Character theory

AlpT (@freaknet.org)
http://freaknet.org/alpt

May 29, 2009

Abstract

Questo testo e' una rielaborazione personale degli appunti presi durante il corso di Algebra, tenuto dal Prof. Gabriel Navarro presso il dipartimento di Matematica, Perugia, Scuola Matematica Interuniversitaria, A.A. 2007/2008.
Saro' ben lieto di correggere ogni eventuale errore che mi comunicherai.
Buon lettura.

^_^

Copyright ©2008 Andrea Lo Pumo aka AlpT <alpt@freaknet.org>. All rights reserved.

This document is free; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this document; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Contents

1 Preliminari **1**

2 Algebre **1**
2.1 Moduli 5
2.2 Moduli semisemplici 11
2.3 Algebre semisemplici 13

3 Algebra di un gruppo **19**

4 Rappresentazioni **23**

5 Caratteri **32**

6 Interi algebrici **43**

7 Teorema di Burnside **48**

8 * **53**

1 Preliminari

Definition 1.1. . Sia A un anello (o gruppo). Se B e' 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 unita', cioe'

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

   Quindi ogni anello unitario ha almeno 2 elementi.

2. Ogni anello sara' ritenuto implicitamente unitario.

Remark 1.1. Tutti gli spazi vettoriali che considereremo saranno di dimensione finita.

2 Algebre

Definition 2.1. Sia A un F-spazio vettoriale finitamente generato e un anello[1].

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

Definition 2.2. Sia $B \subseteq A$,

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

Se B e' una sottoalgebra di A utilizzeremo la seguente notazione:

$$B \preceq A$$

Remark 2.1. Una sottoalgebra e' un'algebra

Proposition 2.3.

$$B \preceq A \Leftrightarrow \begin{cases} x - y \in B \\ \lambda x \in B \\ xy \in B \\ 1_A \in B \end{cases} \qquad \forall x, y \in B, \ \ \forall \lambda \in F$$

Example 2.4. I seguenti insiemi sono delle algebre:

1. $A = F^{n \times n}$
2. $A = \mathrm{Hom}(V, V)_F$, con V spazio vett. finitamente generato.

Definition 2.5. Definiamo il centro dell'algebra A:

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

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

Remark 2.2. $Z(A) \preceq A$

Proposition 2.6. *Sia $e_1, \dots, e_n$ una base di A, allora*

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

Definition 2.7. Sia data una mappa $f : A \longrightarrow B$, con A, B algebre.

$$f \text{ e' un omomorfismo di algebre (alg-hom)} \overset{\text{def}}{\Leftrightarrow} \begin{cases} f \text{ e' una applicazione lineare} \\ f \text{ e' un omomorfismo di anelli} \\ f(1_A) = 1_B \end{cases} \Leftrightarrow \begin{cases} f(\lambda x + \mu y) = \lambda f(x) + \mu f(y \\ f(xy) = f(x)f(y) \\ f(1_A) = 1_B \end{cases}$$

Example 2.8. Sia A una F-algebra, allora la funzione

$$\begin{aligned} f : F &\longrightarrow A \\ \lambda &\mapsto \lambda 1_A \end{aligned}$$

e' una omomorfismo di algebre iniettivo.

Proof: E' facile vedere che e' f un omomorfismo, verifichiamo solo che $f(\lambda\mu) = f(\lambda)f(\mu)$

$$f(\lambda\mu) = (\lambda\mu)1_A \underbrace{=}_{\text{assiomi dei vettori}} \lambda(\mu 1_A) =$$

$$= \lambda(1_A(\mu 1_A)) \underbrace{=}_{\text{assioma algebra}} (\lambda 1_A)(\mu 1_A) = f(\lambda)f(\mu)$$

f e' iniettiva, infatti,

$$\begin{aligned} &\ker f = \{\lambda \in F \mid \lambda 1_A = 0\} \\ &\lambda 1_A = 0 \Leftrightarrow \lambda = 0 \vee 1_A = 0 \\ &\lambda \neq 0 \Rightarrow 1_A = 0 \text{ assurdo} \\ &\Rightarrow \ker f = \{0\} \end{aligned}$$

□

Definition 2.9. Con $I \trianglelefteq A$ indichiamo un ideale (bilatero) di A. Con $I \overset{d}{\trianglelefteq} A$ un ideale destro di A.

Proposition 2.10. *Sia $I \overset{d}{\trianglelefteq} A$ un ideale destro di A, allora*

$$I \overset{d}{\trianglelefteq} A \Rightarrow I \leq A$$

ovvero, I e' un sottospazio vettoriale di A.

Proof: Basta verificare che $\lambda x \in I \ \ \forall x \in I, \ \forall \lambda \in F$.

$$\lambda x = \lambda(x 1_A) \underbrace{=}_{\text{Assioma algebra}} x(\lambda 1_A) \underbrace{\in}_{I \text{ e' ideale destro e } x \in I} I$$

□

Proposition 2.11. *Sia $\{e_{ij} \mid i, j = 1, \dots, n\}$ la base canonica di $F^{n \times n}$, ovvero e_{ij} e' la matrice formata tutta da zeri, con 1 nel posto i, j.*

Sia $a \in F^{n\times n}$ Si ha,

1. $e_{ij}e_{kl} = \delta_{jk}e_{il}$
2. $ae_{kl} = \sum_i a_{ik}e_{il} = \begin{bmatrix} 0 & \dots & 0 & a_{1k} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2k} & 0 & \dots & 0 \\ \vdots & & & & & & \\ 0 & \dots & 0 & a_{nk} & 0 & \dots & 0 \end{bmatrix}$
3. $e_{kl}a = \sum_i a_{li}e_{ki} = \begin{bmatrix} 0 & & \dots & 0 \\ 0 & & \dots & 0 \\ \vdots & & & \\ 0 & & \dots & 0 \\ a_{l1} & a_{l2} & \dots & a_{ln} \\ 0 & & \dots & 0 \\ \vdots & & & \\ 0 & & \dots & 0 \end{bmatrix}$
4. $e_{rs}ae_{kl} = a_{sk}e_{rl}$

Intuitivamente,

1. *ae_{kl} e' la matrice con la colonna k-esima di a messa nella colonna l e con tutti gli altri posti nulli*
2. *$e_{kl}a$ e' la matrice con la riga l-esima di a posta nella riga k e con tutti gli altri posti nulli.*
3. *$e_{rs}ae_{kl}$ e' la matrice che ha l'elemento a_{sk} nel posto r,l. Tutti gli altri suoi elementi sono nulli.*

Proof:
$\langle 1\rangle$ Dim 2.

$$a = \sum_{i,j} a_{ij}e_{ij}$$
$$ae_{kl} = \sum_{i,j} a_{ij}e_{ij}e_{kl} \underbrace{=}_{1.} \sum_{i,j} a_{ij}\delta_{jk}e_{il} = \sum_i a_{ik}e_{il}$$

$\langle 2\rangle$ Dim 4.

$$e_{rs}a \underbrace{=}_{3.} = \sum_i a_{si}e_{ri}$$
$$e_{rs}ae_{kl} = (e_{rs}a)e_{kl} = \sum_i a_{si}e_{ri}e_{kl} \underbrace{=}_{1.} \sum_i a_{si}\delta_{ik}e_{rl} = a_{sk}e_{rl}$$

□

Proposition 2.12. *Sia p_{ij} la matrice di permutazione che scambia la riga (colonna) i con la*

riga (colonna) j. Allora si ha,

1. $p_{ij} = 1 - e_{jj} - e_{ii} + e_{ij} + e_{ji}$
2. $p_{ij}a$ *e' la matrice ottenuta scambiando le righe* i, j *di* a
3. ap_{ij} *e' la matrice ottenuta scambiando le colonne* i, j *di* a
4. $p_{ij}e_{jk} = e_{ik}$
5. $e_{ij}p_{jk} = e_{ik}$

Proposition 2.13.

$$Z(F^{n\times n}) = \{\mathrm{diag}(\lambda, \lambda, \dots, \lambda) \mid \lambda \in F\}$$

Proof:

$$Z(A) \underbrace{=}_{[2.6,\text{pg.2}]} \{a \in A \mid ae_{ij} = e_{ij}a \ \ \forall i, j = 1, \dots, n\}$$

$$ae_{ij} = e_{ij}a \underbrace{\Leftrightarrow}_{[2.11,\text{pg.2}]} \begin{bmatrix} 0 & \dots & 0 & a_{1i} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2i} & 0 & \dots & 0 \\ \vdots & & & & & & \\ 0 & \dots & 0 & \underbrace{a_{ni}}_{\text{colonna } j} & 0 & \dots & 0 \end{bmatrix} = \begin{bmatrix} 0 & & \dots & 0 \\ 0 & & \dots & 0 \\ \vdots & & & \\ 0 & & \dots & 0 \\ a_{j1} & a_{j2} & \dots & \underbrace{a_{jn}}_{\text{riga } i} \\ 0 & & \dots & 0 \\ \vdots & & & \\ 0 & & \dots & 0 \end{bmatrix}$$

$$\Rightarrow \begin{cases} a_{jj} = a_{ii} \\ a_{ki} = 0 \qquad k \neq i \\ a_{jh} = 0 \qquad j \neq h \end{cases}$$

E poiche' questo vale per ogni i, j, si ha la tesi. □

Definition 2.14. Sia A un anello,

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

In altre parole, A e' semplice quando non ha ideali non banali.

Theorem 2.15. *Sia* $A = F^{n\times n}$*, con* F *campo, allora,*

$$A \text{ } e' \text{ } un'algebra \text{ } semplice$$

Proof: Sia $I \trianglelefteq A$ e supponiamo che $I \neq 0$. Dimostriamo che $I = A$.

$$I \neq 0 \Rightarrow \exists a \neq 0 \in I \Rightarrow \exists a_{rs} \neq 0$$
$$e_{sr}a \in I \text{ perche' } a \in I \trianglelefteq A$$
$$(e_{sr}a)e_{ss} \in I$$
$$I \ni e_{sr}ae_{ss} \underbrace{=}_{[2.11,\text{pg.}2]} a_{rs}e_{ss} \in I$$
$$\underbrace{a_{rs}}_{\in F} \neq 0 \Rightarrow \exists {a_{rs}}^{-1} \in F$$
$$\begin{cases} a_{rs}e_{ss} \in I \\ I \underbrace{\leq}_{\text{sott. vettoriale}} A \\ {a_{rs}}^{-1} \in F \text{ e' uno scalare} \end{cases} \Rightarrow {a_{rs}}^{-1}(a_{rs}e_{ss}) \in I \Leftrightarrow e_{ss} \in I$$
$$e_{ss} \in I \trianglelefteq A \underbrace{\Rightarrow}_{\text{ideale}} p_{is}e_{ss}p_{sj} \in I \Leftrightarrow e_{ij} \in I$$

e questo $\forall i, j$. Quindi

$$\{e_{ij} \mid i, j\} \text{ base di } A \subseteq I \Rightarrow A = I$$

□

Remark 2.3. Anche se non esistono ideali non banali, possono esistere ideali destri o sinistri. Ad esempio,

$$I = \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix} \mid \alpha, \beta \in F \right\}$$

e' un ideale destro di $A = F^{n \times n}$

2.1 Moduli

Definition 2.16. Sia A un F-algebra, e V un F-spazio vettoriale, allora

$$V \text{ e' un } A\text{-modulo, secondo l'operazione } \cdot : V \times A \longrightarrow V \quad \overset{\text{def}}{\Leftrightarrow}$$
$$\overset{\text{def}}{\Leftrightarrow} \begin{cases} 1.\ v1_A = v \\ 2.\ (v+w)a = va + wa \\ 3.\ (va)b = v(ab) \\ 4.\ v(a+b) = va + vb \\ 5.\ (\lambda v)a = v(\lambda a) = \lambda(va) \end{cases} \quad \forall \lambda \in F,\ \forall a, b \in A,\ \ \forall v, w \in V$$

In pratica, si puo' pensare A come un particolare insieme di scalari per V (moltiplicati pero' a destra).

Example 2.17.
1. $A = F^{n \times n}$, $V = F^n$ e' 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°

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

Definition 2.18. Sia V un A-modulo, e $W \leq V$,

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

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

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

Example 2.19. I sottomoduli di A° sono gli ideali destri.

Proposition 2.20. *Sia V un A-mod e W un suo sottomodulo,allora*

$$V/W \text{ e' un } A\text{-modulo con l'operazione } (v+W)a = va + W$$

Proof:
$\langle 1 \rangle$ L'operazione e' ben definita

$$v + W = v' + W \Rightarrow v - v' \in W \Rightarrow (v - v') \in W \underbrace{\Rightarrow}_{W \text{ sottomodulo}} (v - v')a \in W \Rightarrow va + W = v'a + W$$

□

Example 2.21. Dato V A-modulo e $v \in V$,

$$vA = \{va \mid a \in A\} \text{ e' un } A\text{-sottomodulo}$$

e in generale

$$v_1A + \cdots + v_sA \text{ e' un } A\text{-sottomodulo}$$

Example 2.22. Sia V un A-mod, allora l'applicazione

$$\begin{aligned} &\rho : A \longrightarrow \mathrm{End}_F(V) \\ &a \mapsto \rho_a \\ &\text{dove } \rho_a : V \longrightarrow V \\ &\qquad v \mapsto va \end{aligned}$$

e' una algebra-omomorfismo.

Definition 2.23. Sia V un A-modulo,

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

$\mathrm{ann}_A(V)$ e' l'*annullatore* di V in A.

Proposition 2.24.

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

Definition 2.25. Sia V un A-modulo,

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

Theorem 2.26. *Sia $A = F^{n\times n}$, $V = F^n$ A-mod con l'usuale moltiplicazione tra vettori e matrici, allora*

$$V \text{ e' semplice}$$

Proof: Supponiamo per assurdo che $\exists W$ sotto A-mod : $0 < W < V$, allora

$$\exists v \in V\backslash W, \ \exists w \in W\backslash\{0\}$$

Sia f un endomorfismo t.c.

$$f(w) = v$$

e sia $c \in A$ la sua matrice associata (secondo la base canonica), e quindi [3]

$$wc = f(w) = v$$

ma essendo W un sottomodulo,

$$wc \in W \Rightarrow v \in W$$

assurdo contro $v \in V\backslash W$.

□

Definition 2.27. Siano V, W due A-moduli.

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

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

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

Proposition 2.28. *Sia $f : V \longrightarrow W$ un A-omomorfismo.*

$$\ker f \text{ e' un sottomodulo di } V$$
$$f(V) \text{ e' un sottomodulo di } W$$

Example 2.29. Sia W un A-sottomodulo di V I seguenti sono A-omomorfismi:

1. $i : W \longrightarrow V$ inclusione
2. $\pi : V \longrightarrow V/W$ surriez. naturale

Sia U un A-sottomodulo di V e supponiamo $V = U \oplus V$, allora

$$\pi_U : V \longrightarrow U$$
$$v = u + v \mapsto u$$

e' un A-omomorfismo.

Proposition 2.30.

$$V \overset{A}{\simeq} W \Rightarrow \text{ann}_A(V) = \text{ann}_A(W)$$

Ovvero, moduli isomorfi hanno lo stesso annulatore.

