Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Triennale in Matematica

UNA INTRODUZIONE ALLA TEORIA DELLE RAPPRESENTAZIONI DEI GRUPPI FINITI

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa NICOLETTA CANTARINI

Presentata da:
STEFANO LORINI

Sessione III

Anno Accademico 2013/2014

Indice

1 Rappresentazioni di gruppi finiti **3**

1.1 Definizioni e primi esempi . . . 3

1.2 La completa riducibilità . . . 6

1.3 Il lemma di Schur . . . 12

2 Teoria del carattere **14**

2.1 Definizione e prime proprietà . . . 14

2.2 Risultati fondamentali . . . 17

2.3 Carattere della rappresentazione regolare . . . 22

2.4 Il numero di rappresentazioni irriducibili . . . 23

3 L'algebra di gruppo $\mathbb{C}[G]$ **26**

3.1 Rappresentazioni di $\mathbb{C}[G]$ . . . 26

3.2 Il centro di $\mathbb{C}[G]$ . . . 30

3.3 Dimensione di rappresentazioni irriducibili . . . 32

4 Esempi **36**

4.1 Il numero di classi di coniugio di S_n . . . 36

4.2 Rappresentazioni irriducibili di S_3 . . . 39

4.3 Rappresentazioni irriducibili di S_4 . . . 43

Bibliografia **49**

Introduzione

Questa tesi è dedicata allo studio degli elementi di base e di alcuni risultati fondamentali della teoria delle rappresentazioni dei gruppi finiti. Come sempre nella teoria delle rappresentazioni, l'idea è quella di leggere, attraverso omomorfismi, ogni gruppo finito come un gruppo di matrici, in modo da confrontare un oggetto astratto con un oggetto in qualche modo più concreto, e da utilizzare gli strumenti dell'algebra lineare per poter capire e studiare le proprietà del gruppo stesso.

Per semplicità si è scelto di lavorare sul campo complesso. Laddove lo si è ritenuto particolarmente interessante, ma non troppo complicato, sono state osservate analogie o differenze con casi diversi da questo.

La tesi è suddivisa in quattro capitoli. Il primo capitolo, oltre alle definizioni e ad alcuni esempi di base, è prevalentemente dedicato al Teorema di Maschke, di cui vengono fornite due dimostrazioni: una valida sul campo complesso e l'altra in maggiore generalità. Si tratta di un teorema particolarmente importante che stabilisce la completa riducibilità delle rappresentazioni finito-dimensionali di un gruppo finito, purché la caratteristica del campo non divida l'ordine del gruppo.

Nel secondo capitolo vengono introdotti e studiati i caratteri delle rappresentazioni. L'idea è che il carattere di una rappresentazione contiene tutte le informazioni essenziali sulla rappresentazione stessa. Più precisamente una rappresentazione complessa di un gruppo finito è completamente determinata, a meno di isomorfismi, dal suo carattere. La situazione nel caso di rappresentazioni su campi di caratteristica positiva è più complicata e non viene affrontata nella tesi.

Nel terzo capitolo viene introdotta l'algebra gruppale $\mathbb{C}[G]$. L'algebra gruppale è un'algebra associativa con unità, avente una base indicizzata dagli elementi del gruppo. Ogni rappresentazione di G individua univocamente una rappresentazione di $\mathbb{C}[G]$ e viceversa, quindi studiare le rappresentazioni del gruppo G equivale a studiare le rappresentazioni dell'algebra associativa $\mathbb{C}[G]$. Questa equivalenza si dimostra talvolta particolarmente utile perché consente di utilizzare i metodi ed i risultati della teoria delle rappresentazioni delle algebre associative. In particolare nel capitolo tre questo punto di vista viene adottato per dimostrare che la dimensione di ogni rappresentazione irriducibile di un gruppo G divide l'ordine di G.

Infine, nell'ultimo capitolo della tesi, i risultati descritti nei primi tre capitoli vengono illustrati nel caso dei gruppi simmetrici S_3 ed S_4.

Capitolo 1

Rappresentazioni di gruppi finiti

1.1 Definizioni e primi esempi

La teoria delle rappresentazioni lineari dei gruppi serve a conoscere delle proprietà che ha un determinato gruppo. Qui considereremo gruppi finiti, cioè che abbiano un numero finito di elementi. In più, per evitare ambiguità, supporremo che le rappresentazioni siano lineari. Ogni volta, quindi, che scriveremo *gruppo* o *rappresentazione* omettendo rispettivamente *finito* e *lineare*, questi ultimi saranno sottointesi.
L'idea alla base di questa teoria è interpretare il gruppo come gruppo di trasformazioni di uno spazio vettoriale, considerato qui di seguito sempre non nullo e di dimensione finita.
Cominciamo introducendo il concetto di *azione* di un gruppo su un insieme.

Definizione 1.1.1 *Siano G un gruppo e X un insieme. Si dice che G agisce su X se esiste un'applicazione*

$$\begin{aligned} \theta\ :\quad G \times X &\longrightarrow X \\ (g,x) &\longmapsto gx \end{aligned}$$

tale che, indicando con $\cdot$ l'operazione del gruppo e con 1_G la sua unità, per ogni $g, h \in G$ e per ogni $x \in X$ valgano le seguenti proprietà:

1) $1_G\, x = x\,;$
2) $(g \cdot h)x = g(hx)\,.$

Definiamo adesso l'oggetto di studio vero e proprio:

Definizione 1.1.2 *Sia G un gruppo e sia V uno spazio vettoriale. Una rappresentazione lineare di G su V è un omomorfismo di gruppi $\rho : G \longrightarrow GL(V)$, cioè un'applicazione tale che, per ogni $g, h \in G$:*

1) $\rho(1_G) = id_V$;
2) $\rho(g \cdot h) = \rho(g) \circ \rho(h)$.

Indicheremo una siffatta rappresentazione con (ρ, V) quando il gruppo G risulterà chiaro dal contesto. Con un abuso di notazione, a volte indicheremo la rappresentazione semplicemente con V.
Denoteremo l'immagine di un elemento g di G tramite ρ con ρ_g.
Se il campo su cui è definito lo spazio vettoriale V è $\mathbb{R}$ o $\mathbb{C}$, la rappresentazione si dice rispettivamente reale o complessa. Nel seguito tratteremo soltanto rappresentazioni complesse, a meno che diversamente specificato.

Definizione 1.1.3 *Si chiama dimensione della rappresentazione la dimensione dello spazio vettoriale V.*

Se V è uno spazio vettoriale di dimensione n, ricordiamo che l'applicazione

$$\begin{aligned} T \ : \quad GL(V) &\longrightarrow GL_n(\mathbb{C}) \\ f &\longmapsto F \end{aligned}$$

che associa ad ogni automorfismo di V la sua matrice rispetto ad una base fissata di V, è un isomorfismo di gruppi.

Osservazione 1.1.1 *Dato uno spazio vettoriale complesso V e fissata una sua base B, si può equivalentemente definire una rappresentazione di un gruppo G su V come un omomorfismo di gruppi*

$$\begin{aligned} \rho \ : \quad G &\longrightarrow GL_n(\mathbb{C}) \\ g &\longmapsto F_g \end{aligned}$$

dove F_g è la matrice di ρ_g rispetto a B.

Definizione 1.1.4 *Un omomorfismo di due rappresentazioni (ρ, V) e (ρ', V') di un gruppo G è una funzione lineare $f : V \longrightarrow V'$ tale che per ogni $g \in G$ si abbia*

$$f \circ \rho_g = \rho'_g \circ f \, .$$

Se inoltre f è invertibile diremo che f è un isomorfismo e scriveremo $\rho \cong_G \rho'$.

Definizione 1.1.5 *Sia G un gruppo, sia V uno spazio vettoriale e sia $\rho : G \longrightarrow GL(V)$ una rappresentazione di G su V. Sia inoltre W un sottospazio vettoriale di V. W è detto sottorappresentazione di V se si ha $\rho_g(w) \in W$ per ogni $w \in W$ e per ogni $g \in G$. In questo caso il sottospazio W si dice G-invariante.*

Osservazione 1.1.2 *Se f è un omomorfismo di due rappresentazioni (ρ, V) e (ρ', V') di un gruppo G, allora $Ker(f)$ e $Im(f)$ sono sottospazi G-invarianti rispettivamente di V e V'.*

Infatti, presi $v \in Ker(f)$ e $g \in G$, si ha

$$f(\rho_g(v)) = \rho'_g(f(v)) = \rho'_g(0) = 0 \quad \Rightarrow \quad \rho_g(v) \in Ker(f).$$

Analogamente, se $v' \in Im(f)$, $g \in G$ e $v \in V$, abbiamo

$$\rho'_g(v') = \rho'_g(f(v)) = f(\rho_g(v)) \quad \Rightarrow \quad \rho'_g(v') \in Im(f).$$

Esempio 1.1.1 *Siano G un gruppo e V uno spazio vettoriale. Il più semplice esempio di rappresentazione (ρ, V) è quella tale che*

$$\rho_g(v) = v \qquad \forall\, g \in G, \quad \forall\, v \in V.$$

Questa rappresentazione è detta rappresentazione banale.

Esempio 1.1.2 *Sia G un gruppo finito di ordine n e sia V uno spazio vettoriale di dimensione n, con una base $\{e_g\}_{g \in G}$ indicizzata dagli elementi di G. Consideriamo $g \in G$ e definiamo la seguente applicazione:*

$$\begin{aligned} R_g \ : \quad & V \longrightarrow V \\ & e_h \longmapsto e_{g \cdot h} \end{aligned}$$

(estesa per linearità su tutto lo spazio V). Questa è una rappresentazione di G su V, detta rappresentazione regolare.

Infatti, per ogni $g \in G$, R_g è un automorfismo di V. Questo perché l'applicazione $\hat{g} : g \longmapsto g \cdot h$, definita su un gruppo, è biiettiva. Inoltre vale $R_{h \cdot l}(v) = (R_h \circ R_l)(v)$ per ogni $h, l \in G$ e per ogni $v \in V$. Basta vederlo su un elemento della base di V:

$$R_{g\cdot h}(e_l) = e_{(g\cdot h)\cdot l} = e_{g\cdot(h\cdot l)} = R_g(e_{h\cdot l}) = (R_g \circ R_h)(e_l).$$

La dimensione di questa rappresentazione, per costruzione, è uguale all'ordine di G.
Notiamo che, posto $w = \sum_{g\in G} e_g$, si ha, per ogni $h \in G$:

$$hw = h\sum_{g\in G} e_g = \sum_{g\in G} he_g = \sum_{g\in G} e_{h\cdot g} = w.$$

Quindi $W := Span\{w\}$ è una sottorappresentazione di V.

Esempio 1.1.3 *Siano G un gruppo e X un insieme finito. Supponiamo che G agisca su X.*
Similmente a quanto visto nell'esempio precedente, sia V uno spazio vettoriale con una base $\{e_x\}_{x\in X}$ indicizzata dagli elementi di X, e sia ρ_g, per ogni $g \in G$, l'applicazione lineare

$$\begin{aligned} \rho_g \ : \quad & V \longrightarrow V \\ & e_x \longmapsto e_{gx} \,. \end{aligned}$$

La rappresentazione di G così ottenuta è chiamata rappresentazione di permutazione associata a X.

1.2 La completa riducibilità

Il nostro obiettivo è studiare le rappresentazioni di un gruppo finito G. Un passo fondamentale in questa direzione è la decomposizione di una rappresentazione in componenti irriducibili.

Definizione 1.2.1 *Una rappresentazione V si dice irriducibile se non contiene alcuna sottorappresentazione propria.*

Per sottorappresentazione *propria* intendiamo una sottorappresentazione diversa da $\{0\}$ e da V.
Una rappresentazione non irriducibile si dice *riducibile.*

Esempio 1.2.1 *Ogni rappresentazione di dimensione 1 è irriducibile. Infatti, per ragioni dimensionali, non esistono sottorappresentazioni proprie.*

Esempio 1.2.2 *Sia G un gruppo. Consideriamo la rappresentazione regolare di G. Allora, se $|G| > 1$, essa non è irriducibile, come abbiamo già notato nell'Esempio 1.1.2.*

Esempio 1.2.3 *Consideriamo il numero complesso i. Esso è una radice quarta dell'unità, ovvero $i^4 = 1$. L'insieme $\{1, i, i^2, i^3\} = \{1, i, -1, -i\}$ è un gruppo ciclico generato da i. Indichiamo con G questo gruppo e definiamo la seguente applicazione:*

$$\begin{aligned} \rho \ : \quad & G \longrightarrow GL_2(\mathbb{C}) \\ & g \longmapsto \rho_g := \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix} . \end{aligned}$$

Per ogni elemento del gruppo G, ρ_g risulta essere un automorfismo di $\mathbb{C}^2$. Si verifica facilmente che ρ è un omomorfismo di gruppi e quindi definisce una rappresentazione di G su $\mathbb{C}^2$:

$$\rho_{g \cdot h} = \begin{pmatrix} 1 & 0 \\ 0 & g \cdot h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & g \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & h \end{pmatrix} = \rho_g \circ \rho_h \qquad \forall\, g, h \in G.$$

Notiamo che tale rappresentazione non è irriducibile. Infatti è immediato vedere che

$$W := Span \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} \qquad e \qquad W' := Span \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

sono sottospazi di $\mathbb{C}^2$ (di dimensione 1) G-invarianti.

Definizione 1.2.2 *Sia G un gruppo e siano (ρ, V), (ρ', V') due rappresentazioni di G. Definiamo la seguente applicazione:*

$$\begin{aligned} \rho \oplus \rho' \ : \quad & G \longrightarrow GL(V \oplus V') \\ & g \longmapsto \rho_g \oplus \rho'_g . \end{aligned}$$

Questa è ancora una rappresentazione di G, si dice somma diretta delle rappresentazioni ρ e ρ' e si denota con $(\rho \oplus \rho', V \oplus V')$.

