UNIVERSITÀ DEGLI STUDI DI CATANIA
FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
CORSO DI LAUREA IN MATEMATICA

ANDREA LO PUMO

IL TEOREMA DI BURNSIDE

TESI DI LAUREA

RELATORE: PROF. M. D'ANNA

ANNO ACCADEMICO 2008/2009

Indice

1 Introduzione

Il teorema di Burnside è uno dei teoremi più noti della teoria dei caratteri: attraverso un elegante uso delle proprietà algebriche dei caratteri, dimostra che per un gruppo non risolubile devono esistere almeno tre primi distinti che dividono il suo ordine.

William Burnside (2 Luglio 1852 - 21 Agosto 1927) è stato un matematico inglese, conosciuto come uno dei primi studiosi della teoria dei gruppi finiti. Burnside, nato a Londra, frequentò l'Università di Cambridge, dove dieci anni dopo insegnò come lecturer.

Alla fine dell'800, la teoria dei gruppi non era un campo largamente studiato, tuttavia, durante la sua carriera, Burnside fu un ricercatore molto attivo e pubblicò più di 150 articoli che ottennero diffusi riconoscimenti. La parte principale del lavoro di Burnside riguarda le rappresentazioni dei gruppi. I suoi contributi hanno permesso lo sviluppo di alcuni aspetti fondamentali della teoria. Uno dei suoi risultati più noti è il cosidetto Teorema $p^a q^b$, che dimostra come ogni gruppo finito il cui ordine è divisibile da meno di tre primi sia risolubile.

In questa tesi presenteremo la dimostrazione classica del teorema di Burnside.

Nel secondo capitolo richiameremo i concetti e i risultati fondamentali sulle algebre, i moduli, le algebre di gruppo e le rappresentazioni. Vedremo che adoperando il teorema di Maschke è possibile costruire su ogni gruppo finito un'algebra semisemplice. Per questo motivo, ci interesseremo più particolarmente del teorema di Wedderburn, che consente di "spezzettare" un'algebra semisemplice in una somma di strutture più facili da gestire. Tramite le rappresentazioni, per lo studio delle algebre semisemplici di gruppo, potremo far ricorso a strumenti più concreti, come le matrici. Per questioni di brevità, tutte le dimostrazioni della prima parte saranno omesse.

Nel terzo capitolo, definiremo i caratteri come una versione ridotta delle rappresentazioni e studieremo le loro proprietà che risulteranno utili per l'analisi dei gruppi finiti. Presenteremo due teoremi fondamentali che riguardano i caratteri: il primo afferma che i caratteri sono tutte e sole quelle funzioni di classe che si possono scrivere come combinazione lineare intera degli elementi di $\mathrm{Irr}(G)$; il secondo mostra che i caratteri indotti da due rappresentazioni sono uguali se e solo se le rappresentazioni sono simili.

Il quarto capitolo è dedicato alle relazioni che intercorrono tra gli interi algebrici e i caratteri. Ad esempio, vedremo che un carattere valutato in un elemento del suo gruppo è un intero algebrico che appartiene ad un'estensione finita di $\mathbb{Q}$.

Nell'ultimo capitolo, sarà presentata la dimostrazione del teorema di Burnside, in cui verranno applicati tutti i risultati ottenuti nei capitoli precedenti: l'espres-

sione che caratterizza il carattere regolare ρ_G come somma di caratteri irriducibili, la possibilità di scrivere un carattere come somma di radici n-esime dell'unità, la relazione che intercorre tra le classi di coniugio del gruppo di un carattere fissato. Infine, un passo decisivo della dimostrazione sarà costituito dall'applicazione delle proprietà che scaturiscono dal considerare i caratteri come dei particolari interi algebrici dell'estensione $\mathbb{Q}(\xi)$.

2 Preliminari

In questa prima parte della tesi verranno enunciati, senza dimostrazione, i teoremi più significativi riguardanti le Algebre e le Rappresentazioni di gruppi finiti. Per ulteriori approfondimenti, faremo riferimento a [1].

Definizione 2.1. Sia A un anello (o gruppo). Se B è un sottoanello (o sottogruppo) di A, scriveremo $B \leq A$.

1. Supporremo che in ogni anello unitario, $0_A \neq 1_A$, ovvero che lo zero dell'anello sia diverso dall'elemento unità, cioè

$$\{0\} \subset \{0,1\} \subseteq A$$

   Quindi ogni anello unitario ha almeno 2 elementi.

2. Ogni anello sarà ritenuto implicitamente unitario.

Osservazione 2.2. Tutti gli spazi vettoriali che considereremo saranno di dimensione finita.

2.1 Algebre

Definizione 2.3. Sia A un F-spazio vettoriale finitamente generato e un anello[1].

$$A \text{ è un'algebra} \overset{\text{def}}{\Leftrightarrow} \lambda(ab) = (\lambda a)b = a(\lambda b) \ \ \forall a, b \in A, \ \forall \lambda \in F$$

Definizione 2.4. Sia $B \subseteq A$,

$$B \text{ è una sottoalgebra di } A \overset{\text{def}}{\Leftrightarrow} B \begin{cases} \text{è un sottospazio vettoriale di A} \\ \text{è un sottoanello di A} \\ 1_A \in B \end{cases}$$

Se B è una sottoalgebra di A utilizzeremo la seguente notazione:

$$B \preceq A$$

Osservazione 2.5. Una sottoalgebra è un'algebra

[1] usiamo la stessa operazione di somma sia nello spazio che nell'anello. NOTA: l'anello è unitario

Definizione 2.6. Si definisce centro dell'algebra A il seguente insieme:

$$Z(A) = \{a \in A \mid ab = ba \ \ \forall b \in A\}$$

Osservazione 2.7. $Z(A) \preceq A$

Proposizione 2.8. *Sia $e_1, \ldots, e_n$ una base di A, allora*

$$Z(A) = \{a \in A \mid ae_i = e_i a \ \ \forall i = 1, \ldots, n\}$$

Definizione 2.9. Sia data una mappa $f : A \longrightarrow B$, con A, B algebre.

$$f \text{ è un omomorfismo di algebre (alg-hom)} \overset{\text{def}}{\Leftrightarrow} \begin{cases} f \text{ è una applicazione lineare} \\ f \text{ è un omomorfismo di anelli} \\ f(1_A) = 1_B \end{cases}$$

$$\text{o equivalentemente se: } \begin{cases} f(\lambda x + \mu y) = \lambda f(x) + \mu f(y) \\ f(xy) = f(x)f(y) \\ f(1_A) = 1_B \end{cases} \qquad \forall x, y \in A \ \ \forall \lambda, \mu \in F$$

Notazione 2.10. Con $I \trianglelefteq A$ indichiamo un ideale (bilatero) di A. Con $I \overset{d}{\trianglelefteq} A$ un ideale destro di A.

Definizione 2.11. Sia A un anello,

$$A \text{ è semplice } \overset{\text{def}}{\Leftrightarrow} \begin{cases} \forall I \trianglelefteq A \ \ I = A \vee I = 0 \\ A \neq 0 \end{cases}$$

Teorema 2.12. *Sia $A = F^{n \times n}$, con F campo, allora,*

$$A \text{ è un'algebra semplice}$$

2.2 Moduli

Definizione 2.13. Sia A un F-algebra e V un F-spazio vettoriale, allora

$$V \text{ è un } A\text{-modulo, secondo l'operazione } \cdot : V \times A \longrightarrow V \ \overset{\text{def}}{\Leftrightarrow}$$

$$\overset{\text{def}}{\Leftrightarrow} \begin{cases} 1. \ v1_A = v \\ 2. \ (v + w)a = va + wa \\ 3. \ (va)b = v(ab) \\ 4. \ v(a + b) = va + vb \\ 5. \ (\lambda v)a = v(\lambda a) = \lambda(va) \end{cases} \qquad \forall \lambda \in F, \ \forall a, b \in A, \ \ \forall v, w \in V$$

Esempio 2.14.

1. $A = F^{n\times n}$, $V = F^n$ è un A-modulo con l'usuale operazione di moltiplicazione tra vettore (riga) e matrice[2]
2. A algebra, $V = A$. Questo A-modulo si chiama l'*A-modulo regolare*, e si indica con A°

Definizione 2.15. Sia V un A-modulo, e $W \leq V$,

$$W \text{ è un sotto } A\text{-modulo di } V \overset{\text{def}}{\Leftrightarrow} wa \in W \ \ \forall w \in W \ \forall a \in A$$

Per indicare che W è un A-sottomodulo di V useremo la seguente notazione:

$$W \overset{A}{\leq} V$$

Esempio 2.16. I sottomoduli di A° sono gli ideali destri.

Definizione 2.17. Sia V un A-modulo, chiameremo *annullatore* di V in A il seguente insieme:

$$\text{ann}_A(V) \overset{\text{def}}{=} \{a \in A \mid Va = 0\}$$

Proposizione 2.18. *Sia A un anello unitario; allora*

$$\text{ann}_A(V) \trianglelefteq A$$

Definizione 2.19. Sia V un A-modulo,

$$V \text{ è semplice } \overset{\text{def}}{\Leftrightarrow} \text{ gli unici sottomoduli di } V \text{ sono } 0, V$$

Teorema 2.20. *Sia $A = F^{n\times n}$ e sia $V = F^n$.*
V è un A-modulo con l'usuale moltiplicazione tra vettori e matrici, inoltre V è semplice.

Definizione 2.21. Siano V, W due A-moduli.

$$f : V \longrightarrow W \text{ è un A-omomorfismo } \overset{\text{def}}{\Leftrightarrow} \begin{cases} 1. \ f \text{ è lineare} \\ 2. \ f(va) = f(v)a \ \ \forall v \in V, \ \forall a \in A \end{cases}$$

Se f è biettiva, diremo che f è un A-isomorfismo e scriveremo:

$$V \overset{A}{\simeq} W$$

[2] la moltiplicazione è a destra: $v \cdot a$, con $a \in A$

Proposizione 2.22. *Siano V, W degli A-moduli.*

$\mathrm{Hom}_A(V,W) \overset{def}{=} \{f : V \longrightarrow W \mid f \text{ } A\text{-omomorfismo}\}$ *è uno spazio vettoriale*

$\mathrm{End}_A(V) \overset{def}{=} \mathrm{Hom}_A(V,V)$ *è una sottoalgebra di* $\mathrm{End}_F(V)$

Teorema 2.23. *(Schur). Siano V, W degli A-moduli. Si ha che:*

$$\begin{cases} f : V \longrightarrow W \text{ } A\text{-omomorfismo} \\ V, W \text{ semplici} \\ \mathrm{Im}\, f \neq \{0\} \end{cases} \Rightarrow f \text{ è un } A\text{-isomorfismo}$$

Corollario 2.24. *Sia F un campo algebricamente chiuso, V un A-modulo semplice; allora*

$$f \in \mathrm{End}_A(V) \Leftrightarrow \exists \lambda \in F : \quad f = \lambda \mathrm{id}_V$$

Teorema 2.25. *Sia V un A-modulo, allora le seguenti condizioni sono equivalenti:*

1. $\forall U \overset{A}{\leq} V \ \exists W \overset{A}{\leq} V : \quad V = U \oplus W$
   (È possibile completare ogni sottomodulo di V)
2. $V = \sum_{i \in I} U_i$, *con* U_i *A-sottomodulo semplice*
3. $V = W_1 \oplus \cdots \oplus W_k$, *con* W_i *A-sottomodulo semplice, per ogni* $i = 1, \ldots, k$

2.3 Moduli semisemplici

Definizione 2.26. Un A-modulo V che soddisfa il Teorema 2.25 si dirà *semisemplice*.

Teorema 2.27. *Sia A una F-algebra; allora A° è semisemplice se e solo se ogni V A-modulo è semisemplice*

2.4 Algebre semisemplici

Definizione 2.28. Sia A una F-algebra,

$$A \text{ è semisemplice } \overset{\text{def}}{\Leftrightarrow} A^\circ \text{ è semisemplice}$$

Proposizione 2.29. *Sia V un A-modulo. Definiamo $A(V)$ come la somma di tutti gli ideali destri di A che sono A-isomorfi a V (nota[3]):*

$$A(V) \stackrel{def}{=} \sum_{I \stackrel{d}{\trianglelefteq} A^\circ :\, I \stackrel{A}{\simeq} V} I$$

Si ha:

$$V \text{ semplice } \Rightarrow A(V) \trianglelefteq A$$

Teorema 2.30. *(Wedderburn). Sia A una F-algebra semisemplice, allora*

1. $$V \text{ } A\text{-modulo semplice } \Leftrightarrow \exists I \stackrel{d}{\trianglelefteq} A \text{ minimale: } V \stackrel{A}{\simeq} I$$

   Ovvero, gli A-moduli semplici sono isomorfi ad A°-sottomoduli.

2. *Esistono $I_1, \dots, I_k \stackrel{d}{\trianglelefteq} A$ minimali tale che*

   $$I_i \not\simeq I_j \ \ \forall i \neq j$$
   $$I \stackrel{d}{\trianglelefteq} A \text{ minimale } \Rightarrow \exists i : \ I \stackrel{A}{\simeq} I_i$$

   Ovvero, se consideriamo la relazione d'equivalenza indotta da $\stackrel{A}{\simeq}$, otteniamo solo k classi di A°-sottomoduli semplici.

3. $A = A(I_1) \oplus \cdots \oplus A(I_k)$

4. $\operatorname{ann}_A(I_i) = \sum_{j \neq i} A(I_j)$

5. $A(I_i) \trianglelefteq A$ *è minimale per ogni* $i = 1, \dots, k$

6. $$\phi_i : A(I_i) \longrightarrow \operatorname{End}_F(I_i) \underbrace{\simeq}_{algebra} F^{m_i \times m_i}, \quad m_i = \dim I_i$$
   $$x \mapsto r_x : I_i \longrightarrow I_i$$
   $$u \mapsto ux$$

   è un omomorfismo di algebra iniettivo.
   Inoltre, se F è algebricamente chiuso, ϕ_i è biettiva e quindi si ha:

   $$A(I_i) \simeq \operatorname{End}_F(I_i) \simeq F^{m_i \times m_i}$$

[3] o in altre parole, la somma dei sottomoduli di A°, isomorfi a V

Nota: questi sono isomorfismi di algebre. $A(I_i)$ è un algebra la cui unità è e_i, dove $(e_1, \ldots, e_k) \in A(I_1) \times \ldots \times A(I_k)$ è quell'unica n-upla t.c.

$$1 = e_1 + \cdots + e_k$$

Corollario 2.31. *Un'algebra semisemplice è somma (diretta) di algebre semplici.*

Corollario 2.32. *Sia A un'algebra semisemplice su F algebricamente chiuso. Si ha:*

1. $A \simeq F^{n_1 \times n_1} \oplus \cdots \oplus F^{n_k \times n_k}$ *dove* $n_i = \dim I_i$
2. $k = \dim Z(A)$
3. $\dim A = \sum_{j=1}^{n} n_j^2$

dove $\{I_1, \ldots, I_k\}$ sono i rappresentanti delle classi di isomorfismo di A-moduli semplici.