[3] stiamo usando una diversa notazione notazione per le matrici: i vettori sono righe, e se A e' la matrice associata ad f, $v^tA = f(v)$ Come matrice associata intenderemo $B = {}^tA$, quindi $f(v) = w \Leftrightarrow vB = f(v)$

Proof:

$V \overset{A}{\simeq} W \Leftrightarrow \exists f : V \longrightarrow W$ A-isomorfismo

$a \in \operatorname{ann}_A(V) \Leftrightarrow Va = 0 \Leftrightarrow f(Va) = 0 \Leftrightarrow f(V)a = 0 \Leftrightarrow Wa = 0 \Leftrightarrow a \in \operatorname{ann}_A(W)$

□

Proposition 2.31. *Siano V, W degli A-mod.*

$$\operatorname{Hom}_A(V,W) \overset{def}{=} \{f : V \longrightarrow W \mid f \ A\text{-omo}\} \ \text{e' uno spazio vettoriale}$$

$$\operatorname{End}_A(V) \overset{def}{=} \operatorname{Hom}_A(V,V) \underbrace{\preceq}_{\text{sotto algebra}} \operatorname{End}_F(V)$$

Theorem 2.32. *di Schur. Siano V, W degli A-mod.*

$$\begin{cases} f : V \longrightarrow W \ A\text{-omo} \\ V, W \ \text{semplici} \\ \operatorname{Im} f \neq \{0\} \end{cases} \Rightarrow f \ \text{e' un } A\text{-isomorfismo}$$

Proof: Per la prop [2.28,pg.7], $\operatorname{Im} f$ e' un A-sottomod di W, e poiche' $\operatorname{Im} f \neq 0$, si ha

$$0 < \operatorname{Im} f \leq W, \ \ W \text{ e' semplice } \Rightarrow \operatorname{Im} f = W \Leftrightarrow f \text{ surriettiva}$$

Analogamente:

$$\operatorname{Im} f \neq \{0\} \Rightarrow \ker f < V \Rightarrow 0 \leq \ker f < V \underbrace{\Rightarrow}_{V \text{ semplice}} \ker f = \{0\} \Rightarrow f \text{ iniettiva}$$

□

Corollary 2.33. *Sia F campo algebricamente chiuso, V A-modulo semplice, allora*

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

Proof:

$\langle 1 \rangle$ Dim $\Leftarrow$

$$f(va) = \lambda(va) = (\lambda v)a = f(v)a$$

$\langle 2 \rangle$ Dim $\Rightarrow$

Poiche' F e' chiuso, f ammette almeno un autovettore $v \in V \setminus \{0\}$ con autovalore $\lambda \in F$ (il polinomio caratteristico ammette radici in F). Allora,

$f(v) = \lambda v$

Sia $g = f - \lambda \mathrm{id}_V$

$f, \lambda \mathrm{id}_V \in \operatorname{End}_A(V) \Rightarrow g \in \operatorname{End}_A(V)$

$g(v) = f(v) - \lambda v = 0 \Rightarrow v \in \ker g \Rightarrow \ker g \neq 0$

Allora per il teorema [2.32,pg.8] deve essere necessariamente $\operatorname{Im} g = \{0\}$ e quindi

$$f = \lambda \mathrm{id}_V$$

□

Proposition 2.34.

$$V \ A\text{-modulo}, \ V \neq 0 \Rightarrow \exists W \overset{A}{\leq} V \ \text{semplice}$$

In altre parole, in un A modulo possiamo sempre trovare un sottomodulo semplice.

Proof: Se V e' semplice, scegliamo $W = V$, altrimenti possiamo trovare un $V_1 \overset{A}{\leq} V$. A questo punto procediamo per induzione su V_1. L'induzione dovra' arrestarsi perche' $\dim V < \infty$. □

Proposition 2.35. *Sia I un insieme di indici qualunque (anche infinito), e sia V uno spazio vettoriale finitamente generato. Sia $\{U_i\}_{i\in I}$ una famiglia di sottospazi di V. Definiamo la seguente somma:*

$$\sum_{i\in I} U_i \overset{def}{=} \left\{ \sum_{j\in J} u_j \mid J \subseteq I,\ \ |J| < \infty \right\}$$

allora si ha

$$V = \sum_{i\in I} U_i \Rightarrow \exists \{i_1, \dots, i_m\} \subseteq I :\ V = U_{i_1} + \cdots + U_{i_m}$$

Proof: Poiche' $V = \sum_{i\in I} U_i$, ogni vettore $v \in V$ si potra' scrivere come somma finita di elementi di certi U_i:

$$v = \sum_{j\in J} u_j,\ \ u_j \in U_j\ \ \forall j \in J$$

Quindi considerando la base $\{v_1, \dots, v_n\}$ di V, avremo

$$v_k = \sum_{j_k \in J_k} u_{j_k}\ \ \forall k = 1, \dots, n$$

e quindi

$$\{v_1, \dots, v_n\} \subseteq \sum_{k=1,\dots,n,\ j_k\in J_k} U_{j_k}$$

e poiche' $|J_k| < \infty$, abbiamo la tesi. □

Proposition 2.36. *Sia W un sottomodulo di V.*

$$W \text{ e' massimale } \Leftrightarrow V/W \text{ e' semplice}$$

Proof: Sia $\pi : V \longrightarrow V/W$ la surriezione naturale,
⟨1⟩ Dim. $\Rightarrow$

$$\overline{U} < V/W \Leftarrow \pi^{-1}(U) \supseteq W \Rightarrow W \text{ non e' massimale}$$

⟨2⟩ Dim. $\Leftarrow$

$$W < W' < V \Rightarrow \pi(W') < V/W \Rightarrow V/W \text{ non semplice}$$

□

Proposition 2.37. *Sia V un A-mod.*

$$V \text{ e' semplice } \Leftrightarrow V \simeq A/I \text{ con } I \overset{d}{\lhd} A \text{ massimale}$$

Proof:
⟨1⟩ Dim. $\Rightarrow$

V semplice, $v \in V \setminus \{0\} \Rightarrow vA = V$
$f : A \longrightarrow vA,\ a \mapsto va$ e' un A-omomorfismo surriettivo $\Rightarrow A/\ker f \simeq vA = V$ (1)
V semplice $\Rightarrow A/\ker f$ semplice $\underbrace{\Rightarrow}_{\text{[2.36,pg.9]}}$ $\ker f$ massimale

Quindi scegliendo $I = \ker f$ si ha la tesi.

Nota: nell'usare la proposizione [2.36,pg.9], abbiamo implicitamente considerato A come modulo, ovvero, A°, e fatto ricorso all'esempio [2.19,pg.6].

⟨2⟩ Dim. $\Leftarrow$

Si procede utilizzando le stesse idee di prima:

$$I \overset{d}{\trianglelefteq} A \text{ massimale } \Leftrightarrow I \leq A^\circ \text{ massimale } \underbrace{\Rightarrow}_{[2.36,\text{pg.9}]} A/I \text{ semplice}$$

□

Lemma 2.38. *Sia V un A-mod, $\{U_i\}_{i\in I}$ una famiglia di sotto A-moduli semplici, con I insieme di indici qualsiasi, allora*

$$V = \sum_{i\in I} U_i \Rightarrow V = U_{i_1} \oplus \cdots \oplus U_{i_t}$$

Remark 2.4. Nella proposizione [2.35,pg.9] ottenevamo un risultato analogo. Stavolta, pero', richiedendo la semplicita' si U_i e la modularita' di A e U_i, otteniamo come risultato una somma diretta.

Proof: Sia $\mathcal{W}$ l'insieme di tutti i sottomoduli che si possono scrivere come somma diretta di alcuni U_i:

$$\mathcal{W} = [W = U_{j_1} \oplus \cdots \oplus U_{j_t} \mid j_1, \ldots, j_t \in I]$$

sia W il massimale di $(\mathcal{W}, \subseteq)$, che sicuramente esiste perche' $\dim V < \infty$.

⟨1⟩ Dimostriamo che $W = V$

Procediamo per assurdo:

$$W < V = \sum_{i\in I} U_i \Rightarrow \exists U_i : \ U_i \not\subseteq W \Rightarrow$$

$$\underbrace{\Rightarrow}_{U_i \subseteq W \ \Leftrightarrow \ U_i = U_i \cap W} U_i \cap W < U_i$$

$$\begin{cases} U_i \cap W < U_i \\ U_i \text{ simple} \end{cases} \Rightarrow U_i \cap W = 0 \Rightarrow W + U_i = W \oplus U_i$$

$$W \oplus U_i \underbrace{=}_{\text{def. di W}} (U_{i_1} \oplus \cdots \oplus U_{i_t}) \oplus U_i$$

e questo e' in contrasto con la massimalita' di W.

□

Theorem 2.39. *Sia V un A-modulo, allora le seguenti condizioni sono equivalenti:*

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

Proof:

⟨1⟩ Dim. 2. $\Leftrightarrow$ 3.

Basta applicare il lemma [2.38,pg.10].

⟨2⟩ 1. $\Rightarrow$ 2.

Sia

$$W = \sum_{U \overset{A}{\leq} V \text{ semplice}} U$$

se $W = V$ abbiamo la tesi. Supponiamo allora $W < V$. Per la 1. abbiamo:

$$\exists U \overset{A}{\leq} V : \ V = U \oplus W \ \ (1)$$

$$W < V, \ \ (1) \Rightarrow U > 0 \underbrace{\Rightarrow}_{[2.34,\text{pg.}8]} \exists U_1 \overset{A}{\leq} U \text{ semplice}$$

Per definizione di W: $U_1 \subseteq W$

$$\Rightarrow 0 < U_1 \leq W \cap U \Rightarrow W \cap U \neq 0$$

assurdo contro $W \oplus U$

$\langle 3 \rangle$ 2. $\Rightarrow$ 1.

Per Hp:

$$V = \sum_{i \in I} U_i, \text{ con } \ U_i \ A\text{-sottomod semplice}$$

Fissato un $U \leq V$, sia W un massimale di

$$\{W \leq V \mid W \cap U = 0\}$$

Supponiamo per assurdo che $W + U \neq V$, allora

$$W + U \neq \sum_{i \in I} U_i \Rightarrow \exists U_i : \ U_i \not\subseteq W + U \Rightarrow U_i \cap W + U < U_i \underbrace{\Rightarrow}_{U_i \text{ e' semplice}} U_i \cap (W + U) = 0 \ \ (2)$$

$\langle 3.1 \rangle$ Dimostriamo che $(W + U_i) \cap U = 0$

Sia $u \in (W + U_i) \cap U$, ovvero

$$u = w + u_i, \ \ u \in U, \ w \in W, \ u_i \in U_i$$

$$\underbrace{u - w}_{\in U + W} = \underbrace{u_i}_{\in U_i} \underbrace{\Rightarrow}_{(2)} u_i = 0 \Rightarrow u = w \in U \cap W \underbrace{=}_{\text{per def. di } W} 0 \Rightarrow u = 0$$

$$\Rightarrow (W + U_i) \cap U = 0$$

Inoltre, $W + U_i > W$, infatti,

$$W + U_i = W \Rightarrow U_i \subseteq W \subseteq W + U \text{ assurdo contro } U_i \not\subseteq W + U$$

Quindi,

$$\begin{cases} W + U_i > W \\ (W + U_i) \cap U = 0 \end{cases} \Rightarrow \text{ assurdo contro la massimalita' di } W$$

□

2.2 Moduli semisemplici

Definition 2.40. Un V A-modulo che soddisfa il teorema [2.39,pg.10] si dira' *semisemplice*.

Proposition 2.41.

$$\begin{cases} V \ \textit{semisemplice} \\ U \overset{A}{\leq} V \end{cases} \Rightarrow U \ \textit{e' semisemplice}$$

In altre parole, i sottomoduli di moduli semisemplici sono a loro volta semisemplici.

Proof: Sia $W \leq U$,

$$V \text{ ssemplice} \underbrace{\Rightarrow}_{[2.39,\text{pg.}10]} \exists V_0 : \ V = W \oplus V_0 \Rightarrow$$

$$\Rightarrow U \cap V = U \cap W + U \cap V_0 \underbrace{=}_{W \subseteq U} W + (U \cap V_0)$$

$$U \underbrace{=}_{U \subseteq V} U \cap V = W + (U \cap V_0) \underbrace{=}_{W \cap V_0 = 0} W \oplus (U \cap V_0)$$

□

Proposition 2.42.

$$\begin{cases} V \text{ semisemplice} \\ U \overset{A}{\leq} V \end{cases} \Rightarrow V/U \text{ e' semisemplice}$$

In altre parole, i quozienti di moduli semisemplici sono a loro volta semisemplici.

Proof:

$$V \text{ ssemplice} \underbrace{\Rightarrow}_{[2.39,\text{pg.}10]} \exists W : \ V = W \oplus U$$

$$W \leq V, \ V \text{ ssemp.} \underbrace{\Rightarrow}_{[2.41,\text{pg.}11]} W \text{ ssemp.}$$

Considerando la proiezione naturale $\pi_W : V \longrightarrow W$ si ha il seguente A-isomorfismo:

$$V/U \simeq W$$

e per la semisemplicita' di W si ha la tesi. □

Proposition 2.43.

$$V = \sum_{i \in I} U_i, \ \text{con } U_i \text{ semisemplice} \Rightarrow V \text{ semisemplice}$$

In altre parole, la somma di moduli semisemplici e' un modulo semisemplice.

Proof: Basta usare il punto 2. del thm [2.39,pg.10]. □

Theorem 2.44. *Sia A una F-algebra, allora*

$$A^\circ \text{ e' semisemplice} \Leftrightarrow \text{Ogni } V \ A\text{-mod e' semisemplice}$$

Proof:

⟨1⟩ Dim. $\Rightarrow$

Sia V un A-mod e $v \in V$. L'applicazione

$$f : A \longrightarrow vA$$
$$a \mapsto va$$

e' un A-omomorfismo surriettivo, quindi

$$A^\circ \text{ ssemp.} \Rightarrow A/\ker f \text{ ssemp.} \Rightarrow A/\ker f \simeq vA \Rightarrow vA \text{ ssemp.}$$

$$\begin{cases} V = \sum_{v \in V} vA \\ vA \text{ ssemp.} \quad \forall v \in V \end{cases} \underbrace{\Rightarrow}_{[2.43,\text{pg.}12]} V \text{ ssemp.}$$

⟨2⟩ Dim. $\Leftarrow$

Basta scegliere $V = A^\circ$ per avere la tesi.

□

2.3 Algebre semisemplici

Definition 2.45. Sia A una F-algebra,

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

Proposition 2.46.

$$A \text{ e' semisemplice} \Leftrightarrow A = \sum_{I \overset{d}{\trianglelefteq} A^\circ,\ I \text{ semp.}} I = \sum_{I \overset{d}{\trianglelefteq} A \text{ minimale}} I$$

Proof:

$$A \text{ e' semisemplice} \Leftrightarrow A^\circ \text{ e' semisemplice} \underbrace{\Leftrightarrow}_{[2.39,\text{pg.}10]} A^\circ = \sum_{W \leq A^\circ,\ W \text{semp.}} W \quad (1)$$

Ricordando dall'esempio [2.19,pg.6] che i sottomoduli di A° sono gli ideali destri A, si ha

$$A^\circ \underbrace{=}_{(1)} \sum_{I \overset{d}{\trianglelefteq} A,\ I \text{ semp.}} I$$

Infine,

I semplice (come A° modulo) $\Leftrightarrow I$ non ha A°-sottomoduli $\Leftrightarrow I$ non ha ideali destri $\Leftrightarrow$

$\Leftrightarrow I$ e' un ideale destro minimale

□

Proposition 2.47. *Sia V un A-mod. Definiamo $A(V)$ come la somma di tutti gli ideali destri di A che sono A-isomorfi a V (nota[4]):*

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

Si ha,

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

Proof: Sia $\mathcal{I} = \left\{ I \overset{d}{\trianglelefteq} A^\circ :\ I \overset{A}{\simeq} V \right\}$.

Poiche' $A(V)$ e' formato da ideali destri di A, bastera' dimostrare che $A(V)$ e' un ideale sinistro di A, ovvero che

$$aI \subseteq A(V) \quad \forall a \in A\ \forall I \in \mathcal{I}$$

Fissiamo un a ed I. L'applicazione

$$l_a : A \longrightarrow A$$
$$x \mapsto ax$$

e' un A-omomorfismo. Osserviamo che

$$I \in \mathcal{I} \Rightarrow I \simeq V,\ V \text{ semplice} \Rightarrow I \text{ semplice}$$

Sia $f = l_{a|I} : I \longrightarrow aI$ la restrizione surriettiva di l_a ad I.
Esistono due possibilita':

- se $\operatorname{Im} f = 0$, allora $aI = 0 \subseteq A(V)$

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

- se $\operatorname{Im} f \neq 0$, allora
$$0 \leq \ker f < I \underbrace{\Rightarrow}_{I \text{ semplice}} \ker f = 0$$
f surriettiva
$$\Rightarrow f \text{ e' un } A\text{-isomorfismo} \Rightarrow V \simeq I \simeq aI \underbrace{\Rightarrow}_{\text{def. di } A(V)} aI \subseteq A(V)$$

In ogni caso, $aI \subseteq A(V)$. □

Proposition 2.48. *Sia A una F-algebra, si ha*
$$A \text{ semplice } \Rightarrow A \text{ semisemplice}$$

Proof: Sia $0 \neq I \overset{A}{\leq} A^\circ$ semplice, che esiste per la prop [2.34,pg.8], allora
$$0 < A(I) \underbrace{\trianglelefteq}_{[2.47,\text{pg.}13]} A \underbrace{\Rightarrow}_{A \text{ semplice}} A = A(I) \overset{\text{def}}{=} \sum_{I \overset{A}{\leq} A^\circ \text{ semp.}} I$$
e quindi per il teorema [2.39,pg.10] si ha la tesi. □

Lemma 2.49. *Sia V un A-mod.*
$$\begin{cases} V = \sum_{i \in I} V_i, \quad \text{con } V_i \text{ semplice } \forall i \in I \\ W \overset{A}{\leq} V \text{ semplice} \end{cases} \Rightarrow \exists i : \ W \overset{A}{\simeq} V_i$$

Proof: Per il teorema [2.39,pg.10] si ha
$$V = V_{i_1} \oplus \cdots \oplus V_{i_k}, \ \ V_{i_j} \text{ semplice}$$
Sia $\pi_{ij} : V \longrightarrow V_{ij}$ la proiezione naturale.
W semplice $\Rightarrow W \neq 0 \Rightarrow \exists w \in W \setminus \{0\} \Rightarrow \pi_{ij}(w) \neq 0$ per qualche j (1)
Sia $f = \pi_{ij|W} : W \longrightarrow V_{ij}$
$$\begin{cases} f \text{ e' un } A\text{-omomorfismo perche' e' una restrizione di un } A\text{-omomorfismo} \\ (1) \Rightarrow \operatorname{Im} f \neq 0 \\ W, V_{ij} \text{ semplici} \end{cases} \underbrace{\Rightarrow}_{\text{Schur [2.32,pg.8]}} W \overset{A}{\simeq} V_{ij}$$
□

Theorem 2.50. *di Wedderburn.*
Sia A una F-algebra semisemplice, allora

1. $$V \ A\text{-mod semplice } \Leftrightarrow \exists I \overset{d}{\trianglelefteq} A \text{ minimale: } V \overset{A}{\simeq} I$$
Ovvero, gli A-moduli semplici sono isomorfi ad A°-sottomoduli.

