\hat{g}x\hat{g}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

E questo vuol dire che tutte le matrici di \mathbb{E} sono coniugate alla stessa. Dato che l'azione di $SU(2)$ è per coniugio, questo vuol dire che c'è un'orbita sola, ovvero l'azione è transitiva.

Mostriamo ora che $\Phi(SU(2))$ contiene tutte le rotazioni intorno ad un asse. Questo è semplice in quanto sappiamo che $\mathbb{S}^1 \subset SU(2)$. Vediamo come agisce

$$\begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \begin{pmatrix} x_1 & x_2 + ix_3 \\ x_2 - ix_3 & -x_1 \end{pmatrix} \begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} x_1 & e^{2i\theta}(x_2 + ix_3) \\ e^{-2i\theta}(x_2 - ix_3) & -x_1 \end{pmatrix}$$

Che è palesemente una rotazione intorno all'asse x_1 di angolo 2θ .

2. Bisogna mostrare che $\text{Ker } \Phi = \{\text{Id}, -\text{Id}\}$. Se vale $\Phi(g) = \text{Id}$, allora vale che

$$\begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \bar{z}_1 & -z_2 \\ \bar{z}_2 & z_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ \Rightarrow \begin{pmatrix} |z_1|^2 - |z_2|^2 & -2z_1z_2 \\ -2\bar{z}_1\bar{z}_2 & |z_2|^2 - |z_1|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

e questo è vero solo per $z_2 = 0$ e $|z_1| = 1$. Se andiamo a considerare il caso studiato al punto precedente, allora è evidente che deve essere solo $z_1 = \pm 1$.

3. La tesi segue dalle proposizioni precedenti applicate insieme al primo teorema di omomorfismo.

□

A questo punto abbiamo mostrato un isomorfismo di gruppi. Ci piacerebbe che il nostro isomorfismo fosse anche continuo, in modo da poter concludere quali siano tutte e sole le rappresentazioni irriducibili di $SO(3)$. Per farlo in qualche modo dobbiamo definire una topologia sul gruppo quoziente in modo astratto e verificare che corrisponda a quella che già conosceamo.

Definizione 8.8. Sia G un gruppo topologico, H un suo sottogruppo normale. Definiamo una topologia nel seguente modo su G/H : un sottoinsieme $U \subseteq G/H$ è aperto $\Leftrightarrow \pi^{-1}(U)$ è aperto in G . Sono banali verifiche che questa sia effettivamente una topologia su G/H . Inoltre questa definizione ci assicura che la mappa π sia continua.

Osservazione. A questo punto possiamo affermare che $SU(2)/\text{Ker } \Phi \cong SO(3)$ come gruppi topologici e non solo come gruppi.

Corollario. Una rappresentazione irriducibile ρ_m di $SU(2)$ si può proiettare su $SO(3)$ se e solo se $-\text{Id} \in \text{Ker } \rho_m$.

Teorema 8.13. Le rappresentazioni irriducibili di $SO(3)$ sono tutte e sole quelle che si ottengono da $SU(2)$ che hanno $-\text{Id}$ nel nucleo, ovvero le ρ_m per m pari.

Teorema 8.14 (Formula di Clebsch-Gordon). Consideriamo il prodotto tensore di due rappresentazioni irriducibili di $SU(2)$. Vale la formula

$$\rho_n \otimes \rho_m = \sum_{j=0}^m \rho_{m+n-2j} \quad (n \geq m)$$

Dimostrazione. Si tratta di un banale conto con i caratteri.

$$\begin{aligned} \chi_{\rho_n \otimes \rho_m} &= \chi_{\rho_n} \chi_{\rho_m} = \frac{e^{i(n+1)\theta} - e^{-i(n+1)\theta}}{e^{i\theta} - e^{-i\theta}} \cdot \sum_{j=0}^m e^{i(m-2j)\theta} = \\ &= \dots = \sum_{j=0}^m e^{i(n+m-2j)\theta} \end{aligned}$$

□

9 Rappresentazioni di algebre

9.1 Prime definizioni e esempi

Definizione 9.1. Un insieme A si dice *algebra* sul campo \mathbb{K} (o più semplicemente \mathbb{K} -algebra) se

- A è uno spazio vettoriale su \mathbb{K}
- il prodotto $\cdot : A \times A \rightarrow A$ è una funzione bilineare

Un'algebra si dice

- *associativa* se il prodotto è associativo
- *unitaria* se $\exists 1_A \in A$ l'elemento neutro per il prodotto
- *commutativa* se il prodotto è commutativo

Esempio 9.1. Alcuni esempi di algebre sono:

1. Algebre di divisione $/\mathbb{R}$ (che abbiamo già incontrato)
2. \mathbb{K} un campo
3. Se V è uno spazio vettoriale su \mathbb{K} allora $\text{End}(V)$ è una \mathbb{K} -algebra
4. $\mathbb{K}[x_1, \dots, x_n]$ è una \mathbb{K} -algebra
5. $\mathbb{K}\langle x_1, \dots, x_n \rangle$ è l'algebra libera con n generatori, sono le parole nell'alfabeto $\{x_1, \dots, x_n\}$, il prodotto è la concatenazione; è generata da $x_{i_1} \cdots x_{i_k}$ (simile come costruzione al gruppo libero su n generatori)
6. Se A è una \mathbb{K} -algebra, I un suo ideale bilatero, allora A/I è una \mathbb{K} -algebra

Esempio 9.2. QUI ANDREBBE L'ALGEBRA UNIVERSALE INVILUPPANTE MA NON SO QUANTO SERVA...

Vorremmo ritrovare la teoria delle rappresentazioni che abbiamo fatto per i gruppi anche nella teoria che faremo sulle algebre, in quest'ottica definiamo il seguente insieme

Definizione 9.2. Sia G un gruppo, definiamo l'insieme delle combinazioni lineari formali degli elementi di G a coefficienti in \mathbb{K}

$$\mathbb{K}[G] = \left\{ \sum a_g e_g, a_g \in \mathbb{K} \right\}$$

dove abbiamo una corrispondenza biunivoca tra $\{g \in G\}$ e $\{e_g\}_{g \in G}$. Si osserva che $\mathbb{K}[G]$ è un \mathbb{K} -spazio vettoriale, definendo poi il prodotto sui vettori di base (ed estendendo per linearità) come $e_g \cdot e_h = e_{gh}$ si ottiene una \mathbb{K} -algebra. Essa è associativa perchè il prodotto in G è associativo e unitaria poichè e_1 è l'unità di $\mathbb{K}[G]$.

Osservazione. L'azione che avevamo nella rappresentazione regolare diventa il prodotto in $\mathbb{K}[G]$.

Definizione 9.3. Siano A e A' \mathbb{K} -algebre, sia $f : A \rightarrow A'$ una funzione, f è un *omomorfismo di \mathbb{K} -algebre* se

- $f : A \rightarrow A'$ è un omomorfismo di spazi vettoriali
- $f(ab) = f(a)f(b)$

- $f(1_A) = 1_{A'}$

Definizione 9.4. Una *rappresentazione di una \mathbb{K} -algebra A* è un omomorfismo di \mathbb{K} -algebre

$$f : A \rightarrow \text{End}(V)$$

con V un \mathbb{K} -spazio vettoriale, allora V viene detto *A -modulo*.

Definizione 9.5. Siano V e W degli A -moduli, un omomorfismo di spazi vettoriali $f : V \rightarrow W$ si dice *omomorfismo di rappresentazioni* se

$$\forall a \in A, \forall v \in V \quad f(av) = af(v)$$

Esercizio 9.1. Se f è un isomorfismo di A -moduli, allora f^{-1} è un isomorfismo di A -moduli.

Esempio 9.3. Alcuni esempi di rappresentazioni sono

1. Se $A = \mathbb{K}$ allora le rappresentazioni di A sono gli spazi vettoriali su \mathbb{K} dove l'azione di A è molto semplice: $\rho(a) = a \text{Id}$.
2. Sia G un gruppo finito, $A = \mathbb{K}[G]$, allora le rappresentazioni di A come \mathbb{K} -algebra sono tutte e sole le rappresentazioni di G come gruppo (le verifiche sono abbastanza semplici, da un lato si restringe l'azione agli elementi di base, dall'altro si estende per linearità).

Definizione 9.6. Siano ρ_1, ρ_2 delle rappresentazioni di A , allora definiamo $\rho_1 + \rho_2$ sulla somma diretta

$$\rho_1 + \rho_2 : A \rightarrow \text{End}(V_1 \oplus V_2)$$

allo stesso modo di come abbiamo definito la somma di rappresentazioni di gruppi (scrivendo le matrici a blocchi).

Definizione 9.7. Sia $\rho : A \rightarrow \text{End}(V)$ una rappresentazione, ρ si dice *irriducibile* se V non ha sottomoduli (sottospazi invarianti per moltiplicazione per elementi di A) non banali, allora V è detto A -modulo *semplice*.

Definizione 9.8. Sia $\rho : A \rightarrow V$ una rappresentazione, ρ è *indecomponibile* (V è indecomponibile come A -modulo) se non è somma diretta di rappresentazioni non banali.

Esempio 9.4. Sia $A = \mathbb{K}[x]$ vista come \mathbb{K} -algebra, allora una rappresentazione è univocamente determinata dall'immagine di x , dunque per identificare una rappresentazione basterà sapere V e $\rho(x)$. Se $\mathbb{K} = \overline{\mathbb{K}}$ si osserva che le rappresentazioni irriducibili sono quelle di grado 1 e sono determinate dal parametro $\lambda \in \mathbb{K}$ tale che $\rho(x) = \lambda$. Si può vedere inoltre che le rappresentazioni indecomponibili sono solo quelle per cui $\rho(x)$ è simile a $J_{n,\lambda}$ dove $J_{n,\lambda}$ è il blocco di Jordan di dimensione n e autovalore λ .

Da questo esempio si osserva che il concetto di irriducibilità è diverso da quello di indecomponibilità.

Esercizio 9.2. QUI CI SAREBBE UN ESERCIZIO CHE RIGUARDA LA MITICA ALGEBRA UNIVERSALE INVILUPPANTE...

Lemma 9.1 (Schur). *Sia A una \mathbb{K} -algebra, $\phi : V \rightarrow W$ un omomorfismo di A -moduli con $\phi \neq 0$, allora*

1. *se V è semplice allora ϕ è iniettivo*
2. *se W è semplice allora ϕ è surgettivo*

Dunque se V e W sono semplici allora ϕ è un isomorfismo.

Dimostrazione. Identica a quella fatta per i gruppi, dove si usa che $\text{Ker } \phi$ e $\text{Im } \phi$ sono sottomoduli rispettivamente di V e W . \square

Corollario. Se \mathbb{K} è algebricamente chiuso, $\phi \in \text{End}_A(V)$, V è un A -modulo semplice, allora $\exists \lambda \in \mathbb{K}^*$ tale che $\phi = \lambda \text{Id}$.

