Università di Torino

QUADERNI DIDATTICI

del

Dipartimento di Matematica

Y. Chen, F. Ferrara

Teoria della Rappresentazione dei Gruppi

Quaderno # 18 - Giugno 2003

Prefazione

Nell'anno accademico 2001/2002 si è tenuto, presso il Dipartimento di Matematica dell'Università di Torino, un corso di Algebra rivolto agli studenti del Dottorato in Matematica. Il corso, tenuto dal prof. Chen e durato 30 ore, aveva lo scopo di introdurre i dottorandi ad un'argomento cruciale dell'algebra che riveste un'importanza fondamentale anche in altri rami della matematica. La teoria classica delle rappresentazioni dei gruppi finiti è stato il tema scelto. Le dispense del corso, curate da Francesca Ferrara, risultano nel presente quaderno.

L'argomento è sostanzialmente diviso in due sottoargomenti: la teoria delle algebre di dimensione finita e la teoria delle rappresentazioni dei gruppi finiti. La prima è centrata sul teorema di Maschke e sul teorema di Wedderburn per le algebre semisemplici; la seconda sviluppa, invece, la teoria dei caratteri ordinari per gruppi finiti. Nel capitolo 7, curato da Francesco Malaspina, viene sviluppata la tavola dei caratteri di A_5.
I prerequisiti per affrontare l'argomento sono l'algebra e la geometria dei due corsi di Algebra I e Geometria I, più la teoria elementare degli anelli e dei moduli. Il testo al quale il corso si è ispirato è il seguente: *Groups and Representations*, di J.L. Alperin e R.B. Bell.

Francesca Ferrara è iscritta al XVII ciclo del Dottorato in Matematica dell'Università di Torino. Yu Chen è professore associato al Dipartimento di Matematica dell'Università.

Indice

Capitolo 1

Moduli e rappresentazioni

Sia F un campo e V uno spazio vettoriale su F di dimensione finita.

Definizione 1.1 *Si dice che un gruppo G agisce su V linearmente, cioè un'azione di G su V è lineare, se:*

$$g \cdot (av + bw) = a \cdot g(v) + b \cdot g(w)$$

per ogni $g \in G, v, w \in V, a, b \in F$.

Proposizione 1.1 *Esiste una corrispondenza biunivoca tra l'insieme degli omomorfismi di G in $GL(V)$ e l'insieme delle azioni lineari di G su V, cioè:*

$$Hom\,(G, GL(V)) \overset{1-1}{\longleftrightarrow} \{azioni\ lineari\ di\ G\ su\ V\}$$

e, inoltre, si ha:

$$\rho \longmapsto g(v) = \rho(g)(v)$$

per ogni $\rho \in Hom\,(G, GL(V)), v \in V, g \in G$.

Definizione 1.2 *Una rappresentazione lineare di G in V è un omomorfismo*

$$G \longrightarrow GL(V)$$

ossia un omomorfismo

$$G \longrightarrow GL(n, F)$$

dove

$$n = dim V$$

n si chiama grado della rappresentazione.

Esempio
Supponiamo $|G| = m$, $F = \mathbf{C}$ e dim$V$=1.
Sia

$$\rho : G \longrightarrow GL(1, \mathbf{C}) = \mathbf{C}^*$$

una rappresentazione lineare di grado 1. Allora, poiché $g^m = 1$ per ogni $g \in G$, anche $\rho(g)^m = 1$ per ogni $g \in G$, cioè

$$\rho(G) \subseteq \{\text{radici m-esime dell'unità}\}$$

Quindi

$$\rho : G \longrightarrow S^2$$

e considerata la circonferenza S^2 di raggio unitario nel piano complesso $\mathbf{C} = \mathbf{R} \times \mathbf{R}$ basta moltiplicare $\frac{2\pi}{m}$ per un generatore di $\rho(G)$.

1.1 Moduli sinistri e destri

Definizione 1.3 ***(moduli sinistri e destri)*** *Siano R un anello con unità, cioè con elemento d'identità moltiplicativo 1, e M un gruppo abeliano rispetto alla somma.*
Si dice che M è un R-modulo sinistro se esiste una funzione

$$R \times M \longrightarrow M : (r, m) \longmapsto rm \in M$$

per ogni $r \in R$ e $m \in M$, che soddisfa le seguenti proprietà:

$$1 \cdot m = m$$
$$(r_1 + r_2)(m_1 + m_2) = r_1 m_1 + r_2 m_1 + r_1 m_2 + r_2 m_2$$
$$r_1(r_2 m) = (r_1 r_2)m$$

per ogni $m, m_1, m_2 \in M, r_1, r_2 \in R$.
Si dice che M è un R-modulo destro se esiste una funzione

$$M \times R \longrightarrow M : (m, r) \longmapsto mr \in M$$

per ogni $m \in M$ e $r \in R$, che soddisfa le seguenti proprietà:

$$m \cdot 1 = m$$
$$(m_1 + m_2)(r_1 + r_2) = m_1 r_1 + m_1 r_2 + m_2 r_1 + m_2 r_2$$
$$m(r_1 r_2) = (m r_1) r_2$$

per ogni $m, m_1, m_2 \in M, r_1, r_2 \in R$.
Sia S un altro anello con unità. Se M è un R-modulo sinistro e un S-modulo destro, si dice che M è un (R, S)-bimodulo.

Definizione 1.4 *Sia M un R-modulo. Si dice che M è finitamente generato se ogni suo elemento può essere scritto come una R-combinazione lineare di elementi di un qualche sottoinsieme finito di M.*

Definizione 1.5 *Siano M un R-modulo e N un sottogruppo di M. Si dice che N è un R-sottomodulo di M se:*

$$rn \in N$$

per ogni $r \in R, n \in N$.

Definizione 1.6 *Ogni R-modulo ha almeno due R-sottomoduli, cioè se stesso e il sottomodulo nullo* $\{0\}$. *Un R-modulo che non ha altri sottomoduli si dice R-modulo semplice.*

Definizione 1.7 *Sia M un R-modulo e N un suo sottomodulo. Possiamo costruire il gruppo quoziente M/N e dotarlo di una struttura di R-modulo definendo*

$$r\,(m+N) = rm + N$$

per ogni $r \in R, m+N \in M/N$.
M/N è un R-modulo, chiamato R-modulo quoziente di M su N.

Definizione 1.8 *Siano M un R-modulo,* N_1 *e* N_2 *due suoi sottomoduli. Definiamo la somma di* N_1 *e* N_2 *come segue:*

$$N_1 + N_2 = \{x + y : x \in N_1, y \in N_2\} \subseteq M$$

Questo è un sottomodulo di M, così come $N_1 \cup N_2$. *Se* $N_1 \cup N_2 = \{0\}$ *si dice che la somma di* N_1 *e di* N_2 *è diretta e si scrive* $N_1 \oplus N_2$ *al posto di* $N_1 + N_2$.

Questa è una nozione interna di somma diretta. Esiste anche una nozione esterna.

Definizione 1.9 *Siano M e N due R-moduli. Possiamo dotare* $M \times N$ *di una struttura di R-modulo attraverso la seguente operazione:*

$$r\,(m,n) = (rm, rn)$$

per ogni $m \in M, n \in N, r \in R$.
Possiamo inoltre scrivere $M \oplus N$ *al posto di* $M \times N$.
Le nozioni di somma diretta interna ed esterna possono essere estese a un qualsiasi numero finito di sottomoduli.
Diciamo infine che un sottomodulo N di un modulo M è un sommando diretto di M se esiste un sottomodulo N' di M tale che si possa scrivere $M = N \oplus N'$.

1.2 Omomorfismi di R-moduli

Definizione 1.10 *Siano M e N due R-moduli, sia* $\varphi : M \longrightarrow N$ *un omomorfismo di gruppi. Diciamo che* φ *è un omomorfismo di R-moduli se:*

$$\varphi\,(rm) = r\,\varphi\,(m)$$

per ogni $r \in R, m \in M$.

Come avviene nel caso dei gruppi, anche per i moduli si parla di monomorfismi, epimorfismi, isomorfismi, endomorfismi, automorfismi. $\operatorname{Ker}\varphi$ e $\operatorname{Im}\varphi$ sono sottomoduli rispettivamente di M e di N. Esiste per i moduli un teorema analogo al teorema fondamentale sugli omomorfismi fra gruppi.

Teorema 1.1 ***(teorema fondamentale sugli omomorfismi fra moduli)*** *Gli R-moduli $M/Ker\varphi$ e $Im\varphi$ sono isomorfi tramite la mappa indotta da φ.*

Lemma 1.1 ***(di Schur)*** *Un omomorfismo non banale fra due R-moduli semplici è sempre un isomorfismo.*

Dim. Siano M e N due R-moduli semplici e sia $\varphi : M \longrightarrow N$ un omomorfismo di R-moduli. Poiché $\mathrm{Ker}\,\varphi$ è un sottomodulo di M, deve essere $\mathrm{Ker}\,\varphi = M$, nel qual caso $\varphi = 0$, o $\mathrm{Ker}\,\varphi = \emptyset$. Analogamente, $\mathrm{Im}\,\varphi$ è un sottomodulo di N; quindi, o $\mathrm{Im}\,\varphi = 0$, da cui segue $\varphi = 0$, o $\mathrm{Im}\,\varphi = N$.
In conclusione, se $\varphi \neq 0$ allora φ è un isomorfismo.

Osservazione
Dati due R-moduli M e N, l'insieme degli omomorfismi di R-moduli da M in N

$$\mathrm{Hom}_R(M,N) = \{R\text{-omomorfismi da } M \text{ in } N\}$$

è un gruppo abeliano rispetto all'operazione somma definita come segue:

$$(\varphi + \rho)(m) := \varphi(m) + \rho(m)$$

per ogni $\varphi, \rho \in \mathrm{Hom}_R(M,N), m \in M$.
Sia ora S un altro anello con unità. Se M è (R,S)-bimodulo, $\mathrm{Hom}_R(M,N)$ è un S-modulo definito da:

$$(s\,\varphi)(m) := \varphi\,(ms)$$

per ogni $s \in S, \varphi \in \mathrm{Hom}_R(M,N), m \in M$.

Si può verificare che, per due spazi vettoriali V e W su un campo F, $\mathrm{Hom}_F(V,W)$ è uno spazio vettoriale su F e che $\dim_F \mathrm{Hom}_F(V,W) = \dim_F V \cdot \dim_F W$.

1.3 Prodotto tensoriale

Definizione 1.11 *Un gruppo abeliano libero generato su un insieme X è un gruppo abeliano rispetto alla somma costituito da elementi della forma*

$$\left\{ \sum_{i<\infty} x_i - \sum_{j<\infty} y_j \ : \ x_i, y_j \in X \right\}$$

tali che:

$$\sum_{i=1}^{m} x_i - \sum_{j=1}^{n} y_j = 0$$

se e solo se $m = n$ e, inoltre, con un riordinamento degli indici, si ha

$$x_i = y_i$$

per $1 \leq i \leq n$.

Definizione 1.12 ***(prodotto tensoriale)*** *Siano M un S-modulo destro e N un S-modulo sinistro. Sia L un gruppo libero abeliano sull'insieme $M \times N$ e sia:*

$$K := \langle (m_1+m_2,n)-(m_1,n)-(m_2,n), (m_1,n_1+n_2)-(m_1,n_1)-(m_1,n_2), (ms,n)-(m,sn)\rangle$$

per ogni $m, m_1, m_2 \in M, n, n_1, n_2 \in N, s \in S$.
L'insieme

$$M \otimes_S N \ := \ L/K$$

è il tensore di M e N su S.
Sia ora $\pi : L \longrightarrow L/K$ l'omomorfismo naturale.
Per $m \in M, n \in N$ si ha

$$m \otimes n \ := \ \pi\left((m,n)\right)$$

Allora:

$$M \otimes_S N = \left\{ \sum_{i<\infty} m_i \otimes n_i \ : \ m_i \in M, n_i \in N \right\}$$

Sono soddisfatte le seguenti identità:

$$\begin{gathered}(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n \\ m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2 \\ ms \otimes n = m \otimes sn \\ -(m \otimes n) = -m \otimes n = m \otimes (-n)\end{gathered}$$

per ogni $m, m_1, m_2 \in M, n, n_1, n_2 \in N, s \in S$.
Se M è anche un R-modulo sinistro, $M \otimes_S N$ è un R-modulo sinistro definito dalla seguente operazione:

$$r(m \otimes n) = rm \otimes n$$

per ogni $r \in R$.

1.4 Prodotto tensoriale di morfismi

Definizione 1.13 ***(prodotto tensoriale di morfismi)*** *Dati $f : M \longrightarrow M'$, morfismo di (R,S)-bimoduli, e $g : N \longrightarrow N'$, morfismo di S-moduli, si ha che*

$$f \otimes g : M \otimes_S N \longrightarrow M' \otimes_S N' : m \otimes n \longmapsto f(m) \otimes g(n)$$

è un morfismo di R-moduli.

Proposizione 1.2 *Siano U e V due spazi vettoriali su un campo F, entrambi di dimensione finita. Sia inoltre*

$$U^* = Hom_F(U, F)$$

Allora la funzione:

$$\gamma : U^* \otimes_F V \longrightarrow Hom_F(U, V)$$

che, per ogni $\varphi \in U^*, u \in U, v \in V$*, opera nel modo seguente*

$$\varphi \otimes v \longmapsto \gamma(\varphi \otimes v) : u \mapsto \varphi(u)v$$

è un isomorfismo di spazi vettoriali su F.

Dim. γ, estendendo linearmente, è un F-omomorfismo.
γ è iniettivo perché prende un elemento di $U^* \otimes V$ della forma

$$\sum_i f_i \otimes v_i$$

con $v_i \in V$, e lo trasforma come segue:

$$\gamma\left(\sum_i f_i \otimes v_i\right)(u_j) = \sum_i \gamma(f_i \otimes v_i)(u_j) = \sum_i f_i(u_j)v_i = v_j$$

Perciò:

$$\gamma\left(\sum_i f_i \otimes v_i\right)(u_j) = 0, v_j = 0\ \forall j \Rightarrow \sum_i f_i \otimes v_i = 0$$

Questo implica che γ è iniettivo. γ è però anche suriettivo. Considerate, infatti, $\{u_1, ..., u_n\}$, base di U, e $\{f_1, ..., f_n\}$, la base duale in U^*, e presi $\sigma \in \mathrm{Hom}_F(U, V)$ e $u = \sum_{i=1}^n a_i u_i \in U$, si ha:

$$\gamma\left(\sum_{i=1}^n f_i \otimes \sigma(u_i)\right)(u) = \sum_{i=1}^n f_i(u)\,\sigma(u_i) = \sum_{i=1}^n a_i\,\sigma(u_i) = \sigma\left(\sum_{i=1}^n a_i u_i\right) = \sigma(u)$$

da cui segue

$$\gamma\left(\sum_{i=1}^n f_i \otimes \sigma(u_i)\right) = \sigma$$

Capitolo 2

F-algebre

Definizione 2.1 *Sia F un campo. Un'algebra su F, o semplicemente una F-algebra, A è un insieme A dotato di una struttura di anello e con una struttura di spazio vettoriale su F che condivide la stessa operazione di somma; inoltre, è tale che valga la seguente relazione:*

$$q\,(a\,b) = (q\,a)\,b = a\,(q\,b)$$

per ogni $a, b \in A, q \in F$.

Esempio
Si consideri $M_n(F) = \{\text{matrici } n \times n \text{ su } F\}$.

- $M_n(F)$ è un anello rispetto alla somma e al prodotto;
- $M_n(F)$ è uno spazio vettoriale.

Inoltre, si ha:

$$q\,(a_{ij}) = (q\,a_{ij})$$

per ogni $q \in F$ e $(a_{ij}) \in M_n(F)$.
Quindi, $M_n(F)$ è una F-algebra.

Esempio
Siano G un gruppo e F un campo. Sia

$$F[G] = \{\sum_{g \in G} q_g g \,:\, q_g \in F\}$$

dove si considera un numero finito di elementi g in G.
Si definiscono due operazioni in $F[G]$, somma e prodotto. Siano $\sum_{g \in G} q_g g$ e $\sum_{g \in G} p_g g$ due elementi qualunque di $F[G]$.
La somma si definisce come segue:

$$\sum_{g \in G} q_g g + \sum_{g \in G} p_g g := \sum_{g \in G} (q_g + p_g) g$$

Il prodotto si definisce come segue:

$$\left(\sum_{g_1\in G} q_{g_1} g_1\right) \cdot \left(\sum_{g_2\in G} p_{g_2} g_2\right) := \sum_{g_1,\, g_2\in G} q_{g_1} p_{g_2} g_1 g_2 = \sum_{g_1\in G} \left(\sum_{g\in G} q_g p_{g^{-1}g_1}\right) g_1$$

L'insieme $F[G]$, con le due operazioni così definite, è una F-algebra, che si chiama *gruppo algebra*. Se G è un gruppo finito, cioè $|G| < \infty$, allora la dimensione di $F[G]$, per definizione, è uguale alla dimensione dello spazio vettoriale $F[G]$ su F:

$$\dim F[G] = |G|$$

2.1 F[G]-moduli e rappresentazione di G

Osservazione
Se G agisce linearmente su uno spazio vettoriale V su F allora V è un $F[G]$-modulo. Si ha cioè che per ogni $v \in V$:

$$\left(\sum_{g\in G} q_g g\right) v := \sum_{g\in G} q_g\,(gv)$$

Vale anche il viceversa, per cui se M è un $F[G]$-modulo allora M è anche uno spazio vettoriale su F. Si ha cioè:

$$qv := q \cdot 1_G v$$

per ogni $q \in F, v \in M$.

Osservazione
Se si considera V spazio vettoriale di dimensione finita, allora V risulta anche essere finitamente generato.
In generale, non vale il viceversa, ovvero se M è finitamente generato *non* è detto che M sia spazio vettoriale di dimensione finita. Il viceversa è garantito sotto opportune ipotesi sul gruppo G, come si può vedere con il seguente lemma.

