UNIVERSITÀ DEGLI STUDI DI FERRARA

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica
Indirizzo Modelli Matematici per l'Economia

RAPPRESENTAZIONI DI GRUPPI E APPLICAZIONI IN STATISTICA

Relatore:
Chiar.mo Prof.
Josef Eschgfäller

Laureanda:
Valentina Elisa Vitale

Anno Accademico 2009-2010

Indice

Introduzione

La tesi tratta una parte della teoria delle rappresentazioni dei gruppi finiti accennando nell'ultimo capitolo alle possibili applicazioni alla statistica e al calcolo delle probabilità . È costituita da dodici capitoli.

Nel primo vengono definiti i concetti fondamentali per il resto della tesi; vengono infatti date le definizioni di rappresentazioni di un gruppo finito su spazi vettoriali in $\mathbb{C}$ e rappresentazioni matriciali di gruppi. Inoltre, molto importante è la definizione di rappresentazione irriducibile. Alla fine viene enunciato e dimostrato il teorema di Maschke, che afferma che una rappresentazione di un gruppo su uno spazio vettoriale di dimensione finita è completamente riducibile.

Nel secondo capitolo si dimostra il lemma di Schur riguardante le rappresentazioni irriducibili che sta alla base delle relazioni di ortogonalità discusse nei capitoli successivi. Di seguito è stato dimostrato che se G possiede una rappresentazione irriducibile iniettiva, allora $Z(G)$ è un gruppo ciclico e di conseguenza se G è un gruppo abeliano non ciclico, allora G non possiede rappresentazioni irriducibili iniettive.

Nel terzo capitolo viene introdotto il concetto di coefficiente di una rappresentazione matriciale e si ottengono i teoremi di ortogonalità tra i coefficienti. Da esso segue che esiste un solo numero finito di rappresentazioni irriducibili non equivalenti di G. Inoltre si definisce un sistema di Burnside di G come una sequenza $(R_1, \ldots, R_\kappa)$ di rappresentazioni matriciali irriducibili e unitarie non equivalenti di cui con $(n_1, \ldots, n_\kappa)$ denotiamo il vettore delle dimensioni. Viene poi dimostrato che $\sum_{\alpha=1}^{\kappa} n_\alpha^2 \leq |G|$. Tutto ciò dà la base per poter dimostrare, attraverso la teoria dei caratteri che verrà trattata nel quarto capitolo, che $\sum_{\alpha=1}^{\kappa} n_\alpha^2 = |G|$.

Nel capitolo 4 si richiamano il concetto di traccia di una matrice e le sue proprietá, perché da quest'ultime si deduce che rappresentazioni di dimensione finita equivalenti possiedono la stessa traccia. Ciò che si dimostrerà in questo capitolo è che viceversa 2 rappresentazioni di dimensione finita che hanno la stessa traccia sono equivalenti. Inoltre si definisce il concetto di carattere di un gruppo finito G come una funzione $\chi : G \longrightarrow \mathbb{C}$ tale che esiste una rappresentazione irriducibile (matriciale o su uno spazio vettoriale) R tale che $\chi = \operatorname{tr} R$. Dunque i caratteri sono le tracce delle rappresentazioni irriducibili di G. Con l'introduzione dell'algebra di gruppo $(\mathbb{C}^G, +, *)$ di G e la definizione di rappresentazione regolare $L : G \longrightarrow GL(\mathbb{C}G)$ è stato possibile dimostrare il teorema di Burside secondo il quale $\sum_{\alpha=1}^{\kappa} n_\alpha^2 = |G|$ e che i coefficienti $R^i_{j\alpha}$, introdotti nel capitolo precedente, formano una base ortogonale di $\mathbb{C}^G$, per cui in particolare per ogni funzione $f : G \longrightarrow G$ esiste una rappresentazione $f = \sum_{\alpha=1}^{\kappa} \sum_{i=1}^{n_\alpha} \sum_{j=1}^{n_\alpha} \lambda^i_{j\alpha} R^i_{j\alpha}$, con $\lambda^i_{j\alpha} \in \mathbb{C}$ univo-

camente determinati e direttamente calcolabili.

Nel quinto capitolo si lavora sui sistemi di Burnside di G, viene definito il concetto di funzione delle classi. Verrà inoltre dimostrato che ogni carattere è una funzione delle classi. Per poi arrivare a dimostrare un teorema che afferma che κ coincide con il numero delle classi di G. Ciò ha due importanti applicazioni:

(1) Siccome è facile determinare il numero delle classi di G, si può facilmente calcolare il numero delle rappresentazioni irriducibili di G.

(2) La costruzione delle tavole dei caratteri.

Nel sesto capitolo, vengono determinate le rappresentazioni irriducibili di S_3 e la tavola dei caratteri.

Nei capitoli 7 e 8 vengono trattati i caratteri dei gruppi abeliani finiti. In particolare nel settimo capitolo si dà la definizione di carattere di un gruppo abeliano finito, si denota con $\widehat{G}$ il gruppo dei caratteri di G. Viene dimostrato che G è isomorfo a $\widehat{G}$. Mentre nell'ottavo capitolo sono state compilate le tavole dei caratteri di alcuni gruppi abeliani finiti: $\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/4, \mathbb{Z}/5, \mathbb{Z}/6, V_4, S_3$.

Nel nono capitolo troveremo un criterio di irriducibilità attraverso un teorema che afferma che una rappresentazione R di G di dimensione finita è irriducibile se e solo se $\| \operatorname{tr} R\|^2 = |G|$.

Nei capitoli 10 e 11 si sviluppano alcuni richiami all'algebra sugli interi algebrici perché si vuole dimostrare che, se $(R_1, \ldots, R_\kappa)$ è un sistema di Burnside di un gruppo finito G e $(n_1, \ldots, n_\kappa)$ il vettore delle dimensioni, allora n_α divide $|G|$.

L'ultimo capitolo dà l'idea dell'applicazione della teoria delle rappresentazioni dei gruppi finiti in statistica e calcolo delle probabilità . Viene fornito un esempio di un'indagine di mercato nella quale 1200 persone hanno scelto, su 3 prodotti proposti, una graduatoria preferenziale.

1. Il teorema di Maschke

Situazione 1.1. Sia G un gruppo finito.

Definizione 1.2. K sia un campo.

(1) Denotiamo con K^n l'insieme dei *vettori colonna* su K con n elementi e con K_m l'insieme dei *vettori riga* su K con m elementi.
(2) K_m^n sia l'insieme delle *matrici* su K aventi n righe e m colonne. Identifichiamo K_1^n con K^n e K_m^1 con K_m.
(3) $GL(n,K)$ sia il gruppo delle *matrici invertibili* in K_n^n.
Denotiamo con δ l'*elemento neutro* di $GL(n,K)$, cioè la *matrice identità* $n \times n$.
(4) Per uno spazio vettoriale V su K sia $GL(V)$ il *gruppo delle applicazioni lineari invertibili* $V \longrightarrow V$.
Denotiamo con *id* l'applicazione *identità*.

Definizione 1.3.

(1) V sia uno spazio vettoriale su $\mathbb{C}$.
Una rappresentazione di G in V è un *omomorfismo di gruppi* $R : G \longrightarrow GL(V)$.
La rappresentazione si dice di dimensione finita, se $\dim V < \infty$.
(2) Una rappresentazione matriciale di rango n di G è un omomorfismo di gruppi $R : G \longrightarrow GL(n, \mathbb{C})$.
Anche in questo caso diremo spesso semplicemente che R è una *rappresentazione*.

Osservazione 1.4. Si possono naturalmente anche definire in modo analogo rappresentazioni in spazi vettoriali o tramite matrici su un campo arbitrario; in tal caso le rappresentazioni su $\mathbb{C}$ introdotte in 1.3 vengono dette *rappresentazioni ordinarie*.

Situazione 1.5.

(1) Sia V uno spazio vettoriale di dimensione finita n su $\mathbb{C}$ ed $R : G \longrightarrow GL(V)$ una rappresentazione.
Scegliendo una base di V ad ogni $g \in G$ corrisponde una matrice invertibile $S(g)$ ed è immediato che l'applicazione $S : G \longrightarrow GL(n, \mathbb{C})$ è una rappresentazione matriciale.
(2) Se viceversa $S : G \longrightarrow GL(n, \mathbb{C})$ è una rappresentazione matriciale, definendo $R(g) := \bigcirc_x S(g)x : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ otteniamo una rappresentazione $R : G \longrightarrow GL(\mathbb{C}^n)$.

Definizione 1.6. Una rappresentazione matriciale $R : G \longrightarrow GL(n, \mathbb{C})$ si dice *reale*, se le matrici $R(g)$ sono tutte reali.

In tal caso scriveremo anche $R : G \longrightarrow GL(n, \mathbb{R})$.

Definizione 1.7. Una rappresentazione $R : G \longrightarrow GL(n, \mathbb{C})$ si dice *unitaria*, se le matrici $R(g)$ sono tutte unitarie.

Una rappresentazione $R : G \longrightarrow GL(n, \mathbb{R})$ si dice *ortogonale*, se le matrici $R(g)$ sono tutte ortogonali.

Definizione 1.8. V e W siano spazi vettoriali su $\mathbb{C}$. Due rappresentazioni $R : G \longrightarrow GL(V)$ ed $S : G \longrightarrow GL(W)$ si dicono *equivalenti*, se esiste un isomorfismo $\varphi : V \longrightarrow W$ tale che il diagramma

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ W & \xrightarrow{S(g)} & W \end{array}$$

sia commutativo per ogni $g \in G$, cioè tale che si abbia

$S(g) = \varphi \circ R(g) \circ \varphi^{-1}$ per ogni $g \in G$.

Definizione 1.9. Due rappresentazioni matriciali $R : G \longrightarrow GL(n, \mathbb{C})$ ed $S : G \longrightarrow GL(n, \mathbb{C})$ si dicono *equivalenti* se esiste una matrice

$T \in GL(n, \mathbb{C})$ tale che $S(g) = TR(g)T^{-1}$ per ogni $g \in G$.

È chiaro che ciò accade se e solo se le rappresentazioni

$$\bigcirc_g \bigcirc_x R(g)x : \mathbb{C}^n \longrightarrow \mathbb{C}^n \text{ e } \bigcirc_g \bigcirc_x S(g)x : \mathbb{C}^n \longrightarrow \mathbb{C}^n$$

sono *equivalenti* nel senso della definizione 1.8.

Definizione 1.10. K sia un campo e V uno spazio vettoriale su K. Per $E = (e_1, \ldots, e_n)$ con $e_1, \ldots, e_n \in V$ ed $x \in K^n$ poniamo
$Ex := x^1 e_1 + \ldots + x^n e_n$. Se E è una base di V, per ogni $v \in V$ esiste un unico $x \in K^n$ tale che $v = Ex$.

Se inoltre $\varphi : V \longrightarrow V$ è un'applicazione lineare, allora $\varphi v = EAx$, dove $A \in K_n^n$ è la matrice associata a φ rispetto alla base E (che infatti può essere definita in questo modo). Poniamo $\varphi E := (\varphi e_1, \ldots, \varphi e_n)$. Osserviamo in particolare che $e_i = E\delta_i$ e quindi $\varphi e_i = EA_i$ per ogni i.

Per dettagli su questa notazione rimandiamo a Paset, pagg. 36-40.

Definizione 1.11. Sia V uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ *un prodotto scalare* su V. $E = (e_1, \ldots, e_n)$ sia una base di V. Allora definiamo la matrice fondamentale (o di Gram) $\|E, E\|$ ponendo

$\|E, E\|_j^i := \|e_i, e_j\|$

La base E è quindi *ortonormale* rispetto a $\|\|$ se e solo se $\|E, E\| = \delta$.

Definizione 1.12. V sia uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. Un'applicazione lineare $\varphi : V \longrightarrow V$ si dice *unitaria* rispetto a $\|\|$, se $\|\varphi v, \varphi w\| = \|v, w\|$ per ogni $v, w \in V$.

Lemma 1.13. *V sia uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. $\varphi : V \longrightarrow V$ sia un'applicazione lineare, $E = (e_1, \ldots, e_n)$ una base di V ed $A \in \mathbb{C}_n^n$ la matrice associata a φ rispetto alla base E. Allora*

$\|\varphi E, \varphi E\| = A^t \|E, E\| \overline{A}$

Dimostrazione. Per ogni i,j abbiamo

$$\begin{aligned}\|\varphi e_i, \varphi e_j\| = \|EA_i, EA_j\| &= \|\sum_\alpha A_i^\alpha e_\alpha, \sum_\beta A_j^\beta e_\beta\| \\ &= \sum_\alpha \sum_\beta A_i^\alpha \overline{A_j^\beta} \|e_\alpha, e_\beta\| = \sum_\alpha \sum_\beta (A^t)_\alpha^i \|E, E\|_\beta^\alpha \overline{A_j^\beta} \\ &= (A^t \|E, E\|_\beta^\alpha \overline{A})_j^i\end{aligned}$$

Corollario 1.14. *V sia uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. $\varphi : V \longrightarrow V$ sia un'applicazione lineare.*

$E = (e_1, \ldots, e_n)$ sia una base ortonormale rispetto a $\|\|$ ed A la matrice di φ rispetto ad E. Allora sono equivalenti:

(1) φ è unitaria rispetto a $\|\|$.

(2) La matrice A è unitaria, cioè $A^* A = \delta$.

Dimostrazione. Per ipotesi $\|E, E\| = \delta$.

Nel lemma 1.13 abbiamo quindi $\|\varphi E, \varphi E\| = A^t \overline{A}$. Ma φ è unitaria se e solo se $\|\varphi E, \varphi E\| = \|E, E\| = \delta$, e quindi se e solo se $A^t \overline{A} = \delta$. Ma ciò a sua volta è equivalente ad $A^* A = \delta$ come si vede formando il complesso coniugato.

Osservazione 1.15. $R : G \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione e $\|\|$ il prodotto scalare comune su $\mathbb{C}^n$. Per $x, y \in \mathbb{C}^n$ definiamo

$$\|x, y\|_R := \sum_{g \in G} \|R(g)x, R(g)y\|$$

Allora:

(1) $\|\|_R$ è un prodotto scalare su $\mathbb{C}^n$.

(2) Per ogni $g \in G$ l'applicazione $\bigcirc_x R(g)x$ è unitaria rispetto a $\|\|_R$.

Dimostrazione. (1) È immediato che $\|\|_R$ è *sesquilineare*.

Per ogni $x \in \mathbb{C}$ inoltre $\|x, x\|_R = \sum_{g \in G} \|R(g)x, R(g)y\| \geq 0$, siccome ogni sommando è ≥ 0. Per la stessa ragione, se $\|x, x\| = 0$ necessariamente $\|R(g)x, R(g)x\| = 0$ per ogni $g \in G$ e quindi $x = 0$, come si vede ad esempio prendendo $g = 1_G$.

(2) Per $x, y \in \mathbb{C}^n$ e $g \in G$

$$\begin{aligned}\|R(g)x, R(g)y\|_R &= \sum_{h \in G} \|R(h)R(g)x, R(h)R(g)y\| = \\ &= \sum_{h \in G} \|R(hg)x, R(hg)y\| = \sum_{h \in G} \|R(h)x, R(h)y\| = \|x, y\|_R\end{aligned}$$

Teorema 1.16. *Ogni rappresentazione $R : G \longrightarrow GL(n, \mathbb{C})$ è equivalente a una rappresentazione unitaria.*

Dimostrazione. Il prodotto scalare $\|\|\|_R$ sia definito come nell'osservazione 1.15. Sia $e_1, \ldots, e_n$ una base *ortonormale* di $\mathbb{C}^n$ rispetto a $\|\|\|_R$ e $T := (e_1, \ldots, e_n) \in GL(n, \mathbb{C})$. Per $g \in G$ sia $U(g)$ la matrice dell'applicazione lineare $\bigcirc\limits_x R(g)x : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ rispetto alla base $(e_1, \ldots, e_n)$.

Dall'oss. 1.15 e dal cor. 1.14 segue che questa matrice è unitaria. D'altra parte però $U(g) = T^{-1}R(g)T$ come è ben noto e come si vede anche considerando $x = Ty$, $R(g)x = TU(g)y$ e quindi $R(g)Ty = TU(g)y$.

Osservazione 1.17. Per ogni rappresentazione $R : G \longrightarrow GL(n, \mathbb{R})$ esiste una matrice $T \in GL(n, \mathbb{R})$ tale che $T^{-1}R(g)T \in O(n)$ per ogni $g \in G$.

Dimostrazione. È immediato che i ragionamenti che hanno portato al teorema 1.16 possono essere ripetuti per il caso reale.

Osservazione 1.18. V sia uno spazio vettoriale e W_1 e W_2 sottospazi vettoriali di V tali che $V = W_1 \oplus W_2$. Se $e_1, \ldots, e_s$ è una base di W_1 ed $e_{s+1}, \ldots, e_n$ è una base di W_2, allora $e_1, \ldots, e_n$ è una base di V.

Definizione 1.19. V sia uno spazio vettoriale e $\varphi : V \longrightarrow V$ un'applicazione lineare. Un sottospazio vettoriale W di V si dice *φ-invariante*, se $\varphi W \subset W$.

