

Dispense del corso di Teoria della Rappresentazione

Fabio Zoratti

10 marzo 2017

Indice

1	Teoria dei gruppi	2
1.1	Proprietà dei gruppi ciclici	7
1.2	Proprietà dei gruppi abeliani	7
1.3	Proprietà dei gruppi simmetrici	8
1.4	Proprietà dei gruppi diedrali	9
2	Algebra lineare	10
3	Algebra multilineare	12
3.1	Alcune generalizzazioni di algebra lineare	12
3.2	Prodotto tensoriale	12
3.3	Prodotto esterno e prodotto simmetrico	16
4	Prime proprietà delle rappresentazioni	17
4.1	Operazioni con le rappresentazioni	20
4.2	Sottospazi invarianti e scomposizione delle rappresentazioni	22
5	Teoria dei caratteri	26
5.1	Tabella dei caratteri	32
5.2	Esempi di rappresentazioni di gruppi finiti	32
5.2.1	I problemi della prima lezione visti con i nuovi strumenti	37
6	Rappresentazioni reali, complesse e quaternioniche	40
6.1	Quaternioni	42
7	Rappresentazioni indotte	49
7.1	Formula di aggiunta	52
7.1.1	Le rappresentazioni dei gruppi diedrali D_{2n}	53
8	Rappresentazioni di gruppi compatti	55

1 Teoria dei gruppi

Definizione 1.1 (Gruppo). Un gruppo è un insieme 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, $\text{card}(G) = n$, si dice che G ha *ordine* n .

Esempi

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 (senza lo 0).
3. $GL_n(\mathbb{R})$ oppure $GL(V)$
4. $f : I \rightarrow I$ biunivoca, con I insieme e con l'operazione di 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 chiama S_n .

Alcuni teoremi 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 $H \leq G$. In altre parole H è sottogruppo se, ereditando l'operazione di G , è esso stesso un gruppo.

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 (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 1.4 (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

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

Definizione 1.5 (Quoziente). Sia G un gruppo, $H < G$, chiamiamo *quoziente* di G per H l'insieme delle classi laterali di H , che indicheremo con G/H , ovvero

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

dove vengono identificati gli insiemi uguali (infatti non è detto che se $g, g' \in G$, con $g \neq g'$, allora $gH \neq g'H$).

Osservazione. Dato G un gruppo, $H < G$, non è difficile mostrare che tutte le classi laterali di H in G hanno la stessa cardinalità, in particolare hanno tutte la cardinalità della classe eH , ma $eH = H$ come insieme, quindi tutte le classi laterali di H hanno la stessa cardinalità di H .

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. Si osserva che $g \in gH$ visto che $gH = \{gh \mid h \in H\}$ e che $e \in H$, se si avesse che $g \in \alpha H$ allora $g = \alpha h_1$ per qualche h_1 . Si osserva allora che i due laterali coinciderebbero:

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

□

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 1.6 (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 (1.5) munito della seguente operazione:

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

Non riportiamo la dimostrazione del fatto che l'operazione così definita rispetti effettivamente gli assiomi dei gruppi.

Osservazione. Attenzione a non farsi ingannare: ci si può chiedere se, dato G gruppo con $H, K \trianglelefteq G$ 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

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

Infatti evidentemente $H \cong \mathbb{Z} \cong K$, ma $G/H \cong \mathbb{Z}_5$ mentre $G/K \cong \mathbb{Z}_7$ ¹.

Definizione 1.7 (Classi di coniugio). Sia G un gruppo, $x \in G$, la classe di coniugio di x è l'insieme $\{gxg^{-1} \mid g \in G\}$. 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 (ATTENZIONE: è raro che unendo a caso classi di coniugio si ottenga 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.

¹Esistono controesempi anche con gruppi finiti.

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*. Indichiamo con $Hom(G, H)$ l'insieme degli omomorfismi da G ad H .

Definizione 1.11. Siano G e H gruppi, $f : G \rightarrow H$ un omomorfismo di gruppi, allora definiamo

$$\begin{aligned} Ker f &= \{g \in G \mid f(g) = e_H\} \\ Imm f &= \{h \in H \mid \exists g \in G \text{ t.c. } f(g) = h\} \end{aligned}$$

Non è difficile verificare che sia $Ker f$ che $Imm f$ sono sempre sottogruppi rispettivamente di G e di H , inoltre si può osservare che $Ker f$ è un sottogruppo normale di G .

Osservazione. Non è difficile dimostrare che, dati G e H due gruppi e $f : G \rightarrow H$ un omomorfismo di gruppi, esso è *iniettivo* se e solo se $Ker f = \{e\}$.

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

$$G/Ker f \cong Imm f$$

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

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

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

Normalmente si usa una notazione abbreviata in cui invece di scrivere $a(g, i)$ si scrive direttamente $g \cdot i$ o addirittura gi

Definizione 1.13 (Azione transitiva). Un'azione di un gruppo G su un insieme $I \neq \emptyset$ si dice *transitiva* se $\forall i, j \in I \exists s \in G \text{ t.c. } j = s \cdot i$.

SAREBBE UTILE SCRIVERE UN COMANDO PER SCRIVERE ORB(X) SOLO CHE NON SO COME SI FA...

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 in G l'insieme $Orb_G(x) = \{g \cdot x \mid g \in G\}$, se il gruppo utilizzato è chiaro si può scrivere semplicemente $Orb(x)$. Si osserva subito che un'azione è transitiva se e solo se induce una unica orbita.

