Dispense del corso di Teoria della Rappresentazione

Fabio Zoratti

17 febbraio 2017

Indice

1 Teoria dei gruppi

Definizione 1.1 (Gruppo)**.** Un gruppo è un insieme dotato di un'operazione binaria $\cdot : G \times G \to G$ 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, $card(G) = n$, 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. $f : I \to I$ biunivoca, con I insieme e con l'operazione di composizione. Nel caso in cui I sia un insieme finito, tanto vale scegliere $I = \{1, 2, 3, \ldots, n\}$. 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 $a_1, a_2, \ldots, a_n$, il prodotto $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ 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 $a^k = \underbrace{a \cdot a \cdot \cdots \cdot a}_{k \text{ volte}}$. 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:

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

   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

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

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 $gH \neq g'H$).

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, $|G/H| = \dfrac{|G|}{|H|}$; 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:

$$(g_1H) \cdot (g_2H) = g_1g_2H$$

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

Definizione 1.7 (Classi di coniugio)**.** Sia G un gruppo, $x \in G$, la classe di coniugio di x è l'insieme $\{gxg^{-1} | g \in G\}$. 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 $G \times H = \{(g, h) | g \in G, h \in H\}$ con l'operazione componente per componente, ovvero separatemente per i due gruppi di partenza.

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

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

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, $f : G \to H$ un omomorfismo di gruppi, allora definiamo

$$Kerf = \{g \in G \mid f(g) = e_H\}$$
$$Immf = \{h \in H \mid \exists g \in G \text{ t.c. } f(g) = h\}$$

Non è difficile verificare che sia $Kerf$ che $Immf$ sono sempre sottogruppi rispettivamente di G e di H, inoltre si può osserevare che $Kerf$ è un sottogruppo normale di G.

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 $a : G \times I \to I$ 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 $\forall\ i, j \in I\ \exists s \in G$ 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. 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 conugio.

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 $\phi : I \to J$ si dice G equivariante se

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

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 $f : \langle a \rangle \to \langle b \rangle$ ponendo $f(a^k) = b^k$ per $0 \leq k < n$.

Proposizione 1.3. *Sia C_n un gruppo ciclico di cardinalità n. Allora*

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

Dimostrazione: Sia a un generatore di C_n. Fissato $\omega \in \mu_n$ posso definire una funzione $f : C_n \to \mathbb{C}^*$ ponendo $f(a^k) = \omega^k$ per $0 \leq k < n$. Verifichiamo che $f \in Hom(C_n, \mathbb{C}^*)$. 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 $f \in Hom(C_n, \mathbb{C}^*)$. 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. □

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 $\quad \forall a, b \in G \quad ab = ba$.

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 1.4. *Ogni gruppo abeliano finito è isomorfo al prodotto diretto di gruppi ciclici.*

Osservazione. Sia G un gruppo abeliano. Allora

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

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 del gruppi simmetrici

Teorema 1.5 (Ogni elemento $\sigma \in S_n$ si scrive in modo unico come prodotto di cicli disgiunti a meno dell'ordine dei fattori)**.**

Proposizione 1.6. *Il segno di un ciclo di lunghezza k è esattamente $(-1)^{k-1}$*

1.4 Proprietà dei gruppi diedrali

Definizione 1.19 (Gruppo diedrale)**.** L'insieme D_n delle rotazioni e simmetrie di un poligono regolare di n lati è un gruppo con l'operazione di composizione. Detta ρ una rotazione di $2\pi/n$ (che ha ordine n, e per inverso ha ρ^n) e σ una qualunque riflessione (che ha ordine 2), esse generano il gruppo D_n, che si può quindi presentare nel seguente modo:

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

Osservazione. Le n potenze distinte di ρ sono tutte e sole le rotazioni di D_n, mentre gli elementi della forma $\sigma\rho^i,\ i = 0, 1, .., n-1$ 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 $M_1, \ldots, M_k \in \mathcal{M}(n, n, \mathbb{K})$, 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 $p(x) = a_n x^n + \ldots + a_0$, allora scriviamo $p(f)$ per intendere $a_n f^n + \ldots + a_0 f^0$ dove $f^0 = Id$ e $f^k = \underbrace{f \circ \ldots \circ f}_{k \text{ volte}}$.
Sia V un $\mathbb{K}$-spazio vettoriale, $f : V \to V$ 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, $f : V \to V$ un endomorfismo di V e $q(x) \in I(f)$. Sia $q = q_1 \cdot \ldots \cdot q_k$ tale che $MCD(q_i, q_j) = 1\ \forall\ i \neq j$, allora $V = Ker(q_1(f)) \oplus \cdots \oplus Ker(q_k(f))$ e gli addendi sono f-invarianti.*
In particolare se f è triangolabile e $\lambda_1, \ldots, \lambda_k$ sono gli autovalori di f con molteplicità geometrica rispettivamente $\alpha_1, \ldots, \alpha_k$, allora $V = Ker\left((f - \lambda_1 Id)^{\alpha_1}\right) \oplus \cdots \oplus Ker\left((f - \lambda_k Id)^{\alpha_k}\right)$.

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

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

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 $h : V \times V \to W$ si dice *forma hermitiana* se $\forall v, w, z \in V,\ \forall \alpha \in \mathbb{C}$ vale che

$$h(v, w) = \overline{h(w, v)}$$
$$h(\alpha v, w) = \alpha h(v, w)$$
$$h(v + z, w) = h(v, w) + h(z, w)$$

Definizione 2.3. Una forma hermitiana $\phi : V \times V \to \mathbb{C}$ è *definita positiva* (rispettivamente *negativa*) se $\forall\ v \in V, v \neq 0$ si ha che $\phi(v, v) > 0$ (rispettivamente $\phi(v, v) < 0$), ossarvare 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 $\phi : V \times V \to \mathbb{C}$ 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 $\{v_1, \ldots, v_n\}$ 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 uno spazio vettoriale e I un insieme; una base di V è una funzione $e : I \to V$ tale che $\forall v \in V,\ \exists!\ a : I \to \mathbb{C}$ a supporto finito per cui vale $v = \sum_{i \in I} a_i e_i$. La funzione a valutata in i prende il valore della i-esima coordinata del vettore v nella base e. Questa definizione è compatibile con la definizione di base come insieme di vettori generatori linearmente indipendenti.

Lemma 3.1. *Sia $e : I \to V$ una base di V e W uno spazio vettoriale. $f : I \to W$ una funzione. Allora $\exists!\ \phi : V \to W$ lineare tale che*

$$\phi(e_i) = f_i$$

Inoltre ϕ è un isomorfismo $\Leftrightarrow$ f 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 $\otimes : V \times W \to V \otimes W$ tale che per ogni data funzione bilineare $h : V \times W \to Z$, esiste unica $\phi : V \otimes W \to Z$ lineare per cui $\phi(v \otimes w) = h(v, w)$. Questa proprietà viene detta proprietà universale e la funzione $\otimes : V \times W \to V \otimes W$ viene detta funzione universale.

Proposizione 3.2. *Se ho due prodotti tensoriali $V \otimes W$ e $V \overline{\otimes} W$, allora esiste un unico isomorfismo $\phi : V \otimes W \to V \overline{\otimes} W$ tale che*

$$\phi(v \otimes w) = v \overline{\otimes} w$$

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 3.3.

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

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

Osservazione.

$$id_V \otimes id_W = id_{V \otimes W}$$

Proposizione 3.4. *Se e_i è una base di V e f_i è una base di W allora $e_i \otimes f_j$ è una base di $V \otimes W$*

Corollario.

$$dim(V \otimes W) = dimV \cdot dimW$$

Definizione 3.4. La *traccia* di un elemento del prodotto tensoriale, ovvero

$$tr(f \otimes g)$$

, è l'unico funzionale lineare $tr : V \otimes W \to \mathbb{K}$ che soddisfa le proprietà:

1. $tr[(v_1 \otimes w_1)(v_2 \otimes w_2)] = tr[(v_2 \otimes w_2)(v_1 \otimes w_1)]$
2. $tr[(id_V \otimes id_W)] = \dim V \cdot \dim W$

Teorema 3.5. *Se $f : V \to V$ e $g : W \to W$ sono endomorfismi di spazi vettoriali, allora vale la formula*

$$tr(f \otimes g) = tr(f)tr(g)$$

DIMOSTRAZIONE: L'applicazione $\phi : VxW \to \mathbb{K}$ che manda $(f \otimes g)$ in $tr(f)tr(g)$ è bilineare, e quindi corrisponde a un funzionale $\Phi : VxW \to \mathbb{K}$ lineare. Bisogna verificare che soddisfa le due proprietà della definizione. È evidente che $\Phi[(id_V \otimes id_W)]$

3.3 Prodotto esterno e prodotto simmetrico

Definizione 3.5 (Applicazione r-lineare simmetrica/alternante)**.** Una applicazione $\phi : V^n \to Z$ si dice r-lineare se è lineare in ogni componente dopo aver fissato le altre $n-1$.