Definizione 1.20. $R : G \longrightarrow GL(V)$ sia una rappresentazione. Un sottospazio vettoriale W di V si dice *R-invariante*, se $R(g)W \subset W$ per ogni $g \in G$.

Si noti che, se inoltre $\dim V < \infty$, questa condizione implica $R(g)W = W$ per ogni $g \in G$.

Lemma 1.21. *V sia uno spazio vettoriale di dimensione finita su un campo K e $\varphi : V \longrightarrow V$ un'applicazione lineare.*

(1) W sia un sottospazio vettoriale φ-invariante di V ed $e_1, \ldots, e_s$ una base di W. Se allunghiamo questa base ad una base $E = (e_1, \ldots, e_n)$ di V, allora la matrice di φ rispetto ad E ha la forma
$$\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$$
con $A \in K_s^s$.

(2) Se viceversa $E = (e_1, \ldots, e_n)$ è una base di V, rispetto alla quale la matrice di φ è della forma
$$\begin{pmatrix} A & X \\ 0 & B \end{pmatrix}$$
con $A \in K_s^s$, allora $W := SV(e_1, \ldots, e_s)$ è un sottospazio vettoriale φ-invariante di V con $\dim W = s$

Proposizione 1.22. *$R : G \longrightarrow GL(V)$ sia una rappresentazione di dimensione finita.*

(1) W sia un sottospazio vettoriale R-invariante di V ed $e_1, \ldots, e_s$ una base di W. Se allunghiamo questa base ad una base $E = (e_1, \ldots, e_n)$ di V, allora per ogni $g \in G$ la matrice di $R(g)$ rispetto ad E ha la forma

$$\begin{pmatrix} A(g) & X(g) \\ 0 & B(g) \end{pmatrix}$$

con $A(g) \in GL(s, \mathbb{C})$.

(2) Se viceversa $E = (e_1, \ldots, e_n)$ *è una base di* V*, rispetto alla quale per ogni* $g \in G$ *la matrice di* $R(g)$ *è della forma*

$$\begin{pmatrix} A(g) & X(g) \\ 0 & B(g) \end{pmatrix}$$

con $A \in GL(s, \mathbb{C})$ *ed* s *non dipende da* g*, allora* $W := SV(e_1, \ldots, e_s)$ *è un sottospazio vettoriale* R*-invariante di* V *con* $\dim W = s$.

(3) In entrambi i casi le applicazioni

$$A := \bigcirc_g A(g) : G \longrightarrow GL(s, \mathbb{C})$$

$$B := \bigcirc_g B(g) : G \longrightarrow GL(n-s, \mathbb{C})$$

sono rappresentazioni matriciali di G.

Lemma 1.23. V *sia uno spazio vettoriale di dimensione finita su un campo* K *e* $\varphi : V \longrightarrow V$ *un'applicazione lineare.*

(1) W_1 *e* W_2 *siano due sottospazi vettoriali* φ*-invariante di* V *tali che* $V = W_1 \oplus W_2$.

$e_1, \ldots, e_s$ *sia una base di* W_1 *ed* $e_{s+1}, \ldots, e_n$ *una base di* W_2*. Per l'oss. 1.18 allora* $e_1, \ldots, e_n$ *è una base di* V *rispetto alla quale la matrice di* φ *è della forma*

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

con $A \in K_s^s$ *e* $B \in K_{n-s}^{n-s}$.

(2) Se viceversa $e_1, \ldots, e_n$ *è una base di* V*, rispetto alla quale la matrice di* φ *è della forma*

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

con $A \in K_s^s$ *e* $B \in K_{n-s}^{n-s}$*, allora gli spazi vettoriali* $W_1 := SV(e_1, \ldots, e_s)$ *e* $W_2 := SV(e_{s+1}, \ldots, e_n)$ *generati rispettivamente da* $e_1, \ldots, e_s$ *e* $e_{s+1}, \ldots, e_n$ *sono entrambi sottospazi vettoriali* φ*-invarianti di* V *tali che* $V = W_1 \oplus W_2$.

Proposizione 1.24. $R : G \longrightarrow GL(V)$ *sia una rappresentazione.*

(1) W_1 *e* W_2 *siano due sottospazi vettoriali* R*-invarianti di* V *tali che* $V = W_1 \oplus W_2$. $e_1, \ldots, e_s$ *sia una base di* W_1 *ed* $e_{s+1}, \ldots, e_n$ *una base di* W_2*. Allora* $e_1, \ldots, e_n$ *è una base di* V *e per ogni* $g \in G$ *la matrice di* $R(g)$ *rispetto ad* E *è della forma*

$$\begin{pmatrix} A(g) & 0 \\ 0 & B(g) \end{pmatrix}$$

con $A(g) \in GL(s, \mathbb{C})$ *e* $B(g) \in GL(n-s, \mathbb{C})$.

(2) Se viceversa $e_1, \ldots, e_n$ è una base di V, rispetto alla quale per ogni $g \in G$ la matrice di $R(g)$ è della forma

$$\begin{pmatrix} A(g) & 0 \\ 0 & B(g) \end{pmatrix}$$

con $A(g) \in GL(s, \mathbb{C})$ ed s non dipende da g, allora $W_1 := SV(e_1, \ldots, e_s)$ e $W_2 := SV(e_{s+1}, \ldots, e_n)$ sono entrambi sottospazi vettoriali R-invarianti di V con $V = W_1 \oplus W_2$.

Definizione 1.25. Una rappresentazione $R : G \longrightarrow GL(V)$ si dice *irriducibile*, se $V \neq 0$ e se gli unici sottospazi vettoriali *R-invarianti* di V sono 0 e V stesso.

Definizione 1.26. $R : G \longrightarrow GL(V)$ sia una rappresentazione. Per $H \subset G$ ed $Y \subset V$ sia $R(H)Y := \{R(h)y \mid h \in H, y \in Y\}$.

Per un vettore $v \in V$ l'insieme $R(G)v$ si chiama l'*orbita* di v sotto R. Questo insieme è finito e lo spazio vettoriale $SV(R(G)v)$ è evidentemente R-*invariante* e di dimensione finita.

Osservazione 1.27. $R : G \longrightarrow GL(V)$ sia una rappresentazione. Allora sono equivalenti:

(1) R è irriducibile.

(2) Per ogni $v \in V$ con $v \neq 0$ lo spazio vettoriale generato dall'orbita di v sotto R coincide con V.

Dimostrazione. (1) $\Longrightarrow$ (2): Ovvio, perché $SV(R(g)v)$ è invariante $\neq 0$.

(2) $\Longrightarrow$ (1): Sia W un sottospazio vettoriale R-invariante $\neq 0$ di V. Allora esiste un $w \in W$ con $w \neq 0$. Per ipotesi $SV(R(G)w) = V$. Però W è R-invariante, per cui $(R(G)w) \subset W$ e quindi anche $SV(R(g)v) \subset W$ e ciò implica $W = V$.

Proposizione 1.28. *La rappresentazione $R : G \longrightarrow GL(V)$ sia irriducibile. Allora $\dim V < \infty$.*

Dimostrazione. Sia $v \in V$ e $v \neq 0$. Per l'oss. 1.27 $SV(R(G)v) = V$. Ma, come già osservato nella def. 1.26, l'orbita $R(g)v$ è finita e dunque $\dim V < \infty$.

Definizione 1.29. $R : G \longrightarrow GL(V)$ sia una rappresentazione e W un sottospazio vettoriale di V.

Allora possiamo considerare l'applicazione

$$\begin{aligned} R_W : G &\longrightarrow GL(W) \\ g &\longmapsto \bigcirc_w R(g)w \end{aligned}$$

Essa è evidentemente ben definita e una rappresentazione di G.

Definizione 1.30. (1) $R : G \longrightarrow GL(V)$ sia una rappresentazione e W_1 e W_2 sottospazi vettoriali *R-invarianti* di V tali che $V = W_1 \oplus W_2$.

Allora scriviamo $R = R_{W_1} \oplus R_{W_2}$.

(2) Se viceversa sono date due rappresentazioni $R_1 : G \longrightarrow GL(V_1)$ e $R_2 : G \longrightarrow GL(V_2)$, allora possiamo definire una rappresentazione

$$R_1 \oplus R_2 := \bigcirc_g \bigcirc_{(v_1,v_2)} (R_1(g)v_1, R_2(g)v_2) : G \longrightarrow GL(V_1 \oplus V_2)$$

Le interpretazioni della *somma diretta* di due rappresentazioni contenute nei punti (1) e (2) sono equivalenti; le rappresentazioni matriciali corrispondenti si ottengono come nella proposizione 1.24.

(3) La *somma diretta* di due rappresentazioni matriciali

$R_1 : G \longrightarrow GL(n_1, \mathbb{C})$ ed $R_2 : G \longrightarrow GL(n_2, \mathbb{C})$

è definita, in accordo con quanto sopra, ponendo

$$(R_1 \oplus R_2)(g) := \begin{pmatrix} R_1(g) & 0 \\ 0 & R_2(g) \end{pmatrix}$$

Definizione 1.31. Una rappresentazione $R : G \longrightarrow GL(V)$ si dice *completamente irriducibile*, se R può essere scritta come somma diretta $R = R_1 \oplus \ldots \oplus R_s$ in cui ogni R_i è *irriducibile*.

Dalla proposizione 1.28 segue che in tal caso $0 < \dim V < \infty$.

Definizione 1.32. V sia uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. Per un sottoinsieme X di V poniamo

$$X^\perp := \{v \in V \mid \|x, v\| = 0 \text{ per ogni } x \in X\}$$

È chiaro che $X^\perp$ è un sottospazio vettoriale di V (anche quando X stesso non è un sottospazio vettoriale).

Nota 1.33. V sia uno spazio vettoriale di dimensione finita su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. W sia un sottospazio vettoriale di V. Allora:

(1) $W \cap W^\perp = 0$.

(2) $\dim V = \dim V + \dim V^\perp$.

(3) $(W^\perp)^\perp = W$.

(4) $V = W \oplus W^\perp$.

Dimostrazione. Corsi di geometria.

Definizione 1.34. V sia uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. Una rappresentazione $R : G \longrightarrow GL(V)$ si dice *unitaria* rispetto a $\|\|$, se per ogni $g \in G$ l'applicazione $R(g)$ è *unitaria* rispetto a $\|\|$ (cfr. def. 1.7).

Lemma 1.35. *V sia uno spazio vettoriale su $\mathbb{C}$ e $\|\|$ un prodotto scalare su V. $R : G \longrightarrow GL(V)$ sia una rappresentazione unitaria rispetto a $\|\|$ e W un sottospazio vettoriale R-invariante di V. Allora:*

(1) La rappresentazione $R_W : G \longrightarrow GL(W)$ è unitaria rispetto alla restrizione del prodotto scalare $\|\|$ a W.

(2) Anche $W^\perp$ è un sottospazio vettoriale R-invariante di V.

(3) La $\dim V < \infty$*, allora* $R = R_W \oplus R_{W^\perp}$.

Dimostrazione. (1) Chiaro.

(2) Siano $v \in W^\perp$ e $g \in G$. Per ogni $w \in W$ allora

$$\|R(g)v, w\| = \|R(g)v, R(g)R(g^{-1})w\| = \|v, R(g^{-1})w\| = 0$$

perché per ipotesi $R(g^{-1})w \in W$.

(3) Ciò segue dalla nota 1.33, tenendo conto del punto (2).

Teorema 1.36 (teorema di Maschke). $R : G \longrightarrow GL(V)$ *sia una rappresentazione e* $0 < \dim V < \infty$*. Allora* R *è completamente riducibile.*

Dimostrazione. Per il teorema 1.16 possiamo assumere che su V sia dato un prodotto scalare rispetto al quale R è unitaria. Per ipotesi $V \neq 0$.

(1) Assumiamo che R non sia *irriducibile*. Allora esiste un sottospazio vettoriale R*-invariante* W di V con $0 < \dim W < \dim V$. Per il lemma 1.35 $R = R_W \oplus R_{W^\perp}$, mentre dal punto (2) della nota 1.33 segue che anche $0 < \dim W^\perp < \dim V$.

(2) Se le rappresentazioni R_W e $R_{W^\perp}$ sono entrambe irriducibili, abbiamo dimostrato l'enunciato. Altrimenti ripetiamo il ragionamento del punto (1) sia per R_W che per $R_{W^\perp}$, entrambe di dimensione finita minore della dimensione di partenza.

Corollario 1.37. *Ogni rappresentazione* 1*-dimensionale di* G *è irriducibile.*

Definizione 1.38. L'*esponente* di G è il più piccolo numero naturale $m \neq 0$ tale che $g^m = 1_G$ per ogni $g \in G$.

Ricordiamo che anche $g^{|G|} = 1_G$ per ogni $g \in G$.

Osservazione 1.39. L'esponente di G divide l'ordine di G.

Dimostrazione. Sia $H := \{n \in \mathbb{Z} \mid g^n = 1_G \text{ per ogni } g \in G\}$. Allora H è un sottogruppo $\neq 0$ di $\mathbb{Z}$. Dal corso di Algebra sappiamo che $H = m\mathbb{Z}$, dove m è il più piccolo elemento > 0 di H. Perciò m coincide con l'esponente di G. Siccome $|G| \in H$, vediamo che $|G|$ è un multiplo di m.

Osservazione 1.40. Una rappresentazione matriciale 1-dimensionale è per definizione un omomorfismo di gruppi

$$R : G \longrightarrow GL(1, \mathbb{C}) = (\mathbb{C} \setminus 0, \cdot)$$

Siano m l'esponente di G e $g \in G$. Allora $g^m = 1_G$, per cui

$$(R(g))^m = R(g^m) = R(1_G) = 1$$

cosicché $R(g)$ è una m-esima radice dell'unità e quindi (o per la stessa ragione) anche una $|G|$-esima radice dell'unità .

In particolare $|R(g)| = 1$ e $R(g^{-1}) = \overline{R(g)}$.

Osservazione 1.41. Due rappresentazioni matriciali 1-*dimensionali* sono equivalenti se e solo se coincidono.

Dimostrazione. Ciò è chiaro dalla def. 1.3, perché il gruppo $GL(1, \mathbb{C})$ è commutativo.

Osservazione 1.42. Se due rappresentazioni 1-*dimensionali* R, $S : G \longrightarrow GL(V)$ nello stesso spazio vettoriale sono equivalenti, allora coincidono.

Dimostrazione. Per ipotesi esiste esiste un isomorfismo $\varphi : V \longrightarrow V$ tale che il diagramma

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ V & \xrightarrow{S(g)} & V \end{array}$$

sia commutativo per ogni $g \in G$. Siccome però $\dim V = 1$, deve esistere un $\lambda \in \mathbb{C} \setminus 0$ tale che $\varphi v = \lambda v$ per ogni $v \in V$.

Per ogni $v \in V$ ed ogni $g \in G$ allora abbiamo

$$S(g)v = \varphi R(g)\varphi^{-1}v = \lambda R(g)\lambda^{-1}v = R(g)v$$

2. Il lemma di Schur

Situazione 2.1. G sia un gruppo finito.

Nota 2.2. Siano date due rappresentazioni $R : G \longrightarrow GL(V)$ ed $S : G \longrightarrow GL(W)$ e un'applicazione lineare $\varphi : V \longrightarrow W$ che rende commutativo il diagramma

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ W & \xrightarrow{S(g)} & W \end{array}$$

per ogni $g \in G$. Se φ è un isomorfismo, le due rappresentazioni sono (per definizione) equivalenti. Cosa si può dedurre invece dalla situazione più generale, in cui φ non è un isomorfismo?

Il lemma di Schur afferma che allora, se le rappresentazioni R ed S sono entrambe irriducibili, l'applicazione φ è identicamente nulla.

Osservazione 2.3. Nella definizione 2.2 $\ker\varphi$ è R-invariante, $\operatorname{im}\varphi$ è S-invariante.

Dimostrazione. Sia $g \in G$.

(1) Sia $v \in \ker\varphi$. Allora $\varphi(R(g)v) = S(g)\varphi v = S(g)0 = 0$, e vediamo che $R(g)v \in \ker\varphi$.

(2) Sia $w \in \operatorname{im}\varphi$. Allora esiste $v \in V$ tale che $w = \varphi v$, per cui $S(g)w = S(g)\varphi v = \varphi R(g)v \in \operatorname{im}\varphi$.

Teorema 2.4 (lemma di Schur). *Siano date due rappresentazioni irriducibili $R : G \longrightarrow GL(V)$ ed $S : G \longrightarrow GL(W)$ e un'applicazione lineare $\varphi : V \longrightarrow W$ che rende commutativo il diagramma*

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ W & \xrightarrow{S(g)} & W \end{array}$$

per ogni $g \in G$. Se $\varphi \neq 0$, allora φ è un isomorfismo.

Dimostrazione. Usiamo l'osservazione 2.3.

(1) Siccome $\varphi \neq 0$, abbiamo $\ker\varphi \neq V$ e $\operatorname{im}\varphi \neq 0$. $\ker\varphi$ è un sottospazio R-invariante di V e quindi per ipotesi si ha $\ker\varphi = 0$ oppure $\ker\varphi = V$ e quindi necessariamente $\ker\varphi = 0$.

