# RAPPRESENTAZIONI LINEARI DEI GRUPPI FINITI

R. BENEDETTI

La teoria delle rappresentazioni lineari (su $\mathbb{C}$) dei gruppi finiti (che rimonta ai lavori di H. Maschke, 1853-1908) è una delle applicazioni più compiute e spettacolari dell'algebra lineare elementare che normalmente a Pisa viene insegnata al primo anno della laurea triennale, sia a Matematica sia a Fisica. Per il lettore interessato ad approfondire l'argomento, oltre queste note, è molto consigliato il testo:

Jean-Pierre Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, 42. New YorkHeidelberg: Springer-Verlag 1977.

## 1. Gruppi

Richiamiamo qui le nozioni essenziali sui gruppi che ci servono per sviluppare il discorso.

Un gruppo $(G, *)$ è un insieme non vuoto $G$, munito di un'operazione $* : G \times G \to G$, che verifica la proprietà associativa, ammette un elemento neutro (necessariamente unico) $u$ ($u * g = g * u = g$) ed è tale che ogni elemento $g$ ammette un inverso $g'$ (necessariamente unico) ($g * g' = g' * g = u$). Non richiediamo che l'operazione sia commutativa. Se questo è il caso diciamo che il gruppo è commutativo o *Abeliano*. Invece di $*$ useremo la *notazione moltiplicativa*, per cui invece di $g * h$ scriveremo semplicemente $gh$, $u$ sarà indicato con il simbolo $1 = 1_G$, mentre l'inverso di $g$ sarà indicato con il simbolo $g^{-1}$. Se il gruppo è commutativo e vogliamo enfatizzare questo fatto, useremo a volte la *notazione additiva* ($g * h \leftrightarrow g + h$, $u \leftrightarrow 0$, $g^{-1} \leftrightarrow -g$). In presenza di due (o più) gruppi faremo spesso l'abuso (indolore) di usare le stesse notazioni per le differenti operazioni in gioco. Quando diremo "$G$ è un gruppo", l'operazione sarà sottointesa.

Se $G$ è un gruppo un sottoinsieme $H \subset G$ è un *sottogruppo* se $1 \in H$, $H$ è chiuso rispetto all'operazione di $G$ ed è un gruppo una volta munito della restrizione dell'operazione.

Una applicazione $\phi : G \to G'$ è un *omomorfismo di gruppi* se per ogni $g, h \in G$, allora $\phi(gh) = \phi(g)\phi(h)$. L'omomorfismo $\phi$ è un *isomorfismo* se è biunivoco e il suo inverso (insiemistico) $\phi^{-1} : G' \to G$ è a sua volta un omomorfismo di gruppi.

Per ogni $g \in G$, l'applicazione $\gamma_g : G \to G$, definita da $\gamma_g(h) = g^{-1}hg$ è un isomorfismo di gruppi (detto anche un *automorfismo interno di* $G$). Due sottoinsiemi $H$ e $H'$ di $G$ (in particolare due sottogruppi) si dicono *coniugati* se esiste $g \in G$ tale che $H' = \gamma_g(H)$. Applicando questa nozione agli elementi di $G$, otteniamo una relazione di equivalenza su $G$. La classe di equivalenza di $g \in G$, indicata con $C(g)$, è detta la *classe di coniugazione* di $g$.

Il lettore può verificare per esercizio i seguenti fatti:

Dato $\phi : G \to G'$ un omomorfismo di gruppi, allora:

- Necessariamente $\phi(1) = 1$, $\phi(g^{-1}) = \phi(g)^{-1}$).
- Ker $\phi := \{g \in G;\ \phi(g) = 1\}$ è un sottogruppo di $G$ mentre l'immagine di $\phi$, Im $\phi$, è un sottogruppo di $G'$. Se $H$ è un sottogruppo di $G$ allora $\phi(H)$ è un sottogruppo di $G'$.
- $\phi$ è un isomorfismo se e solo se è biunivoco.
- $\phi$ è iniettivo se e solo se Ker $\phi = 1$; in tal caso $\phi$ è un isomorfismo tra $G$ è la sua immagine in $G'$, cioè $G$ è identificato (per mezzo di $\phi$) con un sottogruppo di $G'$.

- Se $H$ è un sottogruppo di $G$ e $H$' è un sottoinsieme coniugato ad $H$, allora $H'$ è un sottogruppo di $G$. Un sottogruppo $H$ di $G$ si dice *normale* se coincide con tutti i suoi coniugati. Ker $\phi$ è normale.
- $G$ è Abeliano se e solo se ogni classe di coniugazione $C(g)$ consiste del solo elemento $g$.

1.1. **Esempi e osservazioni.**

(1) Se $(V, +, .)$ è uno spazio vettoriale sul campo $\mathbb{K}$, allora $(V, +)$ è un gruppo Abeliano. Se $\phi : V \to W$ è un'applicazione lineare tra spazi vettoriali, allora $\phi : (V, +) \to (W, +)$ è un omomorfismo di gruppi (Abeliani).

(2) **Gruppi lineari o di matrici.** Se $V$ è come sopra uno spazio vettoriale, $GL(V)$ – detto appunto il *gruppo lineare generale* di $V$ – è il gruppo formato dagli endomorfismi invertibili, cioè gli *automorfismi lineari* di $V$, con operazione data dalla composizione. Se $V = \mathbb{K}^n$, allora $GL(\mathbb{K}^n)$ si identifica canonicamente come il gruppo $GL(n, \mathbb{K})$ delle matrici $n \times n$ invertibili su $\mathbb{K}$, con operazione data dal prodotto di matrici. Se $n > 1$, $GL(n, \mathbb{K})$ non è commutativo.

In generale *un gruppo lineare* (*un gruppo di matrici*) è un sottogruppo di qualche $GL(V)$ ($GL(n, \mathbb{K})$). Vediamo alcuni esempi. Se $V$ è munito di un prodotto scalare non degenere $\Phi$, il gruppo ortogonale $O(\Phi)$ di $(V, \Phi)$ è un sottogruppo di $GL(V)$. Se $V = \mathbb{K}^n$, $\Phi(X, Y) = X^t MY$, $M \in GL(n, \mathbb{K})$, $M = M^t$, allora

$$O(\Phi) = \{P \in GL(n, \mathbb{K}); P^{-1} = M^{-1} P^t M\}$$

che è un sottogruppo di $GL(n, \mathbb{K})$. In particolare se $M = I$, $O(n, \mathbb{K}) = \{P;\ P^{-1} = P^t\}$ è un *gruppo ortogonale (matriciale) classico* su $\mathbb{K}$. Se $\mathbb{K} = \mathbb{R}$ e

$$M = \begin{bmatrix} I_{n-1} & 0 \\ 0 & -1 \end{bmatrix}$$

si ottiene un *gruppo di Lorentz*.

Se $\mathbb{K} = \mathbb{C}$ e $\Phi$ è un prodotto Hermitiano non degenere su $V$, allora il *gruppo unitario* $U(\Phi)$ è definito formalmente come i gruppi ortogonali qui sopra, ed è un sottogruppo di $GL(V)$. Se $V = \mathbb{C}^n$, $\Phi(X, Y) = X^t M \overline{Y}$, $M \in GL(n, \mathbb{C})$, $M^t = \overline{M}$, allora $U(\Phi) = \{P;\ P^{-1} = M^{-1} \overline{P}^t M\}$ ed è un sottogruppo di $GL(n, \mathbb{C})$. Se $M = I$, allora $U(n) = \{P;\ P^{-1} = \overline{P}^t\}$ è un *gruppo unitario (matriciale) classico*.