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

Proposizione 3.6. *Un'applicazione $h : V^n \to W$ è alternante se e solo se $h(v_1, \ldots, v_n) = 0$ se $v_i = v_j$ per qualche $i \neq j$.*

Proposizione 3.7. *Un'applicazione $h : V^n \to W$ è nulla se i vettori $v_1, \ldots, v_n$ sono linearmente dipendenti.*

Definizione 3.6 (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 $\wedge : V^n \to \bigwedge^n V$ che manda $(v_1, \ldots, v_n)$ in $v_1 \wedge v_2 \wedge \ldots \wedge v_n \in \bigwedge^n V$, tale che $\forall h : V^n \to Z$ n-lineare alternante, esiste unica $\phi : \bigwedge^n V \to Z$ lineare per cui vale $\phi(v_1 \wedge v_2 \wedge \ldots \wedge v_n) = h(v_1, \ldots, v_n)$.

Teorema 3.8 (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 $E = \{e_{i_1} \wedge e_{i_2} \wedge \ldots \wedge e_{i_k} | 1 \leq i_1 < i_2 < \ldots < i_k \leq n\}$ è una base di $\bigwedge^k V$ e si ha $|E| = \binom{n}{k}$.*

MANCANO UN SACCO DI PROPRIETA' E LE DIMOSTRAZIONI

Definizione 3.7 (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 $V^n \to \bigwedge^n V$ che manda $(v_1, \ldots, v_n)$ in $v_1 v_2 \ldots v_n \in S^n V$, tale che $\forall h : V^n \to Z$ n-lineare simmetrica, esiste unica $\phi : S^n V \to Z$ lineare per cui vale $\phi(v_1 v_2 \ldots v_n) = h(v_1, \ldots, v_n)$.

Teorema 3.9 (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 $E = \{e_{i_1} \wedge e_{i_2} \wedge \ldots \wedge e_{i_k} | 1 \leq i_1 \leq i_2 \leq \ldots \leq i_k \leq n\}$ è una base di $S^k V$ e si ha $|E| = \binom{n+k-1}{k}$.*

Definizione 3.8 (Potenza simmetrica e potenza esterna di un'applicazione lineare)**.** Sia $f : V \to V$ un endomorfismo di uno spazio vettoriale. Definiamo

$$\bigwedge^k f : \bigwedge^k V \to \bigwedge^k V | f(v_1 \wedge \ldots \wedge v_n) = f(v_1) \wedge \ldots \wedge f(v_n)$$

In modo analogo si definisce la potenza simmetrica.

Proposizione 3.10. *Sia $f : V \to V$ un endomorfismo di uno spazio vettoriale. Allora vale*

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

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 $\rho : G \to GL(V_\rho)$ 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

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

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

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

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 $\rho : S_n \to GL(\mathbb{C}^n)$ 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 $\rho : G \to GL(V_\rho)$ 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. In particolare, tutte le matrici $\rho(s)$ sono simultaneamente diagonalizzabili $\Leftrightarrow$ G è abeliano.*

Dimostrazione: Se G è un gruppo finito, allora $\exists k | g^k = e$[1]. Dato che $\rho : G \to GL(V_\rho)$ mantiene queste proprietà in quanto omomorfismo, dovrà essere

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

[1]Dato che g è finito, se prendo l'insieme delle potenze $I = \{g^k | k \in \mathbb{Z}\}$, proprio perchè G è finito si ha che I ha un numero finito di elementi, quindi ci saranno $m, n \in \mathbb{Z}$ tali che $g^m = g^n = h$. Dato che nei gruppi esiste l'inverso, sarà $g^{n-m} = e$