Osservazione. Le orbite di un gruppo G sull'insieme I formano una partizione dell'insieme. La verifica non è difficile. Vale inoltre la formula $|Orb_G(x)| \cdot |Stab_G(x)| = |G|$

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), 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

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

1.1 Proprietà dei 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 .

Osservazione. 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

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

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

1.2 Proprietà dei gruppi abeliani

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

Osservazione. Un gruppo ciclico è sempre abeliano.

Potrebbe essere utile 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.

Osservazione. Sia G un gruppo abeliano. Allora

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

La dimostrazione si ottiene ricordando che G è prodotto diretto di gruppi ciclici e facendo un ragionamento simile a quello della proposizione analoga per gruppi ciclici. Se invece G non è abeliano allora nella formula precedente all'uguale va sostituito un $>$.

1.3 Proprietà dei 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, 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 tra le parentesi 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 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 aggiungo $(1, 2)(1, 2)$ 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 $f : S_n \rightarrow \mathbb{N}$:

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

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 .

1.4 Proprietà dei 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 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.

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

Corollario. *Date $M_1, \dots, M_k \in \mathcal{M}(n, n, \mathbb{K})$, 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 2.1 (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 $f^0 = Id$ 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 $V = \text{Ker}((f - \lambda_1 Id)^{\alpha_1}) \oplus \dots \oplus \text{Ker}((f - \lambda_k Id)^{\alpha_k})$.

Teorema 2.3 (Forma canonica di Jordan). *Sia $M \in \mathcal{M}(n, n, \mathbb{K})$ 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*

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

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 2.2 (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 2.3. 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 Alcune generalizzazioni di algebra lineare

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 dei \mathbb{K} -spazi vettoriali, sia $e : I \rightarrow V$ una base di V e $f : I \rightarrow W$ una funzione. Allora $\exists!$ $\phi : V \rightarrow W$ lineare tale che

$$\phi(e_i) = f_i$$

Inoltre ϕ è un isomorfismo $\Leftrightarrow f$ 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{C} -spazio vettoriale:

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

Ora è facile osservare che $e : I \rightarrow \mathbb{C}^I$ 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{C} -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 $\alpha \otimes w = \alpha w$.

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:

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

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

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

Ma noi conosciamo già un'applicazione lineare che fa commutare i due diagrammi “più grandi”: l'identità. Quindi per unicità possiamo concludere che $\phi\psi = \psi\phi = id$, 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 delle applicazioni bilineari da V in \mathbb{C} , che sappiamo scriverlo come matrici $n \times n$. Tuttavia se un elemento si scrive in termini di matrici come $z = v \otimes w$, allora la matrice associata a z in una base avrà rango al massimo 1, ben lontano da 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 $v \otimes w$:

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

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

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

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

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

tuttavia il diagramma grande commuta anche con $id_{V \otimes W}$ e quindi $i \circ \psi = id_{V \otimes W} \Rightarrow i$ è surgettiva $\Rightarrow \langle A \rangle = V \otimes W$. \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. $id_V \otimes id_W = id_{V \otimes W}$

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 $w_i \in W$.

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 $e_k^* \otimes id_W : V \otimes W \rightarrow \mathbb{K} \otimes W$. Valutandola in x otteniamo:

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

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 $\text{tr} = t \circ \phi : \text{End}(V) \rightarrow \mathbb{K}$. 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

3.3 Prodotto esterno e prodotto simmetrico

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

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

Proposizione 3.10. Un'applicazione $h : V^n \rightarrow W$ è alternante se e solo se $h(v_1, \dots, v_n) = 0$ se $v_i = v_j$ per qualche $i \neq j$.

Proposizione 3.11. Un'applicazione $h : V^n \rightarrow W$ è nulla se i vettori v_1, \dots, v_n sono linearmente dipendenti.

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 (v_1, \dots, v_n) in $v_1 \wedge v_2 \wedge \dots \wedge v_n \in \bigwedge^n V$, tale che $\forall h : V^n \rightarrow Z$ n -lineare alternante, esiste unica $\phi : \bigwedge^n V \rightarrow Z$ lineare per cui vale $\phi(v_1 \wedge v_2 \wedge \dots \wedge v_n) = h(v_1, \dots, v_n)$.

Teorema 3.12 (Dimensione del prodotto esterno). Sia V uno spazio vettoriale di dimensione n , $\{e_i | 1 \leq i \leq n\}$ una base di V e k un intero positivo. Allora l'insieme $E = \{e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_k} | 1 \leq i_1 < i_2 < \dots < i_k \leq n\}$ è una base di $\bigwedge^k V$ e si ha $|E| = \binom{n}{k}$.

MANCANO UN SACCO DI PROPRIETÀ E LE DIMOSTRAZIONI

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 $\forall h : V^n \rightarrow Z$ n -lineare simmetrica, esiste unica $\phi : S^n V \rightarrow Z$ lineare per cui vale $\phi(v_1 v_2 \dots v_n) = h(v_1, \dots, v_n)$.

Teorema 3.13 (Dimensione del prodotto simmetrico). Sia V uno spazio vettoriale di dimensione n , $\{e_i | 1 \leq i \leq n\}$ una base di V e k un intero positivo. Allora l'insieme $E = \{e_{i_1} \wedge e_{i_2} \wedge \dots \wedge e_{i_k} | 1 \leq i_1 \leq i_2 \leq \dots \leq i_k \leq n\}$ è una base di $S^k V$ e si ha $|E| = \binom{n+k-1}{k}$.

