Rappresentazioni di gruppi finiti e teoria dei caratteri

Paolo Dolce

12 novembre 2012

Indice

Capitolo 1

Rappresentazione di gruppi e FG-moduli

1.1 Concetti principali

Definizione. Sia G un gruppo finito, e sia inoltre V uno spazio vettoriale su un campo F con $dim(V) = n < \infty$. Allora una *rappresentazione* (lineare) di G su V è un omomorfismo di gruppi:

$$\rho : G \longrightarrow GL(V)$$

Il numero naturale $dim(V)$ è detto grado della rappresentazione, e se inoltre ρ è un omomorfismo iniettivo, la rappresentazione si dirà *fedele*.

In pratica, una rappresentazione di un gruppo, è un modo di vedere ogni suo elemento come applicazione lineare invertibile, mantenendo però le proprietà algebriche, che vengono "trasportate" dall'omomorfismo. In questo modo molti problemi di teoria dei gruppi sono trasferiti all'algebra lineare, e dunque è possibile "visualizzare geometricamente" gli elementi di un gruppo.

Esempio 1.1. Sia V uno spazio vettoriale su F con $dim(V) = n$, e sia inoltre $\rho : G \to GL(V)$ con $g\rho = I_n \ \forall g \in G$, allora è chiaro che ρ è una rappresentazione, poiché $(gh)\rho = I_n = I_n I_n = (g\rho)(h\rho)$ ed è detta *rappresentazione banale*. Segue che il grado di una rappresentazione può essere grande a piacere.

Sia ρ una rappresentazione di G su V, allora considerando $T \in GL(V)$, la funzione

$$\begin{array}{rcl} \sigma : G & \longrightarrow & GL(V) \\ g & \longmapsto & T^{-1}(g\rho)T \end{array}$$

è anch'essa una rappresentazione di G su V, infatti:

$$(gh)\sigma = T^{-1}(gh)\rho T = T^{-1}(g\rho)(h\rho)T = (T^{-1}(g\rho)T)(T^{-1}(h\rho)T) = (g\sigma)(h\sigma)$$

Allora in generale:

Definizione. Due rappresentazioni di G su V e W, rispettivamente chiamate ρ e σ, si dicono *equivalenti* se esiste una funzione $T : V \to W$ lineare e invertibile tale che $g\sigma = T^{-1}(g\rho)T$.

È facile provare che quella definita sopra è una relazione di equivalenza e inoltre se $V = W$ allora T è un cambiamento di base.
Si guardi ora all'azione di un gruppo su uno spazio vettoriale:

Definizione. Sia G un gruppo e V uno spazio vettoriale di dimensione $n < \infty$ su un campo F. Allora V si dice un *FG-modulo* se G agisce su V mediante:

$$\begin{array}{rcl} \mu : V \times G & \longrightarrow & V \\ (v, g) & \longmapsto & v^g \end{array}$$

tale che:

i) $(v^g)^h = v^{gh} \quad \forall g, h \in G$ e $\forall v \in V$

ii) $v^1 = v \quad \forall v \in V$

iii) $(\lambda v)^g = \lambda v^g \quad \forall g \in G$, $\forall v \in V$ e $\forall \lambda \in F$

iv) $(v + u)^g = v^g + u^g \quad \forall g \in G$ e $\forall v, u \in V$

Notare come le proprietà *i)* e *ii)* si riferiscono all'azione di G sull'insieme V, mentre le proprietà *iii)* e *iv)* indicano che l'azione è lineare rispetto la prima componente e dunque viene rispettata la struttura algebrica dello spazio vettoriale. Esiste inoltre una strettissima relazione tra FG - moduli e rappresentazioni di gruppi:
Sia V un FG-modulo e si definisca la funzione

$$\begin{array}{rcl} M_g : V & \longrightarrow & V \\ v & \longmapsto & v^g \end{array}$$

Dalle proprietà *iii)* e *iv)* della definizione precedente segue che M_g è un endomorfismo di V, e vale inoltre che

$$v(M_g M_{g^{-1}}) = (v^g)^{g^{-1}} = v^{gg^{-1}} = v$$
$$v(M_{g^{-1}} M_g) = (v^{g-1})^g = v^{g^{-1}g} = v$$

dunque M_g è un automorfismo di V, ovvero appartiene a $GL(V)$. Si definisca ora

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL(V) \\ g & \longmapsto & M_g \end{array}$$

si vede che tale funzione ρ è un omomorfismo di gruppi, infatti:

$$v((gh)\rho) = vM_{gh} = v^{gh} = (v^g)^h = v(M_g M_h) = v((g\rho)(h\rho))$$

e quindi si conclude che ρ è una rappresentazione di G su V. Dunque a un FG-modulo è possibile associare in modo unico una rappresentazione lineare.
Viceversa, sia ρ una rappresentazione lineare di G su V, allora si pone $v^g = v(g\rho)$. Valgono allora le 4 proprietà che definiscono un'azione lineare sullo spazio vettoriale V:

i) $(v^g)^h = v((g\rho)(h\rho)) = v((gh)\rho) = v^{gh} \quad \forall g, h \in G$ e $\forall v \in V$

ii) $v^1 = v(1\rho) = v(id) = v \quad \forall v \in V$

iii) $(\lambda v)^g = \lambda v(g\rho) = \lambda(v(g\rho)) = \lambda v^g \quad \forall g \in G$, $\forall v \in V$ e $\forall \lambda \in F$

iv) $(v+u)^g = (v+u)(g\rho) = v(g\rho) + u(g\rho) = v^g + u^g \quad \forall g \in G$ e $\forall v, u \in V$

Segue che V è un FG-modulo, ovvero ad una rappresentazione di G è possibile quindi associare in modo unico un FG-modulo.
Si può dire di più, infatti data una rappresentazione ρ, come appena mostrato si può costruire un'azione data da $v^g = v(g\rho)$; se a questo punto si vuole ricavare un'ulteriore rappresentazione ρ_1 tale che $g\rho_1 = M_g$ si avrà

$$v(g\rho_1) = vM_g = v^g = v(g\rho) \quad \forall v \in V$$

ovvero $\rho = \rho_1$. Viceversa data un'azione μ, prima si ricava la rappresentazione ρ tale che $g\rho = M_g$, se in seguito da essa si vuole costruire nell'usuale modo un'azione μ_1 si ha:

$$(v, g)\mu_1 = v(g\rho) = vM_g = v^g = (v, g)\mu$$

dunque $\mu = \mu_1$. Si conclude che rappresentazioni di un gruppo su uno spazio vettoriale e le azioni di G sullo stesso spazio vettoriale sono in corrispondenza biunivoca mediante la legge ampiamente descritta. È chiaro dunque che parlare di rappresentazioni di gruppi oppure di FG-moduli è indifferente, e per questo, con un leggero abuso di notazione, spesso si dirà che un FG-modulo è la coppia (V, ρ), dove V è uno spazio vettoriale sul campo F e ρ è una rappresentazione di G su V.
Il seguente lemma risulta utile per decidere quando particolari funzioni sono in realtà rappresentazioni di gruppi:

Lemma 1.2. *Sia D_{2n} il gruppo diedrale di ordine $2n$ e sia inoltre H un gruppo che contiene due elementi x e y tali che $x^n = y^2 = 1$ e $y^{-1}xy = x^{-1}$. Segue allora che la funzione*

$$\begin{array}{rcl} \theta : D_{2n} & \longrightarrow & H \\ a^i b^j & \longmapsto & x^i y^j \end{array}$$

con $0 \leq i \leq n-1$ e $0 \leq j \leq 1$ è un omomorfismo di gruppi.

Dimostrazione. Si considerino $0 \leq r \leq n-1$, $0 \leq s \leq 1$, $0 \leq t \leq n-1$ e $0 \leq u \leq 1$ tali che $a^i b^j = a^r b^s a^t b^u$ per qualche $0 \leq i \leq n-1$ e $0 \leq j \leq 1$. Allora vale che:

$$(a^r b^s a^t b^u)\theta = (a^i b^j)\theta = x^i y^j = {}^{1} = x^r y^s x^t y^u = (a^r b^s)\theta(a^t b^u)\theta$$

Si conclude quindi che θ è un omomorfismo di gruppi. □

[1] Segue dal fatto che che le stesse relazioni che caratterizzano i generatori di D_n valgono per x e y in H

Esempio 1.3. Sia $G = D_8 = \langle a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1} \rangle$ e $V = \mathbb{R}^2$. Siano inoltre

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Vale che $A^4 = B^2 = I$ e $B^{-1}AB = A^{-1}$ allora per il lemma 1.2 la funzione:

$$\begin{array}{rcl} \rho : G & \longrightarrow & GL(V) \\ a^i b^j & \longmapsto & A^i B^j \end{array}$$

è una rappresentazione di G su $\mathbb{R}$ di grado 2. Per quanto detto in precedenza lo spazio vettoriale $\mathbb{R}^2$, insieme all'azione $v^g = v(g\rho)$ è un $\mathbb{R}D_8$-modulo. In particolare $a\rho = A$ e $b\rho = B$, e considerando una base $\mathcal{B} = \{v_1, v_2\}$ con $v_1 = (1, 0)$ e $v_2 = (0, 1)$, si ha che:

$$v_1^a = v_1(a\rho) = (1,0)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (0,1) = v_2$$

$$v_1^b = v_1(b\rho) = (1,0)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (1,0) = v_1$$

$$v_2^a = v_2(a\rho) = (0,1)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (-1,0) = -v_1$$

$$v_2^b = v_2(b\rho) = (0,1)\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = (0,-1) = -v_2$$

Basta la conoscenza di questi quattro valori per deterrminare $v^g \ \forall v \in \mathbb{R}^2$ e $\forall g \in D_8$, infatti:

$$v^g = (\alpha v_1 + \beta v_2)^{a^i b^j} = \alpha (v_1)^{a^i b^j} + \beta (v_2)^{a^i b^j} \qquad \alpha, \beta \in \mathbb{R}$$

In generale dato un FG-modulo V e un gruppo G, se $\{v_1, \ldots, v_n\}$ è una base di V e gli elementi $g_1, \ldots, g_r$ generano G, allora la sola conoscenza di ${v_i}^{g^j}$ con $1 \leq i \leq n$, e $1 \leq j \leq r$ permette di definire l'intera azione lineare di G su V. Fino ad ora sono stati costruiti FG-moduli partendo da rappresentazioni, ma questo non é l'unico modo. Si consideri uno spazio vettoriale V e una sua base $\mathcal{B} = \{v_1, \ldots, v_n\}$, allora è possibile definire l'azione ${v_i}^g$ di un gruppo G su V solamente per gli elementi della base, per poi estendere tale azione per linearità a tutti gli altri elementi di V nel seguente modo:

$$(\lambda_1 v_1 + \ldots + \lambda_n v_n)^g = \lambda_1 {v_1}^g + \ldots + \lambda_n {v_n}^g$$

Chiaramente per poter fare tale operazione è necessario che l'azione di G sugli elementi di $\mathcal{B}$ rispetti certe proprietà espresse dal seguente lemma, che è possibile dimostrare attraverso semplici calcoli di routine:

Lemma 1.4. *Sia V uno spazio vettoriale con una base $\mathcal{B} = \{v_1, \ldots, v_n\}$, e si definisca $(v_i)^g$ per ogni $1 \leq i \leq n$ in modo tale che:*

o) ${v_i}^g \in V \quad \forall v_i \in \mathcal{B}$ *e* $\forall g \in G$

i) $({v_i}^g)^h = {v_i}^{gh} \quad \forall g, h \in G$ *e* $\forall v_i \in \mathcal{B}$

ii) $v_i{}^1 = v_i \quad \forall v_i \in \mathcal{B}$

iii) $(\lambda v_i)^g = \lambda {v_i}^g \quad \forall g \in G,\ \forall v_i \in \mathcal{B}\ e\ \forall \lambda \in F$

iv) $(v_i + v_j)^g = {v_i}^g + {v_j}^g \quad \forall g \in G\ e\ \forall v_i, v_j \in \mathcal{B}$

Allora estendendo l'azione per linearità segue che V è un FG-modulo.

1.2 FG-sottomoduli e FG-omomorfismi

Sia V un FG-modulo, e sia inoltre U un sottospazio vettoriale di V. Si dirà che U è un *FG-sottomodulo* di V se e solo se, U è anch'esso un FG-modulo. Osservando che in U le quattro proprietà che caratterizzano un FG-modulo sono ereditate naturalmente da V, si ricava subito una definizione alternativa e ben più utile di FG-sottomodulo:

Definizione. Un sottospazio vettoriale U di un FG-modulo V, è un FG-sottomodulo di V se e solo se $u^g \in U\ \ \forall u \in U$ e $\forall g \in G$.

In sostanza un FG-sottomodulo non è altro che un sottospazio invariante sotto l'azione del gruppo G.

Esempio 1.5. I sottospazi vettoriali $\{0\}$ e V sono FG-sottomoduli di V.

Definizione. Se un FG-modulo V non ha sottomoduli a parte $\{0\}$ e V, è detto *irriducibile*, altrimenti è *riducibile*.

Esempio 1.6. Considerando lo stesso FG-modulo dell'Esempio 1.3, si dimostra allora che esso è irriducibile. Sia $(u_1, u_2) \in \mathbb{R}^2$, allora

$$(u_1, u_2)^a = (u_1, u_2)A = (-u_2, u_1) \tag{1.1}$$

$$(u_1, u_2)^b = (u_1, u_2)B = (u_1, -u_2) \tag{1.2}$$

Si supponga che esista un sottomodulo U di $\mathbb{R}^2$ diverso da $\mathbb{R}^2$ stesso, quindi tale che $dim(U) \leq 1$. Segue che $U = span\big((x_1, x_2)\big)$ per un certo $(x_1, x_2) \in \mathbb{R}^2$, e siccome U è un sottospazio invariante sotto l'azione di D_8, allora $(x_1, x_2)^a$ e $(x_1, x_2)^b$ devono essere dei multipli scalari di (x_1, x_2). Dalle equazioni 1.1 e 1.2 si evince però che $(x_1, x_2) = (0, 0)$, e quindi $U = \{0\}$. Si può concludere dunque che $(\mathbb{R}^2, \rho)$ è irriducibile.

Si consideri un FG-modulo V ed un suo sottomodulo U, e si costruisca lo spazio vettoriale quoziente V/U. È possibile ora definire un'azione di un gruppo G su V/U nel seguente modo:

$$\begin{array}{rcl} \mu : V/U \times G & \longrightarrow & V/U \\ (U + v,\ g) & \longmapsto & (U + v)^g = U + v^g \end{array}$$

Prima di tutto bisogna provare che tale azione è ben definita:
sia $U + v_1 = U + v_2$ con $v_1 \neq v_2$, quindi $v_1 - v_2 \in U$, ma dal momento che U è un sottomodulo di V, allora ${v_1}^g - {v_2}^g = (v_1 - v_2)^g \in U$. Segue allora che $U + {v_1}^g = U + {v_2}^g$. Restano da verificare i quattro assiomi che caratterizzano un FG-modulo:

i) $((U+v)^g)^h = (U+v^g)^h = (U+v^{gh}) = (U+v)^{gh} \quad \forall g,h \in G$ e $\forall v \in V$

ii) $(U+v)^1 = (U+v^1) = U+v \quad \forall v \in V$

iii) $(\lambda(U+v))^g = (U+\lambda v)^g = U+\lambda v^g = \lambda(U+v)^g \quad \forall g \in G$, $\forall v \in V$ e $\forall \lambda \in F$

iv) $((U+v_1)+(U+v_2))^g = (U+(v_1+v_2))^g = U+({v_1}^g+{v_2}^g) =$
$= (U+v_1)^g + (U+v_2)^g \quad \forall g \in G$ e $\forall v_1, v_2 \in V$

Si conclude quindi che V/U è un FG-modulo ed è detto *FG-modulo quoziente*.

Le funzioni fra FG-moduli che preservano la struttura algebrica sono gli *FG-omomorfismi*.

Definizione. Siano V e W due FG-moduli, allora una funzione $\theta : V \longrightarrow W$ è un FG-omomorfismo se e solo se θ è lineare e inoltre $(v^g)\theta = (v\theta)^g \ \forall v \in V$ e $\forall g \in G$.

In pratica se θ manda v in w, allora si ha che θ manda anche v^g in w^g. Inoltre se θ è anche biunivoca si dice essere un *isomorfismo* e si scrive $V \cong U$, ovvero V è isomorfo a U (mediante l'isomorfismo θ).

Lemma 1.7. *Due FG-moduli V e W sono isomorfi se e solo se le rappresentazioni di G su V e di G su W sono equivalenti.*

Dimostrazione. ($\Leftarrow$) Sia ρ la rappresentazione di G su V e σ la rappresentazione di G su W con $g\sigma = T^{-1}(g\rho)T$ dove T è una funzione lineare e invertibile da V in W. Allora è facile vedere che T è proprio l'isomorfismo fra i due FG-moduli, infatti:

$$(v^g)T = v(\rho g)T = vTT^{-1}(\rho g)T = (vT)\big(T^{-1}(\rho g)T\big) = (vT)^g$$

($\Rightarrow$) Sia $\theta : V \to W$ un isomorfismo fra FG-moduli, e siano ρ con $g\rho = M_g$ e σ con $g\sigma = N_g$ le rappresentazioni[2] rispettivamente di G su V e di G su W. Dal momento che $(v^g)\theta = (v\theta)^g$, allora si ha $(v)M_g\theta = (v)\theta N_g$, ovvero $M_g\theta = \theta N_g$ da cui segue che $N_g = \theta^{-1}M_g\theta$ e quindi le due rappresentazioni sono equivalenti. □

Come nel caso della teoria dei gruppi o degli anelli, un FG-omomorfismo da origine ad alcuni FG-sottomoduli in maniera naturale come espresso dal seguente lemma.

Lemma 1.8. *Siano V e W due FG-moduli e sia θ un FG-omomorfismo fra essi, allora $Ker(\theta)$ è un FG-sottomodulo di V e $Im(\theta)$ è un FG-sottomodulo di W.*

Dimostrazione. Sia $v \in Ker(\theta)$, ovvero $v\theta = 0$; ovviamente si ha che $Ker(\theta)$ è sottospazio di V, e inoltre

$$0 = v\theta = (v\theta)^g = (v^g)\theta \quad \forall v \in Ker(\theta) \text{ e } \forall g \in G$$

[2] M_g è l'automorfismo di V tale che $vM_g = v^g$ mentre N_g è l'automorfismo di W tale che $wN_g = w^g$

quindi $Ker(\theta)$ è un FG-sottomodulo di V.
Sia $w \in Im(\theta)$, ovvero $w = v\theta$; anche in questo caso dall'algebra lineare si sa che $Im(\theta)$ è sottospazio di W, e vale inoltre che

$$w^g = (v\theta)^g = (v^g)\theta \in Im(\theta) \quad \forall w \in Im(\theta) \text{ e } \forall g \in G$$

dunque $Im(\theta)$ è un sottomodulo di W. □

A questo punto, sempre prendendo spunto da quanto si fa per le strutture algebriche di base, è semplice dimostrare il primo teorema di omomorfismo per FG-moduli:

Teorema 1.9. *Se θ è un omomorfismo tra due FG-moduli V e W, allora segue che $V/Ker(\theta) \cong Im(\theta)$.*

1.3 Il teorema di Maschke

Un risultato di estrema importanza nello studio degli FG-moduli, afferma che sotto opportune ipotesi sull'ordine di G, è sufficiente conoscere solamente gli FG-moduli irriducibili per poter esprimere un qualsiasi FG-modulo. Tale risultato come si vedrà a breve è una conseguenza del teorema di Maschke.

In generale per gli spazi vettoriali si ha che, preso un sottospazio U di V, esiste un altro sottospazio W tale che $V = U \oplus W$, se però U è un FG-sottomodulo di V, non è detto che anche W sia anche un FG-sottomodulo.

Definizione. Sia V un FG-modulo di dimensione finita, allora se per ogni FG-sottomodulo U, esiste un FG-sottomodulo W tale che $V = U \oplus W$, si dice che V è *completamente riducibile.*

Lemma 1.10. *Un FG-modulo V è completamente riducibile se e solo se V è somma diretta di suoi FG-sottomoduli irriducibili.*

Dimostrazione. ($\Rightarrow$) Sia S la somma (diretta) di tutti gli FG-sottomoduli irriducibili di V. Si supponga per assurdo che il lemma sia falso, allora $dim(S) < dim(V)$, ma S è un FG-sottomodulo di V che a sua volta è completamente riducibile, perciò esiste un FG-sottomodulo T tale che $V = S \oplus T$. Ma d'altra parte T contiene sicuramente qualche sottomodulo irriducibile di V, e visto che $S \cap T = \{0\}$ si ha una contraddizione sulla struttura di S.
($\Leftarrow$) Sia $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ con V_i FG-sottomodulo irriducibile di V $\forall i \in \{1, \ldots, n\}$ e sia inoltre W un FG-sottomodulo di V. Per il lemma di Zorn, esiste FG-sottomodulo U di V massimale rispetto alla proprietà $W \cap U = \{0\}$, basta dimostrare dunque che $W + U = V$. Si supponga per assurdo che $W + U \neq V$, allora possiamo scegliere un certo V_j con $j \in \{1, \ldots n\}$ che non è sottospazio vettoriale di $W + U$; ma V_j è irriducibile, quindi $(W + U) \cap V_j = \{0\}$. Si consideri ora $W \cap (U + V_j)$, chiaramente $W \cap (U + V_j) \subseteq W + U$ e inoltre:

$$W \cap (U + V_j) \subseteq (W + V_j) \cap (U + V_j) \subseteq (W \cap U) + V_j = V_j$$

Segue quindi che $W \cap (U + V_j) \subseteq (W + U) \cap V_j = \{0\}$, ma chiaramente $U \subset (U + V_j)$, contraddicendo così le ipotesi sulla massimalità su U. □

Teorema 1.11 (di Maschke)**.** *Sia G un gruppo finito e sia inoltre F un campo. Se $char(F) \nmid |G|$, allora ogni FG-modulo è completamente riducibile.*

Dimostrazione. Sia V un FG-modulo e W un suo FG-sottomodulo, esiste allora un sottospazio U_0 complementare a W in V tale che $V = W \oplus U_0$. Sia $\varphi : V \to W$ la proiezione di V su W, con $(w + u_0)\varphi = w$, allora:

$$((w+u_0)+(w'+u_0'))\varphi = w+w' = (w+u_0)\varphi+(w'+u_0')\varphi \ \ \forall w, w' \in W \text{ e } \forall u_0, u_0' \in U_0$$

$$\lambda(w + u_0)\varphi = \lambda w = (\lambda(w + u_0))\varphi \ \ \forall w \in W, \forall u_0 \in U_0 \text{ e } \forall \lambda \in F$$

Dunque φ è lineare. Si definisca ora la funzione, $\theta : V \to W$ tale che:

$$v\theta = \frac{1}{|G|} \sum_{g \in G} ((v^g)\varphi)^{g^{-1}}$$

Dove con $1/|G|$ si intende l'inverso dell'immagine di $|G|$ mediante l'omomorfismo caratteristico tra $\mathbb{Z}$ e F. Si noti che il nucleo di tale omomorfismo caratteristico è $char(F)\mathbb{Z}$, dunque siccome $char(F) \nmid |G|$, segue che $1/|G|$ è sempre definito. Chiaramente dalla linearità di φ e dell'azione di G su V, segue che anche θ è lineare e vale che:

$$(v^h)\theta = \frac{1}{|G|} \sum_{g \in G} ((v^{hg})\varphi)^{g^{-1}} = \frac{1}{|G|} \sum_{g \in G} \left(((v^{hg})\varphi)^{(hg)^{-1}} \right)^h =$$

$$^{3} = \left(\frac{1}{|G|} \sum_{hg \in G} ((v^{hg})\varphi)^{(hg)^{-1}} \right)^h = (v\theta)^h$$

La funzione θ è dunque un FG-omomorfismo. Inoltre se $w \in W$, allora $w^g \in W$, ovvero $(w^g)\varphi = w^g$ e dunque $w\theta = w$. Sia ora $U = Ker(\theta)$ un FG-sottomodulo di V, e sia inoltre $v \in V$. Si ha che $v\theta \in W$ e quindi $(v\theta)\theta = v\theta$ da cui segue che $(v - v\theta)\theta = 0$, ossia $(v - v\theta) \in U$. È ovvio che $W + U \subseteq V$, inoltre $v = v\theta + (v - v\theta) \in W + U$, quindi $V = W + U$. Infine, se $w \in W \cap U$ allora $w\theta = w = 0$, dunque $W \cap U = \{0\}$. Si conclude allora che $V = W \oplus U$, e dunque il teorema è dimostrato. □

Dal teorema di Maschke e dal lemma 1.10, segue immediatamente l'importante conseguenza di cui si era parlato all'inizio di questa sezione:

Corollario 1.12. *Ogni FG-modulo tale per cui $char(F) \nmid |G|$, si può esprimere come somma diretta di FG-sottomoduli irriducibili.*

Appare chiaro che per classificare tutti gli FG-moduli tali che $char(F) \nmid |G|$ basta conoscere solamente gli FG-moduli irriducibili. È evidente inoltre che il teorema di Maschke risulta valido per l'importante classe dei campi di caratteristica 0, come ad esempio $\mathbb{R}$ oppure $\mathbb{C}$.

[3] se g varia in tutto G, allora anche hg con h fissato varia in tutto G, poiché $g \mapsto hg$ è una biiezione.

Capitolo 2

Algebre e moduli

2.1 F-algebre e rappresentazioni di F-algebre

La teoria della rappresentazione dei gruppi può essere inserita in un contesto molto più ampio e generale come quello delle algebre:

Definizione. Sia A uno spazio vettoriale di dimensione finita su un campo F e si definisca inoltre un'ulteriore operazione su A:

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (x, y) &\longmapsto xy \end{aligned}$$

Se con tale operazione $(A, +, *)$ è un anello (associativo) con unità tale che:

$$(\lambda x)y = \lambda(xy) = x(\lambda y) \quad \forall \lambda \in F \text{ e } x, y \in A \tag{2.1}$$

allora si dice che A è una *F-algebra* (associativa).

Si noti che dall'equazione 2.1, insieme alla proprietà distributiva dell'anello, segue che l'operazione $*$ (vista come funzione da $A \times A$ in A) è bilineare.
Di seguito sono presentate alcune F-algebre di estrema importanza per lo studio della rappresentazione dei gruppi:

Esempio 2.1 (algebra degli endomorfismi di uno spazio vettoriale)**.** Si consideri lo spazio vettoriale $End_F(V)$ con le usuali operazioni:

$$v(f + g) = vf + vg \qquad\qquad v(\lambda f) = (\lambda v)f$$

con $f, g \in End_F(V)$, $v \in V$ e $\lambda \in F$. L'ulteriore operazione definita sullo spazio vettoriale è la composizione di funzioni

$$v(fg) = (vf)g$$

Chiaramente $End_F(V)$ è un anello con unità rispetto alla somma e alla composizione con $1 = id$, inoltre con un calcolo di routine è semplice far vedere che:

$$v\big((\lambda f)g\big) = \lambda\big(v(fg)\big) = v\big(f(\lambda g)\big)$$

Si conclude che $End_F(V)$ è una F-algebra.

Esempio 2.2 (algebra gruppale)**.** Sia G un gruppo finito ed F un campo. Si costruisca allora il seguente insieme

$$F[G] = \left\{ \sum_{g \in G} \lambda_g g \ : \ \lambda_g \in F \right\}$$

e si noti bene che gli elementi di $F[G]$ sono esclusivamente somme formali. Con le apposite operazioni di somma vettoriale e moltiplicazione per uno scalare è possibile associare a tale insieme una struttura di spazio vettoriale. Le operazioni sono definite in modo del del tutto analogo a quelle di $\mathbb{R}^n$:

$$v + u = \sum_{g \in G} \lambda_g g \sum_{g \in G} \mu_g g = \sum_{g \in G} (\lambda_g + \mu_g) g \quad \text{con } \lambda_g, \mu_g \in F$$

$$cv = c \sum_{g \in G} \lambda_g g = \sum_{g \in G} (c\lambda_g) g \quad \text{con } \lambda_g, c \in F$$

A questo punto si vuole dare ad $F[G]$ una struttura di F-algebra, dunque è necessario definire un'ulteriore operazione associativa su $F[G]$ (prodotto tra vettori) e controllare che siano verificati gli adeguati assiomi. Anche in questo caso l'operazione richiesta è definita in modo del tutto naturale, difatti si comporta proprio come la moltiplicazione fra polinomi:

$$vu = \left(\sum_{g \in G} \lambda_g g \right) \left(\sum_{h \in G} \mu_h h \right) = \sum_{g,h \in G} (\lambda_g \mu_h) gh \quad \text{con } \lambda_g, \mu_h \in F$$

In quanto spazio vettoriale, $F[G]$ è sicuramente un gruppo abeliano rispetto alla somma, inoltre indicando con e l'identità di G, mediante l'utilizzo del δ di Kronecker si ha che

$$\sum_{g \in G} \delta_{g,e} g$$

è l'elemento neutro per la nuova operazione che sarà indicato con 1 come da convenzione. Vale la proprietà distributiva:

$$(v+u)t = \left(\sum_{g \in G} \lambda_g g + \sum_{g \in G} \mu_g g \right) \left(\sum_{g \in G} \beta_g g \right) = \left(\sum_{g \in G} (\lambda_g + \mu_g) g \right) \left(\sum_{g \in G} \beta_g g \right) =$$

$$= \sum_{g,h \in G} \big((\lambda_g + \mu_g) \beta_h \big) gh = \sum_{g,h \in G} (\lambda_g \beta_h + \mu_g \beta_h) gh = vt + ut$$

Allo stesso modo si prova ch $t(v+u) = tv + tu$, e segue dunque che $F[G]$ è un anello associativo con unità. Inoltre, sia $c \in F$, allora si ha:

$$(cv)u = \left(\sum_{g \in G} (c\lambda_g) g \right) \left(\sum_{g \in G} \mu_g g \right) = \sum_{g,h \in G} (c\lambda_g \mu_h) gh = c \sum_{g,h \in G} (\lambda_g \mu_h) gh = c(vu)$$

ma vale anche

$$\sum_{g,h \in G} (c\lambda_g \mu_h) gh = \sum_{g,h \in G} (\lambda_g c \mu_h) gh = v(cu)$$

Dunque è stato dimostrato che

$$(cv)u = c(vu) = v(cu)$$

e si conclude che $F[G]$ è una F-algebra che viene detta algebra gruppale.
Si trova facilmente la seguente base per $F[G]$:

$$\mathcal{B} = \left\{ \sum_{g \in G} \delta_{h,g} g \in F[G] \ : \ h \in G \right\}$$

ed esiste inoltre un omomorfismo di gruppi iniettivo $\iota : G \to U(F[G])$ dove quest'ultimo è il gruppo delle unità di $F[G]$, tale che

$$h\iota = \sum_{g \in G} \delta_{h,g} g$$

Grazie alla suddetta immersione ι di G in $U(F[G])$, visto che $Im(\iota) = \mathcal{B}$, si conclude innanzitutto che $dim(F[G]) = |G|$, e inoltre viene identificato in modo univoco ogni elemento $g \in G$ con un elemento della base $\mathcal{B}$. Con tale identificazione, le somme formali che compongono $F[G]$ diventano vere e proprie combinazioni lineari di elementi della base. Per quanto appena detto, con un piccolo abuso di notazione e tenendo sempre in mente come è stata definita "la vera" base $\mathcal{B}$, si può dire che G è una base per lo spazio vettoriale $F[G]$.

