Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

TEOREMA DI HURWITZ

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
FABRIZIO CASELLI

Presentata da:
LUCIA DORE

II Sessione
Anno Accademico 2017/2018

Introduzione

Il teorema di Hurwitz, che deve il suo nome al matematico Adolf Hurwitz (1859-1919), è un'interessante risultato riguardante la composizione di forme quadratiche. Questo fu pubblicato postumo nel 1923, e, nel tempo, è stato dimostrato da vari matematici; in particolare, in tale elaborato, seguiremo la dimostrazione data da Eckmann nel 1943. La dimostrazione in analisi si basa sul concetto di rappresentazione di un gruppo, e dunque la tesi si concentra, in un primo momento, su tale argomento.

Il primo capitolo ha lo scopo di fornire le definizioni e alcuni risultati importanti, quali il Teorema di Maschke e il Lemma di Schur, riguardanti le rappresentazioni di gruppi. Il secondo capitolo, invece, vede la dimostrazione di quei teoremi di teoria della rappresentazione dei gruppi che risultano necessari nella dimostrazione di Eckmann; in particolare questi si concentrano sul concetto di rappresentazione irriducibile e di carattere di una rappresentazione.
L'argomento della tesi verrà quindi affrontato nel terzo capitolo, che si divide in due sezioni: la prima vede lo studio di un dato gruppo definito per generatori e relazioni, di cui poi si considereranno le rappresentazioni nella parte successiva; la seconda vede invece la dimostrazione del Teorema di Hurwitz come corollario di un teorema più generale.

Indice

Capitolo 1

Introduzione alle rappresentazioni di gruppi

Di seguito sono raccolte le definizioni e le proprietà principali riguardanti le rappresentazioni di gruppi, le quali saranno necessarie per la comprensione delle nozioni contenute nei capitoli successivi.
Fin da ora indicheremo con G un gruppo finito moltiplicativo, e con $\mathbb{C}$ il campo complesso. Questo a meno che non sia specificato diversamente.

1.1 Rappresentazioni matriciali

In questa sezione diamo una prima definizione di rappresentazione di un gruppo attraverso il concetto di matrice.
Indichiamo con $Mat_d(\mathbb{C})$ l'insieme delle matrici quadrate $d \times d$ a coefficienti in $\mathbb{C}$, e con GL_d l'insieme delle matrici $X \in Mat_d(\mathbb{C})$ invertibili rispetto alla moltiplicazione.

Definizione 1.1. Una **rappresentazione matriciale di un gruppo G** è un omomorfismo tra gruppi

$$\psi : G \to GL_d.$$

Equivalentemente, ad ogni $g \in G$, è assegnata una matrice $\psi(g) \in Mat_d(\mathbb{C})$ tale che

1. $\psi(\epsilon) = I_d$, dove ϵ è l'elemento neutro del gruppo G, ed I_d è la matrice identità $d \times d$,

2. $\psi(gh) = \psi(g)\psi(h)\ \forall g, h \in G$.

Il parametro d è detto il **grado**, o la **dimensione**, della rappresentazione.

Osservazione 1. Notiamo che le due condizioni implicano che $\psi(g^{-1}) = \psi(g)^{-1}$, poiché

$$I_n = \psi(\epsilon) = \psi(gg^{-1}) = \psi(g)\psi(g^{-1}).$$

Esempio 1. Ogni gruppo ha la **rappresentazione banale**, che associa ad ogni elemento $g \in G$ la matrice (1).
Questa è chiaramente una rappresentazione, infatti $\psi(\epsilon) = (1) = I_1$ e

$$\psi(g)\psi(h) = (1)(1) = (1) = \psi(gh) \quad \forall g, h \in G.$$

1.2 G-moduli e algebra gruppo

Poichè le matrici corrispondono alle trasformazioni lineari, possiamo pensare alle rappresentazioni di gruppi in questi termini.
Dato V uno spazio vettoriale, sia $GL(V)$ l'insieme delle trasformazioni lineari invertibili da V a V. Se $\dim V = d$ allora si ha che $GL(V)$ e GL_d sono isomorfi.

Definizione 1.2. Uno spazio vettoriale V è un **G-modulo** se esiste un omomorfismo di gruppi

$$\rho : G \to GL(V).$$

Equivalentemente V è un G-modulo se esiste una moltiplicazione fra elementi di V e di G tale che

1. $gv \in V$,
2. $g(cv + dw) = c(gv) + d(gw)$,
3. $(gh)v = g(hv)$,
4. $\epsilon v = v$

$\forall g, h \in G$; $v, w \in V$; e $c, d \in \mathbb{C}$.

Le due definizioni risultano essere equivalenti; infatti, data una rappresentazione $\psi : G \to GL(V)$, V risulta essere un G-modulo definendo l'azione di G come

$$gv := \psi(g)(v) \text{ per } g \in G, v \in V.$$

Viceversa, un G-modulo V definisce una rappresentazione $\psi : G \to GL(V)$ tale che

$$\psi(g)(v) := gv \text{ per } g \in G, v \in V.$$

Dunque lo studio delle rappresentazioni di G è equivalente allo studio dei G-moduli.

In futuro, il termine G-modulo sarà abbreviato in modulo, allorquando questo non crei confusione.

Definizione 1.3. Diremo che G **agisce su un insieme** S, se quest'ultimo è dotato di una moltiplicazione per elementi di G che soddisfi le condizioni 1, 3 e 4.

Osservazione 2. Notiamo che, se un gruppo G agisce su un insieme S, è sempre possibile definire il G-modulo $\mathbb{C}S$ come segue.
Sia $\mathbb{C}S = \left\{c_1 s_1 + c_2 s_2 + \ldots + c_n s_n;\ c_i \in \mathbb{C} \quad \forall i\right\}$ lo spazio vettoriale generato da S su $\mathbb{C}$, su cui sono definite le operazioni di somma e di prodotto per scalare come:

$$\begin{aligned}(c_1 s_1 + c_2 s_2 + \ldots + c_n s_n) + (d_1 s_1 + d_2 s_2 + \ldots + d_n s_n) = \\ = (c_1 + d_1)s_1 + (c_2 + d_2)s_2 + \ldots + (c_n + d_n)s_n\end{aligned}$$

e

$$c(c_1 s_1 + c_2 s_2 + \ldots + c_n s_n) = (cc_1)s_1 + (cc_2)s_2 + \ldots + (cc_n)s_n.$$

$\mathbb{C}S$ è un modulo se si estende l'azione di G su $\mathbb{C}S$ per linearità, cioè:

$$g(c_1 s_1 + c_2 s_2 + \ldots + c_n s_n) = c_1(gs_1) + c_2(gs_2) + \ldots + c_n(gs_n) \quad \forall g \in G.$$

Definizione 1.4. L'**algebra gruppo di** G è l'algebra

$$\mathbb{C}[G] = \left\{c_1 g_1 + c_2 g_2 + \ldots + c_n g_n;\ c_i \in \mathbb{C} \quad \forall i\right\}.$$

Questa è uno spazio vettoriale per quanto detto sopra, e risulta inoltre essere un'algebra estendendo linearmente il prodotto in G.

Osservazione 3. Notiamo che G agisce su se stesso attraverso la moltiplicazione sinistra: se $g \in G$ e $h \in S = G$, allora l'azione di g su h, gh, è definita come il prodotto usuale del gruppo. Le proprietà 1, 3 e 4 seguono rispettivamente dalla chiusura, dall'associatività e dalla definizione dell'elemento neutro del gruppo.
Si estende quindi l'azione di G sull'algebra gruppo $\mathbb{C}[G]$, che risulta essere un G-modulo.

Definizione 1.5. Data $\tau : G \to GL(\mathbb{C}[G])$, questa è detta la **rappresentazione regolare (sinistra)** se

$$\tau(a) = T_a$$

dove $T_a(x) = ax\ \forall a, x \in G$.

1.3 Riducibilità delle rappresentazioni

Alcune rappresentazioni possono essere costruite a partire da rappresentazioni di dimensione inferiore, mentre altre risultano essere "indivisibili". È da questo concetto che nascono le nozioni di rappresentazioni riducibili e irriducibili, che verranno analizzate in questa sezione.

Definizione 1.6. Se V è un G-modulo, definiamo un **sottomodulo di V** un sottospazio W che è chiuso rispetto all'azione di G, i.e.,

$$w \in W \Rightarrow gw \in W \quad \forall g \in G.$$

Equivalentemente, W è esso stesso un G-modulo.

Esempio 2. Ogni G-modulo V ha come sottomoduli $W = V$ e $W = \{0\}$, che sono detti **sottomoduli banali**. Tutti gli altri sottomoduli sono detti **non banali**.

Definizione 1.7. Un G-modulo V, non nullo, si dice **riducibile** se contiene un sottomodulo W non banale. È detto **irriducibile** altrimenti.

Proposizione 1.3.1. *Un G-modulo V è riducibile se e solo se esiste $0 < f < \dim V$ ed una base $\mathcal{B}$ tale che ad ogni $g \in G$ corrisponde una matrice a blocchi della forma*

$$X(g) = \left(\begin{array}{c|c} A(g) & B(g) \\ \hline 0 & C(g) \end{array}\right)$$

dove $A(g)$ è una matrice quadrata di ordine f e 0 è una matrice non vuota di zeri.

Dimostrazione. Sia V di dimensione d, e sia W un sottomodulo di V di dimensione f, tale che $0\langle f\langle d$. Sia

$$\mathcal{B} = \{w_1, w_2, \ldots, w_f, v_{f+1}, v_{f+2}, \ldots, v_d\}$$

una base di V tale che i primi f vettori siano una base per W. Poichè W è un sottomodulo, $gw_i \in W \ \forall i = 1, \ldots, f$; dunque le ultime $d-f$ coordinate di gw_i saranno tutte zero. Questo ci assicura che il blocco in basso a sinistra della matrice $X(g)$ sia una matrice di zeri. Inoltre la matrice $A(g)$ risulta essere quadrata, in quanto restrizione di G a W.
Viceversa, supponiamo che $X(g)$ sia della forma data, e $A(g)$ abbia ordine f. Consideriamo $W = \mathbb{C}\langle e_1, e_2, \ldots, e_f\rangle$, dove gli e_i rappresentano i vettori della base canonica di $\mathbb{C}^d$.
$X(g)e_i \in W$ per $1 \leq i \leq f$ a causa del blocco di zeri in basso a sinistra nella matrice $X(g)$; quindi W è un sottomodulo di G, ed è non banale poichè la matrice di zeri è non vuota. □

Osservazione 4. Ogni rappresentazione di grado 1 è chiaramente irriducibile.

1.4 Teorema di Maschke

Il teorema di Maschke, che in questa sezione andremo a dimostrare, ci permette di scomporre ogni G-modulo, e quindi ogni rappresentazione, nelle sue componenti irriducibili.

Definizione 1.8. Sia V uno spazio vettoriale e siano U e W sottospazi di V; diremo allora che V è **somma diretta di U e W**, scritto $U \oplus W$, se ogni $v \in V$ può essere scritto in modo unico come

$$v = u + w, \quad u \in U, \quad w \in W.$$

Se V è un modulo e U, W sono sottomoduli, allora diremo che U **e** W **sono complementari**.

Definizione 1.9. Data una matrice X, questa è **somma diretta di matrici** A **e** B, $X = A \oplus B$, se è nella forma diagonale a blocchi

$$X = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$$

Osservazione 5. Notiamo che le due definizioni date di somma diretta per spazi vettoriali e per matrici sono ben definite allorquando si stiano considerando dei G-moduli e le rispettive rappresentazioni di G; infatti:
dato $V = U \oplus W$, sia

$$\mathcal{B} = \{u_1, u_2, \ldots, u_f, w_{f+1}, w_{f+2}, \ldots, w_d\}$$

una base di V tale che i primi f vettori sono una base per U, mentre i restanti $d - f$ sono una base per W.
Poichè U e W sono sottomoduli, abbiamo che

$$gu_i \in U \text{ e } gw_j \in W \quad \forall g \in G, \quad \forall u_i \in U \text{ e } \forall w_j \in W.$$

Allora per ogni $g \in G$ la matrice rispetto alla base $\mathcal{B}$ sarà nella forma:

$$X(g) = \left(\begin{array}{c|c} A(g) & 0 \\ \hline 0 & B(g) \end{array}\right)$$

dove $A(g)$ e $B(g)$ sono le matrici dell'azione di G ristretta, rispettivamente, a U e a W.

Definizione 1.10. Dato V uno spazio vettoriale su $\mathbb{C}$, definiamo un **prodotto hermitiano** su V un'applicazione $\langle . \ , . \rangle : V \times V \to \mathbb{C}$ t.c.

1. $\forall w \in V \quad v \mapsto \langle v, w \rangle$ è lineare,

2. $\langle w, v\rangle = \overline{\langle v, w\rangle}$,

3. $\langle v, v\rangle \geq 0 \quad \forall v \in V, \quad \langle v, v\rangle = 0 \Leftrightarrow v = 0$.