Definizione 3.7 (Potenza simmetrica e potenza esterna di un'applicazione lineare). Sia $f : V \rightarrow V$ un endomorfismo di uno spazio vettoriale. Definiamo

$$\bigwedge^k f : \bigwedge^k V \rightarrow \bigwedge^k V \quad f(v_1 \wedge \dots \wedge v_k) = f(v_1) \wedge \dots \wedge f(v_k)$$

In modo analogo si definisce la potenza simmetrica.

Proposizione 3.14. Sia $f : V \rightarrow V$ un endomorfismo di uno spazio vettoriale. Allora vale

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

4 Prime proprietà delle rappresentazioni

Definizione 4.1 (Rappresentazione). Sia G un gruppo. Una rappresentazione ρ di G è una coppia composta da uno spazio vettoriale di dimensione qualsiasi V_ρ e una funzione $\rho : G \rightarrow GL(V_\rho)$ che manda ciascun elemento del gruppo in un'applicazione lineare di V_ρ , ovvero un suo endomorfismo. Affinché ρ sia una rappresentazione deve essere un omomorfismo di gruppi, ovvero in parole semplici deve rispettare la regola di composizione. In formule, se $s, t \in G$ deve valere

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

La dimensione di V_ρ viene detta grado della rappresentazione.

Proposizione 4.1. $\rho(G)$ è evidentemente un sottogruppo di $GL(V_\rho)$, quindi esistono sempre inversi, potenze e tutte le cose che valgono per i gruppi.

Esempi.

1. La rappresentazione banale, di grado qualsiasi, indicata con ρ_1 che manda qualsiasi elemento di G nell'identità di V_ρ , ovvero

$$\rho(s) = id_{V_\rho} \quad \forall s \in G$$

2. Dato S_n , il segno di un elemento $s \in S_n$ è una rappresentazione di grado 1. Infatti si ha $sgn(st) = sgn(s)sgn(t)$.
3. L'azione naturale di S_n sui vettori della base. Prendiamo quindi $G = S_n$ e uno spazio vettoriale di dimensione n , che sarà sicuramente isomorfo a \mathbb{C}^n . Prendiamo la base canonica di \mathbb{C}^n e la chiamiamo e_i . 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 e vediamo cosa succede. Notiamo innanzitutto che $|S_3| = 3! = 6$
FINISCI DI SCRIVERE

Proposizione 4.2. 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 BENE: 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 esiste un intero positivo k tale che $g^k = e$. Dato che $\rho : G \rightarrow GL(V_\rho)$ mantiene queste proprietà in quanto omomorfismo, dovrà essere

$$\rho(g)^k = id$$

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: due 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

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

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

Rappresentazioni di grado 1 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 4.3. *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

Negli esercizi sarà necessario 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 i generatori del gruppo G , che indicheremo con 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* con cui può essere presentato il gruppo siano rispettate nell'immagine³.

Questo definisce un omomorfismo da G a \mathbb{C}^* : dato $h \in G$ t.c. $h = g_{i_1}^{a_1} \dots g_{i_t}^{a_t}$, 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.

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

Esempio 4.1 (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 $\forall h \in G \exists k \in \mathbb{N}$ t.c. $h = g^k$, 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, supponiamo inoltre di avere $\varphi : \rho_1 \rightarrow \rho_2$ un isomorfismo di rappresentazioni, vediamo che questo è assurdo: se fosse un isomorfismo di rappresentazioni dovrebbe 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 $\rho_1(g) = \rho_2(g) \forall g \in G$, e questo è assurdo perchè differiscono almeno su un generatore di G .

L'esempio di prima 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, conoscendo un quoziente ciclico di G , fornisce alcune rappresentazioni di grado 1 del gruppo.

Sia G un gruppo, $H \trianglelefteq G$ t.c. 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:

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

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.

Esempio 4.2 (Rappresentazioni di grado 1 di S_3).

Esempio 4.3 (Rappresentazioni di grado 1 di $C_n \times C_n$). (generalizzazione a prodotto di C_{n_i})

Osservazione. È possibile generalizzare ulteriormente il secondo procedimento descritto. Sia G un gruppo, $H \trianglelefteq G$ tale che conosciamo le rappresentazioni (irriducibili) 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: $\sigma(g) = \rho(\pi(g))$.

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

4.1 Operazioni con le rappresentazioni

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

$$(\rho + \sigma)(g)v = \rho(g)\pi_{V_\rho}(v) + \sigma(g)\pi_{V_\sigma}(v) \quad \forall v \in V_\rho \oplus V_\sigma$$

Questa definizione ha senso, infatti proiettando v sui due spazi di partenza le due rappresentazioni sono definite e rimangono nello spazio di partenza. Si può poi fare la somma se riportiamo il tutto nello spazio più grande.

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

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

dove si intende ovviamente che la base ha i primi vettori in V_ρ , i secondi in V_σ .

OSSERVAZIONI:

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.
5. se $\deg(\rho) = 1$ allora $\rho(g^{-1}) = \rho(g^{-1})^t = \rho^*(g) \Rightarrow \rho^*(g) = \rho(g)^{-1}$.