(2) $\operatorname{im}\varphi$ è un sottospazio S-invariante di W e quindi per ipotesi $\operatorname{im}\varphi = 0$ oppure $\operatorname{im}\varphi = W$. Ciò implica $\operatorname{im}\varphi = W$.

Corollario 2.5. *Le rappresentazioni matriciali $R : G \longrightarrow GL(n, \mathbb{C})$ ed $S : G \longrightarrow GL(n, \mathbb{C})$ siano irriducibili e $T \in \mathbb{C}_n^m$ una matrice tale che $TR(g) = S(g)T$ per ogni $g \in G$.*

Se $T \neq 0$, allora $n = m$ e la matrice T è invertibile.

Teorema 2.6. *$R : G \longrightarrow GL(V)$ sia una rappresentazione. Allora sono equivalenti:*

(1) R è irriducibile.

(2) $0 < \dim V < \infty$ e per ogni applicazione lineare $\varphi : V \longrightarrow V$ che rende commutativo il diagramma

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ V & \xrightarrow{R(g)} & V \end{array}$$

per ogni $g \in G$, esiste $\lambda \in \mathbb{C}$ tale che $\varphi = \lambda \,\mathrm{id}$.

Dimostrazione. (1) $\Longrightarrow$ (2): Per ipotesi $V \neq 0$ e dalla proposizione 1.28 segue che $\dim V < \infty$. Ciò implica che esiste $\lambda \in \mathbb{C}$ tale che l'applicazione $\varphi - \lambda id$ non è invertibile. È chiaro che per ogni $g \in G$ commuta anche il diagramma

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle\varphi-\lambda id}\downarrow & & \downarrow{\scriptstyle\varphi-\lambda id} \\ V & \xrightarrow{R(g)} & V \end{array}$$

Il lemma di Schur implica che $\varphi - \lambda id = 0$, cioè $\varphi = \lambda id$.

(2) $\Longrightarrow$ (1): R non sia irriducibile. Per il teorema di Maschke possiamo scrivere $V = W_1 \oplus W_2$ con sottospazi R-invarianti non banali.

Sia $\varphi : V \longrightarrow V$, la proiezione su W_1. È chiaro che φ commuta con $R(g)$ per ogni $g \in G$:

$R(g)\varphi(w_1 + w_2) = R(g)w_1$

$\varphi R(g)(w_1 + w_2) = \varphi R(g)w_1 + \varphi R(g)w_2 = \varphi R(g)w_1$

per $w_1 \in W_1$ e $w_2 \in W_2$.

Per ipotesi esiste $\lambda \in \mathbb{C}$ tale che $\varphi = \lambda id$, e ciò è impossibile.

Corollario 2.7. *$R : G \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione matriciale. Allora sono equivalenti:*

(1) R è irriducibile.

(2) Per ogni matrice $T \in \mathbb{C}_n^n$ tale che $R(g)T = TR(g)$ per ogni $g \in G$ esiste $\lambda \in \mathbb{C}$ tale che $T = \lambda\, \delta$.

Definizione 2.8. Il *centro* $Z(G)$ di G è definito da

$Z(G) := \{a \in G \mid ag = ga$ per ogni $g \in G\}$

Osservazione 2.9. $Z(G)$ è un sottogruppo normale di G.

Nota 2.10. $R : G \longrightarrow GL(V)$ sia una rappresentazione ed $a \in Z(G)$. Allora l'applicazione $R(a) : V \longrightarrow V$ è lineare e invertibile e rende commutativo il diagramma

$$\begin{array}{ccc} V & \xrightarrow{R(g)} & V \\ {\scriptstyle R(a)}\downarrow & & \downarrow{\scriptstyle R(a)} \\ V & \xrightarrow{R(g)} & V \end{array}$$

per ogni $g \in G$. Se R è irriducibile, per il teorema 2.6 esiste $\lambda \in \mathbb{C} \setminus 0$ tale che $R(a) = \lambda \,\mathrm{id}$.

Proposizione 2.11. *Se G è un gruppo abeliano, ogni rappresentazione irriducibile di G è 1-dimensionale.*

Dimostrazione. Per ipotesi si ha $Z(G) = G$. Sia data una rappresentazione irriducibile $R : G \longrightarrow GL(V)$. Per la nota 2.10 per ogni $g \in G$ esiste $\lambda \in \mathbb{C}$ tale che $R(g) = \lambda id$. Ma ciò implica che ogni sottospazio vettoriale di V è R-invariante e, siccome R è irriducibile, necessariamente $\dim V = 1$.

Lemma 2.12. *K sia un campo ed H un sottogruppo finito di $(K \setminus 0, \cdot)$. Allora H è ciclico.*

Dimostrazione. Corsi di Algebra.

Proposizione 2.13. *Se G possiede una rappresentazione irriducibile iniettiva, allora $Z(G)$ è un gruppo ciclico.*

Dimostrazione. $R : G \longrightarrow GL(V)$ sia una rappresentazione irriducibile iniettiva. Per la nota 2.10 per ogni $a \in Z(G)$ esiste un $\lambda_a \in \mathbb{C} \setminus 0$ tale che $R(a) = \lambda_a id$. Per l'iniettività di R il numero λ_a è univocamente determinato e ciò a sua volta implica che l'applicazione $\bigcirc\!\!\!\!\!\!\int_a \lambda_a : Z(G) \longrightarrow (\mathbb{C} \setminus 0, \cdot)$ è un omomorfismo iniettivo e quindi $Z(G)$ è isomorfo ad un sottogruppo (necessariamente finito) di $(\mathbb{C}\setminus 0, \cdot)$. Questo sottogruppo è ciclico per il lemma 2.12.

Corollario 2.14. *G sia un gruppo abeliano non ciclico. Allora G non possiede rappresentazioni irriducibili iniettive.*

Osservazione 2.15. Il cor. 2.14 può essere dedotto direttamente dalla prop. 2.11, senza utilizzare la prop. 2.13. Infatti sia R una rappresentazione irriducibile di G. Per la prop. 2.11 R è un omomorfismo $R : G \longrightarrow (\mathbb{C} \setminus 0, \cdot)$. Se G non è ciclico, esiste un $m < |G|$ tale che $g^m = 1$ per ogni $g \in G$. Perciò $R(G)$ è un sottoinsieme dell'insieme $\{z \in \mathbb{C} \mid z^m = 1\}$ e ciò implica $|R(G)| \leq m$. Ma allora R non può essere iniettiva.

3. Teoremi di ortogonalità per i coefficienti

Situazione 3.1. G sia un gruppo finito.

Definizione 3.2. $R : G \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione matriciale. Per ogni i,$j \in \{1, \ldots, n\}$ otteniamo una funzione $R^i_j \in \mathbb{C}^G$ definita da $R^i_j(g) := (R(g))^i_j$.

Le funzioni così ottenute si dicono *coefficienti* di R.

In modo simile definiamo le funzioni $R^i : G \longrightarrow \mathbb{C}_n$ ed $R_j : G \longrightarrow \mathbb{C}^n$ tramite $R^i(g) := (R(g))^i$ e $R_j(g) := (R(g))_j$.

Definizione 3.3. E sia un gruppo abeliano ed $F : G \longrightarrow E$ un'applicazione. Allora poniamo

$$[F] := \sum_{g \in G} F(g)$$

Lemma 3.4. *$R : G \longrightarrow GL(n, \mathbb{C})$ ed $S : G \longrightarrow GL(m, \mathbb{C})$ siano rappresentazioni matriciali ed $A \in \mathbb{C}^n_m$. Sia*

$$P := [RAS^{-1}] = \sum_{g \in G} R(g)AS(g^{-1})$$

Allora $R(g)P = PS(g)$ per ogni $g \in G$.

Dimostrazione. Sia $g \in G$. Allora

$$R(g)P = R(g) \sum_{h \in G} R(h)AS(h^{-1}) = \sum_{h \in G} R(gh)AS(h^{-1}) =$$
$$= \sum_{h \in G} R(h)AS(h^{-1}g)$$

$$PS(g) = (\sum_{h \in G} R(h)AS(h^{-1}))S(g) = \sum_{h \in G} R(h)AS(h^{-1}g)$$

Corollario 3.5. *$R : G \longrightarrow GL(n, \mathbb{C})$ ed $S : G \longrightarrow GL(m, \mathbb{C})$ siano rappresentazioni matriciali e $1 \leq j \leq n$, $1 \leq k \leq m$. Sia*

$$P := [R_j(S^{-1})^k] = \sum_{g \in G} R_j(g)S^k(g^{-1})$$

Allora $R(g)P = PS(g)$ per ogni $g \in G$.

Dimostrazione. $R_j(S^{-1})^k = R\delta_i\delta^k S^{-1}$, cosicché si tratta di un caso speciale del lemma con $A = \delta_i\delta^k$.

Teorema 3.6. *$R : G \longrightarrow GL(n, \mathbb{C})$ ed $S : G \longrightarrow GL(m, \mathbb{C})$ siano rappresentazioni matriciali irriducibili e non equivalenti. Per ogni scelta di indici i,j,k,l allora*

$$\sum_{g \in G} R^i_j(g)S^k_l(g^{-1}) = 0$$

Dimostrazione. Per il cor. 3.5 $R(g)[R_j(S^{-1})^k] = [R_j(S^{-1})^k]S(g)$ per ogni $g \in G$. Il lemma di Schur implica $[R_j(S^{-1})^k] = 0$ (altrimenti R ed S sarebbero equivalenti) e da ciò segue l'enunciato.

Teorema 3.7. *$R : G \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione matriciale irriducibile. Siano $i,j,k,l \in \{1, \ldots, n\}$. Allora:*

(1) $\sum_{g \in G} R^i_j(g) R^j_i(g^{-1}) = \frac{|G|}{n}$.

(2) $\sum_{g \in G} R^i_j(g) R^k_l(g^{-1}) = 0 \quad$ *se* $(i, j) \neq (l, k)$.

Dimostrazione. Per il cor. 3.5 abbiamo
$R(g)[R_j(R^{-1})^k] = [R_j(R^{-1})^k]R(g)$ per ogni $g \in G$, cosicché per il cor. 2.7 esiste $\lambda^k_j \in \mathbb{C}$ tale che $[R_j(R^{-1})^k] = \lambda^k_j \delta$. Adesso distinguiamo due casi:

(1) Per $i \neq l$ quindi $0 = \sum_{g \in G} R^i_j(g) R^k_l(g^{-1})$.

(2) Per $i = l$ otteniamo invece $\lambda^k_j = \sum_{g \in G} R^i_j(g) R^k_i(g^{-1})$ e sommando su i si ha

$$n\lambda^k_j = \sum_{i=1}^{n} \sum_{g \in G} R^i_j(g) R^k_i(g^{-1}) = \sum_{g \in G} \sum_{i=1}^{n} R^k_i(g^{-1}) R^i_j(g) =$$
$$= \sum_{g \in G} R^k_j(1_G) = \sum_{g \in G} \delta^k_j = \delta^k_j \, |G|$$

Per $j \neq k$ perciò $\lambda^k_j = 0$, mentre $\lambda^j_j = \frac{|G|}{n}$.

Definizione 3.8. In $\mathbb{C}^G$ denotiamo con $\|\|$ il prodotto scalare comune, quindi

$$\|u, v\| = \sum_{g \in G} u(g)\overline{v(g)} = [u\overline{v}]$$

Osservazione 3.9. $R \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione matriciale unitaria. Per ogni $g \in G$ allora $R(g^{-1}) = (R(g))^*$. Per ogni coppia di indici i,j abbiamo quindi $R^i_j(g^{-1}) = \overline{R^j_i(g)}$.

Corollario 3.10. *$R : G \longrightarrow GL(n, \mathbb{C})$ ed $S : G \longrightarrow GL(m, \mathbb{C})$ siano rappresentazioni matriciali irriducibili e non equivalenti. La rappresentazione S sia unitaria. Per ogni scelta di indici i,j,k,l allora $\|R^i_j, S^l_k\| = 0$.*

Corollario 3.11. *$R : G \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione matriciale irruducibile e unitaria. Per ogni scelta di indici i,j,k,l allora $\|R^i_j, R^l_k\| = \delta^i_l \delta^j_k \frac{|G|}{n}$.*

Teorema 3.12. *Esiste solo un numero finito di rappresentazioni irriducibili non equivalenti di G.*

Dimostrazione. Per il teorema 1.16 in ogni classe di rappresentazioni irriducibili possiamo scegliere una rappresentazione unitaria R. Essa

determina una funzione $R_1^1 : G \longrightarrow \mathbb{C}$ che, per il corollario 3.10, è ortogonale ai primi coefficienti dei rappresentanti delle altre classi. Ma in $\mathbb{C}^G$ esistono al massimo $|G|$ funzioni ortogonali tra di loro.

Definizione 3.13. κ sia il numero delle rappresentazioni irriducibili non equivalenti di G. Dal teorema 3.12 sappiamo che κ è finito.

Definizione 3.14. Un *sistema di Burnside* di G è una sequenza $(R_1, \ldots, R_\kappa)$ di rappresentazioni matriciali irriducibili e unitarie non equivalenti $R_\alpha : G \longrightarrow GL(n_\alpha, \mathbb{C})$ per $\alpha = 1, \ldots, \kappa$ in cui $R_1 := \bigcirc_g 1$ coincide con la rappresentazione banale. Denotiamo in questo caso i coefficienti di R_α con $R^i_{j\alpha}$. Il vettore $(n_1, \ldots, n_\kappa)$ si chiama il *vettore delle dimensioni* del sistema.

Teorema 3.15. *$(n_1, \ldots, n_\kappa)$ sia il vettore delle dimensioni di un sistema di Burnside di G. Allora $n_1^2 + \ldots + n_\kappa^2 \leq |G|$.*

Dimostrazione. Per ogni $\alpha \in \{1, \ldots, k\}$ e ogni i,$j \in \{1, \ldots, n_\alpha\}$ abbiamo un coefficiente $R^i_{j\alpha} \in \mathbb{C}^G$. Per i cor. 3.10 e 3.11 questi coefficienti sono tra di loro ortogonali. Il loro numero non può quindi superare $|G|$.

Osservazione 3.16. Tramite la teoria dei caratteri saremo in grado di dimostrare che in questa osservazione si ha uguaglianza:
$n_1^2 + \ldots + n_\kappa^2 = |G|$.

4. Il teorema di Burnside

Situazione 4.1. G sia un gruppo finito.

Come nella def. 3.8 sia $|||$ il prodotto scalare comune su $\mathbb{C}^G$.

Definizione 4.2. Sia $A \in \mathbb{C}_n^n$. Definiamo la *traccia* di A, denotata con $\operatorname{tr} A$, come la somma degli elementi sulla diagonale principale di A, quindi $\operatorname{tr} A := \sum_{i=1}^{n} A_i^i$. È chiaro che l'applicazione $\operatorname{tr} : \mathbb{C}_n^n \longrightarrow \mathbb{C}$ è lineare.

Proposizione 4.3. *Siano* $A \in \mathbb{C}_m^n$, $B \in \mathbb{C}_n^m$. *Allora* $\operatorname{tr} AB = \operatorname{tr} BA$.

Si noti che $AB \in \mathbb{C}_n^n$, $BA \in \mathbb{C}_m^m$.

Dimostrazione.

$$\operatorname{tr} AB = \sum_{i=1}^{n} (AB)_i^i = \sum_{i=1}^{n} \sum_{\alpha=1}^{m} A_\alpha^i B_i^\alpha = \sum_{\alpha=1}^{m} \sum_{i=1}^{n} B_i^\alpha A_\alpha^i =$$
$$= \sum_{\alpha=1}^{m} (BA)_\alpha^\alpha = \operatorname{tr} BA$$

Corollario 4.4. *Siano* $A \in \mathbb{C}_n^n$ *e* $T \in GL(n, \mathbb{C})$. *Allora* $\operatorname{tr} T^{-1}AT = \operatorname{tr} A$.

Definizione 4.5. (1) $R : G \longrightarrow GL(n, \mathbb{C})$ sia una rappresentazione matriciale di G. Allora $\operatorname{tr} R := \bigcirc_g \operatorname{tr} R(g) : G \longrightarrow \mathbb{C}$ si chiama la traccia di R.

(2) $R : G \longrightarrow GL(V)$ sia una rappresentazione di dimensione finita di G. Per il cor. 4.4 l'applicazione $\operatorname{tr} R := \bigcirc_g \operatorname{tr} R(g) : G \longrightarrow \mathbb{C}$ è ben definita e si chiama la traccia di R.

Osservazione 4.6. Dal cor. 4.4 è immediato che rappresentazioni di dimensione finita equivalenti possiedono la stessa traccia. Dimostreremo in questo capitolo che viceversa due rappresentazioni di dimensione finita che hanno la stessa traccia sono equivalenti. Siccome è molto facile calcolare la traccia, possiamo altrettanto facilmente stabilire se due rappresentazioni di dimensione finita sono equivalenti.