Corollario. Se V è un A -modulo semplice allora $\text{End}_A(V)$ è un'algebra di divisione.

Quello che abbiamo definito prima più precisamente si chiama A -modulo sinistro, andiamo a dare un'altra definizione

Definizione 9.9. Chiamiamo A^{OP} l'algebra opposta di A , $A^{OP} = A$ come spazio vettoriale, ma il prodotto in A^{OP} è $a * b = ba$.

Definizione 9.10. Un A -modulo destro è una rappresentazione di A^{OP} . Se $\rho : A^{OP} \rightarrow \text{End}(V)$ è una rappresentazione allora V è un A -modulo destro.

Esempio 9.5. Alcuni esempi di algebre isomorfe alle loro algebre opposte

1. $\phi : M_n(\mathbb{K}) \rightarrow M_n(\mathbb{K})$ dove $\phi(x) = x^T$ è un isomorfismo di algebre tra $(M_n(\mathbb{K}))$ e $(M_n(\mathbb{K}))^{OP}$.
2. $\phi : \mathbb{K}[G] \rightarrow \mathbb{K}[G]$ dove $\phi(e_g) = e_{g^{-1}}$ ed estendendolo per linearità, ϕ è un isomorfismo di algebre tra $\mathbb{K}[G]$ e $\mathbb{K}[G]^{OP}$.

Definizione 9.11. Sia $\rho : A \rightarrow \text{End}(V)$ una rappresentazione di A , definiamo la *rappresentazione duale* $\rho^* : A^{OP} \rightarrow \text{End}(V^*)$ dove

$$(\rho^*(x)f)(v) = f(x \cdot v)$$

Proposizione 9.2. Abbiamo un isomorfismo di algebre $A^{OP} \cong \text{End}_A(A)$ dove A è pensato come A -modulo sinistro.

Dimostrazione. Se $x \in A$, definiamo $r_x : A \rightarrow A$ come $r_x(a) = ax$, allora $r_x \in \text{End}_A(A)$ poichè $r_x(ba) = bax = br_x(a)$.

Consideriamo allora $\Phi : A^{OP} \rightarrow \text{End}_A(A)$ tale che $\Phi(x) = r_x$. Se $\phi \in \text{End}_A(A)$ allora $\phi(a) = \phi(a \cdot 1) = a \cdot \phi(1) = r_{\phi(1)}(a)$, cioè Φ è surgettiva.

Vediamo ora che Φ è omomorfismo di algebre: $\Phi(a * b)(t) = \Phi(ba)(t) = r_{ba}(t) = tba = r_a(tb) = r_a \circ r_b(t)$.

Mostriamo infine che è iniettiva: se $\Phi(x) = r_x = \text{Id}$, abbiamo $ax = r_x(a) = a \ \forall a \in A$, e in particolare se $a = 1$, abbiamo $x = 1$ \square

9.2 Ideali e quozienti

Definizione 9.12. Un ideale *sinistro* di $A \supseteq I$ è un sottospazio vettoriale tale che $aI \subseteq I \ \forall a \in A$. Un ideale *destro* è un sottospazio chiuso per la moltiplicazione a destra per elementi di A , un ideale è *bilatero* se è sia destro che sinistro.

Osservazione. I è un ideale destro se e solo se I è un A^{OP} -sottomodulo, I è un ideale sinistro se e solo se è un A -sottomodulo.

Osservazione. Se $I \subseteq A$ è un ideale sinistro allora A/I è un A -modulo, se è un ideale destro allora A/I è un A^{OP} -modulo, se I è bilatero allora A/I è un'algebra definendo $(a + I)(b + I) = ab + I$.

Esempio 9.6. Sia $\phi : A \rightarrow A'$ un omomorfismo di algebre, allora $\text{Ker } \phi$ è un ideale bilatero di A e $\text{Im } \phi \cong A / \text{Ker } \phi$ come algebre.

Definizione 9.13. A è un'algebra semplice se non ha ideali bilateri non banali.

Osservazione. Sia V un A -modulo sinistro, fissiamo $v \in V$, sia $\phi : A \rightarrow V$ come $\phi(x) = x \cdot v$. Si osserva che ϕ è lineare e che è un omomorfismo di A -moduli vedendo A come A -modulo, dunque $\text{Ker } \phi$ è un ideale sinistro.

Osservazione. In aggiunta alle ipotesi di prima sia V un A -modulo semplice, $v \neq 0$, allora $\text{Im } \phi = V$ e dunque $V \cong A / \text{Ker } \phi$ come A -moduli.

Definizione 9.14. Un A -modulo V è detto *semisemplice* se è somma diretta di A -moduli semplici. Equivalentemente V è detto semisemplice se ogni sottomodulo ammette un complementare stabile.

Esercizio 9.3. Sia $A = \mathbb{K}[G]$ (CON G FINITO????), allora ogni A -modulo di dimensione finita è semisemplice.

Proposizione 9.3. Sia V un A -modulo semisemplice, allora V è semplice se e solo se $\text{End}_A(V)$ è un'algebra di divisione.

Dimostrazione. \Rightarrow) Per il lemma di Schur.

\Leftarrow) Supponiamo che $V = V_1 \oplus V_2$ sia una decomposizione in A -moduli. Siano $\pi_1 : V \rightarrow V$ e $\pi_2 : V \rightarrow V$ le proiezioni associate alla decomposizione. Si osserva π_1 e π_2 sono omomorfismi di A -moduli e che entrambi sono diversi da 0, tuttavia $\pi_1 \circ \pi_2 = 0$, quindi avremmo che $\text{End}_A(V)$ non è un'algebra di divisione, assurdo.

□

9.3 Serie di composizione

Definizione 9.15. Sia A una \mathbb{K} -algebra, V un A -modulo di dimensione finita. Si chiama *filtrazione* per V una sequenza di sottomoduli tale che

$$0 = V_0 \subseteq V_1 \subseteq \dots \subseteq V_n = V$$

Diciamo che una filtrazione è una *serie di composizione* (o serie di Jordan-Holder) se i quozienti V_i/V_{i-1} sono tutti A -moduli semplici. Questi quozienti sono detti *fattori di composizione* della serie.

Esercizio 9.4. Se $W \subseteq V$ sono A -moduli, allora W è un sottomodulo proprio massimale se e solo se V/W è semplice.

Proposizione 9.4. Ogni A -modulo V di dimensione finita ammette una serie di composizione di lunghezza finita.

Dimostrazione. Per induzione su $\dim V$: se V è irriducibile ho finito, altrimenti sia V_1 un sottomodulo irriducibile (basta prenderne uno minimale). Consideriamo ora V/V_1 , per ipotesi induttiva esso ammette una serie di decomposizione di lunghezza finita, prendendo le controimmagini della serie per V/V_1 tramite la proiezione al quoziente si ottiene una serie di Jordan-Holder.

FORSE DA SPIEGARE MEGLIO PERCHE'...

□

Osservazione. Se V è somma diretta di irriducibili (V semisemplice), allora i fattori di composizione di qualsiasi serie per V sono proprio gli irriducibili di V contati con molteplicità.

Teorema 9.5 (di Jordan-Holder). Sia V un A -modulo di dimensione finita, allora tutte le serie di composizione per V hanno la stessa lunghezza (che chiamiamo *lunghezza del modulo*), e gli stessi fattori di composizione (contati con molteplicità e a meno di permutazioni).

Dimostrazione. Per induzione su $\dim V$: se V è irriducibile ho finito, supponiamo dunque che abbia sottomoduli non banali, siano

$$\begin{aligned} 0 = V_0 \subseteq \dots \subseteq V_m = V & & W_i = V_i/V_{i-1} \\ 0 = V'_0 \subseteq \dots \subseteq V'_n = V & & W'_i = V'_i/V'_{i-1} \end{aligned}$$

due serie di Jordan-Holder per V . Se $V_1 = V'_1$ considero V/V_1 , per ipotesi induttiva ho l'unicità. Supponiamo dunque che $V_1 \neq V'_1$, visto che V_1 e V'_1 sono irriducibili si ha che $V_1 \cap V'_1 = 0$, dunque $V_1 + V'_1 = V_1 \oplus V'_1$.

Considero il modulo $V/V_1 \oplus V'_1$, siano Z_1, \dots, Z_p i fattori di composizione di una serie di Jordan-Holder per $V/V_1 \oplus V'_1$. Ma allora si ha che

1. V/V_1 ammette due serie di composizione con fattori

$$V'_1, Z_1, \dots, Z_p \quad W_2, \dots, W_m$$

2. V/V'_1 ammette due serie di composizione con fattori

$$V_1, Z_1, \dots, Z_p \quad W'_2, \dots, W'_n$$

Per ipotesi induttiva ho l'unicità delle serie per V/V_1 e V/V'_1 , dunque si ha che $n = m = p + 2$. Sempre per via dell'unicità si ha che

$$\begin{aligned} \{W'_1, Z_1, \dots, Z_p\} &= \{W_2, \dots, W_m\} \\ \{W_1, Z_1, \dots, Z_p\} &= \{W'_2, \dots, W'_m\} \end{aligned}$$

da cui, aggiungendo W_1 agli insiemi¹⁷ nella prima riga e W'_1 a quelli della seconda si ottiene

$$\begin{aligned} \{W'_1, W_1, Z_1, \dots, Z_p\} &= \{W_1, W_2, \dots, W_m\} \\ \{W'_1, W_1, Z_1, \dots, Z_p\} &= \{W'_1, W'_2, \dots, W'_m\} \end{aligned}$$

essendo uguali i membri di sinistra ho uguaglianza anche dei membri di destra e quindi segue la tesi. \square

Esempio 9.7. Sia $A = \mathbb{K}[G]$ con $\text{char } \mathbb{K} \nmid \text{ord}(G)$, allora ogni rappresentazione di dimensione finita è somma di moduli irriducibili. I fattori di composizione coincidono con gli addendi irriducibili contati con molteplicità.

Osservazione. Sia V un A -modulo, $W \subseteq V$ un sottomodulo, allora esiste sempre una serie di Jordan-Holder che contiene W ($W = V_i$ per qualche i): basta considerare prima una serie per W e comporla con la controimmagine tramite la proiezione al quoziente di una serie per V/W .

Corollario. Sia V un A -modulo semplice con $\dim_{\mathbb{K}} A < \infty$, allora V compare come fattore di composizione in qualsiasi serie di Jordan-Holder per A (considerando A come A -modulo sinistro).