2. $\exists I_1, \ldots, I_k \overset{d}{\trianglelefteq} A$ *minimali tale che*
$$I_i \not\simeq I_j \ \ \forall i \neq j$$
$$I \overset{d}{\trianglelefteq} A \text{ minimale } \Rightarrow \exists i : \ I \overset{A}{\simeq} I_i$$
Ovvero, se consideriamo la relazione d'equivalenza indotta da $\overset{A}{\simeq}$, otteniamo solo k classi di A°-sottomoduli semplici.

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

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

5. $A(I_i) \trianglelefteq A$ *e' minimale* $\quad \forall i = 1, \ldots, k$

6.

$$\begin{aligned} \phi_i : A(I_i) &\longrightarrow \mathrm{End}_F(I_i) \underbrace{\simeq}_{algebra} F^{m_i \times m_i}, \quad m_i = \dim I_i \\ x \mapsto r_x : I_i &\longrightarrow I_i \\ u &\mapsto ux \end{aligned}$$

ϕ_i *e' un algebra-omomorfismo iniettivo.*
Inoltre, se F *e' algebricamente chiuso,* ϕ_i *e' biettiva e quindi si ha:*

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

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

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

Proof:
⟨1⟩ Dim. 1.

$$V \text{ semplice } \underbrace{\Leftrightarrow}_{\text{[2.37,pg.9]}} V \overset{A}{\simeq} A/I, \;\; I, \text{ con } I \overset{d}{\trianglelefteq} A$$

$$A \text{ semisemplice } \Leftrightarrow A^\circ \text{ semisemplice } \underbrace{\Rightarrow}_{\text{[2.39,pg.10]}} \exists J \leq A^\circ : \;\; A^\circ = I \oplus J \Rightarrow A^\circ / I \overset{A}{\simeq} J$$

$$\begin{cases} V \overset{A}{\simeq} A^\circ / I \overset{A}{\simeq} J \\ V \text{ semplice} \end{cases} \Rightarrow J \text{ semplice } \Leftrightarrow J \overset{d}{\trianglelefteq} A \text{ minimale}$$

⟨2⟩ Dim 2.

$$A^\circ \text{ ssemp } \underbrace{\Rightarrow}_{\text{[2.39,pg.10]}} A^\circ = J_1 \oplus \cdots \oplus J_m \text{ con } J_i \text{ semplice in } A^\circ \;\; (1)$$

$$I \leq A^\circ \text{ semplice }, \;\; (1) \underbrace{\Rightarrow}_{\text{[2.49,pg.14]}} \exists i : \; I \simeq J_i$$

Quindi ogni A°-sottomodulo semplice e' isomorfo a qualche J_i. Sia allora $\mathcal{I} = \{I_1, \ldots, I_k\} \subseteq \{J_1, \ldots, J_m\}$ l'insieme di addendi non isomorfi tra loro, ovvero, ovvero $I_i \not\simeq I_j \;\; \forall i, j : \; 1 \leq i < j \leq k$.

I vari $\{I_i\}$ sono i rappresentanti delle k classi d'equivalenza indotte dalla relazione $\overset{A}{\simeq}$.

⟨3⟩ Dim 3.

Dalla passo 2 sappiamo che

$$A = J_1 \oplus \cdots \oplus J_m \;\; (2)$$

Inoltre, ogni A-modulo semplice e' isomorfo a qualche I_j, con $1 \leq j \leq k$. In particolare, ogni J_h sara' isomorfo a qualche I_j. Associamo allora gli addendi della (2) in modo opportuno,

sfruttando l'associativita' della somma diretta:

$$B_i \stackrel{\text{def}}{=} \sum_{j=1,\dots,m,\ J_j \simeq I_i} J_j$$

$$A = B_1 \oplus \cdots \oplus B_k$$

B_i e' quindi la somma di tutti i J_j isomorfi a I_i. Ricordiamo che $A(I_i)$ e' la somma di tutti i sottomoduli di A° isomorfi ad I_i.
Dimostriamo che $B_i = A(I_i)$.
$\langle 3.1 \rangle$ $B_i \subseteq A(I_i)$
Per definizione di $A(\cdot)$ (vedi [2.47,pg.13]).
$\langle 3.2 \rangle$ $A(I_i) \subseteq B_i$

$$\begin{cases} A = B_1 \oplus \cdots \oplus B_k \\ B_i \underbrace{\leq}_{\text{passo 3.1}} A(I_i) \leq A \end{cases} \Rightarrow A(I_i) = B_i \oplus \left(\underbrace{A(I_i) \cap \bigoplus_{j \neq i,\ j=1,\dots,k} B_j}_{R} \right)$$

Supponiamo per assurdo che $R \neq 0$.
$R \neq 0 \Rightarrow \exists K \stackrel{A}{\leq} R$ semplice

$$\begin{cases} K \leq R \leq A(I_i) = \sum_{I \stackrel{d}{\trianglelefteq} A^\circ:\ I \stackrel{A}{\simeq} I_i} I \underbrace{=}_{I_i \text{ semplice}} \sum_{I \stackrel{d}{\trianglelefteq} A^\circ:\ I \stackrel{A}{\simeq} I_i,\ I \text{ semplice}} I \\ K \text{ semplice} \end{cases} \underbrace{\Rightarrow}_{[2.49,\text{pg.}14]} K \stackrel{A}{\simeq} I, \quad \text{per qualche addendo } I =$$

$$\Rightarrow K \simeq I \simeq I_i \quad (3)$$

$$\begin{cases} K \leq R \leq \bigoplus_{j \neq i,\ j=1,\dots,k} B_j = \bigoplus_{j \neq i,\ j=1,\dots,k} \sum_{i=1,\dots,m,\ J_i \simeq I_j} J_i \\ I_j, K \text{ semplici} \end{cases} \underbrace{\Rightarrow}_{[2.49,\text{pg.}14]} \exists j \neq i :\ K \simeq I_j \quad (3.1)$$

(3), (3.1) $\Rightarrow 0 \neq I_j \simeq K \simeq I_i \Rightarrow I_j \simeq I_i$
Assurdo.
$\langle 4 \rangle$ Dim. 4.
Nel passo precedente abbiamo dimostrato che

$$A = B_1 \oplus \cdots \oplus B_k, \quad (4)$$
$$\text{con } B_i = A(I_i) \underbrace{\trianglelefteq}_{I_i \text{ semplice, } [2.47,\text{pg.}13]} A$$

Quindi

$$B_i, B_j \trianglelefteq A \Rightarrow B_i B_j \subseteq B_i \cap B_j \underbrace{=}_{B_i, B_j \text{ addendi della somma diretta (4)}}$$

$$\Rightarrow b_i b_j = 0 \ \ \forall i \neq j \quad (5)$$

$$1_A \in A \underbrace{\Rightarrow}_{(4)} \exists! (e_1, \dots, e_k) \in B_1 \times \dots \times B_k :\ \ 1 = e_1 + \cdots + e_k \quad (6)$$

Moltiplicando a sinistra ambo i membri della (6) per b_j otteniamo:

$$b_j = b_j e_1 + \cdots + b_j e_k \underbrace{=}_{(5)} b_j e_j$$

analogamente moltiplicando a destra:

$$b_j = e_j b_j$$

Possiamo cosi' concludere che B_j e' un'algebra la cui unita' e' e_j, ovvero $1_{B_j} = e_j$.

Sempre dalla (5) abbiamo:

$$B_j \subseteq \mathrm{ann}_A(B_i) \underbrace{\subseteq}_{I_i \subseteq B_i} \mathrm{ann}_A(I_i) \Rightarrow \sum_{j\neq i} B_j \subseteq \mathrm{ann}_A(I_i) \quad (6.1)$$

e quindi

$$A = B_i \oplus \sum_{j\neq i} B_j \underbrace{\Rightarrow}_{(6.1)} \mathrm{ann}_A(I_i) = (\mathrm{ann}_A(I_i) \cap B_i) \oplus \sum_{j\neq i} B_j$$

Per avere la tesi basta quindi dimostrare che $\mathrm{ann}_A(I_i) \cap B_i = 0$.

$\langle 4.1 \rangle$ Dim. $\mathrm{ann}_A(I_i) \cap B_i = 0$

Sia $b \in \mathrm{ann}_A(I_i) \cap B_i = 0$. Per vedere che $b = 0$ basta utilizzare la prop [2.30,pg.7]:

$$b \in \mathrm{ann}_A(I_i) = \mathrm{ann}_A(I) \ \ \forall I \leq A^\circ : \ I \simeq I_i \quad (6)$$

$$B_i b = A(I_i)b = \sum_{I \leq A^\circ :\ I \simeq I_i} Ib \underbrace{=}_{(6)} 0 \Rightarrow b \in \mathrm{ann}_A(B_i) \quad (7)$$

$$b \in B_i \underbrace{\Rightarrow}_{(5)} B_j b = 0 \ \ \forall j \neq i \quad (7.1)$$

$$(7),\ (7.1) \Rightarrow B_i b = 0 \ \ \forall i = 1, \ldots, k \quad (7.2)$$

$$Ab = B_1 b \oplus \cdots \oplus B_k b \underbrace{=}_{(7.2)} 0 \Rightarrow 1_A b = 0 \Leftrightarrow b = 0$$

$\langle 5 \rangle$ Dim. 5.

Sappiamo gia' che

$$B_i = A(I_i) \trianglelefteq A$$

Resta da dimostrare la minimalita'. Supponiamo che $\exists C \trianglelefteq A : \ 0 < C < B_i$,

$$B_i \trianglelefteq A \Rightarrow B_i \leq A^\circ, \ \ A^\circ \text{ semisemplice } \Rightarrow B_i \text{ semisemplice}$$

$$C < B_i, \ \ B_i \text{ ssemp. } \Rightarrow \exists R \overset{A}{\leq} B_i : \ B_i = C \oplus R \quad (8)$$

$$C < B_i \Rightarrow R \neq 0$$

$$\begin{cases} R \overset{A}{\leq} B_i \Leftrightarrow R \overset{d}{\trianglelefteq} B_i \\ C \trianglelefteq A \end{cases} \Rightarrow RC \subseteq R \cap C \underbrace{=}_{(8)} 0 \Rightarrow Rc = 0 \ \ \forall c \in C \quad (8.1)$$

$$R \neq 0 \Rightarrow \exists J \leq R \text{ semplice}$$

$$J \subseteq R \subseteq B_i = \sum_{I \leq A^\circ :\ I \simeq I_i} I \underbrace{\Rightarrow}_{[2.49,\text{pg.}14]} J \simeq I_i$$

$$Jc = 0 \Rightarrow c \in \mathrm{ann}_A(J) \underbrace{=}_{J \simeq I_i} \mathrm{ann}_A(I_i)$$

$$c \in B_i$$

$$\Rightarrow c \in B_i \cap \mathrm{ann}_A(I_i) \underbrace{=}_{\text{passo 4}} 0$$

Per l'arbitrarieta' di c concludiamo che $C = 0$.

$\langle 6 \rangle$ Dim 6.

Innanzitutto, e' facile verificare che

1. ϕ_i e' ben posta: $r_x \in \mathrm{End}_F(I_i)$
2. ϕ_i e' un alg-omomorfismo

$\langle 6.1 \rangle$ ϕ_i e' iniettivo

$$\ker \phi_i = \{x \in B_i \mid r_x \equiv 0 \Leftrightarrow ux = 0 \ \ \forall u \in I_i \Leftrightarrow I_i x = 0 \Leftrightarrow x \in \mathrm{ann}_A(I_i)\} = B_i \cap \mathrm{ann}_A(I_i) \underbrace{=}_{\text{passo 4}} 0$$

Supponiamo che F sia algebricamente chiuso e consideriamo l'A-omomorfismo

$$l_x : I_i \longrightarrow I_i$$
$$u \mapsto xu$$

Poiche' I_i e' semplice, applicando il corollario di Schur (vedi [2.33,pg.8]) abbiamo

$$l_x = \lambda_x \mathrm{id}, \quad \text{per qualche } \lambda_x \in F$$

⟨6.2⟩ Dim. che ϕ_i e' surriettiva, ovvero che $\phi_i(B_i) = \mathrm{End}_F(I_i)$

PROOF SKETCH:Dimostreremo che $\phi_i(B_i) \overset{d}{\trianglelefteq} \mathrm{End}_F(I_i)$ e che $\mathrm{id} \in \phi_i(B_i)$ Chiaramente, se $I_i = 0$, ϕ_i e' surriettiva. Supponiamo $I_i \neq 0$.

$$B_i \trianglelefteq A \Rightarrow B_i I_i \subseteq B_i$$
$$I_i \neq 0 \Rightarrow e_i I_i \subseteq B_i I_i \Rightarrow 0 < B_i I_i$$
$$\Rightarrow 0 < B_i I_i \leq B_i \trianglelefteq A$$
$$I_i \overset{d}{\trianglelefteq} A,\ B_i \trianglelefteq A \Rightarrow B_i I_i \trianglelefteq A$$
$$\begin{cases} 0 < B_i I_i \leq B_i \\ B_i I_i \trianglelefteq A \\ B_i \trianglelefteq A \text{ minimale (per il passo 5)} \end{cases} \Rightarrow B_i I_i = B_i \quad (9)$$

Sia $b \in B_i$.

⟨6.2.1⟩ Dim. $\phi_i(b) f \in \phi_i(B_i)\ \ \forall f \in \mathrm{End}_F(I_i)$

$$b \in B_i \underbrace{=}_{(9)} B_i I_i \Rightarrow b = \sum_{j \in J} x_j y_j \text{ con } x_j \in B_i,\ y_j \in I_i\ \ \forall j \in J,\ \ |J| < +\infty$$

Per la linearita' di ϕ_i, basta considerare un solo addendo xy di b.

⟨6.2.1.1⟩ Dimostriamo che $\phi_i(xy) f = r_{xy} f = r_{xf(y)} = \phi_i(xf(y)) \in \phi_i(B_i)$

Si ha[5]:

$$(r_{xy} f)(z) = f(r_{xy}(z)) = f(zxy) = f(l_{zx}(y)) = f(\lambda_{zx} y) \underbrace{=}_{f \in \mathrm{End}_F} \lambda_{zx} f(y) = l_{zx}(f(y)) = zxf(y) = r_{xf(y)}(z)$$

⟨6.2.1.2⟩ Dim. $\mathrm{id} \in \phi_i(B_i)$

$$\phi_i(e_i) = r_{e_i}$$
$$r_{e_i}(z) = ze_i,\ \ z \in I_i \subseteq B_i,\ \ e_i = 1_{B_i} \Rightarrow ze_i = z \Rightarrow r_{e_i} = z$$
$$\Rightarrow r_{e_i} = \mathrm{id}$$

⟨6.2.1.3⟩ Q.E.D.

$$\begin{cases} \phi_i(B_i) \overset{d}{\trianglelefteq} \mathrm{End}_F(I_i) \\ 1_{\mathrm{End}_F(I_i)} = \mathrm{id} \in \phi_i(B_i) \end{cases} \Rightarrow \phi_i(B_i) = \mathrm{End}_F(I_i)$$

□

Corollary 2.51.