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 $\rho\sigma^5$ definita sullo spazio $V_\rho \otimes V_\sigma$ tale che

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

Non è restrittivo dare la definizione solo per gli elementi di $V_\rho \otimes V_\sigma$ decomponibili, in quanto sappiamo che sono una base dello spazio. Gli altri si otterranno per linearità.

OSSERVAZIONI:

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

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^* tale che $\rho^*(s) = \rho(s^{-1})^t$

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.

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. $\rho^*(s) = \rho(s^{-1})^t = (\rho(s)^{-1})^t = (\rho(s)^t)^{-1}$. Inoltre, notare che la presenza di inverso e trasposto fa in modo che $\rho^*(s)$ sia una rappresentazione.

OSSERVAZIONE: vale

$$(\rho + \sigma)^* \cong \rho^* + \sigma^*$$

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

Definizione 4.8 (Rappresentazione regolare). Consideriamo un gruppo G , per semplicità finito, e consideriamo uno spazio vettoriale V_ρ di dimensione $|G|$ su \mathbb{C} . Una base di questo spazio ha sicuramente dimensione $|G|$. Possiamo indicare gli elementi della base con $e_g, \quad \forall g \in G$. 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 in questo modo:

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

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 .

4.2 Sottospazi invarianti e scomposizione delle rappresentazioni

Definizione 4.9 (Sottorappresentazione). Sia ρ una rappresentazione di G su V_ρ , una sottorappresentazione di ρ è un sottospazio vettoriale $W \subseteq V_\rho$ tale che $\rho(s)(W) \subseteq W \forall s \in G$. Posso definire una rappresentazione σ con $V_\sigma = W$ e $\sigma(s) = \rho(s)|_W$ (la indicherò con $\sigma \subseteq \rho$).

Notazione: $V_\rho^G = \{v \in V_\rho : \rho(s)v = v \forall s \in G\}$.

Definizione 4.10 (Rappresentazione irriducibile). Una rappresentazione ρ di G è *irriducibile* se

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

Definizione 4.11 (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. Normalmente la cosa che si fa più spesso in teoria della rappresentazione è cercare di scomporre la rappresentazione di un gruppo come somma di rappresentazioni irriducibili. Vedremo quindi adesso diversi teoremi che ci aiuteranno in questi problemi.

Esempio 4.4 (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

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

É 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 *far partire la somma da un indice 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 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 $Im(f)$ è una sottorappresentazione di σ e $Ker(f)$ è una sottorappresentazione di ρ .*

Dimostrazione. Se $v \in Ker(f)$ 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 $\rho(s)v \in Ker(f)$. Allo stesso modo, se $w \in Im(f)$ allora $w = f(v)$ per qualche $v \in V_\rho$ e quindi sempre per la definizione di omomorfismo di rappresentazione $\sigma(s)w = \sigma(s)f(v) = f(\rho(s)v) \in Im(f)$. \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 (4.2): 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 $1 \leq i \leq n$ $Span(v_i)$ è una sottorappresentazione di grado 1 di G (perché invariante per G), visto che $V_\rho = Span(v_1) \oplus \dots \oplus Span(v_n)$, allora $\rho \cong \rho_1 + \dots + \rho_n$, dove $\rho_i : G \rightarrow GL(Span(v_i))$. \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*

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

DIMOSTRAZIONE:

Consideriamo il lato destro dell'uguaglianza. Un elemento $\phi_i \in Hom(\rho_i, \sigma)$ 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

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

in modo ovvio e mostriamo che è un isomorfismo.

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

Innanzitutto la funzione $\phi_1 + \phi_2 : V_{\rho_1} \oplus V_{\rho_2}$ 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 inettiva 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 PERCHÉ?

\square

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 $f - \lambda Id : V_\rho \rightarrow V_\rho$ 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 $f - \lambda Id$ è identicamente nullo, da cui ricaviamo che f è la moltiplicazione per uno scalare (λ). \square

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*

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

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

OSSERVAZIONI:

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 $[\rho_1] = I_n \Rightarrow \text{tr}(\rho_1) = n$ 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. $\chi_{\rho\sigma}(s) = \chi_\rho(s)\chi_\sigma(s)$.
Questo deriva dal seguente fatto generale:

Lemma 5.1. Se $f : V \rightarrow V$ e $g : W \rightarrow W$ sono endomorfismi di spazi vettoriali, allora $\text{tr}(f \otimes g) = \text{tr}(f)\text{tr}(g)$.

Dimostrazione: 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.

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

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

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

⁷Si veda la proposizione 4.2

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

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

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

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

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

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

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

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

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

Definizione 5.2 (Prodotto hermitiano dei caratteri).

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

Teorema 5.2 (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 5.3. *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

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

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

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

E questo isomorfismo segue semplicemente dalle proprietà del prodotto tensore di spazi vettoriali. Definiamo su $Z^{10} = \text{Hom}(V_\rho, V_\sigma)$ la seguente rappresentazione: se $f \in Z$, allora possiamo definire la rappresentazione $\tau, V_\tau = Z$ di G in questo modo

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

Si verifica manualmente che sia una buona definizione. Ora vogliamo vedere che Z e $V_{\rho^* \sigma}$ sono isomorfi anche come rappresentazioni. Chiamo $\Psi : V_\rho^* \otimes V_\sigma \rightarrow \text{Hom}(V_\rho, V_\sigma)$ la mappa tale che

$$\Psi(\phi \otimes v)(w) = \phi(w)v \quad \forall \phi \in V_\rho^*, \forall v \in V_\sigma, \forall w \in V_\rho$$