Più precisamente, fissato $g \in G$ e presi $v \in V$, $v' \in V'$, si ha:

$$\begin{aligned} \rho_g \oplus \rho'_g \ : \quad V \oplus V' &\longrightarrow V \oplus V' \\ (v, v') &\longmapsto (\rho_g(v), \rho'_g(v')) \end{aligned}$$

così $(\rho \oplus \rho', V \oplus V')$ è una rappresentazione di G poiché (ρ, V) e (ρ', V') lo sono.

Definizione 1.2.3 *Sia G un gruppo e siano (ρ, V), (ρ', V') due rappresentazioni di G. Definiamo la seguente applicazione:*

$$\begin{aligned} \rho \otimes \rho' \ : \quad G &\longrightarrow GL(V \otimes V') \\ g &\longmapsto \rho_g \otimes \rho'_g \end{aligned}$$

dove $V \otimes V'$ è il prodotto tensoriale fra V e V'.
Questa è ancora una rappresentazione di G, si dice prodotto tensoriale delle rappresentazioni ρ e ρ' e si denota con $(\rho \otimes \rho', V \otimes V')$.

Analogamente alla rappresentazione somma diretta, fissato $g \in G$ e presi $v \in V$, $v' \in V'$, si ha:

$$\begin{aligned} \rho_g \otimes \rho'_g \ : \quad V \otimes V' &\longrightarrow V \otimes V' \\ v \otimes v' &\longmapsto \rho_g(v) \otimes \rho'_g(v') \end{aligned}$$

così $(\rho \otimes \rho', V \otimes V')$ è una rappresentazione di G poiché lo sono (ρ, V) e (ρ', V').

Definizione 1.2.4 *Una rappresentazione V di un gruppo G si dice completamente riducibile se si può scrivere come somma diretta di rappresentazioni irriducibili.*

Notiamo che, in generale, la riducibilità di una rappresentazione non implica la completa riducibilità.

Esempio 1.2.4 *Consideriamo $G = \mathbb{C}$, $V = \mathbb{C}^2$ e la rappresentazione*

$$\begin{aligned} \rho \ : \quad \mathbb{C} &\longrightarrow GL(\mathbb{C}^2) \\ z &\longmapsto \rho_z := \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} . \end{aligned}$$

Innanzitutto osserviamo che

$$\rho_z \circ \rho_w = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ z+w & 1 \end{pmatrix} = \rho_{z+w} \qquad \forall\, z, w \in \mathbb{C}$$

quindi ρ è una rappresentazione di $\mathbb{C}$ come gruppo additivo. Si ha che

$$W := Span\left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

è un sottospazio di V G-invariante, ma non esiste un altro sottospazio proprio W' di V G-invariante tale che $V = W \oplus W'$.
Infatti, sia $(z_1, z_2) \in \mathbb{C}^2$ tale che (z_1, z_2) e $(0, 1)$ siano linearmente indipendenti (cioè $z_1 \neq 0$). Allora

$$\rho_z \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} z_1 \\ z\, z_1 + z_2 \end{pmatrix} \notin Span\left\{ \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\} \qquad \text{(a meno che } z = 0\text{)}.$$

Dimostriamo un primo, significativo risultato:

Teorema 1.2.1 ***(di Maschke)*** *Sia $\rho : G \longrightarrow GL(V)$ una rappresentazione di G su V e sia W una sua sottorappresentazione. Allora esiste una sottorappresentazione W' di V tale che $V = W \oplus W'$.*

Dimostrazione. Sia $\tilde{W}$ un arbitrario sottospazio complementare di W in V e sia $p : V \longrightarrow W$ la corrispondente proiezione di V su W. Definiamo la funzione lineare $p_0 : V \longrightarrow V$, detta la *media dei coniugati di p tramite gli elementi di G*:

$$p_0 := \frac{1}{|G|} \sum_{g \in G} \rho_g \circ p \circ \rho_g^{-1}$$

dove $|G|$ è l'ordine di G.
Poiché W è una sottorappresentazione di V, $\rho_g(w) \in W$ per ogni $w \in W$. Analogamente $\rho_{g^{-1}}(w) = \rho_g^{-1}(w) \in W$ per ogni $w \in W$; pertanto valgono le seguenti uguaglianze:

$$p \circ \rho_g^{-1}(w) = \rho_g^{-1}(w), \quad \rho_g \circ p \circ \rho_g^{-1}(w) = w, \quad p_0(w) = w \qquad \forall\, w \in W.$$

Di conseguenza l'immagine di p_0 è contenuta in W e $p_{0|W} = id_W$. Perciò $p_0 \circ p_0 = p_0$. Allora anche p_0 è una proiezione di V su W.
Notiamo ora che $\rho_h \circ p_0 = p_0 \circ \rho_h$ per ogni $h \in G$. Infatti:

$$\rho_h \circ p_0 \circ \rho_h^{-1} = \frac{1}{|G|} \sum_{g \in G} \rho_h \circ \rho_g \circ p \circ \rho_g^{-1} \circ \rho_h^{-1} = \frac{1}{|G|} \sum_{g \in G} \rho_{h \cdot g} \circ p \circ \rho_{h \cdot g}^{-1} = p_0.$$

La prima uguaglianza viene semplicemente dalla linearità di p e di ρ_g per ogni $g \in G$; nella seconda abbiamo usato $(\rho_h \circ \rho_g)^{-1} = \rho_g^{-1} \circ \rho_h^{-1}$; nell'ultima il fatto che l'applicazione $\hat{g} : g \longmapsto g \cdot h$, definita su un gruppo, è biiettiva, quindi di fatto nell'ultima sommatoria possiamo sostituire $h \cdot g$ con g.
Il fatto che p_0 sia una proiezione su W ci permette di decomporre V nella somma diretta di sottospazi $V = W \oplus W'$ dove $W' = Ker(p_0)$.
Preso $w' \in W'$, abbiamo $p_0 \circ \rho_h(w') = \rho_h \circ p_0(w') = 0$, cioè $\rho_h(w') \in W'$, quindi W' è una sottorappresentazione di V.

□

Osservazione 1.2.1 *Notiamo che nella dimostrazione del Teorema di Maschke appena fatta non abbiamo usato alcuna ipotesi sul campo se non che la sua caratteristica non divida l'ordine di G. Il risultato visto vale dunque in questa generalità. Nel caso in cui il campo sia $\mathbb{C}$ si può dare anche una dimostrazione più semplice, che fa uso di un prodotto scalare Hermitiano definito sullo spazio vettoriale V. In tal caso il sottospazio complementare di W, G-invariante, sarà semplicemente l'ortogonale di W.*

Osserviamo innanzitutto che, dato un $\mathbb{C}$-spazio vettoriale V, è sempre possibile definire su V il prodotto scalare Hermitiano in modo che valga

$$< gv, gw > = < v, w > \qquad \forall g \in G, \quad \forall v, w \in V.$$

Infatti, sia $< , >_0$ un qualsiasi prodotto scalare Hermitiano su V, e definiamo

$$< v, w > := \sum_{g \in G} < gv, gw >_0 .$$

Il prodotto $< , >$ è certamente un prodotto scalare Hermitiano. Inoltre, per ogni $h \in G$, vale

$$
\begin{aligned}
< hv, hw > &= \sum_{g \in G} < g(hv), g(hw) >_0 = \sum_{g \in G} < (g \cdot h)v, (g \cdot h)w >_0 = \\
&= \sum_{l \in G} < lv, lw >_0 = < v, w > .
\end{aligned}
$$

II Dimostrazione del Teorema di Maschke nel caso complesso.

Consideriamo il sottospazio vettoriale ortogonale a W:

$$
W^{\perp} = \{ v \in V \quad | \quad < v, w >= 0 \quad \forall\, w \in W \} .
$$

Si ha che $V = W \oplus W^{\perp}$. A questo punto dobbiamo solo far vedere che $W^{\perp}$ è una sottorappresentazione di V. Siano $g \in G$, $w' \in W^{\perp}$, $w \in W$. Si ha:

$$
< gw', w >=< gw', (g \cdot g^{-1})w >=< w', (g^{-1}w) >= 0
$$

dal momento che W è G-invariante e w' è ortogonale a tutti gli elementi di W.

$\square$

Corollario 1.2.1 *Ogni rappresentazione si può scrivere come somma diretta di rappresentazioni irriducibili.*

Dimostrazione. Sia G un gruppo e sia (ρ, V) una rappresentazione di G su V. Il teorema si dimostra per induzione sulla dimensione di V.
Se $dim(V) = 0$ il teorema è ovvio.
Supponiamo quindi $n = dim(V) \geq 1$.
Se V è irriducibile non c'è niente da dimostrare.
Altrimenti, sia W un sottospazio proprio di V G-invariante. Per il teorema precedente, V si può decomporre in una somma diretta $W \oplus W'$ di due sottospazi W e W' G-invarianti che hanno dimensione strettamente minore di quella di V. Allora, per ipotesi induttiva, W e W' sono somma diretta di rappresentazioni irriducibili, quindi anche V lo è.

$\square$

1.3 Il lemma di Schur

Nel paragrafo precedente abbiamo visto che ogni rappresentazione si può scomporre in una somma diretta di rappresentazioni irriducibili. Adesso vogliamo dimostrare che questa scomposizione è unica, a meno di isomorfismi.

Lemma 1.3.1 ***(di Schur)*** *Sia G un gruppo e siano $\rho : G \longrightarrow GL(V)$, $\rho' : G \longrightarrow GL(V')$ due rappresentazioni irriducibili di G. Sia $f : V \longrightarrow V'$ un omomorfismo delle rappresentazioni ρ e ρ'. Allora valgono le seguenti affermazioni:*

(1) ρ e ρ' sono isomorfe oppure $f = 0$.
(2) Se $V = V'$ e $\rho \cong_G \rho'$, allora f è un'omotetia (cioè $\exists\, \lambda \in \mathbb{C}$ tale che $f = \lambda\, id_V$).

Dimostrazione.

(1) Come abbiamo visto nell'Osservazione 1.1.2, $Ker(f)$ e $Im(f)$ sono G-invarianti. Ma V per ipotesi è irriducibile, quindi $Ker(f)$ è $\{0\}$ oppure V. Analogamente, essendo anche V' irriducibile, si ha che $Im(f)$ è $\{0\}$ oppure V'. Se f è non nulla allora $Ker(f) = \{0\}$ e $Im(f) = V'$, così f è un isomorfismo.

(2) Ricordiamo che abbiamo fissato fin dall'inizio $\mathbb{K} = \mathbb{C}$. Essendo $\mathbb{C}$ algebricamente chiuso, f ha almeno un autovalore $\lambda \in \mathbb{C}$ quindi l'applicazione $f - \lambda\, id_V$ ha nucleo non banale. D'altra parte questo nucleo è G-invariante e V è irriducibile, quindi $Ker(f - \lambda\, id_V) = V$, da cui $f - \lambda\, id_V = 0$.

□

Teorema 1.3.1 *Ogni rappresentazione (ρ, V) di un gruppo finito G può essere scritta come somma diretta*

$$V = V_1^{\oplus m_1} \oplus \ \ldots \ \oplus V_n^{\oplus m_n}$$

dove $m_1, \ldots, m_n \in \mathbb{N}$ e per ogni $i = 1, \ldots, n$, V_i è una sottorappresentazione irriducibile di V tale che $V_i \not\cong V_j$ per $i \neq j$. Questa decomposizione è unica a meno di isomorfismi.

Dimostrazione. Sappiamo già che una decomposizione del genere esiste, grazie al teorema di Maschke. Dobbiamo dimostrare l'unicità.
Sia W una sottorappresentazione irriducibile di V. Dobbiamo mostrare che $W \cong V_i$ per un certo i. Fissiamo i, con $1 \leq i \leq n$ e consideriamo la proiezione di V su V_i ristretta a W:

$$p_{i\,|\,W} \;:\quad W \longrightarrow V_i\,.$$

W e V_i sono entrambe sottorappresentazioni irriducibili di V, quindi per il lemma di Schur abbiamo due possibilità: $W \cong V_i$ oppure $p_{i\,|\,W} = 0$.
Nel primo caso abbiamo subito la tesi.
Nel secondo caso, considerando tutte le altre proiezioni di V su V_j per $j \neq i$ ristrette a W, ne esisterà sicuramente una (e solo una) tale che risulti $W \cong V_j$ per un qualche j, poiché le proiezioni non possono essere tutte nulle.

$\square$

Capitolo 2

Teoria del carattere

2.1 Definizione e prime proprietà

D'ora in avanti, per non appesantire troppo la notazione, ometteremo i simboli dell'operazione del gruppo e di composizione di funzioni.

Definizione 2.1.1 *Sia G un gruppo e sia (ρ, V) una rappresentazione di G. Si chiama carattere di (ρ, V), e si denota con χ_ρ, la funzione che ad ogni elemento g del gruppo G associa la traccia di ρ_g su V:*

$$\begin{aligned} \chi_\rho \ : \quad & G \longrightarrow \mathbb{C} \\ & g \longmapsto Tr(\rho_g)\,. \end{aligned}$$

Definizione 2.1.2 *Sia G un gruppo e sia $g \in G$. Si definisce classe di coniugio di G il seguente insieme:*

$$C_g := \{h\,g\,h^{-1} \quad | \quad h \in G\}\,.$$

Definizione 2.1.3 *Sia G un gruppo e sia $f : G \longrightarrow \mathbb{C}$. Si dice che f è una funzione di classe se si ha $f(g) = f(h\,g\,h^{-1})$ per ogni $g, h \in G$.*

Proposizione 2.1.1 *Sia G un gruppo e sia $f : G \longrightarrow \mathbb{C}$. Allora f è una funzione di classe se e solo se $f(g\,h) = f(h\,g)$ per ogni $g, h \in G$.*

Dimostrazione.
Sia f una funzione di classe. Mostriamo che vale $f(g\,h) = f(h\,g)$ per ogni $g, h \in G$.
Per ipotesi $f(g) = f(h\,g\,h^{-1})$ per ogni $g, h \in G$. Ponendo $g\,h = g'$ si ha $f(g\,h) = f(g') = f(h\,g'\,h^{-1}) = f(h\,g\,h\,h^{-1}) = f(h\,g\,(h\,h^{-1})) = f(h\,g)$.