Un prodotto hermitiano si dice **invariante sotto l'azione di** G se vale

$$\langle gv, gw\rangle = \langle v, w\rangle \quad \forall g \in G \text{ e } \forall v, w \in V.$$

Definizione 1.11. Sia V uno spazio vettoriale e sia W un suo sottospazio; il sottospazio di V

$$W^{\perp} = \left\{v \in V; \ \langle v, w\rangle = 0 \quad \forall w \in W\right\}$$

è detto **complementare ortogonale** di W.

Osservazione 6. È sempre vero che $V = W \oplus W^{\perp}$.

Proposizione 1.4.1. *Se V è un G-modulo, W un suo sottomodulo, e $\langle .\ ,\ .\rangle$ un prodotto hermitiano invariante sotto l'azione di G, allora anche $W^{\perp}$ è un G-sottomodulo.*

Dimostrazione. Sia $u \in W^{\perp}$ e $w \in W$; allora

$$\begin{aligned}\langle gu, w\rangle &= \langle g^{-1}gu, g^{-1}w\rangle && \text{(per l'invarianza di g)}\\ &= \langle u, g^{-1}w\rangle \\ &= 0 && (u \in W^{\perp}, \text{ e } g^{-1}w \in W \text{ poichè } W \text{ è un sottomodulo}).\end{aligned}$$

□

Teorema 1.4.2 (Teorema di Maschke)**.** *Sia G un gruppo finito e V un G-modulo non nullo, allora*

$$V = W^{(1)} \oplus W^{(2)} \oplus \ldots \oplus W^{(k)}$$

dove ogni $W^{(i)}$ per $i = 1, 2, \ldots, k$ è un sottomodulo irriducibile di V.

Dimostrazione. Procediamo per induzione su $d = \dim V$.
Se $d = 1$, allora V è irriducibile e si ha $k = 1$ e $W^{(1)} = V$.
Supponiamo quindi $d > 1$. Se V è irriducibile ricadiamo nel caso precedente; possiamo allora suppore che V sia riducibile, e dunque abbia un sottomodulo W non banale.
Sia $\mathcal{B} = \left\{v_1, v_2, \ldots, v_d\right\}$ una base di V e $\langle .\ ,\ .\rangle$ l'unico prodotto hermitiano che soddisfa

$$\langle v_i, v_j\rangle = \delta_{i,j}$$

per gli elementi della base, dove $\delta_{i,j}$ è la delta di Kronecher. A partire da questo, definiamo un secondo prodotto hermitiano ponendo

$$\langle v, w\rangle' = \sum_{g\in G}\langle gv, gw\rangle, \quad \forall v, w \in V.$$

Abbiamo che $\langle .\ ,\ .\rangle$ risulta chiaramente essere un prodotto hermitiano, e verifichiamo che questo è G-invariante; infatti $\forall h \in G$ e $\forall v, w \in V$ si ha:

$$\begin{aligned}\langle hv, hw\rangle' &= \sum_{g\in G}\langle ghv, ghw\rangle \\ &= \sum_{f\in G}\langle fv, fw\rangle \qquad (f = gh, \text{ che è ancora un elemento di } G) \\ &= \langle v, w\rangle'.\end{aligned}$$

Definiamo $W^\perp = \{v \in V : \quad \langle v, w\rangle' = 0\}$; allora per la proposizione 1.4.1 si ha che $W^\perp$ è un sottomodulo di V tale che

$$V = W \oplus W^\perp.$$

Si ha che $\dim W, \dim W^\perp < d$, possiamo quindi applicare l'induzione su W e $W^\perp$ ed otteniamo il risultato cercato. □

Corollario 1.4.3. *Sia G un gruppo finito e X una sua rappresentazione matriciale di dimensione $d > 0$, allora esiste una matrice T tale che ogni matrice $X(g)$, $g \in G$, è della forma*

$$TX(g)T^{-1} = \begin{pmatrix} X^{(1)}(g) & 0 & \dots & 0 \\ 0 & X^{(2)}(g) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & X^{(k)}(g) \end{pmatrix},$$

dove ogni $X^{(i)}$ è una rappresentazione matriciale irriducibile di G.

Dimostrazione. Sia $V = \mathbb{C}^d$ su cui è definita l'azione di G

$$gv = X(g)v \quad \forall g \in G \text{ e } \forall v \in V.$$

Per il teorema di Maschke, si ha che

$$V = W^{(1)} \oplus W^{(2)} \oplus \dots \oplus W^{(k)},$$

dove ogni $W^{(i)}$ è un sottomodulo irriducibile di dimensione d_i. Si consideri una base $\mathcal{B}$ di V tale che i primi d_1 vettori sono una base per $W^{(1)}$, i seguenti d_2 lo sono per $W^{(2)}$, etc; allora T è la matrice di cambiamento di base dalla base canonica di $\mathbb{C}^d$ alla base $\mathcal{B}$. □

1.5 G-omomorfismo e Lemma di Schur

Lo studio dei G-moduli può essere approfondito attraverso l'introduzione di una funzione che preservi le operazioni, detta G-omomorfismo. Il lemma di Schur ci permette di compiere, attraverso la nozione di G-omomorfismo, interessanti osservazioni sui G-moduli definiti sul campo complesso.

Definizione 1.12. Siano V e W due G-moduli, una trasformazione lineare $\theta : V \to W$ tale che

$$\theta(gv) = g\theta(v) \quad \forall g \in G \text{ e } v \in V$$

è detta **G-omomorfismo**; in tal caso V e W sono detti **G-omomorfi**.
Se θ risulta essere biettiva, allora è detta **G-isomorfismo**. .

Se non vi sono rischi di confusione, si scriverà omomorfismo in luogo di G-omomorfismo, ed analogamente per isomorfismo.

Definizione 1.13. Siano ψ e θ due rappresentazioni di G; queste sono dette **equivalenti** se V e W sono G-isomorfi, $V \cong W$. Altrimenti sono dette **inequivalenti**.

$$\begin{array}{ccccc} & V & \underrightarrow{P} & W & \\ \psi(g) & \downarrow & & \downarrow & \theta(g) \\ & V & \underrightarrow{P} & W & \end{array}$$

Dal diagramma si evince che $P\theta(g) = \psi(g)P \quad \forall g \in G$, dove $P : V \to W$ è un omomorfismo. Se P è biettiva, e dunque un isomorfismo, la condizione precedente è equivalente a $\theta(g) = P^{-1}\psi(g)P \quad \forall g \in G$; questa risulta essere una relazione di equivalenza.
Quando si parlerà di rappresentazione, spesso si parlerà in realtà di classi di equivalenza stesse.

Proposizione 1.5.1. *Sia $\theta : V \to W$ un G-omomorfismo, allora*

1. $\ker\theta$ *è un sottomodulo di* V,
2. $\mathrm{Im}\,\theta$ *è un sottomodulo di* W.

Dimostrazione. 1. Sappiamo, dalla teoria degli spazi vettoriali, che $\ker\theta$ è un sottospazio vettoriale di V, dobbiamo quindi verificarne la chiusura rispetto all'azione di G.

$$\begin{aligned} \theta(gv) &= g\theta(v) && \text{(poichè } \theta \text{ è un omomorfismo)} \\ &= g0 && (\mathrm{v} \in \ker\theta) \\ &= 0 \end{aligned}$$

Dunque $gv \in \ker\theta$.

2. Analogamente, dovremo solo verificare la chiusura di W rispetto all'azione di G. Per la chiusura di V rispetto all'azione di G, si ha che $gv \in V \quad \forall v \in V$; allora $\theta(gv) \in \operatorname{Im}\theta$ per definizione di $\operatorname{Im}\theta := \{w \in W | w = \theta(v) \text{ per un certo } v \in V\}$. Poiché $g\theta(v) = \theta(gv)$, allora $g\theta(v) \in \operatorname{Im}\theta$.

□

Teorema 1.5.2 (Lemma di Schur)**.** *Siano V e W due G-moduli irriducibili. Se $\theta : V \to W$ è un G-omomorfismo, allora*

1. *θ è un G-isomorfismo, oppure*

2. *θ è l'applicazione identicamente nulla.*

Dimostrazione. Poichè V è irriducibile, i suoi unici sottomoduli sono $\{0\}$ e V stesso. Per la proposizione 1.5.1 $\ker\theta$ è un sottomodulo di V, dunque si ha che $\ker\theta = \{0\}$ oppure $\ker\theta = V$. Analogamente l'irriducibilità di W comporta che $\operatorname{Im} W = \{0\}$ o $\operatorname{Im}\theta = W$.
Se $\ker\theta = V$, o $\operatorname{Im}\theta = \{0\}$ allora θ è l'applicazione identicamente nulla. Viceversa, se $\ker\theta = \{0\}$ e $\operatorname{Im}\theta = W$, θ sarà un G-isomorfismo, poichè si ha la biettività. □

Analogamente, in termini matriciali:

Corollario 1.5.3. *Siano X e Y due rappresentazioni matriciali irriducibili di G. Se T è una matrice tale che $TX(g) = Y(g)T \quad \forall g \in G$, allora*

1. *T è invertibile, oppure*

2. *T è la matrice nulla.*

Corollario 1.5.4. *Dato V un modulo irriducibile e $\theta : V \to V$ un omomorfismo non nullo, allora*

$$\theta(v) = \lambda \quad \lambda \in \mathbb{C},\ \forall v \in V.$$

Dimostrazione. Poiché $\mathbb{C}$ è algebricamente chiuso, esiste un autovalore $\lambda \in \mathbb{C}$ tale che $\theta - \lambda I$ è un'applicazione con nucleo non banale. Per il lemma di Schur, si ha che allora $\theta - \lambda I = 0$, e quindi $\theta = \lambda I$. □

Analogamente:

Corollario 1.5.5. *Data X una rappresentazione matriciale irriducibile di G, allora tutte e sole le matrici T che commutano con $X(g)$, $\forall g \in G$, sono della forma $T = \lambda I$ con $\lambda \in \mathbb{C}$.*

Corollario 1.5.6. *Se G è abeliano, allora le sue rappresentazioni irriducibili sono di grado 1.*

Dimostrazione. Consideriamo V un modulo irriducibile e $\psi : G \to GL(V)$ una rappresentazione di G. Per comodità useremo in questa dimostrazione la notazione $g.v := \psi(g)(v)$. Dato $g \in G$, sia $\rho : V \to V$ l'applicazione tale che $\rho(v) = g.v$. Questa si dimostra essere un omomorfismo, infatti $\forall g, g' \in G$ si ha:

$$g.(g'.v) = gg'.v$$

e

$$g'.(g.v) = g'g.v.$$

Ma $gg'.v = g'g.v$ poichè G è abeliano per ipotesi. Allora, per il corollario 1.5.4, esiste λ tale che

$$g.v = \lambda v \quad \forall g \in G,\ \forall v \in V.$$

Quindi ogni sottospazio è un sottomodulo, ma poichè V è irriducibile per ipotesi, questo deve avere dimensione 1, così da non avere sottospazi non banali. □

1.6 Algebra commutante e prodotto tensoriale

Il corollario 1.5.5 suggerisce che l'insieme delle matrici che commutano con le matrici di una data rappresentazione abbiano particolare rilevanza. Questo, per i G-moduli, corrisponde all'insieme dei G-omomorfismi da un G-modulo a se stesso. In questa sezione andremo quindi a caratterizzare tali insiemi.

Definizione 1.14. Data una rappresentazione matriciale $X : G \to GL_d$, l'**algebra commutante** risulta essere

$$\mathrm{Com}X = \left\{T \in Mat_d(\mathbb{C}) \ ; \ TX(g) = X(g)T \quad \forall g \in G\right\}.$$

Definizione 1.15. Dato V un G-modulo, l'**algebra degli endomorfismi** risulta essere

$$\mathrm{End}V = \left\{\theta : V \to V \ ; \ \theta \text{ è un G-omomorfismo}\right\}.$$

Osservazione 7. Tali definizioni soddisfano gli assiomi di un'algebra. Inoltre, se V è il G-modulo corrispondente alla rappresentazione matriciale X; si ha che Com$X$ e End$V$ sono isomorfi come algebre.

Proposizione 1.6.1. *Se $X = \bigoplus_{i=1}^{k} X^{(i)}$, dove gli $X^{(i)}$ sono le componenti irriducibili inequivalenti, allora*

$$ComX = \left\{\bigoplus_{i=1}^{k} c_i I_{d_i} \ ; \ c_i \in \mathbb{C}\right\},$$

dove d_i è il grado di $X^{(i)}$.

Osservazione 8. Si noti che allora $\deg X = \sum_{i=1}^{k} d_i$; e $\dim \mathrm{Com}X = k$.