2.5 Algebre di gruppo

L'obiettivo di questa sezione sarà quello di sfruttare il teorema di Wedderburn per ricavare informazioni sui gruppi finiti. Per far ciò, per ogni gruppo finito G, costruiremo un'algebra semisemplice strettamente legata ad esso.

Definizione 2.33. Sia G un gruppo finito, F un campo. Denoteremo con FG l'insieme delle combinazioni lineari formali[4] di G su F:

$$FG \stackrel{\text{def}}{=} \langle G \rangle_F = \left\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in F \right\}$$

Possiamo rendere FG un'algebra ponendo:

$$0 \stackrel{\text{def}}{=} \sum_{g \in G} 0g$$
$$1 \stackrel{\text{def}}{=} 1_F 1_G + \sum_{g \in G \setminus \{1_G\}} 0g$$

[4]possiamo considerare una somma formale $\sum_{g \in G} \lambda_g g$ come la scrittura simbolica di una funzione $\lambda : G \longrightarrow F$ tale che $\lambda(g) = \lambda_g$. Avremo così che:

$$\sum_{g \in G} \lambda_g g = \sum_{g \in G} \mu_g g \leftrightarrow \lambda_g = \mu_g \ \ \forall g \in G$$

e definendo le seguenti operazioni:

$$\sum_{g\in G}\lambda_g g+\sum_{g\in G}\mu_g g\overset{\text{def}}{=}\sum_{g\in G}(\lambda_g+\mu_g)g$$

$$\lambda\cdot\left(\sum_{g\in G}\lambda_g g\right)\overset{\text{def}}{=}\sum_{g\in G}(\lambda\lambda_g)g$$

$$\left(\sum_{g\in G}\lambda_g g\right)\cdot\left(\sum_{g\in G}\mu_g g\right)\overset{\text{def}}{=}\sum_{g,h\in G}\lambda_g\mu_h gh=\sum_{z\in G}\left(\sum_{g,h\in G:\ gh=z}\lambda_g\mu_h\right)z=$$

$$\underbrace{=}_{h=g^{-1}z}\ \sum_{z\in G}\left(\sum_{g\in G}\lambda_g\mu_{g^{-1}z}\right)z$$

Proposizione 2.34.

1. *FG è un'algebra*
2. $\dim FG=|G|$

Definizione 2.35. Sia G un gruppo finito e $X\subseteq G$; definiamo:

$$x^g\overset{\text{def}}{=}g^{-1}xg\ \ \forall x,g\in G$$

$$\underbrace{C_G(x)}_{\text{centralizzante di } x}\overset{\text{def}}{=}\{g\in G\mid xg=gx\}$$

$$\underbrace{x\sim y}_{x \text{ coniugato con } y}\overset{\text{def}}{\Leftrightarrow}\exists g\in G:\ x=y^g$$

$$\underbrace{\mathrm{cl}_G(x)}_{\text{classe di coniugio}}\overset{\text{def}}{=}x^G\overset{\text{def}}{=}\{x^g\mid g\in G\}$$

$$\mathrm{cl}(G)\overset{\text{def}}{=}\{\mathrm{cl}_G(x)\mid x\in G\}$$

$$\widehat{X}\overset{\text{def}}{=}\sum_{x\in X}x$$

Teorema 2.36. *Sia* $\mathrm{cl}(G)=\{K_1,\dots,K_k\}$*, allora*

1. $Z(FG)=\left\langle\widehat{K_1},\dots,\widehat{K_k}\right\rangle$
2. $\left\{\widehat{K_1},\dots,\widehat{K_k}\right\}$ *sono l.i.*
3. $\dim Z(FG)=k$

L'insieme $\left\{\widehat{K_1},\dots,\widehat{K_k}\right\}$ *è quindi una base dello spazio vettoriale* $Z(FG)$*.*

Teorema 2.37. *(Maschke). Sia* ch F *la caratteristica del campo* F*. Allora:*

$$\text{ch } F \not| |G| \Rightarrow FG \text{ è semisemplice}$$

Grazie al teorema di Maschke, se ch $F \not| |G|$, possiamo applicare il teorema di Wedderburn all'algebra semisemplice FG. Inoltre, utilizzando il Corollario 2.32 e il Teorema 2.36 otteniamo il seguente

Corollario 2.38.

1. *Se* F *è algebricamente chiuso:*
    1. $FG \simeq F^{n_1 \times n_1} \oplus \cdots \oplus F^{n_k \times n_k}$
       dove $n_i = \dim I_i$, $\{I_1, \ldots, I_k\}$ *rappresentanti delle classi di isomorfismo di* FG*-moduli semplici;*
    2. $n_1^2 + \cdots + n_k^2 = \dim FG = |G|$;
    3. $k = \dim Z(FG) = |\text{cl}(G)|$.
2. V FG*-modulo* $\Rightarrow V \simeq m_1 I_1 \oplus \cdots \oplus m_k I_k$ *dove* $m_i \geq 0$, $m_i I_i = \underbrace{I_i \oplus \cdots \oplus I_i}_{m_i \text{ volte}}$
3. $FG \simeq n_1 I_1 \oplus \cdots \oplus n_k I_k$

2.6 Rappresentazioni

Le algebre di gruppo e i loro moduli sono costruzioni che si basano sugli spazi vettoriali. Per questo motivo, è possibile dare una loro interpretazione concreta tramite l'algebra lineare delle matrici.

In questa sezione definiremo e studieremo delle particolari applicazioni lineari, chiamate *rappresentazioni*. Le rappresentazioni sono equivalenti ai moduli e codificano come matrice ogni elemento di un algebra di gruppo.

Definizione 2.39. Sia G un gruppo finito e F un campo. Chiameremo *rappresentazione* di G un qualsiasi omomorfismo di gruppi $\mathfrak{X} : G \longrightarrow \text{GL}(n, F)$ [5].
La rappresentazione dell'algebra FG sarà un qualsiasi omomorfismo di algebre del tipo $\mathfrak{X} : FG \longrightarrow F^{n \times n}$.

Poniamo inoltre

$$\dim \mathfrak{X} \overset{\text{def}}{=} n$$

[5] $\text{GL}(n, F) = \{M \in F^{n \times n} \mid \exists M^{-1}\}$

Proposizione 2.40. *Se $\mathfrak{X}$ è una rappresentazione di G, l'applicazione $\mathfrak{X}' : FG \longrightarrow F^{n\times n}$, ottenuta estendendo linearmente $\mathfrak{X}$, è una rappresentazione di FG. Viceversa, se $\mathfrak{X}'$ è una rappresentazione di FG, $\mathfrak{X} = \mathfrak{X}'_{|G}$ è una rappresentazione di G.*

Illustriamo adesso un metodo per ottenere un FG-modulo da una rappresentazione $\mathfrak{X}$ di FG, e viceversa.

Proposizione 2.41.

1. *Sia $\mathfrak{X} : FG \longrightarrow F^{n\times n}$ una rappresentazione di FG e sia $V = F^n$. V diventa un FG-modulo con l'operazione*

$$v{\cdot}g = v\mathfrak{X}(g)$$

2. *Sia V un FG-modulo. La funzione*

$$\begin{aligned} f : G &\longrightarrow \mathrm{GL}(V) \\ g \mapsto r_g : V &\longrightarrow V \\ v &\mapsto v{\cdot}g \end{aligned}$$

è un omomorfismo di gruppi. Scelta una base $B = [v_1, \dots, v_n]$ di V, definiamo la funzione

$$\begin{aligned} \mathfrak{X} : G &\longrightarrow \mathrm{GL}(n, F) \\ g &\mapsto M_B(f(g)) = M_B(r_g) \end{aligned}$$

dove $M_B(r_g)$ è la matrice associata dell'isomorfismo r_g, secondo la base B, ovvero

$$\underbrace{(M_B(r_g))_i}_{\text{riga } i-\text{esima}} = \underbrace{[r_g(v_i)]_B}_{\text{vettore delle componenti di } r_g(v_i) \text{ secondo } B} = [v_i{\cdot}g]_B$$

In altre parole,

$$v_i{\cdot}g = \sum_{j=1}^{n} x_{ij}(g)v_j \Rightarrow (\mathfrak{X}(g))_{ij} = x_{ij}(g)$$

Osservazione 2.42. Applicando in successione le due costruzioni esposte nella Proposizione 2.41 (usando la base canonica $B = \{e_1, \dots, e_n\}$), si riottiene il modulo o la rappresentazione di partenza.

Definizione 2.43. Siano $\mathfrak{X}, \mathfrak{Y} : G \longrightarrow \mathrm{GL}(n, F)$ due rappresentazioni. Diremo che $\mathfrak{X}, \mathfrak{Y}$ sono *simili* se:

$$\mathfrak{X} \sim \mathfrak{Y} \overset{\text{def}}{\Leftrightarrow} \exists M \in \mathrm{GL}(n, F) : \quad \mathfrak{X}(g) = M^{-1}\mathfrak{Y}(g)M = \mathfrak{Y}(g)^M \qquad \forall g \in G$$

Osservazione 2.44. Se $\mathfrak{X}$ è una rappresentazione, lo è anche $\mathfrak{X}(g)^M$, in quanto la coniugazione è un isomorfismo di gruppi.

Definizione 2.45. Sia $\mathfrak{X}$ una rappresentazione.

$$\mathfrak{X} \text{ è riducibile } \overset{\text{def}}{\Leftrightarrow} \exists M \in \mathrm{GL}(n, F) : \ \forall g \in G \ \mathfrak{X}(g) = M^{-1} \begin{bmatrix} X(g) & Y(g) \\ \underline{0} & Z(g) \end{bmatrix} M$$
$$\text{con } Z(g) \in F^{r\times r},\ X(g) \in F^{s\times s},\ Y(g) \in F^{s\times r}$$

ovvero

$$\mathfrak{X} \text{ è riducibile } \Leftrightarrow \mathfrak{X} \text{ è simile ad una matrice a blocchi del tipo } \begin{bmatrix} X & Y \\ \underline{0} & Z \end{bmatrix}$$

Proposizione 2.46. *Sia $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, F)$ una rappresentazione e $V = F^n$ il suo modulo indotto, allora*

$$\mathfrak{X} \textit{ irriducibile } \Leftrightarrow V \textit{ semplice}$$

Proposizione 2.47. *Sia V un FG-modulo, $U, W \overset{FG}{\leq} V$ e sia $\mathfrak{X}$ la rappresentazione indotta da V secondo la base canonica. Infine, sia $B_U = \{u_1, \ldots, u_s\}$ una base di U e $B_W = \{w_1, \ldots, w_r\}$ una base di W. Si ha*

$$V = W \oplus U \Rightarrow \mathfrak{X} \sim \begin{bmatrix} \underline{W} & \underline{0} \\ \underline{0} & \underline{U} \end{bmatrix}$$

dove $\underline{W}, \underline{U}$ sono rispettivamente le rappresentazioni indotte da W, U su B_W, B_U

Proposizione 2.48. *Siano V, W due FG-moduli e sia $f : V \longrightarrow W$ una applicazione lineare tra essi, allora*

$$f \textit{ è un } FG\textit{-omomorfismo } \Leftrightarrow \mathfrak{X}(g)M_{B,C}(f) = M_{B,C}(f)\mathfrak{Y}(g) \ \ \forall g \in G$$

dove $\mathfrak{X}, \mathfrak{Y}$ sono le rappresentazioni indotte dai moduli V, W secondo le basi $B = \{v_i\}_{i=1}^n$, $C = \{w_i\}_{i=1}^m$ e $M_{B,C}(f)$ è la matrice associata a f.

Proposizione 2.49. *Siano $\mathfrak{X}, \mathfrak{Y}$ due rappresentazioni di FG e siano V_1, V_2 i moduli indotti, allora*

$$V_1 \overset{FG}{\simeq} V_2 \Leftrightarrow \mathfrak{X} \sim \mathfrak{Y}$$

Ovvero, le rappresentazioni sono simili se e solo se i loro moduli indotti sono isomorfi.

Proposizione 2.50. *Sia G un gruppo finito.*

$$\begin{cases} \mathfrak{X} \text{ rappr. irriducibile} \\ \exists M \in F^{n\times n} : \quad M\mathfrak{X}(g) = \mathfrak{X}(g)M \ \ \forall g \in G \\ F \text{ alg. chiuso} \end{cases} \Rightarrow M = \lambda I, \quad \text{con } \lambda \in F$$

Proposizione 2.51. *Sia G un gruppo finito.*

$$\begin{cases} h \in Z(G) \\ \mathfrak{X} \text{ rappr. irriducibile} \\ F \text{ alg. chiuso} \end{cases} \Rightarrow \mathfrak{X}(h) = \lambda I, \ \text{con } \lambda \in F$$

Proposizione 2.52. *Sia G un gruppo finito.*

$$\begin{cases} G \text{ abeliano} \\ \mathfrak{X} \text{ rappr. irriducibile} \\ F \text{ alg. chiuso} \end{cases} \Rightarrow \dim \mathfrak{X} = n = 1, \ \text{ovvero } \mathfrak{X} : G \longrightarrow F^*$$

In questo caso, diremo che $\mathfrak{X}$ è lineare.

Osservazione 2.53. Da adesso in poi considereremo solo l'algebra $\mathbb{C}G$, così da assicurare la chiusura algebrica del campo e la condizione ch $\mathbb{C} \nmid |G|$

Enunciamo infine il teorema di Wedderburn per le rappresentazioni.