Esempio 2.3 (somma di F-algebre)**.** Siano $A_1, A_2, \ldots, A_n$ delle F-algebre, e si costruisca nell'usuale modo lo spazio vettoriale somma

$$A = \sum_{i=1}^{k} A_i$$

Definendo inoltre un prodotto associativo su A nella seguente maniera:

$$\left(\sum_{i=1}^{k} x_i \right) \left(\sum_{i=1}^{k} y_i \right) = \sum_{i=1}^{k} (x_i y_i) \quad \forall x_i, y_i \in A_i$$

si verifica facilmente che A è una F-algebra tale che

$$1_A = \sum_{i=1}^{k} 1_{A_i}$$

ovvero l'identità di A è la somma delle identità di ogni A_i.

Esempio 2.4 (algebra quoziente)**.** Siano A una F-agebra e I un suo ideale destro o sinistro. Ovviamente I è chiuso rispetto alla somma e contiene lo 0, inoltre per ogni $y \in I$ si ha che:

$$\lambda y = \lambda(1y) = \lambda(y1) = y(\lambda 1) \in I \quad \text{con } \lambda \in F \quad \text{(caso in cui l'ideale è destro)}$$

$$\lambda y = \lambda(1y) = (\lambda 1)y \in I \quad \text{con } \lambda \in F \quad \text{(caso in cui l'ideale è sinistro)}$$

Segue dunque che I è anche un sottospazio vettoriale di A. Si badi bene che se $I \neq A$ chiaramente I non può essere un'algebra poiché non contiene l'unità. A

questo punto sotto l'ipotesi che I sia un ideale bilatero di A, l'insieme A/I ha la struttura sia di anello quoziente unitario che di spazio vettoriale quoziente in cui l'operazione di prodotto continua ad essere bilineare; perciò A/I è un'algebra detta F-algebra quoziente. Se dalla definizione di F-algebra si omettesse il fatto che A possiede l'unità rispetto al prodotto, allora I non sarebbe un sottospazio vettoriale di A e tutta la suddetta costruzione non avrebbe alcun senso.

Anche nel caso delle F-algebre si possono definire le sottostrutture e gli adeguati morfismi:

Definizione. Una *F-sottoalgebra* di una F-algebra A è un sottospazio vettoriale B di A che è anche un sottoanello unitario di A.

Esempio 2.5. Sia A una F-algebra in cui si indicherà l'unità con 1, allora $F1 = \{\lambda 1 : \lambda \in F\}$ è una sottoalgebra di A (è facile verificarlo). È possibile inoltre identificare $F1$ con F dal momento che sono isomorfi mediante la mappa $\lambda \mapsto \lambda 1$.

In modo naturale è inoltre possibile definire i morfismi per le F- algebre, che saranno chiamati *F-omomorfismi*:

Definizione. Sia φ una funzione (non "zero") tra due F-algebre A e B. Se φ è lineare e inoltre è un omomorfismo di anelli, allora si dice che φ è un F-omomorfismo.

Si dimostra facilmente che l'immagine di un F-omomorfismo tra A e B è una F-sottoalgebra di B, mentre ciò non vale per il nucleo poiché esso è un ideale bilatero di A (diverso da A stesso) e dunque non contiene l'unità moltiplicativa. Vale comunque il primo teorema di isomorfismo per F-algebre.
A questo punto, in modo analogo a come è stato fatto per i gruppi, è possibile avere una "visualizzazione geometrica" anche per le F-algebre:

Definizione. Sia A una F-algebra e V uno spazio vettoriale di dimensione finita su F. Una rappresentazione di A su V è allora un F-omomorfismo:

$$\bar{\rho} : A \longrightarrow End_F(V)$$

La funzione $\bar{\rho}$ risulta essere ben definita come F-omomorfismo, poiché nell'esempio 2.1 si è visto che $End_F(V)$ è una F-algebra.

2.2 A-moduli

In modo analogo a quanto detto nel primo capitolo, è possibile far agire una F-algebra su uno spazio vettoriale, ma chiaramente essendoci due operazioni gli assiomi da rispettare saranno di più rispetto a quelli che caratterizzavano le azioni di gruppi su spazi vettoriali:

Definizione. Sia A una F-algebra e V uno spazio vettoriale di dimensione finita su F. Allora V si dice un *A-modulo* se A agisce mediante:

$$\begin{aligned} \bar{\mu} : V \times A &\longrightarrow V \\ (v, x) &\longmapsto v^x \end{aligned}$$

tale che:

i) $(v^x)^y = v^{xy} \quad \forall x, y \in A$ e $\forall v \in V$

ii) $v^1 = v \quad \forall v \in V$

iii) $(\lambda v)^x = \lambda v^x = v^{\lambda x} \quad \forall x \in A$, $\forall v \in V$ e $\forall \lambda \in F$

iv) $(v+u)^x = v^x + u^x \quad \forall x \in A$ e $\forall v, u \in V$

v) $v^{x+y} = v^x + v^y \quad \forall x, y \in A$ e $\forall v \in V$

Si noti che in questo caso le ultime tre proprietà rendono l'azione *bilineare*.
Esiste anche in questo caso una corrispondenza fra rappresentazioni di F-algebre e A-moduli:
Sia V un A-modulo (su un campo F) e si definisca:

$$\begin{array}{rcl} M_x : V & \longrightarrow & V \\ v & \longmapsto & v^x \end{array}$$

È ovvio che M_x è un endomorfismo di V, inoltre la funzione:

$$\begin{array}{rcl} \bar{\rho} : A & \longrightarrow & End_F(V) \\ x & \longmapsto & M_x \end{array}$$

è un F-omomorfismo, infatti siano $v \in V$, $x, y \in A$ e $\lambda \in F$ si ha che $\bar{\rho}$ è lineare:

$$v\big((x+y)\bar{\rho}\big) = vM_{x+y} = v^{x+y} = v^x + v^y = vM_x + vM_y = v(x\bar{\rho}) + v(y\bar{\rho})$$

$$v\big((\lambda x)\bar{\rho}\big) = vM_{\lambda x} = v^{\lambda x} = \lambda v^x = \lambda(vM_x) = v\big(\lambda(x\bar{\rho})\big)$$

e $\bar{\rho}$ è omomorfismo di anelli:

$$v\big((xy)\bar{\rho}\big) = vM_{xy} = v^{xy} = (v^x)^y = vM_xM_y = v(x\bar{\rho})(y\bar{\rho})$$

Ovvero $\bar{\rho}$ è una rappresentazione di una F-algebra su V. In sostanza da un A-modulo è stata determinata in modo unico una rappresentaione.
Viceversa, sia $\bar{\rho}$ una rappresentazione di una F-algebra A su V, allora si pone $v^x = v(x\bar{\rho})$ $\forall v \in V$ e $\forall x \in A$ e si dimostra che è un'azione di A su V. Siano infatti $v, u \in V$, $\lambda \in F$ e $x, y \in A$, allora:

i) $(v^x)^y = v\big((x\bar{\rho})(y\bar{\rho})\big) = v\big((xy)\bar{\rho}\big) = v^{xy}$

ii) $v^1 = v(1\bar{\rho}) = v(id) = v$

iii) $(\lambda v)^x = (\lambda v)(x\bar{\rho}) = \lambda\big(v(x\bar{\rho})\big) = \lambda v^x$
e
$(\lambda v)^x = (\lambda v)(x\bar{\rho}) = v\big(\lambda(x\bar{\rho})\big) = v\big((\lambda x)\bar{\rho}\big) = v^{(\lambda x)}$

iv) $(v+u)^x = (v+u)(x\bar{\rho}) = v(x\bar{\rho}) + u(x\bar{\rho}) = v^x + u^y$

v) $v^{x+y} = v\big((x+y)\bar{\rho}\big) = v(x\bar{\rho} + y\bar{\rho}) = v(x\bar{\rho}) + v(y\bar{\rho}) = v^x + v^y$

Quindi V è un A-modulo che è stato costruito in modo unico da una rappresentazione di una F-algebra.
Come fatto in precedenza si può mostrare che tale corrispondenza è biunivoca, dunque parlare di rappresentazioni di F-algebre oppure di A-moduli è dunque indifferente, e anche in tale contesto, con abuso di notazione, si indicherà spesso un A-modulo con la coppia $(V, \bar{\rho})$.

Esempio 2.6. Si faccia agire una F-algebra A su se stessa mediante $v^x = vx$, ovvero l'usuale moltiplicazione a destra. È facile vedere come le cinque proprietà sopra descritte sono rispettate e dunque con tale azione A è detto *A-modulo regolare* ed è indicato con A^o.

In modo del tutto naturale si definiscono le sottostrutture (come sottospazi invarianti):

Definizione. Sia U un sottospazio vettoriale di un A-modulo V, allora U è un *A-sottomodulo* di V se e solo se $u^x \in U$ $\forall u \in U$ e $\forall x \in A$.

Esempio 2.7. Sia V un A-modulo e $v \in V$, allora si definisce l'insieme

$$v^A = \{v^x \ : \ x \in A\}$$

che è un sottospazio vettoriale di V:

$$v^x + v^y = v^{x+y} \in v^A \quad \forall x, y \in A$$

$$\lambda v^x = v^{\lambda x} \in v^A \quad \forall \lambda \in F \text{ e } \forall x \in A$$

ed è invariante sotto l'azione di A:

$$(v^x)^y = v^{xy} \in v^A \quad \forall x, y \in A$$

Si conclude che v^A è un A-sottomodulo di V, ed è il più piccolo A-modulo contenente v. Se esiste un certo $v \in V$ tale per cui $V = v^A$, allora V è un *A-modulo ciclico*. Mediante calcoli di routine, si dimostra inoltre, che la relazione in V data da:

$$v \sim u \text{ se e solo se } u = v^x \text{ per qualche } x \in A$$

è una relazione di equivalenza, e u^A è la classe di equivalenza che contiene il vettore u. Segue dunque che un qualsiasi A-modulo è partizionato nell'unione disgiunta dei suoi sottomoduli ciclici.

Le definizioni di A-modulo *irriducibile* e *completamente riducibile* sono identiche a quelle date per gli FG-moduli. Vale l'analogo del lemma 1.10 la cui dimostrazione è uguale a quella data in precedenza.

Lemma 2.8. *Un A-modulo V è completamente riducibile se e solo se V è somma diretta di suoi A-sottomoduli irriducibili.*

Anche per quanto riguarda i morfismi, si ha una definizione molto naturale e coerente con quanto detto fin'ora:

Definizione. Sia θ una funzione tra due A-moduli V e W, allora θ è un *A-omomorfismo* se e solo se θ è lineare e vale che $(v^x)\theta = (v\theta)^x$ $\forall v \in V$ e $\forall x \in A$. Se θ è inoltre biunivoca, allora è un *A-isomorfismo*.

Gli *A-moduli quozienti* V/U vengono definiti in modo usuale e vale il primo teorema di isomorfismo. In tale contesto, il modulo regolare destro A^o risulta essere molto importante poiché contiene una copia di tutti gli A-moduli ciclici:

Lemma 2.9. *Sia v^A (su un campo F) un A-modulo ciclico, allora v^A è isomorfo ad un A-modulo quoziente del modulo regolare destro A^o*

Dimostrazione. Si definisca la funzione

$$\begin{array}{rcl} f : A^o & \longrightarrow & v^A \\ x & \longmapsto & v^x \end{array}$$

che è lineare:

$$(x+y)f = v^{x+y} = v^x + v^y = xf + yf \quad \forall x, y \in A^o$$

$$x(cf) = (cx)f = v^{cx} = cv^x = c(xf) \quad \forall x \in A^o \text{ e } \forall c \in F$$

e rispetta le azioni:

$$(xa)f = v^{xa} = (v^x)^a = (xf)^a \quad \forall x, a \in A^o$$

Segue dunque che f è un A-omomorfismo con

$$Ker(f) = Ann_{A^o}(v) = \{x \in A^o \ : \ v^x = 0\}$$

A questo punto per il primo teorema di isomorfismo tra A-moduli si conclude che $A^o/Ann_{A^o}(v) \cong v^A$. □

Corollario 2.10. *Sia V (su un campo F) un A-modulo irriducibile, allora V è isomorfo ad un A-modulo quoziente del modulo regolare destro A^o*

Dimostrazione. La tesi segue immediatamente osservando che un A-modulo irriducibile è anche ciclico, dal momento che se $v^A \subseteq V$ e $v \neq 0$, allora $v^A = V$. □

Esempio 2.11. Sia V un A-modulo su un campo F e si consideri l'insieme

$$End_A(V) = \{\varphi : V \to V \ \text{ t.c. } \ \varphi \text{ è un } A\text{-omomorfismo}\}$$

Chiaramente $End_A(V) \subseteq End_F(V)$, inoltre siano $\varphi, \psi \in End_A(V)$, $c \in F$, $v \in V$ e $x \in A$, allora:

$End_A(V)$ è sottospazio vettoriale di $End_F(V)$

$$(v^x)0 = (v0)^x = 0$$

$$v^x(\varphi + \psi) = v^x\varphi + v^x\psi = (v\varphi)^x + (v\psi)^x = \big(v(\varphi+\psi)\big)^x$$

$$v^x(c\varphi) = (cv^x)\varphi = c(v^x\varphi) = c(v\varphi)^x = \big(v(c\varphi)\big)^x$$

$End_A(V)$ è sottoanello unitario di $End_F(V)$

$$v^x(\varphi\psi) = (v^x\varphi)\psi = \big((v\varphi)^x\big)\psi = \big((v\varphi)\psi\big)^x = \big(v(\varphi\psi)\big)^x$$

$$v^x(id) = v^x = \big(v(id)\big)^x$$

Dunque $End_A(V)$ è una F-sottoalgebra di $End_F(V)$. Sia inoltre $\bar{\rho}$ la rappresentazione associata a V (come A-modulo) tale che $v^a = v(a\bar{\rho})$ $\forall a \in A$ e $\forall v \in V$, allora considerando $\varphi \in End_A(V)$ si ha che:

$$(v^a)\varphi = v(a\bar{\rho})\varphi \quad \text{e} \quad (v\varphi)^a = v\varphi(a\bar{\rho})$$

E siccome $(v^a)\varphi = (v\varphi)^a$, allora $v(a\bar{\rho})\varphi = v\varphi(a\bar{\rho})$ da cui segue che $End_A(V)$ è il centralizzante di $A\bar{\rho}$ in $End_F(V)$, ovvero in simboli:

$$End_A(V) = C_{End_F(V)}(A\bar{\rho})$$

In generale, dati due A-moduli V e W, nello stesso modo appena visto si prova che l'insieme

$$Hom_A(V,W) = \{\varphi : V \to W \text{ t.c. } \varphi \text{ è un } A\text{-omomorfismo}\}$$

è un'algebra.

Si torni ora all'algebra gruppale $F[G]$ definita nell'esempio 2.2, è importante vedere come è indifferente parlare di $F[G]$-moduli, oppure di FG-moduli, e dunque tutta la teoria riguardante la rappresentazione di gruppi può essere estesa alla teoria della rappresentazione di algebre: Una rappresentazione dell'algebra gruppale è un F-omomorfismo:

$$\bar{\rho} : F[G] \quad \longrightarrow \quad End_F(V)$$

Si restringa $\bar{\rho}$ alla base di $F[G]$ che è G, allora è ovvio che

$$(gh)\bar{\rho} = (g\bar{\rho})(h\bar{\rho}) \quad \forall g, h \in G$$

e inoltre siccome $(g\bar{\rho})(g^{-1}\bar{\rho}) = (g^{-1}\bar{\rho})(g\bar{\rho}) = e\bar{\rho} = id$, ovvero ogni elemento dell'immagine è invertibile, segue che $Im(\bar{\rho}_{|_G}) \subseteq GL(V)$. Si conclude perciò che $\bar{\rho}_{|_G}$ è una rappresentazione di G su V.
Al contrario si consideri una rappresentazione di un gruppo G su uno spazio vettoriale V:

$$\rho : G \quad \longrightarrow \quad GL(V)$$

Ricordando che $GL(V) \subseteq End_F(V)$ definisca quindi ora la funzione:

$$\begin{array}{ccc} \bar{\rho} : F[G] & \longrightarrow & End_F(V) \\ \sum_{g\in G} \lambda_g g & \longmapsto & \sum_{g\in G} \lambda_g (g\rho) \end{array}$$

che risulta essere un F-omomorfismo, infatti $\forall x, y \in F[G]$ e $\forall c \in F$ si ha:

$$(x+y)\bar{\rho} = \sum_{g\in G} (\lambda_g + \mu_g)(g\rho) = \sum_{g\in G} \lambda_g(g\rho) + \sum_{g\in G} \mu_g(g\rho) = x\bar{\rho} + y\bar{\rho}$$

$$(cx)\bar{\rho} = \sum_{g\in G} (c\lambda_g)(g\rho) = c\sum_{g\in G} \lambda_g(g\rho) = c(x\bar{\rho})$$

$$(xy)\bar{\rho} = \sum_{g,h\in G} (\lambda_g\lambda_h)\big((gh)\rho\big) = \sum_{g,h\in G} (\lambda_g\lambda_h)\big((g\rho)(h\rho)\big) = (x\bar{\rho})(y\bar{\rho})$$

Si conclude dunque che $\bar{\rho}$ è una rappresentazione di $F[G]$ su V. Un'importante conseguenza di quanto appena detto è che vale l'equivalente del teorema di Maschke anche per gli $F[G]$-moduli:

Teorema 2.12. *Siano G un gruppo finito e V un $F[G]$-modulo. Se $char(F) \nmid |G|$ allora V è completamente riducibile.*

Dimostrazione. Sia $\bar{\rho}$ la rappresentazione di $F[G]$ su V, allora all'$F[G]$-modulo $(V, \bar{\rho})$ corrisponde in modo unico un FG-modulo (V, ρ) come spiegato sopra. Per il teorema di Maschke (V, ρ) si esprime come somma diretta di FG-sottomoduli irriducibili, dunque ancora una volta per la suddetta corrispondenza, anche $(V, \bar{\rho})$ si esprime come somma diretta di $F[G]$-sottomoduli irriducibili e dunque è completamente riducibile. □

Due rappresentazioni $\bar{\rho}$ e $\bar{\mu}$ di una F-algebra A, rispettivamente su due spazi vettoriali V e W si dicono equivalenti se esiste una trasformazione lineare invertibile $\theta : V \to W$ tale per cui $x\bar{\mu} = \theta^{-1}(x\bar{\rho})\theta$. Inoltre in modo del tutto analogo a quanto fatto nel capitolo precedente, si dimostra $\bar{\mu}$ e $\bar{\rho}$ sono equivalenti se e solo se i rispettivi A-moduli associati sono isomorfi.

2.3 Classificazione di F-algebre semisemplici

In questa sezione si focalizzerà l'attenzione su una particolare classe di algebre, ovvero le algebre semisemplici. Si dimostrerà che esse hanno la caratteristica di poter essere sempre decomposte in una forma molto comoda, ovvero come somma diretta di algebre di endomorfismi, e per tale motivo la classificazione di tali algebre è completa e immediata.

Definizione. Una F-algebra A si dice *semisemplice* se il modulo regolare destro A^o è completamente riducibile.

Esempio 2.13. Si consideri l'agebra gruppale $F[G]$, se $char(F) \nmid |G|$ allora per il teorema di Maschke si ha che $F[G]$ è semisemplice.

Definizione. Sia V un A-modulo completamente riducibile, e sia M un A-modulo irriducibile. La *componente omogenea* di M in V denotata con $M(V)$ è la somma di tutti gli A-sottomoduli di V che sono isomorfi a M. Il numero di tali sottomoduli che compongono $M(V)$ si indica con $n_M(V)$.

Spesso, quando è sottinteso il riferimento al modulo V invece che $n_M(V)$, si scriverà, per alleggerire la notazione, semplicemente n_M. Inoltre dal momento che A-moduli irriducibili diversi hanno sempre intersezione banale, allora si ha che $M(V)$ è in realtà somma diretta di A-moduli irriducibili.
Siccome l'isomorfismo fra A-moduli è una relazione di equivalenza, segue che se $M \cong N$ allora vale evidentemente che $M(V) = N(V)$. Nel lemma 2.8 si è visto che per un A-modulo, essere completamente riducibile è equivalente al fatto di essere somma diretta di sottomoduli irrudicibili, dunque nel proseguio si farà indistintamente riferimento ad una delle due caratteristiche senza ricordare ogni volta l'equivalenza con l'altra non menzionata.

Lemma 2.14. *Sia V un A-modulo tale che $V = W_1 \oplus W_2 \oplus \ldots \oplus W_n$, con W_i A-sottomodulo irriducibile di V $\forall i \in \{1, \ldots, n\}$. Sia inoltre M un A-modulo irriducibile, allora:*

i) $M(V)$ *è un* $End_A(V)$*-sottomodulo*[1] *di* V*.*

ii) $M(V) = \bigoplus_{W_i \cong M} W_i$

[1]Si intende che $End_A(V)$ agisce in modo naturale su V, overo $v^\theta = v\theta$ $\forall v \in V$ e $\forall \theta \in End_A(V)$. Chiaramente con tale azione V è un $End_A(V)$-modulo.

iii) *Il numero $n_M(V)$ di sottomoduli W_i isomorfi a M è un invariante di V, ovvero è indipendente dalla decomposizione di V come somma diretta di A-sottomoduli irriducibili.*

Dimostrazione. Sia $M(V) = U_1 \oplus U_2 \oplus \ldots \oplus U_t$, con $U_i \cong M \ \forall i \in \{1, \ldots, t\}$:
i) Ovviamente $M(V)$ è sottospazio vettoriale di V e bisogna provare dunque che $M(V)$ è invariante sotto l'azione di $End_A(V)$. Sia $\theta \in End_A(V)$, allora $\theta|_{U_j}$ è un A-omomorfismo da U_j in V per un certo $j \in \{1, \ldots, t\}$, ma U_j è un A-modulo irriducibile dunque $Ker(\theta|_{U_j}) = \{0\}$. Segue che $M \cong U_j \cong U_j\theta$, ovvero $U_j\theta \subseteq M(V)$, perciò data l'arbitrarietà di j si ha che $\forall x \in M(V)$

$$x\theta = (u_1 + u_2 + \ldots + u_t)\theta = u_1\theta + u_2\theta + \ldots + u_t\theta \in M(V)$$

ii) È chiaro che $\bigoplus_{W_i \cong M} W_i \subseteq M(V)$. Si consieri ora un generico U_ℓ con $\ell \in \{1, \ldots, t\}$ e inoltre la proiezione π_j da V su W_j. In questo caso, dal momento che tutti i W_i sotto A-sottomoduli, segue che la proiezione è un A-omomorfismo, infatti nella dimostrazione del teorema di Maschke si era visto che è una funzione lineare e inoltre:

$$(w_1 + \ldots w_j \ldots + w_n)^x \pi_j = ({w_1}^x + \ldots {w_j}^x \ldots + {w_n}^x)\pi_j =$$

$$= {w_j}^x = \big((w_1 + \ldots w_j \ldots + w_n)\pi_j\big)^x$$

In particolare π_j ristretta a U_ℓ è ancora un A-omomorfismo tra U_ℓ e W_j e si noti che se $\pi_j \neq 0$, allora $U_\ell \cong W_j$ poiché U_ℓ e W_j sono A moduli irriducibili (W_j lo è per definizione, mentre $U_\ell \cong M$ che è irriducibile). Segue che $U_\ell\pi_j \subseteq \bigoplus_{W_i \cong M} W_i$ e questo vale $\forall j \in \{1, \ldots, n\}$, ma $U_\ell \subseteq \bigoplus_{j=1}^{n} U_\ell\pi_j$, quindi siccome $\bigoplus_{W_i \cong M} W_i$ è uno spazio vettoriale (dunque chiuso rispetto alla somma), si conclude che $U_\ell \subseteq \bigoplus_{W_i \cong M} W_i$.
iii) Dal punto *ii*), utilizzando la formula di Grassman, segue che:

$$dim(M(V)) = dim\left(\bigoplus_{W_i \cong M} W_i\right) = \bigoplus_{W_i \cong M} dim(W_i) = n_M(V) \cdot dim(M)$$

quindi

$$n_M(V) = \frac{dim(M(V))}{dim(M)}$$

Ed è chiaro che tale quantità non dipende dalla decomposizione di V. □

Il punto *ii*) del lemma precedente dice che un A-modulo completamente riducibile è somma diretta di *tutti* i suoi sottomoduli irriducibili. Inoltre tale A-modulo può essere espresso come somma diretta di componenti omogenee distinte:

$$V = M_1(V) \oplus M_2(V) \oplus \ldots \oplus M_k(V) \quad \text{con} \quad M_i(V) \neq M_j(V) \ \ \forall i, j \in \{1, \ldots, k\} \tag{2.2}$$

Segue che i moduli irriducibili M_i non possono essere isomorfi tra loro, ovvero non appartengono alla stessa classe di isomorfismo. Si costruisce quindi un insieme di rappresentati delle classi di isomorfismo denotato con $\mathcal{R}(A)$ e gli M_i verranno selezionati in tale insieme. Quindi se V è un A-modulo completamente riducibile dall'equazione 3.12, in notazione compatta si può scrivere:

$$V = \bigoplus_{M_i \in \mathcal{R}(A)} M_i(V) \tag{2.3}$$

Dove è chiaro che se in V non vi è alcun sottomodulo isomorfo a M_i, allora $M_i(V) = \emptyset$. Ogni addendo $M_i(V)$ della 2.3 è a sua volta somma diretta di copie isomorfe di uno stesso sottomodulo irriducibile W_i di V, dunque con un abuso di notazione si scriverà $M_i(V) = n_{M_i} W_i$ e ancora una volta dall'equazione 3.12 si ha un'ulteriore (ed equivalente) scrittura della decomposizione di V:

$$V = n_{M_1} W_1 \oplus n_{M_2} W_2 \oplus \ldots \oplus n_{M_k} W_k \tag{2.4}$$

Il lemma che segue fornisce un risultato importantissimo in quanto afferma che in realtà tutti gli A-moduli irriducibili sono contenuti nel modulo regolare destro A^o. Dunque tramite lo studio della struttura di A^o è possibile classificare qualunque A-modulo completamente riducibile:

Lemma 2.15. *Sia A una F-algebra semisemplice, allora ogni A-modulo irriducibile è isomorfo ad un A-sottomodulo di A^o.*

Dimostrazione. Sia V un A-modulo irriducibile, allora per il lemma 2.9 (e per il suo corollario), si ha che $A^o / Ann_{A^o}(v) \cong V$. Per ipotesi A^o è completamente riducibile, dunque esiste un A-sottomodulo di A^o denotato con U tale che $A^o = Ann_{A^o}(v) \oplus U$, si consideri quindi la proiezione π di A^o su U che è ancora una volta un A-omomorfismo surgettivo. Chiaramente $Ker(\pi) = Ann_{A^o}(v)$, perciò per il primo teorema di isomorfismo $A^o / Ann_{A^o}(v) \cong U$ da cui segue che $U \cong V$, ovvero la tesi. □

Richiedere che un sottospazio vettoriale S di A^o sia un sottomodulo significa che esso deve essere invariante rispetto all'azione di moltiplicazione a destra, ma ciò equivale a dire che S "assorbe" la moltiplicazione a destra, dunque si conclude che gli ideali destri di A sono tutti e soli gli A-sottomoduli di A^o. Quindi se A è un'algebra semisemplice, tutti gli A-moduli completamente riducibili si posso esprimere come somma diretta di sottomoduli isomorfi (come A-moduli) a ideali destri di A^o.
Si consideri sempre una F-algebra semisemplice A, e si restringa l'attenzione esclusivamente allo studio di A^o che è un A-modulo completamente riducibile, allora per quanto detto in precedenza si ha che:

$$A^o = \bigoplus_{M_i \in \mathcal{R}(A)} M_i(A^o) \tag{2.5}$$

dove ogni componente omogenea $M_i(A^o)$ è somma di ideali destri di A che sono inoltre minimali poiché per ipotesi si prende M_i irriducibile e dunque tutti gli ideali di A isomorfi a M_i sono A-moduli irriducibili, ovvero non possono contenere altri ideali diversi da $\{0\}$. Si noti inoltre che per via del lemma 2.15, nell'equazione 2.5 si ha che $M_i(A^o) \neq \emptyset$ forall $M_i \in \mathcal{R}(A)$.
L'obiettivo è ora quello di arrivare attraverso alcuni lemmi preliminari, alla dimostrazione del teorema di Wedderburn-Artin.