Dimostrazione. Ci limitiamo a dimostrare l'enunciato per $k = 2$. Per il corollario 1.4.3 possiamo supporre che la matrice X sia della forma

$$X = \begin{pmatrix} X^{(1)} & 0 \\ 0 & X^{(2)} \end{pmatrix}$$

senza perdere di generalità.
Consideriamo la matrice

$$T = \begin{pmatrix} T_{1,1} & T_{1,2} \\ T_{2,1} & T_{2,2} \end{pmatrix}$$

tale che $TX = XT$. Tale uguaglianza, una volta svolta la moltiplicazione, risulta essere

$$\begin{pmatrix} T_{1,1}X^{(1)} & T_{1,2}X^{(2)} \\ T_{2,1}X^{(1)} & T_{2,2}X^{(2)} \end{pmatrix} = \begin{pmatrix} X^{(1)}T_{1,1} & X^{(1)}T_{1,2} \\ X^{(2)}T_{2,1} & X^{(2)}T_{2,2} \end{pmatrix}.$$

Equivalentemente

$$\begin{aligned} T_{1,1}X^{(1)} &= X^{(1)}T_{1,1} \\ T_{1,2}X^{(2)} &= X^{(1)}T_{1,2} \\ T_{2,1}X^{(1)} &= X^{(2)}T_{2,1} \\ T_{2,2}X^{(2)} &= X^{(2)}T_{2,2}. \end{aligned}$$

Grazie ai risultati esposti nel corollario 1.5.5, ed alla non equivalenza di $X^{(1)}$ e di $X^{(2)}$, si ha che

$$T_{1,1} = c_1 I_{d_1}, \quad T_{1,2} = T_{2,1} = 0, \quad T_{2,2} = c_2 I_{d_2},$$

dove $c_1, c_2 \in \mathbb{C}$. Dunque

$$T = \begin{pmatrix} c_1 I_{d_1} & 0 \\ 0 & c_2 I_{d_2} \end{pmatrix}.$$

□

Definizione 1.16. $mX := \overbrace{X \oplus X \oplus \ldots \oplus X}^{\text{m volte}}$, $m \in \mathbb{N}$; ovvero X è somma di m rappresentazioni equivalenti, dove m è detta **molteplicità di** X.

Proposizione 1.6.2. *Se $X = mX^{(1)}$, dove $X^{(1)}$ è una rappresentazione irriducibile, allora*

$$Com X = \left\{ \begin{pmatrix} c_{1,1}I_d & \ldots & c_{1,m}I_d \\ \vdots & \ddots & \vdots \\ c_{m,1}I_d & \ldots & c_{m,m}I_d \end{pmatrix} \; ; \, c_{i,j} \in \mathbb{C} \quad \forall i,j \right\}$$

dove $d = \deg X^{(1)}$.

Dimostrazione. Ci limitiamo a dimostrare l'enunciato per $m = 2$.
Analogamente alla dimostrazione 1.6, consideriamo X della forma

$$X = \begin{pmatrix} X^{(1)} & 0 \\ 0 & X^{(1)} \end{pmatrix}$$

Svolgendo il prodotto $TX = XT$ otteniamo quattro equazioni, della forma

$$T_{i,j}X^{(1)} = X^{(1)}T_{i,j} \quad \forall i, j = 1, 2.$$

Grazie all'osservazione 1.5.5, otteniamo

$$T_{i,j} = c_{i,j}I_d,$$

con $c_{i,j} \in \mathbb{C}$. □

Definizione 1.17. Siano $X = (x_{i,j})$ e Y due matrici, il loro **prodotto tensoriale** è la matrice a blocchi

$$X \otimes Y = (x_{i,j}Y) = \begin{pmatrix} x_{1,1}Y & x_{1,2}Y & \dots \\ x_{2,1}Y & x_{2,2}Y & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}.$$

Osservazione 9. Si noti che se $X = mX^{(1)}$, allora $T \in \mathrm{Com}X$ può essere scritto come

$$T = \begin{pmatrix} c_{1,1} & \dots & c_{1,m} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \dots & c_{m,m} \end{pmatrix} \otimes I_d =: M_m \otimes I_d.$$

Proposizione 1.6.3. *Se $X = m_1X^{(1)} \oplus m_2X^{(2)} \oplus \ldots \oplus m_kX^{(k)}$, dove $X^{(i)}$ sono rappresentazioni irriducibili inequivalenti di grado d_i, allora*

$$ComX = \left\{ \oplus_{i=1}^{k} (M_{m_i} \otimes I_{d_i}) \ ; \ M_{m_i} \in Mat_{m_i} \quad \forall i \right\}.$$

Dimostrazione. Tale enunciato è ovvio, combinando i risultati delle proposizioni 1.6.1, 1.6.2 e dell'osservazione 9. □

Osservazione 10. Se $X = m_1X^{(1)} \oplus m_2X^{(2)} \oplus \ldots \oplus m_kX^{(k)}$ allora si ha

$$\deg X = m_1 \deg X^{(1)} + m_2 \deg X^{(2)} + \ldots + m_k \deg X^{(k)} = m_1d_1 + m_2d_2 + \ldots + m_kd_k$$

e

$$\dim \mathrm{Com}X = \dim M_{m_1} + \dim M_{m_2} + \ldots + \dim M_{m_k} = m_1^2 + m_2^2 + \ldots + m_k^2.$$

Definizione 1.18. Sia A un'algebra, il suo **centro** è l'insieme

$$Z_A = \left\{ a \in A \ ; \ ab = ba \quad \forall b \in A \right\}.$$

Proposizione 1.6.4. *Il centro di Mat_d è*

$$Z_{Mat_d} = \left\{ cI_d \ ; \ c \in \mathbb{C} \right\}.$$

Dimostrazione. Consideriamo $C \in Z_{Mat_d}$, si ha che

$$CE_{i,i} = E_{i,i}C \quad \forall i = 1, \ldots, d$$

dove $E_{i,i}$ è la matrice della base canonica, che ha tutti gli elementi nulli, eccetto l'elemento di posto (i,i). Notiamo che

$$CE_{i,i} = \begin{pmatrix} c_{1,1} & \ldots & c_{1,i} & \ldots & c_{1,d} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{i,1} & \ldots & c_{i,i} & \ldots & c_{i,d} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{d,1} & \ldots & c_{d,i} & \ldots & c_{d,d} \end{pmatrix} \begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 1 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix} = \begin{pmatrix} 0 & \ldots & c_{1,i} & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & c_{i,i} & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & c_{d,i} & \ldots & 0 \end{pmatrix}$$

e, analogamente,

$$E_{i,i}C = \begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{i,1} & \ldots & c_{i,i} & \ldots & c_{i,d} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}.$$

Poichè $CE_{i,i} = E_{i,i}C$, si ha che

$$c_{i,j} = 0 \quad \forall j \neq i,$$

ovvero C è una matrice diagonale. Similarmente, se $j \neq i$, si ha che

$$C(E_{i,j} + E_{j,i}) = (E_{i,j} + E_{j,i})C.$$

Da tale uguaglianza si ottiene che tutti gli elementi della diagonale di C devono essere uguali, $c_{1,1} = c_{2,2} = \ldots = c_{d,d} =: c$; dunque $C = cI_d$.
Chiaramente le matrici di questa forma commutano con ogni altra matrice. □

Lemma 1.6.5. *Date $A, X \in Mat_d$ e $B, Y \in Mat_f$, si ha che*

1. $(A \oplus B)(X \oplus Y) = AX \oplus BY$,
2. $(A \otimes B)(X \otimes Y) = AX \otimes BY$.

Dimostrazione. 1.

$$(A \oplus B)(X \oplus Y) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) \left(\begin{array}{c|c} X & 0 \\ \hline 0 & Y \end{array}\right) = \left(\begin{array}{c|c} AX & 0 \\ \hline 0 & BY \end{array}\right) = AX \oplus AY$$

2.

$$\begin{aligned}(A\otimes B)(X\otimes Y) &= (a_{i,j}B)(x_{i,j}Y) && \text{(definizione di } \otimes)\\ &= (\sum_k a_{i,k}Bx_{k,j}Y) && \text{(moltiplicazione a blocchi)}\\ &= ((\sum_k a_{i,k}x_{k,j})BY) && \text{(distributività)}\\ &= AX\otimes BY && \text{(definizione di } \otimes)\end{aligned}$$

□

Proposizione 1.6.6. *Data $X = m_1X^{(1)} \oplus m_2X^{(2)} \oplus \ldots \oplus m_kX^{(k)}$, dove $X^{(i)}$ sono rappresentazioni irriducibili inequivalenti di grado d_i, si ha che*

$$Z_{ComX} = \left\{ \begin{pmatrix} c_1I_{m_1d_1} & 0 & \ldots & 0 \\ 0 & c_2I_{m_2d_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & c_kI_{m_kd_k} \end{pmatrix} ; c_i \in \mathbb{C} \quad \forall i \right\}.$$

Dimostrazione. Sia $C \in \mathrm{Com}X$, tale che

$$CT = TC \quad \forall T \in \mathrm{Com}X.$$

Poichè sia T che $C \in \mathrm{Com}X$ si ha, per la proposizione 1.6.3,

$$T = \oplus_{i=1}^k (M_{m_i} \otimes I_{d_i}) \text{ e } C = \oplus_{i=1}^k (C_{m_i} \otimes I_{d_i}).$$

Allora

$$\begin{aligned}CT &= (\oplus_{i=1}^k C_{m_i} \otimes I_{d_i})(\oplus_{i=1}^k M_{m_i} \otimes I_{d_i})\\ &= \oplus_{i=1}^k (C_{m_i} \otimes I_{d_i})(M_{m_i} \otimes I_{d_i}) && \text{(per il punto 1 del lemma 1.6.5)}\\ &= \oplus_{i=1}^k (C_{m_i}M_{m_i} \otimes I_{d_i}) && \text{(per il punto 2 del lemma 1.6.5).}\end{aligned}$$

Analogamente

$$TC = \oplus_{i=1}^k (M_{m_i}C_{m_i} \otimes I_{d_i}).$$

Allora $CT = TC$ se e solo se

$$C_{m_i}M_{m_i} = M_{m_i}C_{m_i} \quad \forall M_{m_i} \in Mat_{m_i},$$

ovvero se e solo se $C_{m_i} \in Z_{Mat_{m_i}}$; dunque, per la proposizione 1.6.4,

$$C_{m_i} = c_iI_{m_i}$$

per un certo $c_i \in \mathbb{C}$. Quindi

$$\begin{aligned} C &= \bigoplus_{i=1}^{k} c_i I_{m_i} \otimes I_{d_i} \\ &= \bigoplus_{i=1}^{k} c_i I_{m_i d_i} \\ &= \begin{pmatrix} c_1 I_{m_1 d_1} & 0 & \dots & 0 \\ 0 & c_2 I_{m_2 d_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & c_k I_{m_k d_k} \end{pmatrix}. \end{aligned}$$

□

Osservazione 11. Si noti che $\dim Z_{\mathrm{Com}X} = k$.
Riassumiamo i precedenti risultati nel seguente teorema:

Teorema 1.6.7. *Sia X una rappresentazione matriciale tale che*

$$X = m_1 X^{(1)} \oplus m_2 X^{(2)} \oplus \ldots \oplus m_k X^{(k)},$$

dove le $X^{(i)}$ sono rappresentazioni irriducibili inequivalenti di grado d_i; allora

1. $\deg X = m_1 d_1 + m_2 d_2 + \ldots + m_k d_k$,
2. $ComX = \left\{ \bigoplus_{i=1}^{k} (M_{m_i} \otimes I_{d_i});\ M_{m_i} \in Mat_{m_i} \quad \forall i \right\}$,
3. $\dim(ComX) = m_1^2 + m_2^2 + \ldots + m_k^2$,
4. $Z_{ComX} = \left\{ \bigoplus_{i=1}^{k} c_i I_{m_i d_i}\ ;\ c_i \in \mathbb{C} \quad \forall i \right\}$,
5. $\dim Z_{ComX} = k$.

Tale risultato può essere riformulato in termini di G-moduli nel modo seguente:

Teorema 1.6.8. *Sia V un G-modulo tale che*

$$V = m_1 V^{(1)} \oplus m_2 V^{(2)} \oplus \ldots \oplus m_k V^{(k)},$$

dove i $V^{(i)}$ sono G-moduli irriducibili inequivalenti di grado d_i; allora

1. $\dim V = m_1 d_1 + m_2 d_2 + \ldots + m_k d_k$,
2. $EndV \cong \bigoplus_{i=1}^{k} Mat_{m_i}$,
3. $\dim(EndV) = m_1^2 + m_2^2 + \ldots + m_k^2$,
4. Z_{EndV} *è isomorfo all'algebra delle matrici diagonali di grado k,*
5. $\dim Z_{EndV} = k$.

1.7 Carattere di una rappresentazione

In questa sezione si introduce la nozione di carattere di una rappresentazione, che fornisce importanti risultati sulle rappresentazioni irriducibili, come vedremo nel secondo capitolo.

Definizione 1.19. Sia ψ una rappresentazione di G, definiamo il **carattere** di ψ, χ_ψ, come $\chi_\psi(g) = tr\psi(g)$.
Se non vi è il rischio di fraintendimenti, si scriverà χ in luogo di χ_ψ.