Voglio mostrare che Ψ è un isomorfismo di rappresentazioni. Innanzitutto notiamo che è stato sufficiente definirlo per i tensori decomponibili, dato che per il resto dello spazio basta estenderlo per linearità. Precedentemente abbiamo già mostrato che Ψ è un isomorfismo di spazi vettoriali. Quindi per concludere la dimostrazione è sufficiente dimostrare che è un omomorfismo di rappresentazione ovvero

$$\Psi((\rho^* \otimes \sigma(s))(\phi \otimes v)) = \tau(s)(\Psi(\phi \otimes v)) \quad \forall v \in V_\sigma, \phi \in V_\rho^*, s \in G$$

e questo è vero sse

$$\Psi((\rho^* \otimes \sigma(s))(\phi \otimes v))(w) = \tau(s)(\Psi(\phi \otimes v))(w) \quad \forall w \in V_\rho, v \in V_\sigma, \phi \in V_\rho^*, s \in G$$

Riscriviamo il secondo membro

$$\tau(s)(\Psi(\phi \otimes v))(w) = \sigma(s) \circ \Psi(\phi \otimes v) \circ \rho^{-1}(s)(w) = \sigma(s)(\phi(\rho^{-1}(s)(w))v) = \phi(\rho^{-1}(s)(w))\sigma(s)(v)$$

ed ora il primo

$$\Psi(\rho^* \otimes \sigma(s)(\phi \otimes v))(w) = \Psi(\rho^*(s)(\phi) \otimes \sigma(s)(v))(w) = \rho^*(s)(\phi)(w)\sigma(s)(v)$$

e dato che l'applicazione duale è stata definita come l'unica tale che

$$\rho_s^*(\phi) \circ \rho_s = \phi$$

⁹Non necessariamente irriducibili

¹⁰Dato che sono spazi vettoriali in questo caso si tratta semplicemente di applicazioni lineari

allora i due membri sono uguali e Ψ è un omomorfismo di rappresentazione. Ne segue 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 $\dim(V_{\rho^* \sigma})^G$.

Lemma 5.4. *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 5.2:

A questo punto la tesi del teorema 5.2 segue dal lemma precedente applicato insieme al lemma di Schur. □

OSSERVAZIONI:

- 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

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

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 5.3: Lemma di Burnside). *Consideriamo un'azione di un gruppo G su un insieme I e consideriamo una rappresentazione dell'azione di G , (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 $V_{\rho_I}^G = \{\sum a_i e_i | \text{Alcune condizioni}\}$ 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

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

□

Teorema 5.5. *Sia G un gruppo finito e siano ρ_1, \dots, ρ_r le sue rappresentazioni irriducibili. Sia inoltre*

$$Cl(G)$$

Lo spazio delle funzioni da G in \mathbb{C} costanti sulle classi di coniugio di G

Chiaramente $\dim Cl(G) = \text{numero di classi di coniugio di } G := s$. 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 $f \in Cl(G)$ 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 $f(s) = 0 \quad \forall s \in G$ 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 $r = s$. □

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	$orb(g_1)$	$orb(g_2)$
	1	$ orb(g_1) $	$ 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 5.1 (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 $Fix(s)$, possiamo scrivere

$$Fix(s) = 1 + \chi_\rho$$

Da cui si ricava subito il carattere della rappresentazione ρ

Esempio 5.2 (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 5.6. *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

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

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

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

Che abbiano lo stesso grado deriva dal fatto che

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

Essendo ϵ di grado 1 e ρ irriducibile allora anche $\rho\epsilon$ è un'altra rappresentazione irriducibile.

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

E 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 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

Ossevezione: 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 potremmo trovarci in una situazione in cui i seguenti lemmi si rivela utile

Lemma 5.7. 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 5.8. *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,*

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

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 5.3 (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 5.4 (Problema 1 prima lezione).

Esempio 5.5 (Problema 2 prima lezione).

Esempio 5.6 (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 cubo¹¹. 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

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

È 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

$$gT = Tg$$

¹¹Che ha quindi 6 elementi

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 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.

É 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

Ci poniamo un problema nuovo: quand'è che una rappresentazione, che abbiamo sempre definito su \mathbb{C} , funziona in modo uguale anche definendola solo su \mathbb{R} ? Diamo una definizione più precisa

Definizione 6.1. Diciamo che una rappresentazione (ρ, V_ρ) del gruppo G è reale se esiste una base di V_ρ tale che

$$\rho(g) \in M_n(\mathbb{R}) \quad \forall g \in G$$

Questa definizione è equivalente a chiedere che $\exists V_0 \subset V$ sottospazio vettoriale reale tale che: V_0 sia stabile (G -invariante) e che

$$V = \mathbb{C} \otimes_{\mathbb{R}} V_0 = V_0 \oplus iV_0$$

Ne segue che $\dim_{\mathbb{R}} V_0 = \dim_{\mathbb{C}} V$. Non è sempre detto che esista.

Esempio 6.1. Prendiamo come gruppo un gruppo ciclico, per esempio $\mathbb{Z}/3\mathbb{Z}^{12}$. Evidentemente tutte le rappresentazioni non banali di G non sono reali, in quanto sono di grado 1 e sono le radici dell'unità.