Lemma 2.16 (di Wedderburn)**.** *Sia A un'algebra semisemplice e M un A-modulo irriducibile, allora:*

i) $M(A^o)$ *è un ideale bilatero di* A*.*

ii) Se W *è un* A*-modulo irriducibile, allora* $W \cong M$ *oppure* $M(A^o) \subseteq Ann_A(W)$*.*

iii) Sia $\bar{\rho}$ *la rappresentazione di* A *su* M*, allora* $M(A^o)$ *è una* F*-algebra e inoltre* $M(A^o) \cong A\bar{\rho}$*.*

iv) $M(A^o)$ *è un ideale bilatero minimale di* A*.*

v) l'insieme di rappresentanti $\mathcal{R}(A)$ *ha cardinalità finita.*

Dimostrazione. i) $M(A^o)$ per definizione è somma di ideali destri di A, quindi è un ideale destro di A. Sia $\theta_a : A^o \to A^o$ tale che $x\theta_a = ax \ \ \forall x, a \in A$, ovviamente θ è lineare e inoltre $(xy)\theta_a = (x\theta_a)y$ con $y \in A$, da cui segue che $\theta \in End_A(A^o)$. Per lemma 2.14(i) si ha che $M(A^o)$ è invariante sotto l'azione naturale di $End_A(A^o)$ e quindi $aM(A^o) = M(A^o)\theta_a \subseteq M(A^o)\ \forall a \in A$, ovvero la componente omogenea di M in A^o è anche un ideale sinistro di A.
ii) Si supponga che $W \ncong M$, allora $W(A^o) \cap M(A^o) = \{0\}$ con $W(A^o) \neq \emptyset$ e $M(A^o) \neq \emptyset$ per il lemma 2.15. Dal punto precedente si sa che entrambe le componenti omogenee sono ideali bilateri, dunque il loro prodotto è contenuto nell'intersezione, da cui segue che $W(A^o)M(A^o) = \{0\}$. Esiste dunque un sottomodulo U di A^o isomorfo a W tale per cui $M(A^o) \subseteq Ann_A(U)$. Resta da provare che l'annullatore di W è uguale all'annullatore di U: sia φ l'isomorfismo da W in U e sia $x \in Ann_A(W)$, allora

$$x \in Ann_A(W) \Leftrightarrow 0 = W^x \Leftrightarrow 0 = (W^x)\varphi = (W\varphi)^x = Ux \Leftrightarrow x \in Ann_{A^o}(U)$$

da cui segue la tesi.
iii) Siccome è stato dimostrato che $M(A^o)$ è un ideale bilatero di A, basta provare che $M(A^o)$ possiede un'identità moltiplicativa. Si consideri la decomposizione dell'identità di A come somma di elementi delle componenti omogenee

$$1 = \sum_{e_i \in M_i(A^o)} e_i$$

Chiaramente sarà $M = M_j$ per qualche $M_j \in \mathcal{R}(A)$ allora preso un generico $m \in M_j(A^o)$, per il lemma 2.16(ii) si ha

$$m = m1 = \sum_{e_i \in M_i(A^o)} me_i = me_j$$

e allo stesso modo si prova che $e_j m = m$, dunque e_j è l'identità moltiplicativa che si cercava. La funzione candidata ad essere l'isomorfismo richiesto è $\bar{\rho}\big|_{M(A^o)}$, ovvero la restrizione di $\bar{\rho}$ a $M(A^o)$. Innanzitutto si ricordi che dato il modulo M è possibile costruire la relativa rappresentazione $x\bar{\rho} = L_x$, [2]dove $L_x \in End_F(M)$ tale che $mL_x = m^x \ \forall m \in M$. La funzione $\bar{\rho}\big|_{M(A^o)}$ è sicuramente un F-omomorfismo, si veda ora che è suriettiva: sia $L_x \in A\bar{\rho}$ con $x = \sum_{y_i \in M_i(A^o)} y_i$, ponendo

[2]In precedenza tale funzione era stata indicata con M_x, ma in questo caso è stata cambiata la notazione per evitare confusioni.

sempre $M = M_j$ per un certo $M_j \in \mathcal{R}(A)$. Siccome $M_\ell \ncong M \ \forall \ell \neq j$, per il punto *ii*) si ha che $M_\ell(A^o)$ annulla M e perciò

$$mL_x = m^x = m^{\sum y_i} = m^{y_j} = mLy_j$$

Data l'arbitrarietà di m, si ha che $L_x = L_{y_j}$ è un elemento dell'immagine di $\bar{\rho}\big|_{M(A^o)}$ che perciò è suriettiva. Per verificare che tale funzione è inoltre iniettiva, si consideri $y \in Ker\big(\bar{\rho}\big|_{M(A^o)}\big)$, quindi y è tale che $m^y = 0 \ \forall m \in M$, ovvero y annulla tutto M. Siccome $y \in M(A^o)$, ancora una volta per il punto *ii*), si deduce che allora y annulla anche tutti gli A-moduli irriducibli non isomorfi ad M. Di conseguenza y annulla tutti gli A-moduli completamente riducibili. Prendendo in particolare A^o si ha $y = 1y \in A^o y = 0$ e si conclude che $\bar{\rho}\big|_{M(A^o)}$ è anche iniettiva.
iv) Sia I un ideale di A tale che $I \subset M(A^o)$, allora deve esistere un certo sottomodulo di A^o $W \in M(A^o)$ per cui vale che $I \nsubseteq W$. Siccome W è irriducibile $I \cap W = \{0\}$ e quindi $WI \subseteq I \cap W = \{0\}$ (si ricordi che I è ideale bilatero, mentre W è ideale destro), ovvero come si è visto in *ii*), I annulla $M \cong W$. Sia ora $z \in I$, si vede subito che L_z è la funzione "zero" su $M(A^o)$ e vale quindi che $z\bar{\rho}\big|_{M(A^o)} = 0$, ovvero $I \subseteq Ker\big(\bar{\rho}\big|_{M(A^o)}\big) = \{0\}$ per il punto precedente.
v) Si guardi l'equazione 2.5: per ipotesi $dim(A) < \infty$ e inoltre $M_i(A) \neq \emptyset$ $\forall M_i \in \mathcal{R}(A)$. Segue che la somma diretta in questione è finita e perciò la cardinalità di $\mathcal{R}(A)$ è finita. □

Si evince che l'algebra A si esprime come somma diretta di sue sottoalgebre (che sono anche ideali minimali di A) non isomorfe tra loro, ovvero riscrivendo l'equazione 2.5 e intendendola come uguaglianza tra algebre si ha:

$$A = \bigoplus_{M_i \in \mathcal{R}(A)} M_i(A^o) \tag{2.6}$$

Le sottoalgebre $M_i(A^o)$, per il lemma 2.16(*iii*) sono inoltre isomorfe a sottoalgebre di algebre di endomorfismi di $M_i \ \forall M_i \in \mathcal{R}(A)$.

Lemma 2.17 (di Schur)**.** *Se V e W sono due A-moduli irriducibili, allora $Hom_A(V, W)$ è un corpo.*

Dimostrazione. Bisogna provare che ogni elemento di $Hom_A(V, W)$ diverso dallo 0 ammette un inverso. Sia $\varphi \in Hom_A(V, W)$ tale che $\varphi \neq 0$, allora $Ker(\varphi)$ è un sottomodulo di V e $Im(\varphi)$ è un sottomodulo di W. Siccome V e W sono irriducibili, segue che $Ker(\varphi) = \{0\}$ e $Im(\varphi) = W$, ovvero φ è un A-isomorfismo e dunque è invertibile. □

In particolare se $V = W$, allora $End_A(V)$ è un corpo.

Corollario 2.18. *Sia A una F-algebra con F algebricamente chiuso e sia inoltre V un A-modulo irriducibile. Allora posto*

$$\Lambda = \{f_\lambda : V \to V \ \ t.c. \ \ vf_\lambda = \lambda v \ \ con \ \lambda \in F\}$$

si ha che $End_A(V) = \Lambda \cong F$.

Dimostrazione. Chiaramente $\Lambda \subseteq End_A(V)$. Viceversa sia $\varphi \in End_A(V)$, allora siccome il campo F è algebricamente chiuso, il polinomio caratteristico $det(\varphi - \lambda I)$ ha almeno una radice su F e quindi φ ammette almeno un autovalore $\bar{\lambda}$. Segue che $Ker(\varphi - \bar{\lambda} I) \neq \{0\}$, ovvero $\varphi - \bar{\lambda} I \in End_A(F)$ non è invertibile. Per il lemma di Schur $\varphi - \bar{\lambda} I = 0$, quindi $\varphi = \bar{\lambda} I \in \Lambda$. Il corpo Λ è in realtà un campo e si ha che $\Lambda \cong F$ mediante l'isomorfismo di campi tale che $f_\lambda \mapsto \lambda$ $\forall \lambda \in F$. □

L'insieme Λ contiene tutte le moltiplicazioni per scalari, e molto spesso viene identificato con F stesso.

Teorema 2.19 (del doppio centralizzante)**.** *Siano A una F-algebra semisemplice e $\bar{\rho}$ una sua rappresentazione su un A-modulo irriducibile M. Si ponga inoltre $D = End_A(M)$, allora $End_D(M) = A\bar{\rho}$.*

Dimostrazione. È possibile sostituire M con un A-modulo ad esso isomorfo, dunque per il lemma 2.15 si può considerare M come sottomodulo di A^o. Nell'usuale modo, la rappresentazione di A induce l'azione su M tale che $m^x = m(x\bar{\rho})$, dunque fissato $x \in A$, per ogni $\varphi \in D$ si ha che:

$$\big(m(x\bar{\rho})\big)\varphi = (m\varphi)(x\bar{\rho}) \quad \forall m \in M$$

In pratica $x\bar{\rho}$ oltre a essere un'applicazione lineare da M in sè, commuta con φ, ovvero "rispetta" l'azione naturale di D; segue che $x\bar{\rho} \in End_D(M)$ e dunque $A\bar{\rho} \subseteq End_D(M)$. Per comodità si ponga $M(A^o) = I$ e si ricordi che per il lemma 2.16(ii) I è un ideale bilatero di A, mentre M (che è contenuto in I) è un ideale destro di A. Si consideri ora la funzione lineare:

$$\begin{array}{rccl} \beta_m : M & \longrightarrow & M & \\ x & \longmapsto & mx & \text{con } m \in M \end{array}$$

quindi $\forall a \in A$ e $\forall x, m \in M$ si ha che:

$$(xa)\beta_m = m(xa) = (mx)a = (x\beta_m)a$$

ovvero $\beta_m \in D$. Per tal motivo, preso $\theta \in End_D(M)$, allora per due generici $m, n \in M$ vale che:

$$(mn)\theta = (n\beta_m)\theta = (n\theta)\beta_m = m(n\theta) \tag{2.7}$$

ciò perché θ deve rispettare l'azione naturale di D. Si fissi ora $n \in M$ tale che $n \neq 0$ e si ricordi che si è visto che I possiede un'identità e. Dal momento che $n \in I$, allora $AnA = \Big\{\sum_i a_i n b_i \ : \ a_i, b_i \in A \quad \forall i \in \mathbb{N}\Big\} \subseteq I$, ma per il lemma 2.16$(iv)$ I è ideale minimale, quindi $AnA = I$ e di conseguenza $e \in AnA$. Se $m \in M$ si può scrivere dunque:

$$m = me = m\sum_i a_i n b_i = \sum_i (ma_i)(nb_i) \quad \text{per certi } a_i, b_i \in A$$

Siccome (ma_i) e (nb_i) appartengono ad M, dall'equazione 2.7 segue che:

$$m\theta = \sum_i \big((ma_i)(nb_i)\big)\theta = \sum_i (ma_i)\big((nb_i)\theta\big) = m\sum_i a_i\big((nb_i)\theta\big)$$

Ponendo $\sum_i a_i\big((nb_i)\theta\big) = u$, si ha dunque che $m\theta = mu$ ovvero $\theta = T_u$ che è l'immagine di u mediante la rappresentazione $\bar{\rho}$. Si conclude quindi che $End_D(M) \subseteq A\bar{\rho}$. □

Nell'esempio 2.11 si era visto che $End_A(M) = C_{End_F(M)}(A\bar{\rho})$, e inoltre nello stesso modo si vede subito che $End_D(V) = C_{End_F(M)}\big(End_A(M)\big)$. È quindi spiegato il nome "teorema del doppio centralizzante", dal momento che, sotto opportune ipotesi, tale teorema afferma che

$$C\big(C(A\bar{\rho})\big) = A\bar{\rho}$$

dove è sottinteso che si sta parlando di centralizzanti in $End_F(M)$.
Con tutto il background sviluppato fino ad ora, è possibile dimostrare finalmente il teorema di Wedderburn-Artin:

Teorema 2.20 (di Wedderburn-Artin)**.** *Sia A una F-algebra semisemplice con F algebricamente chiuso, allora*

$$A \cong \bigoplus_{M_i \in \mathcal{R}(A)} End_F(M_i)$$

Dimostrazione. Per quanto visto fino ad ora, l'algebra A si decompone nel modo seguente:

$$A = \bigoplus_{M_i \in \mathcal{R}(A)} M_i(A^o) \cong \bigoplus_{i=1}^{|\mathcal{R}(A)|} A\bar{\rho}_i$$

dove $\bar{\rho}_i$ è la rappresentazione di A su M_i $\forall i \in \{1, \dots, |\mathcal{R}(A)|\}$. Per il corollario del lemma di Schur si ha $End_A(M_i) = \Lambda \cong F$ e inoltre per il teorema del doppio centralizzante $A\bar{\rho}_i = End_\Lambda(M_i) = End_F(M_i)$. Ovviamente quanto detto vale al variare dell'indice i, perciò segue la tesi. □

Dalla dimostrazione appena fatta si evince inoltre che se A è una F-algebra semisemplice su un campo algebricamente chiuso, ed M un A-modulo irriducibile, allora la rappresentazione di A su M è una funzione suriettva.
Il teorema di Wedderburn-Artin può essere espresso in forma più generale senza limitarsi alle algebre semisemplici su campi algebricamente chiusi, ed assume una connotazione leggermente diversa. Il teorema 2.20 appena dimostrato risulta in realtà un corollario del teorema di Wedderburn-Artin, dovuto a Theodor Molien. Con le notazioni usate in precedenza si hanno inoltre i seguenti corollari:

Corollario 2.21.

$$dim(A) = \sum_{M_i \in \mathcal{R}(A)} dim(M_i)^2$$

Dimostrazione. Si può vedere $End_F(M)$ come spazio vettoriale di matrici quadrate di dimensione $d \times d$ dove $d = dim(M)$. Segue che $dim(End_F(M)) = d^2$, e quindi per il teorema di Wedderburn-Artin si ha la tesi. □

Corollario 2.22.

$$n_M(A^o) = dim(M)$$

Dimostrazione. Sia $d = dim(M)$, quindi come conseguenza del corollario precedente si ha che $dim\big(M(A^o)\big) = d^2$. Dal momento che $M(A^o)$ è somma diretta di $n_M(A^o)$ sottomoduli isomorfi, allora $d^2 = n_M(A^o) \cdot d$, ovvero $d = n_M(A^o)$. □

Sotto opportune ipotesi sono state classificate in modo unico tutte le F-algebre semisemplici come somma diretta di algebre di matrici. Tornando alla rappresentazione di gruppi, si è visto che ad ogni $F[G]$-modulo corrisponde in modo unico un FG-modulo e quindi una rappresentazione di G. In particolare il campo dei complessi $\mathbb{C}$ ha caratteristica 0 e inoltre è algebricamente chiuso, dunque il teorema di Wedderburn-Artin vale per $\mathbb{C}[G]$. Per tale motivo in seguito verranno considerati solamente $\mathbb{C}[G]$-moduli e quindi rappresentazioni di gruppi su spazi vettoriali sul campo dei complessi.

Per ulteriori approfondimenti sulle F-algebre si guardi il testo:

Drozd, Kirichenko - Finite Dimensional Algebras (Springer-Verlag, 1994*).*

Capitolo 3

Caratteri

3.1 Definizioni e prime proprietà

Nel capitolo 1 si è visto come un gruppo può avere tantissime rappresentazioni equivalenti su uno spazio vettoriale V, e per il lemma 1.7 ciò vuol dire che esistono tantissimi FG-moduli isomorfi. Bisogna cercare di limitare tale inutile abbondanza poiché in algebra le strutture isomorfe fra loro possono essere considerate uguali, dunque la cosa più ovvia da fare è quella di considerare le classi di isomorfismo di FG-moduli. La conoscenza delle suddette classi è un'informazione importantissima poiché equivale a conoscere tutte le rappresentazioni lineari di un gruppo G se sono verificate le ipotesi del teorema di Maschke. Il problema è che non è affatto semplice individuare ognuna delle classi di isomorfismo, quindi si sente il bisogno di costruire un tool che caratterizzi in modo univoco ogni classe di isomorfismo di FG-moduli:

Definizione. Sia ρ la rappresentazione di G un gruppo finito su uno spazio vettoriale V di dimensione finita su un campo F, allora la funzione

$$\begin{aligned} \chi_\rho : G &\longrightarrow F \\ g &\longmapsto tr(g\rho) \end{aligned}$$

è detta *carattere di G associato a ρ*, dove con $tr(g\rho)$ si indica la traccia della matrice associata a $g\rho \in GL(V)$.

Prima di proseguire bisogna fare alcune osservazioni. Innanzitutto da ora in poi si considereranno soltanto rappresentazioni su spazi vettoriali costruiti sul campo $\mathbb{C}$. Inoltre, siccome ad ogni rappresentazione di G corrisponde in modo unico una rappresentazione dell'algebra gruppale $\mathbb{C}[G]$, la funzione χ_ρ può essere definita su tutto $\mathbb{C}[G]$ indicando con ρ la rappresentazione di $\mathbb{C}[G]$ su V (per semplicità si evita la ridondante notazione $\bar{\rho}$). In sostanza quando si parlerà di carattere di G, si intenderà, a dispetto della definizione formale, la funzione:

$$\begin{aligned} \chi_\rho : \mathbb{C}[G] &\longrightarrow \mathbb{C} \\ x &\longmapsto tr(x\rho) \end{aligned}$$

di cui interessa in particolar modo il valore assunto sulla base G. Spesso, quando è chiaro dal contesto si ometterà il riferimento alla rappresentazione ρ e si

scriverà semplicemente χ, mentre l'insieme di tutti i caratteri di G si indicherà con $Char(G)$. Infine per ulteriore chiarezza l'immagine di g mediante χ_ρ sarà indicata con l'usuale notazione $\chi_\rho(g)$, abbandonando in tal caso la "postfix notation" tanto amata dagli algebristi.
Tornando allo sviluppo della teoria, si hanno i seguente lemmi:

Lemma 3.1. *Se ρ e μ sono due rappresentazioni equivalenti di $\mathbb{C}[G]$, allora $\chi_\rho = \chi_\mu$.*

Dimostrazione. Sia $g\mu = T^{-1}(g\rho)T \ \ \forall g \in G$, allora per le proprietà della traccia si ha che:

$$\chi_\mu(g) = tr(g\mu) = tr\big(T^{-1}(g\rho)T\big) = tr(g\rho) = \chi_\rho(g)$$

□

Lemma 3.2. *Sia ρ una rappresentazione di $\mathbb{C}[G]$ su V, allora χ_ρ è costante sulle classi di coniugio di G.*

Dimostrazione. Siano $g, h \in G$, allora:

$$\chi_\rho(h^{-1}gh) = tr\big((h^{-1}gh)\rho\big) = tr\big((h\rho)^{-1}(g\rho)(h\rho)\big) = tr(g\rho) = \chi_\rho(g)$$

Data l'arbitrarietà di g e h segue la tesi. □

Esempio 3.3. Sia ρ la rappresentazione di $\mathbb{C}[G]$ su V, allora ovviamente $1\rho = I_V$, quindi vale che $\chi_\rho(1) = tr(I_V) = dim(V)$. La quantità $\chi_\rho(1)$ è detta grado di χ_ρ e tutti i caratteri di grado 1 sono chiamati *caratteri lineari*.

L'insieme dei caratteri è anche chiuso rispetto alla somma:

Lemma 3.4. *Siano ρ e μ due rappresentazioni di $\mathbb{C}[G]$ rispettivamente sugli spazi vettoriali V e U, allora $\chi_\rho + \chi_\mu$ è il carattere associato alla rappresentazione di $\mathbb{C}[G]$ su $V \oplus U$ (somma diretta esterna).*

Dimostrazione. Si costruisca la rappresentazione τ di G su $(V \oplus U)$ mediante l'utilizzo di una matrice diagonale a blocchi, nel seguente modo:

$$g\tau = \left(\begin{array}{c|c} g\rho & 0 \\ \hline 0 & g\mu \end{array}\right) \quad \forall g \in G$$

Allora si vede che la traccia di $g\tau$ è uguale alla somma delle tracce di $g\rho$ e $g\mu$, ovvero $\chi_\rho(g) + \chi_\mu(g) = \chi_\tau(g)$. □

Anche il prodotto fra caratteri è un carattere, ma questo verrà provato più avanti.

Lemma 3.5. *Sia χ un carattere associato ad una rappresentazione ρ di $\mathbb{C}[G]$ su uno spazio vettoriale V allora:*

i) $\chi(g+h) = \chi(g) + \chi(h) \ \ \forall g, h \in G$

ii) Se χ è un carattere lineare allora $\chi(gh) = \chi(g)\chi(h) \ \ \forall g, h \in G$, ovvero χ è un omomorfismo di gruppi tra G e $\mathbb{C}^*$

Dimostrazione. Si sfrutta il fatto che ρ è un F-omomorfismo tra $\mathbb{C}[G]$ ed $End_{\mathbb{C}}(V)$:

$$i) \quad \chi(g+h) = tr\big((g+h)\rho\big) = tr\big((g\rho)+(h\rho)\big) = tr(g\rho)+tr(h\rho) = \chi(g)+\chi(h)$$

$$ii) \quad \chi(gh) = tr\big((gh)\rho\big) = (gh)\rho = (g\rho)(h\rho) = tr(g\rho)\cdot tr(h\rho) = \chi(g)\chi(h)$$

In tal caso il codominio di $\rho_{|G}$ è $\mathbb{C}^*$ e dunque χ è un omomorfismo di gruppi tra G e $\mathbb{C}^*$. □

Definizione. Un carattere χ_ρ associato ad una rappresentazione irriducibile (ovvero ad un $\mathbb{C}[G]$ modulo irriducibile) è detto *carattere irriducibile*, mentre un carattere associato ad una rappresentazione fedele è detto *carattere fedele*.

L'insieme di tutti i caratteri irriducibili di G è indicato con $Irr(G)$, e per semplicità un generico elemento di tale insieme verrà sempre indicato con χ_i dove ovviamente $i \in \mathbb{N}$.

3.2 Equazione delle classi e tavola dei caratteri

In questa sezione si ricaverà innanzitutto un risultato di estrema importanza chiamato equazione delle classi, che coinvolge l'ordine di un gruppo e le classi di coniugio e inoltre si indicherà come classificare tutte le rappresentazioni di un gruppo. Prima però è necessario dimostrare alcuni lemmi preliminari.

Definizione. Il centro di una F-algebra è l'insieme

$$Z(A) = \{a \in A \ : \ ax = xa \ \ \forall x \in A\}$$

che è a sua volta un'algebra.

Lemma 3.6. *Sia V uno spazio vettoriale di dimensione finita su $\mathbb{C}$, allora $Z\big(End_{\mathbb{C}}(V)\big) = \Lambda$.*

Dimostrazione. Si consideri l'algebra $A = End_{\mathbb{C}}(V)$ che agisce in modo naturale su V. Segue che V è un A-modulo irriducibile, poiché se U fosse un A-modulo proprio di V si avrebbe $U\varphi \subseteq U \ \ \forall \varphi \in A$. Ma ciò è assurdo perché è sempre possibile trovare una funzione lineare che mappa un punto di U fuori da U; ad esempio se una base $\{u_1, \dots, u_s\}$ di U si completa ad una base $\mathcal{B} = \{u_1, \dots, u_s, v_1 \dots, v_t\}$ di V, basta prendere una funzione biunivoca da $\mathcal{B}$ in $\mathcal{B}$ che manda u_1 in v_1 ed estenderla per linearità. Quindi per il corollario 2.18 si ha che

$$Z\big(End_{\mathbb{C}}(V)\big) = C_{End_{\mathbb{C}}(V)}(End_{\mathbb{C}}(V)) = End_A(V) = \Lambda$$

□

Per dimostrare il lemma precedente, si può anche non fare riferimento al lemma di Schur e utilizzare soltanto risultati di algebra lineare (è un buon esercizio di ripasso).

Lemma 3.7. *Sia $A{=}B \oplus C$ una F-algebra, con B e C ideali bilateri di A, allora $Z(A) = Z(B) \oplus Z(C)$*

Dimostrazione. sia $b+c \in Z(A)$, allora $(b+c)(x+y) = (x+y)(b+c)\ \forall (x+y) \in A$ (dove chiaramente $x \in B$ e $y \in C$). In partcolare

$$(b+c)(x+0) = (x+0)(b+c) \Rightarrow bx + cx = xb + xc$$

Siccome B e C sono ideali bilateri di A, allora $cx \in B \cap C$ e $xc \in B \cap C$ da cui segue che $cx = xc = 0$. Ma allora si ha che $bx = xb\ \forall x \in B$, ovvero $b \in Z(B)$ e in modo del tutto simile si prova che $c \in Z(C)$. Ovviamente $Z(B) \cap Z(C) = \{0\}$, quindi $Z(A) \subseteq Z(B) \oplus Z(C)$. D'altro canto si vede facilmente che $Z(B) \oplus Z(C) \subseteq Z(A)$, poiché preso $(b+c) \in Z(B) \oplus Z(C)$, per ogni $x + y \in A$ si ha che:

$$(b+c)(x+y) = bx + by + cx + cy = xb + yb + xc + yc = (x+y)(b+c)$$

dove per lo stesso motivo espresso in precedenza $by = yb = cx = xc = 0$. □

Lemma 3.8. *Sia $A = I_1 \oplus I_2 \oplus \ldots \oplus I_k$ una F-algebra, con $k \geq 2$ e con I_j ideale bilatero di $A\ \forall j \in \{1, \ldots, k\}$, allora $Z(A) = Z(I_1) \oplus Z(I_2) \oplus \ldots \oplus Z(I_k)$.*

Dimostrazione. Si procede per induzione su k, se $k = 2$, allora la tesi è vera per il lemma precedente. Si supponga ora che la tesi valga per la somma di $k-1$ ideali; allora $A = (I_1 \oplus I_2 \oplus \ldots \oplus I_{k-1}) \oplus I_k$ quindi ancora una volta per il lemma precedente:

$$Z(A) = Z(I_1 \oplus I_2 \oplus \ldots \oplus I_{k-1}) \oplus Z(I_k)$$

Dall'ipotesi induttiva segue l'asserto. □

L'equazione delle classi discende direttamente dal seguente teorema che in gran parte e' stato già dimostrato:

Teorema 3.9. *Sia G un gruppo finito, allora le seguenti quantità sono uguali:*

i) Il numero delle classi di isomorfismo dei $\mathbb{C}[G]$ moduli irriducibili.

ii) Il numero degli addendi di una decomposizione di $\mathbb{C}[G]$ come somma diretta di ideali bilateri e minimali.

iii) Il numero delle classi di coniugio di G.

iv) $dim(Z(\mathbb{C}[G]))$.