Per ogni gruppo di matrici $G$, è definito il sottogruppo "*speciale*"

$$SG = \{A \in G;\ \det A = 1\}\ .$$

Si noti che $\det_{|G} : G \to \mathbb{K}$ è un omomorfismo di gruppi (Binet) e quindi $SG = \text{Ker } \det_{|G}$.

(3) **Gruppi di trasformazioni.** Dato un insieme non vuoto $X$, il *gruppo completo delle trasformazioni di* $X$ (a volte dette anche le *simmetrie* di $X$), è il gruppo

$$S(X) = \{f : X \to X;\ f \text{ biunivoca}\}$$

dove l'operazione è data dalla composizione. In generale *un gruppo di trasformazioni di* $X$ è un sottogruppo di $S(X)$. Per esempio, se $X = V$ è come sopra uno spazio vettoriale, allora $GL(V)$ è un sottogruppo di $S(V)$ e quindi un gruppo di trasformazioni di $V$. Lo stesso vale per tutti i gruppi lineari.

Diciamo che un gruppo $G$ *agisce su un insieme* $X$ se esiste un omomorfismo di gruppi $\phi : G \to S(X)$. In tal caso *l'azione* è data da $a : G \times X \to X$, $a(g, x) = \phi(g)(x)$. Per esempio $S(X)$ agisce su $X$ ($\phi = \text{Id}$), $GL(V)$ agisce su $V$ ($\phi$ è l'inclusione di $GL(V)$ in $S(V)$). Se $Y$ è un sottoinsieme non vuoto di $X$, e $G$ è un gruppo di trasformazioni

di $X$ allora allora $G(Y) = \{f \in G;\ Y \ \text{f}-\text{invariante}\}$ è contemporaneamente un sottogruppo di $G$ e si $S(Y)$ e quindi agisce su entrambi $X$ e $Y$.

Per ogni gruppo $G$ e per ogni $g \in G$, definiamo $s_g : G \to G$ come $s_g(h) = gh$ (la *moltiplicazione a sinistra per* $g$). Si ha immediatamente che:

$$s_{gg'} = s_g \circ s_{g'},\ s_1 = s_{g^{-1}g} = s_{g^{-1}} \circ s_g = \mathrm{Id}$$

per cui in particolare $s_g \in S(G)$. Inoltre $s_g = s_{g'}$ se e solo se $g = g'$, infatti se $gh = g'h$, moltiplicando a destra per $h^{-1}$ abbiamo la tesi. Riassumendo, abbiamo dimostrato:

**Lemma 1.1.** *Per ogni gruppo $G$, la moltiplicazione a sinistra definisce un omomorfismo iniettivo $\mathfrak{s} : G \to S(G)$ e quindi un'azione di $G$ su $G$. In particolare ogni gruppo è isomorfo ad un gruppo di traformazioni.*

(4) **Gruppi di isometrie geometriche.** Sia $(V, \Phi)$ uno spazio reale munito di un prodotto scalare definito $> 0$, oppure uno spazio complesso munito di un prodotto Hermitiano definito $> 0$. Concretamente possiamo pensare a $V = \mathbb{R}^n$ con prodotto $\Phi(X, Y) = X^t Y$, oppure $V = \mathbb{C}^n$ con prodotto $\Phi(X, Y) = X^t \overline{Y}$. In entrambi i casi $d(v, w) := \sqrt{\Phi(v - w, v - w)}$ definisce una distanza su $V$. Nei casi concreti questa è la distanza Euclidea su $\mathbb{R}^n$ o su $\mathbb{R}^{2n} \cong \mathbb{C}^n$ (come $\mathbb{R}$-spazi). Definiamo allora

$$\mathcal{I}(V, d) = \{f : V \to V;\ \forall (v, w),\ d(v, w) = d(f(v), f(w))\}\ .$$

Osserviamo che *non* richiediamo che $f \in GL(V)$, e non richiediamo neanche che $f$ sia biunivoca (benché sia necessariamente iniettiva). Mostreremo che in effetti $\mathcal{I}(V, d)$ è un ben determinato gruppo di trasformazioni di $V$ che preservano la distanza. Evidentemente il gruppo ortogonale (o unitario) $O(\Phi)$ ($U(\Phi)$) è contenuto in $\mathcal{I}(V, d)$. Per ogni $v \in V$ è definita la *traslazione* $\tau_v : V \to V$, $\tau_v(w) := w + v$, che è lineare solo quando $v = 0$. E' immediato che le traslazioni formano un gruppo $\mathcal{T}(V)$ di trasformazioni di $V$, canonicamente isomorfo a $(V, +)$, anch'esso contenuto in $\mathcal{I}(V, d)$. Quindi l'unione $O(\Phi) \cup \mathcal{T}(V)$ ( $U(\Phi) \cup \mathcal{T}(V)$), genera un gruppo di trasformazioni $\mathcal{A}(V, d)$ contenuto in $\mathcal{I}(V, d)$. Il generico elemento $g \in \mathcal{A}(V, d)$ è della forma

$$g = g_1 \circ \cdots \circ g_k$$

per qualche $k \in \mathbb{N}$, dove ogni $g_j$ appartiene a $O(\Phi)$ ($O(\Phi)$) oppure a $\mathcal{T}(V)$.

**Lemma 1.2.** $\mathcal{A}(V, d) = \{\tau_v \circ g;\ v \in V,\ g \in O(\Phi)\ (O(\Phi))\}$.

*Dimostrazione.* Basta dimostrare che ogni $g \circ \tau_v$ può essere espresso nella forma prescritta dall'enunciato. Poi si conclude facilmente per induzione su $k$. D'altra parte, per ogni $w \in V$, $g \circ \tau_v(w) = g(w + v) = g(w) + g(v) = \tau_g(v) \circ g(w)$. Si noti anche che $\tau_v \circ g^{-1} = \tau_{g^{-1}(-v)} \circ g^{-1}$.

□

Vogliamo infine dimostrare

**Proposizione 1.3.** $\mathcal{I}(V, d) = \mathcal{A}(V, d)$.

*Dimostrazione.* Sia $f \in \mathcal{I}(V, d)$. Se $v = f(0)$, allora $h = \tau_{-v} \circ f \in \mathcal{I}(V, d)$ e $h(0) = 0$. Basta allora dimostrare che tale $h \in O(\Phi)$ ($\in U(\Phi)$). Poiché, per ogni $w \in V$, $\Phi(w, w) = d^2(w, 0) = d^2(h(w), h(0)) = \Phi(h(w), h(w))$, abbiamo verificato che $h$ preserva la norma dei vettori. Poiché, per ogni $w, z \in V$ $\Phi(w - z, w - z) = d^2(w, z) = d^2(h(w), h(z)) = \Phi(h(w) - h(z), h(w) - h(z)$, sviluppando per bilinearità i due prodotti scalare (Hermitiani) e sfruttando l'invarianza delle norme gia' stabilita, si deduce che $\Phi(w, z) = \Phi(h(w), h(z))$. Cioè $h$ preserva tutto il prodotto scalare (Hermitiano).

Quindi se $\{v_1, \ldots, v_n\}$ è una base ortonormale (unitaria) di $(V, \Phi)$ ne segue che anche $\{h(w_1), \ldots, h(v_n)\}$ è una base ortonormale (unitaria). Per ogni $w \in V$, $w = \sum_j a_j v_j$, $h(w) = \sum_j b_j h(v_j)$. Infine, per ogni $j = 1, \ldots, n$, $a_j = \Phi(w, v_j) = \Phi(h(w), h(v_j)) = b_j$. Quindi $h$ è lineare e appartiene a $O(\Phi)$ ($(U(\Phi))$ come voluto.