Dimostrazione. Fisso $v \in V, v \neq 0$ e considero $\phi : A \rightarrow V$ tale che $\phi(a) = av$, allora ϕ è surgettiva (siccome V è semplice), $I = \text{Ker } \phi \subseteq A$ è un ideale sinistro e si ha che $V \cong A/I$ come A -moduli. I è un sottomodulo di A , quindi esiste una serie di composizione per A che contiene I : esistono I_0, \dots, I_n ideali sinistri di A tali che

$$0 = I_0 \subseteq \dots \subseteq I_n = A \quad \text{con } I_k/I_{k-1} \text{ semplice } \forall k$$

¹⁷non sono esattamente insiemi dato che devono contare i fattori con molteplicità

Sia $p \in \mathbb{N}$ tale che $I = I_p$, si osserva che $p = n - 1$ poichè A/I è semplice (dunque non posso allungare la serie), quindi $I_n/I_{n-1} = A/I \cong V$. Abbiamo provato dunque che in una serie di composizione troviamo un fattore uguale a V , avendo dimostrato l'unicità dei fattori della serie col teorema 9.5 segue la tesi. \square

Esempio 9.8. Sia $A = \mathbb{K}[x]/(x^n)$, consideriamo la serie

$$0 \subset (x^{n-1})/(x^n) \subset (x^{n-2})/(x^n) \subset \dots \subset \mathbb{K}[x]/(x^n)$$

Tutti i fattori di composizione sono isomorfi alla rappresentazione banale (dove x agisce come 0 e gli scalari agiscono come scalari), dunque l'unico modulo irriducibile è quello banale (OVVERO IL CAMPO \mathbb{K} ??). In particolare $\mathbb{K}[x]/(x^n)$ ammette un'unica rappresentazione irriducibile a meno di isomorfismo.

Esempio 9.9. Sia $A = M_n(\mathbb{K})$, un modulo irriducibile è \mathbb{K}^n , per ogni $i = 1, \dots, n$ sia

$$V_i = \{M \in A : M_{p,q} = 0 \ \forall q > i\}$$

ovvero V_i è l'insieme delle matrici appartenenti ad A con le ultime $n - i$ colonne nulle (in realtà è un sottomodulo). Consideriamo la serie

$$0 \subset V_1 \subset \dots \subset V_n = M_n(\mathbb{K})$$

si osserva che $V_i/V_{i-1} \cong \mathbb{K}^n$, dunque tutti i quozienti sono irriducibili e isomorfi tra loro, ma allora \mathbb{K}^n è l'unica rappresentazione irriducibile di $M_n(\mathbb{K})$ a meno di isomorfismo.

9.4 Teorema di Krull-Schmidt

Definizione 9.16. Sia $x \in A$, x è *nilpotente* se $\exists n \in \mathbb{N}$ tale che $x^n = 0$, x è *idempotente* se $x^2 = x$.

Proposizione 9.6. Sia V un A -modulo, allora V è indecomponibile se e solo se per ogni $\phi \in \text{End}_A(V)$ idempotente si ha che $\phi = 0$ o $\phi = \text{Id}$.

Dimostrazione. \Leftarrow) Se V non è indecomponibile allora $V = W \oplus W'$ con $W, W' \neq V$, sia $p \in \text{End}_A(V)$ la proiezione su W associata, allora $p^2 = p$, $p \neq 0$, $p \neq \text{Id}$, assurdo.

\Rightarrow) Sia $p \in \text{End}_A(V)$ tale che $p^2 = p$, voglio vedere che $p = 0$ o $p = \text{Id}$. Si osserva subito che $\text{Ker } p \cap \text{Im } p = 0$ (per l'ipotesi $p^2 = p$), dunque $V = \text{Ker } p \oplus \text{Im } p$, ma allora deve succedere che $\text{Ker } p = 0$ o $\text{Im } p = 0$ (poichè V è indecomponibile), se $\text{Im } p = 0$ allora $p = 0$, se $\text{Ker } p = 0$ allora $p = \text{Id}$ poichè $p^2 = p$. \square

Lemma 9.7. Siano V, W degli A -moduli indecomponibili di dimensione finita su \mathbb{K} , siano $\alpha \in \text{Hom}_A(V, W)$ e $\beta \in \text{Hom}_A(W, V)$ tali che $\beta \circ \alpha$ è un isomorfismo su V , allora α e β sono isomorfismi.

Dimostrazione. Vediamo che $W = \text{Ker } \beta \oplus \text{Im } \alpha$:

1. $\text{Ker } \beta \cap \text{Im } \alpha = 0$ poichè altrimenti $\beta \circ \alpha$ avrebbe nucleo diverso da 0 ma sappiamo che $\beta \circ \alpha$ è un isomorfismo.
2. Sia $x \in W$, sia $y = (\alpha \circ (\alpha \circ \beta)^{-1} \circ \beta)(x)$, allora $y \in \text{Im } \alpha$, consideriamo ora $\beta(y) = (\beta \circ \alpha) \circ (\beta \circ \alpha)^{-1} \circ \beta(x) = \beta(x)$, dunque $x - y \in \text{Ker } \beta$, quindi $W = \text{Im } \alpha \oplus \text{Ker } \beta$.

Ma W è indecomponibile, quindi $\text{Ker } \beta = 0$ o $\text{Im } \alpha = 0$, la seconda situazione non può accadere (altrimenti $\beta \circ \alpha$ non sarebbe un isomorfismo), ma allora $\text{Ker } \beta = 0$ e $\text{Im } \alpha = W$, visto che necessariamente α è iniettivo (altrimenti non lo sarebbe $\beta \circ \alpha$) si ha che α è un isomorfismo, e dunque anche β lo è. \square

Proposizione 9.8. *Sia V un A -modulo indecomponibile e $\phi \in \text{End}_A(V)$, allora ϕ è un isomorfismo oppure è nilpotente.*

Dimostrazione. Sia $\phi \in \text{End}_A(V)$, considero le due successioni

$$\begin{aligned} \dots \supseteq \text{Ker } \phi^n \supseteq \text{Ker } \phi^{n-1} \supseteq \dots \supseteq \text{Ker } \phi^0 \\ \dots \subseteq \text{Im } \phi^n \subseteq \text{Im } \phi^{n-1} \subseteq \dots \subseteq \text{Im } \phi^0 \end{aligned}$$

Queste successioni si devono stabilizzare, sia dunque N tale che $\text{Ker } \phi^N = \text{Ker } \phi^{N+1}$ e $\text{Im } \phi^N = \text{Im } \phi^{N+1}$, allora si ha che $\text{Ker } \phi^N \cap \text{Im } \phi^N = 0$ (altrimenti non si sarebbero stabilizzate le successioni), ma allora $V = \text{Ker } \phi^N \oplus \text{Im } \phi^N$ per questioni di dimensioni.

Per ipotesi V è indecomponibile dunque $\text{Im } \phi^N = 0$ oppure $\text{Ker } \phi^N = 0$, se $\text{Im } \phi^N = 0$ allora ϕ è nilpotente, se invece $\text{Ker } \phi^N = 0$ allora a maggior ragione $\text{Ker } \phi = 0$ e dunque ϕ è un isomorfismo. \square

Corollario. *Sia V un A -modulo indecomponibile, siano $\theta_1, \dots, \theta_s \in \text{End}_A(V)$ con θ_i nilpotente per $i = 1, \dots, s$, allora $\theta_1 + \dots + \theta_s$ è nilpotente.*

Dimostrazione. Sia $\theta = \sum_{i=1}^s \theta_i \in \text{End}_A(V)$, per la proposizione precedente sappiamo che θ è un isomorfismo oppure è nilpotente. Procediamo per induzione su s :

- Se $s = 1$ allora $\theta = \theta_1$ che è nilpotente.
- Supponiamo la tesi vera per $s = n - 1$ e dimostriamola per $s = n$: supponiamo per assurdo che θ sia un isomorfismo, allora avremmo che

$$\text{Id} = \theta^{-1}\theta_1 + \dots + \theta^{-1}\theta_n$$

Si osserva subito che $\theta^{-1}\theta_i$ è nilpotente (dato che ha nucleo non nullo non è un isomorfismo e dunque è nilpotente), quindi

$$\text{Id} - \theta^{-1}\theta_n = \theta^{-1}\theta_1 + \dots + \theta^{-1}\theta_{n-1}$$

Sappiamo per ipotesi induttiva che la somma di $n - 1$ endomorfismi nilpotenti è ancora nilpotente, dunque il termine di destra dell'equazione è nilpotente, ma questo è assurdo essendo quello di sinistra un isomorfismo: se ϕ è nilpotente con indice di nilpotenza k allora $\text{Id} - \phi$ è un isomorfismo, infatti

$$(\text{Id} - \phi) \cdot (1 + \phi + \dots + \phi^{k-1}) = \text{Id} - \underbrace{\phi^k}_{=0} = \text{Id}$$

\square

Teorema 9.9 (Krull-Schmidt). *Sia A una \mathbb{K} -algebra di dimensione finita, V un A -modulo con $\dim V < \infty$. Allora V si decompone in modo unico come somma di rappresentazioni indecomponibili (a meno di isomorfismo e permutazioni).*

Dimostrazione. Poiché V ha dimensione finita, per induzione lo spezzo finché non ho tutti addendi diretti indecomponibili. Occorre adesso provare l'unicità.

Sia $V = \bigoplus_{i=1}^m W_i = \bigoplus_{i=1}^n W'_i$; allora ho le inclusioni e proiezioni standard:

$$\begin{array}{ll} i_p : W_p \rightarrow V & \pi_p : V \rightarrow W_p \\ i'_p : W'_p \rightarrow V & \pi'_p : V \rightarrow W'_p \end{array}$$

Definiamo ora $\theta_s = \pi_1 \circ i'_s \circ \pi'_s \circ i_1$ seguendo la catena $W_1 \xrightarrow{i_1} V \xrightarrow{\pi'_s} W'_s \xrightarrow{i'_s} V \xrightarrow{\pi_1} W_1$. Poiché le proiezioni e le inclusioni sono omomorfismi di A -moduli, allora abbiamo $\theta_s \in \text{End}_A(W_1)$.

Osserviamo ora che $\theta_1 + \dots + \theta_n = \text{Id}_{W_1}$: se infatti prendiamo una base $\{w'_{i,j}\}_j$ di W'_i , concatenandole otteniamo una base di V ; scriviamo ora un elemento $v \in W_1$ in coordinate: $v = (a_{i,j})$. La mappa i_1 non fa nulla; quando proietto su W'_s invece annullo tutte le coordinate non relative a quel sottospazio, ovvero $\pi'_s \circ i_1(v) = (0, \dots, 0, a_{s,1}, \dots, a_{s, \dim W'_s}, 0, \dots, 0)$; di nuovo l'inclusione non cambia le coordinate. Infine $\sum \theta_s(v) = \sum \pi_1 \circ i'_s \circ \pi'_s \circ i_1(v) = \pi_1 \left(\sum i'_s \circ \pi'_s \circ i_1(v) \right)$ e per quanto detto prima, quando sommiamo su tutti i W'_s è come se reincollassimo tutte le componenti; in particolare $\sum i'_s \circ \pi'_s \circ i_1(v) = (a_{i,j})$ e quindi $\pi_1(a_{i,j}) = v$.