Dimostrazione. Nel capitolo 2 si è visto che $i) = ii)$.
$i) = iv)$ Dal teorema di Wedderburn-Artin è noto che

$$\mathbb{C}[G] \cong \bigoplus_{M_i \in \mathcal{R}(\mathbb{C}[G])} End_{\mathbb{C}}(M_i)$$

dove ogni $End_{\mathbb{C}}(M_i)$ è isomorfo ad un ideale bilatero di A, quindi per il lemma 3.8:

$$Z(\mathbb{C}[G]) \cong \bigoplus_{M_i \in \mathcal{R}(\mathbb{C}[G])} Z(End_{\mathbb{C}}(M_i))$$

Ma nel lemma 3.37 si è visto che $Z(End_{\mathbb{C}}(M_i)) = \Lambda$ che ha dimensione 1, quindi

$$dim(Z(\mathbb{C}[G])) = \bigoplus_{M_i \in \mathcal{R}(\mathbb{C}[G])} dim(\Lambda) = \sum_{M_i \in \mathcal{R}(\mathbb{C}[G])} 1 = |\mathcal{R}(\mathbb{C}[G])|$$

iii) = *iv*) Si considerino le classi di coniugio di G denotate con $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_t$, e si ponga

$$z_i = \sum_{g \in \mathcal{C}_i} g \qquad \text{con } i \in \{1, \ldots, t\}$$

Ovvero in $\mathbb{C}[G]$ si considera la somma (operazione dello spazio vettoriale) degli elementi della base appartenenti alla stessa classe di coniugio $\mathcal{C}_i$. Allora preso un generico $h \in G$ vale che

$$h^{-1} z_i h = h^{-1} \left(\sum_{g \in \mathcal{C}_i} g \right) h = \sum_{g \in \mathcal{C}_i} h^{-1} g h = z_i$$

L'ultima uguaglianza segue dal fatto che il coniugio è un automorfismo di G e le classi di coniugio sono sottoinsiemi invarianti, dunque semplicemente si fa la somma con gli addendi scritti in ordine diverso. Si è appena visto che $z_i h = h z_i$, $\forall h \in G$, ovvero z_i commuta con tutti gli elementi della base da cui segue per linearità che z_i commuta con tutti gli elementi di $\mathbb{C}[G]$, dunque $z_i \in Z(\mathbb{C}[G])$. Si consideri ora l'equazione

$$\sum_{j=1}^{t} \lambda_j z_j = 0 \qquad \text{con } \lambda_j \in \mathbb{C} \quad \forall j \in \{1, \ldots, t\}$$

essa equivale a eguagliare una combinazione lineare di tutti gli elementi di G a zero, poiché le classi di coniugio partizionano il gruppo. Segue allra che $\lambda_j = 0$ $\forall j \in \{1, \ldots, t\}$ e dunque $\{z_i, z_2, \ldots, z_t\}$ è un insieme di vettori linearmente indipendenti di $Z(\mathbb{C}[G])$. Sia inoltre ζ un generico elemento di $Z(\mathbb{C}[G])$, allora $h^{-1}\zeta h = \zeta \ \forall h \in G$. quindi:

$$\zeta = \sum_{g \in G} \lambda_g g = h^{-1} \left(\sum_{g \in G} \lambda_g g \right) h = \sum_{g \in G} \lambda_g (h^{-1} g h) \tag{3.1}$$

Data l'arbitrarietà di h, quanto appena scritto significa che i coefficienti λ_g sono costanti sulle classi di coniugio, ovvero tutti gli elementi coinvolti nella somma che appartengono a $\mathcal{C}_i$ avranno lo stesso coefficiente indicato con $\lambda_{\mathcal{C}_i}$. Riordinando gli addendi dell'ultima sommatoria dell'equazione 3.1 in "pacchetti" dove ogni pacchetto è una classe di coniugio, si ottiene:

$$\zeta = \sum_{g \in G} \lambda_g (h^{-1} g h) = \sum_{j=1}^{t} \left(\lambda_{\mathcal{C}_j} \sum_{g \in \mathcal{C}_j} g \right) = \sum_{j=1}^{t} \lambda_{C_j} z_j$$

Segue che $\{z_1, z_2, \ldots, z_t\}$ è anche un insieme di generatori per $Z(\mathbb{C}[G])$ e dunque è una base di cardinalità t. Si conclude perciò che

$$dim(Z\mathbb{C}[G]) = t = \left| \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_t\} \right|$$

ovvero *iii*) = *iv*). □

Corollario 3.10 (Equazione delle classi)**.** *Sia G un gruppo finito; se G ha k classi di coniugio, allora $|G|$ è somma di k quadrati*

Dimostrazione. Per il corollario 2.21 si ha che

$$|G| = dim(\mathbb{C}[G]) = \sum_{i=1}^{k} {d_i}^2$$

dove $k = \left|\mathcal{R}(\mathbb{C}[G])\right|$ e d_i è la dimensione dell'i-esimo elemento di $\mathcal{R}(\mathbb{C}[G])$. Per il teorema precedente, k è anche il numero delle classi di coniugio di G, dunque segue che $|G|$ è somma di k quadrati. □

Ricordando inoltre che $\chi_i(1) = d_i$, allora si può riscrivere:

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2$$

Corollario 3.11. *Sia G un gruppo finito con k classi di coniugio, allora G possiede esattamente k caratteri irriducibili distinti.*

Dimostrazione. Dal teorema 3.9 segue che ci sono esattamente k $\mathbb{C}[G]$ moduli irriducibili a meno di isomorfismi. Di conseguenza ci sono k rappresentazioni irriducibili, ovvero k caratteri irriducibili per G. Bisogna ora vedere che tutti i caratteri irriducibili χ_i sono funzioni distinte su $\mathbb{C}[G]$:
si consideri ancora una volta l'equazione:

$$\mathbb{C}[G] = \bigoplus_{i=1}^{k} M_i(\mathbb{C}[G]^o)$$

allora la rappresentazione di $\mathbb{C}[G]$ su M_j è l'omorfismo di algebre:

$$\begin{array}{rcl} \rho_j : \mathbb{C}[G] & \longrightarrow & End_{\mathbb{C}}(M_j) \\ x & \longmapsto & L_x \end{array}$$

con $m_j L_x = {m_j}^x$. L'identità di $\mathbb{C}[G]$ si scrive come:

$$1 = \sum_{i=1}^{k} e_i \quad \text{con } e_i \in M_i(\mathbb{C}[G]^o)$$

quindi

$$1\rho_j = \sum_{i=1}^{k} e_i \rho_j = I$$

ma nel lemma 2.16(ii) si è visto che $M_i(\mathbb{C}[G]^o)$ annulla M_j se $i \neq j$, quindi facendo qualche conto si ha che $e_j\rho_j = 1\rho_j = I$ ed $e_i\rho_j = 0$ se $i \neq j$. Tornando ai caratteri si conclude facilmente che $\chi_j(e_j) = \chi_j(1) \neq 0$ mentre $\chi_j(e_i) = 0$ $\forall i \neq j$, quindi al variare di $j \in \{1, \dots k\}$ i caratteri irriducibili sono funzioni distinte. □

Un risultato molto importante, che nel seguito verrà esteso, è che l'insieme dei caratteri irriducibili $Irr(G)$, genera tutti i caratteri di G.

Corollario 3.12. *Sia G un gruppo con k classi di coniugio e sia inoltre ρ una rappresentazione di $\mathbb{C}[G]$, allora*

$$\chi_\rho = \sum_{i=1}^{k} c_i \chi_i \quad \text{con } c_i \in \mathbb{N}, \ \ \forall i \in \{1, \dots, t\}$$

Dimostrazione. Sia V il $C[G]$-modulo indotto da ρ, allora per il teorema di Maschke e per quanto visto nel capitolo 2, V si decompone nel seguente modo come somma di sottomoduli irriducibili:

$$V = n_{M_1} W_1 \oplus n_{M_2} W_2 \oplus \ldots \oplus n_{M_t} W_t$$

con $t \leq k$. A questo punto ponendo $c_i = n_{M_i} \ \forall i \in \{1, \dots, |Irr(G)|\}$ e notando che $c_i \neq 0$ se $i \leq t$ e $c_i = 0$ altrimenti, dal lemma 7.1 segue la tesi. □

La sola conoscenza dei caratteri irriducibili determina tutti i $\mathbb{C}[G]$-moduli irriducibili e dunque per il teorema di Maschke tutte le rappresentazioni di G. Fortunatamente dal corollario 3.11, si evince che per esaurire la descrizione di tutte le rappresentazioni (lineari) di G ci si riduce a determinare solamente le k funzioni di classe χ_i con $i \in \{1, \dots, k\}$.
La *tavola dei caratteri* è una tabella $k \times k$ con orlo, in cui sono esplicitati tutti i caratteri irriducibili di un gruppo finito G:

	$\mathcal{C}_1$	$\mathcal{C}_2$	$\cdots$	$\mathcal{C}_k$
χ_1	$\chi_1(\mathcal{C}_1)$	$\chi_1(\mathcal{C}_2)$	$\cdots$	$\chi_1(\mathcal{C}_k)$
χ_2	$\chi_2(\mathcal{C}_1)$	$\chi_2(\mathcal{C}_2)$	$\cdots$	$\chi_2(\mathcal{C}_k)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
χ_k	$\chi_k(\mathcal{C}_1)$	$\chi_k(\mathcal{C}_2)$	$\cdots$	$\chi_k(\mathcal{C}_k)$

Tabella 3.1. Tavola dei caratteri

Sull'orlo superiore della tabella ci sono le classi di coniugio del gruppo, sull'orlo di sinistra i caratteri irriducibili, mentre all'interno della tabella si trova il valore di ciascun carattere calcolato sulle classi di coniugio (si ricordi che un carattere è una funzione di classe; inoltre per convenzione si pone sempre $\mathcal{C}_1 = [1]$. Una volta costruita la tavola dei caratteri, sono state classificate tutte le rappresentazioni lineari di G. È importante sottolineare che se due gruppi sono isomorfi hanno chiaramente la stessa tavola dei caratteri, ma il viceversa non vale, infatti ad esempio Q_8 e D_8 non sono isomorfi ma hanno la stessa tavola dei caratteri.

3.3 Un lungo esempio: la tavola dei caratteri di S_3

Purtroppo costruire la tavola dei caratteri per un generico gruppo non è per niente semplice, tant' è che le informazioni in possesso fino ad ora non permettono di scrivere quasi nessuna tavola dei caratteri. Nelle prossime sezioni verranno dimostrate alcune proprietà dei caratteri utili a tal proposito, ma per il momento è molto didattico costruire, anche se in modo lungo e tortuoso, la tavola dei caratteri per S_3.

È noto che $S_3 = D_3$, quindi è possibile dare la seguente presentazione in termini di generatori e relazioni:

$$S_3 = \{\rho, \tau \ : \ \rho^3 = \tau^2 = 1,\ \tau^{-1}\rho\tau = \rho^{-1}\} = \{\rho^i\tau^j \ : \ 0 \leq i \leq 2 \ \text{ e } \ 0 \leq j \leq 1\}$$

Il gruppo in questione ha 3 classi di coniugio, ovvero 1, $\mathcal{C}_\rho = \{\rho, \rho^2\}$ che è formata da tutte rotazioni di un triangolo e $\mathcal{C}_\tau = \{\tau, \rho\tau, \rho^2\tau\}$ formato invece dalle trasposizioni. Dall'equazione delle classi segue che l'ordine di S_3 è somma di 3 quadrati, ma l'unica possibilità è $|S_3| = 6 = 1 + 1 + 2^2$. Per il corollario 2.21 si evince che S_3 ha due rappresentazioni irriducibili di grado 1 e una rappresentazione irriducibile di grado 2; non resta dunque che indagare a fondo la struttura di tali rappresentazioni e trovare i valori dei caratteri ad esse associati. Innanzitutto la rappresentazione banale è irriducibile, perciò la prima riga della tavola dei caratteri è nota:

	1	$\mathcal{C}_\rho$	$\mathcal{C}_\tau$
χ_1	1	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Per convenzione, si pone χ_1 uguale al carattere associato alla rappresentazione banale in ogni tavola dei caratteri. Inoltre, siccome si conosce la dimensione dei $\mathbb{C}G$-moduli irriducibili, oltre che la prima riga, è nota anche la prima colonna della tavola dei caratteri, infatti $\chi_2(1) = 1$ e $\chi_3(1) = 2$ (si ricordi l'esempio 3.3):

	1	$\mathcal{C}_\rho$	$\mathcal{C}_\tau$
χ_1	1	1	1
χ_2	1	$?$	$?$
χ_3	2	$?$	$?$

Restano da determinare i quattro valori contrassegnati dal punto interrogativo. Si consideri ora la funzione f da S_3 in $\mathbb{C}^* \cong \Lambda$ fatta nel seguente modo:

$$f(g) = \begin{cases} 1 & \text{se } g \in \mathcal{C}_\rho \vee g = 1 \\ -1 & \text{se } g \in \mathcal{C}_\tau \end{cases}$$

Visto che il prodotto di due rotazioni è ancora una rotazione, mentre il prodotto fra una rotazione ed una trasposizione è una trasposizione, appare chiaro che f è un omomorfismo di gruppi e dunque è una rappresentazione ovviamente non equivalente a quella banale. Siccome $\mathbb{C}^*$ ha dimensione 1 si conclude che la rappresentazione è irriducibile ed è possibile quindi completare la seconda riga della tavola dei caratteri, notando che banalmente la traccia di uno scalare complesso è lo scalare stesso:

	1	$\mathcal{C}_\rho$	$\mathcal{C}_\tau$
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	$?$	$?$

Sono state trovate le due rappresentazioni irriducibili di grado 1, e si è visto che una è quella banale, mentre l'altra contraddistingue le due classi di coniugio non banali con il segno. Riguardo la rappresentazione irriducibile di grado 2, si considerino le matrici quadrate a valori complessi

$$R = \begin{pmatrix} e^{i\frac{2}{3}\pi} & 0 \\ 0 & e^{i\frac{4}{3}\pi} \end{pmatrix} \quad T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Vale che $R^3 = T^2 = I$ e $T^{-1}RT = R^{-1}$ quindi per il lemma 1.2 la funzione

$$\begin{array}{rcl} \theta : S_3 & \longrightarrow & GL_{\mathbb{C}}(\mathbb{C}^2) \\ \rho^i\tau^j & \longmapsto & R^iT^j \end{array}$$

è una rappresentazione di S_3.
Si supponga che esista un FG-sottomodulo non banale U di $\mathbb{C}^2$ di dimensione uno, significa che U deve essere lo span di un certo vettore $(z_1, z_2) \in \mathbb{C}^2$ e inoltre deve essere invariante sotto l'azione di S_3. In particolare si deve verificare che

$$(z_1, z_2)^\tau = (z_1, z_2)T = (z_2, z_1) = \lambda(z_1, z_2) \tag{3.2}$$
$$(z_1, z_2)^\rho = (z_1, z_2)R = (e^{i\frac{2}{3}\pi}z_1, e^{i\frac{4}{3}\pi}z_2) = \mu(z_1, z_2) \tag{3.3}$$

Le equazioni (3.2) e (3.3) sono entrambe verificate se e solo se $z_1 = z_2 = 0$ contraddicendo l'ipotesi $U \neq \{0\}$. Segue che la rappresentazione è irriducibile, perciò $\chi_3(\rho) = tr(R) = -1$ e $\chi_3(\tau) = tr(T) = 0$. La tavola dei caratteri per S_3 è così completa:

	1	$\mathcal{C}_\rho$	$\mathcal{C}_\tau$
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

Tabella 3.2. Tavola dei caratteri di S_3

Con le dovute generalizzazioni, l'idea di tale procedimento può essere utilizzata per ricavare la tavola dei caratteri di un generico gruppo diedrale.

3.4 Ulteriori proprietà dei caratteri

In questa sezione vengono dimostrati alcuni fatti fondamentali che riguardano i caratteri:

Lemma 3.13. *Un gruppo finito G è abeliano se e solo se ogni suo carattere irriducibile è lineare*

Dimostrazione. Sia $|G| = k$; il gruppo G è abeliano se e solo se ha k classi di coniugio, ovvero per l'equazione delle classi

$$|G| = k = \sum_{i=1}^{k} \chi_i(1)^2 \tag{3.4}$$

Ma $\forall i \in \{1, \dots k\}$ vale che $\chi_i(1) \geq 1$, allora l'equazione 3.4 è vera se e solo se $\chi_i(1) = 1 \ \ \forall i \in \{1, \dots k\}$. □

La costruzione della tavola dei caratteri di un gruppo abeliano dovrebbe essere dunque leggermente più semplice, dal momento che nel caso di caratteri lineari si è visto che essi sono omomorfismi di gruppi. Il seguente lemma impone alcune condizioni molto restrittive riguardo il valore che può essere assunto dai caratteri irriducibili:

Lemma 3.14. *Sia G un gruppo finito e χ un carattere di grado d relativo alla rappresentazione di $\mathbb{C}[G]$ su V, allora:*

i) *Se $g \in G$ è tale che che $o(g) = n$, allora $\chi(g)$ è somma di d radici n-esime dell'unità.*

ii) $\chi(g^{-1}) = \overline{\chi(g)} \ \ \forall g \in G$.

iii) *Se g e g^{-1} sono due elementi coniugati in G, allora $\chi(g) = \chi(g^{-1})$ è un numero reale.*

iv) $|\chi(g)| \leq \chi(1) \ \ \forall g \in G$.

Dimostrazione. *i)* Ovviamente $d = dim(V)$ e si ponga $\mu = \rho_{\big|_{\mathbb{C}[<g>]}}$. Segue che V è un $\mathbb{C}[< g >]$-modulo, ma $< g >$ è un gruppo abeliano dunque per il lemma 3.13 tutti i suoi caratteri irriducibili sono lineari. In pratica V si decompone come somma diretta di d $\mathbb{C}[<g>]$-sottomoduli di dimensione 1 che sono degli autospazi di dimensione 1 per la funzione lineare $g\mu$. Ci sono quindi esattamente d autovalori $\lambda_1, \ldots, \lambda_d$ per $g\mu$ ed esiste una base $\mathcal{B}$ formata da autovettori tale che:

$$\big[g\mu\big]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & 0 \\ & & \ddots & \\ 0 & & & \lambda_d \end{pmatrix}$$

La funzione $g\mu$ è un omomorfismo di gruppi, quindi

$$I = [(g^n)\mu]_{\mathcal{B}} = \Big(\big[g\mu\big]_{\mathcal{B}}\Big)^n = \begin{pmatrix} {\lambda_1}^n & & & \\ & {\lambda_2}^n & & 0 \\ & & \ddots & \\ 0 & & & {\lambda_d}^n \end{pmatrix}$$

ovvero $\lambda_i^n = 1 \ \forall i \in \{1, \ldots, d\}$. Siccome il carattere è una funzione invariante per cambiamenti di base segue che

$$tr([g\mu]_{\mathcal{B}}) = tr(g\mu) = tr(g\rho) = \chi_\rho(g) = \lambda_1 + \ldots + \lambda_d$$

e dunque la tesi.
ii) Siccome ρ è un omomorfismo di gruppi, allora $g^{-1}\rho = (g\rho)^{-1}$. Per il punto *i)* esiste una base $\mathcal{B}$ di autovettori per cui la matrice $\big[g\rho\big]_{\mathcal{B}}$ è diagonale, quindi:

$$\big[(g\rho)^{-1}\big]_{\mathcal{B}} = \begin{pmatrix} \frac{1}{\lambda_1} & & & \\ & \frac{1}{\lambda_2} & & 0 \\ & & \ddots & \\ 0 & & & \frac{1}{\lambda_d} \end{pmatrix}$$

Ancora dal punto *i)* segue che $\forall j \in \{1, \ldots, d\}$, il valore λ_j è una radice n-esima dell'unità, ovvero $|\lambda_j| = 1$. Ma è noto che $\frac{1}{\lambda_j} = \frac{\overline{\lambda_j}}{|\lambda_j|^2}$, quindi $\frac{1}{\lambda_j} = \overline{\lambda_j}$ e si

conclude che:

$$\chi(g^{-1}) = tr\big((g\rho)^{-1}\big) = \sum_{j=1}^{d} \frac{1}{\lambda_j} = \sum_{j=1}^{d} \overline{\lambda_j} = \overline{\lambda_1 + \lambda_2 + \ldots + \lambda_d} = \overline{\chi(g)}$$

iii) Siccome ogni carattere è una funzione di classe si ha che

$$\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$$

dove l'ultima uguaglianza vale per il punto *ii*). Se un numero complesso è uguale al suo coniugato vuol dire che esso è reale, nel caso specifico $\chi(g) \in \mathbb{R}$.
iv) Si ponga $d = dim(V)$, allora per il punto *i*) e per la disuguaglianza triangolare si ha

$$|\chi(g)| = |\lambda_1 + \lambda_2 \ldots + \lambda_d| \leq |\lambda_1| + |\lambda_2| + \ldots + |\lambda_d| = d = \chi(1)$$

. □

L'ultimo punto del lemma precedente implica che nella tavola dei caratteri, considerando una singola riga, il numero con massimo modulo si trova in corrispondenza della prima colonna.
Data la sua importanza bisogna definire a parte un particolare carattere:

Definizione. Il carattere associato alla rappresentazione regolare[1] di $\mathbb{C}[G]$, si chiama *carattere regolare*, e viene indicato con χ_{reg}.

Lemma 3.15. *Sia G un gruppo con k classi di coniugio, allora riguardo il carattere regolare, vale che:*

$$\chi_{reg} = \sum_{i=1}^{k} \chi_i(1)\chi_i$$

Dimostrazione. Come nell'equazione 2.4, il modulo $\mathbb{C}[G]^o$ si decompone nella somma di sottomoduli irriducibili:

$$\mathbb{C}[G]^o = n_{M_1} W_1 \oplus n_{M_2} W_2 \oplus \ldots \oplus n_{M_k} W_k$$

Per il corollario 2.22 vale che $n_{M_i} = dim(M_i) = dim(W_i)$, quindi ricordando come si comporta il carattere relativo ad una somma diretta di $\mathbb{C}[G]$-moduli, segue facilmente la tesi. □

Lemma 3.16. *Sia χ_{reg} il carattere regolare di un gruppo finito G, allora:*

$$\chi_{reg}(g) = \begin{cases} |G| & se\ g = 1 \\ 0 & se\ g \neq 1 \end{cases}$$

Dimostrazione. Ovviamente se $g = 1$, $\chi_{reg}(1) = dim(\mathbb{C}[G]^o) = |G|$. Si supponga ora $g \neq 1$; la moltiplicazione a destra per g è in realtà una permutazione degli elementi della base di $\mathbb{C}[G]^o$, quindi l'applicazione $g\rho$ è rappresentata da una matrice di permutazione. La traccia di una matrice di permutazione in generale è il numero di punti fissi, quindi nel caso in oggetto

$$\chi_{reg}(g) = \big|\{g_j \in G \,:\, g_j g = g_j\}\big|$$

È chiaro però che se $g \neq 1$, la moltiplicazione a destra per g non possiede punti fissi, perciò $\chi_{reg}(g) = 0$. □

[1] si intende la rappresentazione corrispondente al modulo regolare destro $\mathbb{C}[G]^o$

3.5 Lo spazio di Hilbert delle funzioni di classe

Sia G un gruppo, e si indichi con $c\ell(G)$ l'insieme delle funzioni di classe (di coniugio) definite su G e a valori in $\mathbb{C}$; per uniformità di notazione con i caratteri, anche per gli elementi di $c\ell(G)$ non si userà la "postfix notation". Con le usuali operazioni di somma tra funzioni e prodotto di una funzione per uno scalare, risulta che $c\ell(G)$ è uno spazio vettoriale sul campo $\mathbb{C}$. È facile verificare, infatti, che presi $\varphi, \theta \in c\ell(G)$, allora $\varphi(g)+\theta(g)$ è ancora costante sulle classi di coniugo, e lo stesso vale per $c\varphi(g)$ con $c \in \mathbb{C}$. Notare che $Char(G)$ non è un sottospazio vettoriale di $c\ell(G)$ poiché se χ è un carattere allora $\psi = -\chi$ non lo è, infatti se ψ fosse un carattere si avrebbe $\psi(1) = -\chi(1) < 0$ che è un assurdo. Si definisce ora una funzione

$$\langle\ ,\ \rangle : c\ell(G) \times c\ell(G) \longrightarrow \mathbb{C}$$

tale che

$$\langle \varphi, \theta \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta(g)}$$

Si verifica quindi che $\langle\ ,\ \rangle$ è una forma Hermitiana definita positiva, infatti:

$$\begin{aligned}
\langle c_1\varphi_1 + c_2\varphi_2, \theta \rangle &= \frac{1}{|G|} \sum_{g \in G} \Big(c_1\varphi_1(g) + c_2\varphi_2(g) \Big)\overline{\theta(g)} = \\
&= \frac{1}{|G|} \left(\sum_{g \in G} c_1\varphi_1(g)\overline{\theta(g)} + \sum_{g \in G} c_2\varphi_2(g)\overline{\theta(g)} \right) = \\
&= \frac{c_1}{|G|} \sum_{g \in G} \varphi_1(g)\overline{\theta(g)} + \frac{c_2}{|G|} \sum_{g \in G} \varphi_2(g)\overline{\theta(g)} = \\
&= c_1\langle \varphi_1, \theta \rangle + c_2\langle \varphi_2, \theta \rangle
\end{aligned}$$

$$\begin{aligned}
\langle \varphi, c_1\theta_1 + c_2\theta_2 \rangle &= \frac{1}{|G|} \sum_{g \in G} \varphi(g) \Big(\overline{c_1\theta_1(g)} + \overline{c_2\theta_2(g)} \Big) = \\
&= \frac{1}{|G|} \left(\sum_{g \in G} \varphi(g)\overline{c_1\theta_1(g)} + \sum_{g \in G} \varphi(g)\overline{c_2\theta_2(g)} \right) = \\
&= \frac{\overline{c_1}}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta_1(g)} + \frac{\overline{c_2}}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta_2(g)} = \\
&= \overline{c_1}\langle \varphi, \theta_1 \rangle + \overline{c_2}\langle \varphi, \theta_2 \rangle
\end{aligned}$$

$$\langle \varphi, \theta \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta(g)} = \frac{1}{|G|} \sum_{g \in G} \overline{\theta(g)}\varphi(g) = \frac{1}{|G|} \sum_{g \in G} \overline{\theta(g)\overline{\varphi(g)}} = \overline{\langle \theta, \varphi \rangle}$$

$$\langle \varphi, \varphi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\varphi(g)} > 0 \quad \text{se } \varphi \neq 0 \qquad \text{mentre } \langle 0, 0 \rangle = 0$$

Segue che $\langle\ ,\ \rangle$ definisce un prodotto interno in $c\ell(G)$, ovvero $\Big(c\ell(G), \langle\ ,\ \rangle \Big)$ è uno spazio prehilbertiano. Il seguente lemma però permette di poter dire molto di più:

Lemma 3.17. *Sia G un gruppo finito con k classi di coniugio, allora $c\ell(G)$ è uno spazio vettoriale di dimensione finita e si ha che $dim(c\ell(G)) = k$.*

Dimostrazione. Siano $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k$ le classi di coniugio di G e siano inoltre i e j due indici che scorrono da 1 a k. Basta dimostrare che l'insieme

$$\mathcal{B} = \{\varphi_i \in c\ell(G) \,:\, \varphi_i(C_j) = \delta_{ij}\}$$

formato dalle k funzioni distinte che valgono 1 su una determinata classe di equivalenza e 0 altrove, è una base di $c\ell(G)$. Sia θ una generica funzione di $c\ell(G)$ tale che $\theta(\mathcal{C}_i) = a_i$, allora è evidente che:

$$\theta = \sum_{i=1}^{k} a_i \varphi_i$$

quindi $\mathcal{B}$ genera $c\ell(G)$. Si consideri ora la seguente combinazione lineare a coefficienti in $\mathbb{C}$:

$$c_1\varphi_1 + c_2\varphi_2 + \ldots + c_k\varphi_k = 0$$

Sia $g_j \in \mathcal{C}_j$, allora vale che

$$c_1\varphi_1(g_j) + c_2\varphi_2(g_j) + \ldots + c_k\varphi_k(g_j) = c_j\varphi_j(g_j) = c_j = 0$$

data l'arbitrarietà di g_j segue che i coefficienti della combinazione lineare sono tutti nulli, ovvero $\mathcal{B}$ è un insieme di k vettori linearmente indipendenti. Si conclude che $\mathcal{B}$ è una base per $c\ell(G)$. □

Siccome ogni spazio prehilbertiano di dimensione finita è uno spazio di Hilbert, dal lemma precedente segue che $\Big(c\ell(G), \langle\ ,\ \rangle\Big)$ è in realtà uno spazio di Hilbert. In precedenza si è visto che i caratteri irriducibili di un gruppo G generano tutti i caratteri di G mediante combinazioni lineari a coefficienti in $\mathbb{N}$, ma in realtà vale il seguente teorema:

Teorema 3.18. *Sia G un gruppo finito, allora $Irr(G)$ è una base di $c\ell(G)$.*

Dimostrazione. Se G ha k classi di coniugio, dal lemma precedente segue che $c\ell(G)$ ha dimensione k e inoltre per il corollario 3.11 ci sono esattamente k caratteri irriducibili. Per dimostrare che essi formano una base, basta dunque far vedere che sono linearmente indipendenti. Si consideri come al solito una combinazione lineare dei caratteri irriducibili, a coefficienti in $\mathbb{C}$, uguagliata a 0:

$$c_1\chi_1 + c_2\chi_2 + \ldots + c_k\chi_k = 0$$

si scelga ora una generica componente omogenea $M_j(\mathbb{C}[G]^o)$ dell'algebra gruppale $\mathbb{C}[G]$ con $j \in \{1, \ldots, k\}$ e si valutino i caratteri irriducibili in e_j. Per quanto visto nella dimostrazione del corollario 3.11, si ha che $\chi_i(e_j) = 0$ se $i \neq j$, mentre $\chi_j(e_j) \neq 0$, perciò:

$$c_1\chi_1(e_j) + c_2\chi_2(e_j) + \ldots + c_k\chi_k(e_j) = c_j\chi_j(e_j) = 0$$

da cui segue che $c_j = 0$. Dall'arbitrarietà di j, si evince che tutti i coefficienti della combinazione lineare sono nulli e quindi $Irr(G)$ è una base per $c\ell(G)$. □

Corollario 3.19. *Sia G un gruppo finito con k classi di coniugio e siano inoltre $g, h \in G$; g e h sono coniugati se e solo se $\chi_i(g) = \chi_i(h) \ \ \forall i \in \{1, \dots, k\}$.*

Dimostrazione. ($\Rightarrow$) È ovvio visto che i caratteri sono funzioni di classe.
($\Leftarrow$) Sia $\mathcal{C}_g$ la classe di coniugio di g e si consideri la funzione di classe ψ che vale 1 su $\mathcal{C}_g$ e 0 altrove. Per il teorema precedente ψ si decompone in modo unico nella seguente maniera:

$$\psi = \sum_{i=1}^{k} c_i \chi_i \quad \text{con } c_i \in \mathbb{C} \ \ \forall i \in \{1, \dots, k\}$$

Utilizzando ora le ipotesi si ottiene la seguente catena di uguaglianze:

$$1 = \psi(g) = \sum_{i=1}^{k} c_i \chi_i(g) = \sum_{i=1}^{k} c_i \chi_i(h) = \psi(h)$$

Segue che $h \in \mathcal{C}_g$, ovvero g e h sono coniugati. □

Corollario 3.20. *Sia G un gruppo finito con k classi di coniugio, allora $g \in G$ è coniugato a g^{-1} se e solo se $\chi_i(g) \in \mathbb{R} \ \ \forall i \in \{1, \dots, k\}$.*

Dimostrazione. Si utilizza pesantemente il lemma 3.14 *ii*), ovvero il fatto che $\chi(g^{-1}) = \overline{\chi(g)}$ per ogni carattere χ di G.
($\Rightarrow$) Se g e g^{-1} sono coniugati, $\chi_i(g) = \chi_i(g^{-1}) = \overline{\chi_i(g)}$, ovvero $\chi_i \in \mathbb{R} \ \ \forall i \in \{1, \dots, k\}$.
($\Leftarrow$) Viceversa se $\chi_i(g) \in \mathbb{R}$, allora $\chi_i(g) = \overline{\chi_i(g)} = \chi_i(g^{-1}) \ \ \forall i \in \{1, \dots, k\}$, quindi per il corollario 3.19 segue la tesi. □

Si noti che i due corollari precedenti possono essere riformulati sostituendo a $Irr(G)$ l'insieme $Char(G)$, ovvero le proprietà sopra dimostrate valgono per tutti i caratteri di G e non solo per quelli che compongono la tavola dei caratteri. A questo punto è possibile dare una caratterizzazione per le rappresentazioni di un gruppo G, esclusivamente mediante i caratteri associati:

Teorema 3.21. *Due rappresentazioni ρ e μ di $\mathbb{C}[G]$ a cui sono associati rispettivamente i moduli V e V', sono equivalenti se e solo se $\chi_\rho = \chi_\mu$.*

Dimostrazione. ($\Rightarrow$) È il lemma 3.1.
($\Leftarrow$) Supponendo che $|Irr(G)| = k$, per il lemma 3.12 si ha che:

$$\chi_\rho = \sum_{i=1}^{k} n_{M_i} \chi_i \qquad \text{e} \qquad \chi_\mu = \sum_{i=1}^{k} n'_{M_i} \chi_i$$

dove n_{M_i} sta per $n_{M_i}(V)$, e n'_{M_i} per $n_{M_i}(V')$. Dalle ipotesi si ha che $\chi_\rho = \chi_\mu$, inoltre nel teorema precedente si è visto che i caratteri irriducibili formano una base per $c\ell(G)$, allora segue che $n_{M_i} = n'_{M_i} \ \forall i \in \{1, \dots, k\}$. Riguardo la decomposizione dei moduli V e V' si ha quindi:

$$V = n_{M_1} W_1 \oplus n_{M_2} W_2 \oplus \dots \oplus n_{M_k} W_k$$

$$V' = n_{M_1} W'_1 \oplus n_{M_2} W'_2 \oplus \dots \oplus n_{M_k} W'_k$$

con $M_i \cong W_i \cong W'_i \ \forall i \in \{1, \dots, k\}$ per definizione. Si faccia attenzione al fatto che nelle due decomposizioni precedenti, alcuni coefficienti che precedono i sottomoduli possono essere nulli; ad esempio se n_{M_s} è nullo, vuol dire che non ci sono sottomoduli di V isomorfi ad M_s dunque quello che viene indicato con W_s è un sottomodulo puramente fittizio. Si conclude che $V \cong V'$, ovvero che le rappresentazioni ρ e μ sono equivalenti. □

3.6 Prodotto interno di caratteri

Una volta definita una base per $c\ell(G)$, si veda come si comporta il prodotto interno $\langle\ ,\ \rangle$ su di essa. Si ricaveranno dunque le *relazioni di ortoginalità* che impongono alcune condizioni su come devono essere costituite le righe e le colonne della tavola dei caratteri.