□

**Osservazioni 1.4.** Se $Y$ è una "molecola" in $(\mathbb{R}^3, d)$ il gruppo $\mathcal{I}(\mathbb{R}^3, d)(Y)$ delle "simmetrie geometriche" di $Y$ è particolarmente studiato in chimica. In geometria classica sono particolarmente studiati i gruppi $\mathcal{I}(\mathbb{R}^3, d)(Y)$ dove $Y$ è un poliedro convesso, per esempio "platonico".

**Esercizi 1.5.** (a) Sia $Y \subset V$ e consideriamo $\mathcal{I}(V, d)(Y)$. Mostrare che $\mathcal{I}(V, d)(Y)$ è coniugato ad un sottogruppo di $O(\Phi)$ ($U(\Phi)$) $\subset \mathcal{I}(V, d)$, se e solo se esiste un punto fisso per $\mathcal{I}(V, d)(Y)$, cioè $v \in V$ tale che $h(v) = v$ per ogni $h \in \mathcal{I}(V, d)(Y)$.
(b) Un "segmento" (chiuso e limitato) in $\mathbb{R}^3$ è un sottoinsieme della forma $I = \{tv_0 + (1-t)v_1; 0 \leq t \leq 1,\ v_0, v_1 \in \mathbb{R}^3\}$. Mostrare che se $Y \subset \mathbb{R}^3$ è unione di un insieme finito di segmenti, allora $\mathcal{I}(\mathbb{R}^3, d)(Y)$ è coniugato ad un sottogruppo di $O(\Phi)$. Individuare condizioni necessarie e/o sufficienti su $Y$ in modo che $\mathcal{I}(\mathbb{R}^3, d)(Y)$ risulti finito.

## 2. Rappresentazioni lineari di un gruppo.

In questa Sezione fissiamo alcune nozioni essenziali sulle rappresentazioni lineari.

- Un omomorfismo di gruppi $\rho : G \to GL(n, \mathbb{K})$ è detto una *rappresentazione lineare di $G$ (su $\mathbb{K}$) di dimensione finita uguale a $n$*. Ad ogni rappresentazione corrisponde un'azione di $G$ su $\mathbb{K}^n$. La rappresentazione è *fedele* se è iniettiva. In tal caso $G$ risulta isomorfo ad un gruppo di matrici. Può capitare che una rappresentazione sia a valori in qualche gruppo di matrici più ristretto. Ad esempio, una rappresentazione $\rho$ è detta *ortogonale* se è a valori in $O(n, \mathbb{K})$. Se $\mathbb{K} = \mathbb{C}$, $\rho$ è detta *unitaria* se è a valori in $U(n)$). Considereremo solo rappresentazioni di dimensione finita e questo sarà sottointeso in tutto il resto della nota.
- Due rappresentazioni lineari $\rho$ e $\rho'$ di $G$ (su $\mathbb{K}$) sono dette *coniugate* se hanno la stessa dimensione $n$, ed esiste $P \in GL(n, \mathbb{K})$ tale che, per ogni $g \in G$, $\rho'(g) = P^{-1}\rho(g)P$. La "coniugazione" definisce una relazione di equivalenza sull'insieme di tutte le rappresentazioni lineari (su $\mathbb{K}$) di un gruppo $G$ dato. Il problema generale è quello di studiare l'insieme quoziente. Indicheremo con $[\rho]$ la classe di equivalenza (di coniugazione) di $\rho$. Diremo che una classe è (per esempio) ortogonale o unitaria se contiene un rappresentante con quella proprietà.
- Date due rappresentazioni lineari $\rho$ e $\rho'$ (su $\mathbb{K}$) di $G$ di dimensione $n$ e $n'$ rispettivamente, possiamo definire una rappresentazione $\rho \oplus \rho'$ di dimensione $n + n'$ come segue; per ogni $g \in G$:

$$\rho \oplus \rho'(g) := \begin{bmatrix} \rho(g) & 0 \\ 0 & \rho'(g) \end{bmatrix}$$

Una rappresentazione lineare $\beta$ di $G$ di dimensione $m$ si dice *riducibile* se esistono $n, n' > 0$, $m = n + n'$, e due rappresentazioni $\rho$ e $\rho'$ di dimensione $n$ e $n'$ rispettivamente, tali che $\beta$ è coniugata a $\rho \oplus \rho'$. Altrimenti $\beta$ è detta *irriducibile*. E' immediato che l'essere (o no) riducibile è una proprietà invariante a meno di coniugazione, per cui ha senso dire che la classe di coniugazione $[\beta]$ è (o no) riducibile, in tal caso scriveremo $[\beta] = [\rho] \oplus [\rho']$. Anche il seguente Lemma è di dimostrazione immediata.

**Lemma 2.1.** *(1) Condizione necessaria e sufficiente affinché $\beta$ sia riducibile è che esista una decomposizione in somma diretta non banale $V = W_1 \oplus W_2$, tale che entrambi gli addendi siano $\beta$– invarianti, cioè $W_j$ è $\beta(g)$–invariante per ogni $g \in G$.*

*(2) Condizione necessaria affinché $\beta$ sia riducibile è che esista un sottospazio vettoriale non banale (cioè $1 \leq \dim W < n$) $W \subset \mathbb{K}^n$ che sia $\beta$–invariante.*

*Inoltre il verificarsi o meno di queste condizioni è una proprietà invariante per coniugazione, dunque è una proprietà della classe di coniugazione $[\beta]$.*

*(3) $[\rho] \oplus [\rho'] = [\rho'] \oplus [\rho]$*

**Osservazioni 2.2.** In generale la condizione (2) non è sufficiente. Ad esempio si consideri $\beta : (\mathbb{Z}, +) \to GL(2, \mathbb{C})$, $\rho(n) = A^n$, dove

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

L'autospazio dell'autovalore $\lambda = 1$ di $A$ è $\beta$-invariante, ma $\beta$ non è riducibile perché $A$ non è diagonalizzabile.

## 3. Gruppi finiti

Dopo avere stabilito le precedenti generalità, da ora in poi ci specializzeremo al caso dei gruppi finiti, di cui studieremo le rappresentazioni lineari su $\mathbb{C}$ (e solo parzialmente su $\mathbb{R}$).