Osservazione 12. Si noti che il carattere di una rappresentazione non dipende da ψ, ma dalla sua classe di equivalenza; infatti, se ψ e θ sono equivalenti si ha

$$\chi_\theta(g) = tr\theta(g) = trP^{-1}\psi(g)P = tr\psi(g) = \chi_\psi(g).$$

Osservazione 13. Dato $G = \{g_1, g_2, \ldots, g_n\}$, consideriamo la rappresentazione regolare su $\mathbb{C}$[G], e chiamiamo $\chi^{reg}(g)$ il suo carattere. Poichè $X(\epsilon) = I_n$, si ha che $\chi^{reg}(\epsilon) = o(G)$.
Consideriamo la base $\mathcal{B} = \{g_1, g_2, \ldots, g_n\}$. Dato $g \in G, g \neq \epsilon$, $X(g)$ è la matrice di permutazione per l'azione di g in $\mathcal{B}$, quindi $\chi^{reg}(g)$ è il numero di valori fissati dall'azione di g. Ma se $gg_i = g_i$ allora $g = \epsilon$, e questo è assurdo; dunque non vi sono valori fissati per $g \neq \epsilon$. Riassumendo

$$\chi^{reg}(g) = \begin{cases} o(G) & \text{se } g = \epsilon, \\ 0 & altrimenti. \end{cases}$$

1.8 Rappresentazioni di algebre

Data A un'algebra finito-dimensionale, possiamo estendere a questa il concetto di rappresentazione e, conseguentemente, i risultati visti in tale capitolo. Dato V uno spazio vettoriale, indichiamo con $End(V)$ l'insieme degli endomorfismi di V.

Definizione 1.20. Dato V uno spazio vettoriale di dimensione finita, una **rappresentazione di** A è un omomorfismo tra algebre

$$\phi : A \to End(V).$$

Tale applicazione soddisfa quindi

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$,
3. $\phi(\alpha a) = \alpha\phi(a)$,

4. $\phi(\epsilon) = 1$

$\forall a, b \in A, \forall \alpha \in \mathbb{C}$ ed ϵ è l'elemento neutro di A.

Osservazione 14. Se G agisce su un certo V, si ha che anche $\mathbb{C}[G]$ agisce su quest'ultimo nel modo seguente:

$$(c_1 g_1 + c_2 g_2 + \ldots + c_n g_n)v = c_1(g_1 v) + c_2(g_2 v) + \ldots + c_n(g_n v).$$

Osservazione 15. I risultati ottenuti in tale elaborato sulle rappresentazioni dei gruppi sono estendibili anche alle rappresentazioni di algebre.

Capitolo 2

Teoremi sulle rappresentazioni di gruppi

In questo capitolo saranno enunciati e dimostrati taluni teoremi di teoria della rappresentazione dei gruppi necessari alla dimostrazione del teorema di Hurwitz, che verrà affrontata nel terzo capitolo.

2.1 Prodotto hermitiano di caratteri

Lo studio del carattere di una rappresentazione è un valido strumento per determinare quando una rappresentazione è irriducibile; inoltre questo ci permette di dimostrare che il numero di irriducibili è uguale al numero delle classi di coniugio.

Possiamo pensare al carattere χ di un gruppo $G = \{g_1, g_2, \ldots, g_n\}$ come un vettore riga di numeri complessi:

$$\chi = (\chi(g_1), \chi(g_2), \ldots, \chi(g_n)).$$

Definizione 2.1. Dato $a \in G$, definiamo la **classe di coniugio** di g l'insieme

$$C(g) = \left\{aga^{-1} \ ; \ a \in G\right\}.$$

Definizione 2.2. Date $\chi, \xi : G \to \mathbb{C}$, il **prodotto hermitiano** di χ e ξ è

$$\langle \chi, \xi \rangle = \frac{1}{o(G)} \sum_{g \in G} \chi(g)\overline{\xi(g)}.$$

Proposizione 2.1.1. *Siano χ e ξ due caratteri, allora*

$$\langle \chi, \xi \rangle = \frac{1}{o(G)} \sum_{g \in G} \chi(g)\xi(g^{-1}). \tag{2.1}$$

Dimostrazione. Consideriamo V un G-modulo che abbia carattere ξ; nella dimostrazione del teorema di Maschke, abbiamo visto che esiste un prodotto hermitiano invariante rispetto all'azione di G. Scegliendo una base ortonormale per V, otteniamo una rappresentazione matriciale Y con carattere ξ, dove ogni $Y(g)$ è unitaria, cioè

$$Y(g^{-1}) = Y(g)^{-1} = \overline{Y(g)}^{t}.$$

Quindi

$$\overline{\xi(g)} = tr\overline{Y(g)} = trY(g^{-1})^t = trY(g^{-1}) = \xi(g^{-1}).$$

□

Osservazione 16. Per un campo arbitrario, l'equazione (2.1) è presa come definizione del prodotto hermitiano:

$$\langle \chi, \xi \rangle' = \frac{1}{o(G)} \sum_{g \in G} \chi(g)\xi(g^{-1});$$

ma nel campo complesso questo non è un prodotto hermitiano. Chiaramente la restrizione ai caratteri comporta $\langle \chi, \xi \rangle = \langle \chi, \xi \rangle'$.

Osservazione 17. Notiamo che, poichè il carattere è costante sulle classi di coniugio, abbiamo

$$\langle \chi, \xi \rangle = \frac{1}{o(G)} \sum_{K} |K| \chi_K \overline{\xi_K},$$

dove la sommatoria è su tutte le classi di coniugio di G e $\chi_K = \chi(g)\ \forall g \in K$.

Teorema 2.1.2. *Siano χ e ξ caratteri irriducibili di un gruppo G, allora*

$$\langle \chi, \xi \rangle = \delta_{\chi,\xi}$$

dove $\delta_{\chi,\xi}$ è la delta di Kronecker.

Dimostrazione. Supponiamo che χ e ξ siano caratteri di rappresentazioni matriciali A e B di grado, rispettivamente, d e f.
Sia $X = (x_{i,j})$ una generica matrice di ordine $d \times f$ e consideriamo la matrice

$$Y = \frac{1}{o(G)} \sum_{g \in G} A(g) X B(g^{-1}).$$

Notiamo che $A(h)Y = YB(h)$, infatti

$$\begin{aligned} A(h)YB(h)^{-1} &= \frac{1}{o(G)} \sum_{g \in G} A(h)A(g)XB(g^{-1})B(h^{-1}) \\ &= \frac{1}{o(G)} \sum_{g \in G} A(hg)XB(g^{-1}h^{-1}) \\ &= \frac{1}{o(G)} \sum_{\substack{\tilde{g} \in G \\ \tilde{g}=hg}} A(\tilde{g})XB(\tilde{g}^{-1}) \\ &= Y. \end{aligned}$$

Da ciò, per i corollari 1.5.3 e 1.5.5,

$$Y = \begin{cases} 0 & \text{se } A \ncong B, \\ cI_d & = A \cong B. \end{cases} \tag{2.2}$$

Consideriamo dapprima il caso in cui $\chi \neq \xi$, e dunque $A \ncong B$. In tal caso $y_{i,j} = 0 \quad \forall i, j$, ovvero

$$\frac{1}{o(G)} \sum_{k,l} \sum_{g \in G} a_{i,k}(g) x_{i,j} b_{i,j}(g^{-1}) = 0 \quad \forall i, j.$$

Poiché tale polinomio è nullo, i coefficienti di ogni $x_{k,l}$ devono essere nulli, ovvero

$$\frac{1}{o(G)} \sum_{g \in G} a_{i,k}(g) b_{i,j}(g^{-1}) = 0 \quad \forall i, j, k, l.$$

Quest'ultima condizione, per la difinizione di $\langle ., . \rangle'$, è equivalente a

$$\langle a_{i,k}, b_{i,j} \rangle' = 0 \quad \forall i, j, k, l.$$

Poichè

$$\chi = trA = a_{1,1} + a_{2,2} + \ldots + a_{d,d}$$

e

$$\xi = trB = b_{1,1} + b_{2,2} + \ldots + b_{f,f},$$

si ha che

$$\langle \chi, \xi \rangle = \langle \chi, \xi \rangle' = \sum_{i,j} \langle a_{i,i}, b_{j,j} \rangle' = 0.$$

Consideriamo ora il caso in cui $\chi = \xi$. Possiamo suppore $A = B$, poichè siamo interessati unicamente ai valori del carattere. Dall'equazione (2.2) sappiamo che $y_{i,j} = c\delta_{i,j}$ per un certo $c \in \mathbb{C}$. Dunque, analogamente ai calcoli

svolti in precedenza, si ha che $\langle a_{i,k}, a_{l,j}\rangle' = 0 \quad \forall i \neq j$.
Per $i = j$ avremo invece

$$y_{i,i} = \frac{1}{o(G)} \sum_{g \in G} A(g) X A(g^{-1}) = cI_d.$$

Considerando la traccia di entrembi i membri dell'uguaglianza, si ha:

$$\begin{aligned} cd &= trcI_d \\ &= \frac{1}{o(G)} \sum_{g \in G} tr(A(g) X A(g^{-1})) \\ &= \frac{1}{o(G)} \sum_{g \in G} trX \\ &= trX. \end{aligned}$$

Da ciò, si ha $y_{i,i} = c = \frac{1}{d} trX$, che può essere riscritto come

$$\frac{1}{o(G)} \sum_{k,l} \sum_{g \in G} a_{i,k}(g) x_{k,l} a_{l,i}(g^{-1}) = \frac{1}{d}(x_{1,1} + x_{2,2} + \ldots + x_{d,d}).$$

Considerando i coefficienti di $x_{k,l}$ si ottiene

$$\langle a_{i,k}, a_{l,i}\rangle' = \frac{1}{o(G)} \sum_{g \in G} a_{i,k}(g) a_{l,i}(g^{-1}) = \frac{1}{d} \delta_{k,l}.$$

Ne segue che

$$\begin{aligned} \langle \chi, \chi \rangle &= \sum_{i,j=1}^{d} \langle a_{i,i}, a_{j,j} \rangle' \\ &= \sum_{i=1}^{d} \langle a_{i,i}, a_{i,i} \rangle' \\ &= \sum_{i=1}^{d} \frac{1}{d} \\ &= 1. \end{aligned}$$

□

Corollario 2.1.3. *Sia X una rappresentazione matriciale di G con carattere χ, tale che*

$$X \cong m_1 X^{(1)} + m_2 X^{(2)} + \ldots + m_k X^{(k)},$$

dove gli $X^{(i)}$ sono rappresentazioni inequivalenti irriducibili con carattere $\chi^{(i)}$. Allora

1. $\chi = m_1\chi^{(1)} + m_2\chi^{(2)} + \ldots + m_k\chi^{(k)}$,

2. $\langle \chi, \chi^{(j)} \rangle = m_j \quad \forall j$,

3. $\langle \chi, \chi \rangle = m_1^2 + m_2^2 + \ldots + m_k^2$.

Dimostrazione. 1. Usando il fatto che la traccia di una somma diretta è la somma delle tracce, si ha

$$\chi = trX = tr \bigoplus_{i=1}^{k} m_i X^{(i)} = \sum_{i=1}^{k} m_i \chi^{(i)}.$$

2. Abbiamo, per il precedente teorema,

$$\langle \chi, \chi^{(j)} \rangle = \langle \sum_i m_i \chi^{(i)}, \chi^{(j)} \rangle = \sum_i m_i \langle \chi^{(i)}, \chi^{(j)} \rangle = m_j.$$

3. Sempre per il teorema precedente, abbiamo

$$\langle \chi, \chi \rangle = \langle \sum_i m_i \chi^{(i)}, \sum_j m_j \chi^{(j)} \rangle = \sum_{i,j} m_i m_j \langle \chi^{(i)}, \chi^{(j)} \rangle = \sum_i m_i^2.$$

□

2.2 Decomposizione dell'algebra gruppo

In questa sezione applicheremo i risultati ottenuti al problema della decomposizione dell'algebra gruppo $\mathbb{C}[G]$. Durante il procedimento determineremo il numero di rappresentazioni inequivalenti, irriducibili di ogni gruppo.

Dato un gruppo G e la sua algebra gruppo, il cui carattere $\chi = \chi^{reg}$, per il teorema di Maschke possiamo scrivere

$$\mathbb{C}[G] = \bigoplus_i m_i V^{(i)},$$

dove i $V^{(i)}$ sono moduli inequivalenti, irriducibili, e solo un numero finito di m_i sono non nulli.

Proposizione 2.2.1. *Dato* $\mathbb{C}[G] = \bigoplus_i m_i V^{(i)}$*, allora*

1. $m_i = \dim V^{(i)}$,
2. $o(G) = \sum_i (\dim V^{(i)})^2$,
3. $\dim Z_{\mathbb{C}[G]} = \dim Z_{End\mathbb{C}[G]}$.