Lemma 3.22. *Siano χ e ψ due caratteri, allora $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle \in \mathbb{R}$.*

Dimostrazione. Si svolgono i calcoli utilizzando il lemma 3.14 *ii*):

$$\langle \chi, \psi \rangle = \sum_{g \in G} \chi(g)\psi(g^{-1})$$

$$\langle \psi, \chi \rangle = \sum_{g \in G} \psi(g)\chi(g^{-1}) = \sum_{g^{-1} \in G} \chi(g^{-1})\psi(g)$$

È chiaro che far variare g in G è lo stesso che far variare g^{-1} in G, perciò $\langle \chi, \psi \rangle = \langle \psi, \chi \rangle$. A questo punto dalla definizione di forma Hermitiana si ha che $\langle \chi, \psi \rangle = \overline{\langle \psi, \chi \rangle} = \langle \psi, \chi \rangle$, ma quando un numero complesso è uguale al suo coniugato, segue che in realtà è un numero reale. □

Si consideri ora l'algebra gruppale $\mathbb{C}[G]$ e si definisca la seguente funzione sulla base:

$$[\ ,\ ] : G \times G \longrightarrow \mathbb{C}$$

con $[g, h] = \frac{1}{|G|}\chi_{reg}(gh^{-1})$; estendendo tale funzione per (sesqui)linearità su tutta l'algebra gruppale $\mathbb{C}[G]$ si ottiene facilmente una forma Hermitiana definita positiva. Si noti inoltre, che per il lemma 3.16, vale che $[g, h] = \delta_{g,h}$, dunque G è una base ortonormale per $\mathbb{C}[G]$. Dalla teoria delle forme Hermitiane, si sa che in presenza di una base ortonormale è possibile scomporre un generico vettore in un modo molto comodo, in questo caso sia infatti $x \in \mathbb{C}[G]$, allora:

$$x = \sum_{g \in G} [x, g]g$$

dove $[x, g]$ è evidentemente la proiezione di x su g, ovvero il coefficiente moltiplicativo di g nella decomposizione canonica di x come combinazione lineare di elementi della base.

Lemma 3.23. *Sia G un gruppo con k classi di coniugio, e sia e_j l'identità dell'algebra $M_j(\mathbb{C}[G]^o)$ con $j \in \{1, \dots, k\}$. Se χ_j è il carattere irriducibile relativo alla rappresentazione ρ_j di $\mathbb{C}[G]$ su M_j allora*

$$e_j = \frac{1}{|G|} \sum_{g \in G} \chi_j(1)\chi_j(g^{-1})g$$

Dimostrazione. Innanzitutto si scompone e_j in $\mathbb{C}[G]$

$$e_j = \sum_{g\in G} a_g g \quad \text{con } a_g \in \mathbb{C}$$

ora, per quanto detto sulle forme Hermitiane si può scrivere:

$$e_j = \sum_{g\in G}[e_j, g]g = \sum_{g\in G}\frac{1}{|G|}\chi_{reg}(e_j g^{-1})g = \sum_{g\in G}\left(\frac{1}{|G|}\sum_{i=1}^{k}\chi_i(1)\chi_i(e_j g^{-1})\right)g \tag{3.5}$$

con l'ultima uguaglianza valida grazie al lemma 3.15. Per ogni rappresentazione irriducibile ρ_i su M_i si ha che $(e_j g^{-1})\rho_i = (e_j\rho_i)(g^{-1}\rho_i)$. Ma d'altra parte $e_j\rho_i = L_{e_j} \in End_{\mathbb{C}}(M_i)$ con $m_i L_{e_j} = m_1^{e_j} = 0$ per ogni $m_i \in M_i$ poiché $M_j(\mathbb{C}[G]^o)$ annulla tutto M_i. Ricordando che $\delta_{ij}I = e_j\rho_i$, segue dunque che $(e_j g^{-1})\rho_i = \delta_{ij}(g^{-1})\rho_i$, ovvero $\chi_i(e_j g^{-1}) = \delta_{ij}\chi_i(g^{-1})$. Applicando quanto appena detto all'equazione 3.5 si ottiene la tesi:

$$e_j = \sum_{g\in G}\left(\frac{1}{|G|}\sum_{i=1}^{k}\chi_i(1)\chi_i(e_j g^{-1})\right)g = \frac{1}{|G|}\sum_{g\in G}\chi_j(1)\chi_j(g^{-1})g$$

□

Teorema 3.24. *(I relazione di ortogonalità) Sia G un gruppo finito con k classi di coniugio, e siano inoltre χ_i e χ_j due caratteri irriducibili di G con $i, j \in \{1, \dots, k\}$. Allora si ha che:*

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} = \delta_{i,j}$$

ovvero $Irr(G)$ è una base ortonormale di $c\ell(G)$.

Dimostrazione. Al solito siano e_i ed e_j rispettivamente le identità delle algebre $M_i(\mathbb{C}[G]^o)$ e $M_j(\mathbb{C}[G]^o)$. È ormai noto che

$$e_i e_j = \delta_{i,j} e_i \tag{3.6}$$

e dunque si applica il lemma 3.23 ad entrambi i membri dell'equazione appena scritta:

$$\delta_{i,j} e_i = \sum_{g\in G}\frac{\delta_{i,j}}{|G|}\chi_i(1)\chi_i(g^{-1})g \tag{3.7}$$

$$e_i e_j = \left(\sum_{\ell\in G}\frac{1}{|G|}\chi_i(1)\chi_i(\ell^{-1})\ell\right)\left(\sum_{h\in G}\frac{1}{|G|}\chi_j(1)\chi_j(h^{-1})h\right) = \tag{3.8}$$

$$= \sum_{\ell,h\in G}\frac{\chi_i(1)\chi_j(1)}{|G|^2}\chi_i(\ell^{-1})\chi_j(h^{-1})\ell h$$

Ponendo $\ell h = g$ (dunque $\ell = gh^{-1}$) nell'ultimo membro dell'equazione 3.8, si può riscrivere

$$e_i e_j = \sum_{g\in G}\left(\frac{\chi_i(1)\chi_j(1)}{|G|^2}\sum_{h\in G}\chi_i(hg^{-1})\chi_j(h^{-1})\right)g \tag{3.9}$$

A questo punto dall'equazione 3.6, segue che è possibile uguagliare i generici coefficienti moltiplicativi delle equazioni 3.7 e 3.9:

$$\frac{\chi_i(1)\chi_j(1)}{|G|^2}\sum_{h\in G}\chi_i(hg^{-1})\chi_j(h^{-1}) = \frac{\delta_{i,j}}{|G|}\chi_i(1)\chi_i(g^{-1})$$

da cui segue che

$$\frac{1}{|G|}\sum_{h\in G}\chi_i(hg^{-1})\chi_j(h^{-1}) = \delta_{i,j}\frac{\chi_i(g^{-1})}{\chi_j(1)} \tag{3.10}$$

L'equazione 3.10 è detta *relazione di ortogonalità generalizzata*, e ponendo in essa $g = 1$ si ha

$$\frac{1}{|G|}\sum_{h\in G}\chi_i(h)\chi_j(h^{-1}) = \delta_{i,j}$$

ovvero la tesi ricordando che $\chi_j(h^{-1}) = \overline{\chi_j(h)}$. □

Un'importante conseguenza del teorema precedente è una caratterizzazione per i caratteri irriducibili:

Corollario 3.25. *Un carattere χ è irriducibile se e solo se $\langle\chi,\chi\rangle = 1$.*

Dimostrazione. ($\Rightarrow$) Se χ è irriducibile, allora per il teorema precedente è ovvio che $\langle\chi,\chi\rangle = 1$.
($\Leftarrow$) Per il lemma 3.12 vale che $\chi = n_1\chi_1 + n_2\chi_2 + \ldots + n_k\chi_k$ con $n_i \in \mathbb{N}$ $\forall i \in \{1,\ldots,k\}$; allora ancora una volta dal teorema precedente segue che $\langle\chi,\chi\rangle = {n_1}^2 + {n_2}^2 + \ldots + {n_k}^2 = 1$. Tale equazione è verificata se e solo se un solo coefficiente n_j con $j \in \{1,\ldots,k\}$ è uguale a 1 e tutti gli altri sono nulli, ovvero $\chi = \chi_j$. □

Corollario 3.26. *Se χ è un carattere irriducibile, allora anche $\overline{\chi}$ è irriducibile.*

Dimostrazione. La tesi segue dal facilmente corollario precedente, notando che $\langle\chi,\chi\rangle = \langle\overline{\chi},\overline{\chi}\rangle = 1$. □

Sia χ un generico carattere, allora il termine $\langle\chi,\chi_i\rangle \in \mathbb{N}$ è il coefficiente moltiplicativo di χ_i nella decomposizione di χ come combinazione lineare di elementi della base $Irr(G)$. Se $\langle\chi,\chi_i\rangle > 0$, si dirà dunque che χ_i è un *costituente di* χ.

Teorema 3.27 (II relazione di ortogonalità)**.** *Sia G gruppo finito con k classi di coniugio, allora $\forall g,h \in G$ si ha che:*

$$\sum_{i=1}^{k}\chi_i(g)\overline{\chi_i(h)} = \begin{cases} |C_G(g)| & \text{se } g \text{ e } h \text{ sono coniugati} \\ 0 & \text{altrimenti} \end{cases}$$

Dimostrazione. Dalla prima relazione di ortogonalità si ha che

$$|G|\delta_{i,j} = \sum_{g\in G}\chi_i(g)\overline{\chi_j(g)} \tag{3.11}$$

Indicando con $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k$ le classi di coniugio di G e ponendo per comodità $g_\ell \in C_\ell \ \forall \ell \in \{1, \ldots, k\}$, l'equazione 3.11 può essere riscritta nel modo seguente poiché i caratteri sono funzioni di classe:

$$|G|\delta_{i,j} = \sum_{\ell=1}^{k} |\mathcal{C}_\ell| \chi_i(g_\ell)\overline{\chi_j(g_\ell)} \tag{3.12}$$

Sia ora D la seguente matrice $k \times k$

$$D = \begin{pmatrix} |\mathcal{C}_1| & & & \\ & |\mathcal{C}_2| & & 0 \\ & & \ddots & \\ 0 & & & |\mathcal{C}_k| \end{pmatrix}$$

e X la tavola dei caratteri di G, dove i caratteri irriducibili sono valutati sui rappresentanti $g_1, \ldots, g_k$ delle classi di coniugio. Al variare dei due indici i e $j \in \{1, \ldots, k\}$, l'equazione 3.12 può essere vista come un insieme di k^2 uguaglianze riassunte nel prodotto matriciale

$$|G| I_{k\times k} = X D \overline{X}^t \tag{3.13}$$

Segue che $I_{k\times k} = X\left(\frac{1}{|G|} D\overline{X}^t\right)$, ovvero $\frac{1}{|G|} D\overline{X}^t$ è un'inversa destra di X, ma siccome si parla di matrici quadrate, essa deve essere anche un'inversa sinistra. In sostanza la tavola dei caratteri X è invertibile e si può scrivere:

$$|G| I_{k\times k} = D\overline{X}^t X \tag{3.14}$$

Esplicitando l'equazione 3.14 si ottiene:

$$|G|\delta_{i,j} = \sum_{\ell=1}^{k} |\mathcal{C}_i| \overline{\chi_\ell(g_i)} \chi_\ell(g_j)$$

da cui infine

$$\frac{|G|}{|C_i|}\delta_{i,j} = |C_G(g_i)|\delta_{i,j} = \sum_{\ell=1}^{k} \overline{\chi_\ell(g_i)} \chi_\ell(g_j)$$

La tesi segue notando che $\delta_{i,j} = 1$ solo quando g_j e g_i condividono lo stesso pedice, ovvero se appartengono alla stessa classe di coniugio. □

Una volta scritta la tavola dei caratteri per un gruppo, dalla II relazione di ortogonalità è possibile dunque ricavare le cardinalità delle varie classi di coniugio che partizionano il gruppo.

Esempio 3.28 (la tavola dei caratteri di C_3)**.** Sia $C_3 = \{1, a, a^2\}$ il gruppo ciclico di ordine 3, esso è abeliano e dunque possiede esattamente 3 classi di coniugio e tre caratteri irriducibili lineari. Il carattere χ_1 è ovviamente quello banale; i generatori di C_3 sono a e a^2, e siccome si sta parlando di caratteri lineari, $\chi_2(a)$ e $\chi_2(a^2)$ sono radici terze dell'unità. Segue che χ_2 è un omomorfismo da G nel gruppo moltiplicativo delle radici terze dell'unità denotato con U. Tale omomorfismo, visto che è non banale, è necessariamente suriettivo, poiché U

non ha sottogruppi propri. Posto $\omega = e^{\frac{2\pi i}{3}}$ i candidati a comporre la seconda riga della tavola dei caratteri sono dunque $\chi_2(1) = 1$ $\chi_2(a) = \omega$ e $\chi_2(a^2) = \omega^2$. Ovviamente χ_2 essendo di grado 1 è irriducibile ma è possibile verificare questo fatto mediante l'uso delle relazioni di ortogonalità:

$$\begin{aligned}\langle \chi_2, \chi_2 \rangle &= \frac{\chi_2(1)\overline{\chi_2(1)} + \chi_2(a)\overline{\chi_2(a)} + \chi_2(a^2)\overline{\chi_2(a^2)}}{3} = \\ &= \frac{1 \cdot 1 + \omega \cdot \overline{\omega} + \omega^2 \cdot \overline{\omega^2}}{3} = \frac{1 \cdot 1 + \omega \cdot \omega^2 + \omega^2 \cdot \omega}{3} = 1\end{aligned}$$

Dal momento che χ_2 è irriducibile, basta porre $\chi_3 = \overline{\chi_2}$ per completare la tavola dei caratteri.

	1	a	a^2
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

Tabella 3.3. Tavola dei caratteri di C_3

3.7 Caratteri e sottogruppi normali

Dato un generico gruppo finito G, per trovare le sue immagini omomorfe è necessario determinarne tutti i sottogruppi normali, ma ciò non è affatto semplice. In questa sezione si vedrà che tutte le informazioni sui sottogruppi normali G sono in realtà contenute nella sua tavola dei caratteri.

Definizione. Sia dato un carattere χ di G, allora il *nucleo di* χ è l'insieme

$$Ker(\chi) = \{g \in G : \chi(g) = \chi(1)\}$$

Lemma 3.29. *Sia ρ una rappresentazione di un gruppo finito G su uno spazio vettoriale V di dimensione d. Sia inoltre χ il carattere associato a ρ, allora $Ker(\chi) = Ker(\rho)$.*

Dimostrazione. Sia $g \in Ker(\rho)$, allora $\chi(g) = tr(g\rho) = tr(I_{d\times d}) = \chi(1)$, quindi $g \in Ker(\chi)$ e si ha che $Ker(\rho) \subseteq Ker(\chi)$. Viceversa si consideri $g \in Ker(\chi)$, ovvero tale che $\chi(g) = \chi(1)$; per il lemma 3.14 *i*), vale che:

$$d = \chi(g) = \sum_{i=1}^{d} \lambda_i \qquad \text{con } |\lambda_i| = 1 \ \forall i \in \{1, \dots, d\}$$

Si verifica quindi facilmente che

$$\left| \sum_{i=1}^{d} \lambda_i \right| = \sum_{i=1}^{d} |\lambda_i|$$

ovvero i vettori λ_i sono tutti uguali, e siccome la loro somma è proprio d che è un numero reale segue che $\lambda_i = 1 \ \forall i \in \{1, \dots, d\}$. Sempre nel lemma 3.14 *i*) si è

visto che esiste una rappresentazione μ di G, $g\mu = T^{-1}(g\rho)T$, con $T \in Aut(V)$ tale per cui

$$g\mu = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & 0 \\ & & \ddots & \\ 0 & & & \lambda_d \end{pmatrix} = I_{d\times d}$$

Segue facilmente che $g\rho = I_{d\times d}$, ovvero $g \in Ker(\rho)$ da cui si conclude $Ker(\chi) \subseteq Ker(\rho)$. □

A questo punto è ovvio che il nucleo di un carattere è un sottogruppo normale di G e dunque dalla tavola dei caratteri di G si possono trovare alcuni sottogruppi normali.

Esempio 3.30. Si consideri S_3 con la sua tavola dei caratteri (tabella 3.2). Chiaramente $Ker(\chi_1) = S_3$, ma guardando il carattere χ_2, si nota che $Ker(\chi_2) = 1 \cup \mathcal{C}_\rho = A_3$ ovvero un sottogruppo normale di S_3.

Resta ancora aperto il problema di determinare tutti i sottogruppi normali di un gruppo finito G dalla tavola dei caratteri, e a tal proposito è di fondamentale importanza il seguente teorema molto simile al teorema di corrispondenza per gruppi:

Teorema 3.31. *Sia G un gruppo finito ed $N \trianglelefteq G$, allora esiste una corrispondenza biunivoca tra gli insiemi $\{\chi \in Char(G) : N \subseteq Ker(\chi)\}$ e $Char(G/N)$. Inoltre mediante tale biiezione, a caratteri irriducibili corrispondono caratteri irriducibili.*

Dimostrazione. Sia $\hat{\chi} \in Char(G/N)$ associato alla rappresentazione $\hat{\rho}$ di G/N su un certo spazio vettoriale V, e si costruisca la funzione $\chi : G \to \mathbb{C}$ tale che $\chi(g) = \hat{\chi}(Ng)$. Prima di tutto si prova che χ è un carattere di G, e per fare ciò bisogna trovare una rappresentazione ρ di G che ha come carattere associato proprio χ. Utilizzando in questo caso la notazione da destra verso sinistra per la composizione di funzioni, si ponga $\rho = \hat{\rho} \circ \pi$, dove π è la proiezione canonica di G su G/N. Si ha evidentemente che ρ in quanto composizione di omomorfismi è un omomorfismo da G in $GL(V)$, inoltre:

$$\chi_\rho(g) = tr(g\rho) = tr((Ng)\hat{\rho}) = \hat{\chi}(Ng) = \chi(g)$$

da cui segue che χ è un carattere di G. A questo punto si vuole provare che la funzione f definita su $Char(G/N)$ tale per cui $f(\hat{\chi}) = \chi$ è la biiezione cercata. Sia $n \in N$, allora $\chi(n) = \hat{\chi}(Nn) = \hat{\chi}(N) = \chi(1)$, ovvero $N \subseteq Ker(\chi)$, dunque effettivamente si ha che:

$$f : Char(G/N) \longrightarrow \{\chi \in Char(G) : N \subseteq Ker(\chi)\}$$

Per provare che tale funzione è inoltre biunivoca si può procedere cercando una sua inversa bilatera. Sia χ un carattere di G tale che $N \subseteq Ker(\chi)$ associato alla rappresentazione ρ, in analogia a quanto fatto in precedenza si definisce $\hat{\chi} : G/N \to \mathbb{C}$ con $\hat{\chi}(Ng) = \chi(g)$, bisogna dunque verificare che la funzione $\hat{\chi}$

definisce un carattere di G/N. Sia $\hat{\rho} : G/N \to V$ tale che $(Ng)\hat{\rho} = g\rho$, essa è ben definita, infatti presi $g, h \in G$ tali che $Ng = Nh$ (ovvero $h^{-1}g \in N$) si ha:

$$I = (h^{-1}g)\rho = (h\rho)^{-1}g\rho$$

da cui $h\rho = g\rho$ e quindi $(Nh)\hat{\rho} = (Ng)\hat{\rho}$. La funzione $\hat{\rho}$ è un omomorfismo:

$$((Ng)(Nh))\hat{\rho} = (Ngh)\hat{\rho} = (gh)\rho = (g\rho)(h\rho) = ((Ng)\hat{\rho})((Nh)\hat{\rho})$$

e inoltre

$$\chi_{\hat{\rho}} = tr((Ng)\hat{\rho}) = tr(g\rho) = \chi(g) = \hat{\chi}(Ng)$$

Segue che $\hat{\chi}$ è un carattere di G/N come si voleva e la funzione $\tilde{f}$, tale per cui $\tilde{f}(\chi) = \hat{\chi}$ è l'inversa bilatera di f. L'ultima parte della dimostrazione è abbastanza semplice: la rappresentazione $\hat{\rho}$ su V è un omomorfismo tra le algebre $\mathbb{C}[G/N]$ ed $End_{\mathbb{C}}(V)$, mentre la rappresentazione ρ tale per cui $g\rho = (Ng)\hat{\rho}$ è un omomorfismo tra $\mathbb{C}[G]$ ed $End_{\mathbb{C}}(V)$. Sia W un sottospazio vettoriale di V e si considerino le azioni di $\mathbb{C}[G]$ e di $\mathbb{C}[G/N]$ su di esso, relativamente alle rispettive rappresentazioni ρ e $\hat{\rho}$, allora $\forall g \in G$ si ha:

$$w^{Ng} = w((Ng)\hat{\rho}) = w(g(\pi\hat{\rho})) = w(g\rho) = w^g$$

Dunque W è un $\mathbb{C}[G]$-sottomodulo di V se e solo se è un $\mathbb{C}[G/N]$-sottomodulo di V. Segue che $\hat{\rho}$ è una rappresentazione irriducibile se e solo se lo è anche ρ, ovvero $\hat{\chi}$ è un carattere irriducibile, se e solo se anche $f(\hat{\chi}) = \chi$ è irriducibile. □

Definizione. Dato un carattere $\hat{\chi}$ di G/N, allora il carattere χ di G tale che $\chi(g) = \chi(Ng)$ come definito nella dimostrazione del precedente teorema, è detto il *sollevamento* di $\hat{\chi}$.

Il teorema appena dimostrato, mostra che è possibile ricavare l'intera tavola dei caratteri di G/N da quella di G. Il viceversa non è del tutto vero, poiché dai caratteri irriducibili di G/N non è possibile ricavare tutti i caratteri irriducibili di G, bensì solo quelli che contengono N nel nucleo (e non completamente). In ogni caso siccome G/N ha ordine minore di G, la sua tavola dei caratteri in generale dovrebbe essere più semplice da scrivere, a questo punto da essa si possono trarre importanti informazioni sui caratteri irriducibili di G. Tale procedimento risulta utile nel caso di gruppi con ordine molto piccolo:

Esempio 3.32 (la tavola dei caratteri di S_4)**.** Il gruppo S_4 possiede un sottogruppo normale $K = \langle (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ detto sottogruppo di Klein, e dalla teoria dei gruppi è noto inoltre che $S_4/K \cong S_3$. La tavola dei caratteri di S_3 è ormai nota, dunque l'obiettivo è quello di ricavare da essa alcune informazioni riguardo la tavola ei caratteri di S_4. Con χ_1 si indica come al solito il carattere di S_4 associato alla rappresentazione banale, mentre con χ_2 si indica il carattere che manda A_4 in 1 e $G \setminus A_4$ in -1, dunque la situazione quella mostrata in figura 3.4, notando che S_4 possiede 5 classi di coniugio e dunque 5 caratteri irriducibili. Si indichi con $\hat{\chi}_3$ il terzo carattere di S_3, allora utilizzando il teorema 3.31, si pone χ_3 come sollevamento di $\hat{\chi}_3$. È facile verificare che l'elemento $K(1\,2)$ ha ordine 2 in S_4/K mentre $K(1\,2\,3)$ ha ordine 3 in S_4/K, quindi considerando l'isomorfismo tra S_3 e S_4/K, ovviamente $K(1\,2)$ è

	1	$[(1\,2)(3\,4)]$	$[(1\,2\,3)]$	$[(1\,2)]$	$[(1\,2\,3\,4)]$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	$?$	$?$	$?$	$?$	$?$
χ_4	$?$	$?$	$?$	$?$	$?$
χ_5	$?$	$?$	$?$	$?$	$?$

Tabella 3.4

l'immagine di una trasposizione mentre $K(1\,2\,3)$ è l'immagine di una rotazione. Per definizione di sollevamento si ha:

$$\chi_3(1) = \hat{\chi}_3(K) = 2, \quad \chi_3\big((1\,2\,3)\big) = \hat{\chi}_3\big(K(1\,2\,3)\big) = -1, \quad \chi_3\big((1\,2)\big) = \hat{\chi}_3\big(K(1\,2)\big) = 0$$

Inoltre $(1\,2)(3\,4) \in K$, quindi $\chi_3\big((1\,2)(3\,4)\big) = \chi_3(1) = 2$ e mediante un semplice conto si vede che $(1\,2\,3\,4) = (1\,2)(3\,4)(1\,3) \in K(1\,3)$, perciò:

$$\chi_3\big((1\,2\,3\,4)\big) = \hat{\chi}_3\big(K(1\,2\,3\,4)\big) = \hat{\chi}_3\big(K(1\ 3)\big) = \chi_3\big((1\,3)\big) = \chi_3\big((1\,2)\big) = 0$$

È stata composta la terza riga della tavola dei caratteri di S_4 con il sollevamento di $\hat{\chi}_3$, perciò restano da determinare le ultime due righe. Dall'equazione delle classi si ha che:

$$|S_4| = 24 = \sum_{i=1}^{5} \chi_i(1)^2 = 1 + 1 + 4 + \chi_4(1)^2 + \chi_5(1)^2$$

da cui segue che $\chi_4(1) = \chi_5(1) = 3$. La tavola dei caratteri, ancora parziale, si presenta dunque nel seguente modo aggiungendo sull'orlo in alto l'ordine delle classi di coniugio e dei centralizzanti:

	1	$[(1\,2)(3\,4)]$	$[(1\,2\,3)]$	$[(1\,2)]$	$[(1\,2\,3\,4)]$
$\lvert g^G\rvert$	1	3	8	6	6
$\lvert C_G(g)\rvert$	24	8	3	4	4
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	3	a_1	a_2	a_3	a_4
χ_5	3	b_1	b_2	b_3	b_4

Per trovare gli elementi rimanenti si fa largo uso delle relazioni di ortogonalità: Si consideri $g \in [(1\,2)(3\,4)]$, si applica la II relazione di ortogonalità:

$$8 = |C_G(g)| = \sum_{i=1}^{5} \chi_i(g)\overline{\chi_i(g)} = 1^2 + 1^2 + 2^2 + {a_1}^2 + {b_1}^2$$

da cui si ottiene ${a_1}^2 + {b_1}^2 = 2$. Sempre con lo scopo di trovare a_1 e b_1 si scelgano 1 e $g \in [(1\,2)(3\,4)]$ e si applichi ancora una volta la II relazione di ortogonalità:

$$0 = \sum_{i=1}^{5} \chi_i(1)\overline{\chi_i(g)} = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 + 3a_1 + 3b_1 = 6 + 3a_1 + 3b_1$$

In sostanza si ottiene il seguente sistema di due equazioni e due incognite:

$$\begin{cases} {a_1}^2 + {b_1}^2 = 2 \\ 3a_1 + 3b_1 + 6 = 0 \end{cases}$$

che ha come soluzione $a_1 = b_1 = -1$. Sia ora $g \in [(1\,2\,3)]$ e si allora procedendo come prima si ha:

$$3 = |C_G(g)| = \sum_{i=1}^{5} \chi_i(g)\overline{\chi_i(g)} = 1^2 + 1^2 + (-1)^2 + {a_2}^2 + {b_2}^2$$

ovvero ${a_2}^2 + {b_2}^2 = 0$. Considerando inoltre 1 e $g \in [(1\,2\,3)]$ vale che:

$$0 = \sum_{i=1}^{5} \chi_i(1)\overline{\chi_i(g)} = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot (-1) + 3a_2 + 3b_2 = 3a_2 + 3b_2$$

Il sistema in questo caso è

$$\begin{cases} {a_2}^2 + {b_2}^2 = 0 \\ 3a_2 + 3b_2 = 0 \end{cases}$$

che ha soluzione $a_2 = b_2 = 0$. Si procede nello stesso modo considerando $g \in [(1\,2)]$ e 1:

$$4 = |C_G(g)| = \sum_{i=1}^{5} \chi_i(g)\overline{\chi_i(g)} = 1^2 + (-1)^2 + 0^2 + {a_3}^2 + {b_3}^2$$

$$0 = \sum_{i=1}^{5} \chi_i(1)\overline{\chi_i(g)} = 1 \cdot 1 + 1 \cdot (-1) + 2 \cdot 0 + 3a_3 + 3b_3 = 3a_3 + 3b_3$$

e quindi il sistema

$$\begin{cases} {a_3}^2 + {b_3}^2 = 2 \\ 3a_3 + 3b_3 = 0 \end{cases}$$

Questa volta ci sono due soluzioni: $a_3 = 1 \vee b_3 = -1$ e $a_3 = -1 \vee b_3 = -1$. Guardando attentamente la tavola dei caratteri ancora parziale si vede che si otterrebbe lo stesso risultato per a_4 e b_4 se procedessimo allo stesso modo. Si può porre dunque $a_3 = 1$, $b_3 = -1$, $a_4 = -1$ e $b_4 = 1$, poiché scambiando i valori di a_3 e a_4 e di b_3 e b_4 si avrebbe semplicemente una permutazione tra i caratteri χ_4 e χ_5. Inoltre non può essere $a_3 = a_4$ e $b_3 = b_4$ poiché altrimenti sarebbe. La tavola dei caratteri di S_4 è finalmente completa (figura 3.5).