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 finire l'ultima parte della dimostrazione: due endomorfismi di uno spazio vettoriale diagonalizzabili sono simultaneamente diagonalizzabili $\Leftrightarrow$ commutano. Da questo teorema segue facilmente la seconda parte dell'enunciato. $\square$

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 vettorali $\varphi : V_\rho \to V_\sigma$ 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

Teorema 4.3 (Le classi di isomorfismo delle rappresentazioni di grado 1 sono gli omomorfismi da G in $\mathbb{C}^*$)**.**

Esempio 4.1 (Rappresentazioni di grado 1 di C_n)**.**

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})

4.1 Operazioni con le rappresentazioni

Definizione 4.4 (Somma di rappresentazioni)**.**

Osservazioni:

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

Definizione 4.5 (Prodotto di rappresentazioni)**.**

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

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

Osservazione: vale

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

E l'isomorfismo è canonico. SCRIVI DIMOSTRAZIONE.

Definizione 4.7 (Rappresentazione regolare)**.**

Esempio 4.4 (La rappresentazione regolare di S_3)**.**

Teorema 4.4.

$$\mathcal{R}_G \cong \sum_i deg(\rho_i)\rho_i$$

4.2 Sottospazi invarianti e scomposizione delle rappresentazioni

Definizione 4.8 (Sottospazio invariante)**.** NON VA MESSO TUTTO ASSIEME NELLA DEFINIZIONE DI SOTTORAPPRESENTAZIONE???

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 $\sigma \subseteq \rho$).

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).

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 4.5 (Rappresentazione regolare di S_3)**.**

Teorema 4.5 (Le rappresentazioni di un gruppo finito sono completamente riducibili)**.**

Proposizione 4.6 (Prodotto hermitiano invariante)**.**

Lemma 4.7. *Sia $h : V_\rho \times V_\rho \to \mathbb{C}$ una forma hermitiana definita positiva e invariante per $\rho : G \to GL(V_\rho)$ e sia $\rho|_W : G \to GL(W)$ una sottorappresentazione di ρ. Allora se $W^\perp$ è l'ortogonale di W, $\rho|_{W^\perp} : G \to GL(W^\perp)$ è una sottorappresentazione.*

Lemma 4.8. *Sia $\rho : G \to GL(V_\rho)$ una rappresentazione di un gruppo finito G. Sia $\rho|_W : G \to GL(W)$ una sottorappresentazione di ρ. Allora esiste una sottorappresentazione $\sigma : G \to GL(W')$ tale che*

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

Osservazione. Notare che il teorema precedente è falso per gruppi finiti. (Esempio con $\mathbb{Z}^+$ che Salvatore non ha scritto con cura. Porco salvatore)

Teorema 4.9. *Se $\rho : G \to GL(V_\rho)$ e $\sigma : G \to GL(V_\sigma)$ sono rappresentazioni di G e $f : V_\rho \to V_\sigma$ è un omomorfismo di rappresentazioni, allora $Im(f)$ è una sottorappresentazione di σ e $Ker(f)$ è una sottorappresentazione di V_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 $\sigma(s)w = \sigma(s)f(v) = f(\rho(s)v) \in Im(f)$ □

Teorema 4.10. *Sia G un gruppo abeliano finito. Allora ogni rappresentazione di G è isomorfa alla somma di rappresentazioni di grado 1.*

Proposizione 4.11. *La rappresentazione regolare $\mathcal{R}$ di C_n è isomorfa alla somma delle n rappresentazioni irriducibili di grado 1 di C_n.*

Lemma 4.12. *Date ρ_1, ρ_2, σ rappresentazioni di G, allora*

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

Teorema 4.13 (Lemma di Schur)**.** *Siano ρ e σ due rappresentazioni irriducibili di G gruppo finito e $\phi : \rho \to \sigma$ un omomorfismo di rappresentazioni, allora ϕ è un isomorfismo oppure è identicamente nullo. Se poi $f : \rho \to \rho$ è un omomorfismo di rappresentazioni, allora f è una moltiplicazione per scalare.*

Dimostrazione. Supponiamo che $\phi \neq 0$, allora sappiamo che $Ker(\phi) \subseteq V_\rho$ è una sottorappresentazione di ρ, ma ρ è irriducibile e quindi $Ker(\phi) = 0 \Rightarrow \phi$ iniettiva. Ma anche $Im(\phi) \subseteq V_\sigma$ 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 $f - \lambda Id : V_\rho \to V_\rho$ 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). □

Teorema 4.14. *Sia $\rho : G \to GL(V_\rho)$ 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.