Dimostrazione. 1. Per il punto 2 del corollario 2.1.3, abbiamo

$$m_i = \langle \chi, \chi^{(i)} \rangle = \frac{1}{o(G)} \sum_{g \in G} \chi(g)\chi^{(i)}(g^{-1}).$$

Ma dall'osservazione 13 sappiamo che $\chi(g) \neq 0$ se e solo se $g = \epsilon$, ed in tal caso $\chi(\epsilon) = o(G)$, dove $\chi = \chi^{reg}$. Abbiamo allora

$$\begin{aligned} m_i &= \frac{1}{o(G)} \chi(\epsilon)\chi^{(i)}(\epsilon) = \frac{1}{o(G)} o(G) tr I_{\dim V^{(i)}} \\ &= \frac{1}{o(G)} o(G) \dim V^{(i)} = \dim V^{(i)}. \end{aligned}$$

2.

$$o(G) = \dim \mathbb{C}[G] = \dim(\oplus_i m_i V^{(i)}) = \sum_i m_i \dim V^{(i)} = \sum_i (\dim V^{(i)})^2.$$

3. Dato $v \in \mathbb{C}[G]$, consideriamo l'applicazione $\phi_v : \mathbb{C}[G] \to \mathbb{C}[G]$ tale che

$$\phi_v(w) = wv \quad \forall w \in \mathbb{C}[G].$$

Questa è chiaramente lineare, e dunque $\phi_v \in End\mathbb{C}[G]$. Consideriamo $\phi : \mathbb{C}[G] \to End\mathbb{C}[G]$, data da

$$\phi(v) = \phi_v.$$

Ne proviamo la linearità:

$$\begin{aligned} \phi(av + bv')(w) = \phi_{av+bv'}(w) = w(av + bv') = wav + wbv' \\ = a(wv) + b(wv') = a\phi_v(w) + b\phi_{v'}(w) = (a\phi(v) + b\phi(v'))(w) \end{aligned}$$

$\forall a, b \in \mathbb{C},\ \forall v, v' \in \mathbb{C}[G]$. L'applicazione ϕ risulta essere iniettiva, infatti, se ϕ_v è l'applicazione nulla, allora

$$0 = \phi_v(\epsilon) = \epsilon v = v.$$

Per la suriettività, invece, supponiamo $\theta \in End\mathbb{C}[G]$ e consideriamo $\theta(\epsilon)$. Sicuramente avremo $\theta(\epsilon) = v$ per un certo $v \in \mathbb{C}[G]$; e da ciò segue che $\theta = \phi_v$, poiché, dato $g \in G$,

$$\theta(g) = \theta(g\epsilon) = g\theta(\epsilon) = gv = \phi_v(g),$$

e due trasformazioni lineari che sono uguali su una base, lo sono ovunque (ricordiamo infatti che G è una base per $\mathbb{C}[G]$). Abbiamo quindi dimostrato che $\mathbb{C}[G] \cong End\mathbb{C}[G]$ come spazi vettoriali; per quanto riguarda le algebre abbiamo, invece, che ϕ è un antiisomorfismo, poichè inverte l'ordine della moltiplicazione:

$$\phi_v\phi_w = \phi_{wv} \quad \forall v, w \in \mathbb{C}[G].$$

Dunque ϕ induce un antiisomorfismo sui centri di $\mathbb{C}[G]$ e $End\mathbb{C}[G]$, e da ciò

$$dimZ_{\mathbb{C}[G]} = dimZ_{End\mathbb{C}[G]}.$$

□

Corollario 2.2.2. *$\mathbb{C}[G]$ è commutativa se e solo se il numero di rappresentazioni inequivalenti irriducibili di $\mathbb{C}[G]$ è esattamente $o(G)$.*

Dimostrazione. Per il corollario 1.5.6 tutte le rappresentazioni irriducibili di $\mathbb{C}[G]$ hanno dimensione 1; quindi, per il punto 2 della proposizione 2.2.1,

$$o(G) = \sum_i (dimV^{(i)})^2 = \sum_i 1^2 = \sum_i 1 = k,$$

dove k è il numero di rappresentazioni irriducibili inequivalenti. □

2.3 Teoremi sul numero delle rappresentazioni irriducibili

In questa sezione si riportano due risultati interessanti che ci permettono di avere ulteriori informazioni sul numero di rappresentazioni irriducibili inequivalenti di un gruppo G.

Definizione 2.3. Dato un gruppo G,

$$G' = \left\{a^{-1}b^{-1}ab;\, a, b \in G\right\}$$

è detto il **sottogruppo dei commutatori**, o **derivato di** G.

Teorema 2.3.1. *Dato un gruppo G e G' il suo derivato, il numero di rappresentazioni di grado 1 di G è esattamente $o(G/G')$.*

Dimostrazione. Dato G/G', questo si dimostra essere abeliano, infatti, dati $a, b \in G$, abbiamo che $ab \sim ba$ poichè $ab = ba(a^{-1}b^{-1}ab)$ e $a^{-1}b^{-1}ab \in G'$. Poiché G/G' è abeliano, per il corollario 1.5.6, tutte le rappresentazioni irriducibili di G/G' sono di grado 1.
Data $\overline{\theta}$ una rappresentazione irriducibile di G/G', possiamo definire una rappresentazione θ di G nel seguente modo:

$$\theta(g) := \overline{\theta}([g]) \quad \forall g \in G,$$

dove $[g]$ indica la classe di equivalenza di g, e $\overline{\theta}$ è chiaramente di grado 1. Allora, per il corollario 2.2.2, tutte le $o(G/G')$ rappresentazioni di grado 1 di G/G' inducono rappresentazioni distinte di grado 1 su G.
Viceversa, se θ è una rappresentazione di grado 1 di G, allora $\theta(G)$, come sottogruppo di $\mathbb{C}^*$, è abeliano; perciò $G' \subset \ker\theta$ poiché θ è un omomorfismo, e quindi

$$\theta(a^{-1}b^{-1}ab) = \theta(a)^{-1}\theta(b)^{-1}\theta(a)\theta(b) = \theta(a)^{-1}\theta(a)\theta(b^{-1})\theta(b) = 1.$$

Definiamo allora una rappresentazione $\overline{\theta}$ di G/G' come

$$\overline{\theta}([g]) := \theta(g) \quad \forall g \in G.$$

Questa risulta essere ben definita poichè $G' \subset \ker\theta$, ed è chiaramente di grado 1. Dunque G ha al più $o(G/G')$ rappresentazioni distinte di grado 1. □

Teorema 2.3.2. *Il numero di rappresentazioni irriducibili inequivalenti distinte di G è uguale al numero delle classi di coniugio distinte di G.*

Dimostrazione. Per il punto 5 del teorema 1.6.8 sappiamo che il numero di rappresentazioni irriducibili inequivalenti distinte di G è uguale alla dim $Z_{End\mathbb{C}[G]}$, e quest'ultima, per il punto 3 della proposizione 2.2.1, è a sua volta uguale alla dim $Z_{\mathbb{C}[G]}$.
Dato $g \in G$, sia $C_g = \sum_{x \in C(g)} x$; vogliamo allora verificare che C_g commuta con tutti gli elementi di G.
Sia $x \in C(g)$, cioè $x = aga^{-1}$ e $b \in G$, allora

$$xb = aga^{-1}b = bb^{-1}aga^{-1}b = b(b^{-1}a)g(b^{-1}a)^{-1} = bx_1$$

con $x_1 \in C(g)$. Se si dimostra che la corrispondenza fra $C(g) \to C(g)$ che manda $x \mapsto x_1$ è biunivoca, allora $bC_g = b(\sum_{x \in C(g)}) = (\sum_{x \in C(g)})b = C_g b$.
Verifichiamo l'iniettività di $x \mapsto x_1$:

$$\begin{aligned}(b^{-1}a)g(b^{-1}a)^{-1} &= (b^{-1}c)g(b^{-1}c)^{-1} \\ \Rightarrow b^{-1}aga^{-1}b^{-1} &= b^{-1}cgc^{-1}b \\ \Rightarrow aga^{-1} &= cgc^{-1}.\end{aligned}$$

La suriettività è ovvia per questioni di cardinalità.
Abbiamo quindi appena dimostrato che C_g commuta con tutti gli elementi di G, e quindi con tutti gli elementi di $\mathbb{C}[G]$; allora $C_g \in Z(\mathbb{C}[G])$. Poiché gli elementi del gruppo sono linearmente indipendenti su $\mathbb{C}$, allora i C_g sono linearmente indipendenti su $\mathbb{C}$.
Vogliamo allora dimostrare che i C_g sono una base di $Z(\mathbb{C}[G])$ su $\mathbb{C}$. Sia $z_i = \sum_i \alpha_i g_i$ un elemento di $Z(\mathbb{C}[G])$ dove $\alpha_i \in \mathbb{C}$ e $g_i \in G$. Se $x \in G$, allora

$$\sum_i \alpha_i g_i = z = xzx^{-1} = \sum_i \alpha_i x g_i x^{-1}.$$

Poiché gli elementi del gruppo sono linearmente indipendenti, dalla comparazione dei coefficienti del primo e dell'ultimo termine dell'uguaglianza si ha che ogni coniugato di g_i compare in z con lo stesso coefficiente di g_i. Perciò $z = \sum_i \alpha_i C_{g_i}$, e dunque i C_g sono una base di $Z(\mathbb{C}[G])$.
Allora $\dim Z(\mathbb{C}[G])$ è uguale al numero di classi di coniugio di G. □

2.4 Caratteri ed interi algebrici

In tale sezione dimostreremo taluni risultati che ci permetteranno di vedere come il grado di una rappresentazione irriducibile di G divida sempre l'ordine del gruppo stesso.

Definizione 2.4. Dato $\alpha \in \mathbb{C}$, questo è detto **intero algebrico** se esiste un polinomio monico a coefficienti interi $p(x) \in \mathbb{Z}[x]$ tale che $p(\alpha) = 0$.

Lemma 2.4.1. *Se α e β sono interi algebrici, allora*

1. *$\alpha + \beta$ è ancora un intero algebrico;*
2. *$\alpha\beta$ è ancora un intero algebrico.*

Dimostrazione. Per la dimostrazione, non riportata in questa sede, si invita a fare riferimento a "The theory of algebraic numbers" di Harry Pollard. □

Lemma 2.4.2. *Dato χ il carattere di una rappresentazione di G, $\forall g \in G$ si ha che $\chi(g)$ è un intero algebrico.*

Dimostrazione. Consideriamo la rappresentazione ψ di G, che ha χ come carattere; allora, $\forall g \in G$,

$$(\psi(g))^{o(G)} = \psi(g^{o(G)}) = \psi(1) = I.$$

Dunque gli autovalori di $\psi(g)$ sono radici dell'unità, ovvero sono radici del polinomio monico a coefficienti interi

$$x^n - 1$$

con $n = o(G)$. Consideriamo ora $\chi(g) = tr\psi(g)$, questo è somma di interi algebrici, e dunque, per il punto 1 del lemma 2.4.1, è ancora un intero algebrico. □

Teorema 2.4.3. *Data ψ una rappresentazione irriducibile di G di grado d, si ha che*

$$\psi(C_g) = c(g)I_d \tag{2.3}$$

dove $c(g)$ è un intero algebrico.

Dimostrazione. Per quanto visto nella dimostrazione del teorema 2.3.2, sappiamo che $C_g \in Z(\mathbb{C}[G])$; dunque $\psi(C_g) \in Z(Mat_d)$ e, per la proposizione 1.6.4,

$$\psi(C_g) = c(g)I_d$$

con $c(g) \in \mathbb{C}$.
Dobbiamo ora dimostrare che $c(g)$ è un intero algebrico. Dati $a, b \in G$, allora

$$C_aC_b = \sum_{g\in G} \gamma_{abg}C_g,$$

dove γ_{abg} è il numero di volte in cui $g = a'b'$ con a' coniugato di a e b' coniugato di b. Applicando ψ all'uguaglianza, si ottiene

$$\psi(C_aC_b) = \sum_{g\in G} \gamma_{abg}\psi(C_g)$$

e quindi

$$\psi(C_a)\psi(C_b) = \sum_{g\in G} \gamma_{abg}\psi(C_g).$$

Abbiamo quindi

$$c(a)c(b) = \sum_{g\in G} \gamma_{abg}c(g).$$

Sia a fissato e b che varia sulle distinte classi di coniugio, assumendo i valori di $b_1, b_2, \ldots, b_k$. Il sistema di equazioni diventa:

$$\begin{cases} (c(g)(a) - \gamma_{ab_1b_1})c(b_1) - \gamma_{ab_1b_1}c(b_2) - \ldots - \gamma_{ab_1b_1}c(b_k) = 0 \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ -\gamma_{ab_kb_1}c(b_1) - \ldots - \gamma_{ab_kb_{k-1}}c(b_{k-1}) + (c(a) - \gamma_{ab_kb_k})c(b_k) = 0. \end{cases}$$