	1	$[(1\,2)(3\,4)]$	$[(1\,2\,3)]$	$[(1\,2)]$	$[(1\,2\,3\,4)]$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	3	-1	0	1	-1
χ_5	3	-1	0	-1	1

Tabella 3.5. Tavola dei caratteri di S_4

È possibile ora dimostrare il teorema che permette di tovare tutti i sottogruppi normali di un gruppo esclusivamente dalla tavola dei caratteri.

Teorema 3.33. *Sia G un gruppo finito con k classi di coniugio ed $N \leq G$; N è un sottogruppo normale di G se e solo se esistono s $(\leq k)$ caratteri irriducibili*[2] *di G, tali per cui*

$$N = \bigcap_{i=1}^{s} Ker(\chi_i)$$

Dimostrazione. ($\Leftarrow$) Per il lemma 3.29, $\forall i \in \{1, \ldots, s\}$, tutti i nuclei $Ker(\chi_i)$ sono sottogruppi normali di G, dunque la loro intersezione N è un sottogruppo normale di G.
($\Rightarrow$) Sia $N \trianglelefteq G$. Si consideri $g \in G$ tale che g appartiene al nucleo di tutti i caratteri irriducibili di G, ciò significa che $\chi_i(g) = \chi_i(1)\ \ \forall i \in \{1, \ldots, k\}$, quindi per il corollario 3.19 si ha che g è coniugato a 1, ovvero $g = 1$. È stato provato che:

$$\bigcap_{i=1}^{k} Ker(\chi_i) = \{1\}$$

dunque se $\hat{\chi}_1, \hat{\chi}_2, \ldots, \hat{\chi}_s$ sono i caratteri irriducibili di G/N (si noti che per il teorema 3.31 $|Irr(G/N)| \leq |Irr(G)|$), allora:

$$\bigcap_{i=1}^{s} Ker(\hat{\chi}_i) = \{N\}$$

Siano $\chi_1, \chi_2, \ldots, \chi_s$ i sollevamenti dei caratteri irriducibili di G/N; per il teorema 3.31 essi sono irriducibili e inoltre i loro nuclei contengono N, perciò:

$$N \subseteq \bigcap_{i=1}^{s} Ker(\chi_i)$$

Viceversa sia $g \in Ker(\chi_i)\ \ \forall i \in \{1, \ldots, s\}$, allora per ogni carattere irriducibile di G/N si ha che $\hat{\chi}_i(N) = \chi_i(1) = \chi_i(g) = \hat{\chi}_i(Ng)$, ovvero per quanto detto in precedenza:

$$Ng \in \bigcap_{i=1}^{s} Ker(\hat{\chi}_i) = \{N\}$$

da cui segue che $g \in N$ e dunque

$$\bigcap_{i=1}^{s} Ker(\chi_i) \subseteq N$$

□

[2] Dati i k caratteri irriducibili di G non è detto che gli s caratteri di cui parla il teorema siano proprio $\chi_1, \chi_2, \ldots, \chi_s$ scritti nell'usuale ordine in base al grado, però nulla vieta di riorganizzare gli indici in modo tale che essi lo siano. In generale l'ordine con cui vengono elencati i caratteri non è importante.

3.8 Semplicità, risolubilità e nilpotenza

Dalla tavola dei caratteri di un gruppo finito G possono essere ricavate altre importanti informazioni sulla struttura di G stesso. Con quanto visto riguardo i sottogruppi normali di G sarà facile trattare la semplicità e la risolubilità mentre prima di parlare di nilpotenza bisognerà introdurre qualche concetto nuovo. In questa sezione viene data per scontata la conoscenza di una buona parte della teoria dei gruppi finiti.

Teorema 3.34. *Un gruppo finito G con k classi di coniugio è semplice se e solo se, indicando con χ_1 il carattere banale, si ha che $Ker(\chi_i) = \{1\}\ \forall i \in \{2, \dots, k\}$*

Dimostrazione. ($\Leftarrow$) Sia $Ker(\chi_i) = \{1\}\ \forall i \in \{2, \dots, k\}$ allora per quanto visto nel teorema 3.33, ogni sottogruppo normale è intersezione di nuclei di caratteri irriducibili, ma con le ipotesi fatte tale intersezione può essere $\{1\}$ oppure G, perciò segue perciò che il gruppo è semplice.
($\Rightarrow$) Viceversa se G è semplice, sempre per il teorema 3.33 si ha che tutte le possibili intersezioni di nuclei di caratteri irriducibili possono essere G oppure $\{1\}$. siccome $Ker(\chi_1) = G$ e i caratteri irriducibili sono tutti distinti, segue che $Ker(\chi_i) = \{1\}\ \forall i \in \{2, \dots, k\}$. □

Accanto alla definizione standard di gruppo risolubile che utilizza le serie subnormali di un certo gruppo finito ce n'è un'altra che coinvolge invece le serie normali:

Lemma 3.35. *Un gruppo finito G è risolubile se e solo se esiste una serie*

$$N_0 = \{1\} < N_1 < N_2 < \ldots < N_{t-1} < G = N_t$$

tale che $\forall i \in \{1, \dots, t\}$ si abbia:

- $N_i \lhd G$
- $|N_{i+1} : N_i| = p^r$ *per un certo p primo ed $r \in \mathbb{N}$*

Per la dimostrazione si rimanda ad un testo di teoria dei gruppi finiti.

Come ampiamente visto, dalla tavola dei caratteri di G è possibile risalire a tutti i sottogruppi normali di G e ai relativi ordini, perciò risulta molto agevole verificare l'esistenza di una serie normale descritta dal precedente lemma. Il problema di decidere se un gruppo è risolubile o meno si riconduce dunque a quello di analizzare a fondo i nuclei dei caratteri irriducibili di G e cercare di costruire con le loro intersezioni una serie da G ad $\{1\}$ con determinate proprietà. Prima di trattare il problema di decidere se un gruppo è nilpotente o meno in base alla sua tavole dei caratteri, bisogna introdurre qualche nuovo concetto:

Definizione. Sia G un gruppo finito e χ un suo carattere, allora l'insieme

$$Z(\chi) = \{g \in G : |\chi(g)| = \chi(1)\}$$

è detto *centro* di χ. Si vede subito che $Ker(\chi) \subseteq Z(\chi)$.

Lemma 3.36. *Sia ρ una rappresentazione irriducibile di $\mathbb{C}[G]$ su V allora si ha che $C_{End_{\mathbb{C}}(V)}(G\rho) = \Lambda$.*

Dimostrazione. Ovviamente $\Lambda = Z(End_{\mathbb{C}}(V)) \subseteq C_{End_{\mathbb{C}}(V)}(G\rho)$. Viceversa sia $\varphi \in C_{End_{\mathbb{C}}(V)}(G\rho)$, allora $v(g\rho)\varphi = (v\varphi)(g\rho)$ per ogni $v \in V$, e passando alle azioni ciò vuol dire che $(v^g)\varphi = (v\varphi)^g$. Ciò significa che $\varphi \in End_{\mathbb{C}[G]}(V)$, ma siccome sono verificate a pieno le ipotesi del corollario del lemma di Schur, vale che $End_{\mathbb{C}[G]}(V) = \Lambda$. □

Lemma 3.37. *Sia χ un carattere di un gruppo finito G associato ad una certa rappresentazione ρ, allora valgono le seguenti proposizioni:*

i) $Z(\chi) = \{g \in G : g\rho \in \Lambda\}$

ii) $Z(\chi)$ *è un sottogruppo di* G

iii) $Z(\chi)/Ker(\chi) \subseteq Z(G/Ker(\chi))$

iv) Se χ *è irriducibile allora* $Z(\chi)/Ker(\chi) = Z(G/Ker(\chi))$

Dimostrazione. *i)* È noto che $\chi(g) = \sum_{i=1}^{d} \lambda_i$ dove d è la dimensione di V e i λ_i sono radici n-esime del'unità per $n = o(g)$. Esiste inoltre una base $\mathcal{B}$ tale per cui

$$[g\rho]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & 0 \\ & & \ddots & \\ 0 & & & \lambda_d \end{pmatrix}$$

Allora $\chi(1) = \sum_{i=1}^{d} |\lambda_i| = \left|\sum_{i=1}^{d} \lambda_i\right| = |\chi(g)|$ se e solo se i λ_i sono tutti uguali (ma non necessariamente reali), ovvero se $[g\rho]_{\mathcal{B}} = \lambda I$. A questo punto la tesi segue notando semplicemente che l'unica matrice simile a λI è essa stessa.
ii) Siano $g, h \in Z(\chi)$, allora per il punto precedente esistono due numeri complessi α e β tali che $g\rho = \alpha I$ e $h\rho = \beta I$. Dunque

$$(gh)\rho = (g\rho)(h\rho) = \alpha I \cdot \beta I = (\alpha\beta)I \in \Lambda$$

$$(g^{-1})\rho = (g\rho)^{-1} = \frac{1}{\alpha} I \in \Lambda$$

Utilizzando ancora una volta il punto *i)* si conclude che $Z(\chi)$ è un gruppo.
iii) dal punto *i)* segue che $Z(\chi)\rho = \Lambda$ e inoltre ovviamente $\Lambda \subseteq Z(G\rho)$. In sostanza è stato stabilito che $Z(\chi)\rho \subseteq Z(G\rho)$, ma per il primo teorema di omomorfismo fra gruppi $Z(\chi)\rho \cong Z(\chi)/Ker(\rho)$ e $G\rho \cong G/Ker(\rho)$, dunque $Z(\chi)/Ker(\rho) \subseteq Z(G/Ker(\rho))$. Infine ricordando che $Ker(\rho) = Ker(\chi)$ si ha la tesi.
iv) Si noti che $Z(G\rho) \subseteq C_{End_{\mathbb{C}}(V)}(G\rho)$, ma per ipotesi ρ è irriducibile dunque vale il lemma 3.36, perciò $Z(G\rho) \subseteq \Lambda$. Unendo tale risultato a quanto visto in precedenza si evince che $Z(\chi)\rho = Z(G\rho)$, dunque riproponendo lo stesso ragionamento fatto per il punto *iii)* (questa volta con il simbolo di uguaglianza) si conclude che $Z(\chi)/Ker(\chi) = Z(G/Ker(\chi))$. □

È possibile ora vedere la relazione che intercorre fra il centro di un gruppo è il centro dei suoi caratteri irriducibili:

Teorema 3.38. *Sia G un gruppo finito con k classi di coniugio, allora*

$$Z(G) = \bigcap_{i=1}^{k} Z(\chi_i)$$

Dimostrazione. Si prova dapprima che $Z(G) \subseteq Z(\chi_j)$ per ogni carattere irriducibile χ_j. Si considerino due generici elementi $z(Ker(\chi_j)) \in Z(G)/ker(\chi_j)$ e $g(Ker(\chi_j)) \in G/Ker(\chi)$, allora

$$z(Ker(\chi_j))g(Ker(\chi_j)) = zg(Ker(\chi_j)) = gz(Ker(\chi_j)) = g(Ker(\chi_j))z(Ker(\chi_j))$$

ovvero $Z(G)/ker(\chi_j) \subseteq Z(G/Ker(\chi))$. Per il punto iv) del lemma 3.37 si ha dunque che $Z(G)/ker(\chi_j) \subseteq Z(\chi_j)/ker(\chi_j)$ e perciò passando alle controimmagini della proiezione canonica si ottiene $Z(G) \subseteq Z(\chi_j)$. Viceversa sia $g \in Z(\chi_j)$ per ogni $j \in \{1, \ldots, k\}$, allora ancora una volta per l punto iv) del lemma 3.37 vale che $g(Ker(\chi_j)) \in Z(G/Ker(\chi_j))$. Per ogni $x \in G$ si consideri ora il commutatore $[g, x] = g^{-1}x^{-1}gx$, allora indicando con ρ_j la rappresentazione relativa al carattere χ_j, per certi $h_1, h_2 \in ker(\chi_j)$ si ha

$$([g, x])\rho_j = (g^{-1}x^{-1}gx)\rho_j = (g^{-1}x^{-1}(gh_1)(xh_2))\rho_j$$

Per le ipotesi fatte su g gli elementi (gh_1) e (xh_2) commutano, dunque:

$$([g, x])\rho_j = (g^{-1}x^{-1}(xh_2)(gh_1))\rho_j = I$$

ovvero $[g, x] \in Ker(\chi_j)$. Data l'arbitrarietà di j si conclude che

$$[g, x] \in \bigcap_{i=1}^{k} Ker(\chi_i) = \{1\}$$

ovvero g commuta con ogni elemento x di G. □

Dalla tavola dei caratteri è dunque molto semplice trovare il centro di un gruppo G. Una volta trovato $Z(G)$ si costruisce la tavola dei caratteri di $G/Z(G)$ e si individua il centro di $G/Z(G)$ e così via. Mediante tale procedura è possibile (ma non immediato) costruire la serie centrale ascendente, e dunque se essa raggiunge G si può concludere che G è nilpotente.
Ovviamente tutti i processi mostrati in questa sezione sono improponibili se l'ordine del gruppo è elevato, ma dal punto di vista teorico è stato mostrato che molte informazioni sui gruppi finiti sono contenute esclusivamente nei caratteri irriducibili.

Capitolo 4

Il teorema $p^\alpha q^\beta$ di Burnside

Per quanto fatto fino ad ora, sembrerebbe che la teoria della rappresentazione non dia un grande contributo alla teoria dei gruppi. Dalla tavola dei caratteri sono state ricavate alcune informazioni utili riguardo struttura di un gruppo, ma non è stato aggiunto nulla di nuovo, poiché tali informazioni possono essere trovate senza l'utilizzo dei caratteri. La più nota applicazione della teoria della rappresentazione, è la dimostrazione del teorema $p^\alpha q^\beta$ di Burnside, che dice che tutti i gruppi con ordine divisibile per esattamente due primi, sono risolubili. La dimostrazione originale di Burnside faceva largo uso dei caratteri, ed essa è stata l'unica dimostrazione nota fino al 1970, anno in cui Goldschmidt provò il suddetto teorema senza utilizzare la teoria dei caratteri. In questo capitolo verrà presentata la dimostrazione "classica" data da Burnside.

4.1 Interi algebrici

Prima di presentare la dimostrazione del teorema, bisogna esaminare a fondo il legame che intercorre fra i caratteri e gli interi algebrici.

Definizione. Un *intero algebrico* è un numero complesso α che è radice di un polinomio monico $p(x) \in \mathbb{Z}[x]$.

Esiste una caratterizzazione diversa per gli interi algebrici che risulterà utile nel seguito:

Lemma 4.1. *$\alpha \in \mathbb{C}$ è un intero algebrico se e solo se è un autovalore di una matrice quadrata a coefficienti in $\mathbb{Z}$.*

Dimostrazione. ($\Leftarrow$) Sia α un autovalore di $A \in \mathcal{M}(n, \mathbb{Z})$, allora α è radice del polinomio $p(x) = det(xI - A)$ che è il polinomio caratteristico di A. Per quanto noto dall'algebra lineare, $p(x)$ è monico di grado n, e inoltre siccome A è a coefficienti in Z, allora $p(x) \in \mathbb{Z}[x]$.
($\Rightarrow$) Sia α radice del polinomio $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, allora sempre dall'algebra lineare, segue che α è autovalore della matrice C_p

compagna (companion matrix) di $p(x)$:

$$C_p = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & 0 \\ 0 & & \ddots & \ddots & \\ & & & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}$$

□

È interessante cercare di capire dove sono "posizionati" gli interi algebrici su $\mathbb{C}$, e a tal proposito il seguente lemma prova che non esistono interi algebrici in $\mathbb{Q} \setminus \mathbb{Z}$:

Lemma 4.2. *L'insieme degli interi algebrici razionali coincide con $\mathbb{Z}$.*

Dimostrazione. Sia $\alpha \in \mathbb{Z}$, allora esso è radice del polinomio $x - \alpha$ da cui segue che α è un intero algebrico (razionale). Viceversa sia $\frac{r}{s}$ un intero algebrico razionale con $(r, s) = 1$, esiste dunque un polinomio $p(x) \in \mathbb{Z}[x]$ monico di grado n tale per cui:

$$p\Big(\frac{r}{s}\Big) = \frac{r^n}{s^n} + a_{n-1}\frac{r^{n-1}}{s^{n-1}} + \ldots + a_1\frac{r}{s} + a_0 = 0$$

moltiplicando tutto per s^n ed esplicitando rispetto r^n si ottiene

$$r^n = s(-a_{n-1}r^{n-1} - \ldots - a_1 r s^{n-2} - a_0 s^{n-1})$$

ovvero $s \big| r^n$. Dal momento che $(r, s) = 1$, si può scrivere $\lambda r + \mu s = 1$ per certi $\lambda, \mu \in \mathbb{Z}$. Sia $k_0 \in \mathbb{Z}$ tale che $r^n = sk_0$, e si definisca per ricorsione il numero

$$k_i = \lambda k_{i-1} + \mu r^{n-i} \quad \forall i \in \{1, \ldots, n\}$$

Si dimostra per induzione su i che $r^{n-i} = sk_i$.
Per $i = 0$ si ha la base dell'induzione; si supponga vera la relazione per l'indice $i - 1$, allora:

$$sk_i = \lambda s k_{i-1} + \mu s r^{n-i} = \lambda r^{n-i+1} + \mu s r^{n-i} = r^{n-i}(\lambda r + \mu s) = r^{n-i}$$

Ponendo $i = n - 1$ si ha $r = sk_{n-1}$, ovvero $s \big| r$ da cui $s = \pm 1$, visto che $(r, s) = 1$.
Si conclude dunque che in realtà $\frac{r}{s} \in \mathbb{Z}$. □

Una caratteristica importantissima degli interi algebrici, per niente ovvia dalla definizione, è che essi formano un anello. Tale proprietà verrà dimostrata premettendo due lemmi tecnici:

Lemma 4.3. *Sia $X = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ un insieme finito di interi algebrici, allora esiste un anello S, con $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, finitamente generato come $\mathbb{Z}$-modulo*[1] *e tale che $X \subseteq S$.*

[1] Essere finitamente generato come $\mathbb{Z}$-modulo significa che esiste un insieme finito $Y \subseteq S$ tale che, ogni elemento di S si scrive come combinazione lineare a coefficienti in $\mathbb{Z}$ di elementi di Y.

Dimostrazione. Dalla definizione di intero algebrico si ha che $\alpha_i^{n_i} = f_i(\alpha_i)$ dove f_i è un polinomio di grado $n_i - 1 \ \forall i \in \{1, \dots, k\}$. Si costruisca dunque l'insieme finito

$$Y = \left\{ \prod_{i=1}^{n} \alpha_i^{r_i} \ : \ 0 \leq r_i \leq n_i - 1, \ \forall i = 1, 2, \dots, k \right\}$$

e sia S l'insieme di tutte le combinazioni lineari degli elementi di Y a coefficienti in $\mathbb{Z}$. Si dimostra innanzitutto che S è un sottoanello di $\mathbb{C}$: sia $\ell = |Y|$ e $y_j \in Y \ \forall j \in \{1, \dots, \ell\}$, allora riguardo la somma è facile verificare la chiusura e l'esistenza dell'inverso, infatti considerando $\lambda_j, \mu_j \in \mathbb{Z}$ si ha

$$\sum_{j=i}^{\ell} \lambda_j y_j + \sum_{j=i}^{\ell} \mu_j y_j = \sum_{j=1}^{\ell} (\lambda_j + \mu_j) y_j \in S$$

$$\sum_{j=1}^{\ell} -\lambda_j y_j \in S$$

Resta da verificare la chiusura rispetto al prodotto, ovvero basta mostrare che $\alpha_i^m \in S \ \forall m \in \mathbb{Z}$ e $\forall i \in \{1, \dots, k\}$. Se $m < n_i$ è tutto ovvio, dunque si pone $m = n_i + t$ con $t \geq 0$ e si procede per induzione su t. Se $t = 0$, allora $m = n_i$ ma $a_i^{n_i} = f_i(a_i) \in S$; si supponga ora che la tesi sia vera per $m < n_i + t$, allora

$$\alpha_i^{n_i + t} = \alpha_i^{n_i} \alpha_i^t = \alpha_i^t f_i(\alpha_i)$$

ma $deg\big(\alpha_i^t f_i(\alpha_i)\big) < n_i + t$, dunque per l'ipotesi induttiva $\alpha_i^{n_i+t} \in S$. Si conclude che S è un anello tale che $X \subseteq S$; inoltre $1 = \alpha_1^0 \alpha_2^0 \dots \alpha_k^0 \in S$, dunque $\mathbb{Z} \subseteq S$. □

Lemma 4.4. *Sia S un anello tale che $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$. Se S è finitamente generato come $\mathbb{Z}$-modulo, allora ogni $s \in S$ è un intero algebrico.*

Dimostrazione. Siccome S è finitamente generato come $\mathbb{Z}$-modulo, esiste un insieme finito $Y = \{y_1, y_2, \dots, y_\ell\} \subseteq S$ tale per cui per ogni elemento di S si scrive come combinazione lineare a coefficienti in $\mathbb{Z}$ degli elementi di Y. Sia $s \in S$, in particolare si ha che $sy_i \in S \ \forall i \in \{1, \dots, \ell\}$, quindi

$$sy_i = \sum_{j=1}^{\ell} a_{ij} y_j \quad \text{con } a_{ij} \in \mathbb{Z}$$

Si consideri ora la matrice $A = (a_{ij})_{i,j}$ e sia $v = (y_1, \dots, y_\ell)^t \in \mathbb{C}^n$; per come è definito il prodotto riga per colonna si ha che

$$Av = \begin{pmatrix} \sum_{j=1}^{\ell} a_{1j} y_j \\ \vdots \\ \sum_{j=1}^{\ell} a_{\ell j} y_j \end{pmatrix} = \begin{pmatrix} sy_1 \\ \vdots \\ sy_\ell \end{pmatrix} = sv$$

In pratica s è un autovalore della matrice A a coefficienti in $\mathbb{Z}$, dunque per il lemma 4.1 è un intero algebrico. □

È ora possibile dimostrare il seguente teorema:

Teorema 4.5. *L'insieme degli interi algebrici è un sottoanello unitario di* $\mathbb{C}$.

Dimostrazione. Chiaramente $1 \in \mathbb{Z}$ è un intero algebrico. Siano α e β due interi algebrici, allora per il lemma 4.3, esiste un anello S tale che $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, finitamente generato come $\mathbb{Z}$-modulo che contiene α e β. Segue che $-\alpha \in S$, $\alpha + \beta \in S$ e $\alpha\beta \in S$; dunque per il lemma 4.4 gli elementi $-\alpha$, $\alpha + \beta$ e $\alpha\beta$ sono interi algebrici. Sono verificate così tutte le proprietà che caratterizzano un sottoanello. □

Un importante corollario del teorema precedente mostra il legame strettissimo che intercorre tra i caratteri e gli interi algebrici.

Corollario 4.6. *Sia* χ *un carattere di un gruppo finito* G*, allora* $\chi(g)$ *è un intero algebrico* $\forall g \in G$.

Dimostrazione. Sia $o(g) = n$, allora per il lemma 3.14 *i)* $\chi(g)$ è somma di radici n-esime dell'unità, ovvero è somma di radici del polinomio $x^n - 1$. In pratica $\chi(g)$ è somma di interi algebrici, e dunque per il teorema precedente è un intero algebrico. □

Tale corollario, da un lato è utile per la dimostrazione del teorema $p^\alpha q^\beta$ di Burnside, dall'altro fornisce ulteriori informazioni sulla tavola dei caratteri di un gruppo. Ad esempio per via del lemma 4.2 segue che la tavola dei caratteri non può contenere elementi dell'insieme $\mathbb{Q} \setminus \mathbb{Z}$.

4.2 La dimostrazione del teorema

In questa sezione verrà data una dimostrazione del teorema $p^\alpha q^\beta$ di Burnside dopo aver provato alcuni lemmi:

Lemma 4.7. *Sia* ρ *una rappresentazione irriducibile di* $\mathbb{C}[G]$ *su* V*, allora* $(Z(\mathbb{C}[G]))\rho \subseteq Z(End_{\mathbb{C}}(V))$.

Dimostrazione. Per quanto visto nella dimostrazione del teorema di Wedderburn-Artin, si ha che ρ è una funzione suriettiva. Si considerino $z \in Z(\mathbb{C}[G])$ e $\varphi \in End_{\mathbb{C}}(V)$; esiste allora $x \in \mathbb{C}[G]$ tale che $x\rho = \varphi$ e dunque $\forall v \in V$ si ha che

$$v(z\rho)\varphi = v(z\rho)(x\rho) = v((zx)\rho) = v((xz)\rho) = v(x\rho)(z\rho) = v\varphi(z\rho)$$

Segue che $z\rho \in Z(End_{\mathbb{C}}(V))$, ovvero la tesi. □

Una conseguenza del lemma precedente e del lemma 3.37, è che nel caso di una rappresentazione irriducibile ρ di $\mathbb{C}[G]$, $\forall z \in Z(\mathbb{C}[G])$, la funzione $z\rho$ è in realtà una moltiplicazione per uno scalare, ovvero $z\rho = cI$ con $c \in \mathbb{C}$. Siccome l'unica matrice simile a cI è se stessa, segue che lo scalare c oltre a dipendere dall'elemento z, dipende dal carattere $\chi \in Irr(G)$ associato a ρ. Si noti che se cI avesse matrici simili diverse da se stessa, il numero c dipenderebbe dalla scelta della rappresentazione e non dal carattere associato. Si definisca quindi una funzione $\omega_\chi : Z(\mathbb{C}[G]) \to \mathbb{C}$ dove il numero complesso $\omega_\chi(z)$ è tale che $z\rho = \omega_\chi(z)I$. È facile provare che ω_χ è un omomorfismo di algebre:

$$\omega_\chi(z + y)I = (z + y)\rho = z\rho + y\rho = (\omega_\chi(z) + \omega_\chi(y))I$$

$$\omega_\chi(\lambda z)I = (\lambda z)\rho = \lambda(z\rho) = \lambda\omega_\chi(z)I$$
$$\omega_\chi(zy)I = (zy)\rho = (z\rho)(y\rho) = \omega_\chi(z)\omega_\chi(y)I$$

In particolare è possibile ricavare il valore della funzione ω_χ su ogni elemento del suo dominio, conoscendo esclusivamente il comportamento su una base di $Z(\mathbb{C}[G])$. Sia G un gruppo con k classi di coniugio $\mathcal{C}_1, \dots \mathcal{C}_k$, nel capitolo 3 si è visto che l'insieme

$$\mathcal{B} = \left\{ z_i = \sum_{g \in \mathcal{C}_i} g \ : \ i \in \{1, \dots, k\} \right\}$$

è una base per $Z(\mathbb{C}[G])$. Non resta che calcolare il valore di $\omega_\chi(z_i)$, e per farlo basta scrivere in due modi diversi $\chi(z_i)$:

$$\chi(z_i) = tr(z_i\rho) = tr\big(\omega_\chi(z_i)I\big) = \chi(1)\omega_\chi(z_i)$$

$$\chi(z_i) = \chi\left(\sum_{g \in \mathcal{C}_i} g\right) = \sum_{g \in \mathcal{C}_i} \chi(g) = |\mathcal{C}_i|\chi(g)$$

segue dunque che

$$\omega_\chi(z_i) = |\mathcal{C}_i|\frac{\chi(g)}{\chi(1)} \quad \text{con } g \in \mathcal{C}_i \tag{4.1}$$

In sostanza il valore della funzione ω_χ può essere trovato facilmente dalla tavola dei caratteri di G.

Lemma 4.8. *Sia G un gruppo finito con k classi di coniugio e siano $z_i, z_j \in \mathcal{B}$ (base di $Z(\mathbb{C}[G])$). Allora il prodotto*

$$z_i z_j = \sum_{t=1}^{k} a_{ijt} z_t$$

è tale che $a_{ijt} \in \mathbb{N} \ \forall t \in \{1, \dots, k\}$.