Dato un gruppo finito $G$ il numero dei suoi elementi, $|G| \in \mathbb{N}$, viene detto l'*ordine* di $G$. Se $|G| = n$, fisseremo a volte un ordinamento ausiliario dei suoi elementi $G = \{g_1 = 1, g_2, \ldots, g_n\}$, cioè, posto $X_n := \{1, \ldots, n\}$, fissiamo un' applicazione biunivoca $\tau : X_n \to G$, $\tau(1) = 1_G$. Il gruppo delle simmetrie $S_n := S(X_n)$ è anche noto come gruppo delle *permutazioni* degli elementi di $X_n$, o anche come *gruppo simmetrico* (sugli $n$ elementi di $X_n$). $S_n$ è uno dei più importanti gruppi finiti; è ben noto che $|S_n| = n!$ . Per messo di $\tau$ è evidentemente fissato anche un isomorfismo di gruppi (indicato ancora con $\tau$) $\tau : S_n \to S(G)$. Usando il Lemma 1.1 abbiamo infine:

**Lemma 3.1.** *Per ogni gruppo finito $G$, $|G| = n$, e ogni ordinamento $\tau$ dei suoi elementi, la moltiplicazione a sinistra induce un omomorfismo iniettivo $\tau^* : G \to S_n$. In particolare ogni gruppo finito è isomorfo ad sottogruppo di $S_n$, $n = |G|$. I sottogruppi di $S_n$ associati a diversi ordinamenti di $G$ sono tra loro coniugati.*

Si noti che $n = |G|$ divide $n! = |S_n|$. Questo è un caso particolare del seguente:

**Lemma 3.2.** *Se $G$ è un gruppo finito e $H$ è un sottogruppo di $G$ allora $|H|$ divide $|G|$ (cioè $|G| = k|H|$).*

*Dimostrazione.* Consideriamo su $G$ la seguente relazione: $g \sim_H g'$ se esistono $h$ e $h'$ in $H$ tali che $gh = g'h'$. E facile vedere che è una relazione di equivalenza. La classe di equivalenza di $g$ è detta *classe laterale destra* di $g$ rispetto a $H$, ed è indicata con $gH$. Supponiamo che ci siano $k$ classi di equivalenza. Le classi di equivalenza formano una partizione di $G$. Se dimostriamo che sono tutte formate da $m = |H|$ elementi abbiamo finito. Adesso, $gH = \{gh_1, \ldots, gh_m\}$ ($h_i \neq h_j$ se $i \neq j$), con a priori delle ripetizioni. Affermiamo invece che sono tutti distinti. Altrimenti $gh_i = gh_j$, per qualche $i \neq j$ implicherebbe $h_i = h_j$.

□

Dato $g \in G$, poniamo $g^0 = 1$, $g^1 = g$, $g^n = g^{n-1}g$ per ogni intero $n \geq 1$, $g^n = (g^{-1})^{-n}$) per ogni intero $n < 0$. Allora $< g >= \{g^n;\ n \in \mathbb{Z}\}$ è un sottogruppo di $G$, detto il *sottogruppo ciclico generato da $g$*. L'ordine di $< g >$ (che divide $|G|$) è anche detto l'ordine dell'elemento $g$.

**Esercizi 3.3.** L'ordine dell'elemento $g \in G$ è il minimo $n \geq 1$ tale che $g^n = 1$.

**Esempio 3.4. (Alcuni esempi di gruppi finiti.)** (1) I gruppi finiti Abeliani sono classificati a meno di isomorfismo: ogni tale $G$ è isomorfo ad un prodotto della forma

$$\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

dove ogni $p_j \geq 2$ è primo, e $p_j > p_{j+1}$. Inoltre $\{(p_j, n_j)\}$ è un invariante completo a meno di isomorfismi di gruppi.

(2) Ogni gruppo di matrici su un campo di scalari $\mathbb{K}$ finito è un gruppo finito.

Entriamo adesso nel vivo delle rappresentazioni lineari di un gruppo finito.

## 4. La rappresentazione regolare.

Consideriamo un gruppo simmetrico $S_n$. Indichiamo con

$$I = (E^1, E^2, \ldots, E^n)$$

la matrice identità di $GL(n, \mathbb{K})$, dove le $E^j$ sono le colonne. Per ogni permutazione $\sigma \in S_n$, la matrice elementare (del "primo tipo") $E(\sigma)$ è definita da:

$$E(\sigma) = (E^{\sigma(1)}, E^{\sigma(2)}, \ldots, E^{\sigma(n)})$$

cioè è ottenuta permutando le colonne di $I$ in accordo con $\sigma$. La dimostrazione del seguente Lemma è lasciata per esercizio.

**Lemma 4.1.** $\theta_n : S_n \to GL(n, \mathbb{K})$ , $\theta_n(\sigma) := E(\sigma)$, *è una rappresentazione lineare fedele detta* la rappresentazione tautologica di $S_n$.

Si noti che in effetti $\theta_n$ è ortogonale, cioe' a valori in $O(n, \mathbb{K})$, e data l'inclusione $O(n, \mathbb{R}) \subset U(n)$, è unitaria quando $\mathbb{K} = \mathbb{C}$.

Sia $G$ un gruppo finito, $|G| = n$. Fissato un ordinamento $\tau$ degli elementi di $G$, usando il Lemma 3.1, possiamo definire la rappresentazione fedele $\theta_n \circ \tau^* : G \to O(n, \mathbb{K})$ che sarà detta una *rappresentazione regolare* di $G$. E' facile verificare che cambiando l'ordinamento $\tau$ si ottengono comunque rappresentazioni regolari tra loro coniugate. Dunque $R_G := [\theta_n \circ \tau^*]$ è una ben definita classe di coniugazione, detta *regolare*, che dipende solo da $G$. Nel caso di $G = S_n$, non si confondano la rappresentazione tautologica (che è a valori in $O(n, \mathbb{K})$) e quella regolare (che è a valori in $O(n!, \mathbb{K})$).

## 5. Unitarietà

In questa Sezione $\mathbb{K} = \mathbb{C}$, $\mathbb{R}$ e mostreremo risultati che valgono (essenzialmente con la stessa dimostrazione) in entrambi i casi.

Se $\Phi$ è un prodotto scalare su $\mathbb{R}^n$ definito positivo, o un prodotto Hermitiano definito positivo su $\mathbb{C}^n$, per non appesantire l'esposizione indicheremo con $\mathcal{U}(\Phi)$ sia il gruppo ortogonale $O(\Phi)$ sia il gruppo unitario $U(\Phi)$. Inoltre useremo solo il termine "unitario" anche nel caso reale.

Su ogni $\mathbb{R}^n$ fissiamo il prodotto scalare definito positivo standard $< X, Y >= X^t Y$, su $C^n$ quello Hermitiano standard $< X, Y >= X^t \overline{Y}$.

Sia $G$ un gruppo finito, $|G| = n$. Fissiamo una rappresentazione lineare $\rho : G \to GL(n, \mathbb{K})$. Per ogni $X, Y \in \mathbb{K}^n$, definiamo

$$\Phi_\rho(X, Y) := \sum_{g \in G} < \rho(g)X, \rho(g)Y > \ .$$

Abbiamo

**Lemma 5.1.** *$\Phi_\rho$ è un prodotto scalare (Hermitiano) definito positivo su $\mathbb{K}^n$, e per ogni $g \in G$, $\rho(g) \in \mathcal{U}(\Phi)$.*

*Dimostrazione.* Che si tratti di un prodotto scalare (Hermitiano) definito positivo è una verifica diretta. D'altra parte,

$$\Phi_\rho(\rho(g)X, \rho(g)Y) = \sum_{h\in G} < \rho(gh)X, \rho(gh)Y >=$$

$$\sum_{h\in G} < \rho(h)X, \rho(h)Y >= \Phi_\rho(X, Y)$$

perché le due sommatorie differiscono giusto per una permutazione degli addendi.

□

**Teorema 5.1.** *(1) Ogni rappresentazione $\rho : G \to GL(n, \mathbb{K})$ è coniugata ad una rappresentazione unitaria; in altre parole $[\rho]$ è unitaria.*

*(2) Una rappresentazione $\rho : G \to GL(n, \mathbb{K})$ è riducibile se e solo se esiste un sottospazio non banale $W$ di $\mathbb{K}^n$ che sia $\rho$-invariante.*

*Dimostrazione.* Ogni prodotto scalare (Hermitiano) definito positivo ammette basi unitarie. Nelle coordinate rispetto ad una qualsiasi tale base $\mathcal{B}$ per $\Phi_\rho$, ogni $\rho(g)$ è rappresentato da una $\rho'(g) \in \mathcal{U}(n, \mathbb{K})$. Infine $\rho$ e $\rho'$ sono coniugate per mezzo della matrice $P$ di cambiamento di base dalla base canonica di $\mathbb{K}^n$ a $\mathcal{B}$. Questo prova (1).