Lemma 2.1 *Sia G un gruppo di cardinalità finita. Allora:*
M è un $F[G]$-modulo finitamente generato se e solo se M è uno spazio vettoriale di dimensione finita su F.

Dim. L'implicazione verso sinistra è ovvia.
Dimostriamo quindi l'implicazione verso destra.
Siano $\{v_1, ..., v_n\}$ i generatori di M, $F[G]$-modulo. Allora:

$$\{gv_i : \forall g \in G, 1 \le i \le n\}$$

è una base per M come spazio vettoriale su F.

Proposizione 2.1 *Siano G un gruppo, di cardinalità finita, e F un campo. Allora:*

$$\{F[G]\text{-moduli finitamente generati}\}$$
$$\updownarrow$$
$$\{\text{azioni lineari di } G \text{ su } F\text{-spazi vettoriali di dimensione finita}\}$$
$$\updownarrow$$
$$\{\text{rappresentazioni lineari di } G\}$$

cioè esiste una corrispondenza biunivoca tra l'insieme degli $F[G]$-moduli finitamente generati, l'insieme delle azioni lineari di G su spazi vettoriali su F di dimensione finita e l'insieme delle rappresentazioni lineari di G.

Dim. Sia V un $F[G]$-modulo finitamente generato. Allora la dimensione di V su F è finita per il Lemma 2.1 e, inoltre, la funzione

$$G \times V \longrightarrow V$$

che si ottiene restringendo su $G \times V$ l'omomorfismo fra moduli

$$FG \times V \longrightarrow V$$

è un'azione lineare di G su V.
Viceversa, supponiamo che V sia uno spazio vettoriale su F di dimensione finita sul quale G agisce linearmente. Allora diamo a V una struttura di $F[G]$-modulo definendo

$$\left(\sum_{g\in G} \alpha_g g\right) v = \sum_{g\in G} \alpha_g (gv)$$

per $v \in V$ e $\sum_{g\in G} \alpha_g g \in F[G]$.
Con ciò la proposizione è dimostrata.

Osservazione
Sappiamo che se V è uno spazio vettoriale e $W \subset V$ un suo sottospazio, allora esiste $W' \subset V$ tale che $V = W \oplus W'$. Si procede allo stesso modo per studiare gruppi, anelli, moduli: ognuno si può scrivere come somma diretta di altri gruppi, anelli, moduli. Vogliamo studiare come si comportano gli $F[G]$-moduli rispetto alla somma diretta: ci aiuta il seguente teorema (da qui in avanti si parlerà sempre di moduli finitamente generati).

Teorema 2.1 ***(Maschke)*** *Sia F un campo, con CharF = 0 oppure CharF coprimo con $|G|$, cioè CharF non divide $|G|$, che è finita (dove CharF indica la caratteristica di F). Allora, per ogni F[G]-sottomodulo V di un F[G]-modulo U dato esiste un F[G]-sottomodulo V' di U tale che*

$$U = V \oplus V'$$

Dim. Come spazio vettoriale U si può scrivere come somma diretta di due suoi sottospazi, cioè $U = V \oplus W$. Si consideri ora la seguente funzione

$$p : U = V \oplus W \longrightarrow V : u = v + w \longmapsto v \in V$$

proiezione canonica.
Si definisce

$$p' : U \longrightarrow U : u \longmapsto p'(u) := \frac{1}{\|G\|} \sum_{\forall g \in G} g\, p\,(g^{-1}u)$$

e si ha:

1. p' è ben definita come funzione ed è anche un omomorfismo di gruppi abeliani e di spazi vettoriali;

2. p' é un omomorfismo di $F[G]$-moduli.

Per verificare la 2. basta verificare che:

$$p'(xu) = x\, p'(u) \qquad (*)$$

per ogni $x \in G$.
In (*), si dovrebbe considerare un elemento x di $F[G]$ ma basta prenderlo in G perché ogni elemento di $F[G]$ è combinazione finita di elementi di G.
Dimostriamo quindi (*).

$$p'(xu) = \frac{1}{\|G\|} \sum_{\forall g \in G} g\, p\,(g^{-1}xu) = \frac{1}{\|G\|} \sum_{\forall g \in G} x\, x^{-1}\, g\, p\,(g^{-1}xu)$$

$$= \frac{1}{\|G\|} \sum_{\forall h \in G} x\, h\, p\,(h^{-1}u) = \frac{1}{\|G\|}\, x \sum_{\forall h \in G} h\, p\,(h^{-1}u) = xp'(u)$$

dove la seconda uguaglianza deriva dal fatto che $xx^{-1} = 1$, la terza dal fatto di aver posto $x^{-1}g = h$ (per cui $x^{-1}g = h \in G$ e $g^{-1}x = h^{-1} \in G$ sono uno l'inverso dell'altro) e la quarta dal fatto che x non dipende da h.
Allora, Kerp', nucleo di un omomorfismo tra moduli, è un $F[G]$-sottomodulo di U.
Ora:

$$p'(u) = \frac{1}{\|G\|} \sum_{\forall h \in G} h\, p\,(h^{-1}u) \in V$$

poiché $p\,(h^{-1}u) \in V$.
Si ha quindi che, per ogni $u \in U$

$$p'(u) \in V$$

e, per ogni $v \in V$

$$p'(v) = v$$

Allora, per ogni $u \in U$, si ha:

$$p'^2(u) = p'(u)$$

che equivale a

$$p'(u) - p'^2(u) = 0$$

dove con p'^2 si intende p' applicata due volte.
Da qui segue:

$$(p' - p'^2)(u) = 0$$

cioè

$$p'[(\mathbf{1} - p')(u)] = 0$$

dove $\mathbf{1}$ è l'identità.
Quindi, $(\mathbf{1} - p')U \subseteq \mathrm{Ker}p'$.
Ora, sia $u \in U$. Si ha

$$u = u + p'(u) - p'(u) = p'(u) + (\mathbf{1} - p')(u)$$

con $p'(u) \in V$ e $(\mathbf{1} - p')(u) \in (\mathbf{1} - p')U \subseteq \mathrm{Ker}p'$.
Allora, si può scrivere

$$U = V + \mathrm{Ker}p'$$

e, tenendo conto del fatto che

$$V \cap \mathrm{Ker}p' = \{0\}$$

poiché $p'(v) = v$, si ha

$$U = V \oplus \mathrm{Ker}p'$$

Ponendo V' dell'enunciato del teorema uguale a $\mathrm{Ker}p'$ si ha la tesi.

Nel caso degli spazi vettoriali ci si ferma nella decomposizione quando si ha la somma diretta di spazi vettoriali di dimensione 1. Nel caso dei moduli invece ci si ferma con sottomoduli semplici.

Definizione 2.2 *Un modulo si chiama semisemplice se è somma diretta dei suoi sottomoduli semplici.*

Corollario *(del Teorema di Maschke)* *Sia F un campo, con CharF = 0 oppure CharF che non divide |G|, che è finita. Allora, ogni F[G]-modulo é semisemplice.*

Come conseguenza del Teorema di Maschke si può dire che se F è un campo la cui caratteristica non divide l'ordine di un gruppo finito G allora ogni $F[G]$-modulo può essere scritto come una somma diretta di moduli semplici. E' possibile indagare la struttura delle F-algebre di dimensione finita che abbiano questa proprietà e, in tal modo, classificarle. Per fare ciò si ricorre alla *Teoria di Wedderburn.*

Capitolo 3

Teoria di Wedderburn

Sia A una F-algebra. Vale il seguente lemma.

Lemma 3.1 *Per un A-modulo M, sono equivalenti le tre seguenti condizioni.*

1. *Ogni sottomodulo di M è un addendo diretto.*

2. *M è semisemplice.*

3. *M è una somma di sottomoduli semplici.*

Dim. (1) implica (2) e (2) implica (3) sono ovvie. Dimostriamo allora che (3) implica (2). Consideriamo il caso semplice in cui M sia somma di due soli sottomoduli semplici N_i, con i = 1, 2, cioè $M = N_1 + N_2$. $N_1 \cap N_2$ è sottomodulo sia di N_1 sia di N_2. Quindi $N_1 \neq N_2$, da cui segue $N_1 \cap N_2 = \{0\}$, cioè $M = N_1 \oplus N_2$ è semisemplice.
Dimostriamo infine che (2) implica (1).
Sia $M = N_1 \oplus ... \oplus N_r$, con N_i semplici. $N \subset M$ è un sottomodulo di M.
Allora

$$N = \left\{ a_{i_1} + a_{i_2} + ... + a_{i_s} : \text{qualche } a_{i_j} \in N_{i_1} \right\}$$

Se $a_{i_l} \neq 0$ si considera la proiezione canonica: p_{i_l}: $M \to N_{i_l}$. $p_{i_l}(N) \supset \{0\}$. $p_{i_l}(N)$ è un sottomodulo di N_{i_l}, perciò $p_{i_l}(N) = N_{i_l}$. Ma $N_{i_l} \subseteq N$; allora alla fine si trova che

$$N = N_{i_*} \oplus ... \oplus N_{i_*}$$

e

$$N' = \oplus N_j$$

con $j \notin \{i_*\}$.
Si avrà quindi $M = N \oplus N'$.

Lemma 3.2 *Sottomoduli e quozienti di un modulo semisemplice sono semisemplici.*

Dim. Sia M un A-modulo semisemplice. Per il Lemma 3.1 e per il primo teorema sugli omomorfismi fra moduli, si ha che ogni sottomodulo di M è isomorfo a un modulo quoziente di M. E' così sufficiente dimostrare che i moduli quozienti di M sono semisemplici. Sia M/N un modulo quoziente arbitrario, e sia $\eta : M \longrightarrow M/N$ la proiezione canonica. Poiché M è semisemplice, dal Lemma 3.1 segue che M si può scrivere come somma di sottomoduli semplici, cioè

$$M = S_1 + ... + S_n$$

Si deve quindi avere

$$M/N = \eta(M) = \eta(S_1) + ... + \eta(S_n)$$

Ora, però, ogni $\eta(S_i)$ è isomorfo a un modulo quoziente di S_i per ogni $i = 1, ..., n$ e, come tale, deve essere o nullo o semplice. Perciò, M/N è una somma di moduli semplici e, per il Lemma 3, è semisemplice.

Proposizione 3.1 *Un'algebra A è semisemplice se e solo se come A-modulo è semisemplice.*

Lemma 3.3 *Se A è semisemplice allora tutti gli A-moduli (finitamente generati) sono semisemplici.*

Dim. Sia M un A-modulo, di generatore $\{m_1, ..., m_r\}$. La funzione

$$A^r = \underbrace{A \oplus ... \oplus A}_{r \text{ volte}} \longrightarrow M : \sum_{i=1}^{r} a_i \longmapsto \sum_{i=1}^{r} a_i m_i$$

è un epimorfismo di A-moduli. M quindi è isomorfo ad un quoziente dell'A-modulo semisemplice A^r e, per il Lemma 4, è semisemplice.

Proposizione 3.2 *Sia A un'algebra semisemplice. Come A-modulo, A può essere scritta come $A = S_1 \oplus ... \oplus S_r$, dove gli S_i sono A-moduli semplici. Allora, ogni A-modulo semplice è isomorfo ad un qualche S_i.*

Dim. Sia S un A-modulo semplice. Fissato $s \in S$ non nullo, definiamo l'omomorfismo di A-moduli

$$\varphi : A \longrightarrow S : a \longmapsto as$$

per ogni $a \in A$.
Tale funzione è un omomorfismo di A-moduli. Allora, per la semplicità di S_i e S, $\varphi(S_i)$ è uguale a $\{0\}$ oppure uguale a S. Se $\varphi(S_i) = S$, per il Lemma di Schur si ha $S_i \cong S$.

Proposizione 3.3 *Sia M un modulo semisemplice. Se vale*

$$M \cong S_1 \oplus S_2 \oplus ... \oplus S_r \cong T_1 \oplus T_2 \oplus ... \oplus T_l$$

dove S_i e T_j sono moduli semplici. Allora, si ha

$$r = l$$

e, per almeno un riordinamento degli indici:

$$S_i \cong T_i$$

per $1 \leq i \leq r$.

Dim. Si procede per induzione su r.
Se $r = 1$, M è semplice. Allora $M = S_1 = T_1$.
Se $r > 1$, sia $p_i : M \longrightarrow T_i$ la proiezione canonica per ogni i. Per $1 \leq i \leq r$, esiste almeno un T_i tale che

$$p_i(S_1) \cap T_i \supset \{0\}$$

Riordinando gli indici poniamo $i = 1$. Dalla semplicità di T_1 segue che $p_1(S_1) = T_1$. Si ha quindi

$$\bigoplus_{i=2}^{r} S_i \cong M/S_1 \cong M/T_1 \cong \bigoplus_{j=2}^{l} T_j$$

Per l'ipotesi induttiva si ottiene $r = l$ e $S_i \cong T_i$ (per $i = 1$, $p_1|_{S_1} : S_1 \tilde{\to} T_1$ dal Lemma di Schur).

Definizione 3.1 *Un'algebra è semplice se non ha alcun ideale bilatero non banale.*

Lemma 3.4 *Un'algebra semplice è semisemplice.*

Dim. Siano $a \in A$ e $S \subseteq A$ un A-sottomodulo semplice dell'algebra semplice A.
L'omomorfismo che opera come segue

$$S \longrightarrow Sa : x \longmapsto xa$$

per ogni $x \in S$, implica che Sa sia un A-sottomodulo semplice di A oppure $Sa = 0$, cioè il caso banale.
In entrambi i casi, se Σ è somma di tutti gli A-sottomoduli semplici, si ha

$$Sa \subseteq \Sigma$$

per ogni sottomodulo semplice S e per ogni $a \in A$; Quindi, Σ è un ideale destro di A (Σ è ovviamente un ideale di sinistra), cioè Σ è un ideale bilatero. Allora, essendo A semplice e $\Sigma \neq 0$, A è uguale a Σ che, come somma di moduli semplici, è semisemplice (per il Lemma 3 e il Lemma 5).

Teorema 3.1 *Siano D un'algebra di divisione, $n \in \mathbf{N}$. Allora $M_n(D)$ è un'algebra semplice.*

Dim. In primo luogo, occorre precisare che un'algebra D è detta *algebra di divisione* se gli elementi non nulli di D formano un gruppo con la moltiplicazione.
Sia ora $M \neq 0 \in M_n(D)$. Basta dimostrare che l'ideale bilatero J generato da M è uguale a $M_n(D)$.
M è diverso da 0; allora

$$M = \begin{pmatrix} & \vdots & \\ \cdots & x & \cdots \\ & \vdots & \end{pmatrix}_{n \times n}$$

dove $x \neq 0$ è l'elemento che si trova all'incrocio tra l'i-esima riga e la j-esima colonna, per qualche i e j.
Sia ora $J = \langle M \rangle$. Segue che

$$E_{ji}(x^{-1}) M E_{jj}(1) = E_{jj}(1) \in J$$

Per $1 \leq r, s \leq n$, si può scrivere

$$E_{rs}(1) \cdot E_{jj}(1) \in J$$

con

$$E_{rs}(1) = \begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 0 & \cdots\cdots & 1 & & & & \\ & & & \vdots & 1 & & \vdots & & & \\ & & & \vdots & & \ddots & \vdots & & & \\ & & & \vdots & & & 1 \; \vdots & & & \\ & & & 1 & \cdots\cdots & & 0 & & & \\ & & & & & & & 1 & & \\ & & & & & & & & \ddots & \\ & & & & & & & & & 1 \end{pmatrix}$$

dove la matrice centrale è delimitata dalle righe j-esima e r-esima e dalle colonne j-esima e s-esima. Inoltre

$$E_{jj}(1) = \begin{pmatrix} 1 & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & 1 & & & & & & & \\ & & & 0 & \cdots\cdots & 1 & & & & \\ & & & \vdots & 0 & \vdots & & & & \\ & & & \vdots & \ddots & \vdots & & & & \\ & & & \vdots & & 0 & \vdots & & & \\ & & & 1 & \cdots\cdots & 0 & & & & \\ & & & & & & 1 & & & \\ & & & & & & & \ddots & & \\ & & & & & & & & 1 & \end{pmatrix}$$

dove la matrice centrale è delimitata dalle righe e dalle colonne s-esima e j-esima.
Da qui segue $J = M_n(D)$, poiché J contiene tutti i generatori $\{E_{rs}(1)\}$.

Proposizione 3.4 *Sia D un'algebra di divisione. Allora ogni $M_n(D)$-modulo semplice è isomorfo a*

$$D^n = \left\{ \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} : d_i \in D \right\}$$

Dim. D^n è un $M_n(D)$-modulo semplice perché per qualsiasi $d \in D^n$, con $d \neq 0$, si ha

$$M_n(D) \cdot d = D^n$$

Come $M_n(D)$-modulo

$$M_n(D) = C_1 \oplus ... \oplus C_n$$

dove

$$C_i = \left\{ \begin{pmatrix} 0 & \cdots & 0 & d_1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & d_n & 0 & \cdots & 0 \end{pmatrix} : d_i \in D \right\} \cong D^n$$

Per la Proposizione 5, ogni $M_n(D)$-modulo semplice è isomorfo ad un C_i, quindi a D^n.

Proposizione 3.5 *Siano $D_1, D_2, ..., D_r$ delle F-algebre di divisione. Allora*

$$\bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

con $n_i \in \mathbf{N}$, per $1 \leq i \leq r$, è un'algebra semisemplice con esattamente r classi isomorfe di moduli semplici e esattamente 2^r ideali bilateri, cioè tutte le somme

$$\bigoplus_{j \in J} M_{nj}(D_j)$$

per $J \subseteq \{1, ..., r\}$.

Dim. Prima parte: dato un $M_{n_j}(D_j)$-modulo M, si definisce un $\bigoplus_{i=1}^{r} M_{n_i}(D_i)$-modulo come segue:

$$(m_1 + ... + m_r) \cdot m := m_j m$$

per $m_1 + m_2 + ... + m_r \in \bigoplus_i M_{n_i}(D_i)$ e $m \in M$.