Lemma 4.15. *Sia ρ una rappresentazione di G e $\mathcal{R}$ la sua rappresentazione regolare. Allora*

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

Teorema 4.16. *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 $n_i = deg(\rho_i)$

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 $\rho : G \to GL(V_\rho)$ 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

$$\chi_\rho(s) := tr(\rho(s)) \qquad \forall s \in G$$

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

Vediamo delle proprietà elementari del carattere
Osservazioni:

1. Se $deg(\rho) = 1$ allora il carattere di s è uguale a $\rho(s)$
2. $\chi_{\rho_1} = deg(\rho)$. [2]
   Questo è vero poichè $[\rho_1] = I_n \Rightarrow tr(\rho_1) = n$ 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 $f : V \to V$ e $g : W \to W$ sono endomorfismi di spazi vettoriali, allora $tr(f \otimes g) = tr(f)tr(g)$.*

   Dimostrazione: Iniziamo a considerare il caso in cui sia f che g siano diagonalizzabili: prendendo due basi $a : I \to V$, $b : J \to W$ 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 matrice 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, $\forall s \in G\ \rho(s)^n = id$ dove $n = |G|$: dunque tutti gli autovalori di $\rho(s)$ sono radici ennesime dell'unità e $\rho(s)$ è diagonalizzabile[3]. In tale base è evidente che:

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

   in quanto, avendo gli autovalori modulo 1, l'inverso coincide con il coniugio.
6. $\chi_{\rho^*}(s)^4 = \overline{\chi_\rho(s)}$.
   Per l'osservazione precedente vale che

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

[2] Al solito ρ_1 è la rappresentazione che manda ogni elemento nell'identità di V_ρ
[3] Si veda la proposizione 4.2
[4] Ricordiamo 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
$$\chi_{\rho_I}(s) = \#punti\ fissi\ di\ \rho_I(s) = |I^s|$$
   dove $I^s := \{i \in I | s \circ i = i\}$. La veridicità di questo fatto si vede scrivendo esplicitamente la matrice che rappresenta $\rho_I(s)$.

9. Consideriamo la rappresentazione per permutazioni regolare R. Calcoliamone il carattere:
$$\chi_{\mathcal{R}}(s) = \begin{cases} |G| & \text{se } s = id \\ 0 & \text{se } s \neq id \end{cases}$$
   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*
$$\langle \chi_\rho|\chi_\sigma\rangle = \begin{cases} 1 & \textit{se } \rho \cong \sigma \\ 0 & \textit{altrimenti} \end{cases}$$

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 rappresentazioni* [5] *di G, allora vale*

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

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

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

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

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

E questo isomorfismo segue semplicemente dalle proprietà del prodotto tensore di spazi vettoriali. Notiamo che sullo spazio degli omomorfismi[6] $Z = Hom(V_\rho, V_\sigma)$ è possibile definire una rappresentazione completamente analoga a $\rho\sigma^*$ in questo modo: se $f \in Z$, allora possiamo definire la rappresentazione $\tau, V_\tau = Z$ di G in questo modo

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

É possibile mostrare che se chiamo Ψ la mappa tale che

$$\begin{cases} V_\rho^* \otimes V_\sigma \xrightarrow{\Psi} Hom(V_\rho, V_\sigma) \\ \rho\sigma^* \xrightarrow{\Psi} \tau \end{cases}$$

Allora Ψ è un isomorfismo di rappresentazioni. Dimostriamolo rapidamente. Innanzitutto definiamo in modo esplicito Ψ. Basterà definirlo per i tensori decomponibili, per il resto dello spazio basterà estenderlo per linearità.