Abbiamo già osservato in generale nel Lemma 2.1 che la condizione di (2) è necessaria (ma non sufficiente). D'altra parte, grazie a (1) non è restrittivo assumere che $\rho$ sia unitaria. Ma in tal caso $\mathbb{K}^n = W \perp W^\perp$ e i due addendi sono entrambi $\rho$-invarianti, per cui la condizione (1), questa necessaria e sufficiente, nel Lemma 2.1 è verificata. Il Lemma è dimostrato.

□

## 6. Forte ortogonalità per le rappresentazioni unitarie.

In questa Sezione $\mathbb{K} = \mathbb{C}$. Solo alla fine discuteremo quali argomenti valgono anche per $\mathbb{K} = \mathbb{R}$ e quali no. Come prima $\mathbb{C}^n$ è munito del prodotto Hermitiano definito positivo standard $< \cdot, \cdot >$. Per ogni matrice $A$, $p \times p$, $A_{i,j}$ indicherà l'entrata di posto $(i, j)$ di $A$, per ogni $(i, j) \in \{1, \dots, p\}^2$.

**Teorema 6.1.** *Sia $G = \{g_1 = 1, g_2, \dots, g_n\}$, $|G| = n$, un gruppo finito e siano $\alpha : G \to U(p)$ e $\beta : G \to U(q)$ due rappresentazioni unitarie irriducibili non coniugate tra loro. Per ogni coppia di indici $(i, j) \in \{1, \dots, p\}^2$ definiamo il vettore $v(\alpha)_{i,j} := (\alpha(g_1)_{i,j}, \dots, \alpha(g_n)_{i,j})^t \in \mathbb{C}^n$. Analogamente, per ogni $(k, l) \in \{1, \dots, q\}^2$, definiamo il vettore $v(\beta)_{k,l} \in \mathbb{C}^n$. Allora:*

(1) *Per ogni $(i, j), (k, l)$ come sopra:*

$$< v(\alpha)_{i,j}, v(\beta)_{k,l} >= 0 \ .$$

(2) *Per ogni $(i, j), (I, J) \in \{1, \dots, p\}^2$ :*

$$< v(\alpha)_{i,j}, v(\alpha)_{I,J} >= \delta_{i,I}\delta_{j,J}\frac{n}{p}$$

*dove questo significa che i due vettori sono ortogonali se sono diversi, mentre hanno norma uguale a $\sqrt{\frac{n}{p}}$ se coincidono.*

Deriviviamo subito alcune conseguenze importanti.

**Corollario 6.1.** *Se $\omega_1, \ldots, \omega_k$ sono classi di coniugazione irriducibili distinte di rappresentazioni lineari del gruppo finito $G$, di dimensione $n_1, \ldots, n_k$ rispettivamente, allora $\sum_j n_j^2 \leq |G|$. In particolare le classi di coniugazione irriducibili distinte di rappresentazioni lineari di $G$ sono in numero finito.*

*Dimostrazione.* Possiamo supporre che ogni classe $\omega_j$ abbia un rappresentante unitario $\rho_j$. Applicando i due punti del Teorema precedente a questi rappresentanti, costruiamo $\sum_j n_j^2$ vettori in $\mathbb{C}^{|G|}$, non isotropi, due a due ortogonali rispetto al prodotto Hermitiano standard. Quindi sono linearmente indipendenti e il loro numero non può eccedere la dimensione.

□

*Dimostrazione del Teorema.* Dimostriamo il punto (1). Indichiamo con $X_{j,l}$ la matrice complessa $p \times q$ che ha entrata $x_{j,l} = 1$, mentre tutte le altre entrate sono nulle. Poniamo

$$C_{j,l} := \sum_{s=1}^{n} \alpha(g_s) X_{j,l} \beta(g_s)^{-1}.$$

Usando il fatto che le matrici che costituiscono le due rappresentazioni sono unitarie, si osserva che le uguaglianze prescritte dall'enunciato (1), per una coppia di indici $(j, l)$ fissata, possono essere riscritte nella forma

$$C_{j,l} = 0$$

per cui (1) è equivalente all'annullarsi di tutte le $C_{j,l}$ al variare della coppia $(j, l)$. Inoltre poiché le matrici $X_{j,l}$ formano una base (quella canonica) delle matrici $p \times q$, la precedente affermazione è equivalente ad affermare che

$$C_M := \sum_{s=1}^{n} \alpha(g_s) M \beta(g_s)^{-1} = 0$$

per ogni matrice $p \times q$ $M$. E' questo che dimostreremo. L'osservazione cruciale è la seguente:

*Per ogni matrice $M$, per ogni $g \in G$, $\alpha(g) C_M = C_M \beta(g)$.*

Infatti:

$$\alpha(g) C_M = \sum_{s=1}^{n} \alpha(g)\alpha(g_s) M \beta(g g_s)^{-1} \beta(g) = \sum_{s=1}^{n} \alpha(g g_s) X \beta(g g_s)^{-1} \beta(g) = C_M \beta(g)$$

poiché la penultima sommatoria e quella che definisce $C_M$ differiscono giusto per una permutazione degli addendi.

Dunque basta dimostrare che

*La matrice nulla $C = 0$ è l'unica matrice $C$ $p \times q$ tale che $\alpha(g) C = C \beta(g)$ per ogni $g \in G$.*

Supponiamo intanto che $p = q$. Allora $C$ non è invertibile, altrimenti le due rappresentazioni sarebbero tra loro coniugate per mezzo di $C$, contro l'ipotesi. Allora se $C \neq 0$, le sue colonne generano un sottospazio proprio $W$ di $\mathbb{C}^p$. La relazione $\alpha(g) C = C \beta(g)$ per ogni $g \in G$, implica che $W$ è $\alpha$–invariante, e questo (grazie al punto (2) del Teorema 5.1) comporta che $\alpha$ è riducibile contro l'ipotesi. Quindi necessariamente $C = 0$.

Se $p > q$, il rango di $C$ è $\leq q < p$, e lo stesso argomento di prima si applica.

Se $p < q$ allora

$$\alpha(g) C = C \beta(g) \Leftrightarrow \overline{C}^t \overline{\alpha(g)}^t = \overline{\beta(g)}^t \overline{C}^t$$

e anche $\overline{\alpha}^t$, $\overline{\beta}^t$ sono rappresentazioni unitarie. Se $C \neq 0$, l'argomento precedente dice che $\overline{\beta}^t$ è riducibile. E' facile concludere che in tal caso anche $\beta$ è riducibile, contro l'ipotesi. Il punto (1) del Teorema è completamente dimostrato.