Viceversa, sia f una funzione a valori complessi tale che $f(g\,h) = f(h\,g)$ per ogni $g, h \in G$ e mostriamo che f è una funzione di classe.
Ponendo $h = h'\,g^{-1}$, con $h' \in G$, si ha
$f(g\,h'\,g^{-1}) = f(g\,(h'\,g^{-1})) = f((h'\,g^{-1})\,g) = f(h'\,(g^{-1}\,g)) = f(h')$.

$\square$

Proposizione 2.1.2 *Sia G un gruppo. Valgono le seguenti affermazioni:*

(1) Il carattere è una funzione di classe.
(2) Se (ρ, V) è una rappresentazione di G, allora $\chi_\rho(1_G) = dim(V)$.
(3) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)} \quad \forall g \in G$.
(4) Se due rappresentazioni (ρ, V) e (ρ', V') di G sono isomorfe, allora $\chi_\rho = \chi_{\rho'}$.
(5) Se (ρ, V) e (ρ', V') sono rappresentazioni di G, allora $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$.
(6) Se (ρ, V) e (ρ', V') sono rappresentazioni di G, allora $\chi_{\rho\otimes\rho'} = \chi_\rho\,\chi_{\rho'}$.

Dimostrazione.

(1) Per ogni $g, h \in G$ si ha

$$\chi_\rho(h\,g\,h^{-1}) = Tr(\rho_{h\,g\,h^{-1}}) = Tr(\rho_h\,\rho_g\,\rho_{h^{-1}}) = Tr(\rho_h\,\rho_g\,\rho_h^{-1}) = Tr(\rho_g) = \chi_\rho(g).$$

(2) $\qquad \chi_\rho(1_G) = Tr(\rho_{1_G}) = Tr(id_V) = dim(V).$

(3) Abbiamo $\chi_\rho(g^{-1}) = Tr(\rho_{g^{-1}}) = Tr(\rho_g^{-1})$ per ogni $g \in G$. Sappiamo che la traccia di ρ_g è la somma degli autovalori di ρ_g e ricordiamo che gli autovalori di ρ_g^{-1} sono gli inversi degli autovalori di ρ_g, per ogni $g \in G$.
Osserviamo che, essendo G un gruppo finito, esisterà $m \in \mathbb{N}$ tale che $g^m = 1_G$, con $g \in G$. Ciò implica $\rho_{g^m} = (\rho_g)^m = I$. Quindi, se λ_i è un autovalore di ρ_g, si ha $\lambda_i^m = 1$, cioè tutti gli autovalori di ρ_g sono radici m-esime dell'unità. Pertanto $|\lambda_i|^2 = \lambda_i\,\overline{\lambda_i} = 1$. Supponendo che ρ_g abbia n autovalori e che λ_i abbia molteplicità n_i, per $i = 1, ..., n$, si ha dunque

$$\chi_\rho(g^{-1}) = Tr(\rho_g^{-1}) = \sum_{i=1}^{n} n_i\,\lambda_i^{-1} = \sum_{i=1}^{n} n_i\,\overline{\lambda_i} = Tr(\overline{\rho_g}) = \overline{Tr(\rho_g)} = \overline{\chi_\rho(g)}.$$

(4) Per ipotesi (ρ, V) e (ρ', V') sono isomorfe, quindi esiste $f \in Hom(V, V')$

invertibile tale che $\rho'_g = f\,\rho_g\,f^{-1}$. La tesi allora segue dalla definizione di carattere e dalle proprietà della traccia.

(5) Fissata una base C di $V \oplus V'$ data dall'unione di una base B di V e di una base B' di V', l'applicazione $\rho_g \oplus \rho'_g$, per ogni $g \in G$, è rappresentata, rispetto a C, da una matrice a blocchi

$$\begin{pmatrix} F_g & 0 \\ 0 & F'_g \end{pmatrix}$$

dove F_g è la matrice di ρ_g rispetto a B e F'_g è la matrice di ρ'_g rispetto a B'. Si ha dunque

$$\chi_{\rho\oplus\rho'}(g) = Tr(\rho_g + \rho'_g) = Tr(\rho_g) + Tr(\rho'_g) = \chi_\rho(g) + \chi_{\rho'}(g).$$

(6) Consideriamo un elemento $g \in G$. Supponiamo che ρ_g abbia come autovalori su V $\lambda_1, ..., \lambda_n$, con $n = dim(V)$ e che ρ'_g abbia come autovalori su V' $\mu_1, ..., \mu_m$, con $m = dim(V')$. Allora gli autovalori di $\rho_g \otimes \rho'_g$ su $V \otimes V'$ sono $\lambda_i\,\mu_j$, con $i = 1, ..., n$ e $j = 1, ..., m$. Quindi

$$\chi_{\rho\otimes\rho'}(g) = \sum_{i,j} \lambda_i\,\mu_j = (\sum_{i=1}^{n} \lambda_i)\,(\sum_{j=1}^{m} \mu_j) = \chi_\rho(g)\,\chi_{\rho'}(g) \qquad \forall\, g \in G.$$

□

Definizione 2.1.4 *Dato un gruppo G, poniamo*

$$\mathbb{C}_{class}(G) := \{f : G \longrightarrow \mathbb{C} \quad | \quad f \text{ è funzione di classe}\}.$$

In particolare, grazie alla Proposizione 2.1.2 (1), il carattere di una rappresentazione di G appartiene a $\mathbb{C}_{class}(G)$. Possiamo definire su $\mathbb{C}_{\text{class}}(G)$ una struttura di $\mathbb{C}$-spazio vettoriale come segue:

- SOMMA:

$$(f_1 + f_2)(g) := f_1(g) + f_2(g) \qquad \forall\, f_1, f_2 \in \mathbb{C}_{\text{class}}(G), \quad \forall\, g \in G.$$

- PRODOTTO PER UNO SCALARE:

$$(\lambda\, f)(g) := \lambda\, f(g) \qquad \forall\, \lambda \in \mathbb{C}, \quad \forall\, f \in \mathbb{C}_{\text{class}}(G), \quad \forall\, g \in G.$$

Inoltre possiamo definire, per ogni $\phi, \psi \in \mathbb{C}_{class}(G)$, i seguenti prodotti:

$$< \phi, \psi > := \frac{1}{|G|} \sum_{g \in G} \phi(g) \, \psi(g^{-1}) \qquad (\star)$$

$$(\phi, \psi) := \frac{1}{|G|} \sum_{g \in G} \phi(g) \, \overline{\psi(g)} \qquad (\star\star)$$

La prima è una forma bilineare simmetrica. Il secondo, invece, è un prodotto scalare Hermitiano.
Dato che il carattere è una funzione di classe, allora, se abbiamo due rappresentazioni (ρ, V) e (ρ', V'), possiamo scrivere

$$< \chi_\rho, \chi_{\rho'} > = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \, \chi_{\rho'}(g^{-1}) \, ;$$

$$(\chi_\rho, \chi_{\rho'}) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \, \overline{\chi_{\rho'}(g)} \, .$$

Osservazione 2.1.1 *Sia G un gruppo e sia $g \in G$. Siano inoltre ρ e ρ' due rappresentazioni di G. Allora vale $(\chi_\rho, \chi_{\rho'}) =< \chi_\rho, \chi_{\rho'} >$.*

Infatti, applicando la Proposizione 2.1.2 (3) alla rappresentazione ρ' si ha $\overline{\chi_{\rho'}(g)} = \chi_{\rho'}(g^{-1})$. Allora

$$(\chi_\rho, \chi_{\rho'}) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \, \overline{\chi_{\rho'}(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \, \chi_{\rho'}(g^{-1}) =< \chi_\rho, \chi_{\rho'} > .$$

2.2 Risultati fondamentali

La prossima proposizione è un corollario del lemma di Schur.

Proposizione 2.2.1 *Siano (ρ, V) e (ρ', V') due rappresentazioni irriducibili di un gruppo G e sia $\phi : V \longrightarrow V'$ un'applicazione lineare. Poniamo:*

$$\phi_0 := \frac{1}{|G|} \sum_{g \in G} (\rho'_g)^{-1} \, \phi \, \rho_g \, .$$

Allora:

(1) Se ρ e ρ' non sono isomorfe, $\phi_0 = 0$.
(2) Se $V = V'$ e $\rho \cong_G \rho'$ si ha $\phi_0 = \lambda \, id_V$, con $\lambda = \frac{Tr(\phi)}{dim(V)}$.

Dimostrazione. Risulta $\rho'_h\, \phi_0 = \phi_0\, \rho_h$, infatti:

$$(\rho'_h)^{-1}\, \phi_0\, \rho_h = \frac{1}{|G|} \sum_{g\in G} (\rho'_h)^{-1}\, (\rho'_g)^{-1}\, \phi\, \rho_g\, \rho_h = \frac{1}{|G|} \sum_{g\in G} (\rho'_{g\,h})^{-1}\, \phi\, \rho_{g\,h} = \phi_0 .$$

Così, dal lemma di Schur, si ottengono (1) e (2). Inoltre

$$dim(V)\, \lambda = Tr(\phi_0) = \frac{1}{|G|} \sum_{g\in G} Tr(\rho_g^{-1}\, \phi\, \rho_g) = \frac{1}{|G|} \sum_{g\in G} Tr(\phi) = Tr(\phi).$$

□

Questa proposizione può essere riformulata descrivendo le rappresentazioni ρ e ρ' in termini matriciali: siano $\rho_g = (a_{i_1,\, j_1}(g))$, $\rho'_g = (b_{i_2,\, j_2}(g))$ le matrici di ρ_g e ρ'_g rispetto ad una base B di V e ad una base B' di V'. Indichiamo con $(x_{i_2,\, i_1})$ la matrice di ϕ rispetto a B e B' e con $(x^0_{i_2,\, i_1})$ la matrice di ϕ_0. Allora, per definizione di ϕ_0, si ha:

$$x^0_{i_2,\, i_1} = \frac{1}{|G|} \sum_{g,\, j_1,\, j_2} b_{i_2,\, j_2}(g^{-1})\, x_{j_2,\, j_1}\, a_{j_1,\, i_1}(g) \qquad (\star\star\star)$$

Proposizione 2.2.2 *Nel caso (1), per i_1, j_1, i_2, j_2 arbitrari, si ha*

$$\frac{1}{|G|} \sum_{g\in G} b_{i_2,\, j_2}(g^{-1})\, a_{j_1,\, i_1}(g) = 0\, .$$

Dimostrazione. Infatti in (1) abbiamo $x^0_{i_2,\, i_1} = 0$, quindi, per l'espressione $(\star\star\star)$, si ha

$$\frac{1}{|G|} \sum_{g,\, j_1,\, j_2} b_{i_2,\, j_2}(g^{-1})\, x_{j_2,\, j_1}\, a_{j_1,\, i_1}(g) = 0.$$

Possiamo interpretare il primo membro come una funzione lineare nelle variabili $x_{j_2,\, j_1}$. Il coefficiente di $x_{j_2,\, j_1}$, per ogni j_2, j_1 fissati, è

$$\frac{1}{|G|} \sum_{g\in G} b_{i_2,\, j_2}(g^{-1})\, a_{j_1,\, i_1}(g).$$

Segue la tesi.

□

Proposizione 2.2.3 *Nel caso (2) si ha*

$$\frac{1}{|G|}\sum_{g\in G} b_{i_2,\,j_2}(g^{-1})\,a_{j_1,\,i_1}(g)=\frac{1}{dim(V)}\,\delta_{i_2,\,i_1}\,\delta_{j_2,\,j_1}$$

dove δ è la delta di Kronecker.

Dimostrazione. Infatti in (2) abbiamo $\phi_0=\lambda\, id_V$, cioè $x^0_{i_2,\,i_1}=\lambda\,\delta_{i_2,\,i_1}$. Possiamo scrivere $Tr(\phi)=\sum_{j_2,\,j_1}\delta_{j_2,\,j_1}\,x_{j_2,\,j_1}$. Inoltre sappiamo che $\lambda=\frac{Tr(\phi)}{dim(V)}$. Quindi $\lambda=\frac{1}{dim(V)}\sum_{j_2,\,j_1}\delta_{j_2,\,j_1}\,x_{j_2,\,j_1}$. Da qui otteniamo

$$\frac{1}{|G|}\sum_{g,\,j_1,\,j_2} b_{i_2,\,j_2}(g^{-1})\,x_{j_2,\,j_1}\,a_{j_1,\,i_1}(g)=\frac{1}{dim(V)}\sum_{j_2,\,j_1}\delta_{i_2,\,i_1}\delta_{j_2,\,j_1}\,x_{j_2,\,j_1}$$

e, uguagliando i coefficienti di $x_{j_2,\,j_1}$, si ha la tesi.

□

Osservazione 2.2.1 *Notiamo che il prodotto ($\star$) è definito per ogni coppia di funzioni ϕ e ψ da G in $\mathbb{C}$.*

D'altra parte, usando le notazioni precedenti, anche $a_{i,\,j}(g)$ e $b_{i,\,j}(g)$ sono applicazioni da G a $\mathbb{C}$ per ogni coppia (i,j) fissata.
Nelle notazioni precedenti, poniamo

$$< b_{i_2,\,j_2}, a_{j_1,\,i_1} >:=\frac{1}{|G|}\sum_{g\in G} b_{i_2,\,j_2}(g^{-1})\,a_{j_1,\,i_1}(g)\,.$$

In questo modo le ultime due proposizioni diventano rispettivamente

$$< b_{i_2,\,j_2}, a_{j_1,\,i_1} >=0 \qquad (\diamond)$$

$$< b_{i_2,\,j_2}, a_{j_1,\,i_1} >=\frac{1}{dim(V)}\,\delta_{i_2,\,i_1}\delta_{j_2,\,j_1} \qquad (\diamond\,\diamond)$$

A meno di un'opportuna scelta della base degli spazi vettoriali V e V', possiamo supporre che le matrici $(a_{i,\,j}(g))$, $(b_{i,\,j}(g))$, per $g\in G$, siano unitarie. Così si avrà rispettivamente $a_{i,\,j}(g^{-1})=\overline{a_{i,\,j}(g)}$, $b_{i,\,j}(g^{-1})=\overline{b_{i,\,j}(g)}$ e le proposizioni precedenti sono proprio le condizioni di ortogonalità per il prodotto ($\star\star$).