Teorema 2.54. *(Wedderburn). Siano $I_1, \dots, I_k$ i rappresentanti delle classi di isomorfismo dei $\mathbb{C}G$-moduli semplici e siano $\mathfrak{X}_1, \dots, \mathfrak{X}_k$ le relative rappresentazioni indotte. Allora,*

1. $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ *rappresentazione irriducibile* $\Rightarrow \exists! i : \ \mathfrak{X} \sim \mathfrak{X}_i$
2. $k = |\mathrm{cl}(G)|, \ \ |G| = n_1^2 + \cdots + n_k^2, \quad$ *con* $n_i = \dim I_i$
3. $\mathfrak{Y}$ *rappresentazione* $\Rightarrow \mathfrak{Y} \sim \mathrm{diag}(\mathfrak{X}_{i_1}, \dots, \mathfrak{X}_{i_r})$ *matrice diagonale a blocchi*
4. $\begin{cases} \mathfrak{X}_i(B_j) = 0 \ \ \forall j \neq i \\ \mathfrak{X}_i(B_i) = \mathbb{C}^{n_i \times n_i} \end{cases}$, *dove* $B_i = A(I_i)$
5. $1 = e_1 + \cdots + e_k, \ \ e_i \in B_i \Rightarrow \mathcal{X}_i(e_j) = \mathcal{X}_i(1)\delta_{ij}$

dove, $\mathcal{X}_i(x) = \mathrm{Tr}\mathfrak{X}_i(x)$, $\mathrm{Tr}M$ *è la traccia della matrice M e $\delta_{ij} = 1$ se $i = j$ ed è nullo altrimenti.*

3 Caratteri

Le algebre di gruppo e le rappresentazioni consentono di applicare tecniche della teoria degli anelli e dell'algebra lineare allo studio dei gruppi. L'idea fondamentale della teoria dei caratteri è quella di considerare solo una piccola parte delle informazioni che si possono ricavare dalle rappresentazioni. Tale parziale informazione, denominata *carattere*, è d'altra parte più facilmente gestibile. Quindi, i caratteri, pur essendo una versione ridotta delle rappresentazioni, si rivelano uno strumento indispensabile per lo studio dei gruppi finiti e permettono di dedurre risultati notevoli, come ad esempio il teorema di Burnside.

Nota: con G indicheremo sempre un gruppo finito.

Definizione 3.1. Sia $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ una rappresentazione. Sia definita la seguente funzione:

$$\begin{aligned} &\mathcal{X} : G \longrightarrow \mathbb{C} \\ &g \mapsto \mathrm{Tr}\mathfrak{X}(g) \end{aligned}$$

dove Tr è la traccia[6] della matrice $\mathfrak{X}(g)$. A volte, per indicare che $\mathcal{X}$ è la traccia di $\mathfrak{X}$ scriveremo

$$\mathcal{X} = \mathrm{Tr}\mathfrak{X}$$

Chiameremo $\mathcal{X}$ il *carattere* di $\mathfrak{X}$.

Notazione 3.2. Per indicare una matrice diagonale, utilizzeremo la seguente notazione:

$$\mathrm{diag}(a_{11}, \ldots, a_{nn}) \text{ è la matrice quadrata } (a_{ij}) = (a_{ii}\delta_{ij}), \text{ dove } \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

[6] La traccia della matrice M è l'elemento:

$$\mathrm{Tr}M = \sum_i M_{ii}$$

Proposizione 3.3. *Sia $\mathcal{X}$ una rappresentazione e siano A, B, M, X matrici quadrate, allora si ha*

1. $\mathrm{Tr}(AB) = \mathrm{Tr}(BA), \;\; \mathrm{Tr}(M^{-1}XM) = \mathrm{Tr}(X)$
2. $\mathfrak{X} \sim \mathfrak{Y} \Rightarrow \mathrm{Tr}\mathfrak{X} = \mathrm{Tr}\mathfrak{Y}$
3. $\mathcal{X}(1) = n = \dim \mathfrak{X}$

Dimostrazione:
1.

$$\mathrm{Tr}(M^{-1}XM) \underbrace{=}_{\mathrm{Tr}(AB)=\mathrm{Tr}(BA)} \mathrm{Tr}(M(M^{-1}X)) = \mathrm{Tr}(X)$$

2.

$$\mathfrak{X} \sim \mathfrak{Y} \Leftrightarrow \exists M : \; \mathfrak{X} = M^{-1}\mathfrak{Y}M \underbrace{\Rightarrow}_{1.} \mathrm{Tr}\mathfrak{X} = \mathrm{Tr}\mathfrak{Y}$$

3.

$$\mathcal{X}(1) = \mathrm{Tr}\mathfrak{X}(1) = \mathrm{Tr}I = n$$

□

Definizione 3.4. Sia G un gruppo finito.

$\mathcal{X}$ è un carattere di G $\overset{\text{def}}{\Leftrightarrow} \mathcal{X} \in \mathrm{ch}\, G \overset{\text{def}}{\Leftrightarrow} \exists \mathfrak{X}$ rappresentazione di G : $\mathcal{X} = \mathrm{Tr}\mathfrak{X}$

$\mathcal{X}$ è irriducibile $\overset{\text{def}}{\Leftrightarrow} \exists \mathfrak{X}$ rappresentazione irriducibile t.c. $\mathcal{X} = \mathrm{Tr}\mathfrak{X}$

ch G è l'insieme di tutti i caratteri di G

$\mathrm{Irr}(G)$ è l'insieme di tutti i caratteri irriducibili di G

Osservazione 3.5. Sia $\mathcal{X} : G \longrightarrow \mathbb{C}$ una carattere di G. Poiché $\mathrm{Tr} : \mathbb{C}^{n\times n} \longrightarrow \mathbb{C}$ è una applicazione lineare, possiamo estendere $\mathcal{X}$ per linearità su tutta l'algebra $\mathbb{C}G$:

$$\mathcal{X}\left(\sum_{g\in G} \lambda_g g\right) = \mathrm{Tr}\mathfrak{X}\left(\sum_{g\in G} \lambda_g g\right) = \mathrm{Tr}\left(\sum_{g\in G} \lambda_g \mathfrak{X}(g)\right) = \sum_{g\in G} \lambda_g \mathrm{Tr}\mathfrak{X}(g) = \sum_{g\in G} \lambda_g \mathcal{X}(g)$$

Lemma 3.6. *Siano date* $A, C \in F^{n\times n}$, $B, D \in F^{m\times m}$ *e definiamo la matrice a blocchi*

$$A \otimes B \stackrel{def}{=} \begin{bmatrix} a_{11}B & a_{12}B & \dots, & a_{1n}B \\ \vdots & & & \vdots \\ a_{n1}B & a_{n2}B & \dots, & a_{nn}B \end{bmatrix} \in F^{nm\times nm} ,$$

dove $a_{ij} = A_{ij}$ *è l'elemento di posto* i, j *di* A.
Si ha:

$$(A \otimes B)(C \otimes D) = AC \otimes BD$$

Dimostrazione:
Sia $\{e_{ij}\}_{1\le i,j\le n}$ la base canonica di $F^{n\times n}$

$A \otimes B = \sum_{i,j} a_{ij}(e_{ij} \otimes B) \in F^{nm\times nm}$ (1.1)

$C \otimes D = \sum_{i',j'} c_{i'j'}(e_{i'j'} \otimes D) \in F^{nm\times nm}$ (1.2)

$(e_{ij} \otimes B)(e_{i'j'} \otimes D) = \delta_{i'j}e_{ij'} \otimes BD$ (2)

$$(A \otimes B)(C \otimes D) \underbrace{=}_{(1.1),(1.2)} \sum_{i,j,i',j'} a_{ij}c_{i'j'}(e_{ij} \otimes B)(e_{i'j'} \otimes D) \underbrace{=}_{(2)} \sum_{i,j,i',j'} a_{ij}c_{i'j'}\delta_{i'j}e_{ij'} \otimes BD =$$

$$= \sum_{i,j,j'} a_{ij}c_{jj'}e_{ij'} \otimes BD = \sum_{i,j'} \left(\sum_j a_{ij}c_{jj'} \right) e_{ij'} \otimes BD = \sum_{i,j'} (AC)_{ij'}e_{ij'} \otimes BD = AC \otimes BD$$

□

Proposizione 3.7. *Siano* α *e* β *due caratteri; allora"*

$$\alpha + \beta, \quad \alpha\beta \in \text{ch } G$$

Dimostrazione:
1. $\alpha + \beta \in \text{ch } G$
   Siano $\mathfrak{X}, \mathfrak{Y}$ rappresentazioni tali che

$$\alpha = \text{Tr}\mathfrak{X}, \quad \beta = \text{Tr}\mathfrak{Y}.$$

   La matrice a blocchi

$$Z = \begin{bmatrix} \mathfrak{X} & \underline{0} \\ \underline{0} & \mathfrak{Y} \end{bmatrix}$$

   è una rappresentazione per $\alpha + \beta$. Infatti,

$$Z(ab) = \begin{bmatrix} \mathfrak{X}(ab) & \underline{0} \\ \underline{0} & \mathfrak{Y}(ab) \end{bmatrix} = \begin{bmatrix} \mathfrak{X}(a)\mathfrak{X}(b) & \underline{0} \\ \underline{0} & \mathfrak{Y}(a)\mathfrak{Y}(b) \end{bmatrix} = \begin{bmatrix} \mathfrak{X}(a) & \underline{0} \\ \underline{0} & \mathfrak{Y}(a) \end{bmatrix} \begin{bmatrix} \mathfrak{X}(b) & \underline{0} \\ \underline{0} & \mathfrak{Y}(b) \end{bmatrix} =$$
$$= Z(a)Z(b)$$

Infine,

$$\mathrm{Tr}Z = \mathrm{Tr}\mathfrak{X} + \mathrm{Tr}\mathfrak{Y} = \alpha + \beta \Rightarrow \alpha + \beta \in \mathrm{ch}\, G.$$

2. $\alpha\beta \in \mathrm{ch}\, G$

Sia $Z = \mathfrak{X} \otimes \mathfrak{Y}$. Z è una rappresentazione di G, infatti,

$$(\mathfrak{X} \otimes \mathfrak{Y})(ab) = \mathfrak{X}(ab) \otimes \mathfrak{Y}(ab) = (\mathfrak{X}(a)\mathfrak{X}(b)) \otimes (\mathfrak{Y}(a)\mathfrak{Y}(b)) =$$
$$\underbrace{=}_{\text{Lemma 3.6}} (\mathfrak{X}(a) \otimes \mathfrak{Y}(a))(\mathfrak{X}(b) \otimes \mathfrak{Y}(b)) = Z(a)Z(b)$$

Infine, dalla definizione di $\otimes$, è chiaro che

$$\mathrm{Tr}Z = (\mathrm{Tr}\mathfrak{X})(\mathrm{Tr}\mathfrak{Y}) = \alpha\beta$$

Quindi, $\alpha\beta \in \mathrm{ch}\, G$.

□

Teorema 3.8. *Sia G un gruppo finito; allora*

$$\mathrm{Irr}(G) = \{\mathcal{X}_1, \ldots, \mathcal{X}_k\}$$

dove i simboli $\mathcal{X}_i$ indicano i caratteri dati dal teorema di Wedderburn per le rappresentazioni (vedi Teorema 2.54), e $k = |\mathrm{cl}(G)|$

Dimostrazione: Per ipotesi sappiamo già che vale l'inclusione $\supseteq$. Dimostriamo l'inclusione opposta.

$\mathcal{X} \in \mathrm{Irr}(G) \Rightarrow \exists \mathfrak{X}$ rappr. irrid. di G : $\mathcal{X} = \mathrm{Tr}\mathfrak{X}$

$\mathfrak{X}$ irriducibile $\underbrace{\Rightarrow}_{\text{Teor. 2.54}} \exists! i : \ \mathfrak{X} \sim \mathfrak{X}_i \ \underbrace{\Rightarrow}_{\text{Prop. 3.3}} \ \mathrm{Tr}\mathfrak{X} = \mathrm{Tr}\mathfrak{X}_i \Rightarrow \mathcal{X} = \mathrm{Tr}\mathfrak{X}_i \Leftrightarrow \mathcal{X} = \mathcal{X}_i$

□

Definizione 3.9. Sia G un gruppo. Definiamo l'insieme delle *funzioni di classe*:

$$\mathrm{cf}(G) \overset{\text{def}}{=} \{f : G \longrightarrow \mathbb{C} \mid f(x^y) = f(x) \ \ \forall x, y \in G\}$$

O equivalentemente:

$$\mathrm{cf}(G) = \{f : G \longrightarrow \mathbb{C} \mid \ |f(\mathrm{cl}(x))| = 1 \ \forall x \in G\}$$

In altre parole, le funzioni di classe sono quelle funzioni costanti sulle classi di coniugio.

È facile notare che $\mathrm{cf}(G)$ è un $\mathbb{C}$-spazio vettoriale.

Proposizione 3.10. *I caratteri sono delle funzioni di classe, ovvero*

$$\text{ch }(G) \subseteq \text{cf}(G)$$

Dimostrazione: Sia $\mathcal{X} \in \text{ch }(G)$

$$\mathcal{X}(x^y) = \text{Tr}\mathfrak{X}(x^y) = \text{Tr}\left(\mathfrak{X}(y)^{-1}\mathfrak{X}(x)\mathfrak{X}(y)\right) \underbrace{=}_{\text{Proposizione 3.3}} \text{Tr}\mathfrak{X}(x) = \mathcal{X}(x)$$

□

Proposizione 3.11. *Sia* $\text{cl}(G) = \{K_1, \dots, K_k\}$, $k = |\text{cl}(G)|$. *Posto*

$$\delta_i : G \longrightarrow \mathbb{C}$$
$$\delta_i(s) = \begin{cases} 1 & s \in K_i \\ 0 & s \notin K_i \end{cases}$$

allora $\{\delta_1, \dots, \delta_k\}$ *è una base di* $\text{cf}(G)$.

Dimostrazione: È chiaro che $\delta_i \in \text{cf}(G)$.