Osservazione. Supponiamo di avere $\rho : G \rightarrow GL(V_\rho)$ con V_ρ spazio vettoriale su \mathbb{C} di dimensione n (dimensione di V pensato come un \mathbb{C} -spazio vettoriale). Allora possiamo vederlo come uno spazio vettoriale costruito sul campo dei reali e lavorare su quello, se il nostro obiettivo è quello di avere una rappresentazione reale. Quando lo interpreteremo in questo modo scriveremo $V_{\mathbb{R}}$ (che essendo lo stesso spazio vettoriale su \mathbb{R} avrà dimensione $2n$).

Lemma 6.1. Sia V una rappresentazione $/\mathbb{C}$ (tale scrittura significa V visto come spazio vettoriale complesso) che sia però anche reale nel senso prima definito. Allora $V^{\mathbb{R}}$ NON è una rappresentazione irriducibile.

DIMOSTRAZIONE:

Abbiamo detto che il fatto che ρ possa essere vista come una rappresentazione reale equivale all'esistenza di un V_0 che mi faccia il lavoro prima detto. Bene ma allora quel V_0 (essendo reale) lo possiamo in realtà vedere come un sottospazio di $V^{\mathbb{R}}$ G -invariante la cui dimensione è

$$\dim_{\mathbb{R}} V_0 = \dim_{\mathbb{C}} V = \frac{1}{2} \dim_{\mathbb{R}} V^{\mathbb{R}} \Rightarrow G \rightarrow GL(V_0)$$

è una sottorappresentazione di G/\mathbb{R} . □

Ora andremo a fare una classificazione delle rappresentazioni. Vedremo che ne esistono di 3 tipi:

- Reali
- Complesse
- Quaternioniche

La classificazione verrà fatta in base all'esistenza o meno di forme bilineari di un certo tipo invarianti sotto G . Vediamo come farlo formalmente.

Teorema 6.2. Prendiamo una (ρ, V_ρ) rappresentazione $/\mathbb{C}$ che sia reale: allora:

¹²Che per i fisici è isomorfo a C_3

$$1. \chi_\rho(g) \in \mathbb{R} \quad \forall g \in G$$

2. V_ρ possiede una forma bilineare simmetrica G -invariante. 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 . 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. Consideriamo quindi B

$$B \in (S^2 V^*)^G$$

che definiamo sullo spazio $V = V_0 \oplus iV_0$ nel seguente modo

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

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

Vediamo ora il seguente lemma che ci servirà per la classificazione.

Lemma 6.3. *Sia (ρ, V_ρ) una rappresentazione $/\mathbb{C}$. Allora ogni forma bilineare non nulla G -invariante è non degenera (in particolare quindi ne esiste almeno una). Inoltre è unica a meno di scalari, ovvero $\dim(V^* \otimes V^*)^G = 1$.*

DIMOSTRAZIONE:

Prendiamo un elemento B

$$B \in (V^* \otimes V^*)^G$$

É un fatto di algebra che

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

A questo punto, se $\phi : V \rightarrow V^*$ è un omomorfismo di rappresentazioni, per il lemma di Schur o ϕ è nullo o ϕ è un isomorfismo. Dato che la forma è non nulla, allora $\phi = \lambda Id$ con $\lambda \in \mathbb{C}$. \square

Sia V una rappresentazione $/\mathbb{C}$ irriducibile: quando è che \exists una forma bilineare G -invariante? Ovvero quand'è che si ha $(V^* \otimes V^*)^G \neq 0$? Cerchiamo delle condizioni necessarie...

Lemma 6.4. *Sia (ρ, V_ρ) una rappresentazione $/\mathbb{C}$ tale che sia reale: allora esiste un isomorfismo tra V e V^* ovvero esiste un isomorfismo tra ρ e ρ^* (a volte confondiamo la rappresentazione con il suo supporto).*

DIMOSTRAZIONE:

$$\rho \simeq \rho^* \Leftrightarrow \chi_\rho(g) = \chi_{\rho^*}(g) \quad \forall g \in G$$

ma dato che

$$\chi_{\rho^*} = \overline{\chi_\rho}$$

allora

$$\chi_\rho(g) = \chi_{\rho^*}(g) \quad \forall g \in G \Leftrightarrow \chi_\rho(g) = \overline{\chi_\rho}(g) \quad \forall g \in G$$

e questo è vero $\Leftrightarrow \chi_\rho$ è una funzione reale. E ciò è vero se la rappresentazione è definibile $/\mathbb{R}$. \square

Lemma 6.5. *Sia (ρ, V_ρ) una rappresentazione $/\mathbb{C}$: allora*

$$\bullet \quad B \in (V^* \otimes V^*)^G \Rightarrow B \in S^2 V^* \vee B \in \bigwedge^2 V^*$$

Definiamo

$$m_\rho = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g^2)$$

l'indicatore di Frobenius-Schur. Allora

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

DIMOSTRAZIONE:

Abbiamo visto che $V^* \otimes V^*$ si può decomporre come somma diretta delle potenze simmetriche e alternanti ovvero

$$V^* \otimes V^* = S^2 V^* \oplus \bigwedge^2 V^*$$

e inoltre per il lemma precedente sappiamo che $V^* \otimes V^*$ ha dimensione 1. DEVO FINIRE DI SCRIVERLA

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

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

6.1 Quaternioni

Ovviamente la parola quaternionica ha 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 utilizzare il secondo metodo descritto nel paragrafo (4). 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 $Q_8/H_i \cong \mathbb{Z}_2^{13}$. 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 isomorfe¹⁴), 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:

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

¹³Visto che gli H_i sono normali, Q_8/H_i è un gruppo, avendo solo due elementi è necessariamente \mathbb{Z}_2 .