Quindi il $M_{n_j}(D_j)$-modulo semplice è anche un $\bigoplus_i M_{n_i}(D_i)$-modulo semplice.

$M_{n_j}(D_j)$ è una somma di sottomoduli semplici, isomorfa a $D_j^{n_j}$ per ogni j. Allora

$$\bigoplus_i M_{n_i}(D_i)$$

è una somma di sottomoduli semplici (isomorfi a $D_i^{n_i}$ per $1 \leq i \leq r$). Da ciò segue che

$$\bigoplus_i M_{n_i}(D_i)$$

è un'algebra semisemplice e, quindi (per la Proposizione 3.2), i suoi sottomoduli semplici sono isomorfi ad un $D_i^{n_i}$ per $1 \leq i \leq r$. Questo implica che esistono r classi isomorfe di sottomoduli semplici.
La seconda parte della dimostrazione è una facile conseguenza del Teorema 3.1 e del Lemma seguente.

Lemma 3.5 *Se $B = B_1 \oplus ... \oplus B_n$ è una somma diretta di algebre allora gli ideali bilateri di B sono gli insiemi della forma:*

$$J_1 \oplus ... \oplus J_n$$

dove J_i è un'ideale bilatero di B_i.

Dim. Dato $J \trianglelefteq B$, si ha

$$\bigoplus_i (J \cap B_i) \subseteq J$$

Siano ora $b_1 + ... + b_n \in J$ e inoltre $l_1 = 0 + ... + 1_{B_i} + 0 + ... + 0$. Allora

$$(b_1 + ... + b_n)\, l_i = b_i$$

da cui segue

$$b_i \in J_i = B_i \cap J$$

e inoltre

$$J = J_1 \oplus ... \oplus J_n$$

(sempre con $J_i = B_i \cap J$).

Proposizione 3.6 *Sia M un A-modulo. Allora*

$$End_A(M) = \{\textit{endomorfismi dell'}A\textit{-modulo } M \textit{ in se stesso}\}$$

è una F-algebra definita da:

$$(q \cdot \varphi)(am) = \varphi\,(q\,a\,m)$$
$$(\varphi \cdot \varphi')(m) = \varphi\,(\varphi'(m))$$

per ogni $q \in F, a \in A, m \in M$ e $\varphi, \varphi' \in End_A(M)$.

$End_A(M)$ è chiamata *algebra endomorfismo* di M.

Lemma 3.6 *Siano $S_1, ..., S_r$ A-moduli semplici distinti. Siano inoltre*

$$U_i = S_i \oplus ... \oplus S_i$$

per ogni i = 1, ..., 3, e

$$U = U_1 \oplus ... \oplus U_r$$

Allora

$$End_A(U) = End_A(U_1) \oplus ... \oplus End_A(U_r)$$

Dim. 1) Dato un $\varphi \in End_A(U)$, si ha che, fissato i, $\varphi(U_i) \subseteq U_i$.
2) Si definisce la seguente funzione:

$$End_A(U) \longrightarrow End_A(U_1) \oplus End_A(U_2) \oplus ... \oplus End_A(U_r)$$

che opera come segue:

$$\varphi \longmapsto \varphi|_{U_1} + \varphi|_{U_2} + ... + \varphi|_{U_r}$$

e viceversa:

$$(\varphi_1, \varphi_2, ..., \varphi_r) \longmapsto \varphi_1 + \varphi_2 + ... + \varphi_r$$

Tale funzione è una suriezione e un monomorfismo di A-moduli; da ciò segue la tesi.

Lemma 3.7 *Sia S un A-modulo semplice. Allora, per ogni $n \in \mathbf{N}$*

$$End_A(\underbrace{S \oplus ... \oplus S}_{n \text{ volte}}) \cong M_n(End_A(S))$$

Dim. Si identifichi la somma diretta degli S con un vettore di n componenti, cioè

$$S \oplus ... \oplus S \cong \left\{ \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} : s_i \in S \right\}$$

Si può ora definire la funzione

$$M_n(End_A(S)) \longrightarrow End_A(S \oplus ... \oplus S)$$

che opera nel modo seguente

$$(\varphi_{ij})_{n\times n} \longmapsto (\varphi_{ij}) : \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \mapsto (\varphi_{ij}) \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}$$

e viceversa

$$\psi \in End_A \left\{ \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} : s_i \in S \right\} \longmapsto (\psi_{ij})_{n\times n}$$

dove le $\psi_{ij} : S \longrightarrow S$ sono definite da:

$$\psi \begin{pmatrix} s \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \psi_{11}(s) \\ \psi_{21}(s) \\ \vdots \\ \psi_{n1}(s) \end{pmatrix}, ..., \ \psi \begin{pmatrix} 0 \\ 0 \\ \vdots \\ s \end{pmatrix} = \begin{pmatrix} \psi_{1n}(s) \\ \psi_{2n}(s) \\ \vdots \\ \psi_{nn}(s) \end{pmatrix}$$

Si può infine verificare che le due corrispondenze sono l'una inversa dell'altra.

Se S è un A-modulo semplice segue immediatamente dal Lemma di Schur che $\mathrm{End}_A(S)$ è un'algebra di divisione. Se il campo F di partenza è algebricamente chiuso allora possiamo essere più precisi sulla struttura di $\mathrm{End}_A(S)$, come si può vedere dal Lemma seguente.

Lemma 3.8 *Se F è algebricamente chiuso allora per un A-modulo semplice S si ha*

$$End_A(S) \cong F$$

Dim. Dato $\varphi \in End_A(S)$, φ è anche una trasformazione lineare invertibile sullo spazio vettoriale di dimensione finita S su F. Sia $\lambda_\varphi \in F$ un autovalore non nullo di φ (un tale autovalore esiste sempre, poiché F è algebricamente chiuso). Si ha che

$$\varphi - \lambda_\varphi I \in End_A(S)$$

ha nucleo non nullo, cioè non è invertibile. Allora

$$\varphi = \lambda_\varphi I$$

poiché S è semplice e $\mathrm{End}_A(S)$ è un'algebra di divisione. La funzione

$$End_A(S) \longrightarrow F : \varphi \longmapsto \lambda_\varphi$$

è quindi un isomorfismo.

Definizione 3.2 *Data un'algebra A, l'algebra opposta di A, A^{op}, è un'algebra che soddisfa le seguenti condizioni:*

- *come insieme:*
$$A^{op} = A$$
- *come spazio vettoriale:*
$$A^{op} = A$$
- *come anello:*
$$a \circ b := b \cdot a$$
(in A) per $a, b \in A^{op}$

Si deve notare che se A è un'algebra di divisione anche A^{op} è un'algebra di divisione.

Proposizione 3.7
$$(A^{op})^{op} \cong A$$
$$(\bigoplus_i A_i)^{op} \cong \bigoplus_i A_i^{op}$$
$$A^{op} \cong End_A(A)$$

Dim. Per $a \in A$, sia
$$\rho_a : A \longrightarrow A : x \longmapsto xa$$
$\rho_a \in End_A(A)$. Quindi
$$End_A(A) = \{\rho_a : \forall a \in A\}$$
Infatti, per $\varphi \in End_A(A)$
$$\varphi(x) = x\varphi(1)$$
Allora
$$\varphi = \rho_{\varphi(1)}$$
Considerata ora la funzione
$$A^{op} \longrightarrow End_A(A) : a \longmapsto \rho_a$$
si ha che essa soddisfa la seguente relazione tra elementi:
$$a \circ b \ (= b \cdot a) \longmapsto \rho_{a \circ b} = \rho_{b \cdot a} = \rho_a \cdot \rho_b$$
Con ciò la tesi è dimostrata.

Lemma 3.9 *Data un'algebra A, si ha*
$$M_n(A)^{op} \cong M_n(A^{op})$$
per ogni $n \in \mathbf{N}$.

Dim. Si consideri la funzione così definita:

$$M_n(A)^{op} \xrightarrow{\varphi} M_n(A^{op}) : X \longmapsto X^t$$

dove X^t è la trasposta della matrice X. Si tratta di una funzione biiettiva.
Ora, per $X, Y \in M_n(A)^{op}$, con $X = (x_{ij})$ e $Y = (y_{ij})$, si ha

$$\varphi(X \circ Y) = \varphi(Y \cdot X) = (YX)^t = (\sum_l y_{il}x_{lj})^t$$

mentre, in $M_n(A^{op})$, si ha

$$\varphi(X) \cdot \varphi(Y) = X^t \cdot Y^t = (\sum_l y_{jl}x_{li})^t$$

dove le due sommatorie finali coincidono. Da ciò segue che φ è un isomorfismo.

Teorema 3.2 ***(Wedderburn)*** *Un'algebra A è semisemplice se e solo se è isomorfa ad una somma diretta delle algebre di matrici su algebre di divisione.*

Dim. L'implicazione verso sinistra è già stata dimostrata con la Proposizione 3.5.
Dimostriamo che vale l'implicazione verso destra.
A è semisemplice. Allora

$$A = U_1 \oplus ... \oplus U_r$$

dove ogni U_i è una somma diretta di n_i A-moduli semplici S_i, con $S_i \neq S_j$ per $i \neq j$. Si ha allora

$$\begin{aligned} A^{op} &\cong End_A(A) \cong End_A(U_1) \oplus ... \oplus End_A(U_r) \\ &= End_A(\bigoplus_{n_1} S_1) \oplus ... \oplus End_A(\bigoplus_{n_r} S_r) \\ &\cong M_{n_1}(End_A(S_1)) \oplus ... \oplus M_{n_r}(End_A(S_r)) \end{aligned}$$

Quindi:

$$\begin{aligned} A &\cong [M_{n_1}(End_A(S_1)) \oplus ... \oplus M_{n_r}(End_A(S_r))]^{op} \\ &\cong M_{n_1}(End_A(S_1))^{op} \oplus ... \oplus M_{n_r}(End_A(S_r))^{op} \\ &\cong M_{n_1}(End_A(S_1^{op})) \oplus ... \oplus M_{n_r}(End_A(S_r^{op})) \end{aligned}$$

Poiché l'algebra endomorfismo di un modulo semplice è un'algebra di divisione e poiché l'opposta di un'algebra di divisione è ancora un'algebra di divisione, si ottiene la tesi.

Corollario *Un'algebra A è semplice se e solo se esiste un'algebra di divisione D tale che:*

$$A \cong M_n(D)$$

Dim. L'implicazione verso sinistra è dimostrata con il Teorema 3.1.
Dimostriamo che vale l'implicazione verso destra.

Se A è semplice allora A è semisemplice e, per il Teorema 3.2 (Wedderburn), si può scrivere come somma diretta:

$$A \cong M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(D_r)$$

dove le D_i sono algebre di divisione. Ora, la Proposizione 3.5 ci dice che gli ideali di A sono in numero di 2^r; essi hanno la forma seguente:

$$J_1 \oplus ... \oplus J_{n_r}$$

con $J_i \lhd M_{n_i}(D_i)$.
A è però un'algebra semplice, che come tale ammette esattamente 2 ideali 'banali'. Quindi, deve essere

$$n_r = 1$$

Corollario *Sia F algebricamente chiuso. Allora ogni F-algebra semisemplice A è tale che:*

$$A \cong \bigoplus_{i=1}^{r} M_{n_i}(F)$$

per qualche $r \in \mathbf{N}$.

Dim. La dimostrazione deriva immediatamente dal Lemma 3.8 e dalla dimostrazione del Teorema di Wedderburn.

Definizione 3.3 *Sia A una F-algebra.*
Un $x \in A$ si dice nilpotente se

$$x^n = 0$$

per qualche $n \in \mathbf{N}$.
Un ideale $I \subset A$ è nilpotente se

$$I^n := \left\{ \sum_{i<\infty} a_{1_i} \cdot ... \cdot a_{n_i} : a_i \in I \right\} = \{0\}$$

per qualche $n \in \mathbf{N}$.

Lemma 3.10 *Se I e J sono ideali nilpotenti di A allora anche $I + J$ è un ideale nilpotente di A.*

Dim. Siano $m, n \in \mathbf{N}$ tali che $I^m = \{0\}$ e $J^n = \{0\}$. Il prodotto di $m + n$ elementi qualsiasi di $I + J$ può essere scritto come somma di termini della forma $z_1 ... z_{m+n}$, dove ogni z_i, per $i = 1, ..., m + n$, sta o in I o in J. In ognuno di tali termini, o almeno m degli z_i stanno in I o almeno n di essi stanno in J. Nel primo caso, poiché I è un ideale, si può riscrivere $z_1 ... z_{m+n}$ come prodotto di m elementi di I; perciò, si ha $z_1 ... z_{m+n} = 0$ per la nilpotenza di I. Nel secondo caso si procede in modo analogo. Di conseguenza, il

prodotto di $m+n$ qualsiasi elementi di $I+J$ è nullo e, quindi, $(I+J)^{m+n} = \{0\}$.

Osservazione
Esiste quindi un (unico) ideale nilpotente massimale per A. Esso prende il nome di *radicale nilpotente* di A e si indica con $R(A)$.

Lemma 3.11 *Siano M e N due sottomoduli di A tali che A/M e A/N siano A-moduli semisemplici. Allora $A/M \cap N$ è un A-modulo semisemplice.*

Dim. La funzione

$$A/M \cap N \longrightarrow A/M \oplus A/N : a + (M \cap N) \longmapsto (a+M, a+N)$$

è un monomorfismo di A-moduli.
$A/M \cap N$ è quindi semisemplice perché lo è $A/M \oplus A/N$.

Osservazione
Dato un A-modulo M, l'*annullatore* di M

$$Ann(M) = \{a \in A : aM = 0\} \subseteq A$$

è un ideale di A.

Teorema 3.3 *Sia A una F-algebra con unità 1. I tre seguenti insiemi:*

1. *il radicale nilpotente massimale di A*
2. *$\bigcap AnnS$, per ogni A-modulo semplice S (l'annullatore comune di tutti gli A-moduli semplici)*
3. *il più piccolo sottomodulo di A avente quoziente semisemplice*

sono equivalenti.

Dim. Si indichino i tre insiemi, rispettivamente nell'ordine, con R, $\mathcal{A}$ e M.
Dimostriamo che "$R = \mathcal{A}$" (cioè che (1) equivale a (2)).
Dato un ideale nilpotente $J \subseteq A$

$$J^n = \{0\}$$

Per un A-modulo semplice S, si ha che JS è un sottomodulo di S, cioè $JS \subseteq S$. Allora deve essere

$$JS = \{0\}$$

oppure

$$JS = S$$

Ora

$$J^n S = \{0\}$$

implica

$$JS = \{0\}$$

e da ciò $J \subseteq R$; essendo R l'ideale massimale nilpotente di A, segue quindi che $R \subseteq \mathcal{A}$.
Viceversa, avendo A dimensione finita, esiste una serie di sottomoduli A_i incapsulati, cioè

$$A = A_0 \supset A_1 \supset ... \supset A_r = \{0\}$$

con A_i/A_{i+1} semplice. Allora

$$\mathcal{A}(A_i/A_{i+1}) = 0$$

vale a dire

$$\mathcal{A} \cdot A_i \subseteq A_{i+1}$$

Da qui

$$\mathcal{A} \cdot A \subseteq A_r = \{0\}$$

In particolare, si ha $\mathcal{A}^r \subseteq A_r = \{0\}$ che implica $\mathcal{A} \subseteq R$.
Dalla doppia inclusione segue l'uguaglianza, ossia $R = \mathcal{A}$.
Dimostriamo ora che "$\mathcal{A} = M$" (cioè che (2) equivale a (3)).
$\mathcal{A}$ annulla tutti i moduli semplici; quindi, $\mathcal{A}$ annulla anche i moduli semisemplici. In particolare:

$$\mathcal{A}(A/M) = \{0\}$$

implica

$$\mathcal{A}A \subseteq M$$

e inoltre

$$\mathcal{A} = \mathcal{A} \cdot 1 \subseteq \mathcal{A} \cdot A \subseteq M$$

Se $\mathcal{A} \neq M$, cioè $\mathcal{A} \subset M$, esiste un A-modulo semplice S tale che $MS \neq \{0\}$. Allora esiste un $s \in S$ per cui $Ms \neq \{0\}$ e Ms è un sottomodulo di S. Da ciò segue che $Ms = S$ ed esiste $x \in M$ (con $x \neq 1$ perché $M \neq A$) tale che

$$xs = s$$

cioè

$$(x - 1)\, s = 0$$

Sia ora $N \subset A$ (e $N \neq A$) un sottomodulo massimale che contiene $x - 1$ (l'esistenza di N deriva dal fatto che la dimensione di FA è finita); allora A/N è un A-modulo semplice. Poiché M è il più piccolo ideale per cui A/M è semisemplice, deve essere $N \supseteq M$. Ricordando che $x \in M$, si ha

$$1 = x - (x - 1) \in N$$

contro l'ipotesi $N \subset A$ ma $N \neq A$. Quindi

$$\mathcal{A} = M$$

Per la proprietà transitiva dell'uguaglianza segue subito "$R = M$".

Corollario *Se A è un'algebra con unità, A è semisemplice se e solo se $R(A) = \{0\}$.*

Corollario *Esiste una corrispondenza biunivoca tra l'insieme degli A-moduli semplici e l'insieme degli $A/R(A)$-moduli semplici, cioè*

$$\{A\text{-}moduli\ semplici\} \overset{1-1}{\longleftrightarrow} \{A/R(A)\text{-}moduli\ semplici\}$$

Dim. Sia $\pi : A \longrightarrow A/R(A)$ il morfismo canonico.
Se V è un A-modulo irriducibile allora V è anche un $A/R(A)$-modulo irriducibile attraverso π. Presi $a \in A$, $\bar{a} \in A/R(A)$ e $v \in V$, si ha

$$\bar{a} \cdot v := a \cdot v$$

Viceversa, se V è un $A/R(A)$-modulo semplice V è anche un A-modulo definito, per $a \in A$ e $v \in V$, da

$$a \cdot v := \bar{a} \cdot v$$

Questa è una buona definizione perché

$$a \cdot v = 0$$

per ogni $a \in R(A)$.