1. Dimostriamo che $\text{cf}(G) = \langle \delta_1, \dots, \delta_k \rangle$

   Siano $x_1, \dots, x_k \in G$ t.c. $x_i \in K_i$.

   $$f \in \text{cf}(G), \quad x \in K_i \Rightarrow f(x) = f(x)\delta_i(x)$$
   $$x \in K_i \Rightarrow x \notin K_j, \text{ con } j \neq i \Rightarrow \delta_j(x) = 0$$
   $$\Rightarrow \forall x \in K_i \; f(x) = f(x)\delta_i(x) + \sum_{j \neq i} f(x)\delta_j(x) \quad (1)$$
   $$x \in K_i \Rightarrow f(x) = f(y) \;\; \forall y \in K_i \Rightarrow f(x) = f(x_i) \quad (2)$$

   Quindi

   $$x \in K_i \Rightarrow f(x) \underbrace{=}_{(1)} \sum_{i=1}^{k} f(x)\delta_i(x) \underbrace{=}_{(2)} \sum_{i=1}^{k} f(x_i)\delta_i(x)$$

   Poiché $\{K_i\}_i$ è una partizione di G, possiamo concludere che

   $$f = \sum_{i=1}^{k} f(x_i)\delta_i \in \langle \delta_1, \dots, \delta_k \rangle$$

2. $\delta_1, \dots, \delta_k$ sono linearmente indipendenti:

   sia

   $$a_1\delta_1 + \cdots + a_k\delta_k = 0$$

   una combinazione lineare nulla, scegliendo $x \in K_i$ si ha

   $$a_i = 0$$

□

Proposizione 3.12. *Sia G un gruppo finito.*

$$|\mathrm{Irr}(G)| = |\mathrm{cl}(G)|$$
$$\mathrm{Irr}(G) \text{ è una base di } \mathrm{cf}(G)$$

Dimostrazione: Sia $k = |\mathrm{cl}(G)|$. Per il Teorema 3.8 abbiamo $|\mathrm{Irr}(G)| = k$. Poiché

$$\dim \mathrm{cf}(G) \underbrace{=}_{\text{Proposizione 3.11}} k$$
$$\mathrm{Irr}(G) \subseteq \mathrm{ch}\ (G) \underbrace{\subseteq}_{\text{Proposizione 3.10}} \mathrm{cf}(G)$$

basta dimostrare che $\mathrm{Irr}(G) = \{\mathcal{X}_1, \dots, \mathcal{X}_k\}$ è un insieme di vettori linearmente indipendenti.
Per il Teorema 2.54 abbiamo

$$1 = e_1 + \cdots + e_k, \quad e_i = 1_{B_i}$$
$$\mathcal{X}_i(e_j) = \delta_{ij}\mathcal{X}_i(1) \quad (1)$$

Consideriamo una combinazione lineare nulla di $\mathcal{X}_1, \dots, \mathcal{X}_k$:

$$a_1\mathcal{X}_1 + \cdots + a_k\mathcal{X}_k = 0$$

e valutiamola in e_j:

$$0 = \sum_{i=1}^{k} a_i\mathcal{X}_i(e_j) = a_j\mathcal{X}_j(1) \underbrace{\Rightarrow}_{\mathcal{X}_j(1)=\dim B_i \neq 0} a_j = 0$$

Per l'arbitrarietà di j concludiamo che $a_j = 0 \ \ \forall j = 1, \dots, k$. □

Teorema 3.13. *Sia* $\mathrm{Irr}(G) = \{\mathcal{X}_1, \dots, \mathcal{X}_k\}$. *Si ha*

$$\mathcal{X} \in \mathrm{ch}\ G \Leftrightarrow \mathcal{X} = \sum_{i=1}^{k} m_i\mathcal{X}_i, \ \text{con } m_i \in \mathbb{N} \quad \forall i = 1, \dots, k$$

Inoltre, esiste i tale che $m_i > 0$. Quindi i caratteri sono tutte e sole quelle funzioni di classe che si possono scrivere come combinazione lineare intera degli elementi di $\mathrm{Irr}(G)$.

Dimostrazione:
1. ($\Leftarrow$)
   Per la Proposizione 3.7, la somma di caratteri è ancora un carattere. Poiché $\mathrm{Irr}(G) \subseteq \mathrm{ch}\ G$, la combinazione lineare intera $\sum_{i=1}^{k} m_i\mathcal{X}_i$ è ancora un carattere.

2. ($\Rightarrow$)

$$\mathcal{X} \in \text{ch } G \Rightarrow \mathcal{X} = \text{Tr}\mathfrak{X}$$

$$\mathfrak{X} \underbrace{\sim}_{\text{Teorema 2.54}} \text{diag}(\mathfrak{X}_{i_1}, \dots, \mathfrak{X}_{i_r}) \text{ matrice diagonale a blocchi } \Rightarrow$$

$$\Rightarrow \mathcal{X} = \text{Tr}\mathfrak{X} = \sum_{j=1}^{r} \text{Tr}\mathfrak{X}_{i_r} = \sum_{j=1}^{r} \mathcal{X}_{i_r} \underbrace{=}_{\text{per opportuni } m_i \in \mathbb{N}} \sum_{i=1}^{k} m_i \mathcal{X}_i$$

Infine,

$$\mathcal{X}(1) = \dim \mathfrak{X} \neq 0 \Rightarrow \mathcal{X} \neq 0 \Rightarrow \sum_{i=1}^{k} m_i \mathcal{X}_i \neq 0 \Rightarrow \exists j : \ m_j > 0$$

□

Definizione 3.14. Sia $\mathfrak{X} : G \longrightarrow \text{GL}(n, \mathbb{C})$ la rappresentazione indotta dal modulo $\mathbb{C}G^{\circ}$, secondo una qualsiasi base. Il carattere

$$\rho_G = \text{Tr}\mathfrak{X}$$

è detto il *carattere regolare* di G.

Proposizione 3.15. *Il carattere regolare di G soddisfa le seguenti proprietà*

1. $\rho_G = \sum_{\mathcal{X} \in \text{Irr}(G)} \mathcal{X}(1)\mathcal{X}$
2. $\rho_G(g) = \begin{cases} |G| & g = 1 \\ 0 & g \neq 1 \end{cases}$

In particolare, abbiamo

$$\rho_G(1) = \sum_{\mathcal{X} \in \text{Irr}(G)} \mathcal{X}(1)^2 = |G|$$

Dimostrazione:

1.

Per il Corollario 2.38 , si ha

$$\mathbb{C}G^{\circ} \simeq n_1 I_1 \oplus \cdots \oplus n_k I_k \underbrace{\Rightarrow}_{\text{Prop. 2.47}} \mathfrak{X} \sim \text{diag}(\underbrace{\mathfrak{X}_1, \dots, \mathfrak{X}_1}_{n_1 \text{ volte}}, \dots, \underbrace{\mathfrak{X}_k, \dots, \mathfrak{X}_k}_{n_k \text{ volte}}) \Rightarrow$$

$$\Rightarrow \mathcal{X} = \text{Tr}\mathfrak{X} = \sum_{i=1}^{k} n_i \text{Tr}\mathfrak{X}_i = \sum_{i=1}^{k} n_i \mathcal{X}_i \quad (2)$$

$$\mathcal{X}_i(1) \underbrace{=}_{\text{Teorema 2.54}} n_i \quad (3)$$

$$(2), (3) \Rightarrow \mathcal{X} = \sum_{i=1}^{k} \mathcal{X}_i(1)\mathcal{X}_i \underbrace{=}_{\text{Teorema 3.8}} \sum_{\mathcal{X} \in \text{Irr}(G)} \mathcal{X}(1)\mathcal{X}$$

2.

Scegliamo $G = \{g_1, \dots, g_n\}$ come base di $\mathbb{C}G^\circ$ da cui indurre $\mathfrak{X}$. La seguente dimostrazione sarà indipendente da questa scelta perché la traccia non cambia per matrici simili.

Sia $g_{i'} = g_i \cdot g$; si ha

$$g_i \cdot g = g_{i'} \in G \ \ \forall g \in G \Rightarrow [g_i \cdot g]_G = e_{i'}(g) \text{ per qualche } 1 \leq i' \leq n$$

$$\text{dove } e_{i'}(g) = (0, 0, \dots, 0, \underbrace{1}_{\text{posto } i'}, 0, 0, \dots, 0)$$

$$e_{i'}(g) = e_{h'}(g) \Leftrightarrow [g_i \cdot g]_G = [g_h \cdot g]_G \Leftrightarrow g_i \cdot g = g_h \cdot g \Leftrightarrow g_i = g_h \Leftrightarrow h = i$$

$$\mathfrak{X}(g) = M_G(r_g) = \begin{bmatrix} [g_1 \cdot g]_G \\ \vdots \\ [g_n \cdot g]_G \end{bmatrix} = \begin{bmatrix} e_{1'}(g) \\ \vdots \\ e_{n'}(g) \end{bmatrix}$$

Quindi $\mathfrak{X}(g)$ è una matrice di permutazione. Inoltre,

$$\mathfrak{X}(g)_{ii} = ([g_i \cdot g]_G)_i = (e_{i'}(g))_i = \delta_{ii'} = \begin{cases} 1 & i = i' \Leftrightarrow g_i = g_{i'} = g_i g \Leftrightarrow g = 1 \\ 0 & \text{altrimenti} \end{cases} \quad (1)$$

$$\mathcal{X}(g) = \mathrm{Tr}\mathfrak{X}(g) = \sum_{i=1}^{n} \mathfrak{X}(g)_{ii} \underbrace{=}_{(1)} \begin{cases} 1 + 1 + \cdots + 1 = |G| & g = 1 \\ 0 & \text{altrimenti} \end{cases}$$

□

Il seguente teorema è il primo risultato che permette di ricavare informazioni sul gruppo G esaminando solo i caratteri irriducibili.

Teorema 3.16.

$$G \text{ è abeliano } \Leftrightarrow \mathcal{X}(1) = 1 \ \ \forall \mathcal{X} \in \mathrm{Irr}(G)$$

Dimostrazione:

$$G \text{ abeliano } \Leftrightarrow |\mathrm{cl}(g)| = 1 \ \forall g \in G \underbrace{\Leftrightarrow}_{\mathrm{cl}(G) \text{ è una partizione di } G} |\mathrm{cl}(G)| = |G|$$

$$|\mathrm{Irr}(G)| \underbrace{=}_{\text{Teorema 3.8}} |\mathrm{cl}(G)| = |G|$$

$$\rho_G(1) \underbrace{=}_{\text{Prop. 3.15}} \sum_{\mathcal{X} \in \mathrm{Irr}(G)} \mathcal{X}(1)^2 = |G| = |\mathrm{Irr}(G)| \underbrace{\Leftrightarrow}_{\mathcal{X}(1) \in \mathbb{N},\, \mathcal{X}(1) \neq 0} \mathcal{X}(1) = 1 \ \ \forall \mathcal{X} \in \mathrm{Irr}(G)$$

□

Teorema 3.17. *Sia* $\mathcal{X} \in \text{ch } G$

$$\mathcal{X} \in \text{Irr}(G) \Leftrightarrow \mathcal{X} \neq \alpha + \beta \ \ \forall \alpha, \beta \in \text{ch } G$$

Dimostrazione:

1. ($\Rightarrow$)

   Supponiamo per assurdo $\mathcal{X} = \alpha + \beta$,

   $$\alpha, \beta \in \text{ch } G \Rightarrow \mathcal{X} = \alpha + \beta \in \text{ch } G$$

   $$\alpha \in \text{ch } G \underbrace{\Rightarrow}_{\text{Teorema 3.13}} \alpha = \sum_{\mathcal{Y} \in \text{Irr}(G)} m_{\mathcal{Y}} \mathcal{Y}, \text{ con almeno un } m_{\mathcal{Y}} \in \mathbb{N}^* \quad (1)$$

   Analogamente per β:

   $$\beta \in \text{ch } G \underbrace{\Rightarrow}_{\text{Teorema 3.13}} \beta = \sum_{\mathcal{Y} \in \text{Irr}(G)} m'_{\mathcal{Y}} \mathcal{Y}, \text{ con almeno un } m'_{\mathcal{Y}} \in \mathbb{N}^* \quad (2)$$

   Quindi,

   $$\mathcal{X} = \alpha + \beta = \sum_{\mathcal{Y} \in \text{Irr}(G)} (m_{\mathcal{Y}} + m'_{\mathcal{Y}}) \mathcal{Y}$$

   Sia $a_{\mathcal{Y}} = m_{\mathcal{Y}} + m'_{\mathcal{Y}}$. Per la (1) e (2), i casi sono due: almeno due $a_{\mathcal{Y}}$ sono distinti da zero, o almeno un $a_{\mathcal{Y}} \geq 2$. In ogni caso, poiché $\mathcal{X} \in \text{Irr}(G)$, si ha un assurdo contro l'indipendenza lineare degli elementi di $\text{Irr}(G)$ (vedi 3.12).