A algebra semisemplice $\Rightarrow$ *A e' somma (diretta) di algebre semplici*

Proof: Diretta conseguenza della 3. del teorema [2.50,pg.14]. □

[5]stiamo usando la composizione a sinistra, ovvero

$$fg(x) = g(f(x))$$

Corollary 2.52. *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.*

Proof: La 1. e' diretta conseguenza del teorema di Wedderburn (vedi [2.50,pg.14]). Dimostriamo la 2.:

$$1. \Rightarrow Z(A) \simeq Z(F^{n_1 \times n_1}) \oplus \cdots \oplus Z(F^{n_k \times n_k}) \Rightarrow \dim Z(A) = \sum_{i=1}^{k} \dim Z(F^{n_i \times n_i}) = \sum_{i=1}^{k} 1 = k$$

$$1. \Rightarrow \dim A = \sum_{i=1}^{k} \dim F^{n_i \times n_i} = \sum_{i=1}^{k} n_i^2$$

□

3 Algebra di un gruppo

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

Definition 3.1. Sia G un gruppo finito, F un campo. Sia FG l'insieme delle combinazioni lineari formali[6] 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:

$$0 \stackrel{\text{def}}{=} \sum_{g \in G} 0g$$

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

[6] 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 cosi' 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:

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

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

$$\left(\sum_{g\in G}\lambda_g g\right)\cdot\left(\sum_{g\in G}\mu_g g\right) \stackrel{\text{def}}{=} \sum_{g,h\in G}\lambda_g\mu_h gh=\sum_{z\in G}\left(\sum_{g,h\in G:\ gh=z}\lambda_g\mu_h\right)z \underbrace{=}_{h=g^{-1}z} \sum_{z\in G}\left(\sum_{g\in G}\lambda_g\mu_{g^{-1}z}\right)z$$

Proposition 3.2.

1. *FG e' un'algebra*
2. $\dim FG=|G|$

Proof: Per costruzione FG e' uno spazio vettoriale ed e' un anello unitario. Anche l'assioma delle algebre e' immediato:

$$a(\lambda b)=\lambda(ab)=(\lambda a)b$$

Infine, $\dim FG=|G|$ perche' G e' proprio la base dello spazio vettoriale FG. □

Definition 3.3. Diamo alcune definizioni per i gruppi. Sia G un gruppo finito e $X\subseteq G$,

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

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

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

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

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

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

Theorem 3.4. *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. $\dim Z(FG)=k$

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

Proof:
⟨1⟩ Dim. 1.

$$x \in Z(FG) \Leftrightarrow xy = yx \ \forall y \in FG \underbrace{\Leftrightarrow}_{G \text{ base di } FG} xh = hx \ \ \forall h \in G \Leftrightarrow h^{-1}xh = x \ \ (1)$$

$$x \in FG \Leftrightarrow x = \sum_{g\in G} \lambda_g g \Leftrightarrow h^{-1}xh = \sum_{g\in G} \lambda_g h^{-1}gh \underbrace{=}_{z=h^{-1}gh,\ g=hzh^{-1}} = \sum_{z\in G} \lambda_{hzh^{-1}} z \ \ (2)$$

$$\sum_{z\in G} \lambda_{hzh^{-1}} z \underbrace{=}_{(2)} h^{-1}xh \underbrace{=}_{(1)} x = \sum_{z\in G} \lambda_z z \underbrace{\Leftrightarrow}_{G \text{ base di } FG} \lambda_z = \lambda_{hzh^{-1}} \ \ \forall h, z \in G \ \ (3)$$

$$\lambda_z = \lambda_{hzh^{-1}} \ \ \forall h \in G \Leftrightarrow \lambda_z = \lambda_y \ \ \forall y \in \mathrm{cl}(z) \ \ (4)$$

Per la (4) possiamo porre: $\lambda_{\mathrm{cl}(z)} \overset{\text{def}}{=} \lambda_z$ (4.1)

$$x = \sum_{z\in G} \lambda_z z = \sum_{z\in G} \lambda_{\mathrm{cl}(z)} z \ \ (4.2)$$

Raggruppiamo per classe gli addendi nella (4.2):

Sia H l'insieme dei rappresentanti di $\mathrm{cl}(G)$

$$x = \sum_{h\in H} \lambda_{\mathrm{cl}(h)} \left(\sum_{z\in \mathrm{cl}(h)} z \right) = \sum_{h\in H} \lambda_{\mathrm{cl}(h)} \widehat{\mathrm{cl}(h)} = \sum_{i=1}^{k} \lambda_{K_i} \widehat{K_i}$$

Quindi

$$x = \sum_{i=1}^{k} \lambda_{K_i} \widehat{K_i}$$

Poiche' abbiamo usato solo doppie implicazioni, abbiamo implicitamente dimostrato la doppia inclusione:

$$Z(FG) = \left\langle \widehat{K_1}, \ldots, \widehat{K_k} \right\rangle$$

$\langle 2 \rangle$ Dim. 2.

Consideriamo una combinazione lineare nulla:

$$0 = \sum_{K\in \mathrm{cl}(G)} a_K \widehat{K} \underbrace{=}_{G=\bigcup K_j} \sum_{g\in G} a_{\mathrm{cl}(g)} g$$

Abbiamo cosi' ottenuto una combinazione lineare nulla di G. Poiche' G e' una base di FG, si deve avere:

$$a_{\mathrm{cl}(g)} = 0 \ \ \forall g \in G \Leftrightarrow a_K = 0 \ \ \forall K \in \mathrm{cl}(G)$$

□

Lemma 3.5. *Sia $f : V \longrightarrow W$ una applicazione lineare, con V, W FG-moduli, allora*

$$\vartheta : V \longrightarrow W$$
$$v \mapsto \sum_{g\in G} f(vg^{-1})g$$

e' un FG-omomorfismo.

In altre parole, sfruttando l'algebra FG, da una applicazione lineare f possiamo indurre un FG-omomorfismo.

Proof:

- ϑ e' lineare (per la linearita' di f)
- ϑ e' un FG-omo: $\vartheta(va) = \vartheta(v)a$, infatti

$$\vartheta(va) = \sum_{g\in G} f(vag^{-1})g = \sum_{g\in G} f(v(ga^{-1})^{-1})ga^{-1}a \underbrace{=}_{z=ga^{-1}} \left(\sum_{z\in G} f(vz^{-1})z \right) a = \vartheta(v)a$$

□

Lemma 3.6. *Siano V, W due spazi vettoriali e sia $\vartheta : V \longrightarrow W$ una applicazione lineare, con $W \leq V$.*

$$\vartheta^2 = \vartheta \Rightarrow V = \operatorname{Im}\vartheta \oplus \ker\vartheta$$

Proof:

$$v = \vartheta(v) + (v - \vartheta(v)) \quad (1)$$

$$\vartheta(v - \vartheta(v)) = \vartheta(v) - \vartheta^2(v) \underbrace{=}_{\vartheta^2=\vartheta} \vartheta(v) - \vartheta(v) = 0 \Rightarrow v - \vartheta(v) \in \ker\vartheta \quad (2)$$

$$(1), (2) \Rightarrow v \in \operatorname{Im}\vartheta + \ker\vartheta$$

Dimostriamo che la somma e' diretta:

$$w \in \operatorname{Im}\vartheta \cap \ker\vartheta \Rightarrow w = \vartheta(v) \quad (3)$$

$$0 \underbrace{=}_{w\in\ker\vartheta} \vartheta(w) = \vartheta^2(v) = \vartheta(v) \underbrace{\Rightarrow}_{(3)} w = 0$$

$$\Rightarrow \operatorname{Im}\vartheta \cap \ker\vartheta = 0$$

□

Theorem 3.7. *di Maschke.*

$$\operatorname{ch} F \not| |G| \Rightarrow FG \text{ } e' \text{ } semisemplice$$

dove ch F *e' la caratteristica del campo* F.

Proof:

$$FG \text{ ssemp} \quad \underbrace{\Leftrightarrow}_{thm[2.44,\text{pg.}12]} \quad \forall V \ FG\text{-mod} \text{ e' ssemp}$$

Prendiamo quindi un V FG-modulo arbitrario e dimostriamo che e' semisemplice, ovvero che $\forall W \overset{FG}{\leq} V \ \exists U \overset{FG}{\leq} V : \ V = U \oplus W$.

Sia $U_0 \leq V$ sottospazio vettoriale di V t.c. $V = W \oplus U_0$.

$\langle 1 \rangle$ Costruiamo un modulo $U \overset{FG}{\leq} V$ t.c. $V = W \oplus U$

Consideriamo la proiezione canonica:

$$\pi : V \longrightarrow W$$

$$w + u_0 \mapsto w$$

π e' lineare e surriettiva. Poiche' ch $F \not| |G|$, possiamo considerare la seguente applicazione lineare:

$$f : V \longrightarrow W$$

$$f(v) = \frac{1}{|G|}\pi(v)$$

Per il lemma [3.5,pg.21] possiamo costruire, a partire da f, la funzione $\vartheta : V \longrightarrow W$, che

risulta essere un FG-omomorfismo.

$$\vartheta \ FG\text{-omomorfismo} \Rightarrow U \overset{\text{def}}{=} \ker\vartheta \text{ e' un } FG\text{-modulo}$$

$$w \in W \overset{FG}{\leq} V \Rightarrow wg \in W \ \ \forall g \in G \underbrace{\Rightarrow}_{\pi_{|W}=\mathrm{id}} \pi(wg^{-1})g = wg^{-1}g = w \quad (1)$$

$$\vartheta(w) \underbrace{=}_{def.} \frac{1}{|G|}\sum_{g\in G}\pi(wg^{-1})g \underbrace{=}_{(1)} \frac{1}{|G|}\sum_{g\in G} w = \frac{|G|}{|G|}w = w \Rightarrow \vartheta_{|W} = \mathrm{id} \quad (1.1)$$

$$\vartheta(v) \in W \ \ \forall v \underbrace{\Rightarrow}_{(1.1)} \vartheta(\vartheta(v)) = \vartheta(v) \ \ \forall v \Leftrightarrow \vartheta^2 = \vartheta$$

Per il lemma [3.6,pg.22] abbiamo infine:

$$V = \operatorname{Im}\vartheta \oplus \ker\vartheta = W \oplus U$$

□

Corollary 3.8. *Grazie al teorema di Maschke, se* $\mathrm{ch}\, F \nmid |G|$*, possiamo applicare il teorema di Wedderburn all'algebra semisemplice* FG*. In piu', utilizzando il corollario [2.52,pg.19] e il teorema [3.4,pg.20] possiamo dire che:*

1. *Se* F *e' 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. $k = \dim Z(FG) = |\mathrm{cl}(G)|$
2. V *FG-mod* $\Rightarrow V \simeq m_1 I_1 \oplus \cdots \oplus m_k I_k$ *dove* $m_i \geq 0$, $m_i I_i = \underbrace{I_i \oplus \cdots \oplus I_i}_{m_i \ volte}$
3. $FG \simeq n_1 I_1 \oplus \cdots \oplus n_k I_k$

Proof:

⟨1⟩ Dim. 2.

$$\mathrm{ch}\, F \nmid |G| \underbrace{\Rightarrow}_{[3.7,\mathrm{pg}.22]} FG \text{ ssemp} \underbrace{\Rightarrow}_{[2.44,\mathrm{pg}.12]} V \text{ ssemp} \underbrace{\Rightarrow}_{[2.39,\mathrm{pg}.10]} V = \sum_{i\in I} V_i = V_{j_1} \oplus \cdots \oplus V_{j_k}, \quad \text{con } V_i \text{ semplice } \forall i \in I$$

Per il teorema di Wedderburn, $\forall i \in I \exists I \in \{I_1, \ldots, I_k\} : V_i \simeq I$, e quindi la tesi e' acquisita.

⟨2⟩ Dim. 3.

$$FG \text{ ssemp} \underbrace{\Rightarrow}_{[2.50,\mathrm{pg}.14]} FG \simeq B_1 \oplus \cdots \oplus B_k \underbrace{\simeq}_{\text{passo 1}} m_1 I_1 \oplus \cdots \oplus m_k I_k$$

$$m_i I_i \simeq B_i \simeq F^{n_i\times n_i} \Rightarrow n_i^2 = \dim B_i = \dim m_i I_i = m_i \dim I_i = m_i n_i \Rightarrow n_i = m_i$$

□

4 Rappresentazioni

Definition 4.1. Sia G un gruppo finito e F un campo. Chiameremo *rappresentazione* di G un qualsiasi omomorfismo di gruppi $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, F)$ [7].

La rappresentazione dell'algebra FG sara' un qualsiasi omomorfismo di algebre del tipo $\mathfrak{X}$:

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

$FG \longrightarrow F^{n\times n}$.
Poniamo inoltre

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

Proposition 4.2. *Se $\mathfrak{X}$ e' una rappresentazione di G, l'applicazione $\mathfrak{X}' : FG \longrightarrow F^{n\times n}$, ottenuta estendendo linearmente $\mathfrak{X}$, e' una rappresentazione di FG.*
Viceversa, se $\mathfrak{X}'$ e' una rappresentazione di FG, $\mathfrak{X} = \mathfrak{X}'_{|G}$ e' una rappresentazione di G.

Proof: Ci limitiamo ad osservare perche' $\mathfrak{X} = \mathfrak{X}'_{|G}$ e' ben definita, ovvero perche' $\mathfrak{X}(g) \in \mathrm{GL}(n, F)\ \ \forall g \in G$.

$$1 = \mathfrak{X}(1_G) = \mathfrak{X}(gg^{-1}) = \mathfrak{X}(g)\mathfrak{X}(g^{-1}) \Rightarrow \mathfrak{X}(g^{-1}) = (\mathfrak{X}(g))^{-1} \Rightarrow \mathfrak{X}(g) \in \mathrm{GL}(n, F)$$

□

Proposition 4.3. *Illustriamo adesso un metodo per ottenere un FG-modulo da una rappresentazione $\mathfrak{X}$ di FG, e viceversa.*

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*

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

e' un omomorfismo di gruppi. Scelta una base $B = [v_1, \ldots, v_n]$ 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 $M_B(r_g)$ e' 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,

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

Proof:
⟨1⟩ Dim. 1.
E' facile verificare che $V = F^n$ con l'operazione

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

rispetta gli assiomi dei moduli (vedi [2.16,pg.5]).
⟨2⟩ Dim. 2.

1. f e' ben definita, ovvero $r_g \in \mathrm{GL}(V)$:
$$r_g{}^{-1} = r_{g^{-1}}$$
$$r_g \text{ e' lineare}$$
2. Anche $\mathfrak{X}$ e' ben definita: le matrici associate ad isomorfismi sono invertibili, quindi $M_B(r_g) \in \mathrm{GL}(n, F)\ \forall g \in G$.
3. f e' un omomorfismo di gruppi
4. $\mathfrak{X}$ e' un omomorfismo di gruppi, infatti, per le proprieta' della matrice associata:
$$\mathfrak{X}(gh) = M_B(r_{gh}) = M_B(r_g r_h) = M_B(r_g)M_B(r_h) = \mathfrak{X}(g)\mathfrak{X}(h)$$

□

Proposition 4.4. *Applicando le due costruzioni esposte in [4.3,pg.24] in successione (usando la base canonica $B = \{e_1, \dots, e_n\}$), si riottiene il modulo o la rappresentazione di partenza.*

Proof:
⟨1⟩ Esaminiamo il caso
$$\text{Rappresentazione } \mathfrak{X} \longrightarrow \text{Modulo } v{\cdot}g \longrightarrow \text{Rappresentazione } \mathfrak{X}'$$
$$\mathfrak{X} \longrightarrow v{\cdot}g := v\mathfrak{X}(g) \longrightarrow \mathfrak{X}'(g) := \begin{bmatrix} e_1{\cdot}g \\ \vdots \\ e_n{\cdot}g \end{bmatrix} = \begin{bmatrix} e_1\mathfrak{X}(g) \\ \vdots \\ e_n\mathfrak{X}(g) \end{bmatrix} = \begin{bmatrix} (\mathfrak{X}(g))_1 \\ \vdots \\ (\mathfrak{X}(g))_n \end{bmatrix} = \mathfrak{X}(g)$$
⟨2⟩ Esaminiamo il caso
$$\text{Modulo } v{\cdot}g \in V = F^n \longrightarrow \text{Rappresentazione } \mathfrak{X} \longrightarrow \text{Modulo } v \bullet g \in V = F^n$$
$$v{\cdot}g \longrightarrow \mathfrak{X}(g) := \begin{bmatrix} [e_1{\cdot}g]_B \\ \vdots \\ [e_n{\cdot}g]_B \end{bmatrix} \longrightarrow v \bullet g := v\mathfrak{X}(g) \underbrace{=}_{v=\sum_{i=1}^n \lambda_i e_i} (\sum_{i=1}^n \lambda_i e_i)\mathfrak{X}(g) = \sum_{i=1}^n \lambda_i (e_i\mathfrak{X}(g)) =$$
$$= \sum_{i=1}^n \lambda_i [e_i{\cdot}g]_B = \left[\sum_{i=1}^n \lambda_i e_i{\cdot}g\right]_B = [v{\cdot}g]_B \underbrace{=}_{B \text{ base canonica},\ v \in V = F^n} v{\cdot}g$$

□

Definition 4.5. Siano $\mathfrak{X}, \mathfrak{Y} : G \longrightarrow \mathrm{GL}(n, F)$ due rappresentazioni. Diremo che $\mathfrak{X}, \mathfrak{Y}$ sono *simili* se:
$$\mathfrak{X} \sim \mathfrak{Y} \overset{\text{def}}{\Leftrightarrow} \exists M \in \mathrm{GL}(n, F) : \ \mathfrak{X}(g) = M^{-1}\mathfrak{Y}(g)M = \mathfrak{Y}(g)^M \ \ \forall g \in G$$

Remark 4.1. Se $\mathfrak{X}$ e' una rappresentazione, lo e' anche $\mathfrak{X}(g)^M$, in quanto la coniugazione e' un isomorfismo di gruppi.