Capitolo 4

Rappresentazione dei gruppi finiti

Teorema 4.1 *Un gruppo finito ha soltanto un numero finito di rappresentazioni irriducibili non equivalenti (su un campo fisso).*

Dim. Siano G un gruppo finito e F un campo. Sappiamo che esistono le seguenti corrispondenze biunivoche:

$$\begin{array}{c} \{\text{rappresentazioni irriducibili di } G \text{ su } F\} \\ \updownarrow \\ \{\text{moduli irriducibili di } F[G]\} \\ \updownarrow \\ \{\text{moduli irriducibili di } F[G]/R(F[G])\} \end{array}$$

dove $F[G]$ è un'algebra semplice (la cui dimensione è uguale a $|G|$) e $F[G]/R(F[G])$ è semisemplice. Poiché $F[G]/R(F[G])$ è semisemplice, per la teoria di Wedderburn, i moduli irriducibili non equivalenti sono finiti.

Definizione 4.1 *Una rappresentazione $\rho : G \longrightarrow GL(V)$ si dice completamente riducibile se V è una somma diretta di sottospazi, cioè*

$$V = V_1 \oplus ... \oplus V_r$$

dove $\rho(G)V_i \subseteq V_i$ e V_i è un $\rho(G)$-modulo irriducibile, per $i = 1, ..., r$.

Possiamo osservare che esisterà una base di V tale che

$$\rho(G) \subseteq \left\{ \begin{pmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{pmatrix} \right\}$$

dove gli asterischi sulla diagonale corrispondono a $\rho(G)V_i$, con i numero di riga e di colonna.

Osservazione
Se $F[G]$ è un'algebra semisemplice allora tutti gli $F[G]$-moduli sono somma diretta di sottomoduli irriducibili e, quindi, ogni rappresentazione di G è completamente riducibile.

Teorema 4.2 *Se $|G|$ è finita allora $F[G]$ è semisemplice se e solo se CharF non divide $|G|$.*

Dim. Dimostriamo l'implicazione verso sinistra.
Sappiamo che, per il Teorema di Maschke, se Char$F$ non divide $|G|$ allora ogni modulo semisemplice è un addendo della somma diretta, da cui segue la semisemplicità di $F[G]$.
Dimostriamo l'implicazione verso destra.
Poniamo

$$z = \sum_{\forall g \in G} g$$

Allora, per ogni $g' \in G$ si ha:

$$g'z = z = zg' \qquad (*)$$

e

$$z^2 = \left(\sum_{\forall g' \in G} g' \right) z = \sum_{\forall g' \in G} g'z = |G|z$$

dove l'ultima uguaglianza deriva dal fatto che, per $(*)$, $g'z = z$.
Ora, se Char$F$ per assurdo divide $|G|$ allora

$$|G|z = 0z = 0$$

Da ciò segue $z^2 = 0$, cioè z^2 è un elemento nilpotente. $F[G]$ ha quindi un ideale nilpotente nullo, Fz; ma allora $F[G]$ non è semisemplice, contro l'ipotesi.

Teorema 4.3 *Supponiamo che CharF non divida $|G|$. Allora*

$$F[G] = M_{n_1}(D_1) \oplus ... \oplus M_{n_r}(D_r) \cong n_1 S_1 \oplus ... \oplus n_r S_r$$

come $F[G]$-moduli, dove i D_i sono corpi su F mentre gli insiemi

$$S_i \cong \left\{ \begin{pmatrix} d_1 \\ \vdots \\ d_{n_i} \end{pmatrix} : d_i \in D_i \right\}$$

sono $F[G]$-moduli semplici non equivalenti. In più

$$n_i S_i = \underbrace{S_i \oplus ... \oplus S_i}_{n_i \text{ volte}}$$

per $i = 1, ..., r$.
In particolare,

$$dim_F S_i = n_i dim_F D_i$$

e se F *è algebricamente chiuso allora*

$$dim_F S_i = n_i$$

per $i = 1, ..., r$.
Infine, ogni F[G]-modulo è isomorfo (come F[G]-modulo) a qualche

$$m_1 S_1 \oplus ... \oplus m_r S_r$$

per $m_i \in \mathbf{N}$.

Dim. La dimostrazione è una semplice applicazione della Teoria di Wedderburn.

Corollario *Siano* F, G *e* n_i *(con* $1 \leq i \leq r$*) come sopra. Se* F *è algebricamente chiuso allora*

$$|G| = n_1^2 + n_2^2 + ... + n_r^2$$

Dim.

$$|G| = \dim_F F[G] = \dim(\bigoplus_{i=1}^{r} M_{n_i}(F)) = n_1^2 + ... + n_r^2$$

dove la seconda e la terza uguaglianza derivano rispettivamente dal fatto che F è algebricamente chiuso, quindi $D_i = F$, e dal fatto che $\dim M_{n_i}(F) = n_i^2$, per ogni $i = 1, ..., r$.

Proposizione 4.1 *Se* $G = S_n$ *(gruppo simmetrico delle permutazioni su n oggetti) allora*

$$F[G] = \bigoplus_{i=1}^{r} M_{n_i}(F)$$

per ogni campo F.

Corollario *Per ogni* $n \in \mathbf{N}$ *si ha*

$$n! = n_1^2 + ... + n_r^2$$

Questo corollario mette in luce un risultato importante anche in teoria dei numeri, vale a dire il fatto che l'equazione

$$\underbrace{x^2 + y^2 + z^2 + ...}_{\text{r variabili}} = n!$$

ammetta soluzione.

Teorema 4.4 *Siano dati F e G come sopra, con CharF che non divide $|G|$. Se F è algebricamente chiuso allora:*

$$r = \#\{F[G]\text{-moduli irriducibili non equivalenti fra loro}\}$$

$$= \#\{\text{classi di coniugazione di } G\}$$

Prima di dimostrare il teorema è necessario definire la nozione di classe di coniugazione di un gruppo.

Definizione 4.2 *Siano G un gruppo finito e $h, g \in G$. Una coniugazione di G è data da*

$$hgh^{-1}$$

La relazione di coniugazione è una relazione di equivalenza e, come tale, ammette delle classi di equivalenza, che si ottengono tutte mantenendo fisso g in G e facendo variare h. Fissato quindi $g \in G$, l'insieme

$$\left\{hgh^{-1} : \forall h \in G\right\} \subset G$$

è una classe di coniugazione di G.
Una classe di coniugazione è solo un sottoinsieme di G, non un sottogruppo.
Si può quindi scrivere

$$G = C_1 \cup C_2 \cup ... \cup C_s$$

dove le unioni sono disgiunte, cioè a intersezione vuota (C_1 indica la classe di coniugazione dell'identità 1 e così via).

Esempio
Se G è un gruppo abeliano allora

$$\#\{\text{classi di coniugazione di } G\} = |G|$$

Ogni elemento di G è quindi classe di equivalenza rispetto alla relazione di coniugazione.

Esercizio
Determinare tutte le rappresentazioni del gruppo ciclico $G = \langle z \rangle$ di ordine n su $\mathbf{C}$.

Sappiamo che $\mathbf{C}[G]$ è una $\mathbf{C}$-algebra e che

$$|G| = |\langle z \rangle| = n = \sum_{i=1}^{r} n_i^2$$

con r numero delle classi di coniugazione di G.
Essendo G abeliano, ogni suo elemento è classe di coniugazione, quindi:

$$r = n$$

e, inoltre:

$$n = \sum_{i=1}^{n} n_i^2$$

Ora, per ogni i, $n_i \neq 0$, il che implica $n_i = 1$, da cui

$$\mathbf{C}[\langle z \rangle] = S_1 \oplus ... \oplus S_n$$

La dimensione di $\mathbf{C}[\langle z \rangle]$ come spazio vettoriale su $\mathbf{C}$ coincide con n. Allora, essendo

$$\dim_{\mathbf{C}} \mathbf{C}[\langle z \rangle] = \dim_{\mathbf{C}} (S_1 \oplus ... \oplus S_n) = \dim_{\mathbf{C}} (S_1) + ... + \dim_{\mathbf{C}} (S_n)$$

si deve avere, per ogni $i = 1, ..., n$

$$\dim_{\mathbf{C}} (S_i) = 1$$

da cui si può dire

$$S_i \cong \mathbf{C}$$

(come spazi vettoriali). Possiamo perciò scrivere

$$\mathbf{C}[\langle z \rangle] \cong \underbrace{\mathbf{C} \oplus ... \oplus \mathbf{C}}_{n \text{ volte}}$$

(ovviamente sempre come spazi vettoriali).
Le rappresentazioni di G sono allora le funzioni

$$\langle z \rangle \longrightarrow GL(\mathbf{C}) \cong \mathbf{C}^*$$

che operano nel modo seguente:

$$z \longmapsto \left(e^{r \frac{2\pi i}{n}} \right)$$

per ogni $r = 1, ..., n$. Si hanno quindi n rappresentazioni irriducibili distinte.

Definizione 4.3 *Siano G un gruppo finito e F un campo. Si dice centro del gruppo algebra F[G] l'insieme seguente*

$$C(F[G]) = \{x \in F[G] : xy = yx, \forall y \in F[G]\}$$

Il centro di F[G] è uno spazio vettoriale su F, per il quale quindi è lecito parlare di esistenza di una base.

Per la dimostrazione del Teorema 4.3 è necessario il seguente lemma.

Lemma 4.1 *Sia G l'unione delle sue classi di coniugati, cioè*

$$G = C_1 \cup C_2 \cup ... \cup C_s$$

Poniamo:

$$c_i = \sum_{\forall g_i \in C_i} g_i$$

Allora $\{c_1, ..., c_s\}$ è una base per il centro C(F[G]) di F[G].

Dim. Si deve dimostrare che:

1. $c_i \in C(F[G])$ per ogni i;
2. preso un qualsiasi x in $C(F[G])$, x si può scrivere come combinazione lineare dei c_i;
3. i c_i sono linearmente indipendenti.

Punto 1.
Per ogni $g \in G$ si ha:

$$gc_ig^{-1} = \sum_{\forall g_i \in C_i} gg_ig^{-1} = \sum_{\forall g_j \in C_i} g_j = c_i$$

dove la seconda uguaglianza è dovuta al fatto che $gg_ig^{-1} \in C_i$, che è classe di coniugazione. Da qui segue che $c_i \in C(F[G])$.
Punto 2.
Sia

$$c = \sum_{\forall g \in G} \gamma_g g \in C(F[G])$$

dove i γ_g sono i coefficienti di F. Per ogni $h \in G$ si ha:

$$c = hch^{-1} = \sum_{\forall g \in G} \gamma_g \underbrace{hgh^{-1}}_{g'} = \sum_{g' \in G} \gamma_{h^{-1}g'h} g' = \sum_{g \in G} \gamma_{h^{-1}gh} g$$

dove la terza uguaglianza deriva dall'aver posto $g' = hgh^{-1}$, da cui $g = h^{-1}g'h$. Ora però

$$c = \sum_{g \in G} \gamma_g g$$

Allora

$$\sum_{g \in G} \gamma_g g = \sum_{g \in G} \gamma_{h^{-1}gh} g$$

e da qui

$$\gamma_g = \gamma_{h^{-1}gh}$$

per $g \in G$. Ciò significa che gli elementi coniugati hanno lo stesso coefficiente. Si può quindi scrivere:

$$c = \sum_{i=1}^{s} \gamma_i (\sum_{g_i \in C_i} g_i) = \sum_{i=1}^{s} \gamma_i c_i$$

cioè c è combinazione lineare dei c_i.
Punto 3.
c_1, ..., c_s sono ovviamente linearmente indipendenti su F come spazio vettoriale; si tratta infatti di elementi diversi di $F[G]$. Allora $\{c_1, ..., c_s\}$ è una base di $C(F[G])$.

Siamo pronti a questo punto a dimostrare il teorema 4.3.
Dim. (del teorema 4.3) Per ipotesi F è algebricamente chiuso. Allora si può scrivere:

$$F[G] = M_{n_1}(F) \oplus ... \oplus M_{n_r}(F)$$

Ora, si ha:

$$\left\{ \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_r \end{pmatrix} : A_i \in M_{n_i}(F) \right\} \cong F[G]$$

dove le A_i sono matrici a blocchi e l'insieme considerato è un'algebra con la somma e il prodotto di matrici. Inoltre:

$$C(F[G]) \cong \left\{ \begin{pmatrix} C_1 & & & 0 \\ & C_2 & & \\ & & \ddots & \\ 0 & & & C_r \end{pmatrix} : C_i \in C(M_{n_i}(F)) \right\}$$

Le matrici diagonali con gli elementi tutti uguali sulla diagonale, del tipo seguente

$$\begin{pmatrix} a & & & 0 \\ & a & & \\ & & \ddots & \\ 0 & & & a \end{pmatrix}$$

commutano con ogni altra matrice, perciò appartengono al centro di $F[G]$; si ha quindi:

$$C(M_{n_i}(F)) = \left\{ \begin{pmatrix} a & & & 0 \\ & a & & \\ & & \ddots & \\ 0 & & & a \end{pmatrix}_{n_i \times n_i} : \forall a \in F \right\} \cong F$$

(sono isomorfi come campi). Da qui segue

$$C(F[G]) = C(M_{n_1}(F)) \oplus ... \oplus C(M_{n_r}(F)) \cong \underbrace{F \oplus ... \oplus F}_{r \text{ volte}}$$

e inoltre

$$\dim_F C(F[G]) = r = s$$

per il Lemma 14, essendo s il numero delle classi di coniugazione.

Capitolo 5

Gruppi di permutazione

In questa sezione vogliamo prendere in considerazione la rappresentazione irriducibile di S_n.

Lemma 5.1 *$\#\{$classi coniugate di $S_n\} = \#\{$partizioni di $n\} = p(n)$.*

Dim. Prima di procedere con la dimostrazione, apriamo una breve parentesi.
Sia

$$n = r_1 + r_2 + ... + r_s$$

Allora si dice che

$$\alpha = (r_1, ..., r_s)$$

è una *partizione* di n e si indica come segue:

$$\alpha \vdash n$$

Ora si consideri $\sigma \in S_n$; si può scrivere σ in modo unico come prodotto di cicli disgiunti:

$$\sigma = (a_1 ... a_{r_1}) \cdot (b_1 ... b_{r_2}) \cdot ... \cdot (x_1 ... x_{r_h})$$

dove $r_1 + r_2 + ... + r_h = n$ e $r_1 \geq r_2 \geq ... \geq r_h$. Quindi σ individua una partizione $(r_1, r_2, ..., r_n)$ di n.
D'altra parte, data una partizione di n, $(r_1, ..., r_s) \vdash n$, si trova sempre $\sigma \in S_n$, con

$$\sigma = \underbrace{(...)}_{r_1} \cdot \underbrace{(...)}_{r_2} \cdot ... \cdot \underbrace{(...)}_{r_s}$$

Allora: σ e $\sigma' \in S_n$ sono coniugati se e solo se σ e σ' corrispondono alla stessa partizione di n. Per l'unicità si ha:

$$\{\text{classi di coniugazione di } S_n\} \overset{1-1}{\longleftrightarrow} \{\text{partizioni di } n\}$$

5.1 Tavole e diagrammi di Young

Siano $n \in \mathbf{N}$ e $\alpha = (r_1, ..., r_h) \vdash n$, con $r_1 \geq r_2 \geq ... \geq r_h$ (si considerano cioè partizioni ben ordinate). Si consideri ora la figura seguente

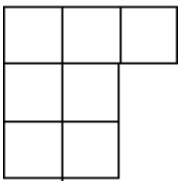

Fig.1: $\mathbf{D}_\alpha$

dove nella prima riga ci sono r_1 quadretti, nella seconda r_2 quadretti e così via fino all'ultima in cui ci sono r_h quadretti. In totale si hanno quindi $r_1 + r_2 + ... + r_h = n$ quadretti. La figura si chiama diagramma di Young e si indica con D_α per $\alpha \vdash n$. Fissando una tavola di Young α e riempiendo gli stessi quadretti con numeri distinti, si ottengono vari diagrammi di Young (si indicano con E_α, F_α e così via; tali diagrammi sono uguali a D_α a meno di numeri diversi in posizioni uguali). Vediamo un esempio, considerando $n = 7$ e $\alpha = (3, 2, 2)$:

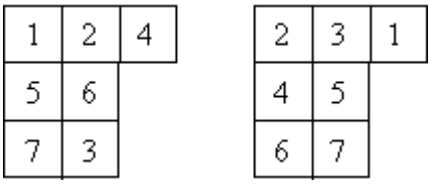

Fig.2: $\mathbf{E}_\alpha, \mathbf{F}_\alpha$

Definizione 5.1 *Siano n fisso e D un diagramma di Young. Sono definiti i due seguenti insiemi:*

$$R(D) = \{\sigma \in S_n : \sigma \textit{stabilizza ogni riga di } D\} \subset S_n$$

e

$$C(D) = \{\tau \in S_n : \tau \textit{stabilizza ogni colonna di } D\} \subset S_n$$

Il primo insieme quindi permuta i numeri sulle righe (ma non le righe tra loro), mentre il secondo permuta i numeri sulle colonne (ma non le colonne fra loro).

Vediamo ora alcune proprietà dei diagrammi di Young.

- $R(D) \cap C(D) = \{id\}$, cioè l'intersezione è ancora una permutazione di n elementi che lascia invariato il posto degli elementi stessi.