2. ($\Leftarrow$)

   Supponiamo per assurdo che $\mathcal{X} \notin \text{Irr}(G)$

   $$\mathcal{X} \in \text{ch } G \Rightarrow \mathcal{X} = \sum_{\mathcal{Y} \in \text{Irr}(G)} m_{\mathcal{Y}} \mathcal{Y}, \text{ con almeno un } m_{\mathcal{Y}} \in \mathbb{N}^*$$

   $$\mathcal{X} \notin \text{Irr}(G) \Rightarrow \mathcal{X} \neq \mathcal{Y} \ \ \forall \mathcal{Y} \in \text{Irr}(G)$$

   Poiché $\mathcal{X}$ non deve coincidere con alcun $\mathcal{Y}$, deve esistere almeno un $m_{\mathcal{Y}} \geq 2$ oppure due $m_{\mathcal{Y}}, m_{\mathcal{Y}'} \neq 0$. Quindi $\mathcal{X}$ è somma di almeno due caratteri. Assurdo. □

Teorema 3.18. *Siano $\mathfrak{X}, \mathfrak{Y}$ due rappresentazioni di G e $\mathcal{X}, \mathcal{Y}$ i rispettivi caratteri. Si ha:*

$$\mathfrak{X} \sim \mathfrak{Y} \Leftrightarrow \mathcal{X} = \mathcal{Y}$$

Dimostrazione:

1. ($\Rightarrow$)
   Segue immediatamente dalla Proposizione 3.3
2. ($\Leftarrow$)
   Procediamo analogamente a quanto abbiamo fatto nella dimostrazione del Teorema 3.13.

$$\mathfrak{X} \underbrace{\sim}_{\text{Teorema 2.54}} \underbrace{\operatorname{diag}(\mathfrak{X}_{i_1}, \dots, \mathfrak{X}_{i_r})}_{\text{matrice diagonale a blocchi}} \underbrace{\sim}_{\text{riordinando i blocchi}} \operatorname{diag}(\underbrace{\mathfrak{X}_1, \dots, \mathfrak{X}_1}_{d_1 \text{ volte}}, \dots, \underbrace{\mathfrak{X}_k, \dots, \mathfrak{X}_k}_{d_k \text{ volte}}) \quad (1)$$

   (qualche d_i potrebbe essere nullo). Ne segue che:

$$\mathcal{X} = \operatorname{Tr}\mathfrak{X} = \sum_{i=1}^{k} d_i \mathcal{X}_i$$

   Analogamente abbiamo:

$$\mathfrak{Y} \sim \operatorname{diag}(\underbrace{\mathfrak{X}_1, \dots, \mathfrak{X}_1}_{d_1' \text{ volte}}, \dots, \underbrace{\mathfrak{X}_k, \dots, \mathfrak{X}_k}_{d_k' \text{ volte}}) \quad (2)$$

$$\mathcal{Y} = \operatorname{Tr}\mathfrak{Y} = \sum_{i=1}^{k} d_i' \mathcal{X}_i$$

$$\begin{cases} \mathcal{X} = \mathcal{Y} \text{ per ipotesi} \\ \{\mathcal{X}_1, \dots, \mathcal{X}_k\} \text{ sono linearmente indipendenti} \end{cases} \Rightarrow d_i = d_i' \ \ \forall i = 1, \dots, k$$

$$\Rightarrow \mathfrak{X} \underbrace{\sim}_{(1)} \operatorname{diag}(\underbrace{\mathfrak{X}_1, \dots, \mathfrak{X}_1}_{d_1 \text{ volte}}, \dots, \underbrace{\mathfrak{X}_k, \dots, \mathfrak{X}_k}_{d_k \text{ volte}}) \underbrace{\sim}_{(2)} \mathfrak{Y}$$

□

Proposizione 3.19. *Sia $g \in G$ e $\mathfrak{X}$ una rappresentazione di G. Sia $o(g) = m$ l'ordine di g. Si ha*

1. $\mathfrak{X}(g) \sim \mathrm{diag}(\xi_1, \dots, \xi_n), \quad n = \mathcal{X}(1), \quad \xi_i \in \mathbb{C} \ \ \forall i = 1, \dots, n$
2. $\mathcal{X}(g) = \sum_{i=1}^{n} \xi_i$
3. $\xi_i^m = 1 \ \ \forall i = 1, \dots, n$
4. $|\mathcal{X}(g)| \leq \mathcal{X}(1)$
5. $\mathcal{X}(g^{-1}) = \overline{\mathcal{X}(g)}$ *dove $\overline{\xi}$ è il coniugato complesso di ξ*

Dimostrazione:
1. e 2.
Sia $H = \langle g \rangle$ il gruppo generato da g e sia $\mathfrak{Y} = \mathfrak{X}_{|H}$.

$$H \text{ abeliano} \underbrace{\Leftrightarrow}_{\text{Teorema 3.16}} \mathcal{Y}_1(1) = \dots = \mathcal{Y}_k(1) = 1 \Rightarrow \mathcal{Y}_i(h) \in \mathbb{C} \ \ \forall h \in H \quad (1)$$

dove $\mathrm{Irr}(H) = \{\mathcal{Y}_1, \dots, \mathcal{Y}_k\}$

$$\mathfrak{Y} \underbrace{\sim}_{\text{Teorema 2.54}} \underbrace{\mathrm{diag}(\mathfrak{Y}_{i_1}, \dots, \mathfrak{Y}_{i_n})}_{\text{matrice diagonale a blocchi}}$$

con $n = \dim \mathcal{Y} = \mathcal{Y}(1) = \mathcal{X}(1), \quad 1 \leq i_j \leq k \quad$ per ogni j

Poniamo $\xi_j = \mathfrak{Y}_{i_j}(g)$. Per la (1), la matrice diagonale a blocchi, simile a $\mathfrak{Y}$, è una semplice matrice quadrata, quindi

$$\mathfrak{X}(g) = \mathfrak{Y}(g) \sim \mathrm{diag}(\xi_1, \dots, \xi_n)$$
$$\mathcal{X}(g) = \mathrm{Tr}\mathfrak{X}(g) = \sum_{j=1}^{n} \xi_j$$

3.

$$m = o(g) \Rightarrow g^m = 1 \Leftrightarrow 1 = \mathfrak{Y}_{i_j}(g^m) = \mathfrak{Y}_{i_j}(g)^m \Leftrightarrow \xi_j^m = 1$$

4.

$$\xi_j^m = 1 \Rightarrow |\xi_j|^m = 1 \Rightarrow |\xi_j| = 1 \quad (2)$$
$$|\mathcal{X}(g)| = \Big| \sum_{j=1}^{n} \xi_j \Big| \leq \sum_{j=1}^{n} |\xi_j| \underbrace{=}_{(2)} n = \mathcal{X}(1)$$

5.

$$\xi_j\overline{\xi_j} = |\xi_j|^2 \underbrace{=}_{(2)} 1 \Rightarrow \overline{\xi_j} = {\xi_j}^{-1} \quad (3)$$

$$\overline{X(g)} = \sum_{j=1}^{n} \overline{\xi_j} = \sum_{j=1}^{n} {\xi_j}^{-1} = \sum_{j=1}^{n} \mathfrak{Y}_{i_j}(g)^{-1} = \sum_{j=1}^{n} \mathfrak{Y}_{i_j}(g^{-1}) = \mathfrak{Y}(g^{-1}) = \mathfrak{X}(g^{-1})$$

□

Proposizione 3.20. *Sia $\mathcal{X} \in \text{ch } G$. Poniamo:*

$$\begin{aligned} \overline{\mathcal{X}} : G &\longrightarrow \mathbb{C} \\ g &\mapsto \overline{\mathcal{X}}(g) \end{aligned}$$

dove $\overline{\xi}$ è il coniugato complesso di ξ.
Si ha:

1. $\overline{\mathcal{X}} \in \text{ch } G$
2. $\mathcal{X} \in \text{Irr}(G) \Leftrightarrow \overline{\mathcal{X}} \in \text{Irr}(G)$
3. $\overline{\mathcal{X}}(g) = \text{Tr}\mathfrak{X}(g^{-1})^{\tau}$

dove A^{τ} è la trasposta della matrice A.

Dimostrazione: Sia

$$\begin{aligned} \mathfrak{Y} : G &\longrightarrow \text{GL}(n, \mathbb{C}) \\ g &\mapsto \mathfrak{X}(g^{-1})^{\tau} \end{aligned}$$

$\mathfrak{Y}$ è una rappresentazione, quindi:

$$\mathfrak{Y}(ab) = \mathfrak{X}((ab)^{-1})^{\tau} = \left(\mathfrak{X}(b^{-1})\mathfrak{X}(a^{-1})\right)^{\tau} = \mathfrak{X}(a^{-1})^{\tau}\mathfrak{X}(b^{-1})^{\tau} = \mathfrak{Y}(a)\mathfrak{Y}(b)$$

Inoltre,

$$\text{Tr}\mathfrak{Y}(g) = \text{Tr}\mathfrak{X}(g^{-1})^{\tau} = \text{Tr}\mathfrak{X}(g^{-1}) = \mathcal{X}(g^{-1}) \underbrace{=}_{\text{Proposizione 3.19}} \overline{\mathcal{X}(g)} = \overline{\mathcal{X}}(g)$$

Quindi $\overline{\mathcal{X}} \in \text{ch } G$. Infine,
$\mathcal{X}$ riducibile $\underbrace{\Leftrightarrow}_{\text{Teorema 3.17}}$ $\mathcal{X} = \alpha + \beta$, con $\alpha, \beta \in \text{ch } G \Leftrightarrow \overline{\mathcal{X}} = \underbrace{\overline{\alpha}}_{\in \text{ch } G} + \underbrace{\overline{\beta}}_{\in \text{ch } G}$, $\Leftrightarrow$

$\underbrace{\Leftrightarrow}_{\text{Teorema 3.17}}$ $\overline{\mathcal{X}}$ riducibile

□

Lemma 3.21. *Siano $\alpha, \beta \in \mathbb{C}$. Si ha:*

$$|\alpha+\beta| = |\alpha| + |\beta| \Rightarrow \alpha = \lambda\beta \quad \textit{con } \lambda \in \mathbb{R}$$

Dimostrazione: Indichiamo con $\alpha{\cdot}\beta$ il prodotto Hermitiano in $\mathbb{C}$. Si hanno le seguenti implicazioni:
$|\alpha+\beta| = |\alpha| + |\beta| \Rightarrow |\alpha+\beta|^2 = |\alpha|^2 + |\beta|^2 + 2|\alpha||\beta|$ (1)
$|\alpha+\beta|^2 = (\alpha+\beta)\overline{(\alpha+\beta)} = \alpha\overline{\alpha} + \alpha\overline{\beta} + \beta\overline{\alpha} + \beta\overline{\beta} = |\alpha|^2 + |\beta|^2 + 2\alpha\overline{\beta}$
$\underbrace{\Rightarrow}_{(1)} |\alpha||\beta| = \alpha\overline{\beta} = \alpha{\cdot}\beta \Rightarrow (\alpha{\cdot}\beta)^2 = (|\alpha||\beta|)^2 = \sqrt{(\alpha{\cdot}\alpha)}^2\sqrt{(\beta{\cdot}\beta)}^2 = (\alpha{\cdot}\alpha)(\beta{\cdot}\beta) \Leftrightarrow$
$\Leftrightarrow (\alpha{\cdot}\beta)^2 = (\alpha{\cdot}\alpha)(\beta{\cdot}\beta) \quad \underbrace{\Rightarrow}_{\text{Disug. di Schwartz}} \quad \alpha \parallel \beta \Leftrightarrow \exists\lambda \in \mathbb{R} : \ \alpha = \lambda\beta$
(dove $\alpha \parallel \beta$ indica che α, β sono due vettori paralleli). □

Lemma 3.22. *$\alpha_1, \ldots, \alpha_t \in \mathbb{C}$, $t \geq 1$*

$$\begin{cases} |\alpha_i| = 1 \ \ \forall i = 1, \ldots, t \\ |\alpha_1 + \cdots + \alpha_t| = t \end{cases} \Rightarrow \alpha_i = \alpha_1 \ \ \forall i = 1, \ldots, t$$

Dimostrazione: Procediamo per induzione su t.
Caso: $t = 1$
Vera.
Caso: $t = 2$

$$|\alpha+\beta| = 2 = |\alpha| + |\beta| \quad \underbrace{\Rightarrow}_{\text{Lemma 3.21}} \quad \exists l \in \mathbb{R} : \ \alpha = l\beta$$
$$|l\beta+\beta| = 2 \Leftrightarrow \underbrace{|\beta|}_{=1}|l+1| = 2 \Leftrightarrow l+1 = \pm 2 \Leftrightarrow l = 1 \vee l = -3 \ \ (1)$$
$$\alpha = l\beta \Rightarrow \underbrace{|\alpha|}_{=1} = |l| \underbrace{|\beta|}_{=1} \Leftrightarrow |l| = 1 \Rightarrow l = \pm 1 \ \ (2)$$
$$(1), (2) \Rightarrow l = 1 \Rightarrow \alpha = \beta$$

Caso: $t \Rightarrow t+1$

$$t+1 = |\alpha_1 + \cdots + \alpha_t + \alpha_{t+1}| \leq |\alpha_1 + \cdots + \alpha_t| + |\alpha_{t+1}| \leq |\alpha_1| + \cdots + |\alpha_{t+1}| =$$
$$\underbrace{=}_{|\alpha_i|=1} t+1 \Rightarrow |\alpha_1 + \cdots + \alpha_t + \alpha_{t+1}| = |\alpha_1 + \cdots + \alpha_t| + \underbrace{|\alpha_{t+1}|}_{=1} = t+1 \Rightarrow$$
$$\Rightarrow |\alpha_1 + \cdots + \alpha_t| = t \quad \underbrace{\Rightarrow}_{\text{Hp induttiva}} \quad \alpha_1 = \alpha_2 = \cdots = \alpha_t$$

Analogamente si vede che
$|\alpha_1 + \cdots + \alpha_t + \alpha_{t+1}| = |\alpha_2 + \cdots + \alpha_t + \alpha_{t+1}| + |\alpha_1| \Rightarrow \alpha_2 = \alpha_3 = \cdots = \alpha_{t+1}$
In definitiva, poiché $t \geq 3$,

$$\alpha_1 = \alpha_2 = \cdots = \alpha_{t+1}$$

□

Definizione 3.23. Sia $\mathcal{X} \in \operatorname{ch} G$. Definiamo il *nucleo* e il *centro* di $\mathcal{X}$ nel seguente modo:

$$\ker \mathcal{X} \overset{\text{def}}{=} \ker \mathfrak{X}$$
$$Z(\mathcal{X}) \overset{\text{def}}{=} \{g \in G \mid \exists \lambda_g \in \mathbb{C} : \ \mathfrak{X}(g) = \lambda_g I\}$$

Nota: la definizione di $\ker \mathcal{X}$ è , come vedremo, indipendente dalla particolare scelta di $\mathfrak{X}$.

Teorema 3.24. *Sia* $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ *una rappresentazione. Valgono le seguenti proposizioni:*

1. $\ker \mathfrak{X} = \{g \in G \mid \mathcal{X}(g) = \mathcal{X}(1)\}$
2. $Z(\mathcal{X}) \underbrace{\trianglelefteq}_{\textit{sottogruppo normale}} G$
3. $Z(\mathcal{X}) = \{g \in G \mid \exists \lambda_g \in U_m : \ \mathfrak{X}(g) = \lambda_g I, \ \ \textit{con } m = o(g)\}$,
   dove U_m *è il gruppo delle radici* m*-esime dell'unità*
4. $Z(\mathcal{X}) = \{g \in G \mid |\mathcal{X}(g)| = |\mathcal{X}(1)|\}$

Dimostrazione:
1. Proviamo la doppia inclusione
   1.1. $(\subseteq)$

$$g \in \ker \mathfrak{X} \Rightarrow \mathfrak{X}(g) = I \Rightarrow \mathcal{X}(g) = \mathcal{X}(1) \Rightarrow g \in \{g \in G \mid \mathcal{X}(g) = \mathcal{X}(1)\}$$

   1.2. $(\supseteq)$
   Sia $g \in \{g \in G \mid \mathcal{X}(g) = \mathcal{X}(1)\}$,

$$\mathcal{X}(g) \underbrace{=}_{\text{Proposizione 3.19}} \xi_1 + \cdots + \xi_n = \mathcal{X}(1) = n$$

   dove $\xi_i \in U_{o(g)}, \ \ |\xi_i| = 1$

$$\underbrace{\Rightarrow}_{\text{Lemma 3.22}} \ \xi_i = \xi_1 \ \ \forall i = 1, \ldots, n \Rightarrow \mathcal{X}(g) = n\xi_1 = \mathcal{X}(1)\xi_1$$

   $n = \mathcal{X}(1) = \mathcal{X}(g) = \mathcal{X}(1)\xi_1 = n\xi_1 \Rightarrow \xi_1 = 1 \Rightarrow \xi_i = 1 \ \ \forall i$

$$\mathfrak{X}(g) \underbrace{\sim}_{\text{Prop. 3.19}} \operatorname{diag}(\xi_1, \ldots, \xi_n) = \operatorname{diag}(1, \ldots, 1) = I \Rightarrow \mathfrak{X}(g) = I \Rightarrow g \in \ker \mathfrak{X}$$

2.