Definition 4.6. Sia $\mathfrak{X}$ una rappresentazione.
$$\mathfrak{X} \text{ e' riducibile} \overset{\text{def}}{\Leftrightarrow} \exists M \in \mathrm{GL}(n, F) : \ \forall g \in G\ \mathfrak{X}(g) = M^{-1}\begin{bmatrix} X(g) & Y(g) \\ \underline{0} & Z(g) \end{bmatrix} M$$
$$\text{con } Z(g) \in F^{r \times r},\ X(g) \in F^{s \times s},\ Y(g) \in F^{s \times r}$$

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

Proposition 4.7. *Sia* $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, F)$ *una rappresentazione e* $V = F^n$ *il suo modulo indotto, allora*

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

Proof:

⟨1⟩ Dim. $\Rightarrow$

Supponiamo per assurdo che $\exists W$ V-sottomodulo t.c. $0 < W < V$.

Sia $\{w_{s+1}, \dots, w_n\}$ una base di W e completiamola ad una base $C = \{w_1, \dots, w_n\}$ di V.

Consideriamo quindi la rappresentazione $\mathfrak{X}'$ indotta dal modulo V secondo la base C:

$$\mathfrak{X}'(g) = M_C(r_g) \quad (1)$$

Prima di continuare notiamo che:

$$W \overset{FG}{\leq} V \Rightarrow w_i \cdot g \in W = \langle w_{s+1}, \dots, w_{s_n} \rangle \ \ \forall i \geq s+1 \quad (2)$$

$$(2) \Rightarrow w_i \cdot g = 0w_1 + \cdots + 0w_s + *w_{s+1} + \cdots + *w_n \Rightarrow [w_i \cdot g]_C = (\underbrace{0, \dots, 0}_{n \text{ volte}}, *, *, \dots, *)$$

(con $*$ indichiamo un qualsiasi coefficiente)

$$\mathfrak{X}'(g) = M_C(r_g) = \begin{bmatrix} [w_1 \cdot g]_C \\ \vdots \\ [w_n \cdot g]_C \end{bmatrix} \underbrace{=}_{\text{e' del tipo}} \begin{bmatrix} X & Y \\ \underline{0} & Z \end{bmatrix} \quad (3)$$

Infine, sfruttando la prop [4.3,pg.24] abbiamo

$$\mathfrak{X}(g) = M_B(r_g) \quad (4)$$

dove $B = \{e_1, \dots, e_n\}$ e' la base canonica di V.

Possiamo cosi' concludere:

$$\mathfrak{X}(g) \underbrace{=}_{(4)} M_B(r_g) \underbrace{\sim}_{\text{basta usare la mat. di passaggio}} M_C(r_g) \underbrace{=}_{(2)} \mathfrak{X}'(g) \underbrace{=}_{(4)} \begin{bmatrix} X & Y \\ \underline{0} & Z \end{bmatrix}$$

$$\Rightarrow \mathfrak{X}(g) \text{ non e' irriducibile}$$

Assurdo contro ipotesi.

⟨2⟩ Dim. $\Leftarrow$

Supponiamo per assurdo che $\mathfrak{X}$ sia riducibile, ovvero che

$$\mathfrak{X} \sim \mathfrak{Y} \equiv \begin{bmatrix} X & Y \\ \underline{0} & Z \end{bmatrix} \Leftrightarrow \exists M : \ \mathfrak{X}(g) = M^{-1}\mathfrak{Y}(g)M \quad (1)$$

$$\text{con } X \in F^{s \times s},\ Y \in F^{n-s \times n-s},\ \underline{0} \in F^{n-s \times s}$$

Sia $c_i = M_i$ la riga i di M.

Poiche' M e' invertibile, fissata $B = \{e_1, \dots, e_n\}$ esiste una sola base C di V tale che $M = P_{C \to B}$, dove $P_{C \to B}$ e' la matrice di passaggio da C a B. In particolare, poiche' B e' la base canonica si ha $C = \{c_1, \dots, c_n\}$.

Sia $h : \ s+1 \leq h \leq n$,

$(1) \Rightarrow \mathfrak{Y}(g)_{hi} = 0 \ \ \forall i \leq s \ \ (1.1)$

$$c_h \cdot g = c_h \cdot \mathfrak{X}(g) = c_h M^{-1}\mathfrak{Y}(g)M = c_h P_{B \to C}\mathfrak{Y}(g)P_{C \to B} = e_h \mathfrak{Y}(g)P_{C \to B} = \mathfrak{Y}(g)_h P_{C \to B} =$$

$$\underbrace{=}_{y := \mathfrak{Y}(g)_h} y \begin{bmatrix} [c_1]_B \\ \vdots \\ [c_n]_B \end{bmatrix} \underbrace{=}_{B \text{ canonica}} y \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} y_i c_{ij} \right) e_j = \sum_{i=1}^{n} y_i \left(\sum_{j=1}^{n} c_{ij} e_j \right) = \sum_{i=1}^{n} y_i c_i = \sum_{i=1}^{n} \mathfrak{Y}(g)_{hi} c_i =$$

$$\underbrace{=}_{(1.1)} \sum_{i=s+1}^{n} \mathfrak{Y}(g)_{hi} c_i \in \langle c_{s+1}, \dots, c_n \rangle$$

Abbiamo cosi' dimostrato che

$$c_h \cdot g \in \langle c_{s+1}, \ldots, c_n \rangle \ \ \forall h: \ s+1 \leq h \leq n, \ \ \forall g \in G$$

Quindi $W = \langle c_{s+1}, \ldots, c_n \rangle$ e' un FG-modulo, in particolare e' un sottomodulo di $\langle c_1, \ldots, c_n \rangle = V$, e questo e' assurdo contro la semplicita' di V.

□

Proposition 4.8. *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

Proof: La rappresentazione $\mathfrak{Y}$ indotta da V secondo la base $B = B_W \cup B_U = \{w_1, \ldots, w_r, u_1, \ldots, u_s\}$ e' una matrice a blocchi diagonale, infatti,

$$W \overset{FG}{\leq} V \Rightarrow w_i \cdot g \in W = \langle w_1, \ldots, w_r \rangle$$

$$U \overset{FG}{\leq} V \Rightarrow u_i \cdot g \in U = \langle u_1, \ldots, u_s \rangle$$

$$\mathfrak{Y}(g) = \begin{vmatrix} [w_1 \cdot g]_B \\ \vdots \\ [w_r \cdot g]_B \\ [u_1 \cdot g]_B \\ \vdots \\ [u_s \cdot g]_B \end{vmatrix} = \begin{bmatrix} \underline{W} & \underline{0} \\ \underline{0} & \underline{U} \end{bmatrix} = \begin{bmatrix} M_{B_W}(r_g) & \underline{0} \\ \underline{0} & M_{B_U}(r_g) \end{bmatrix}$$

$\mathfrak{Y}$ e $\mathfrak{X}$ sono simili perche' sono rappresentazioni indotte dallo stesso modulo V. □

Proposition 4.9. *Sia V, W due FG-moduli e sia $f: V \longrightarrow W$ una applicazione lineare tra essi, allora*

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

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 $M_{B,C}(f)$ e' la matrice associata a f.

Proof:
Sia $M = M_{B,C}(f)$

$$v_i \cdot g \in V = \langle B \rangle \Rightarrow v_i \cdot g = \sum_{j=1}^{n} x_{ij}(g) v_j \quad (1)$$

$$f(v_i) = \sum_{j=1}^{n} ([v_i]_B M)_j w_j = \sum_{j=1}^{n} (e_i M)_j w_j = \sum_{j=1}^{n} M_{ij} w_j \quad (2)$$

$$w_j \cdot g \in W = \langle C \rangle \Rightarrow w_j \cdot g = \sum_{k=1}^{n} y_{jk}(g) w_k \quad (3)$$

$$\mathfrak{X}(g) = M_B(r_g) \Rightarrow (\mathfrak{X}(g))_i = [v_i \cdot g]_B \underbrace{=}_{(1)} (x_{i1}(g), \ldots, x_{in}(g)) \Rightarrow (\mathfrak{X}(g))_{ij} = x_{ij}(g) \quad (4)$$

$$(\mathfrak{Y}(g))_{jk} \underbrace{=}_{(3)} y_{jk}(g) \quad (5)$$

f e' un FG-omo. $\Leftrightarrow f(vg) = f(v)g \ \ \forall g \in G \ \forall v \in V \Leftrightarrow f(v_i g) = f(v_i)g \ \ \forall g \in G \ \ \forall v_i \in B \Leftrightarrow$

$$\underbrace{\Leftrightarrow}_{(1),(2)} f\left(\sum_{j=1}^{n} x_{ij}(g) v_j\right) = \sum_{j=1}^{n} M_{ij} w_j g \underbrace{\Leftrightarrow}_{f \text{ lineare, } (3)} \sum_{j=1}^{n} x_{ij}(g) f(v_j) = \sum_{j=1}^{n} M_{ij} \left(\sum_{k=1}^{n} y_{jk}(g) w_k\right) \Leftrightarrow$$

$$\underbrace{\Leftrightarrow}_{(2)} \sum_{j=1}^{n} x_{ij}(g) \left(\sum_{k=1}^{n} M_{jk} w_k\right) = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} M_{ij} y_{jk}(g)\right) w_k \Leftrightarrow$$

$$\Leftrightarrow \sum_{k=1}^{n} \left(\sum_{j=1}^{n} x_{ij}(g) M_{jk}\right) w_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} M_{ij} y_{jk}(g)\right) w_k \Leftrightarrow$$

$$\underbrace{\Leftrightarrow}_{\{w_k\}_{k=1}^{n} \text{ base}} \sum_{j=1}^{n} x_{ij}(g) M_{jk} = \sum_{j=1}^{n} M_{ij} y_{jk}(g) \underbrace{\Leftrightarrow}_{(4),(5)} (\mathfrak{X}(g)M)_{ik} = (M\mathfrak{Y}(g))_{ik} \ \ \forall i,k \Leftrightarrow \mathfrak{X}(g)M = M\mathfrak{Y}(g)$$

□

Proposition 4.10. *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.

Proof:

$\mathfrak{X} \sim \mathfrak{Y} \Leftrightarrow Y = M^{-1}\mathfrak{X}M \Leftrightarrow \mathfrak{X}M = M\mathfrak{Y} \underbrace{\Leftrightarrow}_{[4.9,\text{pg.}27]}$ $f : V_1 \longrightarrow V_2$ e' un FG-omo.

dove f e' la mappa associata a M

$\exists M^{-1} \Leftrightarrow f$ isomorfismo

□

Proposition 4.11. *Supponendo di avere*

1. $\mathfrak{X}, \mathfrak{Y} : G \longrightarrow \mathrm{GL}(n, F)$ *rappresentazioni irriducibili di G*
2. F *campo algebricamente chiuso*

3. $\mathfrak{X}(g)M = M\mathfrak{Y}(g)\ \ \forall g \in G$ *per qualche* $M \in F^{n\times m}$

si ha

$$M = 0 \text{ oppure } M = \lambda I,\ \lambda \in F^*,\ \mathfrak{X} = \mathfrak{Y},\ n = m$$

Proof: Sia $V = F^n$ il modulo indotto da $\mathfrak{X}$, $W = F^m$ quello indotto da $\mathfrak{Y}$.

$$\mathfrak{X}, \mathfrak{Y} \text{ irriducibili} \underbrace{\Rightarrow}_{[4.7,\text{pg.}26]} V, W \text{ semplici } (1)$$

Sia $f : V \longrightarrow W$ l'applicazione lineare indotta da M rispetto alle basi canoniche B, C di V, W, ovvero:

$$f(e_i) = e_i M$$

Si ha

$$\begin{cases} f \text{ lineare} \\ \mathfrak{X}(g)M = M\mathfrak{Y}(g)\ \ \forall g \in G \end{cases} \underbrace{\Rightarrow}_{[4.9,\text{pg.}27]} f \text{ e' un } FG\text{-omomorfismo } (2)$$

$$(1),\ (2) \underbrace{\Rightarrow}_{[2.32,\text{pg.}8]} f = 0 \vee f \text{ isomorfismo}$$

Nel primo caso abbiamo $M = 0$. Nel secondo,

$$\dim V = \dim W \Rightarrow n = m \Rightarrow V = W \Rightarrow \mathfrak{X} = \mathfrak{Y}$$

$$\begin{cases} f : V \longrightarrow V \\ V \text{ semplice} \\ F \text{ alg. chiuso} \end{cases} \underbrace{\Rightarrow}_{[2.33,\text{pg.}8]} f = \lambda \mathrm{id} \Rightarrow e_i M = f(e_i) = \lambda e_i \Rightarrow M = \lambda I$$

□

Proposition 4.12.

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

Nota[8].

Proof: Basta applicare la prop [4.11,pg.28] con $\mathfrak{Y} = \mathfrak{X}$. □

Proposition 4.13.

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

Proof:

$$h \in Z(G) \Leftrightarrow hg = gh\ \ \forall g \in G \Rightarrow \mathfrak{X}(g)\underbrace{\mathfrak{X}(h)}_{M} = \underbrace{\mathfrak{X}(h)}_{M}\mathfrak{X}(g)\ \ \forall g \in G \underbrace{\Rightarrow}_{[4.11,\text{pg.}28]} \mathfrak{X}(h) = \lambda I$$

□

Proposition 4.14.

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

In questo caso, diremo che $\mathfrak{X}$ *e' lineare.*

[8] Questa proposizione puo' sembrare banale, ma la includiamo perche' sara' utile nel seguito

Proof:

$$G \text{ abeliano } \Rightarrow Z(G) = G \underbrace{\Rightarrow}_{[4.13,\text{pg.}29]} \mathfrak{X}(h) = \lambda_h I \ \ \forall h \in G$$

$$\mathfrak{X} \text{ irriducibile } \underbrace{\Rightarrow}_{[4.7,\text{pg.}26]} V = F^n \text{ modulo indotto e' semplice}$$

Sia $v \in V \setminus \{0\}$

$\langle v \rangle \overset{FG}{\leq} V$, infatti,

$$v \cdot g = v\mathfrak{X}(g) = v\lambda_g I = \lambda_g v \in \langle v \rangle$$

$$\begin{cases} 0 < \langle v \rangle \leq V \\ V \text{ semplice} \end{cases} \Rightarrow V = \langle v \rangle \Rightarrow \dim V = 1$$

□

Remark 4.2. Da adesso in poi considereremo solo l'algebra $\mathbb{C}G$, cosi' da assicurare la chiusura algebrica del campo e la condizione

$$\text{ch } \mathbb{C} \not| |G|$$

Theorem 4.15. *di Wedderburn per le rappresentazioni.*
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. $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ *rappr. 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. $\mathfrak{Y} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ *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, $\mathcal{X}_i(x) = \mathrm{Tr}\mathfrak{X}_i(x)$, $\mathrm{Tr}M$ *e' la traccia della matrice* M, $\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & \textit{altrimenti} \end{cases}$

Proof:

⟨1⟩ Dim. 1.

Sia V il modulo indotto da $\mathfrak{X}$.

$$\mathfrak{X} \text{ irrid. } \Rightarrow V \text{ semplice } \underbrace{\Rightarrow}_{[2.50,\text{pg.}14]} \exists! i : \ V \simeq I_i \underbrace{\Rightarrow}_{[4.10,\text{pg.}28]} \mathfrak{X} \sim \mathfrak{X}_i$$

⟨2⟩ Dim. 2.