Adesso siamo in grado di dimostrare questo risultato:

Teorema 2.2.1 *I caratteri delle rappresentazioni irriducibili di un gruppo G sono fra loro ortonormali rispetto al prodotto scalare Hermitiano* $(\star\star)$.

Dimostrazione. Quello che vogliamo far vedere è che, date due rappresentazioni (ρ, V) e (ρ', V') di G di dimensione rispettivamente n e m, vale

$$(\chi_\rho, \chi_{\rho'}) = \begin{cases} 1 & \text{se } \rho \cong_G \rho'\,; \\ 0 & \text{altrimenti.} \end{cases}$$

Usiamo la notazione matriciale: si avrà $\rho_g = (a_{i_1, j_1}(g))$ e $\rho'_g = (b_{i_2, j_2}(g))$. Così

$\chi_\rho(g) = Tr(\rho_g) = \sum_{i_1=1}^n a_{i_1, i_1}(g)\,; \qquad \chi_{\rho'}(g) = Tr(\rho'_g) = \sum_{i_2=1}^m b_{i_2, i_2}(g)\,.$

Si ha

$$(\chi_\rho, \chi_{\rho'}) = \frac{1}{|G|} \sum_{g \in G} Tr(\rho_g)\, Tr(\rho'_{g^{-1}}) = \frac{1}{|G|} \sum_{g \in G} ((\sum_{i_1=1}^n a_{i_1, i_1}(g))\, (\sum_{i_2=1}^m b_{i_2, i_2}(g^{-1}))) =$$

$$= < \sum_{i_1=1}^n a_{i_1, i_1}, \sum_{i_2=1}^m b_{i_2, i_2} > = \sum_{i_1, i_2} < a_{i_1, i_1}, b_{i_2, i_2} > .$$

Se $\rho \ncong_G \rho'$, allora siamo nel caso della Proposizione 2.2.2 ed abbiamo la condizione $(\diamond)$. Così $\sum_{i_1, i_2} < a_{i_1, i_1}, b_{i_2, i_2} > = 0$, cioè $(\chi_\rho, \chi_{\rho'}) = 0$.

Se invece $\rho \cong_G \rho'$, allora $\chi_\rho = \chi_{\rho'}$ e dunque

$$(\chi_\rho, \chi_{\rho'}) = < \chi_\rho, \chi_\rho > = \sum_{i, j=1}^n < a_{i, i}, a_{j, j} > .$$

In questo caso vale anche $V \cong V'$ (e $n = m$). Ciò implica che possiamo applicare la Proposizione 2.2.3 e la condizione $(\diamond\diamond)$. Abbiamo $< a_{i, i}, a_{j, j} > = \frac{1}{n}\, \delta_{i, j}\, \delta_{i, j} = \frac{1}{n}\, \delta_{i, j}$. Allora

$$\sum_{i, j=1}^n < a_{i, i}, a_{j, j} > = \sum_{i, j=1}^n \frac{1}{n}\, \delta_{i, j} = \frac{1}{n} \sum_{i, j=1}^n \delta_{i, j} = \frac{n}{n} = 1 \quad \Rightarrow \quad (\chi_\rho, \chi_{\rho'}) = 1.$$

$\square$

In particolare il Teorema 2.2.1 mostra che, se χ è il carattere di una rappresentazione irriducibile di G, allora $(\chi, \chi) = 1$. In questo caso il carattere si dice irriducibile.

Teorema 2.2.2 *Sia V una rappresentazione del gruppo G e sia η il carattere di V. Sia $V = V_1 \oplus \ldots \oplus V_n$ la decomposizione di V in sottorappresentazioni irriducibili. Allora, se W è una rappresentazione irriducibile avente carattere χ, il numero dei V_i isomorfi a W è uguale al prodotto (η, χ).*

Dimostrazione. Sia χ_i il carattere di V_i, per ogni $i = 1, ..., n$. Per l'affermazione (5) della Proposizione (2.1.2) si ha $\eta = \chi_1 + \ldots + \chi_n$.
Allora $(\eta, \chi) = (\chi_1 + \ldots + \chi_n, \chi) = (\chi_1, \chi) + \ldots + (\chi_n, \chi)$. Per il teorema precedente:

$$(\chi_i, \chi) = \begin{cases} 1 & \text{se } V_i \cong W\,; \\ 0 & \text{altrimenti.} \end{cases}$$

Segue subito la tesi.

□

Il numero (η, χ) si chiama molteplicità di W in V.

Corollario 2.2.1 *Se due rappresentazioni (ρ, V) e (ρ', V') di un gruppo G hanno lo stesso carattere, allora sono isomorfe.*

Dimostrazione. Siano χ_ρ e $\chi_{\rho'}$ i caratteri rispettivamente di ρ e ρ'. Per ipotesi si ha $\chi_\rho = \chi_{\rho'}$.
Se W è una rappresentazione irriducibile di G con carattere χ, allora $(\chi_\rho, \chi) = (\chi_{\rho'}, \chi)$, quindi la molteplicità di W in V e in V' è la stessa. La tesi segue dal Teorema di Maschke e dalla unicità della decomposizione in irriducibili.

□

Possiamo riassumere l'affermazione (4) della Proposizione 2.1.2 ed il Corollario 2.2.1 nella seguente

Proposizione 2.2.4 *Condizione necessaria e sufficiente affinché due rappresentazioni di un gruppo G siano isomorfe è che abbiano lo stesso carattere.*

Grazie al Teorema 1.3.1 ed ai risultati visti finora possiamo dire che il carattere η di una rappresentazione V di un gruppo G è dato da $\eta = m_1\,\chi_1 + \ldots + m_n\,\chi_n$, dove χ_i è il carattere di V_i (rappresentazione irriducibile) per ogni $i = 1, \ldots, n$ e m_i è la molteplicità di V_i in V: $m_i = (\eta, \chi_i)$. Inoltre, per l'ortonormalità dei caratteri χ_i, $i = 1, ..., n$, vale la formula

$$(\eta, \eta) = \sum_{i=1}^{n} m_i^2 \,.$$

Si ha subito il seguente

Teorema 2.2.3 *Sia V una rappresentazione di un gruppo G e sia η il carattere di V. Allora (η, η) è un numero intero positivo. Inoltre, $(\eta, \eta) = 1$ se e solo se V è irriducibile.*

2.3 Carattere della rappresentazione regolare

Ricordiamo che se (R, V) è la rappresentazione regolare del gruppo G ed $\{e_g\}_{g\in G}$ è una base dello spazio vettoriale V indicizzata dagli elementi di G, si ha che $R_h(e_g) = e_{h\cdot g}$ per ogni $g, h \in G$ (vedi Esempio 1.1.2).
Fissiamo $h \in G$ e consideriamo R_h. Si nota che se $h \neq 1_G$, allora $h \cdot g \neq g$ per ogni $g \in G$, quindi $R_h(e_g) \neq e_g$ per ogni $g \in G$; di conseguenza la matrice che rappresenta R_h rispetto alla base $\{e_g\}_{g\in G}$ ha gli elementi sulla diagonale principale tutti nulli. Ciò implica $Tr(R_h) = 0$ per ogni $h \in G$, $h \neq 1_G$.
Invece, se $h = 1_G$, allora R_h è l'applicazione identità su V, quindi

$$Tr(R_h) = Tr(id_V) = |G|.$$

In conclusione, vale la seguente

Proposizione 2.3.1 *Se (R, V) è la rappresentazione regolare del gruppo G e $h \in G$, allora*

$$Tr(R_h) = \begin{cases} |G| & \textit{se } \; h = 1_G\,; \\ 0 & \textit{altrimenti.} \end{cases}$$

Corollario 2.3.1 *Se W è una rappresentazione irriducibile del gruppo G, allora la molteplicità di W nella rappresentazione regolare (R, V) di G è uguale alla dimensione di W.*

Dimostrazione. Se χ è il carattere di W e χ_R è il carattere della rappresentazione regolare (R, V), allora, per il Teorema 2.2.2, la molteplicità di W in V è (χ_R, χ). Quindi, usando la Proposizione 2.3.1, si ha

$$(\chi_R, \chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\, \chi_R(g^{-1}) = \frac{1}{|G|} |G|\, \chi(1G) = Tr(id_W) = dim(W).$$

$\square$

Corollario 2.3.2 *Se $V_1, \ldots, V_n$ sono le rappresentazioni irriducibili del gruppo G aventi rispettivamente dimensione $m_1, \ldots, m_n$, allora:*

(1) Le dimensioni m_i soddisfano la relazione: $\sum_{i=1}^{n} m_i^2 = |G|$.
(2) Per ogni $g \in G$, $g \neq 1G$, si ha $\sum_{i=1}^{n} m_i\, \chi_i(g) = 0$.

Dimostrazione. Per il Corollario 2.3.1, abbiamo
$\chi_R(g) = \sum_{i=1}^{n} m_i\, \chi_i(g)$ per ogni $g \in G$.
Prendendo $g = 1G$ si ottiene (1); prendendo $g \neq 1G$ si ottiene (2).

$\square$

2.4 Il numero di rappresentazioni irriducibili

Proposizione 2.4.1 *Sia G un gruppo, sia (ρ, V) una rappresentazione di G su V e sia f una funzione in $\mathbb{C}_{class}(G)$. Sia $\rho_f : V \longrightarrow V$ l'applicazione lineare così definita:*

$$\rho_f := \sum_{g \in G} f(g)\, \rho_g\, .$$

Se (ρ, V) è una rappresentazione irriducibile con carattere χ_ρ, allora
$\rho_f = \lambda\, id_V$, con $\lambda = \frac{|G|}{dim(V)}\, (f, \overline{\chi_\rho})$.

Dimostrazione. Mostriamo innanzitutto che $\rho_f\, \rho_h = \rho_h\, \rho_f$ per ogni $h \in G$. Si ha:

$$\rho_h^{-1}\, \rho_f\, \rho_h = \sum_{g \in G} f(g)\, \rho_h^{-1}\, \rho_g\, \rho_h = \sum_{g \in G} f(g)\, \rho_{h^{-1} g\, h}.$$

Ponendo $l = h^{-1}\, g\, h$ si ottiene

$$\rho_h^{-1}\, \rho_f\, \rho_h = \sum_{l \in G} f(h\, l\, h^{-1})\, \rho_l = \sum_{l \in G} f(l)\, \rho_l = \rho_f.$$

Allora, procedendo analogamente a quanto fatto nella dimostrazione della Proposizione 2.2.1, vale $\rho_f = \lambda\, id_V$. Ora

$Tr(\lambda\, id_V) = Tr(\lambda\, I) = dim(V)\, \lambda\,;\qquad Tr(\rho_f) = \sum_{g \in G} f(g)\, \chi_\rho(g) = |G|\, (f, \overline{\chi_\rho}).$

Dunque $dim(V)\, \lambda = |G|\, (f, \overline{\chi_\rho})$, da cui $\lambda = \frac{|G|}{dim(V)}\, (f, \overline{\chi_\rho})$.

□

Teorema 2.4.1 *I caratteri irriducibili $\chi_1, \ldots, \chi_n$ del gruppo G formano una base ortonormale di $\mathbb{C}_{class}(G)$.*

Dimostrazione. Per il Teorema 2.2.1 si ha che $\chi_1, ..., \chi_n$ formano un sistema ortonormale in $\mathbb{C}_{class}(G)$. Dobbiamo solo dimostrare che sono dei generatori di $\mathbb{C}_{class}(G)$.
A tal fine mostriamo che l'ortogonale rispetto al prodotto $(\ ,\ )$ del sottospazio generato dai caratteri χ_i, con $i = 1, ..., n$, è lo spazio nullo: da questo seguirà che $Span\{\chi_i\}_{i=1,\ldots,n} = \mathbb{C}_{class}(G)$. Quindi facciamo vedere che se $f \in \mathbb{C}_{class}(G)$ è tale che $(f, \overline{\chi_i}) = 0$ per ogni $i = 1, ..., n$, allora $f = 0$.
Sia dunque f una siffatta funzione in $\mathbb{C}_{class}(G)$ e sia (ρ, V) una rappresentazione di G su V. Poniamo $\rho_f := \sum_{g \in G} f(g)\, \rho_g$.
La rappresentazione (ρ, V) è somma diretta di rappresentazioni irriducibili. Allora la condizione $(f, \overline{\chi_i}) = 0$ per ogni $i = 1, ..., n$ implica $\rho_f = 0$, per la Proposizione 2.4.1.
In particolare, considerando la rappresentazione regolare R di G su
$V = Span\{e_g \mid g \in G\}$ ed il vettore e_{1_G}, si ha

$$0 = R_f(e_{1_G}) = \sum_{g \in G} f(g)\, R_g(e_{1_g}) = \sum_{g \in G} f(g)\, e_g\,.$$

Dal momento che $\{e_g\}_{g \in G}$ è una base di V vale $f(g) = 0$ per ogni $g \in G$, cioè $f = 0$.

□

Teorema 2.4.2 *Il numero di classi di isomorfismo di rappresentazioni irriducibili di un gruppo G è uguale al numero di classi di coniugio di G.*

Dimostrazione. Sia k il numero di classi di coniugio di G. Se f è una funzione in $\mathbb{C}_{class}(G)$, essa assume lo stesso valore sugli elementi di una medesima classe di coniugio. Quindi f è determinata da k valori di $\mathbb{C}$. Questo implica che $\mathbb{C}_{class}(G)$ è isomorfo a $\mathbb{C}^k$, da cui segue che $\mathbb{C}_{class}(G)$ ha dimensione k. D'altra parte, per il Teorema 2.4.1, la dimensione di $\mathbb{C}_{class}(G)$ è uguale al numero di rappresentazioni irriducibili di G.