Per la proposizione 9.8, essendo V_1 indecomponibile, ogni θ_s è un isomorfismo, oppure nilpotente. Se tutti i θ_s fossero nilpotenti, per il corollario 9.4, anche $\sum \theta_s = \text{Id}_{W_1}$ sarebbe nilpotente. Perciò esiste un indice \tilde{s} , che possiamo supporre essere 1 a meno di riordinare i W'_i , tale che $\theta_{\tilde{s}}$ è un isomorfismo. Allora per il lemma 9.7, abbiamo che $\phi = \pi_1 \circ i'_1$ e $\pi'_1 \circ i_1$ sono isomorfismi tra W_1 e W'_1 .

Siano ora $Z = \bigoplus_{i=2}^m W_i$ e $Z' = \bigoplus_{i=2}^n W'_i$; osserviamo che $V = W'_1 \oplus Z'$, perciò ho la proiezione $\pi : V \rightarrow Z'$, che è omomorfismo di moduli. Osserviamo che $\dim Z = \dim Z'$ grazie all'isomorfismo di W_1 e W'_1 . Possiamo allora definire $\psi : Z \rightarrow Z'$ nel modo ovvio $Z \xrightarrow{i} V \xrightarrow{\pi} Z'$. Mostriamo che ψ è un isomorfismo; essendo le dimensioni degli spazi uguali, basta l'iniettività.

Osserviamo che $\ker \psi = Z \cap \ker \pi = Z \cap i'_1(W'_1)$; se prendiamo $z \in Z \cap i'_1(W'_1)$, avremmo che $\pi_1(z) = 0$, essendo $z \in Z$; inoltre $\pi_1(z) = \phi(w)$ per un qualche $w \in W'_1$. Essendo ϕ un isomorfismo tra W_1 e W'_1 , si ha $w = \phi^{-1}(0) = 0$ da cui $z = i'_1(0) = 0$. \square

9.5 Semisemplicità

Definizione 9.17. Un A -modulo V si dice *semisemplice* se ogni sottomodulo ammette un complemento stabile; ovvero per ogni $W \subset V$ tale che $AW \subset W$, esiste un $W' \subset V$ con $AW' \subset W'$ per cui $V = W \oplus W'$.

Lemma 9.10. *Sia V un A -modulo semisemplice; allora quozienti e sottomoduli di V sono semisemplici.*

Dimostrazione. Sia $W \subset V$ un sottomodulo; consideriamo allora $Z \subset W$ stabile. Ma se guardiamo Z come sottomodulo di V , che è semisemplice, sappiamo trovare un sottomodulo $Z' \subset V$ tale che $V = Z \oplus Z'$; perciò la proiezione $p : V \rightarrow Z$ è omomorfismo di A -moduli. Se guardo la restrizione $p|_W : W \rightarrow Z$ è ancora una proiezione, perciò abbiamo $W = Z \oplus \ker p|_W$, che è quello che volevamo, in quanto il nucleo è A -stabile.

Sia ora W un quoziente di V , ovvero $W \cong V/Z$ per un qualche sottomodulo $Z \subset V$. La proiezione al quoziente $\pi : V \rightarrow W$ è un omomorfismo di A -moduli, poiché Z è stabile: $a\pi(v) = a(v + Z) = av + aZ = av + Z = \pi(av)$.

Allora $\ker \pi$ è un sottomodulo di V , che allora ammette complemento stabile $V = \ker \pi \oplus W'$; sappiamo che $W \cong V/\ker \pi$, ma allora $W \cong W'$ tramite $\pi|_{W'}$. \square

Proposizione 9.11. *Sia V un A -modulo di dimensione finita. Allora sono equivalenti*

1. V è semisemplice
2. V è somma diretta di A -moduli semplici
3. V è somma di A -moduli semplici

Dimostrazione.

$1 \Rightarrow 2$ Per induzione su $\dim V$; se V è semplice, ho finito. Se invece esiste un sottomodulo $W \subset V$, trovo un complemento stabile $V = W \oplus W'$ e ho $\dim W, \dim W' < \dim V$; inoltre per il lemma 9.10 sia W che W' sono semisemplici, quindi posso applicare l'induzione e scriverli come somma diretta di moduli semplici.

$2 \Rightarrow 3$ Ovvio

$3 \Rightarrow 1$ Scriviamo $V = \sum V_i$ con i V_i semplici; prendiamo un sottomodulo W e cerchiamone un complemento.

In particolare, sia W' un sottomodulo massimale tale che $W \cap W' = 0$; supponiamo per assurdo che $W \oplus W' \subsetneq V$. Allora esiste un $V_i \not\subset W \oplus W'$, e in particolare $V_i \cap W \oplus W' = 0$ in quanto V_i è semplice.

Ma allora $V_i \cap W' = 0$, perciò posso considerare $V_i \oplus W'$; inoltre se $z \in V_i \oplus W' \cap W$, vuol dire che $w = v + w'$, cioè $V_i \ni v = w - w' \in W \oplus W'$, ovvero $v = 0$, e poi $w = w' = 0$. Dunque $V_i \oplus W'$ sarebbe un sottomodulo che non interseca W e più grande del massimale, assurdo. Quindi si ha $W \oplus W' = V$.

□

Teorema 9.12 (Maschke). *Sia G un gruppo finito, \mathbb{K} un campo tale che $\text{char } \mathbb{K} \nmid \text{ord } G$. Allora ogni rappresentazione di $\mathbb{K}[G]$ è semisemplice.*

Dimostrazione. Osserviamo che se $\text{char } \mathbb{K} = 0$, l'abbiamo fatto nella prima parte (teorema 4.4).

Chiamiamo $A = \mathbb{K}[G]$ l'algebra e V la rappresentazione. Sia $W \subset V$ un sottomodulo.

Consideriamo intanto $W' \subset V$ complemento di W , non stabile, ma tale che $V = W \oplus W'$; sia $p : V \rightarrow W$ la proiezione.

Definiamo allora l'applicazione lineare

$$\pi(v) = \frac{1}{\text{ord } G} \sum_{g \in G} g \cdot p(g^{-1} \cdot v)$$

Osserviamo che possiamo dividere per $\text{ord } G$ per l'ipotesi sul campo (cioè $\text{ord } G \neq 0$).

Vale banalmente la proprietà $\pi(w) = w$ se $w \in W$: infatti $g^{-1}w \in W$, perciò $gp(g^{-1}w) = w$.

Inoltre $\pi \in \text{Hom}_A(V, W)$, poichè $\pi(hv) = \frac{1}{\text{ord } G} \sum_{g \in G} g \cdot p(g^{-1}hv) = \frac{1}{\text{ord } G} \sum_{g \in G} hg^{-1}g \cdot p((h^{-1}g)^{-1}v) =$

$\frac{1}{\text{ord } G} \sum_{t \in G} ht \cdot p(t^{-1}v) = h\pi(v)$ dove abbiamo effettuato la sostituzione $t = h^{-1}g$ che permuta gli elementi del gruppo.

Infine π è idempotente: $\pi^2(v) = \frac{1}{\text{ord } G} \sum_{g \in G} \pi(g \cdot p(g^{-1} \cdot v)) = \frac{1}{\text{ord } G} \sum_{g \in G} g \cdot \pi(p(g^{-1} \cdot v))$; dato che

p mappa tutto su W , abbiamo $\pi(p(z)) = p(z)$, perciò abbiamo esattamente quello che ci serviva.

Allora π è una proiezione, e vale $V = W \oplus \ker \pi$, dove $\ker \pi$ è un A -modulo, essendo π un omomorfismo di rappresentazioni. □

Definizione 9.18. Una \mathbb{K} -algebra A si dice *semisemplice* se A è un A -modulo semisemplice

Teorema 9.13. *Sia G un gruppo finito, \mathbb{K} un campo. Allora $\mathbb{K}[G]$ è semisemplice se e solo se $\text{char } \mathbb{K} \nmid \text{ord } G$.*

Dimostrazione. Una freccia l'abbiamo appena fatta: basta considerare $\mathbb{K}[G]$ come rappresentazione su se stesso, e applicare 9.12.

Dimostriamo ora che se $\text{char } \mathbb{K} \mid \text{ord } G$, allora $A = \mathbb{K}[G]$ non è semisemplice. Sia $s = \sum_{g \in G} e_g$ e $V_0 = \mathbb{K}s$ che è banalmente un sottomodulo di A .

Supponiamo per assurdo che A sia semisemplice; allora V_0 avrebbe un complementare stabile $A = V_0 \oplus V_1$, e avremmo la proiezione $p : A \rightarrow V_0$ che è omomorfismo di A -moduli.

Allora varrebbe $p(e_g) = p(ge_1) = gp(e_1) = p(e_1)$ poiché su V_0 G agisce banalmente. Perciò $p(s) = \sum p(e_g) = \text{ord } G \cdot p(e_1) = 0$.

Ma questo è assurdo, poiché dovrebbe essere $p(s) = s$ essendo p la proiezione su V_0 . □

9.6 Struttura di $\mathbb{K}[G]$ come algebra

In questa sezione vogliamo dare un teorema di struttura per $\mathbb{K}[G]$ (con $\text{char } \mathbb{K} \nmid |G|$).

Cerchiamo ora di descrivere $\mathbb{K}[G]$ come algebra nel caso di $\mathbb{K} = \overline{\mathbb{K}}$.

Teorema 9.14. *Sia G gruppo finito, $\mathbb{K} = \overline{\mathbb{K}}$ tale che $\text{char } \mathbb{K} \nmid |G|$, e sia V una rappresentazione irriducibile di $\mathbb{K}[G]$. Allora $\dim V < \infty$, e si ha $\text{End}_G(V^{\oplus n}) \cong M_n(\mathbb{K})$ come \mathbb{K} -algebre.*

Dimostrazione. Sia $A = \mathbb{K}[G]$, $0 \neq v \in V$; allora ho un omomorfismo di rappresentazioni $f(a) = av$, la cui immagine è V essendo semplice. Perciò si ha $V \cong A / \ker f$, e poiché A ha dimensione finita, anche V ha dimensione finita.