Basta rileggere la [3.8,pg.23], considerando che $F = \mathbb{C}$.

⟨3⟩ Dim. 3.

Sia V il modulo indotto da $\mathfrak{Y}$.

$$V \ \mathbb{C}G\text{-mod} \underbrace{\Rightarrow}_{[3.8,\text{pg.}23]} V = m_1 I_1 \oplus \cdots \oplus m_k I_k = I_{i_1} \oplus \cdots \oplus I_{i_r} \ \ (1)$$

Ogni I_{i_j} induce una rappresentazione irriducibile $\mathfrak{Y}_{i_j}$,

$$\mathfrak{Y}_{i_j} \text{ irriducibile } \underbrace{\Rightarrow}_{1.} \mathfrak{Y}_{i_j} \sim \mathfrak{X}_{i'_j}$$

Infine, dalla (1), applicando la prop [4.8,pg.27] si ha

$$\mathfrak{Y} \sim \mathrm{diag}(\mathfrak{Y}_{i_1}, \dots, \mathfrak{Y}_{i_r}) \sim \mathrm{diag}(\mathfrak{X}_{i'_1}, \dots, \mathfrak{X}_{i'_r})$$

⟨4⟩ Dim. 4.

Sia $C = \{v_1, \dots, v_{n_i}\}$ la base di I_i dal quale si ottiene la rappresentazione $\mathfrak{X}_i$. Sappiamo gia' che preso $g \in G$,

$$\mathfrak{X}_i(g) = M_C(r_g)$$

vale pero' anche la seguente proposizione: preso $x \in \mathbb{C}G$,

$$\mathfrak{X}_i(x) = M_C(r_x) \quad (1)$$

infatti,

$x = \sum_{g \in G} \lambda_g g$

$$\mathfrak{X}(x) = \sum_{g \in G} \lambda_g \mathfrak{X}(g) = \sum_{g \in G} \lambda_g \begin{bmatrix} [v_1 \cdot g]_C \\ \vdots \\ [v_{n_i} \cdot g]_C \end{bmatrix} = \begin{bmatrix} \sum_{g \in G} \lambda_g [v_1 \cdot g]_C \\ \vdots \\ \sum_{g \in G} \lambda_g [v_{n_i} \cdot g]_C \end{bmatrix} = \begin{bmatrix} [v_1 \cdot \sum_{g \in G} \lambda_g g]_C \\ \vdots \\ [v_{n_i} \cdot \sum_{g \in G} \lambda_g g]_C \end{bmatrix} = \begin{bmatrix} [v_1 \cdot x]_C \\ \vdots \\ [v_{n_i} \cdot x]_C \end{bmatrix} = M_C(r_x)$$

Per il teorema di Wedderburn (vedi [2.50,pg.14]) avevamo i seguenti isomorfismi di algebre:

$$B_i \xrightarrow{\phi_i} \mathrm{End}_F(I_i) \xrightarrow{f} \mathbb{C}^{n_i \times n_i}$$
$$x \mapsto (r_x : I_i \longrightarrow I_i) \mapsto M_C(r_x)$$

Nota: f e' un isomorfismo di algebre.

Abbiamo,

$$(1) \Rightarrow \mathfrak{X}_{i|B_i} = \phi_i f \underbrace{\Rightarrow}_{f, \phi_i \text{ surriettive}} \mathfrak{X}_i(B_i) = \mathbb{C}^{n_i \times n_i}$$

Infine, sempre per il teorema di Wedderburn abbiamo che $B_i B_j = 0$ per $j \neq i$, quindi

$$x_j \in B_j \Rightarrow v_h x_j = 0 \ \ \forall h = 1, \dots, n_i$$

$$\mathfrak{X}_i(x_j) \underbrace{=}_{(1)} \begin{bmatrix} [v_1 \cdot x_j]_C \\ \vdots \end{bmatrix} = 0 \Rightarrow \mathfrak{X}_i(B_j) = 0$$

⟨5⟩ Dim. 5.

$$\mathfrak{X}_i(B_j) = 0 \ \forall i \neq j \Rightarrow \mathfrak{X}_i(e_j) = 0 \Rightarrow \mathcal{X}_i(e_j) = 0$$
$$e_i = 1_{B_i} \underbrace{\Rightarrow}_{\mathfrak{X}_{i|B_i} = \phi_i f \text{ e' un alg-omomorfismo}} \mathfrak{X}_i(e_i) = I \Rightarrow \mathcal{X}_i(e_i) = \mathcal{X}_i(1)$$

□

5 Caratteri

Definition 5.1. Sia $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ una rappresentazione. E sia definita la seguente funzione:

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

dove Tr e' la traccia[9] della matrice $\mathfrak{X}(g)$. A volte, per indicare che $\mathcal{X}$ e' la traccia di $\mathfrak{X}$ scriveremo

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

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

Proposition 5.2.

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. $\mathcal{X}(1) = n = \dim \mathfrak{X}$

Proof:
⟨1⟩ Dim. 1.

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

⟨2⟩ Dim. 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⟩ Dim. 3.

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

□

Definition 5.3. Sia G un gruppo finito.

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

$\mathcal{X}$ e' irriducibile $\overset{\text{def}}{\Leftrightarrow}$ $\exists \mathfrak{X}$ rappresentazione irriducibile t.c. $\mathcal{X} = \mathrm{Tr}\mathfrak{X}$

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

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

Remark 5.1. Sia $\mathcal{X} : G \longrightarrow \mathbb{C}$ una carattere di G. Poiche' $\mathrm{Tr} : \mathbb{C}^{n\times n} \longrightarrow \mathbb{C}$ e' una applicazione lineare, possiamo estendere per linearita' $\mathcal{X}$ su tutta l'algebra $\mathbb{C}G$:

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

[9] La traccia della matrice M e' l'elemento:

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

Lemma 5.4. *Siano date* $A, C \in F^{n\times n}$, $B, D \in F^{m\times m}$, *e poniamo*

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

dove $a_{ij} = A_{ij}$ *e' l'elemento di posto* i, j *di* A.
Nota: $A \otimes B$ *e' una matrice a blocchi.*
Si ha:

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

Proof:
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)

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

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

□

Proposition 5.5.

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

Proof:
⟨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

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

e' 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,

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

⟨2⟩ $\alpha\beta \in \text{ch } G$
Sia $Z = \mathfrak{X} \otimes \mathfrak{Y}$. Z e' una rappresentazione di G, infatti,

$$(\mathfrak{X} \otimes \mathfrak{Y})(ab) = \mathfrak{X}(ab) \otimes \mathfrak{Y}(ab) = (\mathfrak{X}(a)\mathfrak{X}(b)) \otimes (\mathfrak{Y}(a)\mathfrak{Y}(b)) \underbrace{=}_{[5.4,\text{pg.}33]} (\mathfrak{X}(a) \otimes \mathfrak{Y}(a))(\mathfrak{X}(b) \otimes \mathfrak{Y}(b)) = Z(a)Z(b)$$

Infine, dalla definizione di $\otimes$, e' chiaro che

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

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

□

Theorem 5.6.

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

dove $\mathcal{X}_i$ sono i caratteri dati dal teorema di Wedderburn per le rappresentazioni vedi [4.15,pg.30], e $k = |\mathrm{cl}(G)|$

Proof: Per ipotesi sappiamo gia' che vale l'inclusione $\supseteq$. Dimostriamo la $\subseteq$.

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

$$\mathfrak{X} \text{ irriducibile} \underbrace{\Rightarrow}_{[4.15,\text{pg.}30]} \exists! i: \quad \mathfrak{X} \sim \mathfrak{X}_i \underbrace{\Rightarrow}_{[5.2,\text{pg.}32]} \mathrm{Tr}\mathfrak{X} = \mathrm{Tr}\mathfrak{X}_i \Rightarrow \mathcal{X} = \mathrm{Tr}\mathfrak{X}_i \Leftrightarrow \mathcal{X} = \mathcal{X}_i$$

□

Definition 5.7. Sia G un gruppo. Definiamo l'insieme delle *funzioni di classe*:

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

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.
E' facile notare che $\mathrm{cf}(G)$ e' un $\mathbb{C}$-spazio vettoriale.

Proposition 5.8.

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

Ovvero i caratteri sono delle funzioni di classe.

Proof: Sia $\mathcal{X} \in \mathrm{ch}\ (G)$

$$\mathcal{X}(x^y) = \mathrm{Tr}\mathfrak{X}(x^y) = \mathrm{Tr}\left(\mathfrak{X}(y)^{-1}\mathfrak{X}(x)\mathfrak{X}(y)\right) \underbrace{=}_{[5.2,\text{pg.}32]} \mathrm{Tr}\mathfrak{X}(x) = \mathcal{X}(x)$$

□

Proposition 5.9. *Sia* $\mathrm{cl}(G) = \{K_1, \dots, K_k\}$, $k = |\mathrm{cl}(G)|$. *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

$$\{\delta_1, \dots, \delta_k\}$$

e' una base di $\mathrm{cf}(G)$.

Proof: E' chiaro che $\delta_i \in \mathrm{cf}(G)$.
$\langle 1 \rangle$ Dimostriamo che $\mathrm{cf}(G) = \langle \delta_1, \dots, \delta_k \rangle$

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

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

Quindi

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

Poiche' $\{K_i\}_i$ e' una partizione di G, possiamo concludere che

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

$\langle 2 \rangle$ $\delta_1, \dots, \delta_k$ 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

$$a_i = 0$$

□

Proposition 5.10. *Sia G un gruppo finito.*

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

Proof: Sia $k = |\mathrm{cl}(G)|$. Per il thm [5.6,pg.34] abbiamo $|\mathrm{Irr}(G)| = k$. Poiche'

$$\dim \mathrm{cf}(G) \underbrace{=}_{\text{[5.9,pg.34]}} k$$
$$\mathrm{Irr}(G) \subseteq \mathrm{ch}\,(G) \underbrace{\subseteq}_{\text{[5.8,pg.34]}} \mathrm{cf}(G)$$

basta dimostrare che $\mathrm{Irr}(G) = \{\mathcal{X}_1, \dots, \mathcal{X}_k\}$ e' un insieme di vettori linearmente indipendenti. Per il teorema [4.15,pg.30] 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'arbitrarieta' di j concludiamo che $a_j = 0 \;\; \forall j = 1, \dots, k$. □

Theorem 5.11. *Sia* $\mathrm{Irr}(G) = \{\mathcal{X}_1, \dots, \mathcal{X}_k\}$. *Si ha*

$$\mathcal{X} \in \mathrm{ch}\; G \Leftrightarrow \mathcal{X} = \sum_{i=1}^{k} m_i\mathcal{X}_k, \text{ } \textit{con } m_i \in \mathbb{N} \quad \forall i = 1, \dots, k$$
$$\textit{Inoltre,} \quad \exists i : \; m_i > 0$$

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

Proof:
$\langle 1 \rangle$ Dim. $\Leftarrow$
Per la proposizione [5.5,pg.33], la somma di caratteri e' ancora un carattere. Poiche' $\mathrm{Irr}(G) \subseteq \mathrm{ch}\ G$, la combinazione lineare intera $\sum_{i=1}^{k} m_i \mathcal{X}_i$ e' ancora un carattere.
$\langle 2 \rangle$ Dim. $\Rightarrow$

$$\mathcal{X} \in \mathrm{ch}\ G \Rightarrow \mathcal{X} = \mathrm{Tr}\mathfrak{X}$$
$$\mathfrak{X} \underbrace{\sim}_{[4.15,\mathrm{pg}.30]} \mathrm{diag}(\mathfrak{X}_{i_1}, \ldots, \mathfrak{X}_{i_r}) \text{ matrice diagonale a blocchi } \Rightarrow$$
$$\Rightarrow \mathcal{X} = \mathrm{Tr}\mathfrak{X} = \sum_{j=1}^{r} \mathrm{Tr}\mathfrak{X}_{i_r} = \sum_{j=1}^{r} \mathcal{X}_{i_r} \underbrace{=}_{\text{per opportuni } m_i \in \mathbb{N}} \sum_{i=1}^{k} m_i \mathcal{X}_i$$

Infine,

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

□

Definition 5.12. Sia $\mathfrak{X} : G \longrightarrow \mathrm{GL}(n, \mathbb{C})$ la rappresentazione indotta dal modulo $\mathbb{C}G^{\circ}$, secondo una qualsiasi base. Il carattere

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

e' il *carattere regolare*.

Proposition 5.13.

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

In particolare, abbiamo

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

Proof:
$\langle 1 \rangle$ Dim. 1.
Per il corollario [3.8,pg.23] , si ha

$$\mathbb{C}G^{\circ} \simeq n_1 I_1 \oplus \cdots \oplus n_k I_k \underbrace{\Rightarrow}_{[4.8,\mathrm{pg}.27]} \mathfrak{X} \sim \mathrm{diag}(\underbrace{\mathfrak{X}_1, \ldots, \mathfrak{X}_1}_{n_1 \text{ volte}}, \ldots, \underbrace{\mathfrak{X}_k, \ldots, \mathfrak{X}_k}_{n_k \text{ volte}}) \Rightarrow \mathcal{X} = \mathrm{Tr}\mathfrak{X} = \sum_{i=1}^{k} n_i \mathrm{Tr}\mathfrak{X}_i = \sum_{i=1}^{k} n_i \mathcal{X}_i \quad (2)$$

$$\mathcal{X}_i(1) \underbrace{=}_{[4.15,\mathrm{pg}.30]} n_i \quad (3)$$

$$(2), (3) \Rightarrow \mathcal{X} = \sum_{i=1}^{k} \mathcal{X}_i(1)\mathcal{X}_i \underbrace{=}_{[5.6,\mathrm{pg}.34]} \sum_{\mathcal{X} \in \mathrm{Irr}(G)} \mathcal{X}(1)\mathcal{X}$$

⟨2⟩ Dim. 2.

Come base di $\mathbb{C}G^\circ$ da cui indurre $\mathfrak{X}$ scegliamo direttamente $G = \{g_1, \dots, g_n\}$. La seguente dimostrazione sara' indipendente da questa scelta perche' la traccia Tr e' uguale 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 $\mathfrak{X}(g)$ e' una matrice di permutazione. Inoltre,

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

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

□

Theorem 5.14.

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

Remark 5.2. Questo e' il primo teorema che permette di ricavare informazioni sul gruppo G esaminando solo i caratteri irriducibili.

Proof:

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

$$|\mathrm{Irr}(G)| \underbrace{=}_{[5.6,\text{pg.}34]} |\mathrm{cl}(G)| = |G| \ \ (1)$$

$$\rho_G(1) \underbrace{=}_{[5.13,\text{pg.}36]} \sum_{\mathcal{X} \in \mathrm{Irr}(G)} \mathcal{X}(1)^2 = |G| = |\mathrm{Irr}(G)| \underbrace{\Leftrightarrow}_{\mathcal{X}(1) \in \mathbb{N},\ \mathcal{X}(1) \neq 0} \mathcal{X}(1) = 1 \ \ \forall \mathcal{X} \in \mathrm{Irr}(G)$$

□

Theorem 5.15. *Sia* $\mathcal{X} \in \mathrm{ch}\, G$

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

Proof:

⟨1⟩ Dim. ⇒

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

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

$$\alpha \in \text{ch } G \underbrace{\Rightarrow}_{\text{[5.11,pg.35]}} \alpha = \sum_{\mathcal{Y} \in \text{Irr}(G)} m_{\mathcal{Y}} \mathcal{Y}, \text{ con almeno un } m_{\mathcal{Y}} \in \mathbb{N}^* \quad (1)$$

Analogamente per β (1.1)

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

Sia $a_{\mathcal{Y}} = m_{\mathcal{Y}} + m'_{\mathcal{Y}}$. Per la (1) e (1.1), i casi sono due: almeno due $a_{\mathcal{Y}}$ sono distinti da zero, o almeno un $a_{\mathcal{Y}} \geq 2$. In ogni caso, poiche' $\mathcal{X} \in \text{Irr}(G)$, si ha un assurdo contro l'indipendenza lineare degli elementi di $\text{Irr}(G)$ (vedi [5.10,pg.35]).

$\langle 2 \rangle$ Dim. $\Leftarrow$

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

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

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

Poiche' $\mathcal{X}$ 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 $\mathcal{X}$ e' somma di almeno due caratteri. Questo e' assurdo contro ipotesi.