Definizione 4.7. Un *carattere* di G è una funzione $\chi : G \longrightarrow \mathbb{C}$ tale che esiste una rappresentazione irriducibile (matriciale o su uno spazio vettoriale) R tale che $\chi = \operatorname{tr} R$.

I caratteri di G sono quindi le tracce delle rappresentazioni irriducibili di G. Ricordiamo che per la prop. 1.28 ogni rappresentazione irriducibile di G è di dimensione finita e quindi possiede una traccia.

Situazione 4.8. $(R_1, \ldots, R_\kappa)$ sia un sistema di Burnside fissato di G ed $(n_1, \ldots, n_\kappa)$ il corrispondente vettore delle dimensioni. Per ogni $\alpha = 1, \ldots, \kappa$ sia $\chi_\alpha := \operatorname{tr} R_\alpha$. Allora i caratteri di G sono esattamente le funzioni $\chi_1, \ldots, \chi_\kappa$.

Siccome per la def. 3.14 $R_1 = \bigcirc_g 1$, il carattere χ_1 (detto *carattere banale*) coincide con la funzione costante $\bigcirc_g 1$.

Osservazione 4.9. Faremo adesso vedere come le relazioni di ortogonalità per i coefficienti si traducono in relazioni di ortogonalità per i caratteri.

Teorema 4.10. *Per* $\alpha,\beta \in \{1,\dots,\kappa\}$ *vale* $\|\chi_\alpha, \chi_\beta\| = |G|\,\delta^\alpha_\beta$.

Dimostrazione.

$$\|\chi_\alpha, \chi_\beta\| = \sum_{g\in G} \chi_\alpha(g)\overline{\chi_\beta(g)} = \sum_{g\in G}\sum_{j=1}^{n_\alpha}\sum_{k=1}^{n_\beta}(R_\alpha)^j_j(g)\overline{(R_\beta)^k_k(g)} =$$
$$= \sum_{j=1}^{n_\alpha}\sum_{k=1}^{n_\beta}\sum_{g\in G}(R_\alpha)^j_j(g)(R_\beta)^k_k(g^{-1}) = |G|\,\delta^\alpha_\beta$$

Definizione 4.11. Per una rappresentazione (vettoriale o matriciale) di R di G ed $m \in \mathbb{N}$ sia $mR := \underbrace{R \oplus \ldots \oplus R}_{m \text{ volte}}$.

Proposizione 4.12. *Siano* $m_1,\dots,m_\kappa \in \mathbb{N}$ *ed* $R := m_1R_1 \oplus \ldots \oplus m_\kappa R_\kappa$.

Per ogni $\alpha \in \{1,\dots,\kappa\}$ *allora* $m_\alpha = \dfrac{1}{|G|}\,\|\chi_\alpha, \operatorname{tr} R\|$.

Il numero m_α *è in particolare univocamente determinato.*

Dimostrazione. Siccome

$\operatorname{tr} R = m_1 \operatorname{tr} R_1 + \ldots + m_\kappa \operatorname{tr} R_\kappa$

dal teorema 4.10 segue $\|\chi_\alpha, \operatorname{tr} R\| = \|\chi_\alpha, m_\alpha\chi_\alpha\|$ e ciò implica il risultato.

Corollario 4.13. *Ogni rappresentazione di dimensione finita di* G *è equivalente a una rappresentazione della forma* $m_1R_1 \oplus \ldots \oplus m_\kappa R_\kappa$ *con* $m_1,\dots,m_\kappa \in \mathbb{N}$.

Dimostrazione. Per il teorema di Maschke R è completamente riducibile, cioè può essere scritto come $R = R_1 \oplus \ldots \oplus R_\kappa$ dove gli R_i sono irriducibili. Per la rappresentazione 0-dimensionale prendiamo $m_1 = \ldots = m_\kappa = 0$. L'unicità segue dalla prop. 4.12.

Teorema 4.14. *R ed S siano due rappresentazioni di dimensione finita di G. Allora R ed S sono equivalenti se e solo se possiedono la stessa traccia*

Dimostrazione. (1) R ed S siano equivalenti. Dall'oss. 4.6 sappiamo che le tracce di R ed S coincidono.

(2) Sia $\operatorname{tr} R = \operatorname{tr} S$. Per il cor. 4.13 R è equivalente a una rappresentazione $m_1R_1 \oplus \ldots \oplus m_\kappa R_\kappa$, S a una rappresentazione $l_1R_1 \oplus \ldots \oplus l_\kappa R_\kappa$

con $m_1, \ldots, m_\kappa, l_1, \ldots, l_\kappa \in \mathbb{N}$. Dalla prop. 4.12 per ogni $\alpha \in \{1, \ldots, \kappa\}$ si ha però $m_\alpha = \dfrac{1}{|G|} \|\chi_\alpha, \operatorname{tr} R\| = \dfrac{1}{|G|} \|\chi_\alpha, \operatorname{tr} S\| = l_\alpha$.

Per la transitività della relazione di equivalenza ciò implica che R è equivalente ad S.

Definizione 4.15. Sullo spazio vettoriale $\mathbb{C}^G$ introduciamo come moltiplicazione la *convoluzione* $*$ definita da

$$u * v := \bigcirc_g \sum_{h \in G} u(h) v(h^{-1} g)$$

Si verifica facilmente che questa operazione è associativa, mentre è chiaro che è bilineare.

$(\mathbb{C}^G, +, *)$ è quindi una $\mathbb{C}$-algebra che si chiama l'*algebra di gruppo* di G. Essa viene denotata con $\mathbb{C}G$.

Osservazione 4.16. Le algebre $\mathbb{C}^G$ e $\mathbb{C}G$ coincidono come insiemi e come spazi vettoriali, si distinguono invece come anelli, cioè nella moltiplicazione: $\mathbb{C}^G = (\mathbb{C}^G, +, \cdot)$, mentre $\mathbb{C}G = (\mathbb{C}^G, +, *)$.

Definizione 4.17. Per $a \in G$ sia $\varepsilon_a \in \mathbb{C}G$ definita da

$$\varepsilon_a(x) := (x = a) = \begin{cases} 1 & \text{se } x = a \\ 0 & \text{altrimenti} \end{cases}$$

È chiaro che l'applicazione $\varepsilon := \bigcirc_a \varepsilon_a : G \longrightarrow \mathbb{C}G$ è iniettiva.

Osservazione 4.18. ε_{1_G} è l'elemento neutro (rispetto alla convoluzione) di $\mathbb{C}G$.

Dimostrazione. Per $u \in \mathbb{C}G$ e $g \in G$ abbiamo

$$u * \varepsilon_{1_G}(g) = \sum_{h \in G} u(h)(h^{-1} g = 1_G) = u(g)$$

$$\varepsilon_{1_G}(g) * u = \sum_{h \in G} (h = 1_G) u(h^{-1} g) = u(g)$$

Osservazione 4.19. L'applicazione $\varepsilon : G \longrightarrow (\mathbb{C}G, *)$ è un omomorfismo di semigruppi. Insieme all'oss. 4.18 ciò mostra che G può in modo naturale essere considerato come sottomonoide di $(\mathbb{C}G, *)$.

Dimostrazione. Dati $a, b \in G$ dobbiamo dimostrare che $\varepsilon_{ab} = \varepsilon_a * \varepsilon_b$. Sia $g \in G$. Allora

$$(\varepsilon_a * \varepsilon_b)(g) = \sum_{h \in G} (h = a)(h^{-1} g = b) = (g = ab) = \varepsilon_{ab}(g)$$

Osservazione 4.20. G, o più precisamente l'insieme $\{\varepsilon_a \mid a \in G\}$, costituisce una base di $\mathbb{C}^G$ e quindi anche di $\mathbb{C}G$ (che come spazio vettoriale coincide con $\mathbb{C}^G$).

Per $u \in \mathbb{C}^G$ si ha $u = \sum_{a \in G} u(a) \varepsilon_a$.

Dimostrazione. (1) Sia $g \in G$. Allora

$$\sum_{a\in G} u(a)\varepsilon_a(g) = \sum_{a\in G} u(a)(g=a) = u(g)$$

Ciò mostra che G genera $\mathbb{C}^G$.

(2) Dimostriamo la lineare indipendenza.

Sia $\lambda_a \in \mathbb{C}$ per ogni $a \in G$ e $\sum \lambda_a\varepsilon_a = 0$. Per ogni $g \in G$ allora

$$0 = \sum_{a\in G} \lambda_a(a=g) = \lambda_g.$$

Osservazione 4.21. Siano $G = \{a_1, \ldots, a_N\}$ con gli elementi $a_1, \ldots, a_N$ tutti distinti ed u,$v \in \mathbb{C}G$. Allora esistono $\alpha_1, \ldots, \alpha_N$, $\beta_1, \ldots, \beta_N \in \mathbb{C}$ univocamente determinati (ricavabili dall'oss. 4.20) tali che $u = \alpha_1\varepsilon_{a_1} + \ldots + \alpha_N\varepsilon_{a_N}$ e $v = \beta_1\varepsilon_{a_1} + \ldots + \beta_N\varepsilon_{a_N}$.

La convoluzione $u * v$ è allora data da $u * v = \sum_{i=1}^{N}\sum_{j=1}^{N} \alpha_i\beta_j\varepsilon_{a_ia_j}$.

Dimostrazione. Ciò segue dall'oss. 4.19 e dalla bilinearità della convoluzione.

Definizione 4.22. Per $g \in G$ ed $u \in \mathbb{C}G$ sia $L(g)u := \bigcirc_x u(g^{-1}x)$.

È chiaro che l'applicazione $L(g) : \mathbb{C}G \longrightarrow \mathbb{C}G$ è lineare e che $L(1_G) = \mathrm{id}$.

Lemma 4.23. *Per g,$h \in G$ si ha che $L(gh) = L(g)L(h)$.*

Dimostrazione. Siano $u \in \mathbb{C}G$ ed $x \in G$. Allora

$$(L(gh)u)(x) = u((gh)^{-1}x) = u(h^{-1}g^{-1}x)$$

$$(L(g)L(h)u)x = (L(h)u)(g^{-1}x) = u(h^{-1}g^{-1}x).$$

Osservazione 4.24. Per ogni $g \in G$ si ha $L(g) \in GL(\mathbb{C}G)$.

Dimostrazione. Abbiamo già osservato che $L(g)$ è lineare.

Dal lemma 4.23 segue che $L(g)L(g^{-1}) = L(gg^{-1}) = L(1_G) = \mathrm{id}$, per cui $L(g) \in GL(\mathbb{C}G)$.

Definizione 4.25. L'applicazione $L : G \longrightarrow GL(\mathbb{C}G)$ è ben definita e una rappresentazione di G.

Essa si chiama la *rappresentazione regolare* di G.

Osservazione 4.26. L'algebra $\mathbb{C}G$ è commutativa se e solo se G è commutativo.

Dimostrazione. (1) Se $\mathbb{C}G$ è commutativo, lo è anche G, essendo isomorfo a un sottomonoide di $\mathbb{C}G$ come sappiamo dall'oss. 4.19.

(2) G sia commutativo. Siano u,$v \in G$. Per l'oss. 4.21 possiamo scrivere u e v nella forma $u = \alpha_1\varepsilon_{a_1} + \ldots + \alpha_N\varepsilon_{a_N}$, $v = \beta_1\varepsilon_{a_1} + \ldots + \beta_N\varepsilon_{a_N}$, dove $a_1, \ldots, a_N$ sono gli elementi distinti di G. A questo punto è evidente che è sufficiente dimostrare che $\varepsilon_a * \varepsilon_b = \varepsilon_b * \varepsilon_a$ per ogni a,$b \in G$. Ma per l'oss. 4.19 $\varepsilon_a * \varepsilon_b = \varepsilon_{ab} = \varepsilon_{ba} = \varepsilon_b * \varepsilon_a$.

Osservazione 4.27. Siano a,$g \in G$. Allora $L(g)\varepsilon_a = \varepsilon_{ga}$.

Dimostrazione. Infatti

$$L(g)\varepsilon_a = \bigcirc_x \varepsilon_a(g^{-1}x) = \bigcirc_x (g^{-1}x = a) = \bigcirc_x (x = ga) = \varepsilon_{ga}$$

Osservazione 4.28. Siano $G = \{a_1, \ldots, a_N\}$ con gli elementi $a_1, \ldots, a_N$ tutti distinti. Siano $\alpha_1, \ldots, \alpha_N \in \mathbb{C}$ e $g \in G$. Dalla linearità di $L(g)$ e dall'oss. 4.27 segue allora che

$$L(g)(\alpha_1\varepsilon_{a_1} + \ldots + \alpha_N\varepsilon_{a_N}) = \alpha_1\varepsilon_{ga_1} + \ldots + \alpha_N\varepsilon_{ga_N}$$

Corollario 4.29. *La rappresentazione regolare di G è iniettiva.*

Dimostrazione. Siano g,$h \in G$ tali che $L(g) = L(h)$

Sia a un elemento qualsiasi di G. Per l'oss. 4.27 allora $\varepsilon_{ga} = \varepsilon_{ha}$ e ciò implica $ga = ha$ per l'iniettività di ε. Ma allora $g = h$.

Nota 4.30. Dall'oss. 4.27 discende un altro fatto importante.

Per ogni g,$a \in G$ si ha $L(g)\varepsilon_a = \varepsilon_{ga} \in \varepsilon(G)$ e ciò mostra, insieme con l'oss. 4.29, che $L(g)$ induce una permutazione dell'insieme $\varepsilon(G)$.

Se scriviamo ancora $G = \{a_1, \ldots, a_N\}$ con gli a_i tutti distinti, allora possiamo prendere $\varepsilon_{a_1}, \ldots, \varepsilon_{a_N}$ come base ordinata di $\mathbb{C}G$ e rappresentare $L(g)$ mediante una matrice $M(g)$.

Questa matrice è una matrice di permutazione. Siccome inoltre $\varepsilon_{ga} = \varepsilon_a$ implica $g = 1$, vediamo che la matrice di $M(g)$ ha tutti zeri nella diagonale principale tranne che per $g = 1_G$.

Esempio 4.31. Sia $G = V_4 = \{1, a, b, c\}$ con la tavola di moltiplicazione

V_4	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Allora

$L(a)\varepsilon_1 = \varepsilon_a$

$L(a)\varepsilon_a = \varepsilon_{a^2} = \varepsilon_1$

$L(a)\varepsilon_b = \varepsilon_{ab} = \varepsilon_c$

$L(a)\varepsilon_c = \varepsilon_{ac} = \varepsilon_b$

per cui la matrice di $L(a)$ rispetto alla base $\varepsilon_1, \varepsilon_a, \varepsilon_b, \varepsilon_c$ è data da

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

Nota 4.32. Siano di nuovo $G = \{a_1, \ldots, a_N\}$ con gli elementi a_i tutti distinti ed $M(g)$ per $g \in G$ la matrice di $L(g)$ rispetto alla base ortogonale $\varepsilon_{a_1}, \ldots, \varepsilon_{a_N}$. Allora

$$M(g)^i_j = 1 \iff ga_j = a_i \iff g = a_i a_j^{-1}$$

e quindi nella notazione abbreviata già usata in precedenza abbiamo

$$M(g)^i_j = (g = a_i a_j^{-1})$$

Ciò permette di determinare in modo molto veloce la matrice $M(g)$:

Dalla tavola di moltiplicazione di G otteniamo in modo immediato gli inversi x^{-1} per $x \in G$. Formiamo la tabella

	1_G	a_2^{-1}	$\ldots$	a_j^{-1}	$\ldots$	a_N^{-1}
1_G						
a_2						
$\ldots$						
a_i				$a_i a_j^{-1}$		
$\ldots$						
a_N						

Qui assumiamo, per comodità, che $a_1 = 1_G$.

La matrice $M(g)$ si ottiene da questa tabella, sostituendo dapprima g con 1 e tutti gli altri elementi con 0.

Esempio 4.33. Sia $G = \mathbb{Z}/4$. La tavola di moltiplicazione è

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Gli inversi sono dati da $0^{-1} = 0$, $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 1$, per cui la tabella nella nota 4.32 diventa

	0	3	2	1
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

Perciò le matrici $M(x)$, rispetto alla base $\varepsilon_1, \varepsilon_a, \varepsilon_b, \varepsilon_c$, per ogni $x \in G$ sono:

$$M(0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad M(1) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M(2) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad M(3) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Esempio 4.34. Per $G = S_3 = \{\mathrm{id}, (123), (132), (12), (13), (23)\}$. La tavola di moltiplicazione è

S_3	id	(123)	(132)	(12)	(13)	(23)
id	id	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	id	(13)	(23)	(12)
(132)	(132)	id	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	id	(132)	(123)
(13)	(13)	(12)	(23)	(123)	id	(132)
(23)	(23)	(13)	(12)	(132)	(123)	id

Gli inversi sono dati da $\mathrm{id}^{-1} = \mathrm{id}$, $(123)^{-1} = (132)$, $(132)^{-1} = (123)$, $(12)^{-1} = (12)$, $(13)^{-1} = (13)$, $(23)^{-1} = (23)$, per cui la tabella nella nota 4.32 diventa

S_3	id	(132)	(123)	(12)	(13)	(23)
id	id	(123)	(132)	(12)	(13)	(23)
(123)	(123)	id	(132)	(13)	(23)	(12)
(132)	(132)	(123)	id	(23)	(12)	(13)
(12)	(12)	(13)	(23)	id	(132)	(123)
(13)	(13)	(23)	(12)	(123)	id	(132)
(23)	(23)	(12)	(13)	(132)	(123)	id

Perciò le matrici $L(x)$, rispetto alla base $\varepsilon_1, \varepsilon_a, \varepsilon_b, \varepsilon_c, \varepsilon_d, \varepsilon_e$, per ogni $x \in G$ sono:

$$M(\mathrm{id}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad M((123)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M((132)) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \qquad M((12)) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M((13)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \qquad M((23)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Esempio 4.35. Sia $G = D_4$ il gruppo delle simmetrie del quadrato.