Considero ora le immersioni/proiezioni canoniche

$$\begin{aligned} q_i : V &\rightarrow V^{\oplus n} && \text{con } i = 1, \dots, n \\ p_i : V^{\oplus n} &\rightarrow V && \text{con } i = 1, \dots, n \end{aligned}$$

Sia $\varphi \in \text{End}_G(V^{\oplus n})$, consideriamo $\varphi_{ij} : V \rightarrow V$ definita come $\varphi_{ij} = p_i \circ \varphi \circ q_j \in \text{End}_G(V)$:

$$V \xrightarrow{q_i} V^{\oplus n} \xrightarrow{\varphi} V^{\oplus n} \xrightarrow{p_j} V$$

V è irriducibile quindi $\varphi_{ij} = c_{ij} \text{Id}_V$ con $c_{ij} \in \mathbb{K}$ (per Schur), dunque trovo un'applicazione

$$\begin{aligned} \psi : \text{End}_G(V^{\oplus n}) &\rightarrow M_n(\mathbb{K}) \\ \varphi &\rightarrow (c_{ij}) \end{aligned}$$

Mostriamo ora che ψ è un isomorfismo di algebre: ψ è surgettiva, infatti, data $(c_{ij}) \in M_n(\mathbb{K})$, se consideriamo $\varphi = \sum c_{ij} q_i \circ p_j$ abbiamo che $\psi(\varphi) = (c_{ij})$; dimostriamo che è un omomorfismo, infatti siano $\varphi_1 = \sum c_{ij} q_i \circ p_j$ e $\varphi_2 = \sum d_{ij} q_i \circ p_j$, allora $\varphi_1 \circ \varphi_2 = \sum c_{ij} d_{hk} q_i \circ p_j \circ q_h \circ p_k = \sum c_{ij} d_{jk} q_i \circ p_k$ dove l'ultima uguaglianza si ottiene dal fatto che se $j = h$ allora $p_j \circ q_h = \text{Id}_V$, altrimenti è l'endomorfismo nullo, infine $\psi(\varphi_1 \circ \varphi_2) = \sum c_{ij} d_{jk} q_i \circ p_k$ come per il prodotto tra matrici; la verifica dell'iniettività è immediata. □

Teorema 9.15. *Sia $\mathbb{K} = \overline{\mathbb{K}}$ con $\text{char } \mathbb{K} \nmid |G|$ dove G è un gruppo finito. Siano V_1, \dots, V_n le rappresentazioni irriducibili di G su \mathbb{K} (a meno di isomorfismi) e siano m_1, \dots, m_n le loro dimensioni. Allora come \mathbb{K} -algebre abbiamo un isomorfismo $\mathbb{K}[G] \cong M_{m_1}(\mathbb{K}) \times \dots \times M_{m_n}(\mathbb{K})$. In particolare $\mathbb{K}[G]$ è isomorfo ad un prodotto di algebre di matrici e $M_{m_h}(\mathbb{K}) = m_h V_h$.*

Dimostrazione. $\mathbb{K}[G]$ è semisemplice e di dimensione finita, sarà somma diretta di moduli semplici: $\mathbb{K}[G] \cong W_1 \oplus \dots \oplus W_n$ con W_i un G -modulo semplice. Si osserva che tutti gli irriducibili di G compaiono tra i W_i : avevamo visto che tutti gli irriducibili devono comparire come fattori di composizione delle serie di Jordan-Holder di A . Quindi posso riscrivere $\mathbb{K}[G] = \oplus V_i^{p_i}$ dove p_i è la molteplicità di V_i , allora $\dim \text{Hom}_G(\mathbb{K}[G], V_i) = \dim \text{Hom}_G(V_i^{\oplus p_i}, V_i) = p_i$. Considero ora l'omomorfismo $\psi : \text{Hom}_G(\mathbb{K}[G], V_i) \rightarrow V_i$ definito come $\psi(\phi) = \phi(e_1)$, esso è un isomorfismo (la verifica è facile), e quindi $p_i = m_i$. Ma $\mathbb{K}[G] \cong \mathbb{K}[G]^{OP}$ grazie all'applicazione inversa $g \rightarrow g^{-1}$, $\mathbb{K}[G]^{OP}$ lo posso pensare come $\text{End}_{\mathbb{K}[G]}(\mathbb{K}[G]) \cong \text{End}_{\mathbb{K}[G]}(\oplus V_i^{m_i}) \cong \oplus \text{End}_{\mathbb{K}[G]}(V_i^{m_i})$ dove l'ultimo isomorfismo segue da Schur. Per il teorema 9.14 si ha che $\text{End}_{\mathbb{K}[G]}(V_i^{m_i}) \cong M_{m_i}(\mathbb{K})$ ma allora $\mathbb{K}[G] \cong \oplus M_{m_i}(\mathbb{K})$. \square

Da adesso considereremo A un'algebra di dimensione finita.

Proposizione 9.16. *Se A è un'algebra semisemplice allora ogni rappresentazione di A di dimensione finita è semisemplice.*

Dimostrazione. Sia V un A -modulo, $\dim V = r$, consideriamo l' A -modulo di dimensione finita $A^{\oplus r}$ dove A agisce per componenti. Sappiamo che A è semisemplice, quindi $A = \oplus_{j=1}^k I_j$ con I_j irriducibile (ovvero ideali sinistri minimali), allora $A^r = \oplus_{h=1}^r \oplus_{j=1}^k I_{hj}$ dove I_{hj} è I_j immerso nella j -esima copia di A . Gli I_{hj} sono tutti moduli irriducibili quindi A^r è semisemplice. Fissiamo un insieme di generatori $V = \langle v_1, \dots, v_r \rangle$ e consideriamo l'omomorfismo

$$\begin{aligned} \psi : A^r &\rightarrow V \\ (a_1, \dots, a_r) &\rightarrow a_1 v_1 + \dots + a_r v_r \end{aligned}$$

ψ è evidentemente surgettiva ed è un omomorfismo di A -moduli, quindi V è semisemplice poichè $V \cong A^r / \text{Ker } \psi$ e abbiamo dimostrato che quozienti di semisemplici sono semisemplici (lemma 9.10). \square

Definizione 9.19. Un'algebra di divisione D sul campo \mathbb{K} è un'algebra associativa, unitaria su \mathbb{K} tale che ogni suo elemento ammette inverso.

Osservazione. Se $\mathbb{K} = \overline{\mathbb{K}}$ e D è una \mathbb{K} -algebra di divisione con $\dim D < \infty$, allora $D = \mathbb{K}$. Infatti $\mathbb{K} \subset D$ (poichè $\mathbb{K} = \text{Span}(1)$), supponiamo per assurdo che esista $x \in D \setminus \mathbb{K}$, ma visto che $\dim D < \infty$ allora le potenze di x soddisfano un'equazione finita in \mathbb{K} (quindi esiste un polinomio minimo per x a coefficienti in \mathbb{K}), ma dato che $\mathbb{K} = \overline{\mathbb{K}}$ si ha che $x \in \mathbb{K}$, assurdo.

Osservazione. Sia D una \mathbb{K} -algebra di divisione, considero $M_n(D)$: allora essa è una \mathbb{K} -algebra di divisione; se $\dim_{\mathbb{K}} D < \infty$ allora $\dim_{\mathbb{K}} M_n(\mathbb{K}) < \infty$.

Teorema 9.17. *Sia D una \mathbb{K} -algebra di divisione con $\dim_{\mathbb{K}} D = k$, sia $A = M_n(D)$, allora A è un'algebra semisemplice con un'unica rappresentazione irriducibile: D^n .*

Dimostrazione. Come nell'esempio 9.9, possiamo considerare la serie di composizione di A composta dai sottospazi con le ultime colonne nulle. I quozienti di due sottospazi consecutivi sono isomorfi a D^n ; verifichiamo ora che D^n è una rappresentazione irriducibile di A .

Prendiamo un $0 \neq v \in D^n$, quindi avrà una componente non nulla v_i ; se prendo la matrice M che ha tutti zeri, tranne $\frac{1}{v_i}$ in posizione i, i , allora $Mv = e_i$. Considerando ora le matrici M_{jk} che hanno solo un 1 sulla k -esima riga e j -esima colonna; allora $M_{jk}e_j = e_k$, quindi posso generare tutta la base di D^n .

Sappiamo cioè $Av = D^n$ per tutti i v , quindi non esistono sottospazi invarianti non banali, coè D^n è irriducibile.

Dato che i fattori di composizione della serie descritta prima sono solo D^n , e che ogni rappresentazione di A compare come fattore di una serie di A , le rappresentazioni di $M_n(D)$ sono solo $V = D^n$. \square

Definizione 9.20. Una \mathbb{K} -algebra è *semplice* se non ha ideali bilateri non banali.

Proposizione 9.18. Sia A un'algebra semplice di dimensione finita, allora A è semisemplice.

Dimostrazione. Definiamo $J \subset A$ la somma di tutti gli ideali sinistri minimali di A : $J = \sum_j I_j$. J è evidentemente un ideale sinistro, vediamo che è anche destro: considero $a \in A$, $I \subset A$ un ideale minimale, allora $Ia = 0$ oppure Ia è un ideale minimale sinistro isomorfo a I , quindi $Ia \subset J$ e dunque J è un ideale bilatero. A era un'algebra semplice quindi $J = 0$ o $J = A$. Se $J = A$ abbiamo finito in quanto abbiamo scritto A come somma di sottomoduli semplici. Ma nell'ipotesi di $\dim A < \infty$ non avviene che $J = 0$: si può fare per induzione sulla dimensione: se A è irriducibile abbiamo finito, se invece ha un A -sottomodulo ci si può restringere a quello (che ha dimensione strettamente inferiore) e in un numero finito di passi si conclude. \square

Esempio 9.10 (Algebra di Weyl). Il teorema precedente è falso se $\dim A = \infty$: consideriamo $A = \mathbb{C} \left[x, \frac{d}{dx} \right]$ l'algebra dei polinomi in x e nelle derivate rispetto a x . Più formalmente

$$A = \mathbb{C}\langle x, y \rangle / (yx = 1 + xy)$$

infatti $\frac{d}{dx}(xp(x)) = p(x) + x\frac{d}{dx}p(x)$ per cui $\frac{d}{dx}x = 1 + x\frac{d}{dx}$. A è una \mathbb{C} algebra, $\dim_{\mathbb{C}} A = \infty$, A non ha ideali bilateri propri (è semplice) ma non è semisemplice (in particolare non ha ideali minimali sinistri).

Proposizione 9.19. Se V è un A -modulo semisemplice, allora possiede sottomoduli minimali (ovvero rappresentazioni irriducibili)

Dimostrazione. Sia $I \subset A$ un ideale massimale di A , e $0 \neq v \in V$. Osserviamo che $Iv \subset Av$ sono sottomoduli di V , quindi sono semisemplici.