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

Per mostrare che è un isomorfismo di rappresentazioni ci basta mostrare che ha la giusta proprietà di commutazione in quanto sappiamo già che Ψ è un isomorfismo di spazi vettoriali. Vediamo quindi di mostrare che

$$\Psi(\tau(s) \cdot (\phi \otimes v))(w) = \tau(s) \cdot \Psi(\phi \otimes v)(w) \qquad \forall s \in G \quad \text{eccetera}$$

Partiamo dal membro di sinistra e facciamo i calcoli

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

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

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

[5] Non necessariamente irriducibili

[6] Dato che sono spazi vettoriali in questo caso si tratta semplicemente di applicazioni lineari

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

A questo punto possiamo andare a cercare i sottospazi invarianti per τ, ovvero stiamo andando a cercare le sottorappresentazioni irriducibili di τ sperando di usare teoremi che già conosciamo. In particolare stiamo quindi cercando dei sottospazi $W \subset Z = Hom(V_\rho, V_\sigma)$ tali che $\tau(s)W \subset W \quad \forall s \in G$

In particolare, cerchiamo le funzioni $f \in Hom(V_\sigma, V_\rho)$ tali che $\tau(s)f = f$. Dalla definizione di τ si vede che

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

Ovvero le applicazioni f invarianti per τ sono gli omomorfismi di rappresentazioni da (ρ, V_ρ) a (σ, V_σ)

A questo punto

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

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

Visto che ci siamo ricondotti al caso in cui una rappresentazione è banale, ora facciamo i conti cercando di trovare la dimensione dello spazio invariante per G. Scriviamo la definizione di quello che vogliamo calcolare

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

Se definiamo l'operatore T come operatore lineare

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

Allora si nota che

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

Per cui sappiamo che $V_\rho^G \subseteq ImT$. L'obiettivo è mostrare che quella non è una disuguaglianza ma un'uguaglianza. In realtà questa è la disuguaglianza stupida in quanto se $v \in V_\rho^G$ allora è chiaro che $Tv = v$, basta applicare la definizione. Per cui $ImT = V_\rho^G$. A questo punto vogliamo calcolare la sua traccia. Per farlo notiamo che

$$T(Tv) = \ldots = Tv \qquad \text{Verifica banale}$$

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

$$V_\rho = KerT \oplus ImT = KerT \oplus V_\rho^G$$

Per cui $trT = dimImT = dimV_\rho^G$. Ma dalla catena di deduzioni che abbiamo fatto

$$dimHom(V_\sigma, V_\rho) = dim(V_{\sigma^*\rho}^G) = trT = \langle \chi_{\sigma^*\rho} | 1 \rangle = \langle \chi_\sigma | \chi_\rho \rangle$$

□

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

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

  Quindi ottengo una conferma del teorema precedente

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

- 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*

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

Ma è ovvio che

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

Per cui lo spazio $V_{\rho_I}^G = \{\sum a_i e_i | Alcune\ condizioni\}$ sarà composto da i vettori che hanno i coefficienti a_i costanti su ciascuna orbita di G su I, proprio per lasciarlo invariante. Perciò

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

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

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

□

Teorema 5.4. *Sia G un gruppo finito e siano $\rho_1, \ldots, \rho_r$ 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 $dimCl(G) = $ 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: DA SCRIVERE

5.1 Tabella dei caratteri

Dato un gruppo G, possimo 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	$\lvert orb(g_1)\rvert$	$\lvert orb(g_2)\rvert$	

- 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 1	(12) 3	(1 2 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 1	(12) 3	(1 2 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 1	(12) 3	(1 2 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 1	(12) 3	(1 2 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 1	(12) 3	(1 2 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 4.16)

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

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

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

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

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

E andando a calcolare

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

Per cui è effettivamente irriducibile. Aggiungiamola alla tabella.

Abbiamo appena terminato le rappresentazioni che conoscevamo di S_4.

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

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

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

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

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

Quindi...

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

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:

Ossevazione: 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)	(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

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

$$S_4 \to S_3$$

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

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

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

Lemma 5.7. *Se ρ è una rappresentazione di grado d di G, come sempre gruppo finito, allora:*
(a) $|\chi_\rho(s)| \leq d$
(b) Direttamente dal punto (a) si decude che,

$$\chi_\rho(s) = d \Leftrightarrow \lambda_1, ..., \lambda_d = 1 \Leftrightarrow \rho(s) = id$$

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

Dimostrazione: Se $\lambda_1, .., \lambda_d$ sono gli autovalori della matrice $[\rho(s)]$ allora $\chi_\rho(s) = \sum_{i=1}^d \lambda_i$. Inoltre essendo G finito $|\lambda_i| = 1 \forall i \in \{1, ..., d\}$. 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 cubo[7]. 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 soprattuto commuta con le simmetrie del problema. Ora spiegherò meglio questo concetto.