D_4 può essere identificato con un sottogruppo di S_4:

$D_4 = \{\mathrm{id}, (1234), (12)(34), (13)(24), (1432), (14)(23), (13), (24)\}$.

La tavola di moltiplicazione è

D_4	id	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(13)	(24)
id	id	(1234)	(13)(24)	(1432)	(12)(34)	(14)(23)	(13)	(24)
(1234)	(1234)	(13)(24)	(1432)	id	(13)	(24)	(14)(23)	(12)(34)
(13)(24)	(13)(24)	(1432)	id	(1234)	(14)(23)	(12)(34)	(24)	(13)
(1432)	(1432)	id	(1234)	(13)(24)	(24)	(13)	(12)(34)	(14)(23)
(12)(34)	(12)(34)	(24)	(14)(23)	(13)	id	(13)(24)	(1423)	(1234)
(14)(23)	(14)(23)	(13)	(12)(34)	(24)	(13)(24)	id	(1234)	(1432)
(13)	(13)	(12)(34)	(24)	(14)(23)	(1234)	(1432)	id	(13)(24)
(24)	(24)	(14)(23)	(13)	(12)(34)	(14)(32)	(1234)	(13)(24)	id

La tabella nella nota 4.32 diventa quindi

D_4	id	(1432)	(13)(24)	(1234)	(12)(34)	(14)(23)	(13)	(24)
id	id	(1432)	(13)(24)	(1234)	(12)(34)	(14)(23)	(13)	(24)
(1234)	(1234)	id	(1432)	(13)(24)	(13)	(24)	(14)(23)	(12)(34)
(13)(24)	(13)(24)	(1234)	id	(1432)	(14)(23)	(12)(34)	(24)	(13)
(1432)	(1432)	(13)(24)	(1234)	id	(24)	(13)	(12)(34)	(14)(23)
(12)(34)	(12)(34)	(13)	(14)(23)	(24)	id	(13)(24)	(1423)	(1234)
(14)(23)	(14)(23)	(24)	(12)(34)	(13)	(13)(24)	id	(1234)	(1432)
(13)	(13)	(14)(23)	(24)	(12)(34)	(1234)	(1432)	id	(13)(24)
(24)	(24)	(12)(34)	(13)	(14)(23)	(14)(32)	(1234)	(13)(24)	id

Perciò le matrici $L(x)$, rispetto alla base $\varepsilon_1, \varepsilon_a, \varepsilon_b, \varepsilon_c, \varepsilon_d, \varepsilon_e, \varepsilon_f, \varepsilon_g$, per ogni $x \in G$ sono:

$$M(\mathrm{id}) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M((1234)) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$M((13)(24)) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M((1432)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$M((12)(34)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M((14)(23)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M((13)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$M((24)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Osservazione 4.36. Nelle ipotesi della nota 4.30 abbiamo

$$\operatorname{tr} L(g) = \operatorname{tr} M(g) = \begin{cases} |G| & \text{se } g = 1_G \\ 0 & \text{se } g \neq 1_G \end{cases}$$

Dimostrazione. Ciò è una conseguenza immediata della nota 4.30.

Teorema 4.37. *La rappresentazione regolare è equivalente alla rappresentazione* $n_1 R_1 \oplus \ldots \oplus n_\kappa R_\kappa$.

Dimostrazione. Ricordiamo che per le ipotesi nella situazione 4.8 n_α è la dimensione di $R_\alpha : G \longrightarrow GL(n_\alpha, \mathbb{C})$.

Dal cor. 4.13 sappiamo che L è equivalente ad una rappresentazione della forma $m_1 R_1 \oplus \ldots \oplus m_\kappa R_\kappa$. Dobbiamo dimostrare che $m_\alpha = n_\alpha$ per ogni α. Per la prop. 4.12

$$m_\alpha = \frac{1}{|G|} \|\chi_\alpha, \operatorname{tr} L\| = \frac{1}{|G|} \sum_{g \in G} \chi_\alpha(g) \overline{\operatorname{tr} L(g)} =$$
$$\overset{4.36}{=} \frac{1}{|G|} \chi_\alpha(1_G)\, |G| = \chi_\alpha(1_G) = \operatorname{tr} R_\alpha(1_G) = n_\alpha$$

Nota 4.38. Vediamo in particolare che $n_\alpha \neq 0$ per ogni $\alpha = 1, \ldots, \kappa$. Ciò significa che ogni rappresentazione irriducibile di G appare nella rappresentazione regolare la quale contiene quindi (in forma nascosta) l'informazione su tutte le rappresentazioni di dimensione finita di G.

Per questa ragione l'algebra di gruppo è così importante.

Definizione 4.39. Per una rappresentazione $R : G \longrightarrow GL(V)$ con $\dim V = n < \infty$ oppure una rappresentazione matriciale $R : G \longrightarrow GL(n, \mathbb{C})$ sia $\dim R := n$.

Osservazione 4.40. Siano $S_1, \ldots, S_p$ rappresentazioni matriciali o di dimensione finita di G ed $m_1, \ldots, m_p \in \mathbb{N}$. Allora

$$\dim(m_1 S_1 \oplus \ldots \oplus m_p S_p) = m_1 \dim S_1 + \ldots + m_p \dim S_p$$

Teorema 4.41 (teorema di Burnside). $\sum_{\alpha=1}^{\kappa} n_\alpha^2 = |G|$.

Dimostrazione. Per il teorema 4.37 la rappresentazione regolare è equivalente alla rappresentazione $n_1 R_1 \oplus \ldots \oplus n_\kappa R_\kappa$, cosicchè dall'oss. 4.40 si ha

$$|G| = \dim L = n_1 \dim R_1 + \ldots + n_\kappa \dim R_\kappa = n_1^2 + \ldots + n_\kappa^2$$

Teorema 4.42. *I coefficienti $R^i_{j\alpha}$ per $\alpha = 1, \ldots, \kappa$ e $1 \leq i,j \leq n_\alpha$ formano una base ortogonale di $\mathbb{C}^G$.*

In particolare quindi per ogni funzione $f : G \longrightarrow \mathbb{C}$ esiste una rappresentazione

$$f = \sum_{\alpha=1}^{\kappa} \sum_{i=1}^{n_\alpha} \sum_{j=1}^{n_\alpha} \lambda^i_{j\alpha} R^i_{j\alpha}$$

con i coefficienti $\lambda^i_{j\alpha} \in \mathbb{C}$ univocamente determinati.

Dimostrazione. Per i risultati del terzo capitolo i coefficienti sono tra loro ortogonali e perciò linearmente indipendenti, il loro numero è uguale a $\sum_{\alpha=1}^{\kappa} n_\alpha^2$ e coincide per il teorema di Burnside con $\dim \mathbb{C}^G$.

Proposizione 4.43. *I coefficienti $\lambda^i_{j\alpha}$ nella rappresentazione di una funzione $f \in \mathbb{C}^G$ nel teorema 4.42 possono essere esplicitamente calcolati, infatti si ha*

$$\lambda^i_{j\alpha} = \frac{\|f, R^i_{j\alpha}\|}{\frac{G}{n_\alpha}}.$$

Dimostrazione. Siccome i coefficienti formano una base ortogonale di $\mathbb{C}^G$ abbiamo

$$\lambda^i_{j\alpha} = \frac{\|f, R^i_{j\alpha}\|}{\|R^i_{j\alpha}, R^i_{j\alpha}\|} = \frac{\|f, R^i_{j\alpha}\|}{G/n_\alpha}$$

Osservazione 4.44. Più esplicitamente nella nota 4.43 si ha

$$\lambda^i_{j\alpha} = \frac{n_\alpha}{|G|} \sum_{g \in G} f(g) \overline{R^i_{j\alpha}(g)}$$

5. Tavole dei caratteri

Situazione 5.1. G sia un gruppo finito, $(R_1, \ldots, R_\kappa)$ un sistema di Burnside di G e $(n_1, \ldots, n_\kappa)$ il corrispondente vettore delle dimensioni. Per ogni $\alpha = 1, \ldots, \kappa$ sia $\chi_\alpha := \operatorname{tr} R_\alpha$.

Definizione 5.2. Due elementi a,$b \in G$ si dicono *coniugati* (in G), se esiste $g \in G$ tale che $b = g^{-1}ag$. In tal caso scriviamo $a \sim b$. In questo modo otteniamo una relazione di equivalenza su G, le cui classi si chiamano *classi* di G.

Lemma 5.3. *Siano a,$b \in G$ ed $a \sim b$. Allora $\chi_\alpha(a) = \chi_\alpha(b)$ per ogni $\alpha = 1, \ldots, \kappa$.*

Dimostrazione. Per ipotesi $b = g^{-1}ag$ per qualche $g \in G$. Perciò

$$\begin{aligned}\chi_\alpha(b) &= \operatorname{tr} R_\alpha(b) = \operatorname{tr} R_\alpha(g^{-1}ag) = \\ &= \operatorname{tr}((R_\alpha(g))^{-1} R_\alpha(a) R_\alpha(g)) = \operatorname{tr} R_\alpha(a) = \chi_\alpha(a)\end{aligned}$$

Definizione 5.4. Una funzione $f : G \longrightarrow \mathbb{C}$ si chiama una *funzione delle classi*, se è costante su ogni classe di G, cioè se $a \sim b$ implica $f(a) = f(b)$. Per il lemma 5.3 ogni carattere è una funzione delle classi.

Denotiamo con $\widetilde{\mathbb{C}^G}$ l'insieme delle funzioni delle classi su G.

Proposizione 5.5. $\widetilde{\mathbb{C}^G} = SV(\chi_1, \ldots, \chi_\kappa)$.

Dimostrazione. (1) È chiaro che ogni elemento di $SV(\chi_1, \ldots, \chi_\kappa)$ è una funzione delle classi.

(2) Sia $f \in \widetilde{\mathbb{C}^G}$. Allora $f \in \mathbb{C}^G$, perciò esiste una rappresentazione $f = \sum_{\alpha=1}^{\kappa} \sum_{i=1}^{n_\alpha} \sum_{j=1}^{n_\alpha} \lambda^i_{j\alpha} R^i_{j\alpha}$ come abbiamo visto nel teorema 4.42. Nel seguente tralasciamo i limiti di sommazione.

Sia $a \in G$ fissato. Per ogni $g \in G$ abbiamo allora

$$\begin{aligned}f(a) = f(gag^{-1}) &= \sum_\alpha \sum_i \sum_j \lambda^i_{j\alpha} R^i_{j\alpha}(gag^{-1}) = \\ &= \sum_\alpha \sum_i \sum_j \lambda^i_{j\alpha} \sum_r \sum_s R^i_{r\alpha}(g) R^r_{s\alpha}(a) R^s_{j\alpha}(g^{-1})\end{aligned}$$

Sommando su $g \in G$ abbiamo quindi

$$|G|\, f(a) = \sum_\alpha \sum_i \sum_j \lambda^i_{j\alpha} \sum_r \sum_s R^r_{s\alpha}(a) \sum_{g\in G} R^i_{r\alpha}(g) R^s_{j\alpha}(g^{-1}) =$$
$$= \sum_\alpha \sum_i \sum_j \lambda^i_{j\alpha} \sum_r \sum_s R^r_{s\alpha}(a) \frac{1}{n_\alpha} \delta^i_j \delta^s_r =$$
$$= \sum_\alpha \frac{1}{n_\alpha} \sum_i \lambda^i_{i\alpha} \sum_r R^r_{r\alpha}(a) = \sum_\alpha \frac{1}{n_\alpha} \sum_i \lambda^i_{i\alpha} \chi_\alpha(a)$$

per cui

$$f = \frac{1}{|G|} \sum_\alpha \left(\frac{1}{n_\alpha} \sum_i \lambda^i_{i_\alpha} \right) \chi_\alpha \in SV(\chi_1, \ldots, \chi_\kappa)$$

Teorema 5.6. *κ è uguale al numero delle classi di G.*

Dimostrazione. Sia m il numero delle classi di G. Allora $\widetilde{\mathbb{C}^G} \cong \mathbb{C}^m$, e siccome i caratteri sono ortogonali tra loro, si ha
$\dim SV(\chi_1, \ldots, \chi_\kappa) = \kappa$. Dalla prop. 5.5 otteniamo

$$m = \dim \widetilde{\mathbb{C}^G} = \dim SV(\chi_1, \ldots, \chi_\kappa) = \kappa$$

Osservazione 5.7. Il teorema precedente ha due applicazioni pratiche immediate:

(1) Siccome è facile determinare il numero delle classi di G, possiamo facilmente calcolare il numero delle rappresentazioni irriducibili di G. Se ad esempio G è abeliano, il numero delle classi è uguale al numero di elementi di G, per cui esistono $|G|$ rappresentazioni irriducibili inequivalenti di G.

In S_3 invece ci sono tre classi, per cui esistono esattamente 3 rappresentazioni irriducibili inequivalenti di S_3.

(2) Il teorema 5.6 permette la costruzione delle tavole dei caratteri, come vedremo adesso.

Corollario 5.8. *Siano $a, b \in G$. Allora $a \sim b \iff \chi_\alpha(a) = \chi_\alpha(b)$ per ogni $\alpha = 1, \ldots, \kappa$*

Dimostrazione. $\Longrightarrow$: Lemma 5.3.

$\Longleftarrow$: L'ipotesi implica, per la prop. 5.5, che $f(a) = f(b)$ per ogni $f \in \widetilde{\mathbb{C}^G}$. Adesso definiamo una funzione $f : G \longrightarrow \mathbb{C}$ nel modo seguente. Poniamo:

$$f(x) = \begin{cases} 1 & \text{per } x \sim b \\ 0 & \text{altrimenti} \end{cases}$$

È chiaro che f è una funzione delle classi. Ma allora $f(a) = f(b)$ e ciò significa che $a \sim b$.

Osservazione 5.9. Sia $a \in G$. Allora $\chi_\alpha(a^{-1}) = \overline{\chi_\alpha(a)}$ per ogni $\alpha = 1, \ldots, \kappa$.

Dimostrazione. Infatti per l'oss. 3.9 abbiamo

$$\chi_\alpha(a^{-1}) = \operatorname{tr} R_\alpha(a^{-1}) = \operatorname{tr}(R_\alpha(a))^* = \operatorname{tr}\overline{R_\alpha(a)} = \overline{\chi_\alpha(a)}$$

Corollario 5.10. *Sia $a \in G$. Allora*

$a \sim a^{-1}$ *se e solo se* $\chi_\alpha(a) \in \mathbb{R}$ *per ogni* $\alpha = 1, \dots, \kappa$.

Dimostrazione. Per il corollario 5.8 abbiamo
$a \sim a^{-1} \iff \chi_\alpha(a) = \chi_\alpha(a^{-1})$ per ogni α.
Però $\chi_\alpha(a^{-1}) = \overline{\chi_\alpha(a)}$ come sappiamo dall'oss. 5.9.

Nota 5.11. $C_1, \dots, C_\kappa$ siano le classi di G. Questa numerazione sia arbitraria, ma fissata, con $C_1 = \{1\}$. Per $j = 1, \dots, \kappa$ sia $N_j := |C_j|$. I caratteri dipendono solo dalle classi, per cui per $1 \le \alpha, j \le \kappa$ possiamo definire $\chi_\alpha(C_j) := \chi_\alpha(g)$ se $g \in G_j$.

Otteniamo così la tavola dei caratteri di G:

	N_1	$\dots$	N_j	$\dots$	N_κ
	C_1	$\dots$	C_j	$\dots$	C_κ
χ_1					
$\dots$					
χ_α			$\chi_\alpha(C_j)$		
$\dots$					
χ_κ					

Proposizione 5.12. *Per $\alpha, \beta = 1, \dots, \kappa$ vale*

$$\sum_{j=1}^{\kappa} N_j \chi_\alpha(C_j)\overline{\chi_\beta(C_j)} = |G|\,\delta_\beta^\alpha$$

Dimostrazione. La sommatoria coincide con

$$\sum_{g \in G} \chi_\alpha(g)\overline{\chi_\beta(g)} = \|\chi_\alpha, \chi_\beta\| = |G|\,\delta_\beta^\alpha$$

Nota 5.13. Definiamo la matrice $\Gamma \in \mathbb{C}_\kappa^\kappa$ tramite

$$\Gamma_j^\alpha := \sqrt{\tfrac{N_j}{|G|}}\chi_\alpha(C_j)$$

La relazione nella prop. 5.12 diventa allora

$$\sum_{j=1}^{\kappa} \Gamma_j^\alpha \overline{\Gamma_j^\beta} = \delta_\beta^\alpha$$

ovvero

$\|\Gamma^\alpha, \Gamma^\beta\| = \delta_\beta^\alpha$ per ogni $\alpha, \beta = 1, \dots, \kappa$.