In particolare esiste un $W \subset V$ stabile tale che $Av = Iv \oplus W$; se per assurdo W non fosse irriducibile, avremmo $W = W_1 \oplus W_2$, ovvero $Iv \oplus W_1$ sarebbe un sottomodulo di Av , cioè del tipo Jv con $I \subset J \subset A$ ideale; ma le due inclusioni sono entrambe proprie grazie a W_1 e W_2 , contraddicendo la massimalità di I . \square

Proposizione 9.20. Sia D un'algebra di divisione su \mathbb{K} . Allora la \mathbb{K} -algebra $M_n(D)$ è semplice.

Dimostrazione. Sia $J \subset M_n(D)$ un ideale bilatero non nullo.

Consideriamo $J_{ij} = \{x \in D : \exists X \in J, x = [X]_{i,j}\}$ ovvero gli elementi di D che compaiono in posizione ij di una qualche matrice di J . Vediamo che tutti i J_{ij} sono ideali bilateri di D : infatti è ovvio che sia chiuso rispetto alla somma; per vedere che è chiuso a destra e a sinistra per moltiplicazione per $d \in D$, basta moltiplicare a destra o a sinistra per dId .

Essendo D un'algebra di divisione, gli ideali possono essere solo 0 o D : se $d \in I \subset D$, allora anche $1 = d \cdot \frac{1}{d} \in I$, e allora $a \in I \forall a \in D$.

Quindi ogni J_{ij} è 0 o D ; poiché $J \neq 0$, esiste una coppia di indici per cui $J_{ij} = D$, e in particolare $1 \in J_{ij}$. Sia $X \in J$ tale che $[X]_{i,j} = 1$; allora, essendo ideale bilatero, anche $E_{ii}XE_{jj} = E_{ij} \in J$, dove $E_{\alpha,\beta}$ sono le matrici elementari (nulle ovunque tranne un 1 nella posizione α, β).

Poiché $E_{ab}E_{bc} = E_{ac}$, è immediato osservare che $E_{ab} = E_{ai}E_{ij}E_{jb} \in J$, perciò J contiene una base di $M_n(D)$, perciò è tutto. \square

Proposizione 9.21. *Siano A_1, \dots, A_n algebre semisemplici di dimensione finita. Allora $A = A_1 \times \dots \times A_n$ è semisemplice, e gli ideali bilateri di A sono della forma $I = I_1 \times \dots \times I_n$, dove I_i è un ideale bilatero di A_i .*

Dimostrazione. Poiché A_i sono semisemplici, possiamo scrivere $A_i = \bigoplus_j I_{ij}$, dove I_{ij} è un ideale minimale, ovvero un modulo semplice. Allora possiamo anche scrivere $A = \bigoplus_i \bigoplus_j I_{ij}$, dove gli ideali sono ancora minimali.

Sia poi $J \subset A$ un ideale bilatero; se consideriamo $J_j = J \cap A_j$, questo è un ideale bilatero di A_j ; inoltre $\bigoplus J_j \subset J$. Per vedere che sono uguali, prendiamo $a \in J$ e scriviamolo come $a = a_1 + \dots + a_n$ dove $a_i \in A_i$; considero allora l'unità e_i di A_i , e vedo che $e_i a = a_i$ appartiene ancora a J , cioè $a_i \in J_i$.

FORSE VA RISCritta MEGLIO FORMALIZZANDO CON LE N-UPLE AL POSTO DELLE SOMME? COSÌ È PIÙ EVIDENTE CHE LE COMPONENTI NON SI PARLANO

□

9.7 Un teorema di divisibilità

L'obiettivo di questa sezione è dimostrare il seguente teorema:

Teorema 9.22. *Sia G un gruppo finito, V una rappresentazione irriducibile di G su \mathbb{C} (ovvero un $\mathbb{C}[G]$ modulo semplice). Allora*

$$\dim V \mid \text{ord}(G)$$

Osservazione.

- Il teorema è falso su campi non algebricamente chiusi: basta considerare $\mathbb{Z}/3\mathbb{Z}$ su \mathbb{R} che ha una rappresentazione irriducibile di grado 2.
- Il teorema vale più in generale su un campo \mathbb{K} algebricamente chiuso per cui $\text{char } \mathbb{K} \nmid \text{ord}(G)$.
- Se invece $\text{char } \mathbb{K} \mid \text{ord}(G)$, il teorema è in generale falso: consideriamo $G = SL_2(\mathbb{F}_{13})$ e $\mathbb{K} = \overline{\mathbb{F}_{13}}$; prendiamo poi la rappresentazione $V = \mathbb{K}[x, y]_5$, che è irriducibile (IO NON SO FARLO) di grado 6. Tuttavia $\text{ord}(G) = \binom{14}{3} = 2^2 \cdot 7 \cdot 13$, quindi non c'è divisibilità.

Introduciamo ora alcuni concetti di teoria degli anelli.

Sia R un anello commutativo unitario.

Definizione 9.21. Un elemento $x \in R$ si dice *integrale* su \mathbb{Z} se è radice di un polinomio monico a coefficienti interi.

Se $x \in \mathbb{C}$ lo chiamo *intero algebrico*.

Osservazione. Gli interi algebrici di \mathbb{Q} sono esattamente gli interi, per il criterio delle radici razionali.

Possiamo inoltre definire una struttura di modulo usando come scalari gli elementi di R :

Definizione 9.22. Sia M un gruppo abeliano; allora M è un R -modulo se esiste un'applicazione $\cdot : R \times M \rightarrow M$ che soddisfa

- $r \cdot (m + n) = r \cdot m + r \cdot n \quad \forall r \in R \quad \forall m, n \in M$
- $(r + s) \cdot m = r \cdot m + s \cdot m \quad \forall r, s \in R \quad \forall m \in M$

- $r \cdot (s \cdot m) = (rs) \cdot m \quad \forall r, s \in R \quad \forall m \in M$

Diciamo inoltre che M è finitamente generato se lo è come gruppo.

Osservazione. Gli \mathbb{Z} -moduli sono esattamente i gruppi abeliani.

Definiamo ora un'importante proprietà degli anelli

Definizione 9.23. Un anello R è detto *Noetheriano* se tutti i suoi ideali sono finitamente generati; o equivalentemente, se ogni catena ascendente di ideali si stabilizza.

Teorema 9.23 (base di Hilbert). *Se R è un anello Noetheriano, allora anche $R[x]$ è Noetheriano.*

Dimostrazione. Sia $I \subset R[x]$ un ideale per assurdo non finitamente generato. Allora posso costruire una successione di polinomi p_n tali che, se $I_n = (p_1, \dots, p_{n-1})$ allora $p_n \in I \setminus I_n$, e scelgo p_n di grado minimale.

Definiamo ora a_n come il termine di testa di p_n , e consideriamo $R \supset J = (a_1, a_2, \dots)$ l'ideale generato da tutti gli a_i .

Poiché R è Noetheriano, vale che $J = (a_1, \dots, a_{N-1})$ per un certo N ; ma allora posso scrivere $a_N = \sum_{i < N} b_i a_i$ con $b_i \in R$.

Prendo ora il polinomio $f = \sum_{i < N} b_i x^{\deg p_N - \deg p_i} p_i$ (è una buona definizione, poiché i gradi dei

polinomi sono crescenti). Osserviamo che $f \in I_N$ essendo combinazione lineare dei p_i ; inoltre ha lo stesso grado e lo stesso coefficiente di testa di p_N .

Ma allora $p_N - f \in I \setminus I_N$, perché se fosse $p_N - f \in I_N$ avremmo $p_N = (p_N - f) + f \in I_N$; tuttavia $\deg(p_N - f) < \deg p_N$, che è assurdo in quanto p_N ha grado minimo in $I \setminus I_N$ \square

Corollario. *Si vede facilmente per induzione che $R[x_1, x_2, \dots, x_n]$ è Noetheriano se R lo è.*

Proposizione 9.24. *Sia R un anello Noetheriano, M un R -modulo finitamente generato. Allora ogni sottomodulo di M è finitamente generato.*

LUI FA UNA ZINGARATA ASSURDA. CREDO CHE INVECE DEL TEO DI HILBERT SERVA CHE R^n SIA NOETH.

Dimostrazione. Scriviamo $M = Rm_1 + Rm_2 + \dots + Rm_n$, dove m_1, \dots, m_n sono i generatori di M . Consideriamo la mappa $\varphi: R^n \rightarrow M$ tale che $\varphi(a_1, \dots, a_n) = a_1 m_1 + \dots + a_n m_n$, che è surgettiva per ipotesi.

Detto allora $I = \ker \varphi$, si ha $M \cong R^n / I$ e in particolare si ha la corrispondenza tra ideali di M , ovvero sottomoduli, e ideali di R^n che contengono I . Ovvero, se $N \subset M$ è un sottomodulo allora esiste un ideale $J \subset R^n$ tale che $N \cong J / I$.

Se R è Noetheriano, anche R^n è Noetheriano, quindi J è finitamente generato, e quindi lo è anche N (i generatori sono le proiezioni di quelli di J). \square

Possiamo ora dare un criterio di integralità per elementi di R .

Proposizione 9.25. *Dato R anello commutativo unitario e un elemento $x \in R$, sono equivalenti:*

- x è integrale su \mathbb{Z}
- Detto $\mathbb{Z}[x] \subset R$ il sottoanello generato da x , $\mathbb{Z}[x]$ è uno \mathbb{Z} -modulo finitamente generato
- Esiste uno \mathbb{Z} -sottomodulo di R finitamente generato che contiene $\mathbb{Z}[x]$

Dimostrazione. 2) \iff 3) Usiamo la proposizione 9.24 ed il fatto che \mathbb{Z} è Noetheriano.

- 1) \Rightarrow 2) Sia $t^n + a_{n-1}t^{n-1} + \dots + a_0$ un polinomio a coefficienti interi che annulla x ; allora $\mathbb{Z}[x]$ è generato da $\{1, x, \dots, x^{n-1}\}$.
- 2) \Rightarrow 1) Osserviamo che $\mathbb{Z}[x] = \bigcup R_n$, con R_n il sottomodulo generato da $\{1, x, \dots, x^{n-1}\}$. Se $\mathbb{Z}[x]$ è finitamente generato, allora deve essere $\mathbb{Z}[x] = R_N$ per un certo N . Ma allora si ha semplicemente che $x^N = \sum_{i < N} a_i x^i$ con $a_i \in \mathbb{Z}$

□

Per dimostrare un'importante proprietà degli elementi integrali, dobbiamo costruire il prodotto tensore di moduli.