2.1. $Z(\mathcal{X}) \leq G$ sottogruppo

Siano $a, b \in Z(\mathcal{X})$

$$\mathfrak{X}(ab) = \mathfrak{X}(a)\mathfrak{X}(b) = \lambda_a \lambda_b I \Rightarrow ab \in Z(\mathcal{X})$$

E poiché G è finito, questo basta per dimostrare che $Z(\mathcal{X}) \leq G$.

2.2. $Z(\mathcal{X}) \trianglelefteq G$

Sia $g \in Z(\mathcal{X}),\ h \in G$

$\mathfrak{X}(h^{-1}gh) = \mathfrak{X}(h)^{-1}\mathfrak{X}(g)\mathfrak{X}(h) = \mathfrak{X}(h)^{-1}\lambda_g I \mathfrak{X}(h) = \mathfrak{X}(h)^{-1}\mathfrak{X}(h)\lambda_g I = \lambda_g I \Rightarrow$

$\Rightarrow h^{-1}gh \in Z(\mathcal{X})$

3.

3.1. ($\subseteq$)

Sia $g \in Z(\mathcal{X})$ e $m = o(g)$

$$I = \mathfrak{X}(1) \underbrace{=}_{g^m=1} \mathfrak{X}(g^m) = \mathfrak{X}(g)^m \underbrace{=}_{g \in Z(\mathcal{X})} \lambda_g^m I \Leftrightarrow \lambda_g^m I = I \Leftrightarrow \lambda_g^m = 1 \Rightarrow \lambda_g \in U_m$$

3.2. ($\supseteq$)

Basta rileggere la definizione dei due insiemi.

4.

4.1. ($\subseteq$)

$$g \in Z(\mathcal{X}) \underbrace{\Rightarrow}_{3.} \mathfrak{X}(g) = \lambda_g I, \quad \lambda_g \in U_m \Rightarrow \mathcal{X}(g) = \lambda_g n \Rightarrow |\mathcal{X}(g)| = \underbrace{|\lambda_g|}_{=1} n = n =$$

$$= \mathcal{X}(1) = |\mathcal{X}(1)|$$

4.2. ($\supseteq$)

Sia $g \in G$ tale che $|\mathcal{X}(g)| = |\mathcal{X}(1)|$

$$\mathcal{X}(g) \underbrace{=}_{\text{Proposizione 3.19}} \xi_1 + \cdots + \xi_n, \quad \text{con } n = \mathcal{X}(1)$$

$$|\mathcal{X}(g)| = |\mathcal{X}(1)| = n$$

$$\Rightarrow |\xi_1 + \cdots + \xi_m| = n \underbrace{\Rightarrow}_{\text{Lemma 3.22}} \xi_i = \xi_1 \ \ \forall i = 1, \ldots, n$$

$$\mathfrak{X}(g) \underbrace{\sim}_{\text{Proposizione 3.19}} \operatorname{diag}(\xi_1, \ldots, \xi_n) = \operatorname{diag}(\xi_1, \ldots, \xi_1) = \xi_1 I$$

$$\mathfrak{X}(g) \sim \xi_1 I \Leftrightarrow \mathfrak{X}(g) = M^{-1}\xi_1 I M = \xi_1 I \Rightarrow g \in Z(\mathcal{X})$$

□

Proposizione 3.25. *La funzione*

$$\lambda : Z(\mathcal{X}) \longrightarrow \mathbb{C}^*$$
$$g \mapsto \frac{\mathcal{X}(g)}{\mathcal{X}(1)}$$

è un omomorfismo di gruppi. Inoltre, si ha:

$$\ker \lambda = \ker \mathcal{X}$$

Dimostrazione: Si ha:

$$g \in Z(\mathcal{X}) \underbrace{\Rightarrow}_{\text{Teorema 3.24}} \mathfrak{X}(g) = \lambda_g I \Rightarrow \mathcal{X}(g) = \lambda_g \mathcal{X}(1) \underbrace{\Rightarrow}_{\mathcal{X}(1)\neq 0} \lambda_g = \frac{\mathcal{X}(g)}{\mathcal{X}(1)} = \lambda(g)$$

Quindi $\lambda(g) = \lambda_g$ per ogni $g \in Z(\mathcal{X})$. In conclusione, otteniamo,

$$\mathfrak{X}(ab) = \mathfrak{X}(a)\mathfrak{X}(b) = \lambda_a I \lambda_b I = \lambda_a \lambda_b I \Rightarrow \mathcal{X}(ab) = \lambda_a \lambda_b \mathcal{X}(1) \Rightarrow \lambda_a \lambda_b = \frac{\mathcal{X}(ab)}{\mathcal{X}(1)} = \lambda_{ab}$$

□

Proposizione 3.26.

$$\begin{cases} G \text{ non abeliano, semplice} \\ \mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\} \end{cases} \Rightarrow Z(\mathcal{X}) = \{1\}$$

dove 1_G è il carattere irriducibile banale:

$$1_G(g) = 1 \ \ \forall g \in G$$

Dimostrazione: Se per assurdo $\ker \mathcal{X} = G$, si avrebbe

$$\forall g \in G \mathcal{X}(g) = \mathcal{X}(1) = n = n1_G(g) \Rightarrow \begin{cases} \mathcal{X} \text{ riducibile} & n > 1 \\ \mathcal{X} = 1_G & n = 1 \end{cases}$$

In ogni caso abbiamo un assurdo. Ne segue che

$$\begin{cases} \ker \mathcal{X} \trianglelefteq G \\ \ker \mathcal{X} \neq G \\ G \text{ semplice} \end{cases} \Rightarrow \ker \mathcal{X} = 1 \underbrace{\Leftrightarrow}_{\text{Proposizione 3.25}} \ker \lambda = 1$$

$$Z(\mathcal{X}) \trianglelefteq G \Rightarrow Z(\mathcal{X}) = 1 \vee Z(\mathcal{X}) = G$$

Supponiamo per assurdo che $Z(\mathcal{X}) = G$, allora

$$\ker \lambda = 1 \Rightarrow G = Z(\mathcal{X}) \simeq H \leq \mathbb{C}^* \Rightarrow G \text{ abeliano}$$

Assurdo. □

4 Interi algebrici

Un passo decisivo della dimostrazione del teorema di Burnside si compie considerando le proprietà che scaturiscono dal considerare i caratteri come dei particolari *interi algebrici*. In questo capitolo daremo le definizioni di base e quelle proprietà di cui faremo uso per lo studio dei caratteri e che applicheremo immediatamente nel Teorema 4.11. Per ulteriori approfondimenti si rimanda a [3].

Definizione 4.1. Sia $\alpha \in \mathbb{C}$; diremo che

$$\alpha \text{ è un } \textit{intero algebrico} \Leftrightarrow \exists f(x) \in \mathbb{Z}[x] \quad \text{monico:} \quad f(\alpha) = 0$$

Proposizione 4.2. *Sia R l'insieme di tutti gli interi algebrici. Si ha:*

$$R \cap \mathbb{Q} = \mathbb{Z}$$

Dimostrazione:

1. $(\supseteq)$
   Sia $z \in \mathbb{Z}$. z è radice del polinomio $x - z$. Poiché $\mathbb{Z} \subseteq \mathbb{Q}$, si ha la tesi.
2. $(\subseteq)$
   Sia $\alpha \in \mathbb{Q},\ f(x) \in \mathbb{Z}[x],\ f(\alpha) = 0$:
   $$\alpha \in \mathbb{Q} \Rightarrow \alpha = \frac{r}{s}, \quad (r,s) = 1$$
   $$f(\alpha) = 0 \Leftrightarrow \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_0 = 0 \Leftrightarrow$$
   $$\Leftrightarrow r^n + a_{n-1}r^{n-1}s + a_{n-2}r^{n-2}s^2 + \cdots + a_0 s^n = 0 \Leftrightarrow r^n = s\mu \Leftrightarrow s \Big/ r^n \quad (1)$$
   Sia p un primo tale che $p \Big/ s$; dalla (1) segue che $p \Big/ r$. Per l'arbitrarietà di p si ha $s \Big/ r$ e dunque, poiché $(r,s) = 1$, si ottiene $s = \pm 1$, cioè $\alpha = \pm r \in \mathbb{Z}$.

□

Definizione 4.3. Sia S un anello tale che $\mathbb{Z} \subseteq S$

$$S \text{ è } \textit{finitamente generato} \text{ come } \mathbb{Z}\text{-modulo} \overset{\text{def}}{\Leftrightarrow} \exists Y \subseteq S : \quad S = \langle Y \rangle_{\mathbb{Z}}, \quad |Y| < \infty,$$

ovvero, esiste un insieme finito $Y = \{y_1, \ldots, y_k\} \subseteq S$ tale che

$$\forall s \in S \ \ \exists z_1, \ldots, z_k \in \mathbb{Z} : \quad s = z_1 y_1 + \cdots + z_k y_k$$

Lemma 4.4. *Sia* $Y = \{\alpha_1, \ldots, \alpha_t\} \subseteq R$, *allora*

$$\exists S \text{ anello: } \mathbb{Z} \subseteq S \subseteq \mathbb{C},\ Y \subseteq S,\ \ S \text{ finitamente generato come } \mathbb{Z}\text{-modulo}$$

Dimostrazione:
$\alpha_i \in R \Rightarrow \exists f_i \in \mathbb{Z}[x],\ \exists n_i \in \mathbb{N} :\ \ \alpha_i^{n_i} = f(\alpha_i) = a_0 + a_1\alpha_i + \cdots + a_{n_i-1}\alpha_i^{n_i-1} \Rightarrow$
$\Rightarrow \alpha_i^{n_i} \in \langle Z \rangle_{\mathbb{Z}}$ (1)
dove abbiamo posto $Z = \left\{1, \alpha_i, \ldots, \alpha_i^{n_i-1}\right\}$
$\alpha_i^{n_i+1} = \alpha_i f(\alpha_i) = a_0\alpha_i + a_1\alpha_i^2 + a_2\alpha_i^3 + \cdots + \underbrace{a_{n_i-1}\alpha_i^{n_i}}_{\in \langle Z \rangle_{\mathbb{Z}}} \in \langle Z \rangle_{\mathbb{Z}}$

Per induzione si vede facilmente che vale lo stesso per le potenze α_i^m, con $m \geq n_i$. Sia

$$X = \{\alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdots \alpha_t^{m_t} \mid 0 \leq m_i \leq n_i - 1\ \ \forall i = 1, \ldots, t\}$$
$$S = \langle X \rangle_{\mathbb{Z}}$$

Poiché $S \subseteq \mathbb{C}$, per dimostrare che S è un anello, basta vedere che $a, b \in S \Rightarrow ab \in S$, e in particolare che $x, y \in X \Rightarrow xy \in S$:

$$x, y \in X \Rightarrow x = \alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdots \alpha_t^{m_t},\ \ y = \alpha_1^{m'_1} \cdot \alpha_2^{m'_2} \cdots \alpha_t^{m'_t} \Rightarrow$$
$$\Rightarrow xy = \alpha_1^{m_1+m'_1} \cdot \alpha_2^{m_2+m'_2} \cdots \alpha_t^{m_t+m'_t}$$

Se esiste un $i :\ \ m_i + m'_i > n_i$, abbiamo osservato che $\alpha_i^{m_i+m'_i} \in \langle Z \rangle_{\mathbb{Z}} \subseteq S$. Così procedendo per ogni i, riusciamo ad abbassare tutti gli esponenti, ottenendo una combinazione lineare intera degli elementi di X. Quindi $xy \in S$. □

Teorema 4.5. *Sia* S *un anello finitamente generato come* $\mathbb{Z}$ *modulo, tale che* $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$. *Allora,*

$$S \subseteq R$$

Dimostrazione:

$$S \text{ f.g. come } \mathbb{Z} \text{ modulo } \Rightarrow \exists Y \subseteq S,\ |Y| < \infty :\ \ S = \langle Y \rangle_{\mathbb{Z}}$$
$$Y = \{x_1, \ldots, x_n\}$$

Sia $s \in S$. Mostriamo che $s \in R$.

$$S \text{ anello } \Rightarrow \forall i = 1, \ldots, n\ \ sx_i \in S = \langle Y \rangle_{\mathbb{Z}} \Rightarrow$$
$$\Rightarrow \forall i = 1, \ldots, n\ \ \exists a_{i1}, \ldots, a_{in} \in \mathbb{Z} :\ \ sx_i = \sum_{j=1}^{n} a_{ij}x_j\ \ \forall i = 1, \ldots, n \quad (1)$$

Sia $A \in \mathbb{Z}^{n\times n}$: $A_{ij} = a_{ij}$

Sia $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$; per la definizione di Y, gli elementi x_i non sono tutti nulli.