Poiché

$$g^{-1}\epsilon g = g^{-1}g = \epsilon$$

$\forall g \in G$, l'unico coniugato di ϵ è ϵ stesso; dunque $C_\epsilon = \epsilon$. Inoltre sappiamo che $\psi(\epsilon) = I_d$ e quindi $c(\epsilon) = 1$. Allora non tutti i $c(b_j)$ sono nulli, e dunque il sistema di equazioni ha una soluzione non banale. Ciò implica

$$\det \begin{pmatrix} (c(a) - \gamma_{ab_1b_1}) & -\gamma_{ab_1b_2} & \dots & -\gamma_{ab_1b_k} \\ -\gamma_{ab_2b_1} & (c(a) - \gamma_{ab_2b_2}) & \dots & -\gamma_{ab_1b_k} \\ \vdots & \vdots & \ddots & \vdots \\ -\gamma_{ab_kb_1} & -\gamma_{ab_kb_2} & \dots & (c(a) - \gamma_{ab_kb_k}) \end{pmatrix} = 0.$$

Di conseguenza, c(a) è la radice di un polinomio monico a coefficienti $\gamma_{ab_ib_j}$, che sono interi. □

Corollario 2.4.4. *Detto h_g il numero dei coniugati di $g \in G$, allora $\forall g \in G$ $(h_g\chi(g))/d$ è un intero algebrico.*

Dimostrazione. Applicando la traccia all'equazione (2.3) otteniamo

$$h_g\chi_g = dc(g).$$

Allora

$$c(g) = (h_g\chi(g))/d,$$

e questo è un intero algebrico per il teorema precedente. □

Teorema 2.4.5. *Dato d il grado di una rappresentazione irriducibile ψ di G, questo divide l'ordine di G, ovvero*

$$d|o(G).$$

Dimostrazione. Per il lemma 2.4.2, $\overline{\chi(g)}$ è un intero algebrico $\forall g \in G$. Per il corollario 2.4.4 $(h_g\chi(g))/d$ è un intero algebrico, quindi, per il punto 2 del lemma 2.4.1, $(h_g\chi(g)\overline{\chi(g)})/d$ è un intero algebrico $\forall g \in G$. Dati $g_1, g_2, \dots, g_k$ i rappresentanti delle classi di coniugio, abbiamo che

$$\sum_{j=1}^{k} \frac{h_j\chi(g_j)\overline{\chi(g_j)}}{d} = \sum_{g\in G} \frac{\chi(g)\overline{\chi(g)}}{d} = \frac{1}{d}\sum_{g\in G} \chi(g)\overline{\chi(g)}$$

è un intero algebrico. Per il teorema 2.1.2 e per la definizione di prodotto hermitiano di caratteri, $\sum_{g\in G} \chi(g)\overline{\chi(g)} = o(G)$; quindi $o(G)/d$ è un intero algebrico. Poichè $o(G)/d$ è un numero razionale, questo deve essere intero, poichè un razionale non intero non è un intero algebrico. □

Capitolo 3

Teorema di Hurwitz

In questo capitolo dimostreremo un'interessante conseguenza della teoria della rappresentazione dei gruppi: il teorema di Hurwitz. La dimostrazione che seguiremo sarà quella data da Eckmann nel 1943.

3.1 Studio di un gruppo interessante

In questa sezione affronteremo lo studio del gruppo finito G presentato per generatori e relazioni. I generatori sono gli elementi $a_1, a_2, \ldots, a_{m-1}, \eta$, con $m > 2$, tali che

$$a_i^2 = \eta, \quad \eta^2 = 1, \quad a_i a_j = \eta a_i a_j \ \forall i \neq j, \tag{3.1}$$

dove 1 è l'elemento neutro del gruppo.
Lo studio di tale gruppo ci permetterà di dimostrare il Teorema di Hurwitz nella sezione successiva.

Osservazione 18. Notiamo che

$$a_i \eta = a_i a_i^2 = a_i a_i a_i = a_i^2 a_i = \eta a_i,$$

quindi η commuta con ogni elemento di G, ovvero $\eta \in Z_G$.
Notiamo inoltre che

$$(\eta a_i) a_i = \eta a_i^2 = \eta\eta = 1,$$

dunque $a_i^{-1} = \eta a_i$, e $\eta^{-1} = \eta$.

Proposizione 3.1.1. *Il gruppo G, i cui elementi sono del tipo*

$$\eta^{\delta_0} a_1^{\delta_1} \ldots a_{m-1}^{\delta_{m-1}} \text{ con } \delta_i \in \{0, 1\} \quad \forall i = 0, 1, \ldots, m-1,$$

con l'operazione di prodotto

$$\eta^{\delta_0} a_1^{\delta_1} \ldots a_{m-1}^{\delta_{m-1}} * \eta^{\epsilon_0} a_1^{\epsilon_1} \ldots a_{m-1}^{\epsilon_{m-1}} = \eta^{\delta_0 + \epsilon_0 + n} a_1^{\delta_1 + \epsilon_1} \ldots a_{m-1}^{\delta_{m-1} + \epsilon_{m-1}}$$

con

$$n = \sum_{i=1}^{m-1} \epsilon_i \sum_{j=i}^{m-1} \delta_j$$

e la somma degli esponenti in $\mathbb{Z}_2$*, ha ordine* 2^m*.*

Dimostrazione. Dimostriamo inizialmente che gli elementi di G sono al più 2^m. Poiché $a_i a_j = \eta a_j a_i$ e η commuta con tutti gli elementi di G, possiamo sempre supporre che gli elementi di G siano ordinati. Tutti gli elementi del gruppo saranno quindi del tipo

$$\eta^{\delta_0} a_1^{\delta_1} \dots a_{m-1}^{\delta_{m-1}} \text{ con } \delta_i \in \{0,1\} \quad \forall i = 0,1,\dots,m-1.$$

Abbiamo quindi 2^m possibili scelte degli esponenti, e dunque al più 2^m elementi. Consideriamo ora l'insieme

$$H = \mathbb{Z}_2^m$$

su cui è definito il prodotto

$$(b_0, b_1, \dots, b_{m-1}) * (c_0, c_1, \dots, c_{m-1}) = (b_0 + c_0 + \sum_{1 \le i \le j} b_i c_j, b_1 + c_1, \dots, b_{m-1} + c_{m-1})$$

per ogni $(b_0, b_1, \dots, b_{m-1}), (c_0, c_1, \dots, c_{m-1}) \in H$.

Verifichiamo ora che il prodotto su H soddisfa le condizioni (3.1); infatti, ponendo
$1 := (0, 0, \dots, 0)$,
$\eta := (1, 0, \dots, 0)$,
$a_i := (0, 0, \dots, 0, \overbrace{1}^{\text{i-esimo posto}}, 0, \dots, 0)$,
abbiamo che

$$a_i^2 = a_i * a_i = (1, 0, \dots, 0) = \eta$$
$$\eta^2 = \eta * \eta = (1 + 1, 0, \dots, 0) = (0, 0, \dots, 0) = 1$$

e, supponendo $i < j$,

$$a_i * a_j = (1, 0, \dots, 0, \overbrace{1}^{\text{i-esimo posto}}, 0, \dots, 0, \overbrace{1}^{\text{j-esimo posto}}, 0, \dots, 0),$$
$$a_j * a_i = (0, \dots, 0, \overbrace{1}^{\text{i-esimo posto}}, 0, \dots, 0, \overbrace{1}^{\text{j-esimo posto}}, 0, \dots, 0),$$
$$\eta * a_j * a_i = (1, \dots, 0, \overbrace{1}^{\text{i-esimo posto}}, 0, \dots, 0, \overbrace{1}^{\text{j-esimo posto}}, 0, \dots, 0).$$

Dobbiamo ancora dimostrare che $(H, *)$ è un gruppo.
L'elemento neutro è ovviamente 1.
L'elemento inverso è

$$(b_0, b_1, \ldots, b_{m-1})^{-1} = (n_0, b_1, \ldots, b_{m-1})$$

con

$$n_0 = b_0 + \sum_{1 \leq i \leq j} b_i b_j.$$

Per l'associatività abbiamo:

$$\begin{aligned}
&((b_0, b_1, \ldots, b_{m-1}) * (c_0, c_1, \ldots, c_{m-1})) * (d_0, d_1, \ldots, d_{m-1}) = \\
&(b_0 + c_0 + \sum_{1 \leq i \leq j} b_i c_j, b_1 + c_1, \ldots, b_{m-1} + c_{m-1}) * (d_0, d_1, \ldots, d_{m-1}) = \\
&(b_0 + c_0 + \sum_{1 \leq i \leq j} b_i c_j + d_0 + \sum_{1 \leq i \leq j} (b_i + c_i) d_j, b_1 + c_1 + d_1, \ldots, b_{m-1} + c_{m-1} + d_{m-1}) = \\
&(b_0 + c_0 + d_0 + \sum_{1 \leq i \leq j} (b_i c_j + b_i d_j + c_i d_j), b_1 + c_1 + d_1, \ldots, b_{m-1} + c_{m-1} + d_{m-1});
\end{aligned}$$

e similmente

$$\begin{aligned}
&(b_0, b_1, \ldots, b_{m-1}) * ((c_0, c_1, \ldots, c_{m-1}) * (d_0, d_1, \ldots, d_{m-1})) = \\
&(b_0 + c_0 + d_0 + \sum_{1 \leq i \leq j} (b_i c_j + b_i d_j + c_i d_j), b_1 + c_1 + d_1, \ldots, b_{m-1} + c_{m-1} + d_{m-1}).
\end{aligned}$$

Abbiamo allora che H è un gruppo di ordine 2^m.
Consideriamo l'omomorfismo $\phi : G \longrightarrow H$ che manda $\eta^{\delta_0} a_1^{\delta_1} \ldots a_{m_1}^{\delta_{m-1}} \mapsto (\delta_0, \delta_1, \ldots, \delta_{m-1})$, questo è chiaramente suriettivo; e dunque, poiché $o(G) \leq 2^m$ e $o(H) = 2^m$, $o(G) = o(H) = 2^m$. □

Proposizione 3.1.2. *Il derivato di G è*

$$G' = \{1, \eta\}.$$

Dimostrazione. Utilizzando il prodotto definito su H nella dimostrazione della

proposizione 3.1.1 abbiamo che

$$
\begin{aligned}
&(b_0, b_1, \ldots, b_{m-1})^{-1} * (c_0, c_1, \ldots, c_{m-1})^{-1} * (b_0, b_1, \ldots, b_{m-1}) * (c_0, c_1, \ldots, c_{m-1}) \\
=&(b_0 + \sum_{1\leq i\leq j} b_i b_j, b_1, \ldots, b_{m-1}) * (c_0 + \sum_{1\leq i\leq j} c_i c_j, c_1, \ldots, c_{m-1}) * \\
&(b_0, b_1, \ldots, b_{m-1}) * (c_0, c_1, \ldots, c_{m-1}) \\
=&(b_0 + c_0 + \sum_{1\leq i\leq j} (b_i b_j + c_i c_j + b_i c_j), b_1 + c_1, \ldots, b_{m-1} + c_{m-1}) * \\
&(b_0 + c_0 + \sum_{1\leq i\leq j} b_i c_j, b_1 + c_1, \ldots, b_{m-1} + c_{m-1}) \\
=&(\sum_{1\leq i\leq j} (b_i b_j + c_i c_j + 2 b_i c_j + (b_i + c_i)(b_j + c_j)), 0, \ldots, 0) \\
=&(\sum_{1\leq i\leq j} (b_i c_j + c_i b_j), 0, \ldots, 0).
\end{aligned}
$$

Poiché $\sum_{1\leq i\leq j}(b_i c_j + c_i b_j) \in \mathbb{Z}_2$, questo può essere solo 0 o 1, e dunque, grazie all'isomorfismo ϕ, gli elementi del derivato di G, possono essere unicamente 1 e η. □

Proposizione 3.1.3. *Il centro di G è*

1. $Z_G = \{1, \eta\}$ *se m è dispari,*
2. $Z_G = \{1, \eta, a_1 a_2 \ldots a_{m-1}, \eta a_1 a_2 \ldots a_{m-1}\}$, *se m è pari.*

Dimostrazione. In questa dimostrazione lavoreremo sul gruppo H definito nella dimostrazione della proposizione 3.1.1, per poi concludere grazie all'isomorfismo ϕ.
Ci limitiamo a studiare gli elementi che commutano con i generatori, poiché ogni elemento che commuta con tutti i generatori di H, commutaanche con ogni elemento di H. Abbiamo che

$$
\begin{aligned}
&(b_0, b_1, \ldots, b_{m-1}) * (0, \ldots, 0, \overbrace{1}^{\text{k-esimo posto}}, 0, \ldots, 0) \\
=&(b_0 + \sum_{1\leq i\leq k} b_i, b_1, \ldots, b_{k-1}, b_k + 1, b_{k+1}, \ldots, b_{m-1})
\end{aligned}
$$

e

$$
\begin{aligned}
&(0, \ldots, 0, \overbrace{1}^{\text{k-esimo posto}}, 0, \ldots, 0) * (b_0, b_1, \ldots, b_{m-1}) \\
=&(b_0 + \sum_{k\leq i\leq m-1} b_i, b_1, \ldots, b_{k-1}, b_k + 1, b_{k+1}, \ldots, b_{m-1}).
\end{aligned}
$$