Definizione 9.24. Dati due R -moduli M, N si dice prodotto tensore $M \otimes N$ un R -modulo V per cui esiste una funzione bilineare $\psi : M \times N \rightarrow V$ tale che per ogni R -modulo V' con una funzione bilineare $\phi : M \times N \rightarrow V'$ esiste un'unica funzione lineare $\phi' : V \rightarrow V'$ che commuta.

$$\begin{array}{ccc} M \times N & \xrightarrow{\psi} & M \otimes N \\ & \searrow \phi & \downarrow \phi' \\ & & V' \end{array}$$

Si indica $m \otimes n = \psi(m, n)$

Si dimostra che il prodotto tensore esiste ed è unico; un'idea di costruzione è la seguente. Consideriamo il prodotto $M \times N$ con tutti i suoi elementi (m, n) che identifichiamo con i simboli $m * n$; prendiamo ora P il gruppo libero generato da tutti i simboli $m * n$. Quozientiamo poi P per le relazioni che ci interessano, ovvero:

- $m * n + m * n' - m * (n + n')$
- $m * n + m' * n - (m + m') * n$
- $(rm) * n - m * (rn)$

con $m \in M, n \in N, r \in R$.

L'ultima relazione ci dice come dotare questo gruppo di un prodotto per scalare, ovvero $r \cdot (m \otimes n) = (rm) \otimes n = m \otimes (rn)$.

Possiamo ora andare avanti con la seguente

Proposizione 9.26. *L'insieme degli elementi di R integrali su \mathbb{Z} è un sottoanello di R*

Dimostrazione. Per il criterio 9.25 se x, y sono integrali su \mathbb{Z} , allora $\mathbb{Z}[x]$ e $\mathbb{Z}[y]$ sono finitamente generati.

Considero allora l'applicazione lineare $\phi : \mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[y] \rightarrow \mathbb{Z}[x, y]$ data da $\phi(p \otimes q) = p \cdot q$; questa è surgettiva poiché posso scomporre monomio per monomio.

Inoltre il prodotto tensore di due moduli finitamente generati è finitamente generato; ma allora $\mathbb{Z}[x, y]$ è immagine di un modulo finitamente generato, quindi anche lui è finitamente generato.

Applicando di nuovo il criterio 9.25, abbiamo che $x + y$ e xy sono integrali su \mathbb{Z} , in quanto $\mathbb{Z}[x + y]$ e $\mathbb{Z}[xy]$ sono sottomoduli di $\mathbb{Z}[x, y]$

□

Ritorniamo ora al nostro $\mathbb{C}[G]$; ricordiamo che per UN CRITERIO A CASO FATTO PRIMA (MAGARI SI PUÒ SPOSTARE QUA?) $Z(\mathbb{C}[G])$ ha per base gli elementi $c_i = \sum_{x \in \mathcal{C}_i} x$ dove \mathcal{C}_i sono le classi di coniugio di G .

Proposizione 9.27. Sia $Z(\mathbb{C}[G]) \ni u = \sum u_i c_i$; se u_i sono interi algebrici, allora u è integrale su \mathbb{Z} .

Dimostrazione. Poiché gli elementi integrali sono un sottoanello, ci basta mostrare che tutti i c_i sono integrali.

Osserviamo che per ogni j, k l'elemento $c_j c_k$ appartiene ancora al centro, e dunque è combinazione lineare dei c_i ; questo vuol dire che $\mathbb{Z}[c_1, \dots, c_k]$ è finitamente generato (in particolare dai c_i).

Ma allora di nuovo per il criterio 9.25, dato che $\mathbb{Z}[c_i] \subset \mathbb{Z}[c_1, \dots, c_k]$, abbiamo che c_i è integrale. \square

Lemma 9.28. Sia V una rappresentazione irriducibile di G , χ il suo carattere, $Z(\mathbb{C}[G]) \ni u = \sum g u_g$ con u_g interi algebrici. Allora

$$\frac{1}{\dim V} \sum u_g \chi(g)$$

è un intero algebrico.

Dimostrazione. Per Schur, u agisce su V come lo scalare $\frac{\text{tr}(u)}{\dim V} = \frac{\sum u_g \chi(g)}{\dim V}$.

Abbiamo allora un'omomorfismo $\varphi : Z(\mathbb{C}[G]) \rightarrow \mathbb{C}$ dato proprio da $\varphi(u) = \frac{\sum u_g \chi(g)}{\dim V}$, in quanto $(u_1 u_2)v = u_1(u_2 v)$ con $v \in V$, cioè $\varphi(u_1 u_2)v = \varphi(u_1)\varphi(u_2)v$.

Per il lemma precedente sappiamo che u è integrale, quindi soddisfa un polinomio monico; sfruttando il fatto che φ è omomorfismo, sappiamo che anche $\varphi(u)$ soddisfa lo stesso polinomio monico, ovvero $\varphi(u)$ è un intero algebrico. \square

Armati di questo lemma possiamo finalmente dimostrare il teorema 9.22

Dimostrazione. Sia χ il carattere della rappresentazione; poiché il gruppo è finito vale $g^{\text{ord}(G)} = 1$, da cui gli autovalori di g sono tutti radici dell'unità; allora $\chi(g)$ è intero algebrico, essendo somma di radici dell'unità che sono interi algebrici.

Poniamo $u = \sum_{g \in G} \chi(g^{-1})g$ e osserviamo che appartiene al centro: $hu = \sum_{g \in G} \chi((hg)^{-1}h)hg =$

$\sum_{\sigma \in G} \chi(\sigma h)\sigma$ e similmente $uh = \sum_{\tau \in G} \chi(h\tau)\tau$; poiché $\text{tr}(\sigma h) = \text{tr}(h\sigma)$, abbiamo $uh = hu \forall h \in G$.

Ma allora per il lemma 9.28 $z = \frac{1}{\dim V} \sum_{g \in G} \chi(g^{-1})\chi(g)$ è un intero algebrico.

Osserviamo che $z = \frac{\text{ord}(G)}{\dim V} \cdot \frac{\sum \chi(g^{-1})\chi(g)}{\text{ord}(G)} = \frac{\text{ord}(G)}{\dim V} \cdot \langle \chi, \chi \rangle$; essendo V irriducibile, il prodotto dei caratteri vale 1.

Quindi si ha che $\frac{\text{ord}(G)}{\dim V} \in \mathbb{Q}$ è un intero algebrico, e quindi per l'osservazione 9.7 sta in \mathbb{Z} . \square

10 Rappresentazioni di S_n

Cerchiamo ora quali sono le rappresentazioni del gruppo simmetrico; in particolare caratterizziamo i moduli semplici di $A = \mathbb{Q}[S_n]$.

Come prima osservazione, sappiamo che le rappresentazioni irriducibili di un gruppo G sono al più tante quante le classi di coniugio di G ; per $G = S_n$, le classi di coniugio sono in corrispondenza biunivoca con le partizioni di n : infatti tutti gli elementi di una classe condividono la stessa struttura ciclica.

A loro volta, le partizioni possono essere pensate come particolari tabelle, nel modo seguente.

Definizione 10.1. Una n -tabella è un insieme di n quadratini disposti come in una scacchiera, in modo che il numero di quadratini presenti in ogni riga sia minore o uguale al numero di quadratini presenti nella riga sopra.

Per costruire i moduli che ci interessano, è necessario riempire le tabelle con dei numeri.

Definizione 10.2. Un n -diagramma D è una n -tabella dove in ogni quadratino vi è un numero da 1 a n , in modo che ogni numero compaia una ed una sola volta nell'intera tabella.

Esempio 10.1. Sia $n = 7$, \mathcal{C} la classe di coniugio di $(123)(45)(67)$; allora la partizione corrispondente a \mathcal{C} è $3, 2, 2$, che ha la seguente tabella; uno dei possibili diagrammi è

			3	5	6
			1	4	
			2	7	

Osserviamo che S_n agisce transitivamente sull'insieme dei diagrammi con la stessa forma nel modo ovvio.

Fissato un diagramma D , siamo interessati ai seguenti due sottogruppi di S_n :

Definizione 10.3.

- $R(D) = \{\sigma \in S_n : \sigma(i) \text{ sta nella stessa riga di } i \forall i = 1, \dots, n\}$
- $C(D) = \{\sigma \in S_n : \sigma(i) \text{ sta nella stessa colonna di } i \forall i = 1, \dots, n\}$

Osserviamo che $R(D) \cap C(D) = \{id\}$.

Possiamo ora definire l'elemento generatore degli ideali che ci interessano.

Definizione 10.4. Dato un diagramma D , il suo simmetrizzatore è

$$e_D = \left(\sum_{p \in R(D)} p \right) \left(\sum_{q \in C(D)} q \varepsilon_q \right)$$

Inoltre il modulo corrispondente è $V_D = Ae_D$

Proposizione 10.1. Se $p \in R(D)$ e $q \in C(D)$ allora $pe_D = e_D$ e $e_Dq = e_D\varepsilon_q$

Proposizione 10.2. Sia $g \in S_n$; allora $e_{gD} = ge_Dg^{-1}$

Dimostrazione. Vediamo che $R(gD) = gR(D)g^{-1}$. Infatti $\sigma \in R(gD) \iff \sigma(i)$ sta nella stessa riga di i all'interno del diagramma gD , ovvero $\sigma g(j) = g(g^{-1}\sigma g)(j)$ sta nella stessa riga di $g(j)$ (abbiamo scritto $i = g(j)$ con j pensato in D); questo si verifica se e solo se $g^{-1}\sigma g(j)$ sta nella stessa riga di j in D , ovvero $g^{-1}\sigma g(j) \in R(D)$, che è quello che volevamo.

Similmente $C(gD) = gC(D)g^{-1}$.

Allora $e_{gD} = \left(\sum_{p \in R(gD)} p \right) \cdot \left(\sum_{q \in C(gD)} q \varepsilon_q \right) = \left(\sum_{p' \in R(D)} gp'g^{-1} \right) \cdot \left(\sum_{q' \in C(D)} gq'g^{-1} \text{sgn}(gq'g^{-1}) \right)$; tirando fuori dalle parentesi le g e usando $\text{sgn}(gq'g^{-1}) = \text{sgn}(q')$ si ha la tesi. \square

Corollario. Se D e D' sono diagrammi con la stessa forma, allora $V_D \cong V_{D'}$

Dimostrazione. Poiché D e D' hanno la stessa forma, esiste un $g \in S_n$ tale che $D' = gD$, e perciò $e_{D'} = ge_Dg^{-1}$.

Allora $Ae_{D'} = Age_Dg^{-1}$. Osserviamo che $1 = g^{-1}g \in Ag$ perciò $Ag = A$; inoltre $Ae_Dg^{-1} \cong Ae_D$ grazie all'omomorfismo $xe_Dg^{-1} \mapsto xe_D$ che è iniettivo \square

Lemma 10.3. *Sia D un diagramma e $g \in S_n$. Allora possiamo scrivere $g = pq$ con $p \in R(D)$ e $q \in C(D)$ se e solo se nessuna coppia di numeri che si trova nella stessa diga di D sta anche sulla stessa colonna di gD .*

Dimostrazione.