- Siano dati $\alpha \vdash n$, D_α, $\sigma \in S_n$.
  σD_α è ancora un diagramma di Young. Si può allora verificare quanto segue

  $$\sigma^{-1} R(\sigma D_\alpha)\, \sigma = R(D_\alpha)$$

  (si usa il fatto che $\sigma(i_1\ i_2\ ...\ i_r)\, \sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\ ...\ \sigma(i_r))$).
  Lo stesso vale se al posto di $R(D_\alpha)$ si considera $C(D_\alpha)$.
  Si ha quindi:

  $$\begin{cases} R(\sigma D_\alpha) = \sigma R(D_\alpha)\, \sigma^{-1} \\ C(\sigma D_\alpha) = \sigma C(D_\alpha)\, \sigma^{-1} \end{cases}$$

Siano dati l'algebra $F[S_n]$, $\alpha \vdash n$ e un diagramma di Young fissato D_α, che per semplicità indichiamo con D. Sappiamo che $S_n \supset C(D), R(D)$. Si considerino i seguenti elementi di $F[S_n]$:

$$A_D = \sum_{\forall\, \tau \in C(D)} (\operatorname{segn} \tau)\, \tau \in F[S_n]$$

$$S_D = \sum_{\forall\, \sigma \in R(D)} \sigma \in F[S_n]$$

$$F_D = A_D S_D = \sum_{\substack{\forall\, \tau \in C(D) \\ \forall\, \sigma \in R(D)}} (\operatorname{segn} \tau)\, \tau\sigma \in F[S_n]$$

Ora, se esiste $\gamma \in F^*$ tale che

$$e_D = \gamma^{-1} F_D$$

risulta

$$e_D^2 = e_D$$

cioè e_D è un elemento idempotente. Si ha allora:

$$e_D F[S_n] e_D = \gamma^{-2} F_D F[S_n] F_D \qquad (\star)$$

Esiste inoltre una proprietà che dice:

1. per ogni $x \in F[S_n]$ vale la seguente uguaglianza

   $$F_D x F_D = \beta F_D$$

   per qualche $\beta \in F$.

2. In particolare, se $x \in F$, si ha

$$F_D x F_D = x F_D^2 = x\gamma F_D$$

da cui segue

$$F_D^2 = \gamma F_D$$

per qualche $\gamma \in F$, con $\gamma \neq 0$.

Per comodità indichiamo questa seconda proprietà con $(\diamond)$. Applicandola a $(\star)$ si ottiene il seguente lemma.

Lemma 5.2 *Valgono le due seguenti proprietà:*

1. $e_D F[S_n] e_D = \gamma^{-2} F_D F[S_n] F_D = F F_D = F_{e_D}$
   e inoltre
   $$F_{e_D} \xrightarrow{\sim} F : e_D \mapsto 1$$
   dove F è un campo, l'isomorfismo è un isomorfismo di anelli e 1 è l'identità.

2. *Siano $\alpha \vdash n$ e $\beta \vdash n$, D_α un diagramma di Young associato a α e E_β un diagramma di Young associato a β. Allora:*
   $$F[S_n] e_{D_\alpha} \ncong F[S_n] e_{E_\beta}$$
   ovunque $\alpha \neq \beta$, cioè l'isomorfismo si ha se e solo se $\alpha = \beta$.

Dim. Supponiamo $\alpha > \beta$.
Dobbiamo usare il lemma seguente, che non dimostriamo ma di cui diamo solo l'enunciato.

Lemma 5.3 *Siano $\alpha \vdash n$ e $\beta \vdash n$, con $\alpha \geq \beta$. Siano D_α e E_β due diagrammi di Young. Se due numeri che si trovano nella stessa riga di D_α non compaiono mai entrambi in una stessa colonna di E_β, allora $\alpha = \beta$ e inoltre $E_\alpha = \sigma\, \tau D_\alpha$ per qualche $\sigma \in R(D_\alpha)$ e $\tau \in C(D_\alpha)$.*

Per questo lemma, esistono $i, j \in \{1, ..., n\}$ che stanno nella stessa riga di D_α e contemporaneamente nella stessa colonna di E_β. Sia

$$\pi = (i, j) \in R(D_\alpha) \cap C(E_\beta)$$

un 2-ciclo. Ricordiamo che

$$S_{D_\alpha} = \sum_{\sigma \in R(D_\alpha)} \sigma$$
$$A_{E_\beta} = \sum_{\tau \in C(E_\beta)} (segn\tau)\, \tau$$
$$F_{D_\alpha} = A_{D_\alpha} S_{D_\alpha}$$

Si ha:

$$\pi S_{D_\alpha} = S_{D_\alpha} = S_{D_\alpha}\pi$$
$$\pi A_{E_\beta} = -A_{E_\beta}\pi$$

Da qui si ottiene

$$S_{D_\alpha}A_{E_\beta} = S_{D_\alpha}\pi A_{E_\beta} = -S_{D_\alpha}A_{E_\beta} \qquad (\star)$$

e analogamente

$$A_{E_\beta}S_{D_\alpha} = A_{E_\beta}\pi S_{D_\alpha} = -A_{E_\beta}S_{D_\alpha} \qquad (\star\star)$$

Da $(\star)$ segue

$$S_{D_\alpha}A_{E_\beta} = 0$$

e, analogamente, da $(\star\star)$

$$A_{E_\beta}S_{D_\alpha} = 0$$

Ora, per ogni $\rho \in S_n$ consideriamo ρD_α. Allora

$$S_{\rho D_\alpha}A_{E_\beta} = 0 = A_{E_\beta}S_{\rho D_\alpha}$$

Poiché

$$S_{\rho D_\alpha} = \rho S_{D_\alpha}\rho^{-1}$$

si ha quanto segue:

$$S_{D_\alpha}\rho A_{E_\beta} = 0 = A_{E_\beta}\rho S_{D_\alpha}$$

per ogni $\rho \in S_n$, da cui

$$S_{D_\alpha}F[S_n]A_{E_\beta} = 0 = A_{E_\beta}F[S_n]S_{D_\alpha}$$

Essendo

$$e_{D_\alpha} = \gamma_1 F_{D_\alpha}$$

e

$$e_{E_\beta} = \gamma_2 F_{E_\beta}$$

si ha anche:

$$e_{D_\alpha}F[S_n]e_{E_\beta} = \gamma_1 A_{D_\alpha}S_{D_\alpha}F[S_n]\gamma_2 A_{E_\beta}S_{E_\beta} = \gamma_1\gamma_2 A_{D_\alpha}S_{D_\alpha}F[S_n]A_{E_\beta}S_{E_\beta} = 0$$

dove l'ultima uguaglianza deriva dal fatto che $S_{D_\alpha}F[S_n]A_{E_\beta} = 0$.
Per poter andare avanti abbiamo bisogno del seguente lemma.

Lemma 5.4 *Siano A un algebra su F ed $e, f \in A$ due elementi idempotenti (cioè $e^2 = e$, $f^2 = f$). Allora:*

1. *$Hom_A(Ae, Af) \cong eAf$*
   (come gruppi additivi), dove Ae e Af sono A-moduli per i quali

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x)$$

   per ogni $x \in Ae$, mentre eAf è una A-algebra per la quale

$$exf + eyf = e\,(x + y)f$$

   per ogni $x, y \in A$.
   L'isomorfismo opera nel modo seguente:

$$\varphi \longmapsto e\varphi(e) = \varphi(e \cdot e) = \varphi(e^2) = \varphi(e)$$

2. *Sia $e = f$. Si ha:*

$$End_A(Ae) \overset{*}{\cong} eAe$$

   (come anelli), dove $\overset{*}{\cong}$ è un anti-isomorfismo che cambia l'ordine, cioè è tale che:

$$\varphi_1 \cdot \varphi_2 \longmapsto *\,(\varphi_2) \cdot *\,(\varphi_1)$$

3. *S è un A-modulo semplice se e solo se $End_A(S)$ è un corpo.*

4. *Dati S_1 e S_2 A-moduli semplici, $Hom_A(S_1, S_2) = 0$ se e solo se $S_1 \ncong S_2$.*

La dimostrazione è lasciata per esercizio.
Da tale lemma segue che $F[S_n]$ è un A-modulo semplice (o irriducibile). Infatti

$$e_D F[S_n] e_D$$

è isomorfo al campo

$$\mathrm{End}_{F[S_n]}(F[S_n]e_D)$$

per il punto (2) e quindi, per il punto (3), è semplice.
Inoltre, per il punto (1),

$$\mathrm{Hom}_{F[S_n]}(F[S_n]e_{D_\alpha}, F[S_n]e_{E_\beta}) \cong e_{D_\alpha} F[S_n] e_{E_\beta} = 0$$

Allora, $F[S_n]e_{D_\alpha}$ e $F[S_n]e_{E_\beta}$, $F[S_n]$-sottomoduli irriducibili, sono distinti (nel senso di non isomorfi) se $\alpha \neq \beta$.

Lemma 5.5 *Sia A una F-algebra semisemplice. Si ha:*

$$A \cong A_1 \oplus ... \oplus A_r \cong n_1 S_1 \oplus ... \oplus n_r S_r$$

dove gli A_i sono ideali (o sottoalgebre) semplici, gli S_i sono A-sottomoduli semplici di A e

$$A_i \cong n_i S_i = \underbrace{S_i \oplus ... \oplus S_i}_{n_i \text{ volte}}$$

per $i = 1, ..., r$.
Allora:

$$n_i = \frac{dim_F S_i}{dim_F End_A(S_i)}$$

per ogni $i = 1, ..., r$.

Dim. Dalla Teoria di Wedderburn si ha

$$A_i \cong M_{n_i}(D_i)$$

per qualche $n_i \in \mathbf{N}$, dove D_i è un corpo. Dalla dimostrazione del teorema di Wedderburn segue

$$D_i \cong \mathrm{End}_A(S_i)$$

Quindi:

$$\dim_F A_i = \dim_F M_{n_i}(D_i) = n_i^2 \dim_F D_i = n_i^2 \dim_F End_A(S_i)$$

dove la seconda uguaglianza deriva dal fatto che

$$\dim_F M_n(F) = n^2$$

e per questo

$$\dim_F M_n(D) = n^2 \dim_F D$$

mentre la terza deriva da quanto detto sopra.
D'altra parte, essendo

$$A_i \cong n_i S_i$$

segue che

$$\dim_F A_i = n_i \dim_F S_i$$

Allora

$$n_i \dim_F S_i = n_i^2 \dim_F End_A(S_i)$$

da cui, ricavando l'espressione di n_i, si ottiene la tesi.

In particolare, se

$$\mathrm{End}_A(S_i) \cong F$$

allora

$$\dim_F S_i = n_i$$

Nel nostro caso

$$A = F[S_n]$$
$$S_i = F[S_n]e_D$$
$$\mathrm{End}_A(F[S_n]e_D) \cong F$$

quindi:

$$\dim_F F[S_n]e_D = n_i$$

Teorema 5.1 *Ogni $F[S_n]$-modulo semplice è isomorfo a qualche $F[S_n]e_D$ per qualche diagramma di Young D. In più:*

$$F[S_n] \cong M_{n_1}(F) \oplus ... \oplus M_{n_{p(n)}}(F)$$

dove

$$p(n) = \#\{\textit{partizioni di } n\} = \#\{\textit{tavole di Young}\} = \#\{\textit{classi di coniugazione di } S_n\}$$

Dim. Sia $\{\alpha_1, ..., \alpha_{p(n)}\}$ un insieme di partizioni di n (cioè $\alpha_i \vdash n$, $\forall\, i = 1, ..., p(n)$). Poniamo ora

$$S_i = F[S_n]e_{D_i}$$

per ogni $i = 1, ..., p(n)$, dove con D_i indichiamo, per semplicità di scrittura, D_{α_i}. Gli S_i sono moduli semplici; ma sono tutti?
Consideriamo la chiusura algebrica di F, $\overline{F}$, cioè il minimo campo contenente F, che è algebricamente chiuso. Sia inoltre

$$\overline{S}_i = \overline{F} \otimes_F S_i$$

$\overline{S}_i$ è un F-modulo, perché

$$\overline{S}_i = \overline{F} \otimes_F S_i \cong \overline{F}[S_n]e_{D_i}$$

che è un $\overline{F}[S_n]$-modulo semplice. Sappiamo anche

$$\overline{F} \otimes_F F[S_n] \cong \overline{F}[S_n]$$

Ricordando ora la proprietà secondo cui il numero di moduli semplici non equivalenti è uguale al numero delle classi di coniugazione di S_n e contemporaneamente al numero di partizioni di n, si può scrivere:

$$\overline{F}[S_n] = n_1\overline{S}_1 \oplus ... \oplus n_{p(n)}\overline{S}_{p(n)}$$

dove $\overline{S}_i$ e $\overline{S}_j$ sono non equivalenti, perché

$$\overline{F}[S_n]e_{D_i} \ncong \overline{F}[S_n]e_{D_j}$$

Quindi:

$$\overline{F}[S_n] = n_1\overline{S}_1 \oplus ... \oplus n_{p(n)}\overline{S}_{p(n)} = \bigoplus_{i=1}^{p(n)} \left(\dim_{\overline{F}}\overline{S}_i\right) \overline{S_i}$$

Supponiamo ora per assurdo che gli S_i non siano tutti, ma che esista un $F[S_n]$-sottomodulo semisemplice M che non contiene alcun sottomodulo isomorfo a S_i per $1 \leq i \leq p(n)$. Poiché $F[S_n]$ si spezza nella somma diretta dei suoi sottomoduli semplici, si può scrivere:

$$F[S_n] = \left(\bigoplus_{i=1}^{p(n)} m_i S_i\right) \oplus M$$

D'altra parte si ha:

$$m_i = \frac{\dim_F S_i}{\dim_F \mathrm{End}_{F[S_n]}(S_i)} = \dim_F S_i$$

Allora:

$$n! = \dim_F F[S_n] = \sum_{i=1}^{p(n)} (\dim_F S_i)^2 + \dim_F M = \sum_{i=1}^{p(n)} \left(\dim_{\overline{F}} \overline{S}_i\right)^2 + \dim_F M \qquad (*)$$

perché

$$\dim_{\overline{F}} \left(\overline{F} \otimes S_i\right) = dim_F S_i$$

(cambiano i coefficienti ma non la dimensione), e

$$(*) = \dim_{\overline{F}} \left(\bigoplus_{i=1}^{p(n)} \left(\dim_F \overline{S}_i\right) \overline{S}_i \right) + \dim_F M = \dim_{\overline{F}} \left(\overline{F}[S_n]\right) + \dim_F M = n! + \dim_F M$$

da cui segue che $\dim_F M$ deve essere nulla; ma $\dim_F M = 0$ se e solo se $M = \{0\}$. Con ciò il teorema è dimostrato.

Capitolo 6

Teoria dei caratteri

Definizione 6.1 *Siano dati un gruppo G, uno spazio vettoriale V su F e una rappresentazione*

$$\rho : G \longrightarrow GL(V) \cong GL_n(F)$$

essendo $n = dimV$. Per ogni $g \in G$, la funzione

$$\chi_\rho : G \longrightarrow F : g \longmapsto tr\rho(g) \in F$$

(dove $tr\rho(g)$ è la funzione traccia, somma degli elementi della diagonale di $\rho(g)$) si chiama carattere associato a ρ. Inoltre

$$deg\chi_\rho := dim_F V = deg\rho$$

Proprietà elementari dei caratteri

0. χ_ρ *è ben definita.*

Questo significa che χ_ρ non dipende dalla scelta della base di V. Infatti, considerando due basi distinte di V, $\{v_1, ..., v_n\} \subset V$ e $\{w_1, ..., w_n\} \subset V$, si ha:

$$\rho(g) \sim \begin{pmatrix} \rho(g)v_1 \\ \rho(g)v_2 \\ \vdots \\ \rho(g)v_n \end{pmatrix} = A \qquad \rho(g) \sim \begin{pmatrix} \rho(g)w_1 \\ \rho(g)w_2 \\ \vdots \\ \rho(g)w_n \end{pmatrix} = B$$

Esiste allora una trasformazione lineare che ci fa passare da una base all'altra, cioè esiste sempre una matrice D di trasformazione tale che

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = D \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

dove $D \in GL_n(F)$ e

$$\begin{cases} v_1 = D\, w_1 \\ \quad \vdots \\ v_n = D\, w_n \end{cases}$$

Da qui segue

$$A = DBD^{-1}$$

(cioè A e B sono simili), e quindi

$$\mathrm{tr}\, A = \mathrm{tr}\,(DAD^{-1})$$

1. *Se ρ_1, $\rho_2 : G \longrightarrow GL_n(V)$ sono due rappresentazioni equivalenti di G allora*

$$\chi_{\rho_1} = \chi_{\rho_2}$$

È un'ovvia conseguenza del fatto che con rappresentazioni equivalenti si intendono rappresentazioni le cui matrici sono simili, cioè tali che esista una matrice D tale che per ogni $g \in G$ si abbia

$$\rho_1(g) = D\rho_2(g)D^{-1}$$

Allora il numero dei caratteri irriducibili di G (dove i caratteri irriducibili sono i caratteri associati a rappresentazioni irriducibili) è finito, perché il numero di rappresentazioni irriducibili non equivalenti di G, con $|G| < \infty$ è finito.

2. *Per ogni $h \in G$, $g \in G$*

$$\chi_\rho(hgh^{-1}) = \chi_\rho(g)$$

χ_ρ è una funzione di classi di coniugazione di G.
Supponiamo ora, per semplicità, Char$F = 0$ (basterebbe richiedere Char$F \neq n$).

3. *Se CharF = 0 allora*

$$\chi_\rho(\mathbf{1}) = dim_F V = deg\rho$$

1 è l'identità e ρ è quindi un omomorfismo di gruppi che manda l'identità in se stessa.