$\square$

Capitolo 3

L'algebra di gruppo $\mathbb{C}[G]$

3.1 Rappresentazioni di $\mathbb{C}[G]$

Diamo la definizione generale di algebra.

Definizione 3.1.1 *Sia $\mathbb{K}$ un campo. Una $\mathbb{K}$-algebra è un $\mathbb{K}$-spazio vettoriale A con un prodotto, cioè un'applicazione bilineare*

$$* : \quad A \times A \longrightarrow A\,.$$

Una $\mathbb{K}$-algebra si dice *associativa* se il prodotto $*$ è associativo. Si dice *con unità* se esiste un elemento $1 \in A$ tale che $1 * a = a * 1 = a$ per ogni $a \in A$. Nel seguito ometteremo il simbolo $*$ del prodotto.

Definizione 3.1.2 *Sia G un gruppo e sia V uno spazio vettoriale con una base $\{e_g\}_{g\in G}$ indicizzata dagli elementi di G. Poniamo*

$$\mathbb{C}[G] := \{\sum_{g\in G} \lambda_g\, e_g \quad | \quad \lambda_g \in \mathbb{C}\}\,.$$

Per costruzione possiamo identificare gli elementi della base $\{e_g\}_{g\in G}$ di V con gli elementi del gruppo G, quindi, per comodità, scriveremo g al posto di e_g, considerando $\mathbb{C}[G] = \{\sum_{g\in G} \lambda_g\, g \quad | \quad \lambda_g \in \mathbb{C}\}$.

Osservazione 3.1.1 *L'insieme $\mathbb{C}[G]$ coincide con lo spazio vettoriale relativo alla rappresentazione regolare.*

Definizione 3.1.3 *Sia G un gruppo. Definiamo su $\mathbb{C}[G]$ il prodotto:*

$$(\sum_{g\in G} \lambda_g\, g)\,(\sum_{h\in G} \mu_h\, h) := \sum_{g,\,h\in G} \lambda_g\, \mu_h(g\,h)\,.$$

Proposizione 3.1.1 *L'insieme $\mathbb{C}[G]$, con l'operazione appena definita, è una $\mathbb{C}$-algebra associativa con unità.*

Dimostrazione. La bilinearità del prodotto segue subito dalla definizione. La sua associatività dipende dall'associatività del prodotto in G. L'unità in $\mathbb{C}[G]$ è l'unità in G.

$\square$

Definizione 3.1.4 *Sia G un gruppo. L'algebra $\mathbb{C}[G]$ è detta algebra di gruppo.*

Definizione 3.1.5 *Siano V e V' due algebre su un campo $\mathbb{K}$ arbitrario. Un omomorfismo di algebre è una funzione lineare $\Phi : A \longrightarrow A'$ tale che si abbia*

$$\Phi(a\,b) = \Phi(a)\,\Phi(b) \qquad \forall\, a, b \in A.$$

Definizione 3.1.6 *Sia A un'algebra associativa con unità e sia V uno spazio vettoriale. Una rappresentazione di A su V è un omomorfismo di algebre*

$$\tilde{\rho} \;:\quad A \longrightarrow End(V)$$

dove su $End(V)$ si considera la struttura di algebra associativa definita dall'usuale composizione di endomorfismi.

Denotiamo l'immagine di $a \in A$ tramite $\tilde{\rho}$ con $\tilde{\rho}_a$.

Definizione 3.1.7 *Sia A un'algebra associativa con unità e siano V e V' due spazi vettoriali. Siano inoltre $\tilde{\rho}$ una rappresentazione di A su V e $\tilde{\rho'}$ una rappresentazione di A su V'. Un omomorfismo delle rappresentazioni $\tilde{\rho}$ e $\tilde{\rho'}$ è un'applicazione lineare $\Phi : V \longrightarrow V'$ tale che per ogni $a \in A$ si abbia*

$$\Phi \circ \tilde{\rho}_a = \tilde{\rho'}_a \circ \Phi\,.$$

Se la funzione Φ è invertibile, diciamo che le rappresentazioni $\tilde{\rho}$ e $\tilde{\rho'}$ sono isomorfe.

Osservazione 3.1.2 *Ogni rappresentazione $\rho : G \longrightarrow GL(V)$ di G su V definisce una rappresentazione di $\mathbb{C}[G]$ su V.*

Infatti possiamo scrivere

$$\begin{aligned} \widehat{\rho}\ : \quad \mathbb{C}[G] &\longrightarrow End(V) \\ \sum_{g\in G} \lambda_g\, g &\longmapsto \sum_{g\in G} \lambda_g\, \rho_g \end{aligned}$$

Analogamente, ogni rappresentazione di $\mathbb{C}[G]$ su V definisce una rappresentazione di G su V (basterà considerare la restrizione di $\widehat{\rho}$ agli elementi di G).

Osservazione 3.1.3 *Sia A una $\mathbb{C}$-algebra associativa con unità e sia W uno spazio vettoriale. Se $\sigma : A \longrightarrow End(W)$ è una rappresentazione di A su W, allora è definita una rappresentazione*

$$\begin{aligned} \tilde{\sigma}\ :\ A &\longrightarrow End(End(W)) \\ a &\longmapsto \tilde{\sigma}_a\ :\ End(W) \longrightarrow End(W) \\ &\qquad\qquad\qquad f \longmapsto \sigma_a(f)\,. \end{aligned}$$

dove si pone $\sigma_a(f)(w) := \sigma_a(f(w))$.

Infatti, per ogni $a, b \in A$ e per ogni $w \in W$, vale

$$\tilde{\sigma}_{a\,b}(f(w)) = \sigma_{a\,b}(f(w)) = \sigma_a(f(w))\,\sigma_b(f(w)) = \tilde{\sigma}_a(f(w))\,\tilde{\sigma}_b(f(w)).$$

Osservazione 3.1.4 *Sia A una $\mathbb{C}$-algebra associativa con unità e sia W uno spazio vettoriale di dimensione m. Se $\sigma : A \longrightarrow End(W)$ è una rappresentazione di A su W, allora possiamo definire una rappresentazione di A su $W^{\oplus m}$ in questo modo:*

$$\begin{aligned} \widehat{\sigma}\ :\ A &\longrightarrow End(W^{\oplus m}) \\ a &\longmapsto \widehat{\sigma}_a\ :\ W^{\oplus m} \longrightarrow W^{\oplus m} \\ &\qquad\qquad (w_1, ..., w_m) \longmapsto (\sigma_a(w_1), ..., \sigma_a(w_m))\,. \end{aligned}$$

Infatti, per ogni $a, b \in A$ e per ogni $(w_1, ..., w_m) \in W^{\oplus m}$, vale

$$\widehat{\sigma}_{a\,b}(w_1, ..., w_m) = (\sigma_{a\,b}(w_1), ..., \sigma_{a\,b}(w_m)) = (\sigma_a\,\sigma_b(w_1), ..., \sigma_a\,\sigma_b(w_m)) =$$

$$= \widehat{\sigma}_a\,\widehat{\sigma}_b(w_1, ..., w_m).$$

Osservazione 3.1.5 *Sia A una $\mathbb{C}$-algebra associativa con unità e sia W uno spazio vettoriale di dimensione m. Allora $End(W) \cong W^m$ come rappresentazioni di A.*

Infatti: sia $B = \{w_1, ..., w_m\}$ una base di W. Consideriamo l'applicazione lineare $\Phi : End(W) \longrightarrow W^m$ tale che

$$\Phi(f) = (f(w_1), ..., f(w_m)) \qquad \forall\, f \in End(W).$$

L'applicazione Φ è invertibile e, per ogni $a \in A$ e per ogni $f \in End(W)$, si ha:

$$\Phi(\tilde{\sigma}_a(f)) = \Phi(\sigma_a(f)) = (\sigma_a(f(w_1)), ..., \sigma_a(f(w_m))) = \sigma_a(f(w_1), ..., f(w_m)) =$$

$$= \widehat{\sigma}_a(f(w_1), ..., f(w_m)) = \widehat{\sigma}_a(\Phi(f)).$$

Proposizione 3.1.2 *Sia G un gruppo e siano $V_1, \ldots, V_n$ le rappresentazioni irriducibili di G. Allora vale il seguente isomorfismo di algebre:*

$$\mathbb{C}[G] \cong End(V_1) \oplus \ldots \oplus End(V_n)\,.$$

Dimostrazione. La rappresentazione regolare è, per definizione, una rappresentazione di G su $\mathbb{C}[G]$, quindi definisce una rappresentazione di $\mathbb{C}[G]$ su se stessa. D'altra parte, per il Teorema 1.3.1 ed il Corollario 2.3.1, si ha

$$\mathbb{C}[G] = V_1^{\oplus dim(V_1)} \oplus \ldots \oplus V_n^{\oplus dim(V_n)}.$$

A questo punto basta utilizzare le Osservazioni 3.1.2, 3.1.3 e 3.1.4.

$\square$

Osservazione 3.1.6 *Ad ogni rappresentazione irriducibile V_i di un gruppo G di dimensione m_i e con carattere χ_i, con $1 \leq i \leq n$, corrisponde un omomorfismo di algebre*

$$\widehat{\rho}_i \;:\; \mathbb{C}[G] \longrightarrow End(V_i)\,.$$

Proposizione 3.1.3 ***(Formula di inversione di Fourier)***
Sia $u = u_1 \oplus \ldots \oplus u_n$ un elemento di $End(V_1) \oplus \ldots \oplus End(V_n)$ e sia $\alpha = \sum_{g \in G} \lambda_g \, g$ l'elemento di $\mathbb{C}[G]$ tale che $\widehat{\rho}(\alpha) = u$. Allora, il coefficiente λ_g di α è dato dalla formula

$$\lambda_g = \frac{1}{|G|} \sum_{i=1}^{n} m_i \, Tr_{V_i}(\rho_i(g^{-1}) \, u_i)$$

dove m_i è la dimensione di V_i, con $1 \leq i \leq n$.

Dimostrazione. Per linearità è sufficiente verificare che la formula è vera per $\alpha = h \in G$. In questo caso si ha $\lambda_g = \delta_{g,h}$, con $g, h \in G$.
Ora $u_i = \widehat{\rho}_{|V_i}(\alpha) = \rho_i(h)$, da cui $Tr_{V_i}(\rho_i(g^{-1}) \, u_i) = \chi_i(g^{-1} \, h)$.
Allora deve valere

$$\delta_{g,h} = \frac{1}{|G|} \sum_{i=1}^{n} m_i \, \chi_i(g^{-1} \, h).$$

Ma questo è vero, grazie ai Corollari 2.3.1 e 2.3.2.

□

3.2 Il centro di $\mathbb{C}[G]$

Definizione 3.2.1 *Si chiama centro di $\mathbb{C}[G]$ il seguente insieme:*

$$Z(\mathbb{C}[G]) := \{\alpha \in \mathbb{C}[G] \quad | \quad \alpha \, \beta = \beta \, \alpha \quad \forall \, \beta \in \mathbb{C}[G]\} \, .$$

Osservazione 3.2.1 *In particolare, se $\alpha \in Z(\mathbb{C}[G])$, allora α commuta con tutti gli elementi di G.*

Definizione 3.2.2 *Se C_i, con $1 \leq i \leq n$, è una classe di coniugio di G, poniamo*

$$e_{C_i} := \sum_{g_i \in C_i} g_i \, .$$

Proposizione 3.2.1 *L'insieme* $\{e_{C_i}\}_{1 \le i \le n}$ *forma una base del centro di* $\mathbb{C}[G]$.

Dimostrazione. Consideriamo due elementi $\alpha, \beta \in Z(\mathbb{C}[G])$ arbitrari. Siano $\alpha = \sum\limits_{g \in G} \lambda_g\, g\,, \quad \beta = \sum\limits_{h \in G} \mu_h\, h\,$. Si ha

$$\alpha\,\beta = \beta\,\alpha \quad \Longleftrightarrow \quad (\sum_{g \in G} \lambda_g\, g)\,(\sum_{h \in G} \mu_h\, h) = (\sum_{h \in G} \mu_h\, h)\,(\sum_{g \in G} \lambda_g\, g) \quad \Longleftrightarrow$$

$$\Longleftrightarrow \quad \sum_{g,\, h \in G} \lambda_g\, \mu_h\, (g\, h) = \sum_{h,\, g \in G} \mu_h\, \lambda_g\, (h\, g).$$

Ora, ponendo $\lambda_g\, \mu_h := f(g\, h)$, con $f : G \longrightarrow \mathbb{C}$, si ottiene che $f(g\, h) = f(h\, g)$ per ogni $g, h \in G$. Dunque, per la Proposizione 2.1.1, f è una funzione di classe e quindi i coefficienti $\lambda_g\, \mu_h$, al variare di g, h in G, assumono lo stesso valore su una medesima classe di coniugio di G. Ciò implica innanzitutto che gli elementi e_{C_i}, per $i = 1, ..., n$, appartengono al centro di $\mathbb{C}[G]$; in secondo luogo che gli e_{C_i} sono dei generatori del centro di $\mathbb{C}[G]$.
Rimane da mostrare che essi sono linearmente indipendenti, cioè che

$$\sum_{j=1}^{n} \lambda_j\, e_{C_j} = 0 \quad \Rightarrow \quad \lambda_j = 0 \qquad \forall\, j = 1, ..., n.$$

Questo segue dal fatto che gli elementi del gruppo G formano una base di $\mathbb{C}[G]$.