¹⁴La verifica è immediata

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

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

Matrici di spin di Pauli ???

	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.

Lemma 6.6. *Sia (ρ, V_ρ) una rappresentazione irriducibile su \mathbb{C} . Allora ρ è reale secondo la definizione 6.1 $\Leftrightarrow m_\rho = 1$*

DIMOSTRAZIONE: \Rightarrow) già fatto.

\Leftarrow) 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 $V_\rho = V_0 \oplus iV_0$

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 V_ρ che chiamiamo $\phi : V_\rho \rightarrow V_\rho$, definito come

$$B(x, y) = h(\phi(x), y)$$

Questa definizione ha senso per y fissato (per 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

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

SCRIVI PERCHÉ

E quindi purtroppo ϕ non è davvero lineare. Però dato che in mezzo c'è solo il coniugio, possiamo provare a vedere cosa fa ϕ^2

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

E quindi effettivamente ϕ^2 è un omomorfismo di rappresentazioni irriducibili. Per questo motivo possiamo applicare Schur e concludere che

$$\phi^2 = \lambda Id_{V_\rho} \quad \lambda \in \mathbb{C}$$

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 riscalare) scegliere $\lambda = 1$, ovvero $\phi^2 = Id$. 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 □

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 6.7 (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

$$p(x) = a_0 + a_1x$$

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:

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

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 6.8. *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

Lemma 6.9. *Sia $\rho : G \rightarrow GL(V)$ rappresentazione irriducibile su \mathbb{R} . 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

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

\square

7 Rappresentazioni indotte

Supponiamo di avere $\rho : H \rightarrow GL(V)$ una rappresentazione di $H < G$ con G gruppo. Il nostro aim 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:

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

Osservazione: $Ind_H^G(W)$ 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 $Ind_H^G(W) \subseteq N$ e che tale sottospazio è ρ_N -invariante poichè detta $f \in Ind_H^G(W)$ 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 $\rho_N(g)f \in Ind_H^G(W)$. Questo ci dice che $Ind_H^G(W)$ è una sottorappresentazione di ρ_N che chiamiamo $\rho_{ind} : G \rightarrow GL(Ind_H^G(W))$.

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

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

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

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

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 $\rho_{ind} : G \mapsto GL(Ind_H^G(W))$ 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 $V = Ind_H^G(W)$. Ricordandoci il nostro aim, di certo vogliamo che W sia un sottospazio di V .

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

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

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

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 $\{g_i H\}_{i \in |G/H|}$ i rappresentanti delle classi laterali gH al variare di g in G allora

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

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

$$\Rightarrow V = \bigotimes_{i=1}^{|G/H|} V_{g_i H}$$

Voglio ora rintracciare W , in quanto sono interessata 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

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

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

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

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:

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

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} :

$$V_{eH} = \{f : G \rightarrow W : \rho(h)f(gh) = f(g) \forall h, g \text{ e } \text{Supp}(f) \subseteq H\}$$

Φ è un omo. di rapp. sse $\Phi(\rho_{ind}(h)f) = \rho(h)\Phi(f) \forall h \in H$.

$$\Phi(\rho_{ind}(h)f) = \rho(h)\Phi(f) \Leftrightarrow (\rho_{ind}(h)f)(e) = \rho(h)(f(e)) \Leftrightarrow f(h^{-1}e) = f(h^{-1}) = \rho(h)f(e)$$

ma ciò è vero in quanto le $f \in \text{Ind}_H^G(W)$.

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. *Detta $g_1H, \dots, g_{|G/H|}H$ 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

$$\begin{aligned} \text{Ind}_H^G(\mathbb{C}) &= \{f : G \rightarrow \mathbb{C} : \rho(h)f(gh) = f(gh) = f(g) \forall g, h\} \Rightarrow f \text{ è costante sulle classi laterali di } H \\ &\Rightarrow \text{Ind}_H^G(\mathbb{C}) = \{f : G \rightarrow \mathbb{C} : f \text{ è costante sulle classi laterali di } H\} = \mathbb{C}[G/H] \end{aligned}$$

$$\begin{array}{ccc} f : G & \longrightarrow & \mathbb{C} \\ \pi \downarrow & \nearrow f & \\ G/H & & \end{array}$$

G/H è un insieme finito dove G agisce per moltiplicazione a sinistra ($g(g'H) = gg'H$). Quindi

$Ind_H^G(W)$ 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 $dim(W) > 1$, $Ind_H^G(W) = \{f : G \rightarrow \mathbb{C} : f \text{ è costante sulle classi laterali di } H\} = \mathbb{C}[G/H] \otimes W$

Esercizio: Supponiamo che $W = W_1 \oplus W_2$ una rappresentazione di H non riducibile: allora

$$Ind_H^G(W) = Ind_H^G(W_1) \oplus Ind_H^G(W_2)$$

.