□

Theorem 5.16. *Siano $\mathfrak{X}, \mathfrak{Y}$ due rappresentazioni di G e $\mathcal{X}, \mathcal{Y}$ i rispettivi caratteri. Si ha*

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

Proof:

$\langle 1 \rangle$ Dim. $\Rightarrow$

vedi [5.2,pg.32]

$\langle 2 \rangle$ Dim. $\Leftarrow$

Procediamo analogamente a quanto abbiamo fatto nella dimostrazione di [5.11,pg.35].

$$\mathfrak{X} \underbrace{\sim}_{\text{[4.15,pg.30]}} \underbrace{\text{diag}(\mathfrak{X}_{i_1}, \dots, \mathfrak{X}_{i_r})}_{\text{matrice diagonale a blocchi}} \underbrace{\sim}_{\text{riordinando i blocchi}} \text{diag}(\underbrace{\mathfrak{X}_1, \dots, \mathfrak{X}_1}_{d_1 \text{ volte}}, \dots, \underbrace{\mathfrak{X}_k, \dots, \mathfrak{X}_k}_{d_k \text{ volte}}) \quad (1)$$

Nota: qualche d_i potrebbe essere nullo

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

Analogamente abbiamo:

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

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

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

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

□

Proposition 5.17. *Sia $g \in G$ e $\mathfrak{X}$ una rappresentazione di G. Sia $o(g) = m$ l'ordine di g. Si ha*

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

Proof:
$\langle 1 \rangle$ Dim. 1. e 2.
Sia $H = \langle g \rangle$ il gruppo generato da g e sia $\mathfrak{Y} = \mathfrak{X}_{|H}$.
H abeliano $\underbrace{\Leftrightarrow}_{[5.14,\text{pg.}37]}$ $\mathcal{Y}_1(1) = \ldots = \mathcal{Y}_k(1) = 1 \Rightarrow \mathcal{Y}_i(h) \in \mathbb{C} \;\; \forall h \in H \;\; (1)$

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

$\mathfrak{Y} \underbrace{\sim}_{[4.15,\text{pg.}30]} \underbrace{\mathrm{diag}(\mathfrak{Y}_{i_1}, \ldots, \mathfrak{Y}_{i_n})}_{\text{matrice diagonale a blocchi}}$ con $n = \dim \mathfrak{Y} = \mathfrak{Y}(1) = \mathfrak{X}(1), \;\; 1 \leq i_j \leq k \;\; \forall j = 1, \ldots, n$

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

$$\mathfrak{X}(g) = \mathfrak{Y}(g) \sim \mathrm{diag}(\xi_1, \ldots, \xi_n)$$

$$\mathcal{X}(g) = \mathrm{Tr}\mathfrak{X}(g) = \sum_{j=1}^{n} \xi_j$$

$\langle 2 \rangle$ Dim. 3.

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

$\langle 3 \rangle$ Dim. 4.

$$\xi_j^m = 1 \Rightarrow |\xi_j|^m = 1 \Rightarrow |\xi_j| = 1 \;\; (2)$$

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

$\langle 4 \rangle$ Dim. 5.

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

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

□

Proposition 5.18. *Sia $\mathcal{X} \in \mathrm{ch}\, G$. Poniamo:*

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

dove $\overline{\xi}$ e' 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 e' la trasposta della matrice A.

Proof: Sia

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

$\mathfrak{Y}$ e' una rappresentazione:
$\mathfrak{Y}(ab) = \mathfrak{X}((ab)^{-1})^\tau = \mathfrak{X}(b^{-1}a^{-1})^\tau = \big(\mathfrak{X}(b^{-1})\mathfrak{X}(a^{-1})\big)^\tau = \mathfrak{X}(a^{-1})^\tau\mathfrak{X}(b^{-1})^\tau = \mathfrak{Y}(a)\mathfrak{Y}(b)$
Inoltre,

$$\text{Tr}\mathfrak{Y}(g) = \text{Tr}\mathfrak{X}(g^{-1})^\tau = \text{Tr}\mathfrak{X}(g^{-1}) = \mathcal{X}(g^{-1}) \underbrace{=}_{[5.17,\text{pg.}39]} \overline{\mathcal{X}(g)} = \overline{\mathcal{X}}(g)$$

Quindi $\overline{\mathcal{X}} \in \text{ch } G$.
Infine,
$\mathcal{X}$ riducibile $\underbrace{\Leftrightarrow}_{[5.15,\text{pg.}37]}$ $\mathcal{X} = \alpha + \beta$, con $\alpha, \beta \in \text{ch } G \Leftrightarrow \overline{\mathcal{X}} = \underbrace{\overline{\alpha}}_{\in \text{ch } G} + \underbrace{\overline{\beta}}_{\in \text{ch } G}$, $\underbrace{\Leftrightarrow}_{[5.15,\text{pg.}37]}$ $\overline{\mathcal{X}}$ riducibile

□

Lemma 5.19. $\alpha, \beta \in \mathbb{C}$

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

Proof:
$|\alpha + \beta| = |\alpha| + |\beta| \Rightarrow |\alpha + \beta|^2 = |\alpha|^2 + |\beta|^2 + 2|\alpha||\beta|$ (1)
$|\alpha + \beta|^2 = (\alpha + \beta)\overline{(\alpha + \beta)} = \alpha\overline{\alpha} + \alpha\overline{\beta} + \beta\overline{\alpha} + \beta\overline{\beta} = |\alpha|^2 + |\beta|^2 + 2\alpha\overline{\beta}$

$\underbrace{\Rightarrow}_{(1)} |\alpha||\beta| = \alpha\overline{\beta} = \underbrace{\alpha\cdot\beta}_{\text{prodotto Hermitiano in } \mathbb{C}} \Rightarrow (\alpha\cdot\beta)^2 = (|\alpha||\beta|)^2 = \sqrt{(\alpha\cdot\alpha)}^2\sqrt{(\beta\cdot\beta)}^2 = (\alpha\cdot\alpha)(\beta\cdot\beta) \Leftrightarrow$

$\Leftrightarrow (\alpha\cdot\beta)^2 = (\alpha\cdot\alpha)(\beta\cdot\beta) \underbrace{\Rightarrow}_{\text{Disuguaglianza di Schwartz}} \alpha \parallel \beta \Leftrightarrow \exists\lambda \in \mathbb{R} : \ \alpha = \lambda\beta$

Nota: $\alpha \parallel \beta$ indica che α, β sono due vettori paralleli. □

Lemma 5.20. $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$, $t \geq 1$

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

Proof: Procediamo per induzione su t.
Case: $t = 1$
Vera.
Case: $t = 2$

$$|\alpha+\beta| = 2 = |\alpha| + |\beta| \underbrace{\Rightarrow}_{[5.19,\text{pg.}40]} \exists l \in \mathbb{R} : \ \alpha = l\beta$$

$$|l\beta + \beta| = 2 \Leftrightarrow \underbrace{|\beta|}_{=1} |l+1| = 2 \Leftrightarrow l+1 = \pm 2 \Leftrightarrow l = 1 \vee l = -3 \ \ (1)$$

$$\alpha = l\beta \Rightarrow \underbrace{|\alpha|}_{=1} = |l| \underbrace{|\beta|}_{=1} \Leftrightarrow |l| = 1 \Rightarrow l = \pm 1 \ \ (2)$$

$$(1), (2) \Rightarrow l = 1 \Rightarrow \alpha = \beta$$

CASE: $t \Rightarrow t+1$

$$t+1 = |\alpha_1 + \cdots + \alpha_t + \alpha_{t+1}| \leq |\alpha_1 + \cdots + \alpha_t| + |\alpha_{t+1}| \leq |\alpha_1| + \cdots + |\alpha_{t+1}| \underbrace{=}_{|\alpha_i|=1} t+1 \Rightarrow$$

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

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, poiche' $t \geq 3$,

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

□

Definition 5.21. Sia $\mathcal{X} \in \text{ch } G$. Definiamo il *nucleo* e il *centro* di $\mathcal{X}$:

$$\ker \mathcal{X} \stackrel{\text{def}}{=} \ker \mathfrak{X}$$

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

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

Theorem 5.22. *Sia $\mathfrak{X} : G \longrightarrow \text{GL}(n, \mathbb{C})$ 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. $Z(\mathcal{X}) = \{g \in G \mid \exists \lambda_g \in U_m : \ \mathfrak{X}(g) = \lambda_g I, \ \textit{con } m = o(g), \ U_m \textit{ gruppo delle radici } m\textit{-esime dell'unita'}\}$
4. $Z(\mathcal{X}) = \{g \in G \mid |\mathcal{X}(g)| = |\mathcal{X}(1)|\}$

Proof:

⟨1⟩ Dim. 1.

⟨1.1⟩ Dim. $\subseteq$

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

⟨1.2⟩ Dim. $\supseteq$

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

$$\mathcal{X}(g) \underbrace{=}_{[5.17,\text{pg.}39]} \xi_1 + \cdots + \xi_n = \mathcal{X}(1) = n$$

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

$$\underbrace{\Rightarrow}_{[5.20,\text{pg.}40]} \xi_i = \xi_1 \ \ \forall i = 1, \ldots, n \Rightarrow \mathcal{X}(g) = n\xi_1 = \mathcal{X}(1)\xi_1$$

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

$$\mathfrak{X}(g) \underbrace{\sim}_{[5.17,\text{pg.}39]} \operatorname{diag}(\xi_1, \ldots, \xi_n) = \operatorname{diag}(1, \ldots, 1) = I \Rightarrow \mathfrak{X}(g) = I \Rightarrow g \in \ker \mathfrak{X}$$

⟨2⟩ Dim. 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 poiche' G e' finito, questo basta per dimostrare che $Z(\mathcal{X}) \leq G$.

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

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

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

⟨3⟩ Dim. 3.

⟨3.1⟩ Dim. $\subseteq$

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⟩ Dim. $\supseteq$

Basta rileggere la definizione dei due insiemi.

⟨4⟩ Dim. 4.

⟨4.1⟩ Dim $\subseteq$

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

⟨4.2⟩ Dim $\supseteq$

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

$$\mathcal{X}(g) \underbrace{=}_{[5.17,\text{pg.}39]} \xi_1 + \cdots + \xi_n, \quad \text{con } n = \mathcal{X}(1)$$

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

$$\Rightarrow |\xi_1 + \cdots + \xi_m| = n \underbrace{\Rightarrow}_{[5.20,\text{pg.}40]} \xi_i = \xi_1 \ \ \forall i = 1, \ldots, n$$

$$\mathfrak{X}(g) \underbrace{\sim}_{[5.17,\text{pg.}39]} \operatorname{diag}(\xi_1, \ldots, \xi_n) = \operatorname{diag}(\xi_1, \ldots, \xi_1) = \xi_1 I$$

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

□

Proposition 5.23. *La funzione*

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

e' un omomorfismo di gruppi. Inoltre, e' facile verificare che

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

Proof:

$$g \in Z(\mathcal{X}) \underbrace{\Rightarrow}_{[5.22,\text{pg.}41]} \mathfrak{X}(g) = \lambda_g I \Rightarrow \mathcal{X}(g) = \lambda_g \mathcal{X}(1) \underbrace{\Rightarrow}_{\mathcal{X}(1)\neq 0} \lambda_g = \frac{\mathcal{X}(g)}{\mathcal{X}(1)} = \lambda(g)$$

Quindi $\lambda(g) = \lambda_g \quad \forall g \in Z(\mathcal{X})$

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

□

Proposition 5.24.

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

dove 1_G e' il carattere irriducibile banale:

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

Proof: 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.

$$\begin{cases} \ker\mathcal{X} \trianglelefteq G \\ \ker\mathcal{X} \neq G \\ G \text{ semplice} \end{cases} \Rightarrow \ker\mathcal{X} = 1 \underbrace{\Leftrightarrow}_{[5.23,\text{pg.}42]} \ker\lambda = 1$$

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

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. □

6 Interi algebrici

Definition 6.1. Sia $\alpha \in \mathbb{C}$

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

Sia R l'insieme di tutti gli interi algebrici.

Proposition 6.2.

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

Proof:

⟨1⟩ Dim $\supseteq$

Sia $z \in \mathbb{Z}$. z e' radice del polinomio $x - z$. Poiche' $\mathbb{Z} \subseteq \mathbb{Q}$ si ha la tesi.

⟨2⟩ Dim $\subseteq$

Sia $\alpha \in \mathbb{Q},\ f(x) \in \mathbb{Z}[x],\ f(\alpha) = 0$

$\alpha \in \mathbb{Q} \Rightarrow \alpha = \dfrac{r}{s},\ \ (r,s) = 1$

$f(\alpha) = 0 \Leftrightarrow \left(\dfrac{r}{s}\right)^n + a_{n-1}\left(\dfrac{r}{s}\right)^{n-1} + \cdots + a_0 = 0 \Leftrightarrow$

$$\underbrace{\Leftrightarrow}_{\text{moltiplicando per } s^n} \quad r^n + a_{n-1}r^{n-1}s + a_{n-2}r^{n-2}s^2 + \cdots + a_0 s^n = 0 \Leftrightarrow r^n = s\mu \Leftrightarrow s \Big/ r^n \quad (1)$$

Sia p un primo t.c. $p \Big/ s \underbrace{\Rightarrow}_{(1)} p \Big/ r$

Per l'arbitrarieta' di p si ha $s \Big/ r \underbrace{\Rightarrow}_{(r,s)=1} s = \pm 1 \Rightarrow \alpha = \pm r \in \mathbb{Z}$

□

Definition 6.3. Sia S un anello tale che $\mathbb{Z} \subseteq S$

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

ovvero,

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

Lemma 6.4. *Sia $Y = \{\alpha_1, \ldots, \alpha_t\} \subseteq R$, allora*

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

Proof:

$\alpha_i \in R \Rightarrow \exists f_i \in \mathbb{Z}[x],\ \exists n_i \in \mathbb{N}: \ \ \alpha_i^{n_i} = f(\alpha_i) = a_0 + a_1\alpha_i + \cdots + a_{n_i-1}\alpha_i^{n_i-1} \Rightarrow \alpha_i^{n_i} \in \langle Z \rangle_{\mathbb{Z}}$ (1)

dove abbiamo posto $Z = \left\{1, \alpha_i, \ldots, \alpha_i^{n_i-1}\right\}$

$\alpha_i^{n_i+1} = \alpha_i f(\alpha_i) = a_0\alpha_i + a_1\alpha_i^2 + a_2\alpha_i^3 + \cdots + a_{n_i-1}\underbrace{\alpha_i^{n_i}}_{\in \langle Z \rangle_{\mathbb{Z}}} \in \langle Z \rangle_{\mathbb{Z}}$

$\vdots$

$\alpha_i^m \in \langle Z \rangle_{\mathbb{Z}} \ \ \forall m \geq n_i$ (1.1)

Sia

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

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

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

Se esiste un i : $\ \ m_i + m_i'$, possiamo applicare la (1.1) per avere $\alpha_i^{m_i+m_i'} \in \langle Z \rangle_{\mathbb{Z}} \subseteq S$. Cosi' procedendo per ogni i, riusciamo ad abbassare tutti gli esponenti, ottenendo una combinazione lineare intera. Quindi $xy \in S$. □

Theorem 6.5. *Sia S un anello finitamente generato come $\mathbb{Z}$ modulo, tale che $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$. Allora,*

$$S \subseteq R$$

Proof:

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

$$Y = \{x_1, \ldots, x_n\}$$

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

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

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

Sia $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$(1) \Leftrightarrow sX = AX \underbrace{\Rightarrow}_{X \neq 0} X$ autovettore di A, $\quad s$ autovalore

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

Nota: $X \neq 0$ perche' altrimenti si avrebbe:

$$1 \in S = \langle Y \rangle_{\mathbb{Z}} \underbrace{=}_{X=0} \langle 0 \rangle_{\mathbb{Z}} \Rightarrow 1 = 0$$

assurdo. □

Corollary 6.6.
R e' un anello.