Dimostrazione. Per come è definito il prodotto nell'algebra gruppale $\mathbb{C}[G]$, si ha

$$z_i z_j = \sum_{g \in G}^{k} a_{ijg} g$$

ma chiaramente per costruzione degli z_t, gli elementi di G appartenenti alla stessa classe di coniugio hanno lo stesso coefficiente moltiplicativo, ovvero se $g \in \mathcal{C}_t$ allora $a_{ijg} = a_{ijt}$. È facile ora identificare tali coefficienti, infatti

$$a_{ijg} = \left| \left\{ \{x, y\} \ : \ x \in C_i, \, y \in C_j, \, xy = g \right\} \right|$$

ed essendo la cardinalità di un insieme finito $a_{ijg} = a_{ijt} \in \mathbb{N}$. □

Lemma 4.9. *Sia G un gruppo finito con k classi di coniugio e $\chi \in Irr(G)$, allora $\omega_\chi(z_i)$ è un intero algebrico $\forall i \in \{1, \dots, k\}$.*

Dimostrazione. Si consideri l'insieme finito

$$Y = \{\omega_\chi(z_1), \omega_\chi(z_2), \dots, \omega_\chi(z_k)\}$$

e si costruisca l'insieme S di tutte le combinazioni lineari di elementi di Y a coefficienti in $\mathbb{Z}$. Chiaramente S è un gruppo abeliano rispetto alla somma eper il lemma 4.8, $\forall i, j \in \{1, \dots, k\}$ vale che

$$\omega_\chi(z_i)\omega_\chi(z_j) = \omega_\chi(z_i z_j) = \omega_\chi\left(\sum_{t=1}^{k} a_{ijt} z_t\right) = \sum_{t=1}^{k} a_{ijt}\omega_\chi(z_t) \in S$$

da cui segue che S è un anello. Inoltre per definizione $1 \in \{z_1, \dots, z_k\}$, quindi $\omega_\chi(1) = 1 \in S$, ovvero $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$. Dal lemma 4.4 segue che ogni elemento di S è un intero algebrico e in particolare ogni elemento di Y è un intero algebrico. □

Prima di proseguire è importante dimostrare un utile teorema che lega il grado dei caratteri irriducibili all'ordine del gruppo:

Teorema 4.10. *Sia G un gruppo finito con k classi di coniugio; se $\chi \in Irr(G)$ allora $\chi(1)$ divide $|G|$.*

Dimostrazione. Dalla prima relazione di ortogonalità si ha che:

$$|G| = \sum_{g \in G} \chi(g)\overline{\chi(g)} = \sum_{i=1}^{k} |C_i|\chi(g_i)\overline{\chi(g_i)} = \sum_{i=1}^{k} \chi(1)\omega_\chi(z_i)\overline{\chi(g_i)}$$

Ma allora

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{k} \omega_\chi(z_i)\overline{\chi(g_i)}$$

quindi $\frac{|G|}{\chi(1)}$ è un intero algebrico razionale e come tale deve stare in $\mathbb{Z}$. □

In generale il quoziente di due interi algebrici non è un intero algebrico, però in alcuni casi particolari ciò può essere vero:

Lemma 4.11. *Sia G un gruppo finito con k classi di coniugio $\mathcal{C}_1, \dots, \mathcal{C}_k$ e sia inoltre $\chi \in Irr(G)$. Se $\chi(1)$ è coprimo con $|\mathcal{C}_i|$, dove $i \in \{1, \dots, k\}$, allora il numero complesso $\frac{\chi(g)}{\chi(1)}$ con $g \in \mathcal{C}_i$, è un intero algebrico.*

Dimostrazione. Dal momento che $\Big(\chi(1), |\mathcal{C}_i|\Big) = 1$, esistono certi $a, b \in \mathbb{Z}$ tali per cui $a\chi(1) + b|\mathcal{C}_i| = 1$. Si può riscrivere $b|\mathcal{C}_i| = 1 - a\chi(1)$, e quindi dall'equazione 4.1 si ha che:

$$b\omega_\chi(z_i) = b|\mathcal{C}_i|\frac{\chi(g)}{\chi(1)} = \Big(1 - a\chi(1)\Big)\frac{\chi(g)}{\chi(1)} = \frac{\chi(g)}{\chi(1)} - a\chi(g)$$

Siccome $b\omega_\chi(z_i)$ è un intero algebrico e $a\chi(g)$ è un intero algebrico, segue che

$$\frac{\chi(g)}{\chi(1)} = b\omega_\chi(z_i) + a\chi(g)$$

è anch'esso un intero algebrico. □

Per la dimostrazione del seguente lemma dovuto a Burnside si utilizzano alcuni fatti di base della teoria di Galois:

Lemma 4.12. *(di Burnside) Sia G un gruppo finito con k classi di coniugio $\mathcal{C}_1, \ldots, \mathcal{C}_k$ e sia inoltre $\chi \in Irr(G)$. Se $\chi(1)$ è coprimo con $|\mathcal{C}_i|$ e $g \in \mathcal{C}_i$, dove $i \in \{1, \ldots, k\}$, allora $g \in Z(\chi)$ oppure $\chi(g) = 0$.*

Dimostrazione. Sia $\alpha = \frac{\chi(g)}{\chi(1)}$, allora per il lemma precedente α è un intero algebrico. Si supponga che $g \notin Z(G)$, allora $|\chi(g)| < \chi(1)$ e dunque vale che $|\alpha| = \frac{|\chi(g)|}{\chi(1)} < 1$. Si ponga $n = o(g)$ e sia K il campo di spezzamento del polinomio $x^n - 1$ su $\mathbb{Q}$, dal momento che $\chi(g)$ è somma di $\chi(1)$ radici n-esime dell'unità e $\chi(1) \in \mathbb{N}$ si ha che $\alpha \in K$. È noto che ogni elemento σ del gruppo di Galois $Gal(K/\mathbb{Q})$ permuta le radici dei polinomi a coefficienti in $\mathbb{Q}$, dunque $\alpha\sigma$ è un intero algebrico. Ovviamente $\chi(g)\sigma \in K$, ed è anch'esso somma di $\chi(1)$ radici n-esime dell'unità denotate con ξ_i $(i \in \{1, \ldots, \chi(1)\})$, da cui

$$|\chi(g)\sigma| = \left| \sum_{i=1}^{\chi(1)} \xi_i \right| \leq \sum_{i=1}^{\chi(1)} |\xi_i| = \chi(1)$$

ovvero $\alpha\sigma = \frac{\chi(g)\sigma}{\chi(1)}$ è tale che $|\alpha\sigma| \leq 1$. Si consideri l'intero algebrico

$$\beta = \prod_{\sigma \in Gal(K/\mathbb{Q})} \alpha\sigma$$

è ovvio che $|\beta| < 1$; notare non si è scritto il minore uguale poiché per ipotesi $|(\alpha)id| = |\alpha| < 1$. Sia ancora $\tau \in Gal(K/\mathbb{Q})$, allora vale che

$$\beta\tau = \prod_{\sigma \in Gal(K/\mathbb{Q})} \alpha(\sigma\tau) = \prod_{\sigma\tau \in Gal(K/\mathbb{Q})} \alpha(\sigma\tau) = \beta$$

ovvero $\beta \in \mathcal{F}\big(Gal(K/\mathbb{Q})\big) =^{2} \mathbb{Q}$. Per il lemma 4.2 si ha che $\beta \in \mathbb{Z}$, quindi dal momento che $|\beta| < 1$ si può concludere che $\beta = 0$. In sostanza esiste un certo $\sigma \in Gal(K/\mathbb{Q})$ tale per cui $\alpha\sigma = 0$, ma siccome gli elementi del gruppo di Galois sono funzioni lineari e iniettive si ha $\alpha = 0$. A questo punto si ha $0 = \alpha = \frac{\chi(g)}{\chi(1)}$ da cui segue che $\chi(g) = 0$. □

Lemma 4.13. *Sia G un gruppo semplice finito non abeliano, allora $[1]$ è l'unica classe di coniugio con cardialità una potenza di un primo.*

Dimostrazione. Si supponga per assurdo che il lemma sia falso, ovvero che esista un certo $g \neq 1$ tale che $|[g]| = p^r$ con p numero primo. Se χ è un carattere irriducibile non banale di G tale che $p \nmid \chi(1)$, allora per il lemma 4.12 $g \in Z(\chi)$ oppure $\chi(g) = 0$. Siccome G è un gruppo semplice non abeliano $(Ker\chi = \{1\})$ si ha che $Z(G) = Z(\chi) = \{1\}$, dunque per come è stato scelto g si può concludere che $\chi(g) = 0$. Sia ora

$$U = \{\chi \in Irr(G) \,:\, p \,|\, \chi(1)\}$$

[2] l'estensione $K/\mathbb{Q}$ è di Galois

utilizzando ora il carattere regolare di G si ottiene:

$$0 = \chi_{reg}(g) = \sum_{\chi \in Irr(G)} \chi(1)\chi(g) = 1 + \sum_{\chi \in U} \chi(1)\chi(g) \tag{4.2}$$

È evidente inoltre che il seguente elemento è un intero algebrico

$$\gamma = \sum_{\chi \in U} \frac{\chi(1)}{p}\chi(g)$$

allora dall'equazione 4.2 si ricava che $-1 = p\gamma$, ovvero $\gamma = -\frac{1}{p}$ che è un assurdo poiché per il lemma 4.2 gli interi algebrici non possono appartenere all'insieme $\mathbb{Q} \setminus \mathbb{Z}$. □

È possibile ora dimostrare il teorema $p^\alpha q^\beta$ di Burnside:

Teorema 4.14 ($p^\alpha q^\beta$ di Burnside)**.** *Sia G un gruppo tale che $|G| = p^\alpha q^\beta$ con p e q numeri primi e $\alpha, \beta \in \mathbb{N}$, allora G è risolubile.*

Dimostrazione. Se $p = q$ allora G è un p-Gruppo che è sempre risolubile, inoltre la tesi segue ovviamente anche se G è abeliano. Ci si può restringere dunque esclusivamente al caso in cui $p \neq q$ e inoltre G è non abeliano.
Innanzitutto si prova che un gruppo G di ordine $p^\alpha q^\beta$ non può essere semplice. Sia per assurdo G semplice, si consideri un Sylow P di G; chiaramente $Z(P)$ è non banale[3], e si prenda perciò un certo $g \in Z(P) \setminus \{1\}$. È facile mostrare che $P \leq C_G(g)$, infatti scelto un certo $h \in P$ si ha che $h^{-1}gh = g$ in quanto g è un elemento centrale. Sia adesso $[g]$ la classe di coniugio di g in G, allora dalla teoria dei gruppi è noto che $|[g]| = |G : C_G(g)|$, ma $|G : C_G(g)|$ divide $|G : P|$ dal momento che $|P|$ divide $|C_G(g)|$. Siccome P è un Sylow di G, allora $|G : P|$ è una potenza di un primo, e quindi per quanto detto poc'anzi anche $|[g]|$ è una potenza di un primo, ma ciò contraddice il lemma 4.13 poiché era stato scelto $g \neq 1$.
Si supponga ora per assurdo che il teorema sia falso, e si consideri il gruppo G di ordine minimo che soddisfi le ipotesi del teorema ma che non sia risolubile. Siccome G non è semplice, allora possiede un sottogruppo normale massimale proprio N di ordine $p^{\alpha_1}q^{\beta_1}$ che è risolubile date le ipotesi di minimalità fatte sull'ordine di G. Per lo stesso motivo, il gruppo quoziente G/N, che ha ordine $p^{\alpha-\alpha_1}q^{\beta-\beta_1}$, è risolubile. A questo punto, sia $N \rhd H_1 \rhd H_2 \rhd \ldots \rhd \{1\}$ la serie subnormale a quozienti abeliani da N a $\{1\}$; inoltre G/N è semplice per il teorema di corrispondenza (oltre che risolubile), perciò è abeliano. In sostanza G possiede la seguente serie subnormale che termina con $\{1\}$ a quozienti abeliani:

$$G \rhd N \rhd H_1 \rhd H_2 \rhd \ldots \rhd \{1\}$$

ovvero G è risolubile, contraddicendo così le ipotesi assunte per assurdo.

□

[3] il centro di un gruppo che ha ordine una potenza di un primo è sempre non banale

Capitolo 5

Prodotti di caratteri

5.1 "Moltiplicare" due caratteri

Nel capitolo 3 si è visto come definire nel modo più naturale possibile un'azione di $\mathbb{C}[G]$ (o in generale di una qualsiasi algebra gruppale $F[G]$) su una somma diretta di spazi vettoriali, e ora invece si costruirà un'azione di $\mathbb{C}[G]$ sul prodotto tensoriale tra due spazi vettoriali. La definizione non è del tutto semplice e procede per gradi, infatti per prima cosa si vede come agisce la base di $\mathbb{C}[G]$. Sia G un gruppo finito e siano inoltre U e V due $\mathbb{C}[G]$-moduli; se $\{u_i : i \in I\}$ è una base di U e $\{v_j : j \in J\}$ è una base di V, allora si definisca la seguente azione di G sulla base di $U \otimes V$:

$$\begin{aligned} \mu_{tens} : \{u_i \otimes v_j\} \times G &\longrightarrow \{u_i \otimes v_j\} \\ (u_i \otimes v_j,\, g) &\longmapsto (u_i \otimes v_j)^g = {u_i}^g \otimes {v_j}^g \end{aligned}$$

a questo punto, quella che è un'azione di un gruppo su un insieme si estende per linearità su tutti i tensori decomponibili (e dunque su tutto $U \otimes V$):

$$(u \otimes v)^g = \left(\sum_{i,j} \alpha_i \beta_j (u_i \otimes v_j) \right)^g := \sum_{i,j} \alpha_i \beta_j (u_i \otimes v_j)^g = \sum_{i,j} \alpha_i \beta_j ({u_i}^g \otimes {v_j}^g)$$

Prima di verificare che μ_{tens} così estesa è una azione di G su $U \otimes V$, bisogna provare un lemma:

Lemma 5.1. *Siano U e V due spazi vettoriali di dimensione finita, se $x_1, x_2 \ldots, x_s$ sono vettori di U e $y_1, y_2, \ldots, y_t$ sono vettori di V segue che*

$$\left(\sum_{i=1}^{s} x_i \right) \otimes \left(\sum_{j=1}^{t} y_j \right) = \sum_{i,j} x_i \otimes y_j$$

Dimostrazione. Dapprima si sfrutta la prorietà di bilinearità sulla prima componente del prodotto tensoriale

$$\left(\sum_{i=1}^{s} x_i \right) \otimes \left(\sum_{j=1}^{t} y_j \right) = \sum_{i=1}^{s} \left(x_i \otimes \sum_{j=1}^{t} y_j \right)$$

e dunque per ogni indice i fissato si utilizza la bilinerità questa volta sulla seconda componente del prodotto tensoriale

$$\sum_{i=1}^{s}\left(x_i \otimes \sum_{j=1}^{t} y_j\right) = \sum_{i=1}^{s}\left(\sum_{j=1}^{t} x_i \otimes y_j\right) = \sum_{i,j} x_i \otimes y_j$$

□

A questo punto è possibile esprimere il vettore $(u \otimes v)^g$ in maniera più comoda:

$$(u \otimes v)^g = \sum_{i,j} \alpha_i\beta_j({u_i}^g \otimes {v_j}^g) = \sum_{i,j} (\alpha_i u_i)^g \otimes (\beta_j v_j)^g =$$

$$= \left(\sum_i (\alpha_i u_i)^g\right) \otimes \left(\sum_j (\alpha_j v_j)^g\right) = \left(\sum_i \alpha_i u_i\right)^g \otimes \left(\sum_j \beta_j v_j\right)^g = u^g \otimes v^g$$

Di seguito la vrifica che μ_{tens} è un'azione di G su $U \otimes V$:

i) $\left((u \otimes v)^g\right)^h = (u^g \otimes v^g)^h = (u^g)^h \otimes (v^g)^h = u^{gh} \otimes v^{gh} = (u \otimes v)^{gh}$

ii) $(u \otimes v)^1 = u^1 \otimes v^1 = u \otimes v$

iii) $(\lambda u \otimes v)^g = (\lambda u^g) \otimes v^g = \lambda(u^g \otimes v^g) = \lambda(u \otimes v)^g$

iv) $(u \otimes v + x \otimes y)^g = \left(\sum_{i,j} \alpha_i\beta_j(u_i \otimes v_j) + \sum_{i,j} \gamma_i\delta_j(u_i \otimes v_j)\right)^g =$
$= \sum_{i,j} (\alpha_i\beta_j + \gamma_i\delta_j)(u_i \otimes v_j)^g = \sum_{i,j} \alpha_i\beta_j(u_i \otimes v_j)^g + \sum_{i,j} \gamma_i\delta_j(u_i \otimes v_j)^g =$
$= (u \otimes v)^g + (x \otimes y)^g$

Segue che $U \otimes V$ è un $\mathbb{C}G$-modulo, quindi non bisogna far altro che associare ad esso un $\mathbb{C}[G]$-modulo in modo unico. Come mostrato in generale nel secondo capitolo si ottiene un $\mathbb{C}[G]$-modulo facendo agire l'algebra gruppale $\mathbb{C}[G]$ "per estensione bilineare" dell'azione di G:

$$(u \otimes v)^{\sum \lambda_g g} = \sum_{g \in G} \lambda_g (u \otimes v)^g$$

Ovviamente l'azione di $\mathbb{C}[G]$ è stata presentata per i tensori decomponibili, ma si estende naturalmente per linearità su tutto $U \otimes V$. A primo impatto sembrerebbe che tale procedura non sia la più naturale possibile per dare a $U \otimes V$ una struttura di $\mathbb{C}[G]$-modulo, infatti ci si potrebbe chiedere come mai l'azione di $\mathbb{C}[G]$ sugli elementi della base di $U \otimes V$ non sia stata definita nel modo seguente:

$$(u_i \otimes v_j)^x = {u_i}^x \otimes {v_j}^x \quad \text{con } x \in \mathbb{C}[G]$$

Il motivo è semplicemente che in tal modo non si avrebbe un'azione, infatti ad esempio si avrebbe:

$$(u_i \otimes v_j)^{\lambda 1} = {u_i}^{\lambda 1} \otimes {v_j}^{\lambda 1} = \lambda u_i \otimes \lambda v_j = \lambda^2(u_i \otimes v_j)$$

e ovviamente, in generale $\lambda^2(u_i \otimes v_j)$ è diverso da $\lambda(u_i \otimes v_j)$, ovvero da come dovrebbe essere se quella definita fosse un'azione di un'algebra su uno spazio vettoriale.
Al $\mathbb{C}[G]$-modulo, sopra definito, corrisponde una rappresentazione di $\mathbb{C}[G]$, e dunque un carattere di G, è quindi interessante vedere nel dettaglio di che carattere si tratta. Riguardo le notazioni invece, se ρ e μ sono rispettivamente le rappresentazioni di $\mathbb{C}[G]$ su U e su V, allora la rappresentazione di $\mathbb{C}[G]$ su $U \otimes V$ è indicata con $\rho \otimes \mu$.

Teorema 5.2. *Siano, G un gruppo finito e inoltre U e V due spazi vettoriali di dimensione finita. Se ρ e μ sono due rappresentazioni di $\mathbb{C}[G]$ su U e V a cui corrispondono rispettivamente i caratteri χ e ψ, allora il carattere associato alla rappresentazione $\rho \otimes \mu$ è il prodotto $\chi\psi$ (con $\chi\psi(g) = \chi(g)\psi(g)$).*

Dimostrazione. Siano $\{u_i : i \in I\}$ una base per U e $\{v_j : j \in J\}$ una base per V. Innanzitutto si veda nel dettaglio come sono fatti i caratteri χ e ψ:

$$u_i(g\rho) = u_i^g = \sum_{\ell \in I} a_{i\ell} u_\ell \quad \forall i \in I \text{ e con } a_{i\ell} \in \mathbb{C}$$

$$v_j(g\rho) = v_j^g = \sum_{s \in J} b_{js} v_s \quad \forall j \in J \text{ e con } b_{js} \in \mathbb{C}$$

Segue che $\chi(g) = \sum_{\ell \in I} a_{\ell\ell}$ e inoltre $\psi(g) = \sum_{s \in J} b_{ss}$. Riguardo la rappresentazione $\rho \otimes \mu$, $\forall i \in I$ e $\forall j \in J$ si ha invece che:

$$\begin{aligned}(u_i \otimes v_j)\Big(g(\rho \otimes \mu)\Big) &= (u_i \otimes v_j)^g = {u_i}^g \otimes {v_j}^g = \left(\sum_{\ell \in I} a_{i\ell} u_\ell\right) \otimes \left(\sum_{s \in J} b_{js} v_s\right) = \\ &= \sum_{\ell,s} (a_{i\ell} u_\ell) \otimes (b_{js} v_s) = \sum_{\ell,s} a_{i\ell} b_{js} (u_\ell \otimes v_s)\end{aligned}$$

Se θ è il carattere associato alla rappresentazione $\rho \otimes \mu$, allora chiaramente

$$\theta(g) = \sum_{\ell,s} a_{\ell\ell} b_{ss} = \sum_{\ell \in I} a_{\ell\ell} \cdot \sum_{s \in J} b_{ss} = \chi(g)\psi(g)$$

Data l'arbitrarietà dell'elemento $g \in G$ si ha la tesi. □

Il prodotto fra due caratteri è dunque un carattere, ma in generale il prodotto tra due caratteri irriducibili *non* è irriducibile. A prima vista dunque, non viene introdotto alcun ulteriore metodo per trovare nuovi caratteri irriducibili. In realtà però si può dire qualcosa a riguardo.

Teorema 5.3 (di Burnside-Brauer)**.** *Sia χ un carattere fedele di un gruppo finito G. Se al variare di $g \in G$, $\chi(g)$ assume m valori distinti, allora ogni $\psi \in Irr(G)$ è un costituente di almeno un carattere χ^j con $0 \leq j < m$.*

Dimostrazione. Siano $\alpha_1, \alpha_2, \ldots, \alpha_m$ i valori distinti che assume χ, si ponga quindi

$$G_i = \{g \in G : \chi(g) = \alpha_i\}$$

Se $\alpha_1 = \chi(1)$, allora dal momento che χ è fedele si ha $G_1 = Ker(\chi) = \{1\}$. Sia ora ψ un certo carattere irriducibile di G e si ponga inoltre

$$\beta_i = \sum_{g \in G_i} \overline{\psi(g)}$$

quindi $\forall j \geq 0$ si ha

$$\langle \chi^j, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi^j(g)\overline{\psi(g)} = \frac{1}{|G|} \sum_{i=1}^{m} {\alpha_i}^j \beta_i$$

Si supponga ora per assurdo che il teorema si falso, ovvero che tale ψ non sia un costituente di χ^j per ogni j tale che $0 \leq j < m$, allora si ha che:

$$\sum_{i=1}^{m} {\alpha_i}^j \beta_i = 0$$

Al variare di j si ottiene un sistema di m equazioni che può essere riassunto nel modo seguente:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_m \\ \vdots & \vdots & \cdots & \vdots \\ {\alpha_1}^{m-1} & {\alpha_2}^{m-1} & \cdots & {\alpha_m}^{m-1} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

La matrice scritta sopra è la matrice di Vandermonde trasposta che è sempre invertibile dal momento che il determinante dato da

$$\pm \prod_{i<j} (\alpha_i - \alpha_j)$$

è non nullo poiché tutti gli α_i sono distinti. Segue quindi che $\beta_i = 0 \ \forall i \in \{1, \ldots, m\}$, ma questa è una contraddizione poiché $\beta_1 = \overline{\psi(1)} \neq 0$. □

Esempio 5.4. Il carattere regolare χ_{reg} assume esattamente due valori, ovvero $|G|$ e 0, dunque ogni carattere irriducibile è un costituente di $\chi^0_{reg} = \chi_1$, oppure di χ_{reg}. In effetti ciò è vero poiché si è visto in precedenza che il carattere regolare è combinazione lineare dei caratteri irriducibili con coefficienti (in $\mathbb{N}$) tutti positivi.

Ecco un utile modo per trovare nuovi caratteri irriducibili partendo da caratteri noti:

Lemma 5.5. *Sia $\chi \in Irr(G)$ e ξ un carattere lineare di G, allora il carattere $\chi\xi$ è irriducibile.*

Dimostrazione. Basta verificare che il prodotto interno $\langle \chi\xi, \chi\xi \rangle$ è uguale a 1 sfruttando il fatto che se un carattere è lineare, allora è un omomorfismo tra G e $\mathbb{C}^*$:

$$\langle \chi\xi, \chi\xi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\xi(g)\chi(g^{-1})\xi(g^{-1}) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi(g^{-1})\xi(gg^{-1}) =$$

$$= \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi(g^{-1}) = \langle \chi, \chi \rangle = 1$$

□

5.2 Decomposizione di χ^2

Sia ρ una rappresentazione di $\mathbb{C}[G]$ su V a cui è associato il carattere χ, allora alla rappresentazione $\rho \otimes \rho$ su $V \otimes V$ corrisponde il carattere χ^2. Sia $\{v_i : i \in I\}$ una base per V, si definisca allora la funzione τ sulla base di $V \otimes V$ in modo tale che $\tau(v_i \otimes v_j) = v_j \otimes v_i$. Estendendo tale funzione per linearità, si ottiene

$$\tau(x \otimes y) = \tau\left(\sum_{i,j} \alpha_i \beta_j (v_i \otimes v_j)\right) = \sum_{i,j} \alpha_i \beta_j \tau(v_i \otimes v_j) = \sum_{i,j} \beta_j \alpha_i (v_j \otimes v_i) = y \otimes x$$

ovvero τ è un endomorfismo di $V \otimes V$ tale che $\tau(x \otimes y) = y \otimes x$. Si considerino ora i seguenti sottoisiemi di $V \otimes V$:

$$S(V \otimes V) = \{x \in V \otimes V \,:\, \tau(x) = x\}$$

$$A(V \otimes V) = \{x \in V \otimes V \,:\, \tau(x) = -x\}$$

detti rispettivamente *parte simmetrica* e *parte antisimmetrica* di $V \otimes V$. Vale allora il seguente risultato

Lemma 5.6. *Dato un $\mathbb{C}[G]$-modulo V, allora $S(V \otimes V)$ e $A(V \otimes V)$ sono due $\mathbb{C}[G]$-sottomoduli di $V \otimes V$ e inoltre si verifica che*

$$V \otimes V = S(V \otimes V) \oplus A(V \otimes V)$$

Dimostrazione. Innanzitutto si deve provare che $S(V \otimes V)$ e $A(V \otimes V)$ sono due sottospazi vettoriali. Essi sono non vuoti, poiché contengono lo 0; se $x, y \in S(V \otimes V)$ allora

$$\tau(\lambda x) = \lambda \tau(x) = \lambda x$$

$$\tau(x + y) = \tau(x) + \tau(y) = x + y$$

allo stesso modo, presi $w, z \in A(V \otimes V)$ si ha

$$\tau(\lambda w) = \lambda \tau(w) = -\lambda w$$

$$\tau(w + z) = \tau(w) + \tau(z) = -(w + z)$$

Si vuole provare ora che la funzione τ è un omomorfismo di $\mathbb{C}[G]$-moduli, e siccome è gia lineare per definizione bisogna vedere se commuta con l'azione di $\mathbb{C}[G]$:

$$\tau\Big((v \otimes w)^{\sum \lambda_g g}\Big) = \tau\left(\sum_{g \in G} \lambda_g (v \otimes w)^g\right) = \sum_{g \in G} \lambda_g \tau(v^g \otimes w^g) = \sum_{g \in G} \lambda_g (w^g \otimes v^g) =$$

$$= \sum_{g \in G} \lambda_g (w \otimes v)^g = (w \otimes v)^{\sum \lambda_g g} = \Big(\tau(v \otimes w)\Big)^{\sum \lambda_g g}$$

A questo punto si nota che se $x \in S(V \otimes V)$, allora

$$\tau(x^{\sum \lambda_g g}) = \Big(\tau(x)\Big)^{\sum \lambda_g g} = \; x^{\sum \lambda_g g}$$

ovvero $x^{\sum \lambda_g g} \in S(V \otimes V)$. Analogamente se $x \in A(V \otimes V)$ si ha che

$$\tau(x^{\sum \lambda_g g}) = \Big(\tau(x)\Big)^{\sum \lambda_g g} = \ (-x)^{\sum \lambda_g g} = -x^{\sum \lambda_g g}$$

quindi $x^{\sum \lambda_g g} \in A(V \otimes V)$. La parte simmetrica e la parte antisimmetrica di $V \otimes V$ sono dunque entrambe dei $\mathbb{C}[G]$-sottomoduli. Riguardo la seconda parte del lemma notare che se $z \in S(V \otimes V) \cap A(V \otimes V)$, allora vale che $z = \tau(z) = -z$, ovvero $z = 0$; se invece $x \in V \otimes V$, allora $x = \frac{1}{2}\big(x + \tau(x)\big) + \frac{1}{2}\big(x - \tau(x)\big)$, ed è facile verificare che $x + \tau(x) \in S(V \otimes V)$ e $x - \tau(x) \in A(V \otimes V)$. □

Denotando con χ_S e con χ_A rispettivamente i caratteri relativi ai sottomoduli $S(V \otimes V)$ e $A(V \otimes V)$, per lemma appena dimostrato si ha dunque che

$$\chi^2 = \chi_S + \chi_A$$

Se $dim(V) = n$, e $\{v_1 \dots v_n\}$ ne è una base, si noti che gli elementi del tipo $v_i \otimes v_j + v_j \otimes v_i \in S(V \otimes V)$, mentre $v_i \otimes v_j - v_j \otimes v_i \in A(V \otimes V)$. Si definiscano allora i due insiemi

$$\mathcal{B}_S = \{v_i \otimes v_j + v_j \otimes v_i \ : \ 1 \leq i \leq j \leq n\}$$

$$\mathcal{B}_A = \{v_i \otimes v_j - v_j \otimes v_i \ : \ 1 \leq i < j \leq n\}$$

È molto semplice verificare che $\mathcal{B}_S$ è una famiglia di vettori linearmente indipendenti di $S(V \otimes V)$ e che lo stesso vale per $\mathcal{B}_A$ e $A(V \otimes V)$. Perciò vale che

$$dim\big(S(V \otimes V)\big) \geq |\mathcal{B}_S| = \frac{n(n-1)}{2} + n = \frac{n(n+1)}{2}$$

$$dim\big(A(V \otimes V)\big) \geq |\mathcal{B}_A| = \frac{n(n-1)}{2}$$

ma per il lemma 5.6 deve essere che

$$dim(V \otimes V) = n^2 = dim\big(S(V \otimes V)\big) + dim\big(A(V \otimes V)\big)$$

e ciò è vero se e solo se $dim\big(S(V \otimes V)\big) = \mathcal{B}_S$ e $dim\big(A(V \otimes V)\big) = \mathcal{B}_A$. Segue dunque che gli insiemi $\mathcal{B}_S$ e $\mathcal{B}_A$ sono due basi.