4. *Sia $U \subseteq V$ un sottospazio con $\rho(G)U \subseteq U$. Inoltre, sia $V/U = \{v + U : \forall\, v \in V\}$ lo spazio quoziente. Si considerino ora le due seguenti funzioni:*

$$\rho|_U : G \longrightarrow GL(U)$$

e

$$\rho|_{V/U} : G \longrightarrow GL(V/U) : g \longmapsto \rho|_{V/U}(g) : V/U \to V/U : v + U \mapsto \rho(g)v + U$$

Allora, per ogni $g \in G$, si ha:

$$\chi_\rho(g) = \chi_{\rho|_U}(g) + \chi_{\rho|_{V/U}}(g)$$

Per dimostrare questa proprietà si procede nel modo seguente.
Sia $U \subset V$. Consideriamo $\{u_1, ..., u_r, v_{r+1}, ..., v_n\}$ dove i primi r elementi sono una base di U. Per ogni $g \in G$, si ha:

$$\rho(g) = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}_{n \times n}$$

dove $A \in GL_r(F)$, B è una matrice con r righe e $(n-r)$ colonne, $C \in GL_{n-r}(F)$. Quindi:

$$\rho|_U(g) = A$$

rispetto alla base $\{u_1, ..., u_r\}$ di U, mentre

$$\rho|_{V/U}(g) = C$$

rispetto alla base $\{v_{r+1} + U, ..., v_n + U\}$ di V/U. Segue che

$$\operatorname{tr} \rho(g) = \operatorname{tr} A + \operatorname{tr} C$$

5. Siano $\rho_1 : G \longrightarrow GL(V_1)$ e $\rho_2 : G \longrightarrow GL(V_2)$ due rappresentazioni di G, con V_1 e V_2 spazi vettoriali su F. Definita la seguente funzione somma

$$\rho_1 \oplus \rho_2 : G \longrightarrow GL(V_1 \oplus v_2)$$

che opera come segue

$$g \longmapsto \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$$

si ha:

$$\chi_{\rho_1 \oplus \rho_2}(g) = \chi_{\rho_1}(g) + \chi_{\rho_2}(g) := (\chi_{\rho_1} + \chi_{\rho_2})(g)$$

Analogamente, definita la funzione prodotto

$$\rho_1 \otimes \rho_2 : G \longrightarrow GL(V_1 \otimes v_2)$$

che opera come segue

$$g \longmapsto \rho_1(g) \otimes \rho_2(g)$$

si ha:

$$\chi_{\rho_1 \otimes \rho_2}(g) := (\chi_{\rho_1} \cdot \chi_{\rho_2})(\chi_{\rho_1} \cdot \chi\rho_2)(g) := \chi_{\rho_1}(g) \otimes \chi_{\rho_2}(g)$$

Queste definizioni derivano dal fatto che

$$\operatorname{tr}(\rho_1(g) \oplus \rho_2(g)) = \operatorname{tr}(\rho_1(g)) + \operatorname{tr}(\rho_2(g))$$

e rispettivamente

$$\operatorname{tr}(\rho_1(g) \otimes \rho_2(g)) = \operatorname{tr}(\rho_1(g)) \cdot \operatorname{tr}(\rho_2(g))$$

Inoltre, per $a \in F$ si definisce la funzione

$$a\chi_\rho : g \longmapsto a \cdot \chi_\rho(g)$$

Si può quindi dire che i caratteri di G formano uno spazio vettoriale su F.

6. I caratteri irriducibili di G sono linearmente indipendenti su F.

Vediamo come si dimostra questa proprietà.
Ricordiamo, dal Teorema di Wedderburn, gli isomorfismi

$$F[G] \cong \mathrm{End}_{F[G]}(n_1 S_1) \oplus \ldots \oplus \mathrm{End}_{F[G]}(n_r S_r) \cong \bigoplus_{i=1}^{r} M_{n_i}(D_i)$$

dove i D_i sono corpi e gli S_i sono $F[G]$-sottomoduli semplici, per $1 \leq i \leq r$.
Sia ora χ_i il carattere associato alla rappresentazione corrispondente al $F[G]$-modulo S_i (ogni $F[G]$-modulo infatti è una rappresentazione di G). χ_i è irriducibile, perché S_i è semplice (che equivale a irriducibile). Possiamo estendere linearmente χ_i a $F[G]$ con la seguente definizione:

$$\chi_i \left(\sum_{g \in G} \gamma_g g \right) := \sum_{g \in G} \gamma_g \chi_i(g)$$

e, usando l'isomorfismo ricordato sopra, possiamo scrivere:

$$\chi_i : \bigoplus_{i=1}^{r} \mathrm{End}_{F[G]}\,(n_i S_i) \longrightarrow F$$

Sia e_i l'identità di $\mathrm{End}_{F[G]}\,(n_i S_i)$. Deve allora essere:

$$e_i(s_i) = s_i$$

per ogni $s_i \in S_i$, e

$$e_i(s_j) = 0$$

per ogni $s_j \in S_j$ e per $j \neq i$. Quindi:

$$\chi_i(e_i) = \chi_i \left(id_{\mathrm{End}(S_i)} \right) = \dim_F S_i = n_i \neq 0$$

$$\chi_i(e_j) \overset{i \neq j}{=} \chi_i \left(0_{\mathrm{End}(S_j)} \right) = 0$$

Consideriamo ora una combinazione lineare dei caratteri χ_i che si annulla e dimostriamo che tutti i coefficienti della combinazione sono nulli, cioè

$$\sum_{i=1}^{r} a_i \chi_i = 0$$

se e solo se, per ogni i, si ha

$$a_i = 0$$

Si ha:

$$\left(\sum_{i=1}^{r} a_i\chi_i\right)(e_j) = \sum_{i=1}^{r} a_i\chi_i(e_j) = a_j \dim_F S_j$$

Allora essendo $\dim_F S_j = n_j \neq 0$, perché la sommatoria si annulli deve essere proprio $a_j = 0$ per ogni j, da cui si può dire che $\chi_1, ..., \chi_r$ sono linearmente indipendenti, come volevamo dimostrare.

Teorema 6.1 *Siano $\rho_1, ..., \rho_r$ tutte le rappresentazioni irriducibili non equivalenti di G su F, con caratteri corrispondenti $\chi_1, ..., \chi_r$. Allora:*

1. *Ogni carattere di G è della forma*

$$m_i\chi_1 + ... + m_r\chi_r$$

   per $m_1, ..., m_r \in \mathbf{N}$.

2. *Due qualsiasi rappresentazioni di G su F sono equivalenti se e solo se esse hanno lo stesso carattere.*

Dim. Punto 1.
Siano $S_1, ..., S_r$ gli $F[G]$-moduli semplici (o irriducibili) corrispondenti a $\rho_1, ..., \rho_r$, cioè

$$\rho_i : G \longrightarrow GL(S_i)$$

per ogni $i = 1, ..., r$). Ogni $F[G]$-modulo è semisemplice, della forma

$$m_1S_1 \oplus ... \oplus m_rS_r$$

dove

$$m_iS_i = \underbrace{S_i \oplus ... \oplus S_i}_{m_i \text{ volte}}$$

e $m_i \in \mathbf{N}$. Il carattere di tale modulo è dato da

$$m_1\chi_1 + ... + m_r\chi_r$$

Allora ogni carattere è di tale forma.
Punto 2.
L'implicazione verso destra è ovvia per definizione.
Dimostriamo quindi l'implicazione verso sinistra, cioè che se due rappresentazioni hanno lo stesso carattere allora sono equivalenti. Siano U e V i due $F[G]$-moduli (corrispondenti alle due rappresentazioni di G su F), con caratteri rispettivamente χ_U e χ_V, dove per ipotesi

$$\chi_U = \chi_V$$

Un $F[G]$-modulo è sempre semisemplice e, come tale, si può scrivere come somma diretta degli S_i. U e V si possono perciò esprimere come segue:

$$U \cong a_1 S_1 \oplus ... \oplus a_r S_r$$
$$V \cong b_1 S_1 \oplus ... \oplus b_r S_r$$

per $a_i \in \mathbf{N}$ e $b_i \in \mathbf{N}$. Allora:

$$\chi_U = a_1\chi_1 + ...a_r\chi_r$$
$$\chi_V = b_1\chi_1 + ...b_r\chi_r$$

Ma i due caratteri sono equivalenti per ipotesi. Dall'equivalenza si ricava:

$$0 = \sum_{i=1}^{r} (a_i - b_i)\,\chi_i$$

e, essendo i χ_i linearmente indipendenti:

$$a_i = b_i$$

per ogni $i = 1, ..., r$. Quindi

$$U \cong V$$

come $F[G]$-moduli. Da ciò segue la tesi.

Esercizio

1. Sia $A \in GL_n(\mathbf{C})$, con $A^m = \mathbf{1}$ per $m \in \mathbf{N}$ ($\mathbf{1}$ è l'identità). Dimostrare che

$$A \sim \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix}$$

dove $\sim$ indica la relazione di coniugazione, mentre ω_i è l'i-esima radice dell'unità.

2. Supposto che la cardinalità di un gruppo G sia finita e considerata una rappresentazione $\rho : G \longrightarrow GL_n(\mathbf{C})$, si dimostri che vale la seguente disuguaglianza

$$|\chi_\rho(g)| \leq n = deg\rho$$

per ogni $g \in G$.

3. Si dimostri infine che

$$|\chi_\rho(g)| = n$$

se e solo se

$$\rho(g) = \begin{pmatrix} \omega & & 0 \\ & \ddots & \\ 0 & & \omega \end{pmatrix}_{n \times n}$$

dove ω è la $|G|$-esima radice dell'unità.
Questo equivale a dire che

$$|\chi_\rho(g)| = n$$

se e solo se

$$\rho(g) = I$$

Primo punto.
Data $A \in GL_n(\mathbf{C})$, con $A^m = \mathbf{1}$, si ha usando la *forma di Jordan*:

$$A \sim \begin{pmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$$

dove

$$A_i = \begin{pmatrix} \lambda_i^1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i^1 \end{pmatrix}$$

per $i = 1, ..., r$. I λ_i sono gli r autovalori di A.
Ora A coniugata si ottiene da

$$DAD^{-1} = \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix}$$

dove $D \in GL_n(\mathbf{C})$. Quindi

$$A^m \sim (DAD^{-1})^m = DA^mD^{-1} = I$$

da cui segue

$$\begin{pmatrix} \lambda_i^1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i^1 \end{pmatrix}^m = \begin{pmatrix} \lambda_1^m & & * \neq 0 \\ & \ddots & \\ 0 & & \lambda_r^m \end{pmatrix}$$

dove $*$ non può che essere nullo.
Il punto 1 dell'esercizio si può risolvere anche usando subito il fatto che $A^m = I$.
Da ciò si ottiene infatti

$$x^m = 1$$

Ma $x^m - 1$ è il polinomio caratteristico che ammette m radici distinte. Allora non si può avere una matrice del tipo

$$\begin{pmatrix} \lambda_i^1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i^1 \end{pmatrix}$$

ma solo una matrice della forma

$$\begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix}$$

cioè senza 1 sopra la diagonale.
Segue da questo primo punto dell'esercizio una proprietà utile nella risoluzione degli altri punti. Vediamola.

Proprietà
Siano V uno spazio vettoriale e G un gruppo di cardinalità finita m. Sia inoltre

$$\rho : G \longrightarrow GL_n(V) : g \longmapsto \rho(g)$$

una rappresentazione di G su V.
Per ogni $g \in G$, valga

$$g^m = 1$$

Allora anche

$$\rho(g)^m = \mathbf{C}$$

Inoltre

$$\chi_\rho(g) := tr\rho(g) = \sum \omega_i \in \mathbf{C}$$

e

$$\omega_i^m = 1$$

Secondo punto.
In base alla proprietà appena vista, si ha:

$$|\chi_\rho(g)| = |\sum_{i=1}^{n} \omega_i| \leq \sum_{i=1}^{n} |\omega_i| = n$$

La disuguaglianza è così dimostrata.
Terzo punto.
L'uguaglianza si ottiene dalla seguente considerazione. Se a e b sono due numeri complessi, si ha

$$|a + b| = |a| + |b|$$

solo se a e b stanno entrambi sul cerchio di raggio di raggio $|a| = |b|$. Essendo, quindi

$$\rho(g)^m = \mathbf{C}$$

per il primo punto dell'esercizio, si ha

$$\rho(g) \sim \begin{pmatrix} \omega & & 0 \\ & \ddots & \\ 0 & & \omega \end{pmatrix}$$

e perché

$$\chi_\rho(g) = n$$

deve essere

$$\omega = 1$$

Il *carattere* di G è una funzione di classi di coniugati $\{g_i\}$ di G:

$$\chi : G \longrightarrow F$$
$$G = \{g_1\} \cup \{g_2\} \cup ... \cup \{g_r\}$$

Per determinare il valore di un carattere basta quindi determinarlo per ogni classe oppure per un rappresentante della classe.

6.1 Tabella dei caratteri di un gruppo G

Sia $\{\{g_1\}, \{g_2\}, ..., \{g_r\}\}$ l'insieme delle classi di coniugazione complete di G e siano $\chi_1, \chi_2, ..., \chi_r$ i caratteri irriducibili di G su $\mathbf{C}$. La tabella dei caratteri si costruisce come segue:

$$\begin{array}{cccccc} & \{g_1\} & \{g_2\} & \cdots & \{g_r\} \\ \chi_1 & \chi_1(g_1) & \chi_1(g_2) & \cdots & \chi_1(g_r) \\ \chi_2 & \chi_2(g_1) & \chi_2(g_2) & \cdots & \chi_2(g_r) \\ \vdots & \vdots & \vdots & & \vdots \\ \chi_r & \chi_r(g_1) & \chi_r(g_2) & \cdots & \chi_r(g_r) \end{array}$$

Non esiste naturalmente un metodo universale per calcolare i caratteri (talvolta può anche essere complicato).

Esempio: gruppo diedrale $\mathbf{D_{2n}}$ ($|D_{2n}| = 2n$)
Consideriamo i poligoni regolari di n lati (triangoli, quadrati, pentagoni, ecc...) e alcuni movimenti isometrici su di essi, escluse le traslazioni, vale a dire le rotazioni di angolo $\frac{180°}{n}$, nel caso $n = 3$, e $\frac{360°}{n}$, negli altri casi, e le riflessioni rispetto ad un asse verticale passante per il baricentro. L'insieme di tali movimenti e delle loro combinazioni costituisce un gruppo, detto gruppo diedrale del poligono (del triangolo, del quadrato, del pentagono, ecc...).
Prendiamo, ad esempio, il caso del triangolo, in cui $n = 3$. Indicate rispettivamente con r e s la rotazione di 60° e la riflessione rispetto all'asse verticale, si hanno le seguenti rotazioni e riflessioni (escludendo ancora loro eventuali combinazioni):

$$r, r^2, r^3 = id$$
$$s, s^2 = id$$

Quindi l'insieme

$$\{id, r, r^2, s, rs, r^2s\}$$

è un gruppo contenente tutte le simmetrie del triangolo, di ordine 6 (che è uguale a $2n$), i cui elementi inversi sono rappresentati da $s^{-1} = s$ per le riflessioni e da $r^{-1} = r^2$ per le rotazioni. D_6 è generato dalle rotazioni e dalle riflessioni, per cui si può scrivere:

$$D_6 = \langle r, s : r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$$

Vogliamo ora trovare le classi di coniugazione di D_6. Presi l e k con $1 \leq l, k \leq n$, si ha:

$$r^l s r^k = r^{l-k} s \qquad\qquad (r^k s)(r^l s) = r^{k-l}$$

e ancora:

$$D_{2n} = \left\{ r^k s^\epsilon : 1 \leq k \leq n, \epsilon = 0, 1 \right\}$$

Consideriamo le seguenti relazioni:

$$(r^l s) r^k (r^l s)^{-1} = r^{-k} \qquad\qquad k = 1, ..., n-1$$

$$(r^l s) s (r^l s)^{-1} = r^{2l} s$$

e

$$(r^l s)(r^k s)(r^l s)^{-1} = r^{2l-k} s \begin{cases} \sim s\,, & n = 2m+1, \text{ per } \begin{cases} l = \frac{k}{2}, & k \text{ pari} \\ l = m + t, & k = 2t+1 \text{ dispari} \end{cases} \\ \sim rs\,, & n = 2m \text{ e } k \text{ dispari} \\ \sim s\,, & n = 2m \text{ e } k \text{ pari} \end{cases}$$

dove $\sim$ indica la relazione di coniugazione.
Le classi di coniugazione di D_{2n} sono perciò:

- se $n = 2m+1$, $m \geq 1$
  $\{1\}$, $\{r^k\}$ per $k = 1, ..., m$, $\{s\}$
  In totale si hanno $m+2$ classi.

- Se $n = 2m$
  $\{1\}$, $\{r^k\}$ per $k = 1, ..., m$, $\{s\}$, $\{rs\}$
  In totale si hanno $m+3$ classi.

Vediamo ora le rappresentazioni irriducibili di D_{2n} su $\mathbf{C}$:

- se $n = 2m+1$
  $\rho_1 : D_{2n} \longrightarrow GL_1(\mathbf{C}) = \mathbf{C}^* : g \longmapsto \mathbf{1}$ (rappresentazione banale)
  $\rho_2 : D_{2n} \longrightarrow GL_1(\mathbf{C}) : r \longmapsto (\mathbf{1})\ ;\ s \longmapsto (\mathbf{-1})$
  $\sigma_l,\ 1 \leq l \leq m : D_{2n} \longrightarrow GL_2(\mathbf{C}) : r \longmapsto \begin{pmatrix} \omega^l & 0 \\ 0 & \omega^{-l} \end{pmatrix}, \omega = e^{\frac{2\pi i}{n}}\ ;\ s \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  Si tratta di $m+2$ rappresentazioni irriducibili.

- Se $n = 2m$
  ρ_1, ρ_2 coincidono con quelle del caso precedente
  $\rho_3 : D_{2n} \longrightarrow GL_1(\mathbf{C}) : r \longmapsto (\mathbf{-1})$; $s \longmapsto (\mathbf{1})$
  $\rho_4 : D_{2n} \longrightarrow GL_1(\mathbf{C}) : r \longmapsto (\mathbf{-1})$; $s \longmapsto (\mathbf{-1})$
  σ_l, con $1 \leq l \leq m$, coincide con quella del caso precedente
  Si tratta di $m + 3$ rappresentazioni irriducibili.