Ciò significa che le righe della matrice Γ formano un sistema ortonormale, Γ è quindi una matrice unitaria, per cui anche le colonne di Γ formano una base ortonormale, ovvero

$$\sum_{\alpha=1}^{\kappa} \Gamma_j^\alpha \overline{\Gamma_\kappa^\alpha} = \delta_\kappa^j$$

per ogni $j, \kappa = 1, \dots, \kappa$.

Proposizione 5.14. *Per ogni $j, k = 1, \dots, \kappa$ si ha*

$$\sum_{\alpha=1}^{\kappa} \chi_\alpha(C_j)\overline{\chi_\alpha(C_\kappa)} = \frac{|G|}{N_k}\delta_\kappa^j$$

Dimostrazione. Questa relazione non è altro che l'ultima equazione nella nota 5.13. La sommatoria coincide con

$$\begin{aligned}\delta_\kappa^j = \sum_{\alpha=1}^{\kappa} \Gamma_j^\alpha \overline{\Gamma_\kappa^\alpha} = \sum_{\alpha=1}^{\kappa} \sqrt{\frac{N_j}{|G|}}\chi_\alpha(C_j)\sqrt{\frac{N_\kappa}{|G|}}\overline{\chi_\alpha(C_\kappa)} = \\ = \frac{1}{|G|}\sqrt{N_j N_\kappa}\sum_{\alpha=1}^{\kappa} \chi_\alpha(C_j)\overline{\chi_\alpha(C_\kappa)}\end{aligned}$$

evidentemente equivalente all'enunciato.

6. Le rappresentazioni irriducibili di S_3

Definizione 6.1. Il gruppo S_3 è isomorfo al gruppo delle simmetrie piane del triangolo equilatero. Siano $\rho_\alpha := \begin{pmatrix} \cos\alpha & \text{-}\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ la rotazione per α, $\sigma_\alpha := \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & \text{-}\cos 2\alpha \end{pmatrix}$ la riflessione all'angolo α. Otteniamo così una rappresentazione R_3 di S_3:

$$\begin{aligned}
\mathrm{id} &\longmapsto \delta = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
(12) &\longmapsto \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
(23) &\longmapsto \sigma_{\frac{2\pi}{3}} = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix} \\
(13) &\longmapsto \sigma_{\frac{4\pi}{3}} = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix} \\
(123) &\longmapsto \rho_{\frac{2\pi}{3}} = \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \\
(132) &\longmapsto \rho_{\frac{4\pi}{3}} = \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{pmatrix}
\end{aligned}$$

Si vede facilmente che queste matrici non possiedono un autovettore comune; la rappresentazione è perciò irriducibile.

Osservazione 6.2. Siano G un gruppo finito ed $R : G \longrightarrow GL(V)$ una rappresentazione irriducibile, oppure $R : G \longrightarrow GL(n, \mathbb{C})$ una rappresentazione matriciale irriducibile.

Allora anche $\det R := \bigcirc_g \det R(g) : G \longrightarrow \mathbb{C} \setminus 0 = GL(1, \mathbb{C})$ è una rappresentazione, necessariamente irriducibile (essendo una rappresentazione unidimensionale).

Può naturalmente accadere che $\det R(g) = 1$ per ogni $g \in G$; in tal caso questa rappresentazione coincide con la rappresentazione banale.

Nota 6.3. Per la rappresentazione $R_3 : S_3 \longrightarrow GL(2, \mathbb{C})$ della def. 6.1 otteniamo la rappresentazione $R_2 := \det R_3$ descritta dalla seguente tabella:

$$\begin{aligned}
\mathrm{id} &\longmapsto 1 \\
(12) &\longmapsto -1 \\
(23) &\longmapsto -1 \\
(13) &\longmapsto -1 \\
(123) &\longmapsto 1 \\
(132) &\longmapsto 1
\end{aligned}$$

Per $g \in S_3$ si ha quindi semplicemente $R_2(g) = \operatorname{sgn} g$. Dal teorema 4.14 sappiamo che le rappresentazioni R_1 e R_2 non sono equivalenti e naturalmente nessuna delle due è equivalente ad R_3, essendo quest'ultima 2-*dimensionale*. Il numero delle classi di S_3 è uguale a 3, perciò (R_1, R_2, R_3) è un sistema di Burnside per S_3, come sappiamo dall'oss. 5.7. Per il teorema 4.42 i coefficienti $R^1_{11}, R^1_{12}, R^1_{13}, R^1_{23}, R^2_{13}, R^2_{23}$, formano una base ortogonale di $\mathbb{C}^{S_3} \cong \mathbb{C}^6$, che possiamo trascrivere nel seguente schema:

g	R^1_{11}	R^1_{12}	R^1_{13}	R^1_{23}	R^2_{13}	R^2_{23}
id	1	1	1	0	0	1
(12)	1	-1	1	0	0	-1
(23)	1	-1	$-\frac{1}{2}$	$-\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$
(13)	1	-1	$-\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{2}$	$\frac{1}{2}$
(123)	1	1	$-\frac{1}{2}$	$-\frac{\sqrt{3}}{2}$	$\frac{\sqrt{3}}{2}$	$-\frac{1}{2}$
(132)	1	1	$-\frac{1}{2}$	$\frac{\sqrt{3}}{2}$	$-\frac{\sqrt{3}}{2}$	$-\frac{1}{2}$

Osservazione 6.4. Conoscendo così un sistema di Burnside di S_3, calcolando le tracce otteniamo direttamente le tavole dei caratteri:

	1	3	2
	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Osservazione 6.5. Anche quando non si conoscono tutte le rappresentazioni irriducibili di un gruppo, spesso è possibile calcolare le tavole dei caratteri appellandosi alla teoria trattata nei capitoli precedenti. Proviamo a fare ciò per le rappresentazioni di S_3.

(1) Dopo aver denotato, come sempre, con R_1 la rappresentazione banale, considerando il segno di una permutazione arriviamo subito alla $R_2 = \bigcirc_g \operatorname{sgn} g$. Assumiamo invece di conoscere R_3. Dal teorema di Burnside sappiamo che $n_1^2 + n_2^2 + n_3^2 = |S_3|$, ovvero $1 + 1 + n_3^2 = 6$, e ciò implica $n_3 = 2$. In questo modo otteniamo la tavola incompleta :

	1	3	2
	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	a	b

Dobbiamo ancora determinare a e b. Dalla proposizione 5.14 abbiamo però :

$$\begin{cases} 1 \cdot \bar{1} - 1 \cdot \bar{1} + 2 \cdot \bar{a} = 0 \\ 1 \cdot \bar{1} + 1 \cdot \bar{1} + 2 \cdot \bar{b} = 0 \end{cases}$$

da cui segue che $a = 0$ e $b = -1$, in accordo con quanto visto nell'oss.6.4.

7. Caratteri di gruppi abeliani finiti

Situazione 7.1. G sia un gruppo abeliano finito. Poniamo

$\varepsilon := e^{\frac{2\pi i}{|G|}}$.

Proposizione 7.2. *I caratteri di G sono esattamente le applicazioni $\chi : G \longrightarrow \mathbb{C}$ tale che*

$$\chi(1) = 1$$
$$\chi(gh) = \chi(g)\chi(h)$$

Dimostrazione. (1) Ogni funzione della forma indicata può essere considerata come una rappresentazione matriciale 1-dimensionale $G \longrightarrow GL(1, \mathbb{C})$. Essa è quindi irriducibile e coincide con la propria traccia, ed è quindi un carattere di G.

(2) Sia viceversa φ una rappresentazione matriciale irriducibile di G. Per la prop. 2.11 φ è allora 1-dimensionale e coincide quindi con la propria traccia χ. Ma χ è allora un omomorfismo $G \longrightarrow GL(1, \mathbb{C})$ e soddisfa quindi le condizioni nell'enunciato.

Definizione 7.3. Denotiamo con $\widehat{G}$ l'insieme dei caratteri di G.

Osservazione 7.4. $|\widehat{G}| = |G|$

Dimostrazione. Per il teorema 5.6 $|\widehat{G}|$ è uguale al numero delle classi di G. Siccome G è abeliano, si ha però $\kappa = |G|$.

Proposizione 7.5. *Siano $\chi \in \widehat{G}$ e $g \in G$. Allora $\chi(g)$ è una $|G|$-esima radice dell'unità . In particolare vediamo che $|\chi(g)| = 1$.*

Dimostrazione. Infatti $\chi(g)^{|G|} = \chi(g^{|G|}) = \chi(1) = 1$.

Proposizione 7.6. *$\widehat{G}$ diventa un gruppo abeliano finito se per $\chi, \psi \in \widehat{G}$ poniamo*

$$\chi\psi := \bigcirc_g \chi(g)\psi(g)$$

L'elemento neutro di questo gruppo è il carattere banale $\chi_1 := \bigcirc_g 1$, inoltre per $\chi \in \widehat{G}$ si ha $\chi^{-1} = \bar{\chi}$.

Dimostrazione. (1) $\widehat{G}$ è finito essendo $|\widehat{G}| = |G|$ per l'oss. 7.4.

(2) Siano $\chi, \psi \in \widehat{G}$ e $g, h \in G$. Allora

$$(\chi\psi)(gh) = \chi(gh)\psi(gh) = \chi(g)\chi(h)\psi(g)\psi(h) = \chi(g)\psi(g)\chi(h)\psi(h) = \\ = (\chi\psi)(g)(\chi\psi)(h)$$

Inoltre $(\chi\psi)(1) = \chi(1)\psi(1) = 1 \cdot 1 = 1$, e vediamo che sono soddisfatte le condizioni della prop. 7.2. Perciò $\chi\psi \in \widehat{G}$.

(3) È chiaro che χ_1 è l'elemento neutro di $\widehat{G}$.

(4) È inoltre evidente che $\widehat{G}$ è un monoide.

(5) Per $\chi \in \widehat{G}$ e $g \in G$ abbiamo infine

$\overline{\chi}(g) = \overline{\chi(g)} \overset{7.5}{=} \dfrac{1}{\chi(g)}$, cosicché $(\chi\overline{\chi})(g) = \chi(g)\overline{\chi(g)} = 1$. Ciò mostra che $\widehat{G}$ è un gruppo, ovviamente abeliano.

Definizione 7.7. Il gruppo $\widehat{G}$ è detto *gruppo dei caratteri* o *gruppo duale* di G.

Lemma 7.8. *G sia ciclico e t un generatore di G. Allora l'applicazione $\chi_t : G \longrightarrow \mathbb{C}$ definita da*

$$\chi_t(t^k) := \varepsilon^k$$

per $k \in \mathbb{Z}$ è ben definita e un carattere di G. In particolare abbiamo $\chi_t(t) = \varepsilon$.

Dimostrazione. (1) Dimostriamo prima che l'applicazione χ_t è ben definita. Ogni elemento di G è della forma t^κ per qualche $\kappa \in \mathbb{Z}$. Sia $t^\kappa = t^m$. Allora $m = \kappa + j\,|G|$ per qualche $j \in \mathbb{Z}$, per cui
$\varepsilon^m = \varepsilon^{\kappa + j|G|} = \varepsilon^\kappa$.

(2) Dimostriamo che χ_t soddisfa le condizioni della prop. 7.1.

$$\chi_t(1) = \chi_t(t^0) = \varepsilon^0 = 1$$
$$\chi_t(t^k t^m) = \chi_t(t^{k+m}) = \varepsilon^{k+m} = \varepsilon^k \varepsilon^m = \chi_t(t^k)\chi_t(t^m)$$

Teorema 7.9. *G sia ciclico e t un generatore di G. Allora i caratteri $\chi_1, \chi_t, \chi_t^2, \ldots, \chi_t^{|G|-1}$ sono tutti distinti tra di loro e*

$$\widehat{G} = \{\chi_1, \chi_t, \chi_t^2, \ldots, \chi_t^{|G|-1}\}$$

$\widehat{G}$ è quindi un gruppo ciclico (dello stesso ordine di G), generato da χ_t.

Dimostrazione. (1) I numeri
$\chi_1(t) = 1, \chi_t(t) = \varepsilon, \chi_1^2(t) = \varepsilon^2, \ldots, \chi_1^{|G|-1} = \varepsilon^{|G|-1}$ sono tutti distinti tra di loro, perciò lo sono anche le applicazioni $\chi_1, \chi_t, \ldots, \chi_t^{|G|-1}$. Queste sono caratteri come sappiamo dalla prop. 7.6.

(2) Dobbiamo ancora dimostrare che ogni carattere di G è uno dei caratteri elencati. Sia $\chi \in \widehat{G}$. Dalla prop. 7.5 sappiamo che $\chi(t)$ è una $|G|$-esima radice dell'unità; quindi esiste un $k \in \{0, 1, \ldots, |G| - 1\}$ tale che $\chi(t) = \varepsilon^k$. Ma allora $\chi = \chi_t^k$.

Corollario 7.10. *G sia ciclico. Allora $G \cong \widehat{G}$. Questo isomorfismo però non è canonico, perché dipende dalla scelta del generatore t nel teorema 7.9, tranne nel caso $|G| \leq 2$ in cui esiste un solo generatore.*

Corollario 7.11. *G sia ciclico e t un generatore di G. Allora ogni funzione $f : G \longrightarrow \mathbb{C}$ possiede un'unica rappresentazione della forma*

$$f = \alpha_0\chi_1 + \alpha_1\chi_t + \alpha_2\chi_t^2 + \ldots + \alpha_{|G|-1}\chi_t^{|G|-1}$$

con $\alpha_0, \alpha_1, \ldots, \alpha_{|G|-1} \in \mathbb{C}$. *Per* $k \in \mathbb{Z}$ *abbiamo quindi*

$$f(t^k) = \alpha_0 + \alpha_1\varepsilon^1 + \alpha_2\varepsilon^2 + \ldots + \alpha_{|G|-1}\varepsilon^{|G|-1}$$

Dimostrazione. Ciò segue dal teorema 7.9 e dalla prop. 5.5 (o dal teorema 4.42).

Proposizione 7.12. *Sia* H *un altro gruppo abeliano finito. Allora l'applicazione*

$$\begin{aligned} &\widehat{G} \times \widehat{H} \longrightarrow \widehat{G \times H} \\ &(\chi, \psi) \longmapsto \chi \otimes \psi := \bigcirc_{(x,y)} \chi(x)\psi(y) \end{aligned}$$

è ben definito ed è un isomorfismo di gruppi.

Dimostrazione. Facile verifica.

Teorema 7.13. G *è prodotto diretto di gruppi ciclici.*

Dimostrazione. Corso di algebra.

Corollario 7.14. $G \cong \widehat{G}$.

Dimostrazione. Teorema 7.13, prop. 7.12 e cor. 7.10.

8. Esempi di tavole dei caratteri

Situazione 8.1. Nelle tavole dei caratteri dei gruppi abeliani tralasciamo la riga degli N_j, essendo questi tutti uguali ad 1, mentre nella casella della classe scriviamo l'unico elemento di essa. Nel caso dei gruppi ciclici denotiamo con t un generatore.

Esempio 8.2. Tavola dei caratteri di $\mathbb{Z}/2$.

	1	t
χ_1	1	1
χ_2	1	-1

Esempio 8.3. Tavola dei caratteri di $\mathbb{Z}/3$. Sia $\varepsilon := \varepsilon^{\frac{2\pi i}{3}}$, per cui $\varepsilon^3 = 1$.

	1	t	t^2
χ_1	1	1	1
χ_2	1	ε	ε^2
χ_3	1	ε^2	ε

Esempio 8.4. Tavola dei caratteri di $\mathbb{Z}/4$. Sia $\varepsilon := \varepsilon^{\frac{2\pi i}{4}}$, per cui $\varepsilon^4 = 1$.

	1	t	t^2	t^3
χ_1	1	1	1	1
χ_2	1	ε	ε^2	ε^3
χ_3	1	ε^2	1	ε^2
χ_4	1	ε^3	ε^2	ε

Esempio 8.5. Tavola dei caratteri di $\mathbb{Z}/5$. Sia $\varepsilon := \varepsilon^{\frac{2\pi i}{5}}$, per cui $\varepsilon^5 = 1$.

	1	t	t^2	t^3	t^4
χ_1	1	1	1	1	1
χ_2	1	ε	ε^2	ε^3	ε^4
χ_3	1	ε^2	ε^4	ε	ε^3
χ_4	1	ε^3	ε	ε^4	ε^2
χ_5	1	ε^4	ε^3	ε^2	ε

Osservazione 8.6. Si osservi che in un gruppo ciclico finito con generatore t e $\chi_j = \chi_t^j$ si ha $\chi_j(t^\kappa) = \varepsilon^{\kappa j} = \chi_\kappa(t^j)$, per cui la tavola dei caratteri risulta simmetrica.