Lemma 5.7. *Con le notazioni precedenti, per ogni $g \in G$ si ha che:*

$$\chi_S(g) = \frac{1}{2}\big(\chi^2(g) + \chi(g^2)\big)$$

$$\chi_A(g) = \frac{1}{2}\big(\chi^2(g) - \chi(g^2)\big)$$

Dimostrazione. Poichè il campo degli scalari è $\mathbb{C}$, fissato un certo $g \in G$, se ρ è la rappresentazione di G su V, è sempre possibile scegliere una base di V tale per cui $g\rho$ è diagonale. Se $\{e_1, \dots, e_n\}$ è tale base allora si ha che $e_i^g = \lambda_i e_i$, ovvero $\chi(g) = \sum_{i=1}^n \lambda_i$. Allo stesso modo

$$(e_i \otimes e_j - e_j \otimes e_i)^g = \lambda_i e_i \otimes \lambda_j e_j - \lambda_j e_j \otimes \lambda_i e_i = \lambda_i \lambda_j (e_i \otimes e_j - e_j \otimes e_i)$$

Dunque $\mathcal{B}_A$ è una base di autovettori per $g(\rho\otimes\rho)$ ristretta al sottospazio $A(V\otimes V)$, ovvero

$$\chi_A(g) = \sum_{i<j} \lambda_i \lambda_j$$

Vale inoltre che $e_i^{g^2} = e_i(g^2\rho) = e_i(g\rho)^2 = {\lambda_i}^2 e_i$, quindi $\chi(g^2) = \sum_{i=1}^n {\lambda_i}^2$, quindi in sostanza

$$\chi^2(g) = \left(\sum_{i=1}^n \lambda_i\right)^2 = \sum_{i=1}^n {\lambda_i}^2 + 2\sum_{i<j} \lambda_i\lambda_j = \chi(g^2) + 2\chi_A(g)$$

da cui segue che

$$\chi_A(g) = \frac{1}{2}(\chi^2(g) - \chi(g^2))$$

Dalla suddetta equazione, insieme alla relazione $\chi^2(g) = \chi_S(g) + \chi_A(g)$ si ricava infine che

$$\chi_S(g) = \frac{1}{2}\big(\chi^2(g) + \chi(g^2)\big)$$

□

Capitolo 6

Induzione e restrizione di caratteri

Fino ad ora si è visto il legame che intercorre fra la tavola dei caratteri di un gruppo finito G e quella di un suo gruppo quoziente G/N. In questo capitolo, invece, dato un generico sottogruppo H di G, si vogliono scovare alcune relazioni tra i caratteri irriducibili di H e quelli di G. Per semplicità, nel seguito con il simbolo H si indicherà sempre un generico sottogruppo di G.

6.1 Restrizione

Il processo di restrizione, è il modo più naturale per trovare alcuni caratteri di H a partire da quelli di G. Sia ρ una rappresentazione di $\mathbb{C}[G]$ su V, allora la funzione $\rho_{|\mathbb{C}[H]}$ è ancora una rappresentazione di $\mathbb{C}[H]$ su V, dunque $(V, \rho_{|\mathbb{C}[H]})$ è un $\mathbb{C}[H]$-modulo che sarà indicato semplicemente con V_H.

Definizione. Sia χ un carattere di G relativo a (V, ρ), allora il carattere di H relativo a V_H si dirà *carattere di χ ristretto ad H* e sarà indicato con χ_H.

Naturalmente per ogni $h \in H$ si avrà:

$$\chi_H(h) = tr(h\rho_{|\mathbb{C}[H]}) = tr(h\rho) = \chi(h)$$

ovvero il carattere ristretto ad H sarà semplicemente una restrizione, nel senso funzionale del termine, del carattere di G originariamente considerato.

Esempio 6.1. Sia μ il carattere regolare di G e θ il carattere regolare di H allora ci si chiede in che relazione stanno μ_H e θ. Ovviamente

$$\theta(h) = \begin{cases} |H| & \text{se } h = 1 \\ 0 & \text{se } h \neq 1 \end{cases}$$

$$\mu_H(h) = \begin{cases} |G| & \text{se } h = 1 \\ 0 & \text{se } h \neq 1 \end{cases}$$

dunque μ_H è un multiplo (scalare) di θ e vale la relazione $\mu_H = |G : H|\theta$.

Riguardo le rappresentazioni irriducibili, e dunque i caratteri irriducibili, vale invece il seguente lemma la cui dimostrazione è abbastanza ovvia:

Lemma 6.2. *Se V_H è un $\mathbb{C}[H]$-modulo irriducibile, allora V è un $\mathbb{C}[G]$-modulo irriducibile.*

Dimostrazione. Non esiste nessun sottospazio U di V tale che $U^x \subseteq U \ \forall x \in \mathbb{C}[H]$ e dunque a maggior ragione non esisterà nessun sottospazio di V chiuso rispetto all'azione di tutta l'algebra $\mathbb{C}[G]$. □

Il viceversa di tale lemma non vale, ovvero i ristretti di caratteri irriducibili di G non sono in generale dei caratteri irriducibili di H. In ogni caso si vedrà che tutte le informazioni riguardanti la tavola dei caratteri di H sono contenute nella tavola dei caratteri di G anche se ciò non è proprio evidente. Ovviamente il processo di restrizione si può attuare non solo ai caratteri di G bensì a tutte le funzioni di classe di G, infatti se $\varphi \in c\ell(G)$, naturalmente $\varphi \in c\ell_H(H)$.
Sullo spazio vettoriale $c\ell(H)$ è definito lo stesso prodotto interno visto nei capitoli precedenti, ma per distinguere il caso in cui si stanno facendo i calcoli in $c\ell(H)$ oppure in $c\ell(G)$ si utilizzeranno rispettivamente le notazioni $\langle\ ,\ \rangle_H$ e $\langle\ ,\ \rangle_G$ per evitare confusione.

Lemma 6.3. *Sia G un gruppo finito con k classi di coniugio ed H un suo sottogruppo . Se $\psi \in Char(H)$, allora esiste un certo $\chi \in Irr(G)$ tale che $\langle \chi_H, \psi \rangle_H \neq 0$.*

Dimostrazione. Sia μ il carattere regolare di G e θ il carattere regolare di H, allora:

$$\langle \mu_H, \psi \rangle_H = |G : H| \langle \theta, \psi \rangle_H = \psi(1) > 0$$

Ma $\mu_H = \sum_{i=1}^{k} \chi_{i\,H}(1)\chi_{i\,H}$ dove i χ_i sono i caratteri irriducibili di H, dunque

$$\langle \mu_H, \psi \rangle_H = \sum_{i=1}^{k} \chi_{i\,H}(1) \langle \chi_{i\,H}, \psi \rangle_H > 0$$

ovvero almeno un fattore $\langle \chi_{j\,H}, \psi \rangle_H$ è diverso da zero per qualche $j \in \{1, \ldots, k\}$. □

Un'importantissima conseguenza di quanto appena detto è che ogni carattere irriducibile di H è un costituente di qualche carattere irriducibile di G ristretto ad H. Dunque in linea teorica i caratteri irriducibili di H si possono ottenere restringendo tutti i caratteri irriducibili di G, ed è proprio in tal senso si intende che tutte le informazioni sulla tavola dei caratteri di H sono contenute nella tavola dei caratteri di G. Tuttavia, nei fatti è estremamente difficile esprimere $\chi_{i\,H}$ come combinazione lineare di caratteri irriducibili di H, anche se il seguente lemma fornisce un grosso aiuto nei casi in cui $|G : H|$ è un numero piccolo.

Lemma 6.4. *Sia G un gruppo finito ed H un suo sottogruppo. Se $\chi \in Irr(G)$ e $\psi_i, \ldots, \psi_t$ sono i caratteri irriducibili di H allora riguardo la decomposizione*

$$\chi_H = \sum_{i=1}^{t} d_i \psi_i \quad con\ \ d_i \in \mathbb{N}$$

si ha che ${d_1}^2 + {d_2}^2 + \ldots + {d_t}^2 \leq |G : H|$, con l'uguaglianza valida se $\chi(G \setminus H) = 0$.

Dimostrazione. È noto che

$$\langle \chi_H, \chi_H \rangle_H = \sum_{i=1}^{t} {d_i}^2$$

ma siccome χ è un carattere irriducibile di G si ha

$$1 = \langle \chi, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{|H|}{|G|} \langle \chi_H, \chi_H \rangle_H + C$$

con $C = \dfrac{1}{|G|} \displaystyle\sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)} \geq 0$. Ma allora dall'ultima equazione banalmente

$$\sum_{i=1}^{t} {d_i}^2 = (1 - C)|G : H| \leq |G : H|$$

L'uguaglianza vale se $C = 0$, ovvero se $\chi(G \setminus H) = 0$. □

Di seguito un semplice esempio in cui viene messo in atto quanto detto sulla restrizione di caratteri:

Esempio 6.5 (la tavola dei caratteri di A_4)**.** Partendo dalla tavola dei caratteri di S_4 si vuole ricavare la tavola dei caratteri di A_4 sfruttando il fatto che l'indice del sottogruppo è il più piccolo possibile ovvero 2. Tramite dei semplici calcoli si vede che in A_4 ci sono 4 classi di coniugio e dunque tramite l'equazione delle classi si deduce subito che ci sono tre caratteri di grado 1 e un carattere di grado 3.

	1	[(1 2)(3 4)]	[(1 2 3)]	[(1 3 2)]
$\lvert g^G \rvert$	1	3	4	4
$\lvert C_G(g) \rvert$	12	4	3	3
ψ_1	1	1	1	1
ψ_2	1	?	?	?
ψ_3	1	?	?	?
ψ_4	3	?	?	?

Per crendere più comodi i calcoli è importante avere a portata di mano la tavola dei caratteri di S_4:

	1	[(1 2)(3 4)]	[(1 2 3)]	[(1 2)]	[(1 2 3 4)]
χ_1	1	1	1	1	1
χ_2	1	1	1	−1	−1
χ_3	2	2	−1	0	0
χ_4	3	−1	0	1	−1
χ_5	3	−1	0	−1	1

Si ponga $A_4 = H$ e d $S_4 = G$ allora se

$$\chi_{j\,H} = \sum_{i=1}^{4} d_i \psi_i$$

per il lemma 6.4 si ha $\sum_{i=1}^{4} {d_i}^2 \leq 2$, ovvero al massimo due coefficienti sono non nulli e inoltre possono assumere solamente il valore 1 oltre che 0.
Ovviamente $\chi_{1\,H} = \chi_{2\,H} = \psi_1$; inoltre siccome $\chi_{4\,H}$ ha grado 3, l'unica possibilità di esprimerlo come somma di al più due caratteri irriducibili di H è $\chi_{4\,H} = \chi_{5\,H} = \psi_4$.

	1	$[(1\,2)(3\,4)]$	$[(1\,2\,3)]$	$[(1\,3\,2)]$
$\lvert g^G \rvert$	1	3	4	4
$\lvert C_G(g) \rvert$	12	4	3	3
ψ_1	1	1	1	1
ψ_2	1	?	?	?
ψ_3	1	?	?	?
ψ_4	3	-1	0	0

Per quanto riguarda il carattere $\chi_{3\,H}$, si noti che $\chi_4(G \setminus H) = 0$, perciò $\chi_{3\,H}$ è la somma di due caratteri irriducibili di H, che chiaramente devono avere grado 1. Si veda innanzitutto se ψ_1 è un costituente di $\chi_{3\,H}$:

$$\langle \chi_{3\,H}, \psi_1 \rangle_H = \frac{1}{12}\big(1 \cdot (2 \cdot 1) + 3 \cdot (2 \cdot 1) + 4 \cdot (-1 \cdot 1) + 4 \cdot (-1 \cdot 1)\big) = 0$$

Segue dunque che $\chi_{3\,H} = \psi_2 + \psi_3$, perciò:

$$2 = \chi_{3\,H}\big((1\,2)(3\,4)\big) = \psi_2\big((1\,2)(3\,4)\big) + \psi_3\big((1\,2)(3\,4)\big)$$

$$-1 = \chi_{3\,H}\big((1\,2\,3)\big) = \psi_2\big((1\,2\,3)\big) + \psi_3\big((1\,2\,3)\big)$$

$$-1 = \chi_{3\,H}\big((1\,3\,2)\big) = \psi_2\big((1\,3\,2)\big) + \psi_3\big((1\,3\,2)\big)$$

Ma ψ_2 e ψ_3 sono caratteri lineari, dunque $\psi_2\big((1\,2)(3\,4)\big)$ e $\psi_3\big((1\,2)(3\,4)\big)$ devono essere radici quadrate dell'unità mentre $\psi_2\big((1\,2\,3)\big)$, $\psi_3\big((1\,2\,3)\big)$, $\psi_2\big((1\,3\,2)\big)$ e $\psi_3\big((1\,3\,2)\big)$ sono radici terze dell'unità. Ponendo $\omega = e^{\frac{2\pi i}{3}}$ si ha che l'unica possibilità a meno di scambiare l'ordine dei caratteri è la seguente:

	1	$[(1\,2)(3\,4)]$	$[(1\,2\,3)]$	$[(1\,3\,2)]$
ψ_1	1	1	1	1
ψ_2	1	1	ω	ω^2
ψ_3	1	1	ω^2	ω
ψ_4	3	-1	0	0

Tabella 6.1. Tavola dei caratteri di A_4

6.2 Induzione

Verrà ora discusso un procedimento duale di quello di restrizione precedentemente descritto. Dato come sempre un sottogruppo H di un gruppo finito G si vogliono trovare alcuni caratteri di G a partire dai caratteri di H. Ciò è qualcosa di molto interessante poiché dalla tavola dei caratteri di un gruppo piccolo H si puó

pensare di trovare qualche informazione sulla tavola dei caratteri di un gruppo più grande che lo contiene.
Sia φ una funzione di classe di H, allora si definisca $\varphi^o : G \to \mathbb{C}$ tale che

$$\varphi^o(g) = \begin{cases} \varphi(g) & \text{se } g \in H \\ 0 & \text{se } g \in G \setminus H \end{cases}$$

Allora è facile verificare la funzione $\varphi^G : G \to \mathbb{C}$ con

$$\varphi^G(g) = \frac{1}{H} \sum_{x \in G} \varphi^o(x^{-1}gx)$$

è una funzione di classe di G tale che $\varphi^G(1) = |G : H|\varphi(1)$. È stata definita dunque una mappa lineare tra $c\ell(H)$ e $c\ell(G)$ tale che $\varphi \mapsto \varphi^G$, infatti:

$$(c_1\varphi + c_2\sigma)^G = \frac{1}{H} \sum_{x \in G} (c_1\varphi^o + c_2\sigma^o)(x^{-1}gx) = c_1\varphi^G + c_2\sigma^G$$

Teorema 6.6 (di reciprocità di Frobenius)**.** *Sia H un sottogruppo di un gruppo finito G. Se $\varphi \in c\ell(H)$ e $\theta \in c\ell(G)$ allora vale che*

$$\langle \varphi, \theta_H \rangle_H = \langle \varphi^G, \theta \rangle_G$$

Dimostrazione.

$$\langle \varphi^G, \theta \rangle_G = \frac{1}{|G|} \sum_{g \in G} \varphi^G(g)\overline{\theta(g)} = \frac{1}{|G||H|} \sum_{g \in G} \sum_{x \in G} \varphi^o(x^{-1}gx)\overline{\theta(g)}$$

Ponendo $y = x^{-1}gx$, dal momento che θ è una funzione di classe si ha $\theta(g) = \theta(y)$, inoltre far variare g in G oppure $x^{-1}gx$ in G è la stessa cosa visto che il coniugio è un automorfismo. Si ha dunque

$$\langle \varphi^G, \theta \rangle_G = \frac{1}{|G||H|} \sum_{y \in G} \sum_{x \in G} \varphi^o(y)\overline{\theta(y)} = {}^{1} \frac{1}{|G||H|} \sum_{y \in H} \sum_{x \in G} \varphi(y)\overline{\theta(y)} =$$

$$= \frac{1}{|H|} \sum_{y \in H} \varphi(y)\overline{\theta(y)} = \langle \varphi, \theta_H \rangle_H$$

□

Se ψ è un carattere di H è lecito chiedersi se ψ^G è anche un carattere di G o meno, ovvero se il metodo descritto è utile a trovare nuovi caratteri di G oltre che nuove funzioni di classe. Il seguente lemma fornisce una risposta esauriente:

Lemma 6.7. *Sia H un sottogruppo di un gruppo finito G. Se ψ è un carattere di H, allora ψ^G è un carattere di G.*

Dimostrazione. Siccome $\psi(1) > 0$ è evidente che ψ^G non può essere la funzione nulla poiché $\psi^G(1) = |G : H|\psi(1)$. Sia $\chi \in Irr(G)$, allora $\langle \psi, \chi_H \rangle_H$ è un intero non negativo per come è definito il prodotto interno di caratteri e inoltre per il teorema di reciprocità di Frobenius si ha che $\langle \psi, \chi_H \rangle_H = \langle \psi^G, \chi \rangle_G$. Data l'arbitrarietà della scelta di χ segue che è stato appena dimostrato che ψ^G è combinazione lineare a coefficienti in $\mathbb{N}_0$ di caratteri irriducibili di G, dunque è un carattere poiché $\psi^G \neq 0$. □

[1] si usa il fatto che $\varphi^o(g) = 0$ se $g \in G \setminus H$

Sono stati così ottenuti nuovi caratteri di G, però se $\psi \in Irr(H)$ in generale $\psi^G \notin Irr(G)$. Viceversa se ψ non è irriducibile e supponendo che $\{\psi_1, \dots \psi_t\} = Irr(H)$ si ha

$$\psi^G = \left(\sum_{i=1}^{t} c_i \psi_i \right)^G = \sum_{i=1}^{t} c_i {\psi_i}^G$$

ovvero ψ^G non è irriducibile come carattere di G.

Capitolo 7

Gruppi di Frobenius

La teoria dei caratteri oltre a dimostrare una notevole bellezza intrinseca, è di particolare importanza in algebra, poiché senza di essa probabilmente non si sarebbe mai arrivati alla classificazione dei gruppi semplici finiti. Quando una teoria matematica risulta utile su diversi fronti oltre che essere formalmente corretta ci si accorge di essere di fronte ad una "buona" teoria, e ciò è quello accade per la teoria dei caratteri. In questo capitolo verranno presentati i gruppi di Frobenius insieme al teorema di esistenza del nucleo di Frobenius di cui ad oggi l'unica dimostrazione nota fa largo uso dei caratteri. Quanto verrà qui detto, in un certo senso rappresenta il punto di partenza per tutto il lavoro compiuto nella formulazione del teorema di classificazione dei gruppi semplici. Quindi dopo aver visto il teorema $p^\alpha q^\beta$ di Burnside nel capitolo 4 ci si trova di fronte ad una seconda importante applicazione della teoria dei caratteri.
Riguardo la notazione, se G è un gruppo, con il simbolo G^x si indicherà $x^{-1}Gx$.

Definizione. Un gruppo finito G si dice *gruppo di Frobenius* se possiede un sottogruppo H tale che $H \cap H^x = \{1\}\ \forall x \in G \setminus H$. Tale sottogruppo H è detto *complemento di Frobenius di* G.

Lemma 7.1. *Se H è un complemento di Frobenius in G, allora tutti i sottogruppi distinti del tipo H^x al variare di x in $G \setminus H$ hanno intersezione banale.*

Dimostrazione. Sia per assurdo $g \neq 1$ tale che $g \in H^x \cap H^y$ con $H^x \neq H^y$ per certi x e y distinti in $G \setminus H$. Allora $g = x^{-1}h_1x = y^{-1}h_2y$ con $h_1, h_2 \in H$, ovvero $h_1 = (yx^{-1})^{-1}h_2(yx^{-1})$. Segue che $h_1 \in H \cap H^{yx^{-1}}$, ma H è un complemento di Frobenius, perciò $k = yx^{-1} \in H$ con $k \neq 1$ poiché x e y sono diversi. A questo punto scrivendo $y = kx$ si ha $H^y = H^{kx} = H^x$, che contraddice le ipotesi. □

Segue dunque che se il complemento di Frobenius esiste, esso non è determinato univocamente, poiché qualsiasi altro suo coniugato è a sua volta un complemento di Frobenius.
È possibile ora enunciare e dimostrare il teorema del nucleo di Frobenius; per comodità verrà dapprima enunciato il teorema che sarà seguito dalla dimostrazione di alcuni lemmi preliminari e solo successivamente sarà data una dimostrazione completa del suddetto teorema:

Teorema 7.2 (di esistenza del nucleo di Frobenius)**.** *Sia G un gruppo di Frobenius con complemento H, allora esiste $N \trianglelefteq G$ tale che $N \cap H = \{1\}$ e $NH = G$. Tale sottogruppo N è detto nucleo di Frobenius.*

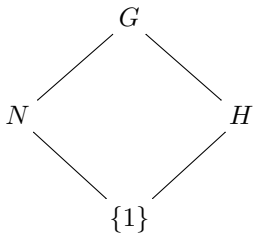

Figura 7.1

Un fatto molto curioso è che è relativamente semplice trovare un insieme che soddisfi le proprietà di nucleo di Frobenius, mentre senza la teoria dei caratteri (attualmente) è impossibile dimostrare che esso è un sottogruppo.

Lemma 7.3. *Sia G un gruppo di Frobenius con complemento H allora l'insieme*

$$N = \left(G \setminus \bigcup_{x \in G} H^x \right) \cup \{1\}$$

ha cardinalità $|G : H|$. Inoltre se $M \trianglelefteq G$ è tale che $M \cap H = \{1\}$, allora $M \subseteq N$.

Dimostrazione. Sia $\mathcal{S}$ l'insieme di tutti i sottogruppi di G, allora G agisce su $\mathcal{S}$ mediante $(H, g) \mapsto H^g$. Per il teorema orbita-stabilizzatore si ha che $\frac{|G|}{|N_G(H)|} = |H^G|$ dove con $|H^G|$ si indica la lunghezza dell'orbita di H, ovvero il numero di sottogruppi di G della forma H^x. Visto che per ipotesi H è un complemento di Frobenius, è chiaro che $N_G(H) = H$ e quindi $|H^G| = |G : H|$. Utilizzando quanto provato nel lemma 7.1 si ha che:

$$|N| = |G| - |G : H|(|H| - 1) = |G| - |G| + |G : H| = |G : H|$$

Sia infine $M \trianglelefteq G$ tale che $M \cap H = \{1\}$, allora per ogni $x \in G$ vale che

$$\{1\} = \{1\}^x = (M \cap H)^x = M^x \cap H^x = M \cap H^x$$

ovvero $M \subseteq N$ per come è stato definito N. □

Appare chiaro che il candidato ad essere il nucleo di Frobenius è proprio l'insieme N definito nel precedente lemma.

Lemma 7.4. *Sia G un gruppo di Frobenius con complemento H. Se θ è una funzione di classe di H tale che $\theta(1) = 0$, allora $(\theta^G)_H = \theta$*

Dimostrazione. Se si considera l'elemento 1, vale che

$$\theta^G(1) = |G : H|\theta(1) = 0 = \theta(1)$$

Sia dunque $h \in H \setminus \{1\}$, allora

$$\theta^G(h) = \frac{1}{|H|} \sum_{x \in G} \theta^o(x^{-1}hx) \tag{7.1}$$

Se $\theta^o(x^{-1}hx) \neq 0$ allora necessariamente $x^{-1}hx \in H \setminus \{1\}$, ma $x^{-1}hx \in H^x$, dunque $1 \neq x^{-1}hx \in H \cap H^x$; ora siccome H è un complemento di Frobenius segue che $x \in H$. Ripercorrendo a ritroso mediante la contronominale quanto appena detto, si nota che è stato provato che se $x \notin H$ allora $\theta^o(x^{-1}hx) = 0$, perciò nella somma dell'equazione 7.1 basta considerare elementi di H.

$$\theta^G(h) = \frac{1}{|H|} \sum_{x \in G} \theta^o(x^{-1}hx) = \frac{1}{|H|} \sum_{x \in H} \theta(x^{-1}hx)$$

Ma d'altra parte se $x \in H$, l'elemento $x^{-1}hx$ è coniugato ad h in H, perciò $\theta(x^{-1}hx) = \theta(h)$. e dunque

$$\theta^G(h) = \frac{1}{|H|} \sum_{x \in H} \theta(x^{-1}hx) = \frac{1}{|H|} \sum_{x \in H} \theta(h) = \theta(h)$$

□

Dal lemma appena provato e dal teorema di reciprocità di Frobenius, nel caso di gruppi di Frobenius con complemento H, si ha che

$$\left\langle \theta^G, \theta^G \right\rangle_G = \left\langle \theta, (\theta^G)_H \right\rangle_H = \left\langle \theta, \theta \right\rangle_H \tag{7.2}$$

Quanto appena scritto fornisce la seguente interpretazione geometrica di tutto il discorso che si sta facendo.
Chiaramente l'insieme $E(H) = \{\theta \in c\ell(H) : \theta(1) = 0\}$ è uno spazio vettoriale, inoltre se H è un complemento di Frobenius, l'applicazione lineare di induzione da $E(H)$ in $c\ell(G)$ tale che $\theta \mapsto \theta^G$ è un isomorfismo (la restrizione è la sua inversa per il lemma 7.4). A questo punto la condizione descritta nell'equazione 7.2 dice semplicemente che che l'induzione è un'isometria tra $E(H)$ e $c\ell(G)$ rispetto al solito prodotto interno, poiché le "distanze" si conservano.

Dimostrazione del teorema 7.2 di esistenza del nucleo di Frobenius. Sia 1_G il carattere banale di G e 1_H il carattere banale di H. Se $\varphi \in Irr(H) \setminus \{1_H\}$ si costruisca la seguente funzione di classe di H in termini della sua decomposizione nella base:

$$\theta := \varphi - \varphi(1)1_H$$

Si ha ovviamente che $\theta(1) = 0$, quindi per il lemma 7.4 e per le proprietà del prodotto interno fra caratteri si ha che

$$\left\langle \theta^G, \theta^G \right\rangle_G = \left\langle \theta, \theta \right\rangle_H = \left\langle \varphi - \varphi(1)1_H, \varphi - \varphi(1)1_H \right\rangle_H = 1 + \varphi(1)^2 \tag{7.3}$$

inoltre per il teorema di reciprocità di Frobenius

$$\left\langle \theta^G, 1_G \right\rangle_G = \left\langle \theta, 1_H \right\rangle_H = -\varphi(1) \tag{7.4}$$

Si costruisca ora un'ulteriore funzione di classe, questa volta di G a partire dall'induzione di θ:

$$\varphi^* := \theta^G + \varphi(1)1_G$$

Nel seguente diagramma è rappresentato il processo di costruzione di tali funzioni di classe attuato fino ad ora

$$\begin{array}{lll} \theta^G + \varphi(1)1_G = \varphi^* \longleftarrow \theta^G & & c\ell(G) \\ \uparrow & & \\ \varphi \longrightarrow \theta = \varphi - \varphi(1)1_H & & c\ell(H) \end{array}$$

Figura 7.2

Per costruzione θ è combinazione lineare a coefficienti interi di caratteri irriducibili di H e siccome la mappa di induzione è lineare, allora anche φ^* è combinazione lineare a coefficienti interi di caratteri irriducibili di G. Inoltre per le equazioni 7.3 e 7.4 vale

$$\begin{aligned} \left\langle \varphi^*, \varphi^* \right\rangle_G &= \left\langle \theta^G + \varphi(1)1_G, \theta^G + \varphi(1)1_G \right\rangle_G = \\ &= \left\langle \theta^G, \theta^G \right\rangle_G + \left\langle \theta^G, \varphi(1)1_G \right\rangle_G + \left\langle \varphi(1)1_G, \theta^G \right\rangle_G + \left\langle \varphi(1)1_G, \varphi(1)1_G \right\rangle_G = \\ &= 1 + \varphi(1)^2 - \varphi(1)^2 - \varphi(1)^2 + \varphi(1)^2 = 1 \end{aligned}$$

Dal tipo di decomposizione di φ^* nella base di $c\ell(G)$ si evince dunque che

$$\left\langle \varphi^*, \varphi^* \right\rangle_G = \sum_{i=1}^{k} {d_i}^2 = 1 \quad \text{con } d_i \in \mathbb{Z}$$

e ciò è vero se e solo se per un solo coefficiente ad esempio di indice j accade $d_j = \pm 1$ mentre tutti gli altri coefficienti sono nulli, ovvero se e solo se φ^* oppure $-\varphi^*$ sono caratteri irriducibili di G. Ma $\varphi^*(1) = \theta^G(1) + \varphi(1)1_G(1) = 0 + \varphi(1) = \varphi(1) > 0$, perciò si può concludere che $\varphi^* \in Irr(G)$ mentre $-\varphi^*$ non è neanche un carattere.
Sia ponga ora

$$M := \bigcap_{\varphi^* \in Irr(G)} Ker(\varphi^*)$$

dove chiaramente $M \trianglelefteq G$; si vuole provare che $M = N$, dove N è l'insieme definito nel lemma 7.3. Sia $x \in M \cap H$, allora siccome $x \in H$, per ogni $\varphi \in Irr(H)$ si ha $\varphi^*(x) = \theta^G(x) + \varphi(1)1_G(x) = \theta(x) + \varphi(1) = \varphi(x)$ mentre visto che $x \in M$ $\varphi^*(x) = \varphi^*(1) = \varphi(1)$. Quindi x appartiene all'intersezione dei nuclei di tutti i caratteri irriducibili di H, da cui segue che $x = 1$. Il sottogruppo M perciò è tale che $M \cap H = \{1\}$, dunque dal lemma 7.3 segue che $M \subseteq N$. Viceversa se $x \in N \setminus \{1\}$, ovvero se x non appartiene a nessun coniugato di H si ha:

$$\theta^G(x) = \frac{1}{|H|} \sum_{y \in G} \theta^o(y^{-1}xy) = 0$$

poiché $y^{-1}xy \in H$ se e solo se $x = yhy^{-1}$ per qualche $h \in H$. Allora si può riscrivere $\theta^G(x) = \varphi^*(x) - \varphi(1) = 0$ e quindi $x \in Ker(\varphi^*)$; data l'arbitrarietà di φ^* segue che $x \in M$. Riassumendo è stato provato che $N = M$ perciò N è un sottogruppo normale di G, inoltre nel lemma 7.3 si era visto che $N \cap H = \{1\}$ e che $N = |G : H|$; si conclude dunque che NH é un sottogruppo di G con cardinalità $|G : H||H| = |G|$, ovvero $NH = G$. È stato così provato che N é il nucleo di Frobenius. □

Si noti infine come la suddetta dimostrazione, nel caso in cui G sia un gruppo di Frobenius di complemento H, illustri un modo di indurre caratteri irriducibili di G da caratteri irriducibili di H e tale cosa non è di poco conto.