Veniamo adesso al punto (2). Analogamente a quanto fatto prima, per ogni matrice $M$ $p \times p$, poniamo adesso $C_M = \sum_{g \in G} \alpha(g) M \alpha(g)^{-1}$, e verifichiamo che $\alpha(g) C_M = C_M \alpha(g)$, per ogni $g \in G$. Cioè $C_M$ commuta con tutte le matrici che costituiscono la rappresentazione $\alpha$. Vale:

**Lemma 6.2. (Lemma di Schur.)** *Se $\alpha$ è una rappresenatzione unitaria e irriducibile di dimensione $p$ del gruppo finito $G$, e $C$ è una matrice $p \times p$ che commuta con tutte le matrici che costituiscono $\alpha$, allora $C$ è un multiplo della matrice identità, $C = cI$, per qualche $c \in \mathbb{C}$.*

*Dimostrazione.* Supponiamo che $C$ non sia un multiplo dell'identità e sia $\lambda$ un autovalore di $C$. Per ipotesi l'autospazio $V_\lambda(C) \neq \mathbb{C}^p$. Poichè $C$ commuta con le matrici di $\alpha$, ne segue che $V_\lambda(C)$ è $\alpha$–invariante, dunque $\alpha$ sarebbe riducibile, contro l'ipotesi.

□

Applichiamo il Lemma a $C_{j,l}$ definita come prima usando $M = X_{j,l}$. Ne segue allora che

$$\sum_{s=1}^{|G|} \alpha(g_s)_{i,j} \overline{\alpha}(g_s)^t_{l,k} = c_{j,l} \delta_{i,k} \ .$$

Per determinare gli scalari $c_{j,l}$, poniamo $i = k$ e sommiamo rispetto a $i$. Otteniamo

$$p c_{j,l} = \sum_{s=1}^{|G|} \sum_{i=1}^{p} \alpha(g_s)(\alpha(g_s)^{-1})_{l,i} = \sum_{s=1}^{|G|} I_{l,j} \ .$$

Dunque, se $l = j$ rusulta $c_{j,j} = |G|/p$. Se $l \neq j$, allora $c_{j,l} = 0$. Il Teorema è così completamente dimostrato.

□

**Osservazioni 6.3.** La dimostrazione del punto (1) del Teorema funziona anche nel caso delle rappresentazioni reali ortogonali. Infatti abbiamo usato solo il Teorema 5.1 che vale anche nel caso reale. Invece la dimostrazione del Lemma di Schur, cruciale nella dimostrazione del punto (2), non si applica al caso reale, perchè la matrice $C$ può non avere autovalori reali.

## 7. Ortogonalità dei caratteri

In questa Sezione consideriamo rappresentazioni su $\mathbb{C}$. E' ben noto che due matrici quadrate $p \times p$ simili hanno la stessa traccia. Per esempio, si può verificare direttamente che

$$\mathrm{tr}(MN) = \mathrm{tr}(NM)$$

e ricavare l'invarianza della traccia come semplice conseguenza, oppure possiamo identificare la traccia come il coefficiente del monomio $t^{p-1}$ nel polimomio caratteristico.

Se $G = \{g_1, \ldots, g_n\}$ è come al solito un gruppo finito, $n = |G|$, e $\omega = [\rho]$ è la classe di coniugazione di una rappresentazione lineare (su $\mathbb{C}$) di $G$, di dimensione uguale a $p$, allora è ben definito il vettore

$$\chi_\omega := (\mathrm{tr}\ \omega(g_1), \ldots, \mathrm{tr}\ \omega(g_n))^t := (\mathrm{tr}\ \rho(g_1), \ldots, \mathrm{tr}\ \rho(g_n))^t \in \mathbb{C}^n$$

che non dipende dalla scelta del rappresentante $\rho$ di $\omega$. Questo vettore è detto *il carattere* di $\omega$. Al solito $\mathbb{C}^n$ è munito del prodotto Hermitiano definito positivo standard.

**Teorema 7.1. (Ortogonalità dei caratteri.)** *(1) Se $\omega$ e $\omega'$ sono due classi coniugate irriducibili distinte di rappresentazioni lineari di $G$, allora*

$$< \chi_\omega, \chi_{\omega'} >= 0 \ .$$

*(2) Se $\omega$ è una classe coniugata irriducibile di rappresentazioni lineari di $G$, allora*

$$< \chi_\omega, \chi_\omega >= |G| \ .$$

*Dimostrazione.* Prendiamo come rappresentante di ogni classe di coniugazione una rappresentazione unitaria, e applichiamo il Teorema 6.1.

Allora il punto (1) del presente Teorema segue dal punto (1) del Teorema 6.1. Basta considerare quella ortogonalità nel caso in cui $j = i$ e $l = k$, e sommare poi rispetto a $i$ e $k$.

In modo analogo si ottiene il punto (2) a partire dal corrispondente punto (2) di 6.1.

□

Il Teorema ha importanti conseguenze sulla struttura delle rappresentazioni lineari di $G$.

**Teorema 7.2.** *Due classi di coniugazione irriducibili $\omega$ e $\omega'$ di rappresentazioni lineari di $G$ sono uguali se e solo se hanno lo stesso carattere: $\chi_\omega = \chi_{\omega'}$.*

*Dimostrazione.* Basta dimostrare che se le due classi sono distinte, allora hanno caratteri diversi. Sappiamo che $< \chi_\omega, \chi_{\omega'} >= 0$; ma se fosse $\chi_\omega = \chi_{\omega'}$, si avrebbe anche $< \chi_\omega, \chi_{\omega'} >= |G| \neq 0$, e questo è impossibile.

□

Sia $\Omega = \{\omega_1, \ldots, \omega_k\}$ l'insieme (che sappiamo essere finito) di tutte le classi di coniugazione irriducibili di rappresentazioni lineari di $G$, due a due distinte. Vale il seguente Lemma

**Lemma 7.1.** *Ogni classe di coniugazione $\omega$ di rappresentazioni lineari del gruppo $G$ può essere scritta nella forma*

$$\omega = \oplus_{j=1}^{k} a_j \omega_j$$

*dove $a_j \in \mathbb{N}$, e $a_j\omega_j = \oplus_{i=1}^{a_j} \omega_j$ (cioè l'addendo $\omega_j$ è ripetuto $a_j$ volte). Ogni tale espressione di $\omega$ è detta una* decomposizione in irriducibili.

*Dimostrazione.* Per induzione sulla dimensione $p \geq 1$ di $\omega$. Se $\omega \in \Omega$, allora $\omega = \omega_j$ per qualche $j$. Altrimenti $\omega = \alpha \oplus \beta$ è riducibile e i due addendi hanno dimensione strettamente minore di $p$. Si conclude quindi per induzione (osservando anche che permutando gli addendi di una decomposizione data non si cambia la classe di coniugazione del risultato).

□

**Teorema 7.3. (Unicità della decomposizione in irriducibili.)** *Per ogni $\omega$ la decomposizione in irriducibili è unica, nel senso che i coefficienti $a_j$ sono univocamente determinati.*

*Dimostrazione.* Il effetti $a_j = \frac{<\chi_\omega, \chi_{\omega_j}>}{|G|}$.

□

Come Corollario possiamo ora estendere il Teorema 7.2 a classi non necessariamente irriducibili.

**Corollario 7.2.** *Due classi di coniugazione $\omega$ e $\omega'$ di rappresentazioni lineari di $G$ sono uguali se e solo se $\chi_\omega = \chi_{\omega'}$.*

*Dimostrazione.* Se hanno gli stessi caratteri, allora hanno la stessa decomposizione in irriducibili e quindi sono uguali.

□

## 8. Sul numero e le dimensioni delle classi di coniugazione irriducibili

Come prima consideriamo rappresentazioni su $\mathbb{C}$. Sia al solito $G$ un gruppo finito, $n = |G|$. Sappiamo che $G$ è ripartito nelle sue classi di coniugazione. Siano $C_1, \ldots, C_r$ queste classi due a due disgiunte, e supponiamo che $|C_j| = d_j$, per cui $\sum d_j = |G|$. Sia $\Omega = \{\omega_1, \ldots, \omega_k\}$ già definito nella sezione precedente e sia $p_j$ la dimensione di $\omega_j$. Lo scopo di questa Sezione è dimostrare il seguente Teorema che stabilisce relazioni conclusive tra diversi dati quantitativi in gioco.