Dunque: $(1) \Leftrightarrow sX = AX \Rightarrow X$ autovettore di A, s autovalore ;

s è quindi radice del polinomio caratteristico di A, che è un polinomio monico di $\mathbb{Z}[x]$. Possiamo così concludere che $s \in R$. □

Corollario 4.6. *L'insieme R degli interi algebrici è un anello.*

Dimostrazione: Siano $\alpha, \beta \in R$ e poniamo $Y = \{\alpha, \beta\}$. Poiché $Y \subseteq R$, dal Lemma 4.4 segue che esiste S anello f.g. come $\mathbb{Z}$-modulo, t.c. $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$, $Y \subseteq S$. Il Teorema 4.5 implica che $Y \subseteq S \subseteq R$ e dunque $\alpha - \beta$, $\alpha\beta \in S \subseteq R$. □

Definizione 4.7. Sia G un gruppo finito, poniamo

$$\exp(G) \overset{\text{def}}{=} \text{mcm}\,(o(g) \mid g \in G)$$

Proposizione 4.8. *Sia $m = \exp(G)$, si ha*

$$\mathcal{X} \in \text{ch } G \Rightarrow \mathcal{X}(g) \in R \cap \mathbb{Q}_m$$

dove $\mathbb{Q}_m$ è la seguente estensione *di $\mathbb{Q}$:*

$$\mathbb{Q}_m = \mathbb{Q}(\xi), \quad \langle \xi \rangle = U_m$$

Nota[7]

Dimostrazione:

$$\mathcal{X}(g) \underbrace{=}_{\text{Proposizione 3.19}} \xi_1 + \cdots + \xi_f$$

$$\xi_i \in U_{o(g)} \Leftrightarrow \xi_i^{o(g)} = 1 \Rightarrow \xi_i \in R \underbrace{\Rightarrow}_{R \text{ anello}} \mathcal{X}(g) \in R$$

D'altronde, per definizione di m,
$o(g) \Big/ m \Rightarrow U_{o(g)} \subseteq U_m = \langle \xi \rangle \Rightarrow \xi_i = \xi^j$ per qualche $j \Rightarrow \xi_i \in \mathbb{Q}(\xi) \Rightarrow \mathcal{X}(g) \in \mathbb{Q}(\xi)$
□

[7] In realta' vale un risultato molto piu' generale: il teorema di Brauer afferma che esiste un rappresentazione $\mathfrak{X}$ di $\mathcal{X}$ del tipo $\mathfrak{X} : G \longrightarrow \text{GL}(n, \mathbb{Q}_m)$

Proposizione 4.9. *Sia* $\mathrm{cl}(G) = \{K_1, \dots, K_k\}$, *allora*

$$\widehat{K_i}\widehat{K_j} = \sum_{r=1}^{k} a_{ijr}\widehat{K_r} \in Z(\mathbb{C}G)$$

dove $a_{ijr} = |\{(x_i, x_j) \mid x_i x_j = x_r,\ \ x_i \in K_i,\ x_j \in K_j\}|$ *con* $x_r \in K_r$ *fissato. In particolare i coefficienti* $a_{ijr} \in \mathbb{N}$

Dimostrazione: Per il Teorema 2.36, $B = \left\{\widehat{K_1}, \dots, \widehat{K_k}\right\}$ è un base di $Z(\mathbb{C}G)$. Posto $K_r = \{g_{r1}, \dots, g_{rt_r}\}$, si ha:

$\widehat{K_i}\widehat{K_j} \in Z(\mathbb{C}G)$

$$\widehat{K_i}\widehat{K_j} \underbrace{=}_{B \text{ base}} \sum_{r=1}^{k} a_{ijr}\widehat{K_r} \underbrace{=}_{\text{def di } \widehat{K_r}} \sum_{r=1}^{k} a_{ijr} \sum_{h=1}^{t_r} g_{rh} = \sum_{r=1}^{k}\sum_{h=1}^{t_r} a_{ijr} g_{rh} \quad (1)$$

$$K_1, \dots, K_k \text{ classi di coniugio } \Rightarrow \{g_{rh} \mid r, h\} = G,\ \ g_{rh} \neq g_{r'h'} \text{ per } (r,h) \neq (r',h') \quad (2)$$

Posto $a_{g_{rh}} = a_{ijr}$, per la (1) e la (2) si ha:

$$\widehat{K_i}\widehat{K_j} = \sum_{g \in G} a_g g \quad (1.1)$$

Inoltre,

$$a_{ijr} = a_{g_{rh}} \ \ \forall h = 1, \dots, t_r \Leftrightarrow a_{ijr} = a_{x_r} \ \ \forall x_r \in K_r \quad (1.2)$$

D'altra parte, il prodotto $\widehat{K_i}\widehat{K_j}$ si puo' scrivere come:

$$\widehat{K_i}\widehat{K_j} = \sum_{h=1}^{t_i}\sum_{s=1}^{t_j} g_{ih}g_{js}$$

Sia $g_{ihjs} = g_{ih}g_{js} \in G$; allora:

$$\widehat{K_i}\widehat{K_j} = \sum_{h=1}^{t_i}\sum_{s=1}^{t_j} g_{ihjs} = \sum_{g \in G} b_g g \quad (3)$$

dove $b_g = |\{(h,s) \mid g_{ihjs} = g\}|$.

Confrontando la (1.1) e la (3), per l'indipendenza lineare di G, si ha

$$a_g = b_g \quad (4)$$

$$a_{ijr} \underbrace{=}_{(1.2)} a_{x_r} \underbrace{=}_{(4)} b_{x_r} \ \ \forall x_r \in K_r$$

$$b_{x_r} = |\{(h,s) \mid g_{ihjs} = x_r\}| = |\{(h,s) \mid g_{ih}g_{js} = x_r\}| =$$
$$= |\{(x_i, x_j) \mid x_i x_j = x_r,\ \ x_i \in K_i,\ x_j \in K_j\}|$$
$$\Rightarrow a_{ijr} = |\{(x_i, x_j) \mid x_i x_j = x_r,\ \ x_i \in K_i,\ x_j \in K_j\}|$$

□

Proposizione 4.10. *Sia $\mathcal{X} \in \mathrm{Irr}(G)$, $K \in \mathrm{cl}(G)$ e $\mathfrak{X}, \mathfrak{Y}$ due rappresentazioni di G che inducono $\mathcal{X}$. Allora, si ha:*

1. $\mathfrak{X}(\widehat{K}) = \omega_{\mathfrak{X}}(\widehat{K})I, \quad$ *con* $\omega_{\mathfrak{X}}(\widehat{K}) \in \mathbb{C}$
2. $\omega_{\mathcal{X}}(\widehat{K}) \overset{def}{=} \omega_{\mathfrak{X}}(\widehat{K}) = \omega_{\mathfrak{Y}}(\widehat{K}) = \dfrac{|K|}{\mathcal{X}(1)}\mathcal{X}(x_k), \ \ \forall x_k \in K$
3. $\omega_{\mathcal{X}}(\widehat{K}) = \dfrac{\mathcal{X}(\widehat{K})}{\mathcal{X}(1)}$

Dimostrazione: 1.

$$\widehat{K} \in \left\{\widehat{K}_1, \dots, \widehat{K}_k\right\} \underbrace{\subseteq}_{\text{Teorema 2.36}} Z(\mathbb{C}G) \Rightarrow x\widehat{K} = \widehat{K}x, \ \ \forall x \in \mathbb{C}G \Rightarrow$$

$$\Rightarrow \mathfrak{X}(g\widehat{K}) = \mathfrak{X}(\widehat{K}g) \ \ \forall g \in G \Leftrightarrow \mathfrak{X}(\widehat{K})\mathfrak{X}(g) = \mathfrak{X}(g)\mathfrak{X}(\widehat{K}) \ \ \forall g \in G \Rightarrow$$

$$\underbrace{\Rightarrow}_{\text{Proposizione 2.50}} \quad \mathfrak{X}(\widehat{K}) = \lambda I$$

Ponendo $\omega_{\mathfrak{X}}(\widehat{K}) = \lambda$ si ha la tesi.

2. Si hanno le seguenti catene di uguaglianze:

$$\mathcal{X}(\widehat{K}) = \mathcal{X}\left(\sum_{x_k \in K} x_k\right) \underbrace{=}_{\mathcal{X} \text{ è additiva}} \sum_{x_k \in K} \mathcal{X}(x_k) \underbrace{=}_{\mathcal{X} \text{ funzione di classe}} \mathcal{X}(x_k)|K| \ \ (1)$$

$$\mathcal{X}(\widehat{K}) = \mathrm{Tr}\mathfrak{X}(\widehat{K}) = \mathrm{Tr}(\omega_{\mathfrak{X}}(\widehat{K})I) = \omega_{\mathfrak{X}}(\widehat{K})\mathrm{Tr}I = \omega_{\mathfrak{X}}(\widehat{K})\mathcal{X}(1) \ \ (2)$$

$$(1), (2) \Rightarrow \omega_{\mathfrak{X}}(\widehat{K}) = \frac{\mathcal{X}(x_k)}{\mathcal{X}(1)}|K|$$

Ripetendo lo stesso ragionamento con $\mathfrak{Y}$, si perviene allo stesso risultato. Quindi

$$\omega_{\mathfrak{X}}(\widehat{K}) = \omega_{\mathfrak{Y}}(\widehat{K})$$

ovvero, $\omega_{\mathcal{X}}(\widehat{K})$ è indipendente dalla scelta della rappresentazione.

3.

Basta rileggere la (2).

□

Teorema 4.11. *Dato $\mathcal{X} \in \mathrm{Irr}(G)$, si ha*

1. $\omega_{\mathcal{X}} : Z(\mathbb{C}G) \longrightarrow \mathbb{C}$ *definito da:*
$$\widehat{K} \mapsto \omega_{\mathcal{X}}(\widehat{K}) \qquad \forall K \in \mathrm{cl}(G)$$
$$\sum_{K\in\mathrm{cl}(G)} a_K \widehat{K} \mapsto \sum_{K\in\mathrm{cl}(G)} a_K \omega_{\mathcal{X}}(\widehat{K})$$
è un omomorfismo di algebre
2. $\omega_{\mathcal{X}}(\widehat{K}) \in R, \ \ \forall K \in \mathrm{cl}(G)$

Dimostrazione: 1.
Sia $x \in Z(\mathbb{C}G)$; per il Teorema 2.36 abbiamo
$$x = \sum_{i=1}^{k} a_K \widehat{K}$$
$$\mathfrak{X}(x) = \sum_{i=1}^{k} a_K \mathfrak{X}(\widehat{K}) \underbrace{=}_{\text{Proposizione 4.10}} \sum_{i=1}^{k} a_K \omega_{\mathfrak{X}}(\widehat{K}) I =$$
$$= \left(\sum_{i=1}^{k} a_K \omega_{\mathfrak{X}}(\widehat{K})\right) I \overset{\text{def}}{=} \omega_{\mathfrak{X}} \left(\sum_{i=1}^{k} a_K \widehat{K}\right) I = \omega_{\mathfrak{X}}(x) I$$
In definitiva, $\mathfrak{X}(x) = \omega_{\mathfrak{X}}(x) I$ per ogni $x \in Z(\mathbb{C}G)$ e dunque, poiché $\mathfrak{X} : \mathbb{C}G \longrightarrow \mathbb{C}^{n\times n}$ e' un omomorfismo di algebre, anche $\omega_{\mathfrak{X}}(x)$ e' un omomorfismo di algebre.

2.
Sia S l'insieme così definito:
$$S = \left\langle \left\{ \omega_{\mathcal{X}}(\widehat{K}) \mid K \in \mathrm{cl}(G) \right\} \right\rangle_{\mathbb{Z}}$$
Dimostriamo che S è un anello finitamente generato come $\mathbb{Z}$ modulo e tale che $\mathbb{Z}\subseteq S\subseteq\mathbb{C}$. Per definizione S è finitamente generato come $\mathbb{Z}$ modulo. Verifichiamo le altre affermazioni:

2.1. $\mathbb{Z}\subseteq S$:
$$\{1\} \in \mathrm{cl}(G) \Rightarrow \widehat{\{1\}} = 1$$
$$\omega_{\mathcal{X}}(1) = \omega_{\mathcal{X}}(\widehat{\{1\}}) \underbrace{=}_{\text{Proposizione 4.10}} \frac{\mathcal{X}(\widehat{\{1\}})}{\mathcal{X}(1)} = \frac{\mathcal{X}(1)}{\mathcal{X}(1)} = 1$$
$$\Rightarrow 1 \in S \underbrace{\Rightarrow}_{S \text{ f.g. come } \mathbb{Z}\text{-mod}} \mathbb{Z}\subseteq S$$

2.2. $(S, +)$ è un gruppo abeliano:
Segue direttamente dalla definizione.

2.3. S è chiuso rispetto al prodotto:

$$a, b \in S \Rightarrow a = \sum_i a_i \omega_{\mathcal{X}}(\widehat{K}), \quad b = \sum_i b_i \omega_{\mathcal{X}}(\widehat{K'}), \quad a_i, b_i \in \mathbb{Z}\ \forall i$$

$$ab = \sum_{i,j} a_i b_j \omega_{\mathcal{X}}(\widehat{K})\omega_{\mathcal{X}}(\widehat{K'}) \underbrace{=}_{\omega_{\mathcal{X}} \text{ omo.}} \sum_{i,j} a_i b_j \omega_{\mathcal{X}}(\widehat{K}\widehat{K'}) \underbrace{=}_{\text{Prop. 4.9}} \sum_{i,j} a_i b_j \omega_{\mathcal{X}} \left(\sum_{h=1}^{k} c_h \widehat{K_h} \right) =$$

dove $c_h \in \mathbb{N} \subseteq \mathbb{Z}\ \ \forall h = 1, \ldots, k, \ \ \mathrm{cl}(G) = \{K_1, \ldots, K_h\}$

$$= \sum_{i,j} \sum_{h=1}^{k} \underbrace{a_i b_j c_h}_{\in \mathbb{Z}} \omega_{\mathcal{X}} \left(\widehat{K_h} \right) \in S$$

2.4.