\Rightarrow Scrivo $g = pq$; siano a, b due numeri sulla stessa riga di D . Allora a, b stanno sulla stessa riga anche in pD . Inoltre $gD = (pqp^{-1})pD$ e $pqp^{-1} \in C(pD)$; perciò gD ha le stesse colonne di pD , e in particolare poiché a, b stavano in colonne diverse di pD , stanno anche su colonne diverse di gD .

\Leftarrow Per transitività mostro che $gD = pqD$ con certi p, q della forma cercata. Guardo la prima colonna di gD : tutti i suoi elementi stanno in righe diverse di D per ipotesi, quindi posso scegliere un $p_1 \in R(D)$ tale che p_1D e gD abbiano gli stessi elementi nella prima colonna. Continuando in questo modo trovo un $p \in R(D)$ tale che pD e gD hanno le stesse colonne; allora esiste un $q' \in C(pD)$ per cui $q'pD = gD$; ma $q' = pqp^{-1}$ con $q \in C(D)$, perciò si ha proprio $pqD = gD$.

□

Osserviamo che le partizioni di n possono essere ordinate in modo lessicografico. Dimostriamo ora questo importante lemma di ortogonalità dei simmetrizzatori.

Lemma 10.4. *Sia D un diagramma di forma λ e D' un diagramma di forma λ' ; allora se $\lambda > \lambda'$ vale $e_{D'} \cdot e_D = 0$*

Dimostrazione. Per prima cosa vogliamo trovare due simboli a, b nella stessa riga di D e nella stessa colonna di D' ; supponiamo per assurdo che non esistano.

Diciamo che $\lambda : a_1 \geq \dots a_k$ e $\lambda' : a'_1 \geq \dots a'_h$; notiamo che gli a_1 simboli della prima riga di D devono stare tutti in colonne diverse di D' , per l'ipotesi di assurdo. Ciò vuol dire che D' ha almeno a_1 colonne, ma valeva anche $a_1 \geq a'_1$: perciò si deve avere $a_1 = a'_1$. Sia ora m il numero di righe lunghe a_1 elementi di λ e m' il suo analogo; poiché $\lambda > \lambda'$ si ha $m \geq m'$. Inoltre tutti gli elementi delle prime m righe di D devono andare nelle prime m' righe di D' , ma allora in D ho ma_1 elementi da mettere in $m'a_1$ posti in D' , ovvero $m' \geq m$, perciò $m = m'$.

Non può essere che queste m righe fossero tutta la tabella, poiché λ e λ' sono diversi; allora le tabelle continuano, e poiché gli elementi delle prime m righe restano nelle prime m righe, possiamo dimenticarci di loro e ripetere il ragionamento togliendo le prime m righe sia da λ che da λ' .

Ma quindi abbiamo creato un processo infinito, in cui ogni volta la lunghezza della prima riga decresce strettamente, il che è assurdo.

Allora abbiamo davvero a, b nella stessa riga di D e nella stessa colonna di D' ; sia $t = (a, b) \in S_n$, allora $t \in R(D) \cup C(D')$.

Si ha dunque $e_{D'} \cdot e_D = e_{D'} \cdot t \cdot e_D = (-e_{D'}) \cdot e_D$ per l'osservazione (10.1), ovvero $2 \cdot e_{D'} \cdot e_D = 0$ □

Troviamo ora una caratterizzazione di V_D

Lemma 10.5. *Fissiamo un diagramma D ; sia $x \in A$ tale che $\forall p \in R(D), q \in C(D)$ si abbia $pxq = \varepsilon_q x$. Allora $\exists \gamma \in \mathbb{Q}$ tale che $x = \gamma e_D$.*

Dimostrazione. Scriviamo $x = \sum a_g g$; l'ipotesi è che $x = \varepsilon_q p^{-1} x^{-1} = \varepsilon_q = \varepsilon_q \sum a_g p^{-1} g q^{-1} \sum a_{pgq} g$ shiftando gli indici $g \mapsto pgq$. Questo ci dice che $\varepsilon_q a_{pgq} = a_g$ per tutti i p, q ; in particolare con $g = \text{id}$ otteniamo $a_p q = \varepsilon_q a_1$, che sono esattamente i coefficienti di e_D .

Dimostriamo che se $g \neq pq$ con $p \in R(D), q \in C(D)$ allora $a_g = 0$; per il lemma (10.3) esistono a, b sulla stessa riga di D e sulla stessa colonna di gD . Allora $t = (a, b) \in R(D) \cap C(gD)$, e inoltre $q = g^{-1}tg \in C(D)$ è una trasposizione.

Allora usiamo la formula trovata con $p = t, q = g^{-1}tg$, da cui $a_g = -a_{tgg^{-1}tg} = -a_g$, cioè $a_g = 0$ □

Proposizione 10.6. *Esiste un $\gamma \in \mathbb{Q}^*$ tale che $e_D^2 = \gamma e_D$, ovvero $u_D = \gamma^{-1} u_D$ è idempotente*

Dimostrazione. Per il lemma precedente, mi basta far vedere che $pe_D^2q = \varepsilon_q e_D^2$; ma questa è ovvia poiché $pe_D^2q = (pe_D)(e_Dq) = e_D \cdot \varepsilon_q e_D$. Allora $e_D^2 = \gamma e_D$.

La cosa che vogliamo è $\gamma \neq 0$. Sia $T : A \mapsto Ae_D$ l'omomorfismo $T(x) = xe_D$, e calcoliamo $\text{tr } T$ in due modi diversi.

Una base di A è $S_n = \{g_1, g_s \dots, g_n\}$ con $g_1 = \text{id}$. Se scriviamo $e_D = \sum a_i g_i$, si vede che il coefficiente di g_j nella scrittura di $T(g_j)$ è esattamente a_1 , poiché la moltiplicazione per un elemento di base permuta i coefficienti. Allora vale $\text{tr } T = a_1 \cdot n! = n!$ in quanto $a_1 = 1$ dalla definizione.

Consideriamo ora $\text{Im } T = Ae_D$ che è un sottospazio di A ; se $x \in Ae_D$, allora $x = ye_D$ per cui $T(x) = ye_D^2 = y\gamma e_D = \gamma x$, ovvero in Ae_D tutti gli elementi sono autovettori. Allora è chiaro che se

prendo una base di Ae_D e la completo a base di A , T si scriverà nella forma

$$\begin{pmatrix} \gamma & & & \\ & \ddots & & \\ & & \gamma & \\ & & & \ddots \\ & & & & 0 \end{pmatrix}$$

perciò $\text{tr } T = \gamma \cdot \dim Ae_D = \gamma m$.

Si ha dunque $n! = \text{tr } T = \gamma m$, da cui $\gamma = \frac{n!}{m} \neq 0$; dato che e_D ha come coefficienti solo ± 1 , allora $e_D^2 \in \mathbb{Z}[S_n]$, perciò si deve avere $\gamma \in \mathbb{N}$, ovvero $\dim V_D \mid |S_n|$ \square

Armati di tutti questi lemmi possiamo avviarcì alla conclusione, ovvero dimostrare che i V_D sono tutte le rappresentazioni irriducibili, al variare della forma di D .

Proposizione 10.7. *Dato un diagramma D , $V_D = Ae_D$ è un ideale minimale, ovvero un sottomodulo semplice*

Dimostrazione. Grazie alla proposizione precedente, sappiamo che u_D è idempotente ed è un multiplo scalare di e_D ; perciò $Ae_D = Au_D$.

Usando il criterio METTERE IL REF QUANDO SARÀ SCRITTO, Au_D è minimale se e solo se $u_D Au_D$ è un corpo, cosa che avviene se e solo se $e_D Ae_D$ lo è.

Prendiamo $x \in e_D Ae_D$, cioè $x = e_D y e_D$; osserviamo che $pxq = (pe_D)y(e_Dq) = e_D y e_D \varepsilon_q = \varepsilon_q x$, perciò per il lemma (10.5) abbiamo $x = ke_D$ con $k \in \mathbb{Q}$.

Allora $e_D Ae_D = \mathbb{Q}e_D = \mathbb{Q}u_D$ che è un corpo isomorfo a \mathbb{Q} con elemento neutro del prodotto proprio u_D . \square

Proposizione 10.8. *Siano D, D' diagrammi di forma diversa $\lambda \neq \lambda'$, allora $V_D \not\cong V_{D'}$*

Dimostrazione. Supponiamo che $\lambda > \lambda'$. Per assurdo $V_D \cong V_{D'}$.

Essendo minimali, esiste un $a \in A$ tale che $Au_D a = Au_{D'}$, cioè $u_{D'} = bu_D a$. Allora $u_{D'}^2 = u_{D'} \cdot u_{D'} = u_{D'} bu_D a$.

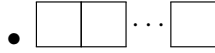
Tuttavia, $\forall g \in S_n$ vale che $u_{D'} g u_D g^{-1} = u_{D'} \cdot u_{gD} = 0$ per il lemma (10.4). Ma allora $u_{D'} bu_D = 0 \forall b \in A$, che porterebbe a $u_{D'} = 0$, assurdo. \square

Possiamo ora unificare tutto il nostro lavoro nel seguente

Teorema 10.9.

1. *C'è una corrispondenza biunivoca $\{\text{classi di coniugio di } S_n\} \leftrightarrow \{\text{partizioni di } n\} \leftrightarrow \{n\text{-tabelle}\}$*
2. *Abbiamo una mappa surgettiva $\{\text{diagrammi}\} \rightarrow \text{Irr}(S_n)$ data da $D \mapsto V_D = Ae_D$*
3. *$V_D \cong V_{D'}$ se e solo se D e D' hanno la stessa forma*

Facciamo ora un po' di esempi e casi particolari.



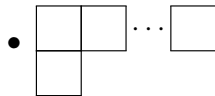
La tabella di una sola riga lunga n , a cui corrisponde $e_D = \sum_{\sigma \in S_n} \sigma$ cioè la rappresentazione banale.



⋮



La tabella di una sola colonna lunga n , a cui corrisponde $e_D = \sum_{\sigma \in S_n} \sigma \varepsilon_\sigma$ che è la rappresentazione segno.



La tabella con $n - 1$ quadratini nella prima riga e 1 nella seconda è la rappresentazione standard di S_n

Concludiamo con una formula che ci permette di calcolare la dimensione di una rappresentazione a partire dalla sua tabella.

Teorema 10.10 (formula degli uncini). *Sia λ una n -tabella, allora*

$$\dim V_\lambda = \frac{n!}{\prod_{i=1}^n \ell_i}$$

dove ℓ_i è la lunghezza dell'uncino che parte dalla casella i , ovvero il massimo percorso a L rovesciata che passa dalla casella i