$\square$

Proposizione 3.2.2 *L'omomorfismo* $\widehat{\rho}_i$, *con* $1 \le i \le n$, *è un'applicazione che associa al centro di* $\mathbb{C}[G]$ *l'insieme delle omotetie di* V_i *e definisce, per ogni* $i = 1, \ldots, n$, *un omomorfismo di algebre*

$$\omega_i \; := \quad Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}\,.$$

Inoltre, se $\alpha = \sum_{g \in G} \lambda_g\, g \in Z(\mathbb{C}[G])$ *e* m_i *è la dimensione di* V_i, *si ha*

$$\omega_i(\alpha) = \frac{1}{m_i} \sum_{g \in G} \lambda_g\, \chi_i(g) = \frac{1}{m_i}\, Tr_{V_i}(\widehat{\rho}_i(\alpha))\,.$$

Dimostrazione. Innanzitutto l'applicazione $\widehat{\rho}_i$, con $1 \leq i \leq n$, è così definita:

$$\begin{aligned} \widehat{\rho}_i \ : \quad \mathbb{C}[G] &\longrightarrow End(V_i) \\ \sum_{g \in G} \lambda_g \, g &\longmapsto \sum_{g \in G} \lambda_g \, \rho_g . \end{aligned}$$

Consideriamo la restrizione di $\widehat{\rho}_i$ a $Z(\mathbb{C}[G])$. Prendendo come base di $Z(\mathbb{C}[G])$ l'insieme $\{e_{C_i}\}_{1 \leq i \leq n}$, si ha che λ_g è costante su una stessa classe di coniugio di G, quindi λ_g è una funzione di classe. Perciò possiamo porre $\lambda_g := f(g)$, con $f \in \mathbb{C}_{class}(G)$. Si ha $\widehat{\rho}_i(\sum_{g \in G} f(g)\, g) = \sum_{g \in G} f(g)\, \rho_g$ per ogni elemento di $Z(\mathbb{C}[G])$. Dunque, per la Proposizione 2.4.1, vale $\sum_{g \in G} f(g)\, g = \lambda_i \, id_{V_i}$, con $\lambda_i \in \mathbb{C}$. Allora è ben definita l'applicazione $\omega_i : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ che ad ogni elemento di $Z(\mathbb{C}[G])$ associa lo scalare λ_i in $\mathbb{C}$. Quest'ultima applicazione risulta essere un omomorfismo di algebre.
Inoltre, ancora grazie alla Proposizione 2.4.1, si ha $\lambda_i = \frac{|G|}{m_i}\,(f, \overline{\chi_i})$, dove χ_i è il carattere della rappresentazione irriducibile V_i.
Quindi, se $\alpha = \sum_{g \in G} f(g)\, g \in Z(\mathbb{C}[G])$, abbiamo

$$\omega_i(\alpha) = \lambda_i = \frac{1}{m_i} \sum_{g \in G} f(g)\, \chi_i(g) = \frac{1}{m_i} \sum_{g \in G} f(g)\, Tr(\rho_{i_g}) = \frac{1}{m_i} Tr_{V_i}(\widehat{\rho}_i(\alpha)).$$

□

Proposizione 3.2.3 *La famiglia $\{\omega_i\}_{1 \leq i \leq n}$ definisce un isomorfismo tra il centro di $\mathbb{C}[G]$ e l'algebra $\mathbb{C}^n$.*

Dimostrazione. Se identifichiamo $\mathbb{C}[G]$ con $End(V_1) \oplus \ldots \oplus End(V_n)$, allora, per la Proposizione 3.2.2, possiamo identificare il centro di $\mathbb{C}[G]$ con la somma di omotetie dei V_i con $i = 1, ..., n$. Allora si ha un isomorfismo tra $Z(\mathbb{C}[G])$ e $\mathbb{C} \times \ \ldots \ \times \mathbb{C}$, con $\mathbb{C}$ ripetuto n volte, cioè $\mathbb{C}^n$.

□

3.3 Dimensione di rappresentazioni irriducibili

Definizione 3.3.1 *Sia A un anello commutativo e sia $a \in A$. Si dice che a è integro su $\mathbb{Z}$ se esistono $n \in \mathbb{N}$, $n \geq 1$ e degli elementi $s_1, \ldots, s_n \in \mathbb{Z}$ tali che*

$$a^n + s_1\, a^{n-1} + \;\ldots\; + s_n = 0 \qquad\qquad (\star\star\star\star)$$

Un numero complesso integro su $\mathbb{Z}$ viene chiamato intero algebrico.

Esempio 3.3.1 *Un numero complesso che è radice dell'unità è un intero algebrico.*

Osservazione 3.3.1 *Se $a \in \mathbb{Q}$ è un intero algebrico, allora $a \in \mathbb{Z}$.*

Infatti, se ciò non fosse vero, potremmo scrivere a nella forma $\frac{p}{q}$, con $p, q \in \mathbb{Z}$, $q \geq 2$ e con p, q relativamente primi. Allora, applicando l'espressione $(\star\star\star\star)$, si avrebbe

$$\frac{p^n}{q^n} + s_1\, \frac{p^{n-1}}{q^{n-1}} + \;\ldots\; + s_n = 0$$

da cui si ricava

$$p^n + s_1\, q\, p^{n-1} + \;\ldots\; + s_n\, q^n = 0$$

e così si deduce che q divide p^n. Ma questo contraddice il fatto che p e q siano relativamente primi.

Proposizione 3.3.1 *Sia A un anello commutativo e sia $a \in A$. Le seguenti affermazioni sono equivalenti:*

(1) a è integro su $\mathbb{Z}$.
(2) Il sottoanello $\mathbb{Z}[a]$ di A generato da a è finitamente generato come $\mathbb{Z}$-modulo.
(3) Esiste un sotto $\mathbb{Z}$-modulo di A finitamente generato che contiene $\mathbb{Z}[a]$.

Dimostrazione. Facciamo vedere (1) $\Longleftrightarrow$ (2) e (2) $\Longleftrightarrow$ (3).

(1) $\Rightarrow$ (2). Per ipotesi $a \in A$ soddisfa un'equazione del tipo

$$a_n + s_1\, a_{n-1} + \;\ldots\; + s_n = 0$$

con $s_1, ..., s_n \in \mathbb{Z}$. Si osserva che se consideriamo il sotto $\mathbb{Z}$-modulo di A generato da $\{1, a, ..., a^{n-1}\}$ e moltiplichiamo un suo elemento arbitrario per a, il prodotto appartiene ancora allo stesso sotto $\mathbb{Z}$-modulo. Allora quest'ultimo coincide con $\mathbb{Z}[a]$.

(2) $\Rightarrow$ (1). Denotiamo con A_n il sotto $\mathbb{Z}$-modulo di A generato da $\{1, a, ..., a^{n-1}\}$. Gli insiemi A_n, per $n \to +\infty$, formano una sequenza crescente e la loro unione è $\mathbb{Z}[a]$. Ma per ipotesi $\mathbb{Z}[a]$ è finitamente generato, quindi si deve avere $A_n = \mathbb{Z}[a]$ per n sufficientemente grande. Questo implica che a^n è una combinazione lineare di $\{1, a, ..., a^{n-1}\}$, da cui (1).

(2) $\iff$ (3). Questa equivalenza segue dal fatto che un sottomodulo di uno $\mathbb{Z}$-modulo finitamente generato è finitamente generato, dal momento che $\mathbb{Z}$ è noetheriano.

$\square$

Corollario 3.3.1 *Se A è uno $\mathbb{Z}$-modulo finitamente generato, allora ogni elemento di A è integro su $\mathbb{Z}$.*

Dimostrazione. Segue dall'implicazione (3) $\Rightarrow$ (1).

$\square$

Corollario 3.3.2 *Sia A un anello commutativo. Allora gli elementi di A che sono integri su $\mathbb{Z}$ formano un sottoanello di A.*

Dimostrazione. Siano $a, b \in A$ tali che sono integri su $\mathbb{Z}$. Allora gli anelli $\mathbb{Z}[a]$ e $\mathbb{Z}[b]$ sono finitamente generati su $\mathbb{Z}$. Questo è vero anche per il loro prodotto tensoriale $\mathbb{Z}[a] \otimes \mathbb{Z}[b]$ e per l'anello $\mathbb{Z}[a, b]$. Quindi tutti gli elementi di $\mathbb{Z}[a, b]$ sono integri su $\mathbb{Z}$.

$\square$

Proposizione 3.3.2 *Sia G un gruppo e sia χ il carattere di una rappresentazione ρ di G. Allora $\chi(g)$ è un intero algebrico, per ogni $g \in G$.*

Dimostrazione. Per ogni $g \in G$, la traccia $\chi(g)$ di ρ_g è la somma degli autovalori di ρ_g e questi ultimi sono radici dell'unità. Applicando il Corollario 3.3.2 si ha la tesi.

$\square$

Per quanto riguarda il centro di $\mathbb{C}[G]$, essendo un anello commutativo, è valida questa proposizione:

Proposizione 3.3.3 *Sia* $u = \sum\limits_{g \in G} \lambda_g \, g$ *un elemento di* $Z(\mathbb{C}[G])$ *tale che* λ_g *è un intero algebrico per ogni* $g \in G$. *Allora* u *è integro su* $\mathbb{Z}$.

Dimostrazione. Per la Proposizione 3.2.1 possiamo scrivere u nella forma $u = \sum\limits_{i=1}^{n} z_i \, e_{C_i}$, con $z_i \in \mathbb{C}$. In virtù del Corollario 3.3.2 basta mostrare che gli e_{C_i}, per $i = 1, ..., n$, sono integri su $\mathbb{Z}$. Ma questo è vero, poiché ogni prodotto $e_{C_i} \, e_{C_j}$ è una combinazione lineare a coefficienti interi degli elementi e_{C_k}, per $j, k = 1, ..., n$. Il sottogruppo $\mathbb{Z} \, e_{C_1} \oplus \ldots \oplus \mathbb{Z} \, e_{C_n}$ del centro di $\mathbb{C}[G]$ è un sottoanello finitamente generato su $\mathbb{Z}$. Allora, per il Corollario 3.3.1, ogni suo elemento è integro su $\mathbb{Z}$. Segue la tesi.

□

Corollario 3.3.3 *Sia* G *un gruppo e sia* ρ *una rappresentazione irriducibile di* G *di dimensione* n *e con carattere* χ. *Sia poi* $u = \sum_{g \in G} \lambda_g \, g \in Z(\mathbb{C}[G])$ *tale che* λ_g *è un intero algebrico per ogni* $g \in G$. *Allora il numero* $\frac{1}{n} \sum\limits_{g \in G} \lambda_g \, \chi(g)$ *è un intero algebrico.*

Dimostrazione. Si osserva che il numero scritto nell'enunciato è l'immagine di u tramite l'omomorfismo $\omega : Z(\mathbb{C}[G]) \longrightarrow \mathbb{C}$ associato a ρ (vedi Proposizione 3.2.2). D'altra parte, per la Proposizione 3.3.3, u è integro su $\mathbb{Z}$. Allora ciò sarà vero anche per la sua immagine tramite ω.

□

Corollario 3.3.4 *La dimensione di ogni rappresentazione irriducibile di un gruppo* G *divide l'ordine di* G.

Dimostrazione. Siano n e χ rispettivamente la dimensione ed il carattere di una rappresentazione irriducibile di G. Consideriamo $u = \sum\limits_{g \in G} \chi(g^{-1}) \, g$. Si ha $u \in Z(\mathbb{C}[G])$, poiché χ è una funzione di classe. Inoltre, per la Proposizione 3.3.2, sappiamo che $\chi(g)$ è un intero algebrico, per ogni $g \in G$. Quindi, per la Proposizione 3.3.3, u è integro su $\mathbb{Z}$. Allora possiamo applicare il Corollario 3.3.3, ottenendo che il numero

$$\frac{1}{n} \sum_{g \in G} \chi(g^{-1}) \, \chi(g) = \frac{1}{n} \, |G| < \chi, \chi > = \frac{|G|}{n}$$

è un intero algebrico. Ma $\frac{|G|}{n} \in \mathbb{Q}$, dunque, per l'Osservazione 3.3.1, $\frac{|G|}{n} \in \mathbb{Z}$, cioè n divide $|G|$.

□

Capitolo 4

Esempi

In questo capitolo determiniamo le rappresentazioni irriducibili dei gruppi simmetrici S_3 e S_4.

4.1 Il numero di classi di coniugio di S_n

Indichiamo con S_n il gruppo simmetrico, cioè il gruppo delle biiezioni tra l'insieme $\{1,...,n\}$ e se stesso. La cardinalità di S_n è $n!$. Mostreremo che il numero di classi di coniugio di S_n è uguale al numero delle partizioni di n, ovvero delle decomposizioni di n nella somma di numeri interi positivi.

Definizione 4.1.1 *Sia $\alpha \in S_n$ e sia $i \in \{1,...,n\}$. Si dice che α muove i se $\alpha(i) \neq i$ e si dice che α fissa i se $\alpha(i) = i$.*

Gli elementi di S_n vengono detti *permutazioni*. Indichiamo la permutazione identità con 1.

Definizione 4.1.2 *Sia $t \in \mathbb{N}$ tale che $1 \leq t \leq n$, sia $l \in \mathbb{N}$ tale che $1 \leq l \leq t$ e siano $i_1,...,i_t$ degli elementi in $\{1,...,n\}$ tali che $i_j \neq i_k$ per $j \neq k$. Denotiamo con $(i_1...i_t)$ il seguente elemento α di S_n:*

$$\alpha(i_l) = \begin{cases} i_{l+1} & se\ \ 1 \leq l \leq t\,; \\ i_1 & se\ \ l = t\,. \end{cases}$$

Inoltre $\alpha(x) = x$ per ogni $x \in \{1,...,n\} \setminus \{i_1,...,i_t\}$.

In questo caso α si dice *ciclo*.

Definizione 4.1.3 *Sia $\alpha = (i_1...i_t) \in S_n$. Il numero t si chiama lunghezza di α e si indica con $|\alpha|$.*

Definizione 4.1.4 *Due cicli $\alpha = (i_1...i_t)$ e $\beta = (j_1...j_k)$ si dicono disgiunti se $\{i_1, ..., i_t\} \cap \{j_1, ..., j_k\} = \varnothing$.*

È facile notare che due cicli disgiunti commutano. È noto che ogni permutazione α di S_n, con $\alpha \neq 1$, si può scrivere come prodotto di cicli disgiunti $\gamma_1...\gamma_q$ e che questa scrittura è unica, a meno dell'ordine.