Dal fatto che S è un anello e uno $\mathbb{Z}$-modulo f.g., e per il Teorema 4.5, si ha

$$\omega_{\mathcal{X}}(\widehat{K}) \in S \subseteq R$$

□

5 Teorema di Burnside

In questo ultimo capitolo presenteremo la dimostrazione classica del teorema di Burnside, utilizzando tutti gli strumenti introdotti nei capitoli precedenti.
Iniziamo con il seguente Lemma:

Lemma 5.1. *Sia* $\mathcal{X} \in \mathrm{Irr}(G)$, $x \in G$ *e* $K = \mathrm{cl}(x)$. *Si ha*

$$(|K|, \mathcal{X}(1)) = 1 \Rightarrow \mathcal{X}(x) = 0 \vee x \in Z(\mathcal{X})$$

Dimostrazione: Sia $m = o(x)$, $e = \exp(G)$,

$$\mathcal{X}(x) \underbrace{=}_{\text{Proposizione 3.19}} \xi^{a_1} + \cdots + \xi^{a_n}$$

$$\text{dove } U_m = \langle \xi \rangle, \;\; n = \mathcal{X}(1)$$

Per la Proposizione 4.8 si ha: $\mathcal{X}(x) \in \mathbb{Q}_e \cap R$ con $e = \exp(G)$.
Sia $\omega \in \mathbb{C}$ tale che $U_e = \langle \omega \rangle$, quindi $\xi = \omega^j$, per qualche j. Supponiamo che $x \notin Z(\mathcal{X})$ e dimostriamo che $\mathcal{X}(x) = 0$.

$$x \notin Z(\mathcal{X}) \underbrace{\Rightarrow}_{\text{Teorema 3.24,Proposizione 3.19}} |\mathcal{X}(x)| < \mathcal{X}(1) = n$$

Ne segue:

$$\frac{|\mathcal{X}(x)|}{\mathcal{X}(1)} < 1 \quad (1)$$

Sia $\mathcal{G} = \mathcal{G}(\mathbb{Q}_e, \mathbb{Q})$ il gruppo di Galois relativo all'estensione di campi $\mathbb{Q} \subseteq \mathbb{Q}_e = \mathbb{Q}(\omega)$.
L'estensione $Q \subseteq \mathbb{Q}(\omega)$ è ciclotomica, ed è quindi un'estensione di Galois. Per il teorema fondamentale della teoria di Galois, segue che

$$\mathbb{Q}_e^{\mathcal{G}} = \mathbb{Q}$$

dove $\mathbb{Q}_e^{\mathcal{G}} = \{q \in \mathbb{Q}_e \mid \sigma(q) = q \;\; \forall \sigma \in \mathcal{G}\}$.
Sia $\sigma \in \mathcal{G}$. Poiché σ è un automorfismo di $\mathbb{Q}_e$, possiamo affermare le seguenti proposizioni:

- $\alpha^k = 1 \Rightarrow \sigma(\alpha)^k = 1$
- $\alpha \in R \Rightarrow \sigma(\alpha) \in R$, infatti:
  $\alpha \in R \Rightarrow \exists f \in \mathbb{Z}[x]$ monico t.c. $f(\alpha) = 0$
  $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0 \Rightarrow \sigma(\alpha) \in R$

Sfruttiamo adesso l'ipotesi $(|K|, \mathcal{X}(1)) = 1$:

$$(|K|, \mathcal{X}(1)) = 1 \underbrace{\Rightarrow}_{\text{identita' di Bezout}} \exists a, b \in \mathbb{Z} : \;\; a|K| + b\mathcal{X}(1) = 1 \Leftrightarrow$$

$$\Leftrightarrow a|K|\frac{\mathcal{X}(x)}{\mathcal{X}(1)} + b\mathcal{X}(x) = \frac{\mathcal{X}(x)}{\mathcal{X}(1)}$$

Poiche' $x \in K$ e $\mathcal{X} \in \mathrm{Irr}(G)$, dalla Proposizione 4.10 segue che

$$|K|\frac{\mathcal{X}(x)}{\mathcal{X}(1)} = \omega_{\mathcal{X}}(\widehat{K}) \in R$$

Dunque l'uguaglianza (2) equivale a

$$a\omega_{\mathcal{X}}(\widehat{K}) + b\mathcal{X}(x) = \frac{\mathcal{X}(x)}{\mathcal{X}(1)}$$

Inoltre:

$$\omega_{\mathcal{X}}(\widehat{K}) \in R,\ \mathcal{X}(x) \in R \Rightarrow \frac{\mathcal{X}(x)}{\mathcal{X}(1)} \in R \quad (3)$$

Sia $\alpha = \frac{\mathcal{X}(x)}{\mathcal{X}(1)}$. Osserviamo che

$$(1) \Rightarrow |\alpha| < 1$$

$$(3) \Rightarrow \alpha \in R \Rightarrow \sigma(\alpha) \in R,\ \ \forall \sigma \in \mathcal{G} \quad (5)$$

$$\sigma(\alpha) = \frac{\sigma(\mathcal{X}(x))}{\sigma(\mathcal{X}(1))} \underbrace{=}_{\mathcal{X}(1)=n\in\mathbb{Q}} \frac{\sigma(\mathcal{X}(x))}{\mathcal{X}(1)}.$$

Inoltre, ricordando che $U_m = \langle \xi \rangle$ e che $\mathcal{X}(x) = \xi^{a_1} + \cdots + \xi^{a_n}$ si ottiene:

$$\sigma(\mathcal{X}(x)) = \sigma(\xi)^{a_1} + \cdots + \sigma(\xi)^{a_n} = \zeta^{a_1} + \cdots + \zeta^{a_n},\ \text{con } \langle \zeta \rangle = U_m$$

$$|\sigma(\mathcal{X}(x))| = |\zeta^{a_1} + \cdots + \zeta^{a_n}| \leq |\zeta^{a_1}| + \cdots + |\zeta^{a_n}| = 1 + \cdots + 1 = n$$

$$|\sigma(\alpha)| = \frac{|\mathcal{X}(x)|}{|\mathcal{X}(1)|} \leq \frac{n}{n} = 1 \quad (6)$$

Consideriamo la norma di α secondo $\mathcal{G}$, ovvero sia

$$\beta = \prod_{\sigma\in\mathcal{G}} \sigma(\alpha);$$

abbiamo

$$\sigma = \mathrm{id} \Rightarrow |\sigma(\alpha)| = |\alpha| \underbrace{<}_{(4)} 1$$

$$|\beta| = \prod_{\sigma\in\mathcal{G}} |\sigma(\alpha)| = |\alpha| \prod_{\sigma\in\mathcal{G}:\ \sigma\neq\mathrm{id}} |\sigma(\alpha)| \underbrace{<}_{(6)} 1 \quad (7)$$

Infine,

$$\sigma(\beta) \underbrace{=}_{\mathcal{G}\text{ è un gruppo}} \beta, \quad \forall \sigma \in \mathcal{G} \Rightarrow \beta \in \mathbb{Q}_e^{\mathcal{G}} = \mathbb{Q}$$

$$(5) \underbrace{\Rightarrow}_{R\text{ è un anello}} \beta \in R \Rightarrow \beta \in R \cap \mathbb{Q} \underbrace{=}_{\text{Prop 4.2}} \mathbb{Z} \underbrace{\Rightarrow}_{(7)} \beta = 0 \Rightarrow$$

$$\Rightarrow \exists \sigma \in \mathcal{G} :\ \ \sigma(\alpha) = 0 \underbrace{\Leftrightarrow}_{\sigma\text{ è biettiva}} \alpha = \sigma^{-1}(0) = 0$$

$$\alpha = 0 \Leftrightarrow \frac{\mathcal{X}(x)}{\mathcal{X}(1)} = 0 \Leftrightarrow \mathcal{X}(x) = 0$$

□

L'enunciato del seguente teorema coinvolge solamente la teoria dei gruppi, eppure, la sua dimostrazione fa esclusivamente ricorso a concetti provenienti dalla teoria dei caratteri.

Teorema 5.2. *Sia $x \in G$, allora*

$$\begin{cases} x \neq 1 \\ |\mathrm{cl}(x)| = p^a, \quad p \text{ primo} \\ a > 0 \end{cases} \Rightarrow G \text{ non è semplice}$$

Dimostrazione: Supponiamo per assurdo che G sia semplice. Sia $\mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\}$. Si ha

$$\begin{cases} |\mathrm{cl}(x)| = p^a > 1 \Rightarrow G \text{ non è abeliano} \\ G \text{ semplice} \\ \mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\} \end{cases} \underbrace{\Rightarrow}_{\text{Proposizione 3.26}} Z(\mathcal{X}) = \{1\}$$

Inoltre si ha:

$$\rho_G(x) \underbrace{=}_{\text{Proposizione 3.15}} \sum_{\mathcal{X} \in \mathrm{Irr}(G)} \mathcal{X}(1)\mathcal{X}(x) \underbrace{=}_{x \neq 1} 0 \quad (1)$$

$$\rho_G(x) = \sum_{\mathcal{X} \in \mathrm{Irr}(G)} \mathcal{X}(1)\mathcal{X}(x) =$$

$$= 1 + \sum_{\mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\}} \mathcal{X}(1)\mathcal{X}(x) =$$

$$= 1 + \underbrace{\sum_{\mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\},\ p / \mathcal{X}(1)} \mathcal{X}(1)\mathcal{X}(x)}_{A} + \underbrace{\sum_{\mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\},\ p \text{ non divide } \mathcal{X}(1)} \mathcal{X}(1)\mathcal{X}(x)}_{B} \quad (2)$$

Sia ora $K = \mathrm{cl}(x)$; allora:

$$|K| = p^a,\ p \not| \mathcal{X}(1) \Rightarrow (|K|, \mathcal{X}(1)) = 1 \Rightarrow \mathcal{X}(x) = 0 \vee x \in \mathbb{Z}(\mathcal{X}) = \{1\} \Leftrightarrow$$

$$\underbrace{\Leftrightarrow}_{x \neq 1} \mathcal{X}(x) = 0 \quad \forall \mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\} : \ p \not| \mathcal{X}(1) \Rightarrow B = 0$$

Infine da $B = 0$, (2), (1) segue che

$$0 = \rho_G(x) = 1 + \sum_{\mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\},\ p / \mathcal{X}(1)} \mathcal{X}(1)\mathcal{X}(x) \Leftrightarrow$$

$$\Leftrightarrow 1 + p \underbrace{\sum_{\mathcal{X} \in \mathrm{Irr}(G) \setminus \{1_G\},\ p / \mathcal{X}(1)} \underbrace{\frac{\mathcal{X}(1)}{p}}_{\in \mathbb{Z}} \underbrace{\mathcal{X}(x)}_{\in R}}_{= \gamma \in R} = 0 \Leftrightarrow \gamma = -\frac{1}{p} \in R \cap \mathbb{Q} \underbrace{=}_{\text{Prop 4.2}} \mathbb{Z} \Rightarrow p = \pm 1$$

Assurdo, in quanto p è un primo. □

Teorema 5.3. *(Burnside) Sia G un gruppo finito*

$$|G| = p^a q^b, \;\; p, q \text{ primi }, \;\; a, b > 0 \Rightarrow G \text{ non è semplice}$$

Dimostrazione: Distinguiamo due casi:
CASO: $p = q$

$|G| = p^{a+b}$, $a, b > 0 \Rightarrow G$ p-gruppo , $|G| > 1 \Rightarrow$
$\Rightarrow \exists$ una catena di sottogruppi normali non banali $\Rightarrow G$ non è semplice
CASO: $p \neq q$
Sia P un p sottogruppo di Sylow di G. Si ha

$$\begin{cases} |P| = p^a, \;\; p \not| q^b \\ \frac{|G|}{|P|} = q^b \end{cases} \qquad (1)$$

$$b > 0 \underbrace{\Rightarrow}_{(1)} P < G$$

Inoltre,

$$P \text{ } p\text{-gruppo } \Rightarrow Z(P) \neq 1 \Rightarrow \exists x \in Z(P) \setminus \{1\}$$

Se non esiste un $x \in Z(P)$ tale che $|\mathrm{cl}_G(x)| > 1$, allora
$x \in Z(G) \Leftrightarrow |\mathrm{cl}_G(x)| = 1 \;\; (*)$
$\forall x \in Z(P) \;\; |\mathrm{cl}_G(x)| = 1 \Rightarrow Z(P) \subseteq Z(G)$
$1 \neq Z(P) \subseteq Z(G) \trianglelefteq G \Rightarrow Z(P) \trianglelefteq G \;\; (**)$
$Z(P) = G \Rightarrow Z(G) = G \Rightarrow G$ abeliano $\Rightarrow P \trianglelefteq G \underbrace{\Rightarrow}_{1 \neq P \neq G} G$ non semplice
$1 \neq Z(P) \neq G \underbrace{\Rightarrow}_{(**)} G$ non semplice

Possiamo quindi supporre che esista un $x \in Z(P)$ tale che $|\mathrm{cl}_G(x)| > 1$. Sia $C_G(x)$ il centralizzante di x in G, allora

$$P \underbrace{\leq}_{x \in Z(P)} C_G(x) \leq G \Rightarrow \frac{|C(x)|}{|P|} [G : C(x)] = \frac{|G|}{|P|} \Rightarrow [G : C(x)] \Big/ \frac{|G|}{|P|} = q^b \;\; (2)$$

$$|\mathrm{cl}(x)| = [G : C(x)] = \frac{|G|}{|C(x)|} \underbrace{=}_{(2)} q^c, \;\; c \leq b \;\; (3)$$

$$|\mathrm{cl}(x)| = q^c \underbrace{>}_{\text{per ipotesi}} 1, \;\; x \neq 1 \underbrace{\Rightarrow}_{\text{Teorema 5.2}} G \text{ non è semplice}$$

□

Corollario 5.4. *Sia G un gruppo finito*

$$|G| = p^a q^b, \;\; p, q \text{ primi } \Rightarrow G \text{ è risolubile}$$

Dimostrazione: Procediamo per induzione forte su $n = |G|$.
I casi in cui $a = 0$ oppure $b = 0$ sono immediati perché

$$G \; p\text{-gruppo } \Rightarrow G \text{ è risolubile}$$

Supponiamo quindi $a, b > 0$. Sia $1 \leq N < G$ un sottogruppo normale di G. Se per assurdo $N = 1$, G sarebbe semplice. Questo è però in contrasto con il Teorema 5.3. Quindi,

$$N > 1 \Rightarrow \left|\frac{G}{N}\right| < n, \;\; \left|\frac{G}{N}\right| = p^{a'} q^{b'} \underbrace{\Rightarrow}_{\text{ipotesi induttiva}} \frac{G}{N} \text{ è risolubile}$$

$$N < G \Rightarrow |N| = p^{a''} q^{b''} < n \underbrace{\Rightarrow}_{\text{ipotesi induttiva}} N \text{ è risolubile}$$

$$\begin{cases} N \trianglelefteq G \\ \frac{G}{N} \text{ è risolubile} \\ N \text{ è risolubile} \end{cases} \Rightarrow G \text{ risolubile}$$

□

Bibliografia

[**1**] I. M. Isaacs, *Character theory of finite groups.* AMS Chelsea Publishing, Providence, RI, 2006.

[**2**] Giulia Maria Piacentini Cattaneo, *Algebra, un approccio algoritmico.* Zanichelli, 1996.

[**3**] Hancock, H. *Foundations of the Theory of Algebraic Numbers*, Vol. 1: Introduction to the General Theory. New York: Macmillan, 1931.