Affinché l'elemento $(b_0, b_1, \ldots, b_{m-1}) \in Z_G$ bisogna avere

$$\sum_{1\leq i\leq k} b_i = \sum_{k\leq i\leq m-1} b_i$$

$\forall k = 1, .., m-1$; ricordando sempre che stiamo lavorando su $H = \mathbb{Z}_2^m$. Ma

$$\begin{aligned}
&\sum_{1\leq i\leq k} b_i = \sum_{1\leq i\leq m-1} b_i + \sum_{k+1\leq i\leq m-1} b_i \\
&\Rightarrow \sum_{k\leq i\leq m-1} b_i = \sum_{1\leq i\leq m-1} b_i + \sum_{k+1\leq i\leq m-1} b_i \\
&\Rightarrow \sum_{1\leq i\leq m-1} b_i = \sum_{k+1\leq i\leq m-1} b_i + \sum_{k\leq i\leq m-1} b_i \\
&\Rightarrow \sum_{1\leq i\leq m-1} b_i = b_k
\end{aligned}$$

$\forall k = 1, \ldots, m-1$; allora

$$b_k = b_{k'} \quad \forall k, k' = 1, \ldots, m-1.$$

Abbiamo quindi che o

$$b_k = 0 \quad \forall k = 1, \ldots, m-1, \tag{3.2}$$

o

$$b_k = 1 \quad \forall k = 1, \ldots, m-1. \tag{3.3}$$

Ma i b_k devono anche soddisfare $\sum_{1\leq i\leq m-1} b_i = b_k$, e questa è sempre soddisfatta nel caso (3.2); nel caso (3.3) abbiamo invece che

$$1 = b_k = \sum_{1\leq i\leq m-1} b_i = m-1 \Leftrightarrow m = 0 \text{ in } \mathbb{Z}_2 \Leftrightarrow m \text{ è pari.}$$

Notiamo che il termine b_0 non è coinvolto nella sommatoria, e dunque questo può essere sia 0 che 1.

□

Proposizione 3.1.4. *La classe di coniugio di $g \in G$ è $C(g) = \{g, \eta * g\}$.*

Dimostrazione. In questa dimostrazione lavoreremo sul gruppo H definito nella dimostrazione della proposizione 3.1.1, per poi concludere grazie all'isomorfismo ϕ.

Considerando $(b_0, b_1, \ldots, b_{m-1}), (c_0, c_1, \ldots, c_{m-1}) \in H$, abbiamo che

$$(c_0, c_1, \ldots, c_{m-1}) * (b_0, b_1, \ldots, b_{m-1}) * (c_0, c_1, \ldots, c_{m-1})^{-1} =$$
$$(c_0, c_1, \ldots, c_{m-1}) * (b_0, b_1, \ldots, b_{m-1}) * (c_0 + \sum_{1 \leq i \leq j} c_i c_j, c_1, \ldots, c_{m-1}) =$$
$$(c_0 + b_0 + \sum_{1 \leq i \leq j} c_i b_j, c_1 + b_1, \ldots, c_{m-1} + b_{m-1}) * (c_0 + \sum_{1 \leq i \leq j} c_i c_j, c_1, \ldots, c_{m-1}) =$$
$$(b_0 + \sum_{1 \leq i \leq j} (c_i b_j + c_i c_j + (c_i + b_i) c_j), b_1, \ldots, b_{m-1}) =$$
$$(b_0 + \sum_{1 \leq i \leq j} (c_i b_j + b_i c_j), b_1, \ldots, b_{m-1}).$$

Poiché $\sum_{1 \leq i \leq j} (c_i b_j + b_i c_j) \in \mathbb{Z}_2$, questo può assumere unicamente i valori 0 e 1, e dunque

$$(b_0 + \sum_{1 \leq i \leq j} (c_i b_j + b_i c_j), b_1, \ldots, b_{m-1}) = (b_0, b_1, \ldots, b_{m-1}),$$

oppure

$$(b_0 + \sum_{1 \leq i \leq j} (c_i b_j + b_i c_j), b_1, \ldots, b_{m-1}) = (b_0 + 1, b_1, \ldots, b_{m-1})$$
$$= (1, 0, \ldots, 0) * (b_0, b_1, \ldots, b_{m-1}).$$

□

Corollario 3.1.5. *Il numero delle classi di coniugio di G è*

1. $2^{m-1} + 1$ *se m è dispari,*

2. $2^{m-1} + 2$ *se m è pari.*

Dimostrazione. Poiché, per la proposizione precedente, le classi di coniugio di G hanno tutte cardinalità 2, abbiamo che allora il numero delle classi di coniugio è dato dal numero degli elementi del centro e dal numero degli elementi non appartenenti al centro diviso per la cardinalità delle classi di coniugio. Dunque, per le proposizioni 3.1.3 e 3.1.4,

1. se m è dispari abbiamo $2 + (2^m - 2)/2 = 2^{m-1} + 1$ classi di coniugio,

2. se m è pari abbiamo $4 + (2^m - 4)/2 = 2^{m-1} + 2$ classi di coniugio.

□

3.2 Teorema di Hurwitz

Dati $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$, ci chiediamo per quali valori di $m, n \in \mathbb{Z}^+$ esistono $f_1, \ldots, f_n : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}$ applicazioni bilineari tali che

$$(x_1^2+x_2^2+\ldots+x_m^2)(y_1^2+y_2^2+\ldots+y_n^2) = f_1^2(x,y)+f_2^2(x,y)+\ldots+f_n^2(x,y). \quad (3.4)$$

In particolare il teorema di Hurwitz riguarda il caso in cui $n = m$.

Proposizione 3.2.1. *Se $m = 2$, esistono $f_1, \ldots, f_n : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}$ applicazioni bilineari che soddisfano* (3.4) *se e solo se n è pari.*

Dimostrazione. Supponiamo che esistano $f_1, \ldots, f_n : \mathbb{R}^2 \times \mathbb{R}^n \to \mathbb{R}$ applicazioni bilineari che soddisfano

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2 + \ldots + y_n^2) = f_1^2(x,y) + f_2^2(x,y) + \ldots + f_n^2(x,y).$$

Per semplificare la notazione, indicheremo $f_i(x,y) = z_i \; \forall i = 1, .., n$, ottendendo

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2 + \ldots + y_n^2) = z_1^2 + z_2^2 + \ldots + z_n^2. \quad (3.5)$$

Poiché gli z_i sono applicazioni bilineari degli x_j e degli y_k, questi possono essere scritti come

$$z_i = \sum_{k=1}^{n} \left(v_i[1,k]x_1y_k + v_i[2,k]x_2y_k \right),$$

con $v_i[j,k] \in \mathbb{C}$. Indicheremo con $v[j,k]$ il vettore $(v_1[j,k], v_2[j,k], \ldots, v_n[j,k]) \in \mathbb{C}^n$.
Dunque

$$z_i^2 = x_1^2 \left(\sum_{k=1}^{n} v_i[1,k]y_k \right)^2 + x_2^2 \left(\sum_{k=1}^{n} v_i[2,k]y_k \right)^2 + 2x_1x_2 \left(\sum_{k=1}^{n} v_i[1,k]y_k \right) \left(\sum_{j=1}^{n} v_i[2,j]y_j \right).$$

Poiché i coefficienti di x_1^2, di x_2^2 e di x_1x_2 devono essere uguali in entrambi i membri dell'uguaglianza (3.5), otteniamo le seguenti condizioni:

1. $\sum_{i=1}^{n} \left(\sum_{k=1}^{n} v_i[1,k]y_k \right)^2 = \sum_{k=1}^{n} y_k^2$,
2. $\sum_{i=1}^{n} \left(\sum_{k=1}^{n} v_i[2,k]y_k \right)^2 = \sum_{k=1}^{n} y_k^2$,
3. $\sum_{i=1}^{n} \left(\sum_{k=1}^{n} v_i[1,k]y_k \right) \left(\sum_{j=1}^{n} v_i[2,j]y_j \right) = 0$.

Consideriamo la forma bilineare simmetrica $\langle \quad , \quad \rangle$ su $\mathbb{C}^*$ data da

$$\langle (x_1, \ldots, x_n), (x'_1, \ldots, x'_n) \rangle = x_1 x'_1 + \ldots + x_n x'_n;$$

sviluppando la condizione 1, otteniamo

$$\sum_{i=1}^{n} v_i[1,k]^2 y_k^2 = y_k^2 \Leftrightarrow \sum_{i=1}^{n} v_i[1,k]^2 = 1 \Leftrightarrow \langle v[1,k], v[1,k] \rangle = 1$$

$\forall k = 1, \ldots, n$; e

$$\sum_{i=1}^{n} v_i[1,k] v_i[1,j] y_k y_j = 0 \Leftrightarrow \sum_{i=1}^{n} v_i[1,k] v_i[1,j] = 0 \Leftrightarrow \langle v[1,k], v[1,j] \rangle = 0$$

$\forall j, k = 1, \ldots, n$; ovvero

$$\langle v[1,k], v[1,j] \rangle = \delta_{jk} \quad \forall j, k = 1, \ldots, n. \tag{3.6}$$

Abbiamo quindi che $\mathcal{V} = (v[1,1], v[1,2] \ldots, v[1,n])$ è una base di $\mathbb{C}^n$.
Sviluppando la condizione 2, si ottiene analogamente che

$$\langle v[2,k], v[2,j] \rangle = \delta_{kj} \quad \forall j, k = 1, .., n; \tag{3.7}$$

e, poiché $\mathcal{V}$ è una base, questi possono anche essere scritti come

$$v[2,j] = \sum_{k=1}^{n} a_{jk} v[1,k] \quad \forall j = 1, \ldots, n.$$

La matrice $A = (a_{jk})_{1 \leq j,k \leq n}$, per le condizioni (3.6) e (3.7), soddisfa

$$A^{-1} = A^t; \tag{3.8}$$

e quindi $(detA)^2 = 1$. Sviluppando la condizione 3, otteniamo

$$\sum_{k=1}^{n} \sum_{j=1}^{n} \langle v[1,k], v[2,j] \rangle y_j y_k = 0,$$

ovvero

$$\langle v[1,k], v[2,j] \rangle + \langle v[1,j], v[2,k] \rangle = 0 \tag{3.9}$$

$\forall j, k = 1, \ldots, n$. Abbiamo inoltre che

$$\langle v[1,k], v[2,j] \rangle = \langle v[1,k], \sum_{l=1}^{n} a_{jl} v[1,l] \rangle = \sum_{l=1}^{n} a_{jl} \langle v[1,k], v[1,l] \rangle = a_{jk}$$

$\forall j, k = 1, \ldots, n$. Possiamo quindi riscrivere la condizione (3.9) come

$$a_{kj} + a_{jk} = 0,$$

ovvero la matrice A è antisimmetrica.
Per la condizione (3.8) e l'antisimmetria di A abbiamo quindi

$$I_n = AA^{-1} = AA^t = A(-A) = -A^2.$$

Passando al determinante e usando il teorema di Binet, otteniamo

$$1 = det(I_n) = det(-A^2) = (-1)^n (detA)^2 = (-1)^n.$$

Questo chiaramente implica che n sia pari.