Definizione 4.1.5 *Due permutazioni $\alpha, \beta \in S_n$ si dicono coniugate se esiste $\sigma \in S_n$, $\sigma \neq 1$, tale che $\beta = \sigma\alpha\sigma^{-1}$.*

Definizione 4.1.6 *Sia $\alpha \in S_n$ e sia $\alpha = \gamma_1...\gamma_q$ la sua decomposizione in cicli disgiunti (possiamo supporre $|\gamma_1| \geq |\gamma_2| \geq \ldots \geq |\gamma_q|$). Chiamiamo $(|\gamma_1|, ..., |\gamma_q|)$ successione caratteristica di α.*

Lemma 4.1.1 *Sia $\sigma \in S_n$ e sia $\gamma = (i_1...i_t) \in S_n$ un ciclo di lunghezza t. Allora vale*

$$\sigma\,\gamma\,\sigma^{-1} = (\sigma(i_1)...\sigma(i_t))\,.$$

In particolare $\sigma\,\gamma\,\sigma^{-1}$ è un ciclo di lunghezza t.

Dimostrazione. Poniamo $\delta := (\sigma(i_1)...\sigma(i_t))$. Mostriamo che $(\sigma\gamma\sigma^{-1})(j) = \delta(j)$ per ogni $j \in \{1, ..., n\}$. Consideriamo un elemento j e distinguiamo due casi:

1) $j \notin \{\sigma(i_1), ..., \sigma(i_t)\}$.
Allora $\delta(j) = j$ e, per ipotesi, $\sigma^{-1}(j) \notin \{i_1, ..., i_t\}$, pertanto $\gamma(\sigma^{-1}(j)) = \sigma^{-1}(j)$.
Si ha dunque $(\sigma\gamma\sigma^{-1})(j) = \sigma(\gamma(\sigma^{-1}(j))) = \sigma(\sigma^{-1}(j)) = j$.

2) $j \in \{\sigma(i_1), ..., \sigma(i_t)\}$.
Sia $j = \sigma(i_l)$, con $1 \leq l \leq t$. Ora

$$\delta(j) = \begin{cases} \sigma(i_{l+1}) & \text{se } \ l < t\,; \\ \sigma(i_1) & \text{se } \ l = t\,. \end{cases}$$

D'altra parte

$$(\sigma\gamma\sigma^{-1})(j) = \sigma(\gamma(\sigma^{-1}(\sigma(i_l)))) = \sigma(\gamma(i_l)) = \begin{cases} \sigma(i_{l+1}) & \text{se } l < t\,; \\ \sigma(i_1) & \text{se } l = t\,. \end{cases}$$

Quindi, in ogni caso, la tesi è verificata.

□

Teorema 4.1.1 *Due permutazioni $\alpha, \beta \in S_n$ sono coniugate se e solo se hanno la stessa successione caratteristica.*

Dimostrazione.
Siano $\alpha, \beta \in S_n$ coniugate e mostriamo che hanno la stessa successione caratteristica.
Sia $\gamma_1 ... \gamma_q$ la decomposizione di α in cicli disgiunti e supponiamo che $|\gamma_1| \geq |\gamma_2| \geq \ldots \geq |\gamma_q|$. Per ipotesi $\beta = \sigma\alpha\sigma^{-1}$ per una certa $\sigma \in S_n$. Possiamo scrivere

$$\sigma\alpha\sigma^{-1} = \sigma\gamma_1 ... \gamma_q\sigma^{-1} = \sigma\gamma_1(\sigma^{-1}\sigma)\gamma_2(\sigma^{-1}\sigma)\ldots\gamma_q\sigma^{-1} =$$

$$= (\sigma\gamma_1\sigma^{-1})(\sigma\gamma_2\sigma^{-1})...(\sigma\gamma_q\sigma^{-1}).$$

Poniamo $\delta_i = \sigma\gamma_i\sigma^{-1}$ per ogni $i = 1, ..., q$. Per il Lemma 4.1.1 si ha $|\delta_i| = |\gamma_i|$ per ogni $i = 1, ..., q$. Mostriamo ora che i cicli $\delta_1, ..., \delta_q$ sono disgiunti. Supponiamo che $\gamma_r = (i_1 ... i_t)\,, \quad \gamma_s = (j_1 ... j_k)\,.$ Per il Lemma 4.1.1 si ha

$$\delta_r = \sigma\gamma_r\sigma^{-1} = (\sigma(i_1)...\sigma(i_t)); \qquad \delta_s = \sigma\gamma_s\sigma^{-1} = (\sigma(j_1)...\sigma(j_k)).$$

A questo punto si tratta di vedere che

$$\{\sigma(i_1), ..., \sigma(i_t)\} \ \cap \ \{\sigma(j_1), ..., \sigma(j_k)\} = \varnothing \qquad (\bullet)$$

Sappiamo che $\{i_1, ..., i_t\} \cap \{j_1, ..., j_k\} = \varnothing$ poiché γ_r e γ_s sono cicli disgiunti. Se per assurdo la proprietà $(\bullet)$ non fosse vera, allora si avrebbe $\sigma(i_h) = \sigma(j_p)$ per qualche $1 \leq h \leq t$ e $1 \leq p \leq k$. Dal momento che $i_h \neq j_p$ e σ è biiettiva

questo non è possibile.
Viceversa, supponiamo che $\alpha, \beta \in S_n$ abbiano la stessa successione caratteristica. Allora sono della forma $\alpha = \gamma_1 ... \gamma_q \, , \quad \beta = \delta_1 ... \delta_q$ con $|\gamma_i| = |\delta_i|$ per ogni $i = 1, ..., q$. Fissiamo i, con $1 \leq i \leq q$, e siano $\gamma_i = (i_1 ... i_t)\,,$
$\delta_i = (j_1 ... j_t)\,.$ Sia σ_i l'applicazione così definita:

$$\begin{aligned} \sigma_i \ : \quad \{i_1, ..., i_t\} &\longrightarrow \{j_1, ..., j_t\} \\ i_l &\longmapsto j_l\,. \end{aligned}$$

Sia $\{l_1, ..., l_p\}$ l'insieme degli elementi fissati da α e sia $\{k_1, ..., k_p\}$ l'insieme degli elementi fissati da β. Sia inoltre $\tilde{\sigma} \, : \, \{l_1, ..., l_p\} \longrightarrow \{k_1, ..., k_p\}$ una biiezione. Costruiamo una permutazione $\sigma \in S_n$, per $j \in \{1, ..., n\}$, nel modo seguente:

$$\sigma(j) := \begin{cases} \sigma_i(j) & \text{se } j \text{ compare nel ciclo } \gamma_i\,; \\ \tilde{\sigma}(j) & \text{se } j \in \{l_1, ..., l_p\}\,. \end{cases}$$

Si ha $\sigma \alpha \sigma^{-1} = \beta$, infatti: $\sigma \alpha \sigma^{-1} = (\sigma \gamma_1 \sigma^{-1}) ... (\sigma \gamma_q \sigma^{-1})$ e, per ogni $i = 1, ..., q$, per il Lemma 4.1.1, vale

$$\sigma \gamma_i \sigma^{-1} = (\sigma(i_1) ... \sigma(i_t)) = (\sigma_i(i_1) ... \sigma_i(i_t)) = (j_1 ... j_t) = \delta_i.$$

Quindi $\sigma \alpha \sigma^{-1} = \delta_1 ... \delta_q = \beta$, cioè α e β sono coniugate.

$\square$

Corollario 4.1.1 *Il numero di classi di coniugio del gruppo simmetrico S_n è uguale al numero delle partizioni di n.*

4.2 Rappresentazioni irriducibili di S_3

Abbiamo già osservato che la cardinalità di S_3 è $3! = 6$ ed il suo numero di classi di coniugio è uguale al numero delle partizioni di 3. Nel caso di S_3 abbiamo 3 classi di coniugio, infatti 3 si può scrivere come

- 3=1+1+1 (corrisponde alla classe di coniugio dell'identità);
- 3=2+1 (corrisponde alla classe di coniugio delle trasposizioni);
- 3=3 (corrisponde alla classe di coniugio dei cicli di lunghezza 3).

Abbiamo dimostrato che il numero di rappresentazioni irriducibili di S_3, a meno di isomorfismi, è uguale al numero di classi di coniugio di S_3 (Teorema 2.4.2). Quindi in questo caso si hanno 3 rappresentazioni irriducibili.
Una rappresentazione irriducibile è la rappresentazione banale: consideriamo $V = \mathbb{C}$ e scriviamo

$$\begin{aligned} \rho \ : \quad S_3 &\longrightarrow GL(V) \\ \sigma &\longmapsto \rho_\sigma \ : \ V \longrightarrow V \\ &\qquad\qquad\quad v \longmapsto v\,. \end{aligned}$$

Un'altra rappresentazione irriducibile di S_3, non isomorfa alla rappresentazione banale, è la rappresentazione detta *alternante*: consideriamo $V' = \mathbb{C}$ e poniamo

$$\begin{aligned} \rho' \ : \quad S_3 &\longrightarrow GL(V') \\ \sigma &\longmapsto \rho'_\sigma \ : \ V' \longrightarrow V' \\ &\qquad\qquad\quad v' \longmapsto sign(\sigma)\, v'\,. \end{aligned}$$

Ricordiamo che la funzione *sign* (segno) è così definita:

$$sign(\sigma) := \begin{cases} 1 & \text{se } \sigma \text{ si decompone in un numero pari di trasposizioni}\,; \\ -1 & \text{altrimenti.} \end{cases}$$

A questo punto rimane da individuare solamente un'altra rappresentazione irriducibile di S_3. Per il Corollario 2.3.2 (1) la somma dei quadrati delle dimensioni delle rappresentazioni irriducibili di S_3 deve essere uguale a $|S_3| = 6$, quindi l'ultima rappresentazione irriducibile deve avere dimensione 2.
Consideriamo $U = \mathbb{C}^3$ con la base canonica $\mathcal{E} = \{e_1, e_2, e_3\}$ e, per $i = 1, 2, 3$, definiamo la seguente applicazione:

$$\begin{aligned} \rho'' \ : \quad S_3 &\longrightarrow GL(U) \\ \sigma &\longmapsto \rho''_\sigma \ : \ U \longrightarrow U \\ &\qquad\qquad\quad e_i \longmapsto e_{\sigma(i)}\,. \end{aligned}$$

Questa è una rappresentazione di S_3 su U.

Si osserva che $\rho''_\sigma(1,1,1) = (1,1,1)$ per ogni $\sigma \in S_3$, quindi il sottospazio W di U generato da $(1,1,1)$ è invariante rispetto all'azione di S_3. Allora $(\rho''_{|W}, W)$ è una sottorappresentazione di (ρ'', U). Si nota che essa è isomorfa alla rappresentazione banale, tramite l'applicazione

$$\begin{aligned} f \ : \quad & W \longrightarrow V \\ \lambda \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} & \longmapsto \lambda\,. \end{aligned}$$

Si ha che il sottospazio V'' di U, ortogonale a W rispetto al prodotto scalare Hermitiano standard ha dimensione 2 e, per la II Dimostrazione del Teorema di Maschke nel caso complesso, individua una sottorappresentazione di (ρ'', U). Si può verificare direttamente che tale sottorappresentazione è irriducibile. Equivalentemente l'irriducibilità segue dal fatto che $(\chi_{V''}, \chi_{V''}) = 1$, come vedremo tra poco.
Per esaminare meglio le rappresentazioni irriducibili trovate utilizziamo la cosiddetta *tabella dei caratteri.* Essa ha questa forma: nella casella in alto a sinistra scriviamo il gruppo; la prima riga contiene l'elenco delle classi di coniugio del gruppo, ognuna individuata da un qualsiasi rappresentante, e al di sopra di ognuna di esse scriviamo il numero di elementi appartenenti alla classe; nella prima colonna elenchiamo le rappresentazioni irriducibili ed indichiamo, tra parentesi, la dimensione di ciascuna di esse. All'interno della tabella viene scritto il valore del carattere della rappresentazione irriducibile corrispondente, calcolato su un rappresentante di ogni classe di coniugio del gruppo.
Ecco la tabella dei caratteri delle prime due rappresentazioni irriducibili trovate:

S_3	1 1	3 (12)	2 (123)
V (1)	1	1	1
V' (1)	1	-1	1

La riga corrispondente a V (la rappresentazione banale) è composta unicamente dal numero 1 poiché, per ogni elemento σ di S_3, l'applicazione ρ_σ è l'identità su $\mathbb{C}$. Nella riga successiva si ha 1 o -1, a seconda del segno della permutazione corrispondente.

Calcoliamo ora la riga relativa alla rappresentazione V''.
Innanzitutto si ha $U = W \oplus V''$, con W e V'' sottorappresentazioni di U. Allora, per la Proposizione 2.1.2 (5), vale $\chi_U = \chi_W + \chi_{V''}$; quindi $\chi_{V''} = \chi_U - \chi_W$. Come abbiamo visto la rappresentazione W è isomorfa alla rappresentazione banale, pertanto, grazie alla Proposizione 2.1.2 (4), vale $\chi_W(\sigma) = \chi_V(\sigma) = 1$ per ogni $\sigma \in S_3$. Allora, per determinare $\chi_{V''}$, dobbiamo calcolare χ_U.
Quindi calcoliamo la traccia della matrice di ρ'' rispetto alla base $\mathcal{E}$ di U su ogni classe di coniugio di S_3:

- $\chi_U(1) = 3$, poiché la matrice di ρ''_{Id} rispetto a $\mathcal{E}$ è I;
- $\chi_U((12)) = 1$, poiché la matrice di $\rho''_{(12)}$ rispetto a $\mathcal{E}$ è
$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} ;$$
- $\chi_U((123)) = 0$, poiché la matrice di $\rho''_{(123)}$ rispetto a $\mathcal{E}$ è
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} .$$

Si ha dunque:

- $\chi_{V''}(1) = \chi_U(1) - \chi_W(1) = 3 - 1 = 2$;
- $\chi_{V''}((12)) = \chi_U((12)) - \chi_W((12)) = 1 - 1 = 0$;
- $\chi_{V''}((123)) = \chi_U((123)) - \chi_W((123)) = 0 - 1 = -1$.