Proof: Sia $\alpha, \beta \in R$ e poniamo $Y = \{\alpha, \beta\}$. Per

$$Y \subseteq R \underbrace{\Rightarrow}_{[6.4,\text{pg.}44]} \exists S \text{ anello f.g. come } \mathbb{Z}\text{-modulo t.c. } \mathbb{Z} \subseteq S \subseteq \mathbb{C},\ Y \subseteq S \underbrace{\Rightarrow}_{[6.5,\text{pg.}44]} Y \subseteq S \subseteq R \underbrace{\Rightarrow}_{S \text{ anello}} \alpha - \beta,\ \alpha\beta \in S \subseteq R$$

□

Definition 6.7. Sia G un gruppo finito, poniamo

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

Proposition 6.8. *Sia $m = \exp(G)$, si ha*

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

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

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

Nota[10]

Proof:

$$\mathcal{X}(g) \underbrace{=}_{[5.17,\text{pg.}39]} \xi_1 + \cdots + \xi_f$$

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

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

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 un qualche $j \Rightarrow \xi_i \in \mathbb{Q}(\xi) \Rightarrow \mathcal{X}(g) \in \mathbb{Q}(\xi)$

□

Proposition 6.9. *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*

$a_{ijr} \in \mathbb{N}$

Proof: Per la proposizione [3.4,pg.20], $B = \left\{\widehat{K_1}, \dots, \widehat{K_k}\right\}$ e' un base di $Z(\mathbb{C}G)$. Posto $K_r = \{g_{r1}, \dots, g_{rt_r}\}$, si ha

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

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

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

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

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

Inoltre, $a_{ijr} = a_{g_{rh}}\ \ \forall h = 1, \dots, t_r \Leftrightarrow a_{ijr} = a_{x_r}\ \ \forall x_r \in K_r$ (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 $g_{ihjs} = g_{ih}g_{js} \in G$

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

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

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

$a_g = b_g$ (4)

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

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

$$\Rightarrow a_{ijr} = |\{(x_i, x_j) \mid x_i x_j = x_r,\ \ x_i \in K_i,\ x_j \in K_j\}|$$

□

Proposition 6.10. *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. $\omega_{\mathcal{X}}(\widehat{K}) = \dfrac{\mathcal{X}(\widehat{K})}{\mathcal{X}(1)}$

Proof:
⟨1⟩ Dim. 1.

$$\widehat{K} \in \left\{\widehat{K}_1, \dots, \widehat{K}_k\right\} \underbrace{\subseteq}_{[3.4,\text{pg.}20]} Z(\mathbb{C}G) \Rightarrow x\widehat{K} = \widehat{K}x \ \ \forall x \in \mathbb{C}G \Rightarrow \mathfrak{X}(g\widehat{K}) = \mathfrak{X}(\widehat{K}g) \ \ \forall g \in G \Leftrightarrow$$

$$\Leftrightarrow \mathfrak{X}(\widehat{K})\mathfrak{X}(g) = \mathfrak{X}(g)\mathfrak{X}(\widehat{K}) \ \ \forall g \in G \underbrace{\Rightarrow}_{[4.12,\text{pg.}29]} \mathfrak{X}(\widehat{K}) = \lambda I$$

E ponendo $\omega_{\mathfrak{X}}(\widehat{K}) = \lambda$ si ha la tesi.
⟨2⟩ Dim. 2.

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

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

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

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

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

ovvero, $\omega_{\mathcal{X}}(\widehat{K})$ e' indipendente dalla scelta della rappresentazione.
⟨3⟩ Dim. 3.
Basta rileggere la (2).

□

Theorem 6.11. *Dato $\mathcal{X} \in \mathrm{Irr}(G)$, si ha*

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

Proof:
⟨1⟩ Dim. 1.

Sia $x \in Z(\mathbb{C}G)$, per la prop [3.4,pg.20] abbiamo

$x = \sum_{i=1}^{k} a_K \widehat{K}$

$$\mathfrak{X}(x) = \sum_{i=1}^{k} a_K \mathfrak{X}(\widehat{K}) \underbrace{=}_{[6.10,\text{pg.}46]} \sum_{i=1}^{k} a_K \omega_{\mathfrak{X}}(\widehat{K}) I = \left(\sum_{i=1}^{k} a_K \omega_{\mathfrak{X}}(\widehat{K}) \right) I \overset{\text{def}}{=} \omega_{\mathfrak{X}} \left(\sum_{i=1}^{k} a_K \widehat{K} \right) I = \omega_{\mathfrak{X}}(x) I$$

In definitiva, $\mathfrak{X}(x) = \omega_{\mathfrak{X}}(x) I \ \ \forall x \in Z(\mathbb{C}G)$ (1)

$\mathfrak{X} : \mathbb{C}G \longrightarrow \mathbb{C}^{n \times n}$ omomorfismo di algebre $\underbrace{\Rightarrow}_{(1)} \omega_{\mathfrak{X}}(x)$ omomorfismo di algebre

⟨2⟩ Dim. 2.

Sia S l'insieme cosi' definito:

$$S = \left\langle \left\{ \omega_{\mathcal{X}}(\widehat{K}) \mid K \in \mathrm{cl}(G) \right\} \right\rangle_{\mathbb{Z}}$$

⟨2.1⟩ S e' un anello finitamente generato come $\mathbb{Z}$ modulo e tale che $\mathbb{Z} \subseteq S \subseteq \mathbb{C}$

Per definizione S e' finitamente generato come $\mathbb{Z}$ modulo.

⟨2.1.1⟩ $\mathbb{Z} \subseteq S$

$$\{1\} \in \mathrm{cl}(G) \Rightarrow \widehat{\{1\}} = 1$$

$$\omega_{\mathcal{X}}(1) = \omega_{\mathcal{X}}(\widehat{\{1\}}) \underbrace{=}_{[6.10,\text{pg.}46]} \frac{\mathcal{X}(\widehat{\{1\}})}{\mathcal{X}(1)} = \frac{\mathcal{X}(1)}{\mathcal{X}(1)} = 1$$

$$\Rightarrow 1 \in S \underbrace{\Rightarrow}_{S \text{ f.g. come } \mathbb{Z}\text{-mod}} \mathbb{Z} \subseteq S$$

⟨2.1.2⟩ $(S, +)$ e' un gruppo abeliano

Direttamente dalla definizione.

⟨2.1.3⟩ S e' chiuso rispetto al prodotto

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

$$ab = \sum_{i,j} a_i b_j \omega_{\mathcal{X}}(\widehat{K}) \omega_{\mathcal{X}}(\widehat{K'}) \underbrace{=}_{\omega_{\mathcal{X}} \text{ omo.}} \sum_{i,j} a_i b_j \omega_{\mathcal{X}}(\widehat{K}\widehat{K'}) \underbrace{=}_{[6.9,\text{pg.}46]} \sum_{i,j} a_i b_j \omega_{\mathcal{X}} \left(\sum_{h=1}^{k} c_h \widehat{K_h} \right) =$$

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

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

⟨2.2⟩ Q.E.D.

Per il passo precedente e per il teorema [6.5,pg.44], si ha

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

□

7 Teorema di Burnside

Lemma 7.1. *Sia $\mathcal{X} \in \mathrm{Irr}(G)$, $x \in G$ e $K = \mathrm{cl}(x)$. Si ha*

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

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

$$\mathcal{X}(x) \underbrace{=}_{[5.17,\text{pg.}39]} \xi^{a_1} + \cdots + \xi^{a_n}$$

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

Per la [6.8,pg.45] si ha: $\mathcal{X}(x) \in \mathbb{Q}_e \cap R$, con $e = \exp(G)$ (1)

Sia $\omega \in \mathbb{C}$: $U_e = \langle \omega \rangle$, quindi $\xi = \omega^j$, per qualche j (1.1)

Supponiamo che $x \notin Z(\mathcal{X})$ e dimostriamo che $\mathcal{X}(x) = 0$.

$$x \notin Z(\mathcal{X}) \underbrace{\Rightarrow}_{[5.22,\text{pg.}41],[5.17,\text{pg.}39]} |\mathcal{X}(x)| < \mathcal{X}(1) = n \quad (2)$$

$$\frac{|\mathcal{X}(x)|}{\mathcal{X}(1)} < 1 \quad (2.1)$$

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 $Q \subseteq \mathbb{Q}(\omega)$ e' ciclotomica, ed e' quindi una estensione di Galois. Per il teorema fondamentale della teoria di Galois, segue che

$$\mathbb{Q}_e^{\mathcal{G}} = \mathbb{Q} \quad (3)$$

dove $\mathbb{Q}_e^{\mathcal{G}} = \{q \in \mathbb{Q}_e \mid \sigma(q) = q \ \ \forall \sigma \in \mathcal{G}\}$

Sia $\sigma \in \mathcal{G}$. Poiche' σ e' un automorfismo di $\mathbb{Q}_e$, possiamo affermare le seguenti proposizioni:

$$\alpha^k = 1 \Rightarrow \sigma(\alpha)^k = 1 \quad (4)$$

$$\alpha \in R \Rightarrow \sigma(\alpha) \in R, \text{ infatti:} \quad (5)$$

$$\alpha \in R \Rightarrow \exists f \in \mathbb{Z}[x] \text{ monico t.c. } f(\alpha) = 0$$

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0 \Rightarrow \sigma(\alpha) \in R$$

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

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

$$x \in K, \ \mathcal{X} \in \text{Irr}(G) \underbrace{\Rightarrow}_{[6.10,\text{pg.}46]} |K|\frac{\mathcal{X}(x)}{\mathcal{X}(1)} = \omega_{\mathcal{X}}(\widehat{K}) \underbrace{\in}_{[6.11,\text{pg.}47]} R$$

$$\Leftrightarrow a\omega_{\mathcal{X}}(\widehat{K}) + b\mathcal{X}(x) = \frac{\mathcal{X}(x)}{\mathcal{X}(1)} \quad (6)$$

$$\omega_{\mathcal{X}}(\widehat{K}) \in R, \ \mathcal{X}(x) \in R \Rightarrow \frac{\mathcal{X}(x)}{\mathcal{X}(1)} \in R \quad (6.1)$$

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

$$(2.1) \Rightarrow |\alpha| < 1 \quad (2.2)$$

$$(6.1) \Rightarrow \alpha \in R \underbrace{\Rightarrow}_{(5)} \sigma(\alpha) \in R \ \ \forall \sigma \in \mathcal{G} \quad (6.2)$$

$$\sigma(\alpha) = \frac{\sigma(\mathcal{X}(x))}{\sigma(\mathcal{X}(1))} \underbrace{=}_{\mathcal{X}(1)=n\in\mathbb{Q},\ (3)} \frac{\sigma(\mathcal{X}(x))}{\mathcal{X}(1)}$$

$$\sigma(\mathcal{X}(x)) = \sigma(\xi)^{a_1} + \cdots + \sigma(\xi)^{a_n} \underbrace{=}_{(4)} \zeta^{a_1} + \cdots + \zeta^{a_n}, \text{ con } \langle \zeta \rangle = U_m$$

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

$$|\sigma(\alpha)| = \frac{|\mathcal{X}(x)|}{|\mathcal{X}(1)|} \leq \frac{n}{n} = 1 \quad (7)$$

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

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

abbiamo

$$\sigma = \mathrm{id} \Rightarrow |\sigma(\alpha)| = |\alpha| \underbrace{<}_{(2.2)} 1 \quad (2.3)$$

$$|\beta| = \prod_{\sigma\in\mathcal{G}} |\sigma(\alpha)| = |\alpha| \prod_{\sigma\in\mathcal{G}:\ \sigma\neq\mathrm{id}} |\sigma(\alpha)| \underbrace{<}_{(2.3)} 1 \quad (7.1)$$

Infine,

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

$$(6.2) \underbrace{\Rightarrow}_{R\text{ e' un anello}} \beta \in R$$

$$\Rightarrow \beta \in R\cap\mathbb{Q} \underbrace{=}_{[6.2,\text{pg.}43]} \mathbb{Z} \underbrace{\Rightarrow}_{(7.1)} \beta = 0 \Rightarrow \exists\sigma\in\mathcal{G}: \ \ \sigma(\alpha) = 0 \underbrace{\Leftrightarrow}_{\sigma\text{ e' biettiva}} \alpha = \sigma^{-1}(0) = 0$$

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

□

Theorem 7.2. *Sia $x \in G$, allora*

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

Questo teorema coinvolge solamente la teoria dei gruppi, eppure, non si conosce attualmente una sua dimostrazione che non faccia ricorso alla teoria dei caratteri.

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

$$\begin{cases} |\mathrm{cl}(x)| = p^a > 1 \Rightarrow G \text{ non e' abeliano} \\ G \text{ semplice} \\ \mathcal{X} \in \mathrm{Irr}(G)\setminus\{1_G\} \end{cases} \underbrace{\Rightarrow}_{[5.24,\text{pg.}43]} Z(\mathcal{X}) = \{1\} \quad (0)$$

$$\rho_G(x) \underbrace{=}_{[5.13,\text{pg.}36]} \sum_{\mathcal{X}\in\mathrm{Irr}(G)} \mathcal{X}(1)\mathcal{X}(x) \underbrace{=}_{x\neq 1} 0 \quad (1)$$

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

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

Sia $K = \mathrm{cl}(x)$,

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

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

$$B = 0,\ (2),\ (1) \Rightarrow 0 = \rho_G(x) = 1 + \sum_{\mathcal{X} \in \mathrm{Irr}(G)\setminus\{1_G\},\ p/\mathcal{X}(1)} \mathcal{X}(1)\mathcal{X}(x) \Leftrightarrow$$

$$\Leftrightarrow 1 + p \underbrace{\sum_{\mathcal{X} \in \mathrm{Irr}(G)\setminus\{1_G\},\ p/\mathcal{X}(1)} \underbrace{\frac{\mathcal{X}(1)}{p}}_{\in \mathbb{Z}} \underbrace{\mathcal{X}(x)}_{\in R}}_{= \gamma \in R} = 0 \Leftrightarrow \gamma = -\frac{1}{p} \in R \cap \mathbb{Q} \underbrace{=}_{[6.2,\mathrm{pg}.43]} \mathbb{Z} \Rightarrow p = \pm 1$$

Assurdo, in quanto p e' un primo. □

Theorem 7.3. *(Burnside)*

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

Proof: Distinguiamo due casi:
Case: $p = q$

$$|G| = p^{a+b},\ a, b > 0 \Rightarrow G\ p\text{-gruppo },\ |G| > 1 \Rightarrow$$
$$\Rightarrow \exists \text{ una catena di sottogruppi normali non banali } \Rightarrow G \text{ non e' semplice}$$

Case: $p \neq q$

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,

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

Se $\nexists x \in Z(P) : \ |\mathrm{cl}_G(x)| > 1$, allora

$$x \in Z(G) \Leftrightarrow |\mathrm{cl}_G(x)| = 1 \ \ (*)$$
$$\forall x \in Z(P) \ \ |\mathrm{cl}_G(x)| = 1 \Rightarrow Z(P) \subseteq Z(G)$$
$$1 \neq Z(P) \subseteq Z(G) \trianglelefteq G \Rightarrow Z(P) \trianglelefteq G \ \ (**)$$
$$Z(P) = G \Rightarrow Z(G) = G \Rightarrow G \text{ abeliano } \Rightarrow P \trianglelefteq G \underbrace{\Rightarrow}_{1 \neq P \neq G} G \text{ non semplice}$$
$$1 \neq Z(P) \neq G \underbrace{\Rightarrow}_{(**)} G \text{ non semplice}$$

Possiamo quindi supporre che $\exists x \in Z(P) : \ |\mathrm{cl}_G(x)| > 1$. Sia $C_G(x)$ il centralizzante di x in

G, allora

$$P \underbrace{\leq}_{x\in Z(P)} C_G(x) \trianglelefteq G \Rightarrow \frac{|C(x)|}{|P|}\left|\frac{G}{C(x)}\right| = \frac{|G|}{|P|} \Rightarrow \left|\frac{G}{C(x)}\right| \Big/ \frac{|G|}{|P|} = q^b \quad (2)$$

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

$$|\mathrm{cl}(x)| = q^c \underbrace{>}_{\text{per ipotesi}} 1, \quad x \neq 1 \underbrace{\Rightarrow}_{\text{[7.2,pg.50]}} G \text{ non e' semplice}$$

□

Corollary 7.4.

$$|G| = p^a q^b, \quad p, q \textit{ primi } \Rightarrow G \textit{ e' risolubile}$$

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

$$G \text{ } p\text{-gruppo } \Rightarrow G \text{ e' risolubile}$$

Supponiamo quindi $a, b > 0$. Sia $1 \leq N < G$ un sottogruppo normale di G. Se per assurdo $N = 1$, G sarebbe semplice. Questo e' pero' in contrasto con il teorema [7.3,pg.51]. Quindi,

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

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

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

□

8 *

Index
*, 53

A(V), 13
A-omomorfismo, 7
Algebra di un gruppo, 19
Algebre, 1
Algebre semisemplici, 13
annullatore, 6

Burnside
    teorem di, 51

carattere, 32
carattere regolare, 36
Caratteri, 32

funzioni di classe, 34

Interi algebrici, 43

Maschke
    teorema di, 22
Moduli, 5
Moduli semisemplici, 11
modulo, 5
    semisemplice, 11
    semplice, 6
modulo regolare, 6

Preliminari, 1

rappresentazione, 23
rappresentazione lineare, 29
Rappresentazioni, 23
rappresentazioni
    irriducibili, 25
    simili, 25

Schur, teorema di, 8

Teorema di Burnside, 48

Wedderburn
    teorema di, 14