Viceversa, se n è pari, ci basta considerare

$$z_i = x_i y_i - x_{i+1} y_{i+1} \text{ e } z_{i+1} = x_i y_{i+1} + x_{i+1} y_i$$

$\forall i = 1, 3, \ldots, n-1$; queste si dimostrano essere bilineari e soddisfano (3.5). □

Teorema 3.2.2. *Se $m > 2$, dato $n = 2^j s$, dove s è dispari, esistono $f_1, \ldots, f_n : \mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}$ applicazioni bilineari che soddisfano* (3.4) *se e solo se $m \leq 2j+2$.*

Dimostrazione. Scriviamo

$$z_i = \sum_{k=1}^{n} a_{ik}(x) y_k,$$

dove le $a_{ik}(x)$ sono applicazioni lineari negli x_j. Avremo allora che

$$z_i^2 = \sum_{k=1}^{n} a_{ik}^2(x) y_k^2 + 2 \sum_{\substack{k,l=1 \\ k<l}}^{n} a_{ik}(x) a_{il}(x) y_k y_l.$$

Inserendo quanto ottenuto nell'uguaglianza (3.4) e confrontandone i coefficienti, abbiamo

$$\sum_{i=1}^{n} a_{ik}(x) a_{il}(x) = 0 \text{ se } k \neq l,$$

e

$$\sum_{i=1}^{n} a_{ik}^2(x) = x_1^2 + x_2^2 + \ldots + x_m^2.$$

Data la matrice $A = (a_{ik}(x))_{1 \leq i,k \leq n}$, le condizioni precedenti possono essere facilmente scritte come

$$AA^t = (x_1^2 + x_2^2 + \ldots + x_m^2) I_n. \tag{3.10}$$

Poiché gli $a_{ik}(x)$ sono funzioni lineari negli x_j, possiamo scrivere

$$A = A_1x_1 + A_2x_2 + \ldots + A_mx_m,$$

dove le A_j sono matrici $n \times n$ su $\mathbb{C}$. Inserendo A così definita nell'uguaglianza (3.10) e confrontando i coefficienti otteniamo

$$A_iA_j^t + A_jA_i^t = 0 \text{ se } i \neq j, \text{ e } A_iA_i^t = I_n \text{ se } i = j. \tag{3.11}$$

Il problema di trovare m che soddisfi (3.4) si riconduce quindi a trovare m matrici complesse $n \times n$ che soddisfino (3.11).
Data $B_i = A_m^tA_i$, abbiamo che

$$B_m = A_mA_m^t = I_n,$$

e

$$B_iB_i^t = A_mA_i^t(A_mA_i^t)^t = A_m(A_i^tA_i)A_m^t = A_mA_m^t = I_n.$$

Inoltre, per $i \neq j$, abbiamo

$$\begin{aligned} B_iB_j^t + B_jB_i^t &= A_mA_i^t(A_mA_j^t)^t + A_mA_j^t(A_mA_i^t)^t \\ &= A_m(A_i^tA_j)A_m^t + A_m(A_j^tA_i)A_m^t \\ &= A_m(A_iA_j^t + A_jA_i^t)A_m^t \\ &= 0. \end{aligned}$$

Se nell'ultima condizione poniamo $j = m$, otteniamo $B_i^t = -B_i \ \forall i \neq m$. Possiamo quindi riscrivere le condizioni come

$$B_iB_j = -B_jB_i, \quad B_i^2 = -I_n, \quad B_m = I_n. \tag{3.12}$$

Ci stiamo quindi chiedendo per quali interi m ed n possiamo trovare $m-1$ matrici $n \times n$ complesse, antisimmetriche, ortogonali che anticommutano tra loro.

Lasciamo da parte le matrici per un momento e consideriamo il gruppo G definito nella sezione precedente.
Per le proposizioni 3.1.2 e 3.1.1 abbiamo che $o(G/G') = 2^{m-1}$, e quindi, per il teorema 2.3.1, G ha esattamente 2^{m-1} rappresentazioni di grado 1. Per il teorema 2.3.2 il numero totale di rappresentazioni irriducibili inequivalenti distinte di G equivale al numero delle classi di coniugio di G. Dunque, per il corollario 3.1.5, se m è dispari G ha $2^{m-1} + 1 - 2^{m-1} = 1$ rappresentazione irriducibile di grado $\zeta \neq 1$. Per il corollario 2.2.2 la somma dei quadrati dei gradi delle rappresentazioni irriducibili di G è proprio l'ordine di G, quindi

$$2^{m-1} + \zeta^2 = 2^m \Leftrightarrow \zeta^2 = 2^m - 2^{m-1} \Leftrightarrow \zeta^2 = 2^{m-1}(2-1) \Leftrightarrow \zeta = 2^{\frac{m-1}{2}}.$$

Se m è pari, G ha $2^{m-1} + 2 - 2^{m-1} = 2$ rappresentazioni irriducibili di grado $\zeta_1, \zeta_2 \neq 1$; quindi $\zeta_1^2 + \zeta_2^2 + 2^{m-1} = 2^m$. Per il teorema 2.4.5 $\zeta_1, \zeta_2 | 2^m$, dunque devono essere entrambi una potenza di 2. Perciò, ponendo $\zeta_1 = 2^a$ e $\zeta_2 = 2^b$ e supponendo $a \leq b$,

$$\begin{aligned}\zeta_1^2 + \zeta_2^2 = 2^{m-1} &\Leftrightarrow 2^{2a} + 2^{2b} = 2^{m-1} \Leftrightarrow 2^{2a}(1 + 2^{2(b-a)}) = 2^{m-1} \\ &\Rightarrow 2^{2(b-a)} = 1 \Leftrightarrow b - a = 0 \Leftrightarrow b = a \Leftrightarrow \zeta_1 = \zeta_2.\end{aligned}$$

Quindi $\zeta_1 = \zeta_2 = 2^{\frac{m-2}{2}}$.

Tornando alla questione matriciale, possiamo considerare la rappresentazione matriciale di G

$$\begin{aligned}\psi : \quad & G \to Mat_n \\ & a_i \mapsto B_i \\ & \eta \mapsto -I.\end{aligned}$$

La nostra domanda si riconduce quindi a trovare i valori di n tali che esiste una rappresentazione di G di grado n in cui η è rappresentato dalla matrice $-I_n$.
Osserviamo che, poiché η è un commutatore, questo è rappresentato dalla matrice (1) in tutte le rappresentazioni di grado 1; infatti, se $\eta = a^{-1}b^{-1}ab$,

$$\begin{aligned}\chi(\eta) &= \chi(a^{-1}b^{-1}ab) \\ &= \chi(a^{-1})\chi(b^{-1})\chi(a)\chi(b) \\ &= \chi(a)^{-1}\chi(b)^{-1}\chi(a)\chi(b) \\ &= \chi(a)^{-1}\chi(a)\chi(b)^{-1}\chi(b) \\ &= (1)(1) = (1)\end{aligned}$$

grazie alla commutatività di $\mathbb{C}$. Dunque la nostra rappresentazione dovrà essere somma diretta di rappresentazioni irriducibili di grado $\neq 1$. Perciò

1. se m è dispari, $n = k2^{\frac{m-1}{2}}$,

2. se m è pari, $n = k2^{\frac{m-2}{2}}$.

Se $n = 2^j s$, dove s è dispari, e m dispari, allora $j \geq \frac{m-1}{2}$, ovvero $m \leq 2j + 1 < 2j + 2$. Analogamente, se m è pari, allora $m \leq 2j + 2$. Dunque, indipendentemente dalla parità di m, abbiamo $m \leq 2j + 2$.

Viceversa, se $m \leq 2j + 2$, ci basta costruire $m - 1$ matrici che soddisfino (3.12), poiché abbiamo già dimostrato che tale condizione è equivalente all'esistenza di $f_1, \ldots, f_n$ applicazioni bilineari che soddisfano (3.4).
Se m è dispari, quindi $m = 2t + 1$ per un certo $1 \leq t \leq j$, sappiamo che esiste

una rappresentazione irriducibile del gruppo di G di grado $2^{\frac{m-1}{2}} = 2^{\frac{2t+1-1}{2}} = 2^t$, del tipo

$$\begin{aligned}\psi :&G \to Mat_{2^t} \\ &a_i \mapsto C_i \quad \forall i = 1, \dots, m-1 \\ &\eta \mapsto -I.\end{aligned}$$

Costruiamo allora per ogni i la matrice diagonale a blocchi

$$B_i = \begin{pmatrix} C_i & 0 & \dots & 0 \\ 0 & C_i & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & C_i \end{pmatrix},$$

che ha sulla diagonale la matrice C_i $2^{j-t}s$ volte, così che l'ordine di B_i sia $2^t 2^{j-t} s = 2^j s = n$.
Verifichiamo ora che effettivamente le matrici B_i sono antisimmetriche, ortogonali e che anticommutano tra loro. L'anticommutatività deriva direttamente dalle relazioni definite sui generatori del gruppo G; difatti la relazione $a_i a_j = \eta a_j a_i \ \forall i, j = 1, \dots, m-1$ si estende alle matrici C_i, e dunque anche alle matrici B_i.
Dimostriamo ora l'ortogonalità. Consideriamo una forma bilineare $\langle\ ,\ \rangle$ e definiamo

$$\langle v, w\rangle' = \frac{1}{|G|} \sum_{g \in G} \langle gv, gw\rangle;$$

questo è G-invariante poiché, $\forall h \in G$,

$$\langle hv, hw\rangle' = \frac{1}{|G|} \sum_{g \in G} \langle hgv, hgw\rangle = \frac{1}{|G|} \sum_{\substack{g' \in G \\ g' = gh}} \langle g'v, g'w\rangle = \langle v, w\rangle'.$$

Poiché lavoriamo in $\mathbb{C}$, si può sempre scegliere una base tale che $\langle\ ,\ \rangle'$ è associato a I, cioè:

$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n)\rangle' = x_1 y_1 + \dots + x_n y_n.$$

Ma allora

$$\langle v, w\rangle' = v^t I w$$

e, poiché $\langle gv, gw\rangle' = \langle v, w\rangle'$,

$$\begin{aligned} v^t I w = (\psi(g)v)^t I (\psi(g)w) = v^t \psi(g)^t I \psi(g) w \\ \Leftrightarrow \psi(g)^t I \psi(g) = I \Leftrightarrow \psi(g)^{-1} = \psi(g)^t. \end{aligned}$$

Dunque le matrici C_i, e di conseguenza anche le B_i, sono ortogonali.
Infine abbiamo che, poiché $a_i^2 = \eta \ \forall i = 1, \ldots, m-1$ e le matrici C_i sono ortogonali,

$$C_i^2 = -I \Leftrightarrow -C_i C_i = I \Leftrightarrow C_i^{-1} = -C_i \Leftrightarrow C_i^t = -C_i \quad \forall i = 1, \ldots, m-1;$$

abbiamo quindi dimostrato che le matrici C_i, e dunque anche le matrici B_i, sono antisimmetriche.
Il ragionamento analogo può essere fatto se m è pari, cioè $m = 2t+2$ per un certo $1 \leq t \leq j$, difatti G avrà rappresentazioni di dimensione $2^{\frac{m-2}{2}} = 2^{\frac{2t+2-2}{2}} = 2^t$.

□

Corollario 3.2.3 (Teorema di Hurwitz)**.** *Esistono* $f_1, \ldots, f_n : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ *applicazioni bilineari che soddisfano*

$$(x_1^2+x_2^2+\ldots+x_n^2)(y_1^2+y_2^2+\ldots+y_n^2) = f_1^2(x,y)+f_2^2(x,y)+\ldots+f_n^2(x,y) \quad (3.13)$$

se e solo se $n = 1, 2, 4, 8$.

Dimostrazione. Se $n = 1$, l'enunciato è ovvio.
Se $n = 2$, l'enunciato è vero per la proposizione 3.2.1.
Se $n > 2$ allora, per il teorema 3.2.2, l'uguaglianza (3.13) è vera se e solo se $n \leq 2j+2$, con $n = 2^j s$ ed s dispari; e tale disuguaglianza è soddisfatta solo per i valori $n = 4$ e $n = 8$. □

Esempio 3 (Identità di Brahmagupta-Fibonacci)**.** Un esempio del teorema di Hurwitz nel caso $n = 2$ è l'identità di Brahmagupta-Fibonacci, che ci dà due possibili definizioni degli z_i:

$$\begin{aligned}(x_1^2 + x_2^2)(y_1^2 + y_2^2) &= (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 \\ &= (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2.\end{aligned}$$

Esempio 4 (Identità dei quattro quadrati di Eulero)**.** Un esempio del teorema di Hurwitz nel caso $n = 4$ è l'identità dei quattro quadrati di Eulero, di cui l'identità di Brahmagupta-Fibonacci è un caso particolare.

$$\begin{aligned}&(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ &(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ &(x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2.\end{aligned}$$

Esempio 5 (Identità degli otto quadrati di Degen)**.** Un esempio del teorema di Hurwitz nel caso $n = 8$ è l'identità degli otto quadrati di Degen.

$$
\begin{aligned}
&(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2 + x_8^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 + y_8^2) = \\
&(x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 - x_7y_7 - x_8y_8)^2 + \\
&(x_2y_1 + x_1y_2 + x_4y_3 - x_3y_4 + x_6y_5 - x_5y_6 - x_8y_7 + x_7y_8)^2 + \\
&(x_3y_1 - x_4y_2 + x_1y_3 + x_2y_4 + x_7y_5 + x_8y_6 - x_5y_7 - x_6y_8)^2 + \\
&(x_4y_1 + x_3y_2 - x_2y_3 + x_1y_4 + x_8y_5 - x_7y_6 + x_6y_7 - x_5y_8)^2 + \\
&(x_5y_1 - x_6y_2 - x_7y_3 - x_8y_4 + x_1y_5 + x_2y_6 + x_3y_7 + x_4y_8)^2 + \\
&(x_6y_1 + x_5y_2 - x_8y_3 + x_7y_4 - x_2y_5 + x_1y_6 - x_4y_7 + x_3y_8)^2 + \\
&(x_7y_1 + x_8y_2 + x_5y_3 - x_6y_4 - x_3y_5 + x_4y_6 + x_1y_7 - x_2y_8)^2 + \\
&(x_8y_1 - x_7y_2 + x_6y_3 + x_5y_4 - x_4y_5 - x_3y_6 + x_2y_7 + x_1y_8)^2.
\end{aligned}
$$

Bibliografia

[1] Bruce E. Sagan, The Symmetric Group, Springer (1991)

[2] I. N. Herstein, Noncommutative Rings, The Mathematical Association of America (1968)

[3] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras , Interscience (1962)

[4] Harry Pollard, The Theory of Algebraic Numbers, Mathematical Association of America (1975)