**Teorema 8.1.** *Sia $\Omega = \{\omega_1, \ldots, \omega_k\}$ l'insieme delle classi di coniugazione irriducibili di rappresentazioni lineari del gruppo $G$, $|G| = n$. Supponiamo che $\omega_j$ sia di dimensione $p_j$ e che $G$ abbia $r$ classi di coniugazione. Allora*

$$\sum_{j=1}^{k} p_j^2 = |G|$$
$$k = r \ .$$

.

Dimostreremo preliminarmente il seguente Lemma che stabilisce intanto delle disuguaglianze.

**Lemma 8.1.** *Sia $\Omega = \{\omega_1, \ldots, \omega_k\}$ l'insieme delle classi di coniugazione irriducibili di rappresentazioni lineari del gruppo $G$, $|G| = n$. Supponiamo che $\omega_j$ sia di dimensione $p_j$ e che $G$ abbia $r$ classi di coniugazione. Allora*

$$\sum_{j=1}^{k} p_j^2 \leq |G|$$
$$k \leq r \ .$$

*Dimostrazione.* La prima disuguaglianza è gia stata dimostrata in Lemma 6.1. Consideriamo la seconda. Poiché per ogni classe di coniugazione di rappresentazioni $\omega$, $\mathrm{tr}(\omega(g)) = \mathrm{tr}(\omega(h))$ se $g$ e $h$ appartengono alla stessa classe $C_j$, possiamo definire il *carattere essenziale* di $\omega$ come il vettore

$$\hat{\chi}_\omega = (\sqrt{d_1}\mathrm{tr}\ \omega(C_1), \ldots, \sqrt{d_r}\mathrm{tr}\ \omega(C_r))^t \in \mathbb{C}^r$$

dove $\mathrm{tr}\ \omega(C_j) := \mathrm{tr}\ \omega(h)$, per qualsiasi $h \in C_j$. Le condizioni di ortogonalità del Teorema 7.1 possono essere allora riscritte nella forma

$$< \hat{\chi}_\omega, \hat{\chi}_{\omega'} >= 0, \ < \hat{\chi}_\omega, \hat{\chi}_\omega >= |G| \ .$$

Applicando questo risultato alle classi di $\Omega$, costruiamo $k = |\Omega|$ vettori non nulli di $\mathbb{C}^r$ due a due ortogonali, per cui $k \leq r$, come voluto.

□

8.1. **Decomposizione della rappresentazione regolare.** In questa sottosezione vogliamo dimostrare la prima uguaglianza del Teorema 8.1. Questo seguirà dall'analisi della decomposizione in irriducibili della classe di coniugazione delle rappresentazioni regolari. Questa classe $R = R_G$ è stata definita nella Sezione 4. Vogliamo dunque determinare i coefficienti della sua decomposizione:

$$R = \sum_{j=1}^{k} a_{R,j}\omega_j \ .$$

**Lemma 8.2.** *Per ogni $g \in G$, $\mathrm{tr}\ R(g) = |G|$ se $g = 1$, mentre $\mathrm{tr}\ R(g) = 0$, se $g \neq 1$.*

*Dimostrazione.* La permutazione di $G$ data da $h \to gh$ è tale che se $g \neq 1$ allora $gh \neq h$ per ogni $h \in G$. Questo implica che, se $g \neq 1$, per qualsiasi rappresentante $\rho$ di $R$, la permutazione delle colonne della matrice identità $I$ che produce la matrice elementare $\rho(g)$, non lascia ferma alcuna colonna di $I$. Ne segue che tutti gli elementi sulla diagonale di $\rho(g)$ sono nulli e a maggior ragione è nulla la sua traccia.

□

**Proposizione 8.3.** *Per ogni $j = 1, \ldots, k$, si ha*

$$a_{R,j} = p_j \ .$$

*Inoltre, per ogni $g \in G$, si ha*

$$\sum_{j=1}^{k} \text{tr } \omega_j(1)\text{tr}\omega_j(g) = \sum_{j=1}^{k} p_j \text{tr } \omega_j(g)$$

*vale $|G|$ se $g = 1$, mentre vale 0 altrimenti.*

*Dimostrazione.* Applicando il Lemma precedente abbiamo che tr $R(g) = \sum_{j=1}^{k} a_{R,j}\text{tr } \omega_j(g) = |G|$ se $g = 1$, oppure è uguale a 0 se $g \neq 1$. D'altra parte sappiamo che $a_{R,j} = \frac{<\chi_R, \chi_{\omega_j}>}{|G|} = \frac{|G|p_j}{|G|}$.

□

**Corollario 8.4.** $\sum_{j=1}^{k} p_j^2 = |G|$

*Dimostrazione.* Segue dalla Proposizione precedente che $|G| = \sum_j a_{R,j}p_j = \sum_j p_j^2$, come voluto.

□

8.2. **"k=r".** Resta da dimostrare la seconda uguaglianza del Teorema 8.1, cioè l'altra disuguaglianza $k \geq r$. Questa sarà una conseguenza immediata della seguente Proposizione.

**Proposizione 8.5.** *Gli $r$ vettori in $\mathbb{C}^k$ definiti come $u(C_j) := (\text{tr } \omega_1(C_j), \ldots, \text{tr } \omega_k(C_j))^t$ , $j = 1, \ldots, r$, sono linearmente indipendenti.*

La dimostrazione della Proposizione risulterà combinando una serie di Lemma che andiamo a sviluppare.

Per ogni classe di coniugazione $C_j$ di $G$ e per ogni rappresentazione lineare irriducibile $\rho$ di $G$ di dimensione $p$, definiamo la matrice $p \times p$:

$$A(C_j) = \sum_{g \in C_j} \rho(g) \ .$$

**Lemma 8.6.** *Per ogni $h \in G$, per ogni classe di coniugazione $C_j$ di $G$, per ogni $\rho$ rappresentazione lineare irriducibile di $G$, le matrici $A(C_j)$ e $\rho(h)$ commutano. Quindi $A(C_j) = b_j I$, per qualche scalare $b_j \in \mathbb{C}$.*

*Dimostrazione.* L'ultima affermazione è un'altra applicazione del Lemma di Schur. D'altra parte osserviamo che

$$\rho(h)A(C_j)\rho(h)^{-1} = \sum_{g \in C_j} \rho(hgh^{-1}) = A(C_j)$$

perchè la penultima sommatoria differisce da quella che definisce $A(C_j)$ giusto per una permutazione degli addendi.

□

Per ogni coppia di classi di coniugazione di $G$, definiamo l' "insieme dei prodotti" come:

$$C_jC_i = \{gh;\ g \in C_j,\ h \in C_i\ \}$$

dove conveniamo che se $(g,h) \neq (g',h')$, anche se $gh = g'h'$ in $G$, $gh$ e $g'h'$ sono considerati come elementi distinti di $C_jC_i$.