Consideriamo il gruppo G delle rotazioni del cubo, ovvero

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

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

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

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

$$gT = Tg$$

Ovvero ci dice che $\forall g \in G$ le due operazioni commutano. Le due frasi precedenti sono state dette un po' alla garibaldina in quanto non è g ad agire sul cubo ma è una sua rappresentazione di grado $|F| = 6$. Di conseguenza è bene scrivere in modo formale che $\tau : G \to GL(V_\tau)$ è una rappresentazione del gruppo di rotazioni del cubo in $\mathbb{C}^6$ e questa rappresentazione commuta con un operatore T, ovvero

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

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

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

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 4.16 sappiamo che tutte

[7] Che ha quindi 6 elementi

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 rispettivaemente dimensione 1,3,2.

SCRIVI PIÚ DETTAGLIATO CHE DEVO ANDARE A LEZIONE

$$V_1 = span(e_1 + e_2 + ... + e_6)$$

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

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

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 $T^n \to$ 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 $\mathbb{Z}/3\mathbb{Z}$[8]. 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 $\rho : G \to GL(V_\rho)$ 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 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

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

è una sottorappresentazine 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:*

[8] Che per i fisici è isomorfo a C_3

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

2. *V_ρ possiede una forma bilineare simmetrica $G-$invariante. Ovvero lo spazio delle forme bilineari simmetriche $S^2V^* \subset V \otimes V$ è tale che $(S^2V^*)^G \neq 0$.*

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 $\mathbb{C}$ da V. Consideriamo ora una forma bilineare simmetrica B_0 non degenere $/\mathbb{R}$

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

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 $\tilde{B}_0 \in (S^2V_0^*)^G$). Possiamo a questo punto estenderla a forma bilineare su V complessificandola in modo ovvio. Consideriamo quindi B

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

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

$$B(v_1 + iv_1', v_2 + iv_2') = \left(\tilde{B}_0(v_1, v_2) - \tilde{B}_0(v_1', v_2')\right) + i\left(\tilde{B}_0(v_1', v_2) + B_0(v_1, v_2')\right)$$

É una banale verifica controllare che rispetta le caratteristiche richieste. □

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 degenere (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

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

A questo punto, se $\phi : V \to V^*$ 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 $\lambda \in \mathbb{C}$. □

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:

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

ma dato che

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

allora

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

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

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

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

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 $m_\rho = 1 \Rightarrow (S^2V^*)^G \neq 0$*
  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

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

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 $\rho : G \to GL(V)$ 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 cercare i sottogruppi normali H_i di Q_8 e quozientare rispetto a quelli per cercare in modo facile delle rappresentazioni di grado 1. L'ultima rappresentazione che si trova deve avere dimensione 2 perché $\sum n_i^2 = |G|$. Vedremo poco sotto che cosa significa questa rappresentazione.

	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.

COSE RANDOM SCRITTE DI FRETTA PERCHÉ devo andare a lezione

Matrici di spin di Pauli

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

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 $h : V_\rho \times V_\rho \to \mathbb{C}$ hermitiana, definita positiva e $G-$invariante. Questa sicuramente esiste, è stato dimostrato nel teorema METTI IL LINK,

Definiamo a questo punto un endomorfismo di V_ρ che chiamiamo $\phi : V_\rho \to V_\rho$, 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

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

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

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

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

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

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

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

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

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

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

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

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 $\cdot : A \times A \to A$ 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 $\rho : G \to GL(V_\rho)$ con V_ρ spazo vettoriale su $\mathbb{R}$. Allora l'insieme degli endomorfismi di ρ

$$End_G(V_\rho)$$

è un'algebra di divisione su 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 $End_G(V_\rho)$ o è la funzione nulla oppure è un isomorfismo, quindi ammette inverso. Se il gruppo è finito, ovviamente l'algebra sarà di dimensione finita.

Presentiamo ora un sorprendente teorema che afferma che non ci sono altre algebre di divisione di dimensione finita 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

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

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

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

Ovvero il polinomio a coefficienti reali

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

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

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

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

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

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

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

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

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

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

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

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 $\psi_z : A \to A$ definita da $\psi_z(x) = zx$. Osserviamo che valgono le seguenti implicazioni:

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

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

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

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