Così la tabella dei caratteri di S_3 è la seguente:

S_3	1 1	3 (12)	2 (123)
V (1)	1	1	1
V' (1)	1	-1	1
V'' (2)	2	0	-1

Come previsto, i caratteri delle tre rappresentazioni irriducibili di S_3 sono ortonormali rispetto al prodotto (,). Infatti:

$$(\chi_V, \chi_V) = \frac{1}{6}(1 \cdot 1 \cdot 1 + 1 \cdot 1 \cdot 3 + 1 \cdot 1 \cdot 2) = 1;$$

$$(\chi_{V'}, \chi_{V'}) = \frac{1}{6}(1 \cdot 1 \cdot 1 + (-1) \cdot (-1) \cdot 3 + 1 \cdot 1 \cdot 2) = 1;$$

$$(\chi_{V''}, \chi_{V''}) = \frac{1}{6}(2 \cdot 2 \cdot 1 + 0 \cdot 0 \cdot 3 + (-1) \cdot (-1) \cdot 2) = 1;$$

$$(\chi_V, \chi_{V'}) = \frac{1}{6}(1 \cdot 1 \cdot 1 + 1 \cdot (-1) \cdot 3 + 1 \cdot 1 \cdot 2) = 0;$$

$$(\chi_V, \chi_{V''}) = \frac{1}{6}(1 \cdot 2 \cdot 1 + 1 \cdot 0 \cdot 3 + 1 \cdot (-1) \cdot 2) = 0;$$

$$(\chi_{V'}, \chi_{V''}) = \frac{1}{6}(1 \cdot 2 \cdot 1 + (-1) \cdot 0 \cdot 3 + 1 \cdot (-1) \cdot 2) = 0.$$

4.3 Rappresentazioni irriducibili di S_4

La cardinalità di S_4 è $4! = 24$. Per determinare il numero di classi di coniugio di S_4, vediamo in quanti modi si può decomporre il numero 4 nella somma di numeri interi positivi:

- 4=1+1+1+1 (corrisponde alla classe di coniugio dell'identità);
- 4=2+1+1 (corrisponde alla classe di coniugio delle trasposizioni);
- 4=2+2 (corrisponde alla classe di coniugio dei prodotti di due trasposizioni disgiunte);
- 4=3+1 (corrisponde alla classe di coniugio dei cicli di lunghezza 3);
- 4=4 (corrisponde alla classe di coniugio dei cicli di lunghezza 4).

Perciò le rappresentazioni irriducibili di S_4 sono 5, per il Teorema 2.4.2. Come nel caso di S_3 la rappresentazione banale e la rappresentazione alternante di S_4 sono irriducibili.
Sia ora $U = \mathbb{C}^4$ con la base canonica $\mathcal{E} = \{e_1, e_2, e_3, e_4\}$ e, per $i = 1, 2, 3, 4$, definiamo

$$\begin{aligned}\rho'' \ : \quad S_4 &\longrightarrow GL(U)\\ \sigma &\longmapsto \rho''_\sigma \ : \ U \longrightarrow U\\ &\qquad\qquad\quad e_i \longmapsto e_{\sigma(i)}\,.\end{aligned}$$

Questa è una rappresentazione di S_4 su U.
Si osserva che il sottospazio $W := Span\{(1,1,1,1)\}$ di U è invariante rispetto all'azione di S_4, quindi $(\rho''_{|W}, W)$ è una sottorappresentazione di (ρ'', U). Come nel caso di S_3, $(\rho''_{|W}, W)$ è isomorfa alla rappresentazione banale.
Il sottospazio V'' di U ortogonale a W rispetto al prodotto scalare Hermitiano standard individua dunque una sottorappresentazione di (ρ'', U). Anche in questo caso l'irriducibilità della rappresentazione $(\rho''_{|V''}, V'')$ segue dal calcolo del carattere.

Scriviamo la tabella dei caratteri per le prime due rappresentazioni irriducibili trovate:

S_4	1 1	6 (12)	3 (12)(34)	8 (123)	6 (1234)
V (1)	1	1	1	1	1
V' (1)	1	-1	1	1	-1

Per quanto riguarda V'', innanzitutto si ha $U = W \oplus V''$, con W e V'' sottorappresentazioni di U. Grazie alla Proposizione 2.1.2 (5) vale
$\chi_U = \chi_W + \chi_{V''}$, da cui $\chi_{V''} = \chi_U - \chi_W$. Dato che W è isomorfa alla rappresentazione banale, risulta $\chi_W = \chi_V$, per la Proposizione 2.1.2 (4). Quindi $\chi_W(\sigma) = \chi_V(\sigma) = 1$ per ogni $\sigma \in S_4$.
Ora, calcolando i valori di χ_U su ogni classe di coniugio di S_4, potremo determinare i rispettivi valori di $\chi_{V''}$. Considerando per ogni rappresentante scelto delle classi di coniugio la matrice di ρ'' rispetto alla base $\mathcal{E}$ di U si ha:

- $\chi_U(1) = 4$, infatti la matrice di ρ''_{Id} rispetto a $\mathcal{E}$ è I;
- $\chi_U((12)) = 2$, infatti la matrice di $\rho''_{(12)}$ rispetto a $\mathcal{E}$ è

$$\begin{pmatrix} 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix};$$

- $\chi_U((12)(34)) = 0$, infatti la matrice di $\rho''_{(12)(34)}$ rispetto a $\mathcal{E}$ è

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix};$$

- $\chi_U((123)) = 1$, infatti la matrice di $\rho''_{(123)}$ rispetto a $\mathcal{E}$ è

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

- $\chi_U((1234)) = 0$, infatti la matrice di $\rho''_{(1234)}$ rispetto a $\mathcal{E}$ è

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Allora i valori di $\chi_{V''}$ sono:

- $\chi_{V''}(1) = \chi_U(1) - \chi_W(1) = 4 - 1 = 3$;
- $\chi_{V''}((12)) = \chi_U((12)) - \chi_W((12)) = 2 - 1 = 1$;
- $\chi_{V''}((12)(34) = \chi_U((12)(34)) - \chi_W((12)(34)) = 0 - 1 = -1$;
- $\chi_{V''}((123)) = \chi_U((123)) - \chi_W((123)) = 1 - 1 = 0$;
- $\chi_{V''}((1234)) = \chi_U((1234)) - \chi_W((1234)) = 0 - 1 = -1$.

Quindi la tabella dei caratteri diventa

S_4	1 1	6 (12)	3 (12)(34)	8 (123)	6 (1234)
V (1)	1	1	1	1	1
V' (1)	1	-1	1	1	-1
V'' (3)	3	1	-1	0	-1

Osserviamo che

$$(\chi_{V''}, \chi_{V''}) = \frac{1}{24}\,(9 \cdot 1 + 1 \cdot 6 + 1 \cdot 3 + 0 \cdot 8 + 1 \cdot 6) = 1.$$

Ciò dimostra che V'' è irriducibile.
A questo punto dobbiamo trovare altre due rappresentazioni irriducibili di S_4. Prima di tutto possiamo determinare la loro dimensione: infatti, per il Corollario 2.3.2 (1), le dimensioni m_i delle rappresentazioni irriducibili soddisfano la relazione:

$$\sum_{i=1}^{5} m_i^2 = |S_4| = 24.$$

Dunque le dimensioni delle ultime due rappresentazioni irriducibili di S_4, cioè m_4 e m_5, soddisfano l'espressione

$$1^2 + 1^2 + 3^2 + m_4^2 + m_5^2 = 24$$

da cui si ottiene

$$m_4^2 + m_5^2 = 24 - 11 = 13.$$

Si vede facilmente che una delle due rappresentazioni irriducibili deve avere dimensione 3 e l'altra deve avere dimensione 2.
Consideriamo il prodotto tensoriale $V' \otimes V''$. Si ha innanzitutto che $V' \otimes V''$ ha dimensione 3. Inoltre, per la Proposizione 2.1.2 (6), vale $\chi_{V' \otimes V''} = \chi_{V'}\,\chi_{V''}$. Quindi:

- $\chi_{V' \otimes V''}(1) = \chi_{V'}(1)\,\chi_{V''}(1) = 1 \cdot 3 = 3;$
- $\chi_{V' \otimes V''}((12)) = \chi_{V'}((12))\,\chi_{V''}((12)) = -1 \cdot 1 = -1;$
- $\chi_{V' \otimes V''}((12)(34)) = \chi_{V'}((12)(34))\,\chi_{V''}((12)(34)) = 1 \cdot (-1) = -1;$
- $\chi_{V' \otimes V''}((123)) = \chi_{V'}((123))\,\chi_{V''}((123)) = 1 \cdot 0 = 0;$
- $\chi_{V' \otimes V''}((1234)) = \chi_{V'}((1234))\,\chi_{V''}((1234)) = -1 \cdot (-1) = 1.$

Si vede che il carattere di $\chi_{V'\otimes V''}$ è diverso da ogni altro carattere delle precedenti rappresentazioni irriducibili. Quindi, per la Proposizione 2.2.4, $V' \otimes V''$ non è isomorfa a nessuna delle precedenti.
Rimane da vedere se $V' \otimes V''$ è irriducibile. Per farlo usiamo il Teorema 2.2.3, cioè verifichiamo se $(\chi_{V'\otimes V''}, \chi_{V'\otimes V''}) = 1$. Si ha:

$$(\chi_{V'\otimes V''}, \chi_{V'\otimes V''}) = \frac{1}{24}(9 \cdot 1 + 1 \cdot 6 + 1 \cdot 3 + 0 \cdot 8 + 1 \cdot 6) = 1.$$

Allora $V' \otimes V''$ è irriducibile, da cui abbiamo che $V' \otimes V''$ è un'altra rappresentazione irriducibile di S_4.
Per determinare l'ultima rappresentazione irriducibile di S_4 (che ricordiamo avere dimensione 2), consideriamo innanzitutto il seguente sottoinsieme di S_4: $K = \{1, (12)(34), (13)(24), (14)(23)\}$. Questo risulta essere un sottogruppo normale in S_4, quindi ha senso considerare l'insieme quoziente S_4/K. Allora è ben definita l'applicazione

$$\begin{aligned} p \ : \quad S_4 &\longrightarrow S_4/K \\ \sigma &\longmapsto [\sigma]_K \,. \end{aligned}$$

L'insieme S_4/K ha $\frac{|S_4|}{|K|} = \frac{24}{4} = 6$ elementi, i quali contengono ciascuno un elemento di S_3. In altri termini:

$$S_4/K = \{[1]_K, [(12)]_K, [(13)]_K, [(23)]_K, [(123)]_K, [(132)]_K\}\,.$$

dove, esplicitamente:

- $[1]_K = K$;
- $[(12)]_K = \{(12), (34), (1423), (1324)\}$;
- $[(13)]_K = \{(13), (24), (1432), (1234)\}$;
- $[(23)]_K = \{(23), (14), (1243), (1342)\}$;
- $[(123)]_K = \{(123), (243), (142), (134)\}$;
- $[(132)]_K = \{(132), (143), (234), (124)\}$.

Quindi possiamo identificare S_4/K con S_3, scrivendo con abuso di notazione $p : S_4 \longrightarrow S_3$.
Adesso consideriamo la rappresentazione irriducibile di dimensione 2 di S_3, che qui chiamiamo $\tilde{\rho}$: possiamo scrivere $\tilde{\rho} : S_3 \longrightarrow GL(\mathbb{C}^2)$. Componendo le applicazioni p e $\tilde{\rho}$ e ponendo $\mathbb{C}^2 = V'''$ otteniamo

$$
\begin{aligned}
\rho''' := \ \tilde{\rho} \circ p \ : \quad & S_4 \longrightarrow S_3 \longrightarrow GL(V''') \\
& \sigma \longmapsto [\sigma]_K = [\tau]_K \longmapsto \rho'''_\tau
\end{aligned}
$$

dove $\tau \in S_3 \subseteq S_4$. Si ha che ρ''' è una rappresentazione di S_4.
Si vede che 1 e la classe di coniugio dei prodotti di due trasposizioni disgiunte appartengono a K, quindi determinano lo stesso carattere, cioè 2.
Inoltre i cicli di lunghezza 4 vengono associati ad una classe modulo K identificata da una trasposizione di S_3. Pertanto il carattere dei cicli di lunghezza 4 è uguale al carattere delle trasposizioni di S_3, cioè 0.
Analogamente il carattere dei cicli di lunghezza 3 di S_4 è -1, poiché essi vengono associati ai cicli di lunghezza 3 di S_3. Quindi:

- $\chi_{\rho'''}(1) = \chi_{\rho'''}((12)(34)) = 2$;
- $\chi_{\rho'''}((12)) = \chi_{\rho'''}((1234)) = 0$;
- $\chi_{\rho'''}((123)) = -1$.

Notiamo che ρ''' è irriducibile: infatti

$$(\chi_{\rho'''}, \chi_{\rho'''}) = \frac{1}{24}(4 \cdot 1 + 0 \cdot 6 + 4 \cdot 3 + 1 \cdot 8 + 0 \cdot 6) = 1.$$

Quindi la tabella dei caratteri completa per S_4 è la seguente:

S_4		1 1	6 (12)	3 (12)(34)	8 (123)	6 (1234)
V	(1)	1	1	1	1	1
V'	(1)	1	-1	1	1	-1
V''	(3)	3	1	-1	0	-1
$V' \otimes V''$	(3)	3	-1	-1	0	1
V'''	(2)	2	0	2	-1	0

Bibliografia

[1] Serre, Jean-Pierre (1977), *"Linear Representations of Finite Groups"*, Springer-Verlag, New York Berlin Heidelberg.

[2] Fulton, William; Harris, Joe (1991), *"Representation Theory. A First Course"*, Springer-Verlag.

[3] Etingof, Pavel; Golberg, Oleg; Hensel, Sebastian; Liu, Tiankai; Schwendner, Alex; Vaintrob, Dmitry; Yudovina, Elena (10/01/2011), *"Introduction to representation theory"*.

[4] Artin, Michael (1991), *"Algebra"*, Prentice-Hall.