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

$$Ind : Rapp(H) \rightarrow Rapp(G)$$

e abbiamo anche "l'inversa" ovvero la restrizione della rappresentazione ad H

$$Res : Rapp(G) \rightarrow Rapp(H)$$

e risulta che $Res_H^G(V) = V$ 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

$$Hom_H(W, Res_H^G(U)) \cong Hom_G(Ind_H^G(W), U)$$

ovvero che ogni $\phi : W \rightarrow Res_H^G(U)$ omomorfismo di H -rappresentazione si estende in modo unico a un $\tilde{\phi} : Ind_H^G(W) \rightarrow U$ omomorfismo di G -rappresentazione

DIMOSTRAZIONE: sia $\phi : W \rightarrow Res_H^G(U)$ un omomorfismo di H -rappresentazione e sia $V := Ind_H^G(W) = \bigotimes_{i=1}^{\#-orbite} \rho_{ind}(g_i) V_{eH}$. Essendo $V_{eH} \cong W$ come H -rappresentazioni, allora $\phi : V_{eH} \rightarrow Res_H^G(U)$: 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

$$V_{g_iH} \xrightarrow{\rho_{g_i^{-1}}} V_{eH} \xrightarrow{\phi} Res_H^G(U) \xrightarrow{\sigma(g)} U \Rightarrow \sigma(g)\phi\rho_{ind}(g_i^{-1}) : V_{g_iH} \rightarrow U$$

Incollando tutte queste applicazioni ottengo $\tilde{\phi} : Ind_H^G(W) \rightarrow U$ dove $\tilde{\phi}(v) = \sigma_g \circ \phi \circ \rho_{ind}(g^{-1})(v)$ con $v \in V_{gH}$. Si verifica che $\tilde{\phi} \in Hom_G(Ind_H^G(W), U)$.

Vediamo ora che questa estensione è unica. Siano $\tilde{\phi}_1$ e $\tilde{\phi}_2$ due estensioni di ϕ : valutiamole nello stesso elemento $v \in V_{gH}$.

$$\tilde{\phi}_1(\rho_{ind}(g^{-1})v) = \phi(\rho_{ind}(g^{-1})(v)) = \tilde{\phi}_2(\rho_{ind}(g^{-1})v)$$

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. \square

7.1.1 Le rappresentazioni dei gruppi diedrali D_{2n}

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 $G = D_{2n}$ si scrive quindi

$$D_{2n} = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \dots, \tau\sigma^{n-1} \mid \tau^2 = \sigma^n = 1, \sigma\tau = \tau\sigma^{n-1}\}$$

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_{2n} . 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 $k = 0$, $\hat{\rho}_k(\sigma) = Id$. 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 di 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

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

Esempio 8.1. 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.

OSSERVAZIONE: Possiamo rapidamente notare che in questo caso la situazione è semplice, in quanto il gruppo è abeliano. Per questo motivo,

$$gh = hg \quad \forall g, h \in G$$

e quindi

$$\rho(g)\rho(h) = \rho(h)\rho(g) \quad \forall g, h \in G$$

Il che vuol dire che, fissato h , $\rho(h)$ è un omomorfismo di rappresentazioni irriducibili su \mathbb{C} . Possiamo allora applicare la versione forte di Schur e dire che $\rho(h) = \lambda(h)Id$ per qualche $\lambda \in \mathbb{C}$. Tuttavia quello che abbiamo fatto vale per ogni $h \in G$, per cui tutti i $\rho(g)$ sono in realtà scalari. Questo ci dice che le rappresentazioni irriducibili di \mathbb{S}^1 sono tutte di grado 1. A questo punto il nostro obiettivo è trovarle.

Proposizione 8.1. *Le rappresentazioni irriducibili di \mathbb{S}^1 sono tutte e sole le $\rho_n : \mathbb{S}^1 \rightarrow \mathbb{C}^*$ definite, al variare da 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, 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. 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:

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\phi} & \mathbb{S}^1 \\ \theta \downarrow & \searrow \hat{\rho} & \downarrow \rho \\ \mathbb{R} & \xrightarrow{\phi} & \mathbb{S}^1 \end{array}$$

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

$$e^{i\theta(x+y)} = \hat{\rho}(x+y) = \hat{\rho}(x)\hat{\rho}(y) = e^{i\theta(x)}e^{i\theta(y)}$$

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 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 $\theta(x) = \alpha x$, con $\alpha \in \mathbb{R}$. Non solo, possiamo dare delle informazioni a riguardo di α . Infatti, dato che $\hat{\rho}$ è “periodico”, deve essere

$$1 = \hat{\rho}(0) = \hat{\rho}(2\pi) = e^{i\alpha 2\pi}$$

per cui in realtà si ha $\alpha \in \mathbb{Z}$. Ricapitolando, abbiamo mostrato che per ogni $x \in \mathbb{R}$ vale che

$$e^{i2\alpha\pi x} = \rho(e^{ix})$$

dove α è un intero fissato. Ovvero per ogni $z \in \mathbb{S}^1$ vale

$$\rho_\alpha(z) = z^\alpha = \rho(z)$$

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}^{15} . 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).

¹⁵Tutto funziona allo stesso modo se al posto di \mathbb{R} mettiamo \mathbb{C} . In futuro non si baderà a questa distinzione.

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 $\rho : G \rightarrow GL(V_\rho)$ una sua rappresentazione continua. Sia I una integrazione su G . Si dice che I è invariante sotto ρ se

$$I(f(x)) = I(f(\rho(g)x)) \quad \forall g \in G$$

Se questa integrazione esiste, allora in analogia a quanto fatto per i gruppi finiti possiamo enunciare e dimostrare il seguente teorema.

Teorema 8.2. *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, in cui al posto di h_G si utilizza I . □