Esempio 8.7. Tavola dei caratteri di $\mathbb{Z}/6$. Sia $\varepsilon := \varepsilon^{\frac{2\pi i}{6}}$, per cui $\varepsilon^6 = 1$.

	1	t	t^2	t^3	t^4	t^5
χ_1	1	1	1	1	1	1
χ_2	1	ε	ε^2	ε^3	ε^4	ε^5
χ_3	1	ε^2	ε^4	1	ε^2	ε^4
χ_4	1	ε^3	1	ε^3	1	ε^3
χ_5	1	ε^4	ε^2	1	ε^4	ε^2
χ_6	1	ε^5	ε^4	ε^3	ε^2	ε

Esempio 8.8. Tavola dei caratteri V_4. Usando l'isomorfismo $V_4 = \mathbb{Z}/2 \times \mathbb{Z}/2$, dalla prop. 7.12 e dall'esempio 8.2 otteniamo

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

dove abbiamo posto $\chi_2 := \varphi_1 \otimes \varphi_2$, $\chi_3 := \varphi_2 \otimes \varphi_1$, $\chi_4 := \varphi_2 \otimes \varphi_2$.

Esempio 8.9. Tavola dei caratteri di S_3, già calcolata nell'oss. 6.4

	1	3	2
	C_1	C_2	C_3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

9. Un criterio di irriducibilità

Situazione 9.1. G sia un gruppo finito, $(R_1, \dots, R_\kappa)$ un sistema di Burnside di G e $(n_1, \dots, n_\kappa)$ il corrispondente vettore delle dimensioni. Per ogni $\alpha = 1, \dots, \kappa$ sia $\chi_\alpha := \operatorname{tr} R_\alpha$.

Lemma 9.2. *Siano $m_1, \dots, m_\kappa \in \mathbb{N}$ ed $R := m_1 R_1 \oplus \dots \oplus_\kappa m_\kappa R_\kappa$. Allora*

$$\| \operatorname{tr} R\|^2 = |G| \sum_{\alpha=1}^{\kappa} m_\alpha^2$$

Dimostrazione. Abbiamo $\operatorname{tr} R = \sum_{\alpha=1}^{\kappa} m_\alpha \chi_\alpha$, per cui

$$\begin{aligned} \| \operatorname{tr} R, \operatorname{tr} R\| &= \sum_{\alpha=1}^{\kappa} \sum_{\beta=1}^{\kappa} m_\alpha m_\beta \|\chi_\alpha, \chi_\beta\| = \sum_{\alpha=1}^{\kappa} \sum_{\beta=1}^{\kappa} m_\alpha m_\beta \, |G| \, \delta_{\alpha\beta} = \\ &= |G| \sum_{\alpha=1}^{\kappa} m_\alpha^2 \end{aligned}$$

Teorema 9.3. *Una rappresentazione R di G di dimensione finita è irriducibile se e solo se $\| \operatorname{tr} R\|^2 = |G|$.*

Dimostrazione. Per il cor. 4.13 possiamo scrivere R nella forma $m_1 R_1 \oplus \dots \oplus m_\kappa R_\kappa$ con $m_1, \dots, m_\kappa \in \mathbb{N}$ univocamente determinati. Allora sono equivalenti:

(1) R è irriducibile.

(2) Esattamente uno degli m_α è uguale a 1 mentre $m_\beta = 0$ per ogni $\beta \neq \alpha$.

(3) $\sum_{\alpha=1}^{\kappa} m_\alpha^2 = 1$.

(4) $|G| \sum_{\alpha=1}^{\kappa} m_\alpha^2 = |G|$.

L'enunciato segue dal lemma 9.2.

Lemma 9.4. $\sum_{g \in G} \chi_\alpha(g) = \begin{cases} |G| & \textit{per } \alpha = 1 \\ 0 & \textit{altrimenti} \end{cases}$

Dimostrazione. Si tratta di un utile caso particolare delle relazioni di ortogonalità per i caratteri. Infatti

$$\sum_{g \in G} \chi_\alpha(g) = \|\chi_\alpha, \chi_1\| = |G| \, \delta_{1\alpha}$$

10. Interi algebrici

Situazione 10.1. Siano E un anello commutativo ed A un sottoanello di E.

Definizione 10.2. Un polinomio in $A[x]$ si dice *monico*, se è di grado $n \geq 1$ e se il coefficiente di x^n è uguale ad 1.

Denotiamo con $A\{x\}$ l'insieme dei polinomi monici in $A[x]$.

Definizione 10.3. Un elemento $\alpha \in E$ si dice *algebrico* su A, se esiste $f \in A[x]$ tale che $f(\alpha) = 0$, e *intero* su A, se esiste $f \in A\{x\}$ tale che $f(\alpha) = 0$.

Denotiamo con $\mathrm{Alg}(E : A)$ l'insieme degli elementi algebrici di E su A e con $\mathrm{Int}(E : A)$ l'insieme degli elementi interi di E su A.

Osservazione 10.4. $A \subset \mathrm{Int}(E : A) \subset \mathrm{Alg}(E : A)$.

Dimostrazione. Per ogni $\alpha \in A$ abbiamo $f := x - \alpha \in A\{x\}$ ed $f(\alpha) = 0$. Ciò mostra la prima inclusione. La seconda è evidente perché $A\{x\} \subset A[x]$.

Osservazione 10.5. Se A è un campo, allora $\mathrm{Int}(E : A) = \mathrm{Alg}(E : A)$.

Definizione 10.6. Denotiamo con $A^\bullet$ l'insieme degli elementi invertibili di A e poniamo $A^\square := A^\bullet \cup \{0\}$.

Definizione 10.7. L'anello A (per ipotesi commutativo) si dice *fattoriale*, se è integro e se ogni elemento di $A \setminus A^\square$ è prodotto di elementi primi.

Proposizione 10.8. *I sia un ideale di A. Allora l'omomorfismo canonico $A[x] \longrightarrow (A/I)[x]$ è suriettivo e il suo nucleo è uguale a $I[x]$. Otteniamo in questo modo un isomorfismo naturale*

$$A[x]/I[x] \cong (A/I)[x]$$

Dimostrazione. Facile verifica.

Proposizione 10.9. *Siano A integro ed $a \in A$. Allora sono equivalenti:*

(1) a è primo in A.

(2) a è primo in $A[x]$.

Dimostrazione. È sufficiente dimostrare che Aa è un ideale primo di A se e solo $A[x]a$ è un ideale primo in $A[x]$. Ma ciò segue dall'isomorfia $A[x]/A[x]a \cong (A/Aa)[x]$ e del fatto che $(A/Aa)[x]$ è integro se e solo se A/Aa è integro.

Osservazione 10.10. A sia fattoriale. Allora per $a_1, \ldots, a_m \in A$ esiste un massimo comune divisore (mcd) di $a_1, \ldots, a_m$, essenzialmente unico (cioè determinato a meno di un fattore invertibile).

Se $(a_1, \ldots, a_m) \neq (0, \ldots, 0)$ e se d è un mcd di $a_1, \ldots, a_m$, allora $d \neq 0$ e gli elementi $\frac{a_1}{d}, \ldots, \frac{a_m}{d}$ sono relativamente primi.

Definizione 10.11. Un polinomio $f \in A[x]$ si dice *primitivo*, se è di grado ≥ 1 e se i coefficienti di f sono relativamente primi.

Lemma 10.12. *Sia A fattoriale e sia K il campo dei quozienti di A. Siano $f, g \in K[x]$ tale che $fg \in A[x]$.*

Allora esiste $\lambda \in K \setminus 0$ tale che $\lambda f, \lambda^{-1} g \in A[x]$.

Dimostrazione. Sia $h := fg$. Per ipotesi $h \in A[x]$.

Siccome K è il campo dei quozienti di A, esiste un $b \in A$ tale che $bf, bg \in A[x]$. Possiamo assumere $f, g \neq 0$. Siano d un massimo comune divisore dei coefficienti di bf ed e un massimo comune divisore dei coefficienti di bg in A. Allora i polinomi $F := \frac{b}{d} f$ e $G := \frac{b}{e} g$ siano primitivi. Inoltre $h = fg = \frac{de}{b^2} FG$, cosicché $b^2 h = deFG$.

Per la prop 10.9 ogni fattore primo di b^2 deve dividere uno dei fattori de, F o G in A. Siccome F e G sono primitivi, necessariamente $b^2 | de$ in A. Perciò esiste $c \in A$ tale che $b^2 c = de$ e quindi $b^2 h = b^2 cFG$.

Corollario 10.13. *A sia fattoriale e K il campo dei quozienti di A. Siano $f \in K\{x\}$ e $g \in K[x]$ tali che $fg \in A\{x\}$.*

Allora $f, g \in A\{x\}$.

Dimostrazione. (1) È chiaro che $g \in K\{x\}$.

(2) Per il lemma 10.12 esiste $\lambda \in K \setminus 0$ con λf, $\lambda^{-1} g \in A[x]$. Ciò implica però , essendo f e g monici, che λ, $\lambda^{-1} \in A$, per cui
$f = \lambda^{-1}(\lambda f) \in A[x]$ e $g = \lambda(\lambda^{-1} g) \in A[x]$.

Definizione 10.14. Siano K un sottocampo di E ed $\alpha \in \mathrm{Alg}(E : K)$. Allora denotiamo con $\pi_{\alpha:K}$ il polinomio di α su K.

Proposizione 10.15. *A sia fattoriale ed E contenga il campo dei quozienti K di A. Sia $\alpha \in \mathrm{Int}(E : A)$. Allora $\pi_{\alpha:K} \in A\{x\}$.*

Dimostrazione. Per ipotesi esiste $h \in A\{x\}$ con $h(\alpha) = 0$. Ciò implica in particolare che $\alpha \in \mathrm{Alg}(E : H)$ e che $\pi_{\alpha:K} | h$ in $K[x]$ e ciò significa che esiste $g \in K[x]$ tale che $\pi_{\alpha:K} g = h$. Dal cor. 10.13 segue $\pi_{\alpha:K} \in A\{x\}$.

Definizione 10.16. Gli elementi di $\mathrm{Int}(\mathbb{C} : \mathbb{Z})$ sono detti interi algebrici.

Osservazione 10.17. α sia un intero algebrico. Allora $\pi_{\alpha:\mathbb{Q}} \in \mathbb{Z}\{x\}$.

Osservazione 10.18. Siano $\alpha \in E$ ed $\alpha^n + a_1 \alpha^{n-1} + \ldots + a_n = 0$ con $a_1, \ldots, a_n \in A$. Allora $\alpha^m \in A + A\alpha + \ldots + A\alpha^{n-1}$ per ogni $m \geq 0$, cosicché

$$A[\alpha] = A + A\alpha + \ldots + A\alpha^{n-1}$$

$A[\alpha]$ è perciò un A-modulo finitamente generato.

Nota 10.19. M sia un E-modulo. Per ogni $n \geq 1$ allora anche M^n è un E-modulo, quindi anche un E_n^n-modulo. Per $v^1, \ldots, v^n \in M$ e $T \in E_n^n$ si ha semplicemente

$$T\begin{pmatrix} v^1 \\ \dots \\ v^n \end{pmatrix} = \begin{pmatrix} w^1 \\ \dots \\ w^n \end{pmatrix}$$

con $w^i = \sum_{k=1}^{n} T_k^i v^k$ per ogni $i = 1, \dots, n$. Per $n = 2$ si ha ad esempio

$$\begin{pmatrix} T_1^1 & T_2^1 \\ T_1^2 & T_2^2 \end{pmatrix} \begin{pmatrix} v^1 \\ v^2 \end{pmatrix} = \begin{pmatrix} T_1^1 v^1 + T_2^1 v^2 \\ T_1^2 v^1 + T_2^2 v^2 \end{pmatrix}$$

Per $S, T \in E_n^n$ si ha $STv = S(Tv)$ per ogni $v \in M^n$.

Osservazione 10.20. M sia un E-modulo e $v \in M^n$. Sia $T \in E_n^n$ tale che $Tv = 0$. Allora $(\det T)v = 0$.

Dimostrazione. Ciò segue da $T_{ad}T = (\det T)\delta$.

Lemma 10.21. *Siano $\alpha \in E$ ed M un $A[x]$-modulo. M sia finitamente generato come A-modulo. Allora esistono $n \geq 1$ e $T \in A_n^n$ tali che $\det(\alpha - T)M = 0$.*

Dimostrazione. Per ipotesi esistono $v^1, \dots, v^n \in M$ tali che $M = Av^1 + \dots + Av^n$. Allora $\alpha v^i = \sum_{k=1}^{n} T_k^i v^k$ per ogni i, con $T_k^i \in A$. Siano

$$v := \begin{pmatrix} v^1 \\ \dots \\ v^n \end{pmatrix} \in M^n \text{ e } T := \begin{pmatrix} T_1^1 & \dots & T_n^1 \\ \dots & & \\ T_1^n & \dots & T_n^n \end{pmatrix} \in A_n^n.$$

Allora $\alpha v = Tv$, perciò $(\alpha - T)v = 0$. Per l'oss. 10.20 allora $\det(\alpha - T)v = 0$, e ciò significa $\det(\alpha - T)v^i = 0$ per ogni i. Siccome però $M = Av^1 + \dots + Av^n$, otteniamo $\det(\alpha - T)M = 0$.

Teorema 10.22. *Per $\alpha \in E$ sono equivalenti :*

(1) $\alpha \in \mathrm{Int}(E : A)$.

(2) $A[\alpha]$ è un A-modulo finitamente generato.

(3) Esiste un sottoanello B di E con $A[\alpha] \subset B$ tale che B sia un A-modulo finitamente generato.

(4) Esiste un $A[\alpha]$-modulo M, finitamente generato come A-modulo tale che $\mathrm{ann}_{A[\alpha]} M = 0$.

(5) Esistono $n \geq 1$ e $T \in A_n^n$ tali che $\det(\alpha - T) = 0$.

Dimostrazione.

(1) $\Longrightarrow$ (2): Segue dall'oss. 10.18.

(2) $\Longrightarrow$ (3): Possiamo prendere $B := A[\alpha]$.

(3) $\Longrightarrow$ (4): Possiamo prendere $M := B$. Infatti, per ipotesi B è un A-modulo finitamente generato. Dobbiamo solo dimostrare che $\mathrm{ann}_{A[\alpha]} B = 0$. Ma ciò è vero perché $1 \in B$.

(4) $\Longrightarrow$ (5): Sia M come nel punto (4). Per il lemma 10.21 esistono $n \geq 1$ e $T \in A_n^n$ tale che $\det(\alpha - T)M = 0$. Per ipotesi $\mathrm{ann}_{A[\alpha]} M = 0$, perciò $\det(\alpha - T) = 0$, essendo chiaramente $\det(\alpha - T) \in A[\alpha]$.

(5) $\Longrightarrow$ (1): Siano $n \geq 1$ e $T \in A_n^n$ con $\det(\alpha - T) = 0$. Allora $f := \det(x - T) \in A\{x\}$ con $f(\alpha) = 0$.

Corollario 10.23. *Sia* $\alpha \in \mathrm{Int}(E : A)$. *Allora* $A[\alpha] \subset \mathrm{Int}(E : A)$.

Dimostrazione. Sia $\beta \in A[\alpha]$. Allora $A[\beta] \subset A[\alpha]$, perciò $A[\alpha]$ è un $A[\beta]$-modulo, il quale è un A-modulo finitamente generato per l'oss. 10.18, perché per ipotesi $\alpha \in \mathrm{Int}(E : A)$. Inoltre $I \in A[\alpha]$, per cui $\mathrm{ann}_{A[\beta]} A[\alpha] = 0$. L'enunciato segue dal punto (4) del teorema 10.22.

Definizione 10.24. E si dice *intero* su A, se $E = \mathrm{Int}(E : A)$, cioè se ogni elemento di E è intero su A.

Osservazione 10.25. Sia E un A-modulo finitamente generato. Allora E è intero su A.

Dimostrazione. Segue dal teorema 10.22.

Osservazione 10.26. Per $\alpha \in E$ sono equivalenti:

(1) $\alpha \in \mathrm{Int}(E : A)$.

(2) $A[\alpha]$ è intero su A

Dimostrazione. Cor. 10.23.

Lemma 10.27. *M sia un E-modulo finitamente generato ed E stesso un A-modulo finitamente generato. Allora M è un A-modulo finitamente generato.*

Dimostrazione. Siano $M = Ev_1 + \ldots + Ev_m$ con $v_1, \ldots, v_m \in M$ ed $E = A\alpha_1 + \ldots + A\alpha_n$ con $\alpha_1, \ldots, \alpha_n \in E$. Allora $M = A\alpha_1 v_1 + \ldots + A\alpha_1 v_m + \ldots + A\alpha_n v_1 + A\alpha_n v_m$.

Proposizione 10.28. *Per $\alpha_1, \ldots, \alpha_n \in E$ sono equivalenti:*

(1) $A[\alpha_1, \ldots, \alpha_n]$ è intero su A.

(2) $\alpha_1, \ldots, \alpha_n \in \mathrm{Int}(E : A)$.

(3) $A[\alpha_1, \ldots, \alpha_n]$ è un A-modulo finitamente generato.

Dimostrazione.

(1) $\Longrightarrow$ (2): Chiaro.