**Lemma 8.7.** *(1) Ogni insieme di prodotti $C_jC_i$ è unione di classi di coniugazione di $G$ ed ogni classe $C_s$ si ripete un ben determinato numero di volte $a_{j,i,s} \in \mathbb{N}$ in $C_jC_i$.*

*(2) Per ogni $(j,i)$ vale l'uguaglianza*

$$b_jb_i = \sum_s a_{j,i,s}b_s\ .$$

*Dimostrazione.* Dato $gh \in C_jC_i$, per ogni $f \in G$, si ha $fghf^{-1} = (fgf^{-1})(fhf^{-1}) \in C_jC_i$. Questo dimostra la prima affermazione. Per quanto riguarda la seconda, applicando il Lemma 8.6, si ha

$$b_jb_jI = \sum_{g\in C_j,\ h\in C_i} \rho(gh) = \sum_s a_{j,i,s}A(C_s) = (\sum_s a_{j,i,s}b_s)I$$

da cui la tesi.

□

Osserviamo che $\mathrm{tr}A(C_j) = d_j\mathrm{tr}\rho(C_j)$, dove $\mathrm{tr}\rho(C_j) := \mathrm{tr}\rho(g)$ e $g$ è un arbitrario elemento di $C_j$. D'altra parte segue dal Lemma 8.6 che $\mathrm{tr}A(C_j) = pb_j$. Combinando queste osservazioni con il Lemma 8.7 deduciamo il seguente Corollario.

**Corollario 8.8.**

$$d_jd_i\mathrm{tr}\ \rho(C_j)\mathrm{tr}\ \rho(C_i) = p\sum_s a_{j,i,s}\mathrm{tr}\ \rho(C_s)d_s\ .$$

□

Indichiamo con $C_1 = \{1_G\}$ la classe di coniugazione di $1_G$, per cui $\mathrm{tr}\rho(C_1) = p$. Quindi possiamo formalmente sostituire if fattore $p$ davanti alla sommatoria nel precedente corollario con $\mathrm{tr}\rho(C_1)$. Calcoliamo adesso la costante $a_{j,i,1}$. Osserviamo che per ogni $C_j$ l'insieme di tutti gli inversi degli elementi di $C_j$ costituiscono un'altra classe di coniugazione di $G$, indicata con $C_{j'}$. Allora il seguente Lemma è di facile verifica.

**Lemma 8.9.** *$a_{j,i,1} = 0$ se $i \neq j'$. $a_{j,i,1} = d_j$ se $i = j'$.*

Applichiamo adesso i risultati così ottenuti ad ogni $\omega_t \in \Omega$ e sommiamo su $t = 1,\dots k$. Si ottiene

$$d_jd_i\sum_t \mathrm{tr}\ \omega_t(C_j)\mathrm{tr}\ \omega_t(C_j) = \sum_s a_{j,i,s}\sum_t \mathrm{tr}\ \omega_t(C_1)\mathrm{tr}\ \omega_t(C_s)d_s\ .$$

Applicando la Proposizione 8.3 vediamo che l'addendo dell'ultima sommatoria vale $|G|$ se $C_s = C_1$, vale 0 altrinenti e che

$$\sum_t \mathrm{tr}\ \omega_t(C_j)\mathrm{tr}\ \omega_t(C_j) = \frac{a_{j,i,1}|G|}{d_jd_i}$$

vale 0 se $i \neq j'$, mentre vale $\frac{|G|}{d_j}$ se $i = j'$. Veniamo infine alla dimostrazione della Proposizione 8.5. Sia $V(x) := \sum_{j=1}^r x_1u(C_j) = 0$, $x = (x_1,\dots,x_r)$, una combinazione lineare di quegli $r$

vettori di $\mathbb{C}^k$ che rappresenti il vettore nullo. Allora, usando i risultati precedenti vediamo che, per ogni $s = 1 \dots k$,

$$< V(x), \overline{u(C_s)} >= \sum_j x_j (\sum_t \text{tr } \omega_t(C_j)^t \text{tr } \omega_t(C_s)) = x_s \frac{|G|}{d_s}$$

da cui $x_s = 0$ per ogni $s$, e la indipendenza lineare è dimostrata. Quindi la Proposizione 8.5 e la seconda uguaglianza del Teorema 8.1 sono così completamente dimostrate.

□

Il Teorema 8.1 è così completamente dimostrato.

Concludiamo proponendo al lettore alcuni esercizi o spunti di riflessione (in ordine sparso e di difficoltà non uniforme).

**Esercizi e spunti.**

(1) Dimostrare che il gruppo finito $G$ è abeliano se e solo se tutte le rappresentazioni irriducibili di $G$ su $\mathbb{C}$ hanno dimensione uguale a 1. L'affermazione resta vera su $\mathbb{R}$?

(2) Per ogni intero $n \geq 1$ una *partizione* di $n$ è una espressione di $n$ in somma di interi della forma $n = \sum_{j=1}^{h} m_j$ tale che $1 \leq m_i \leq m_{i+1}$. Indichiamo con $\mathcal{P}(n)$ il numero delle partizioni distinte di $n$. Dimostrare che esistono interi $p_j \geq 1$, $j = 1, \dots, \mathcal{P}(n)$, tali che $n! = \sum p_j^2$.

(3) (a) Al variare di due interi positivi $m, n \geq 1$, determinare gli elementi distinti e la tavola di moltiplicazione del gruppo Abeliano finito $G_{m,n}$ caratterizzato dalle seguenti proprietà:

*Esistono in $G$ due elementi distinti $g_1$ e $g_2$ di ordine $m$ e $n$ rispettivamente, tali che ogni elemento $g \in G$ è della forma $g = g_1^i g_2^k$, per opportuni interi positivi $i$ e $k$.*

(b) Determinare tutte le classi di coniugazione di rappresentazioni irriducibili di $G$ su $\mathbb{C}$, esibendo un rappresentante per ogni classe.

(4) (a) Al variare dell'intero positivo $n \geq 1$, determinare gli elementi distinti e la tavola di moltiplicazione del gruppo finito $G_n$ caratterizzato dalle seguenti proprietà:

*Esistono in $G_n$ due elementi distinti $g_1$ e $g_2$ di ordine 2 e $n$ rispettivamente, tali che $g_1 g_2 g_1^{-1} = g_2^{-1}$ ed ogni elemento $g \in G_n$ è della forma $g = h_1 \dots h_s$, per qualche intero positivo $s$, dove ogni $h_i = g_1^{s(i)}$ oppure $h_i = g_2^{s(i)}$.*

(b) Determinare tutte le classi di coniugazione di rappresentazioni irriducibili di $G_n$ su $\mathbb{C}$, esibendo un rappresentante per ogni classe.

(c) Trovare un sottoinsieme $Y$ di $\mathbb{R}^3$ per cui $G_n$ sia isomorfo a $\mathcal{I}(\mathbb{R}^3, d)(Y)$.

(5) Sia $\Delta$ un tetraedro regolare in $\mathbb{R}^3$. Determinare tutte le classi di coniugazione di rappresentazioni irriducibili di $G = \mathcal{I}(\mathbb{R}^3, d)(\Delta)$ su $\mathbb{C}$, esibendo un rappresentante per ogni classe.

(6) **(Sulle rappresentazioni reali).** Un ingrediente essenziale della discussione fatta su $\mathbb{C}$ è il Lemma di Schur che non vale su $\mathbb{R}$. D'altra parte, la "unitarietà" che è un altro ingrediente fondamentale vale anche su $\mathbb{R}$. Ci possiamo allora chiedere quale possa essere la "migliore" versione reale della teoria delle rappresentazioni lineari dei gruppi finiti. Il lettore può provare a riflettere su questo problema, anche tenendo presente per esempio lo spirito della discussione sugli operatori normali reali presentata nelle relative note che si trovano in http://www.dm.unipi.it/ benedett, nel settore "Didattica".