Vogliamo infine scrivere la tabella dei caratteri di D_{2n}.

- $n = 2m + 1$

	$\{1\}$	$\{s\}$	$\{r^k\}_{k=1,\ldots,m}$
χ_{ρ_1}	1	1	1
χ_{ρ_2}	1	-1	1
$\chi_{\sigma_{l\ (l=1,\ldots,m)}}$	2	0	$2\cos\frac{2\pi kl}{n}$

- $n = 2m$

	$\{1\}$	$\{s\}$	$\{r^k\}_{k=1,\ldots,m}$	$\{rs\}$
χ_{ρ_1}	1	1	1	1
χ_{ρ_2}	1	-1	1	-1
χ_{ρ_3}	1	1	$(-1)^k$	-1
χ_{ρ_4}	1	-1	$(-1)^k$	1
$\chi_{\sigma_{l\ (l=1,\ldots,m)}}$	2	0	$2\cos\frac{2\pi kl}{n}$	0

Sia ora data una rappresentazione $\rho : G \longrightarrow GL(V)$, con V spazio vettoriale su $\mathbf{C}$. V è un $\mathbf{C}[G]$-modulo. Allora si può scrivere:

$$\chi_\rho = \chi_V$$

Proposizione 6.1 *Dati due C[G]-moduli U e V, $Hom_{\mathbf{C}}(U, V)$ è un C[G]-modulo se, per definizione, si ha:*

$$(\varphi + \psi)(u) = \varphi(u) + \psi(u)$$

per ogni $\varphi, \psi \in Hom_{\mathbf{C}}(U, V)$ e per ogni $u \in U$, e

$$(g\,\varphi)(u) := g\,\varphi(g^{-1}u) \in V$$

per ogni $g \in G$, $\varphi \in Hom_{\mathbf{C}}(U, V)$ e per ogni $u \in U$.
Si ottiene il seguente diagramma:

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & V \\ g\downarrow & & \downarrow g \\ U & \xrightarrow{g\varphi} & V \end{array}$$

Considerati g_1, $g_2 \in G$, si ha inoltre

$$((g_1 g_2)\,\varphi) = g_1(g_2\varphi)$$

Sia ora U^* il duale di U, cioè

$$U^* = Hom_{\mathbf{C}}(U, \mathbf{C})$$

(dove $\mathbf{C}$ è il C[G]-modulo banale). Allora U^* è un C[G]-modulo se U è un C[G]-modulo. Per ogni $g \in G$, $\varphi \in U^*$, $u \in U$, quindi, vale

$$(g\,\varphi)\,(u) = g\,\varphi\left(g^{-1}u\right)$$

Proposizione 6.2 *Sia V spazio vettoriale su $\mathbf{C}$. V è un C[G]-modulo. Allora:*

1. $\chi_{V^*} = \overline{\chi_V}$
   cioè
   $$\chi_{\rho^*}(g) = \overline{\chi_\rho(g)}$$
2. *Dato U C[G]-modulo, $Hom_{\mathbf{C}}(U, V)$ è un C[G]-modulo e*
   $$\chi_{Hom_{\mathbf{C}}(U,V)} = \overline{\chi_U}\chi_V$$

Dim. Dimostriamo prima il punto 2, assumendo vero il punto 1. Per avere la tesi, basta considerare il seguente isomorfismo fra spazi vettoriali:

$$\mathrm{Hom}_{\mathbf{C}}(U, V) \cong U^* \otimes_{\mathbf{C}} V$$

e il fatto che:

$$\chi_{U^*\otimes_{\mathbf{C}} V} = \chi_{U^*}\chi_V$$

Dimostriamo ora il punto 1 nel caso in cui $V = \mathbf{C}$. Sappiamo che ρ e la sua rappresentazione duale ρ^* operano nel modo che segue:

$$\begin{aligned} \rho &: G \longrightarrow GL(\mathbf{C}) \\ \rho^* &: G \longrightarrow GL(\mathbf{C}) : g \longmapsto [\rho(g)^t]^{-1} \end{aligned}$$

Inoltre:

$$\begin{aligned} G &\xrightarrow{\rho} GL(V) \\ G &\xrightarrow{\rho^*} GL(V^*) \\ g &\longmapsto \rho^*(g) : V^* \longrightarrow V^* \\ &\qquad\qquad \varphi \longmapsto \rho^*(g)\varphi : V \to \mathbf{C} \\ &\qquad\qquad\qquad\qquad v \mapsto \rho\,(g^{-1})\,v \end{aligned}$$

Possiamo scrivere:

$$\begin{aligned} \chi_\rho &= \chi_V \\ \chi_{\rho^*} &= \chi_{V^*} \end{aligned}$$

Ora,

$$\rho(g) = \begin{pmatrix} \omega_1 & & 0 \\ & \ddots & \\ 0 & & \omega_n \end{pmatrix}$$

Da qui si ottiene

$$\chi_{\rho^*}(g) = \sum_{i=1}^{n} \omega_i^{-1} = \sum_{i=1}^{n} \overline{\omega_i} = \overline{\sum \omega_i} = \overline{\chi_\rho(g)}$$

dove $\rho(g)$ è una matrice diagonale per qualsiasi gruppo finito, i cui elementi non nulli sono le radici dell'unità (i loro inversi sono quindi i coniugati in $\mathbf{C}$). Da

$$\chi_{\rho^*}(g) = \overline{\chi_\rho(g)}$$

per ogni $g \in G$ segue la tesi, per cui

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

Siano dati un gruppo G e un $C[G]$-modulo U. L'insieme

$$U^G := \{u \in U : gu = u, \forall\ g \in G\}$$

è un sottospazio vettoriale di U. Possiamo notare che il gruppo G non ha alcun effetto sugli elementi di U^G; per tale motivo U^G si chiama *sottospazio fisso* di U.

Lemma 6.1 *Dato un C[G]-modulo U, si ha*

$$dim_{\mathbf{C}} U^G = \frac{1}{|G|} \sum_{\forall\ g \in G} \chi_U(g)$$

Dim. Definiamo

$$e := \frac{1}{|G|} \sum_{\forall\ g \in G} g \in \mathbf{C}[G]$$

Per ogni $g \in G$, si ha

$$g \cdot e = e$$

e, in particolare

$$e \cdot e = e$$

vale a dire

$$e^2 = e \in \mathrm{End}_{\mathbf{C}}(U)$$

Questa scrittura equivale a

$$e(e-1) = 0 \in \mathrm{End}_{\mathbf{C}}(U)$$

Si può per questo dire:

$$U = eU \oplus (e-1)U$$

Ma allora

$$(e-1)U = \mathrm{Ker}\, e$$

da cui si ottiene

$$U = eU \oplus \mathrm{Ker}\, e$$

e

$$eU = U^G$$

Questa seconda uguaglianza segue dalla doppia inclusione. Infatti, da un lato, $eU \subseteq U^G$ è ovvia; dall'altro lato, se $u \in U^G$:

$$eu = \frac{1}{|G|} \sum_{\forall g \in G} gu = \frac{1}{|G|} \sum_{\forall g \in G} u = \frac{|G|}{|G|} u = u$$

Si ha quindi $eu \in eU$ e da questo $eU \supseteq U^G$. L'uguaglianza è così dimostrata.
Come conseguenza dell'uguaglianza, si può scrivere:

$$\dim_{\mathbf{C}} U^G = \dim_{\mathbf{C}} eU = \operatorname{tr} e = \operatorname{tr}\left(\frac{1}{|G|} \sum_{\forall g} g\right) = \frac{1}{|G|} \sum_{\forall g} \operatorname{tr}(g) = \frac{1}{|G|} \sum_{\forall g} \chi_U(g)$$

che è proprio ciò che volevamo dimostrare.

Definizione 6.2 *Siano χ_1 e χ_2 due caratteri di G su $\mathbf{C}$. Si definisce il prodotto interno dei due caratteri come la funzione*

$$(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{\forall\ g \in G} \chi_1(g) \cdot \overline{\chi_2(g)} \in \mathbf{C}$$

che soddisfa le seguenti proprietà:

1. $(\chi, \chi) \geq 0$ *e* $(\chi, \chi) = 0 \Leftrightarrow \chi = 0$
2. $(\chi_1, \chi_2) = \overline{(\chi_1, \chi_2)}$
3. $(a\chi_1, \chi_2) = a\,(\chi_1, \chi_2)$, $(\chi_1, a\chi_2) = \overline{a}\,(\chi_1, \chi_2)$
4. $(\chi_1 + \chi_2, \chi_3) = (\chi_1, \chi_3) + (\chi_2, \chi_3)$

Teorema 6.2 *Siano U e V due $C[G]$-moduli. Allora:*

$$(\chi_U, \chi_V) = dim_{\mathbf{C}} Hom_{\mathbf{C}[G]}(U, V)$$

Dim. Si ha che $\operatorname{Hom}_{\mathbf{C}[G]}(U, V) \subseteq \operatorname{Hom}_{\mathbf{C}}(U, V)$ come sottospazio e, in più

$$\operatorname{Hom}_{\mathbf{C}}(U, V)^G = \operatorname{Hom}_{\mathbf{C}[G]}(U, V)$$

in quanto $\varphi \in \operatorname{Hom}_{\mathbf{C}[G]}(U, V)$. Questo equivale infatti a dire che, per ogni $g \in G$

$$(g\varphi)(u) := g \cdot \varphi\left(g^{-1}u\right) = g \cdot g^{-1}\varphi(u) = \varphi(u)$$

e, quindi

$$\varphi \in \operatorname{Hom}_{\mathbf{C}}(U, V)^G$$

Da ciò segue:

$$(\chi_U, \chi_V) = \frac{1}{|G|} \sum_{\forall\ g \in G} \overline{\chi_U(g)} \chi_V(g) = \frac{1}{|G|} \sum_{\forall\ g \in G} \chi_{\mathrm{Hom}_{\mathbf{C}}(U,V)}(g)$$

$$= \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}}(U,V)^G = \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}[G]}(U,V)$$

dove la seconda uguaglianza deriva dalla Proposizione 12.

Corollario *Siano $\chi_1, \chi_2, ..., \chi_r$ (dove r è il numero delle classe di coniugazione di G) caratteri complessi irriducibili di G. Allora:*

$$(\chi_i, \chi_j) = \delta_{ij} \qquad 1 \leq i, j \leq r$$

6.2 Moduli induttivi

Definizione 6.3 *Siano dati un gruppo G (finito o infinito) e un sottogruppo H di G. Sia V un $F[H]$-modulo. Si chiama modulo induttivo il seguente $F[G]$-modulo:*

$$Ind\,_H^G V := F[G] \otimes_{F[H]} V$$

dove, per ogni $g \in G$, $x \in F[G]$, $v \in V$, si ha:

$$g \cdot (x \otimes v) = gx \otimes v$$

Lemma 6.2 *Siano l'indice di H in G (cioè il numero degli ideali di H in G) finito, cioè $[G : H] = n < \infty$, e*

$$G = s_1 H \cup s_2 H \cup ... \cup s_n H$$

(dove $\{s_1, s_2, ..., s_n\}$ si chiama cross section di G su H). Allora, come spazio vettoriale su F:

$$Ind\,_H^G V = \bigoplus_{i=1}^{n} s_i \otimes V$$

In particolare:

$$dim_F Ind\,_H^G V = [G : H] \cdot dim_F V$$

Dim. Abbiamo un isomorfismo di $F[H]$-moduli destri, per cui:

$$F[G] = \bigoplus_{i=1}^{n} \sum_{\forall g \in s_i H} \gamma_g g = \bigoplus_{i=1}^{n} s_i \sum_{\forall h \in H} \gamma_h h$$

Ora, per ogni $x \in F[G]$, si ha:

$$x = \sum_{i=1}^{n} \sum_{\forall g \in s_i H} \gamma_g g = \sum_{i=1}^{n} \left(s_i \sum_{\forall h \in H} \gamma_h^{(i)} h \right)$$

e per ogni $v \in V$:

$$x \otimes v = \sum_{i=1}^{n} s_i \left(\sum_{\forall h \in H} \gamma_h^{(i)} h \right) \otimes v = \sum_{i=1}^{n} s_i \otimes \sum_{\forall h \in H} \gamma_h^{(i)} h \cdot v \in \bigoplus_{i=1}^{n} s_i V$$

Quindi

$$Ind\,{}_H^G V \subseteq \bigoplus_{i=1}^{n} s_i V$$

L'altra direzione di inclusione è ovvia; allora segue la tesi.

Teorema 6.3 ***(di reciprocità Frobeniusiana)*** *Sia $[G : H] < \infty$. Dati due F[G]-moduli U e V, esiste il seguente isomorfismo fra spazi vettoriali:*

$$Hom_{F[H]}\left(V, Res_H^G U\right) \cong Hom_{F[G]}\left(Ind\,{}_H^G V, U\right)$$

Dim. Consideriamo il seguente diagramma.

$$\begin{array}{ccc} \varphi \in Hom_{F[H]}\left(V, Res_H^G U\right) \ni \delta(\psi): & V \to Res_H^G U \\ & v \mapsto \psi\left(\otimes v\right) \\ \downarrow \qquad \gamma \downarrow \uparrow \delta \qquad\qquad \downarrow & \\ U \leftarrow Ind\,{}_H^G V : \gamma(\varphi) \quad Hom_{F[G]}\left(Ind\,{}_H^G V, U\right) \ni \psi & \\ g\,\varphi(v) \leftarrow g \otimes v & \\ \forall g \in G & \end{array}$$

Ora, da $\gamma \cdot \delta = id$:

$$\left[(\gamma\delta)\left(\psi\right)\right](g \otimes v) = \left[\gamma\left(\delta(\psi)\right)\right](g \otimes v) = g \cdot \delta\left(\psi\right)(v) = g \cdot \psi\left(1 \otimes v\right) = \psi\left(g \otimes v\right)$$

e da $\delta \cdot \gamma = id$:

$$\left[(\delta\gamma)\left(\varphi\right)\right](v) = \left[\delta\left(\gamma(\varphi)\right)\right](v) = \gamma(\varphi)\left(1 \otimes v\right) = \varphi(v)$$

γ è perciò un F-morfismo per definizione e, dunque, γ è un F-isomorfismo.

Definizione 6.4 *Sia S un A-modulo semplice e $V = V_1 \oplus ... \oplus V_n$ una somma diretta di A-moduli semplici. Si definisce la molteplicità di S in V come*

$$\#\{V_i : V_i \cong S,\ i \in \{1, ..., n\}\}$$

Teorema 6.4 *Siano $H \subset G$ e $[G : H] < \infty$. Siano F algebricamente chiuso, U un F[H]-modulo semplice, V un F[G]-modulo semplice e $Ind\,{}_H^G U$ e $Res_H^G V$ completamente riducibili. Allora, la molteplicità di U in $Res_H^G V$ è uguale alla molteplicità di V in $Ind_H^G U$. Quindi, in particolare, nel caso in cui $F = \mathbf{C}$ e $|G| < \infty$, per il Teorema 11, si ha:*

$$\left(\chi_U, \chi_{Res_H^G V}\right) = \left(\chi_{Ind\,{}_H^G U}, \chi_V\right)$$

Dim. Sia $Ind\,_H^G U$ somma diretta di $F[G]$-sottomoduli semplici e sia $Res_H^G V$ somma diretta di $F[H]$-sottomoduli semplici, cioè:

$$Ind\,_H^G U = U_1 \oplus ... \oplus U_n$$

$$Res_H^G V = V_1 \oplus ... \oplus V_m$$

Si può allora dire quanto segue:

$$\begin{aligned}\dim_F \mathrm{Hom}_{F[H]}\left(U, \bigoplus_{i=1}^{m} V_i\right) &= \dim_F \bigoplus_{i=1}^{m} \mathrm{Hom}_{F[H]}(U, V_i) \\ &= \sum \dim_F \mathrm{Hom}_{F[H]}(U, V_i)\end{aligned}$$

che, per il Lemma di Schur, è uguale alla molteplicità di U in $\bigoplus_{i=1}^{m} V_i$ e inoltre la dimensione su F di

$$\mathrm{Hom}_{F[G]}\left(V, \bigoplus_{i=1}^{n} U_i\right)$$

è uguale alla molteplicità di V in $\bigoplus_{i=1}^{n} U_i$.

Dal teorema di reciprocità Frobeniusiana segue quindi che la molteplicità di U in $\mathrm{Res}_H^G V$ è uguale alla molteplicità di V in $\mathrm{Ind}\,_H^G U$.