(2) $\Longrightarrow$ (3): Induzione su n.

$n = 1$: Sia $\alpha_1 \in \mathrm{Int}(E : A)$. Allora per l'oss. 10.18 $A[\alpha]$ è un A-modulo finitamente generato.

$n \longrightarrow n + 1$: Per ipotesi di induzione $A[\alpha_1, \ldots, \alpha_{n-1}]$ è un A-modulo finitamente generato. Inoltre $\alpha_n \in \mathrm{Int}(E : A)$, per cui anche $\alpha_n \in \mathrm{Int}(E : A[\alpha_1, \ldots, \alpha_{n-1}])$. Quindi $A[\alpha_1, \ldots, \alpha_n]$ è un $A[\alpha_1, \ldots, \alpha_{n-1}]$-modulo finitamente generato. Per il lemma 10.27 $A[\alpha_1, \ldots, \alpha_n]$ è un A-modulo finitamente generato.

(3) $\Longrightarrow$ (1): $A[\alpha_1, \ldots, \alpha_n]$ sia un A-modulo finitamente generato e $\beta \in A[\alpha_1, \ldots, \alpha_n]$. Allora $A[\beta] \subset A[\alpha_1, \ldots, \alpha_n]$ e del punto (3) del teorema 10.22 segue che $\beta \in \mathrm{Int}(E : A)$.

Teorema 10.29. $\mathrm{Int}(E : A)$ *è un sottoanello di* E.

Dimostrazione. Siano $\alpha, \beta \in \mathrm{Int}(E : A)$. Per la prop. 10.28 $A[\alpha, \beta] \subset \mathrm{Int}(E : A)$. In particolare quindi $\alpha + \beta, \alpha\beta \in \mathrm{Int}(E : A)$.

Proposizione 10.30. *B sia un sottoanello di E con $A \subset B$. B sia intero su A. Allora* $\mathrm{Int}(E : B) = \mathrm{Int}(E : A)$.

Dimostrazione. (1) Chiaramente $\mathrm{Int}(E : A) \subset \mathrm{Int}(E : B)$.

(2) Sia $\alpha \in \mathrm{Int}(E : B)$. Allora esistono $b_1, \ldots, b_n \in B$ con $\alpha^n + b_1\alpha^{n-1} + \ldots + b_n = 0$. Perciò α è un intero su $D := A[b_1, \ldots, b_n]$, e quindi $D[\alpha]$ è un D-modulo finitamente generato. D stesso è un A-modulo finitamente generato, e dal lemma 10.27 segue che $D[\alpha]$ è un A-modulo finitamente generato.

Corollario 10.31. *B sia un sottoanello di E con $A \subset B$. E sia intero su B e B intero su A. Allora E è intero su A.*

Definizione 10.32. A sia integro. Allora A si dice *integralmente chiuso*, se $\mathrm{Int}(K(A) : A) = A$.

$K(A)$ è il campo quoziente di A.

Teorema 10.33. *Ogni anello fattoriale è integralmente chiuso.*

Dimostrazione. A sia un anello fattoriale ed $\alpha = \dfrac{b}{c}$ con $b, c \in A$, $c \neq 0$, e $\mathrm{mcd}(b, c) = 1$. α sia intero su A. Allora esistono $a_1, \ldots, a_n \in A$ con $\alpha^n + a_1\alpha^1 + \ldots + a_n = 0$, per cui $b^n + a_1 b^{n-1}c + a_2 b^{n-2}c^2 + \ldots + a_n c^n = 0$. Vogliamo dimostrare che $c \in A$. Assumiamo che non sia così. Allora esiste un elemento primo in A con $p|c$. Ciò implica però $p|b^n$ e quindi $p|b$, in contraddizione con l'ipotesi che $\mathrm{mcd}(b, c) = 1$.

Corollario 10.34. *(1) $\mathbb{Z}$ è integralmente chiuso.*

Quindi ogni numero razionale intero su $\mathbb{Z}$ appartiene a $\mathbb{Z}$.

(2) Ogni anello $\mathbb{Z}[x_1, \ldots, x_n]$ è integralmente chiuso.

(3) Ogni anello $K[x_1, \ldots, x_n]$, dove K è un campo, è integralmente chiuso.

(4) Ogni anello ed ideale principale è integralmente chiuso.

11. Il teorema della dimensione

Situazione 11.1. G sia un gruppo finito, $(R_1, \ldots, R_\kappa)$ un sistema di Burnside di G e $(n_1, \ldots, n_\kappa)$ il corrispondente vettore delle dimensioni. Per ogni $\alpha = 1, \ldots, \kappa$ sia $\chi_\alpha := \operatorname{tr} R_\alpha$.

Definizione 11.2. Siano K un campo ed $f = x^n + a_1 x^{n-1} + \ldots + a_n \in K\{x\}$. Allora la matrice

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_n \\ 1 & 0 & \ldots & 0 & -a_{n-1} \\ 0 & 1 & \ldots & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 0 & -a_{n-3} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix}$$

si chiama la *matrice compagna* (talvolta anche *matrice di Frobenius*) di f.

Lemma 11.3. *Siano K un campo ed $f \in K\{x\}$. Allora f coincide con il polinomio caratteristico della sua matrice compagna.*

Dimostrazione. Horn/Johnson, pagg. 146-147, Scheja/Storch, pagg. 260-261, Simon, pag. 44.

Corollario 11.4. *Sia $\alpha \in \mathbb{C}$. Allora sono equivalenti:*

(1) $\alpha \in \operatorname{Int}(\mathbb{C} : \mathbb{Z})$.

(2) α è autovalore di una matrice appartenente a $\mathbb{Z}_n^n$ per qualche $n \in \mathbb{N} + 1$.

(3) α è autovalore di una matrice che appartiene a $(\operatorname{Int}(\mathbb{C} : \mathbb{Z}))_n^n$ per qualche $n \in \mathbb{N} + 1$.

Dimostrazione. $(1) \Longrightarrow (2)$: Sia $\alpha \in \operatorname{Int}(\mathbb{C} : \mathbb{Z})$. Allora esiste $f \in \mathbb{Z}\{x\}$ tale che $f(\alpha) = 0$. Sia A la matrice compagna di f. Chiaramente $A \in \mathbb{Z}_n^n$. Per il lemma 11.3 α è autovalore di A.

$(2) \Longrightarrow (3)$: Chiaro.

$(3) \Longrightarrow (1)$: Poniamo $D := \operatorname{Int}(\mathbb{C} : \mathbb{Z})$. α sia autovalore di una matrice $A \in D_n^n$. Sia f il polinomio caratteristico di A. Allora $f(\alpha) = 0$, mentre l'ipotesi $A \in D_n^n$ implica $f \in D\{x\}$, per cui $\alpha \in \operatorname{Int}(\mathbb{C} : D)$. Dalla prop. 10.30 segue $\alpha \in \operatorname{Int}(\mathbb{C} : \mathbb{Z})$.

Proposizione 11.5. *I caratteri sono ortogonali rispetto alla convoluzione. Più precisamente per ogni $\alpha, \beta = 1, \ldots, \kappa$ abbiamo:*

(1) $\chi_\alpha * \chi_\beta = 0$ *per* $\alpha \neq \beta$.

(2) $\chi_\alpha * \chi_\alpha = \frac{|G|}{n_\alpha} \chi_\alpha$.

Dimostrazione. Per $g \in G$ abbiamo

$$\chi_\alpha * \chi_\beta(g) = \sum_{h\in G} \chi_\alpha(h)\chi_\beta(h^{-1}g) = \sum_{h\in G}\sum_{i=1}^{\kappa}\sum_{j=1}^{\kappa} R^i_{i\alpha}(h)\overline{R^j_{j\beta}(h)}R^j_{j\beta}(g)$$
$$= \sum_{j=1}^{\kappa} R^j_{j\beta}(g)\sum_{i=1}^{\kappa}\|R^i_{i\alpha}, R^j_{j\beta}\|$$

Dal cor. 3.10 segue anche che $\chi_\alpha * \chi_\beta = 0$ per $\alpha \neq \beta$. Infine dal cor. 3.11 abbiamo

$$\chi_\alpha * \chi_\alpha = \sum_{j=1}^{\kappa} R^j_{j\alpha}\|R^j_{j\alpha}, R^j_{j\alpha}\| = \sum_{j=1}^{\kappa} R^j_{j\alpha}\frac{|G|}{n_\alpha} = \frac{|G|}{n_\alpha}\chi_\alpha$$

Corollario 11.6. *Gli elementi $\frac{n_\alpha}{|G|}\chi_\alpha$ sono quindi idempotenti ortogonali in $\mathbb{C}G$.*

Lemma 11.7. *Per ogni $\alpha = 1, \ldots, \kappa$, per ogni $g \in G$ vale $\chi_\alpha(g) \in \mathrm{Int}(\mathbb{C} : \mathbb{Z})$.*

Dimostrazione. Sappiamo che $g^{|G|} = 1$. Perciò la G-esima potenza della matrice $R_\alpha(g)$ è la matrice identica e ciò implica che per ogni autovalore λ di $R_\alpha(g)$ si ha $\lambda^{|G|} = 1$. Ciò mostra in particolare che $\lambda \in \mathrm{Int}(\mathbb{C} : \mathbb{Z})$ e siccome la traccia $\chi_\alpha(g)$ è la somma degli autovalori di $R_\alpha(g)$, per il teorema 10.29 anche $\chi_\alpha(g) \in \mathrm{Int}(\mathbb{C} : \mathbb{Z})$.

Definizione 11.8. In questa parte finale del capitolo usiamo le seguenti notazioni. Sia $\alpha \in \{1, \ldots, \kappa\}$ un indice fissato. Allora:

(1) $g_1 = 1_G, g_2, \ldots, g_{|G|}$ siano gli elementi di G (necessariamente tutti distinti).

(2) Per $i, j = 1, \ldots, |G|$ sia $B^j_i := \chi_\alpha(g_j^{-1}g_i)$. In questo modo otteniamo una matrice $B \in \mathbb{C}^{|G|}_{|G|}$.

(3) Per $i = 1, \ldots, |G|$ sia $v^i := \chi_\alpha(g_i)$. In questo modo otteniamo un vettore $v \in \mathbb{C}^{|G|}$.

Osservazione 11.9. $v \neq 0$

Dimostrazione. Infatti $v^1 = \chi_\alpha(1_G) = n_\alpha \neq 0$.

Lemma 11.10. $Bv = \frac{|G|}{n_\alpha}v$.

Per l'osservazione 11.9 $\frac{|G|}{n_\alpha}$ è quindi autovalore di B.

Dimostrazione. Per ogni $i = 1, \ldots, \kappa$ abbiamo per definizione

$$(Bv)^i = \sum_{j=1}^{\kappa} B^i_j v^j = \sum_{j=1}^{\kappa} \chi_\alpha(g_j^{-1}g_i)\chi_\alpha(g_j) =$$
$$= \chi_\alpha * \chi_\alpha(g_i) \overset{11.5}{=} \frac{|G|}{n_\alpha}\chi_\alpha(g_i) = \frac{|G|}{n_\alpha}v^i$$

.

Osservazione 11.11. $B \in (\mathrm{Int}(\mathbb{C} : \mathbb{Z}))_{|G|}^{|G|}$.

Dimostrazione. Ciò segue dal lemma 11.7.

Corollario 11.12. $\frac{|G|}{n_\alpha} \in \mathrm{Int}(\mathbb{C} : \mathbb{Z})$.

Dimostrazione. Per il lemma 11.10 $\lambda := \frac{|G|}{n_\alpha}$ è un autovalore di B. Ma $B \in (\mathrm{Int}(\mathbb{C} : \mathbb{Z}))_{|G|}^{|G|}$, per cui dalla prop. 10.30 segue $\lambda \in \mathrm{Int}(\mathbb{C} : \mathbb{Z})$.

Teorema 11.13. n_α *divide* $|G|$.

Dimostrazione. Ovviamente $\frac{|G|}{n_\alpha} \in \mathbb{Q}$. Dal cor. 11.12 sappiamo però che $\frac{|G|}{n_\alpha} \in \mathbb{Q} \cap \mathrm{Int}(\mathbb{C} : \mathbb{Z}) \overset{10.34}{=} \mathbb{Z}$.

12. Applicazioni in statististica

Situazione 12.1. Il libro di Diaconis tratta in modo dettagliato l'utilizzo della teoria delle rappresentazioni dei gruppi finiti in statistica e calcolo delle probabilità . Presentiamo l'idea fondamentale di questa tecnica.

Nota 12.2. In un'indagine di mercato 1200 persone hanno scelto, su tre prodotti proposti, una graduatoria preferenziale con il seguente risultato:

123	id	100
213	(12)	500
132	(23)	120
321	(13)	140
231	(123)	300
312	(132)	40

La prima colonna contiene la graduatoria scelta, la seconda la permutazione corrispondente e la terza il numero delle preferenze. L'ultima colonna può essere interpretata come funzione $f : S_3 \longrightarrow \mathbb{C}$ alla quale possiamo applicare la formula di rappresentazione del teorema 4.42:

$$f = \sum_{\alpha=1}^{\kappa} \sum_{i=1}^{n_\alpha} \sum_{j=1}^{n\alpha} \lambda_{j\alpha}^{i}$$

con $\lambda_{j\alpha}^{i} = \dfrac{n_\alpha}{6} \| f, R_{j\alpha}^{i} \|$.

Osservazione 12.3. Dalla tabella della nota 6.3 otteniamo i $\lambda_{j\alpha}^{i}$

$$\begin{aligned}\lambda_{11}^{1} &= \frac{1}{6}[f(\mathrm{id}) + f(12) + f(23) + f(13) + f(123) + f(132)] \\ &= \frac{1}{6}[100 + 500 + 120 + 140 + 300 + 40] = \frac{1200}{6} = 200\end{aligned}$$

$$\begin{aligned}\lambda_{12}^{1} &= \frac{1}{6}[f(\mathrm{id}) - f(12) - f(23) - f(13) + f(123) + f(132)] \\ &= \frac{1}{6}[100 - 500 - 120 - 140 + 300 + 40] = \frac{320}{6} \approx 53\end{aligned}$$

$$\begin{aligned}\lambda_{13}^{1} &= \frac{2}{6}[f(\mathrm{id}) + f(12) - \frac{1}{2}f(23) - \frac{1}{2}f(13) - \frac{1}{2}f(123) - \frac{1}{2}f(132)] \\ &= \frac{2}{6}[100 + 500 - 60 - 70 - 150 - 20] = \frac{600}{6} = 100\end{aligned}$$

$$\begin{aligned}\lambda_{23}^{1} &= \frac{2}{6}[0 + 0 - \frac{\sqrt{3}}{2}f(23) + \frac{\sqrt{3}}{2}f(13) - \frac{\sqrt{3}}{2}f(123) + \frac{\sqrt{3}}{2}f(132)] \\ &= \frac{2}{6}[\sqrt{3}(-60 + 70 - 150 + 20)] = \frac{1}{3}[\sqrt{3}(-120)] \approx -81\end{aligned}$$

$$\lambda^2_{13} = \frac{2}{6}[0 + 0 + \frac{\sqrt{3}}{2}f(23) + \frac{\sqrt{3}}{2}f(13) + \frac{\sqrt{3}}{2}f(123) - \frac{\sqrt{3}}{2}f(132)]$$
$$= \frac{2}{6}[\sqrt{3}(60 + 70 + 150 - 20)] = \frac{1}{3}[\sqrt{3}(260)] \approx 69$$

$$\lambda^2_{23} = \frac{2}{6}[f(\mathrm{id}) - f(12) + \frac{1}{2}f(23) + \frac{1}{2}f(13) - \frac{1}{2}f(123) - \frac{1}{2}f(132)]$$
$$= \frac{2}{6}[100 - 500 + 60 + 70 - 150 - 20] = -\frac{440}{3} \approx 176$$

Abbiamo quindi (approssimativamente)

$$f = 200R^1_{11} - 53R^1_{12} + 100R^1_{13} - 81R^1_{23} + 69R^2_{13} - 176R^2_{23} \quad (^*)$$

La funzione R^1_{11} è costante e quindi statisticamente irrilevante; degli altri coefficienti il più importante è il coefficiente della componente R^2_{23}, che corrisponde all'ultima colonna della tabella nella nota 6.3. Abbiamo invertito i segni in accordo con $(^*)$:

g	$-R^2_{23}(g)$
id	-1
(12)	1
(23)	$-\frac{1}{2}$
(13)	$-\frac{1}{2}$
(123)	$\frac{1}{2}$
(132)	$\frac{1}{2}$

Questa è quindi la componente più significativa della funzione.

Bibliografia

P. Diaconis: Group representations in probability and statistics. IMS 1988.

R. Horn/C. Johnson: Matrix analysis. Cambridge UP 1993.

I. Isaacs: Character theory of finite groups. Dover 1994.

A. Machì: Gruppi. Springer 2007.

F. Paset: Regressione, correlazione e analisi delle componenti principali. Tesi, Ferrara 2003.

B. Simon: Representations of finite and compact groups. AMS 1996.

G. Scheja/U. Storch: Lehrbuch der Algebra II. Teubner 1988.