Esempio

Siano

$$G = D_n = \langle r, s : r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle$$

e

$$H = \langle r \rangle$$

Consideriamo ora

$$\begin{aligned}\sigma : \ H &\longrightarrow GL_1(\mathbf{C}) \\ r &\longmapsto \omega\end{aligned}$$

con $\omega^n = 1$. Si ha:

$$\begin{aligned}\mathrm{Ind}\,_H^G \sigma : \ G &\longrightarrow GL_2(\mathbf{C}) \\ r &\longmapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \ s \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\end{aligned}$$

Quindi

$$\dim_F \mathrm{Ind}\,_H^G \sigma = [G : H] = 2$$

Se $H = \langle s \rangle$ allora

$$\dim_F \mathrm{Ind}\,_H^G \sigma = [G : H] = n$$

e

$$G = H \cup rH \cup ... \cup r^{n-1}H$$

dove:

$$\begin{array}{l} \mathrm{Ind}\,_H^G\sigma : \ G \longrightarrow GL_n(\mathbf{C}) \\ \qquad\qquad r \longmapsto \begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & \dots & 1 & 0 \end{pmatrix}, \ s \longmapsto \begin{pmatrix} -1 & 0 & \dots & \dots & 0 \\ 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & -1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & -1 & \dots & \dots & 0 \end{pmatrix} \end{array}$$

Proposizione 6.3 *Siano $G \supset K \supset H$ con $[G:H]$ finito. Dati U e V, rispettivamente F[G]-modulo e F[H]-modulo, si hanno le seguenti proprietà:*

1. *Come F[G]-moduli*
$$Ind\,_K^G\, Ind\,_H^K U \cong Ind\,_H^G U$$
2. *Se W è un sottomodulo di U allora $Ind\,_H^G W$ è un F[G]-sottomodulo di $Ind\,_H^G U$. Se U è somma diretta di due F[H]-moduli, cioè $U = W_1 \oplus W_2$, allora*
$$Ind\,_H^G\,(W_1 \oplus W_2) = Ind\,_H^G W_1 \oplus Ind\,_H^G W_2$$
3. *Come F[G]-moduli*
$$\left(Ind\,_H^G U\right) \otimes_{F[G]} V \cong Ind\,_H^G \left(U \otimes_{F[H]} Res_H^G V\right)$$

Bisogna notare che per ogni $g \in G, x \in F[G], u \in U, v \in V$ due F[G]-moduli del punto (3) sono definiti dalle seguenti relazioni:

$$g \cdot [(x \otimes u) \otimes v] = g\,(x \otimes u) \otimes gv = (g \cdot x \otimes u) \otimes gv$$
$$g \cdot [x \otimes (u \otimes v)] = gx \otimes (u \otimes v)$$

Dim. Punto 1.
Deriva dal fatto che

$$F[G] \otimes_{F[K]} \left(F[K] \otimes_{F[H]} U\right) \cong F[G] \otimes_{F[H]} U$$

Punto 2.
Deriva dal fatto che

$$F[G] \otimes_{F[H]} (W_1 \oplus W_2) \cong \left(F[G] \otimes_{F[H]} W_1\right) \oplus \left(F[G] \otimes_{F[H]} W_2\right)$$

Punto 3.
Si definisce la seguente funzione:

$$F[G] \otimes_{F[H]} (U \otimes V) \longrightarrow \left[F[G] \otimes_{F[H]} U\right] \otimes_{F[G]} V$$
$$g \otimes (u \otimes v) \longmapsto (g \otimes u) \otimes g \cdot v$$

per ogni $g \in G, u \in U, v \in V$. Basta ora estendere tale funzione a un $F[G]$-morfismo che è iniettivo. Confrontando infine la dimensione di dominio e codominio si ottiene la tesi.

Capitolo 7

La tavola dei caratteri di A_5

Definizione 7.1 *Denotiamo con Σ_n il gruppo delle permutazioni di $\{1, ..., n\}$ e lo chiamiamo gruppo simmetrico di grado n. L'operazione è la composizione di funzioni e l'elemento neutro è l'identità.*

Osservazione

$$|\Sigma_n| = n!$$

Definizione 7.2 *$\rho \in \Sigma_n$ è detto r-ciclo se esistono $1 \leq a_1, ..., a_r \leq n$ distinti tali che*

$$\rho(a_i) = \rho(a_{i+1})$$

e per gli altri $\rho(b) = b$.

Definizione 7.3 *Due cicli si dicono disgiunti se non ci sono due termini tra 1 e n mossi da entrambi i cicli.*

Definizione 7.4 *Ogni $\rho \in \Sigma_n$ si può vedere come prodotto di cicli disgiunti quindi posso associare a ρ una partizione detta struttura ciclica.*

Proposizione 7.1 *$\rho_1, \rho_2 \in \Sigma_n$ sono coniugati se e solo se hanno la stessa struttura ciclica.*

Definizione 7.5 *Chiamiamo A_n l'insieme delle permutazioni pari. Si tratta di un sottogruppo normale massimale di Σ_n.*

Vogliamo dunque studiare la tabella dei caratteri di A_5.
Abbiamo $|A_5| = \frac{5!}{2} = 60$. Inoltre, grazie alla Proposizione 7.1, possiamo facilmente trovare le classi di coniugazione di Σ_5 e tra queste scriviamo solo quelle che stanno in A_5:

$$1 \qquad (12)(34) \qquad (123) \qquad (12345)$$

che sono rispettivamente di ordini 1, 15, 20, 24.
Però due elementi che sono coniugati in Σ_5 non è detto che lo siano in A_5. Dobbiamo

dunque cercare le classi di coniugazione di A_5.

Preso $x \in A_5$ sia K la sua classe di coniugazione in Σ_n e F in A_5. Certamente $F \subseteq K$.

Definizione 7.6 *Dato $x \in G$ si definisce il suo centralizzatore come segue:*

$$C_G(x) = \Big\{ g \in G : gx = xg \Big\}$$

Si dimostra che x ha $|G/C_G(x)|$ coniugati.
Nel nostro caso $|K| = |\Sigma_5/C_{\Sigma_5}(x)|$ e $|F| = |A_5/C_{A_5}(x)|$. Bisogna distinguere due casi:

- $C_{\Sigma_5}(x) \not\subseteq A_5$
  allora $A_5 C_{\Sigma_5}(x) = \Sigma_5$ per la massimalità di A_5; si ha perciò

  $$\Sigma_5/A_5 = A_5 C_{\Sigma_5}(x)/A_5 \simeq C_{\Sigma_5}(x)/C_{\Sigma_5}(x) \cap A_5 = C_{\Sigma_5}(x)/C_{A_5}(x)$$

  e

  $$|A_5/C_{A_5}(x)| = \frac{|\Sigma_5/C_{A_5}(x)|}{|\Sigma_5/A_5|} = \frac{|\Sigma_5/C_{A_5}(x)|}{|C_{\Sigma_5}(x)/CA_5(x)|} = |\Sigma_5/C_{\Sigma_5}(x)|$$

  Quindi $F = K$.

- $C_{\Sigma_5}(x) \subseteq A_5$
  allora $C_{A_5}(x) = C_{\Sigma_5}(x) \cap A_5 = C_{\Sigma_5}(x)$; si ha perciò

  $$|A_5/C_{A_5}(x)| = |A_5/C_{\Sigma_5}(x)| = \frac{1}{2}|\Sigma_5/C_{\Sigma_5}(x)| = \frac{1}{2}|K|$$

  In questo caso K si spezza in A_5 in due classi di uguale cardinalità.

Si vede subito che $1, (12)(34), (123)$ commutano con una permutazione dispari, per esempio

$$(123)(45) = (45)(123)$$

Siamo dunque nel caso $C_{\Sigma_5}(x) \not\subseteq A_5$ e quindi queste tre classi in A_5 coincidono con quelle di Σ_5. Inoltre, poichè 24 non divide 60, la classe di (12345) si scinde in due classi di ordine 12.
Gli ordini delle classi di coniugazione di A_5 sono 1, 15, 20, 12, 12.
Mostriamo ora che $x = (12345)$ e $x^2 = (13524)$ non sono coniugati:
per assurdo, esista $g \in A_5$ tale che

$$gxg^{-1} = x^2$$

ma, allora

$$g < x > g^{-1} =< x^2 >=< x >$$

ovvero

$$g \in N_{A_5}(< x >) = \Big\{ g \in A_5 : g < x > g^{-1} =< x > \Big\}$$

che è detto normalizzatore di $< x >$.

Definizione 7.7 *Sia G un gruppo finito e p un divisore primo di $|G|$. $H \subseteq G$ è un Sylow p-sottogruppo se è un p-sottogruppo di ordine $|G|_p$, dove $|G|_p = p^n$ con n tale che p^n divide $|G|$, ma p^{n+1} non più.*

Teorema 7.1 ***(di Sylow)*** *Dato un guppo G finito, si ha che:*

- *il numero di Sylow p-sottogruppi di G divide $\frac{|G|}{|G|_p}$ ed è congruo 1 modulo p.*
- *Tutti i Sylow p-sottogruppi sono coniugati.*

Dunque, $< x >$ è un Sylow 5-sottogruppo di A_5; per il Teorema di Sylow, A_5 deve avere un numero di Sylow 5-sottogruppi che divida 12 e sia congruo 1 modulo 5. Le possibilità sono quindi 1 o 6. Ma, siccome ogni 5-ciclo genera un sottogruppo di ordine 5, A_5 deve avere necessariamente 6 Sylow 5-sottogruppi tutti coniugati.
A questo punto, dato che un sottogruppo P ha $|G/N_G(P)|$ coniugati, si ha

$$|N_{A_5}(< x >)| = 10$$

In particolare

$$N_{A_5}(< x >) =< x > \times < t >= D_{10}$$

con $t = (25)(34)$. Notiamo ora che

$$txt^{-1} = x^{-1} \neq x^2$$

dunque non può esistere nessun g in $N_{A_5}(< x >)$ tale che

$$gxg^{-1} = x^2$$

il che è appunto assurdo.
Le classi di coniugazione di A_5 sono dunque

$$1 \qquad (12)(34) \qquad (123) \qquad (12345) \qquad (13524)$$

Mostriamo perciò la tecnica con la quale cercheremo i caratteri. Sia X un insieme finito e

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & gx \end{array}$$

un'azione di un gruppo G. Allora lo spazio vettoriale $C(X)$ di base X è un $C[G]$-modulo. Possiamo quindi considerare la rappresentazione associata

$$\begin{array}{rccc} \rho: & G & \longrightarrow & GL(C(X)) \\ & g & \longmapsto & \rho(g) \end{array}$$

dove, la matrice $\rho(g)$ rappresenta una trasformazione lineare definita da g rispetto alla base X. Ed essendo $gx \in X$ per ogni $x \in X$ si tratta di una matrice di permutazione. Il

carattere χ, quindi, associa ad ogni $g \in G$ il numero dei punti fissati da g.
Inoltre, se χ_1 è il carattere principale di G, si verifica che

$$(\chi, \chi_1) = \sum_{\text{orbita } O} 1$$

Dunque se G agisce transitivamente su X (si ha cioè una sola orbita) il carattere $\chi - \chi_1$ non contiene χ_1 nella sua rappresentazione come combinazione lineare di caratteri irriducibili. Per dimostrare ciò abbiamo bisogno del seguente lemma.

Lemma 7.1 *Se $\alpha = \sum_i a_i\chi_i$ è un carattere virtuale, χ_j compare in α con coefficiente (α, χ_j).*

Dim.
Osserviamo innanzitutto che, se $\alpha = \sum_i a_i\chi_i$ e $\beta = \sum_j b_j\chi_j$ sono due caratteri virtuali, allora:

$$(\alpha, \beta) = (\sum_i a_i\chi_i, \sum_j b_j\chi_j) = \sum_i a_i \sum_j b_j(\chi_i, \chi_j) = \sum_i a_i b_i$$

dunque

$$(\alpha, \chi_j) = a_j$$

Vediamo quindi cosa succede per $\chi - \chi_1$:

$$\chi - \chi_1 = (\chi, \chi_1)\chi_1 + ... + (\chi, \chi_r)\chi_r - \chi_1 = (\chi, \chi_2)\chi_2 + ... + (\chi, \chi_r)\chi_r$$

Usiamo tutto questo per trovare i caratteri di A_5:
Prendiamo $X = \{1, 2, 3, 4, 5\}$ e notiamo che A_5 agisce transitivamente su X nel modo naturale. Se denotiamo con π il carattere associato al $C(A_5)$-modulo $C(X)$ allora abbiamo:

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
π	5	1	2	0	0
$\pi - \chi_1$	4	0	1	-1	-1

Inoltre, se chiamiamo k_i gli ordini delle classi di coniugazione:

$$(\pi - \chi_1, \pi - \chi_1) = \frac{1}{|A_5|}\sum_{i=1}^{5} k_i[\pi - \chi_1(g_i)]^2 = \frac{1}{60}(16 + 0 + 20 + 12 + 12) = 1$$

Quindi $\pi - \chi_1$ non contiene χ_1 ed è irriducibile per il seguente Lemma.

Lemma 7.2 *Se α è un carattere virtuale*

$$(\alpha, \alpha) = n \quad (n = 1, 2, 3) \Leftrightarrow \alpha \quad \text{è somma di } n \text{ caratteri irriducibili}$$

Dim.
Come abbiamo visto nel lemma precedente, vale quanto segue:

$$(\alpha, \alpha) = \sum_i a_i^2$$

Dunque perchè $\sum_i a_i^2$ sia n bisogna che ci siano esattamente n coefficienti uguali a 1 e tutti i restanti nulli. Nel nostro caso si ha $n = 1$ quindi $\pi - \chi_1$ è irriducibile ed è diverso da χ_2. Chiamiamo $\chi_2 = \pi - \chi_1$.
Possiamo scrivere le prime due righe della tabella dei caratteri di A_5:

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3					
χ_4					
χ_5					

Consideriamo ora l'insieme Y dei sottoinsiemi di X composti da due elementi, ovvero

$$Y = \Big\{(1,2),(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5),(4,5)\Big\}$$

Abbiamo un'azione transitiva data da A_5 in Y e il carattere irriducibile ψ associato al $C(A_5)$-modulo $C(Y)$ si comporta così:

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
ψ	10	2	1	0	0
$\psi - \chi_1$	9	1	0	-1	-1

Inoltre:

$$(\psi - \chi_1, \psi - \chi_1) = 2$$

quindi $\psi - \chi_1$ è somma di due caratteri irriducibili (per il Lemma 1.1), nessuno dei quali è χ_1 essendo l'azione transitiva.
A questo punto, poiché

$$(\psi - \chi_1, \chi_2) = 1$$

abbiamo che uno dei due moduli irriducibili è proprio χ_2 (per Lemma 1.2) e possiamo chiamare χ_3 l'altro; dunque:

$$\psi - \chi_1 = \chi_2 + \chi_3 \Rightarrow \chi_3 = \psi - \chi_1 - \chi_2$$

Ricordiamo ora che, in generale, $|G| = \sum_i n_i^2$, dove gli n_i sono i gradi di G. Quindi:

$$60 = |A_5| = \sum_i n_i^2 \Rightarrow n_4^2 + n_5^2 = 18 \Rightarrow n_4 = n_5 = 3$$

e la tabella dei caratteri si può completare parzialmente:

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3				
χ_5	3				

Ci serve adesso la seguente proprietà.

Proposizione 7.2 *Sia G un gruppo di ordine n, U un $C[G]$-modulo, ρ la rappresentazione associata e $g \in G$ di ordine n; allora:*

- *$X_U(g)$ è somma di $X_U(1)$ radici dell'unità.*
- *$X_U(g^{-1}) = \overline{X_U(g)}$.*

Inoltre abbiamo bisogno dei noti teoremi di ortogonalità delle righe e delle colonne.

Teorema 7.2 ***(di ortogonalità delle righe)*** *Dato che*

$$(\chi_i, \chi_j) = \delta_{ij}$$

allora

$$\delta_{ij} = \frac{1}{|G|}\sum_{g\in G} X_i(g)\overline{\chi_j(g)} = \frac{1}{|G|}\sum_{t=1}^{r} k_t\chi_i(g_t)\overline{\chi_j(g_t)}$$

Teorema 7.3 ***(di ortogonalità delle colonne)***

$$\sum_{t=1}^{r} \chi_t(g_i)\overline{\chi_t(g_j)} = \frac{|G|}{k_i}\delta_{ij}$$

Dim.
Diamo solo un cenno di dimostrazione. Sia $X = (\chi_i(g_j))$ la matrice tabella dei caratteri di G e K la matrice diagonale con i k_i sulla diagonale principale. Allora:

$$\left(XK\overline{X}^t\right)_{ij} = |G|\delta_{ij}$$

ovvero

$$|G|I = \left(XK\overline{X}^t\right)$$

Siccome, tuttavia, AB è la matrice scalare si ha allora $AB = BA$ e

$$|G|\delta_{ij} = \sum_{t=1}^{r}\left(K\overline{X}^t\right)_{jt}X_{ti} = \sum_{t=1}^{r}\chi_i(g_t)\overline{\chi_j(g_t)}$$

e questo è proprio quello che volevamo dimostrare.

Ora, se $a = \chi_4((12)(34))$ e $b = \chi_5((12)(34))$, grazie all'ortogonalità delle colonne, si trova che

$$0 = \sum_{i=1}^{5} n_i \chi_i((12)(34)) \Rightarrow a + b = -2$$

e, dovendo a e b essere somma di 3 radici dell'unità (per la Proposizione 7.2), necessariamente $a, b \in \{1, 3, -1, -3\}$.
Sempre grazie all'ortogonalità delle colonne poi

$$4 = \frac{60}{15} = \sum_{i=1}^{5} [\chi_i((12)(34))]^2 \Rightarrow a^2 + b^2 = 2$$

Possiamo concludere dunque che $a = b = -1$. Inoltre

$$3 = \frac{60}{20} = \sum_{i=1}^{5} [\chi_i((123))]^2 \Rightarrow \chi_4((123))\chi_5((123)) = 0$$

Aggiorniamo allora la tabella:

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0		
χ_5	3	-1	0		

essendo poi $x = (12345)$ e $x^{-1} = (54321)$ coniugati (in quanto abbiamo visto che $txt^{-1} = x^{-1}$). Inoltre:

$$\chi_4(x) = \chi_4(x^{-1})$$

dunque $\chi_4(x)$ è reale (per la Proposizione 1.2). Lo stesso discorso si può fare per $\chi_5(x)$, $\chi_4(x^2)$ e $\chi_5(x^2)$.
Chiamando allora $c = \chi_4(x)$ e $d = \chi_4(x^2)$, grazie all'ortogonalità delle righe:

$$0 = \sum_{t=1}^{r} k_t \chi_4(g_t)\chi_1(g_t) \Rightarrow c + d = 1$$

ed essendo χ_4 a valori reali:

$$60 = |A_5| = \sum_{t=1}^{r} k_t [\chi_4(g_t)]^2 \Rightarrow c^2 + d^2 = 3$$

Da queste due condizioni si trova che

$$c = \frac{1+\sqrt{5}}{2} \qquad d = \frac{1-\sqrt{5}}{2}$$

In modo analogo si ha che

$$\chi_5(x) = \frac{1-\sqrt{5}}{2} \qquad \chi_5(x^2) = \frac{1+\sqrt{5}}{2}$$

e si può finalmente completare la tabella come segue.

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_5	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$