Alma Mater Studiorum · Università di Bologna

Dipartimento di Fisica e Astronomia "Augusto Righi"
Corso di Laurea in Fisica

Rappresentazioni del Gruppo Simmetrico S_n e Applicazioni

Relatore:
Prof. Alessia Cattabriga

Presentata da:
Matteo Mihnea Telespan

Anno Accademico 2024/2025

Sommario

In questa tesi si vogliono studiare e approfondire alcuni aspetti generali della teoria delle rappresentazioni per poi andare a concentrarsi più in particolare sulle rappresentazioni dei gruppi, più precisamente sulle rappresentazioni dei gruppi finiti. In effetti il risultato principale di questa tesi è la classificazione delle rappresentazioni dei gruppi simmetrici S_n su $\mathbb{C}$ ottenuta individuando e dando una descrizione delle rappresentazioni irriducibili corrispondenti. Al fine di fare ciò si sviluppa una vasta gamma di strumenti principalmente di natura algebrica che ci permetteranno poi anche di applicare la teoria matematica sviluppata allo studio della dinamica di sistemi quantistici aperti.

Indice

Introduzione

La teoria delle rappresentazioni è una branca della matematica in cui si vedono i primi segni di interazione fra algebra e geometria. In effetti l'idea che sta alla base della teoria delle rappresentazioni è quella di prendere oggetti algebrici e farli "agire" su oggetti più geometrici in modo da ottenere più informazione sia sull'algebra che sulla geometria. In termini euristici si potrebbe dire che la teoria delle rappresentazioni è lo studio delle simmetrie di spazi lineari. Le applicazioni che essa ha vanno dalla teoria dei numeri e la combinatoria alla geometria, teoria della probabilità, meccanica quantistica e teoria quantistica dei campi. In effetti è il linguaggio con cui in fisica si formalizza la nozione intuitiva di simmetria.
L'obbiettivo di questa tesi è lo studio e l'approfondimento di alcuni aspetti generali della teoria delle rappresentazioni per poi andare a concentrarsi più in particolare sulle rappresentazioni dei gruppi, più precisamente dei gruppi finiti. In effetti il risultato principale di questa tesi è la classificazione delle rappresentazioni dei gruppi simmetrici S_n su $\mathbb{C}$ ottenuta individuando, e dando una descrizione, delle rappresentazioni irriducibili. Al fine di fare ciò svilupperemo una vasta gamma di strumenti principalmente di natura algebrica che ci permetteranno poi anche di applicare la teoria matematica sviluppata allo studio della dinamica di sistemi quantistici aperti. La tesi segue il seguente schema.
Nel Capitolo 1 si sviluppano alcuni strumenti elementari di Teoria dei Gruppi quindi, definizioni di base, esempi e risultati elementari come ad esempio il Teorema di Lagrange e il Primo Teorema di Omomorfismo. Successivamente ci si concentra sui gruppi di permutazioni S_n e si mostrano alcuni risultati elementari su di essi.
Nel Capitolo 2 iniziamo a sviluppare la teoria generale delle rappresentazioni delle algebre associative studiando gli A-moduli. Vedremo alcuni risultati importanti come ad esempio il Lemma di Schur e il Teorema di Jordan-Hölder che ci prepareranno allo studio di una classe molto importante di algebre e moduli ovvero quelli semisemplici. Riconduciamo poi le rappresentazioni di gruppi alle rappresentazioni dell'algebra associata e useremo questo fatto per dimostrare il Teorema di Maschke il quale ci dirà che una vasta gamma di algebre associate a gruppi finiti sono in realtà semisemplici e useremo questo fatto per dare una prima classificazione delle rappresentazioni di gruppi finiti. Questo capitolo si conclude con alcune nozioni sui prodotti tensoriali e rappresentazioni indotte utili per lo studio delle rappresentazioni dei gruppi simmetrici.
Nel Capitolo 3 giungiamo al risultato centrale della tesi ovvero arriviamo ad individuare i $\mathbb{C}S_n$-moduli irriducibili cosa che permette in questo caso di poter classificare tutti i $\mathbb{C}S_n$-moduli, daremo anche una descrizione concreta di questi moduli utilizzando i diagrammi di Ferrer.
Nel Capitolo 4 infine, con gli strumenti sviluppati nei precedenti capitoli, usiamo le rappresentazioni dei gruppi simmetrici per ottenere delle equazioni di evoluzione dinamica

per sistemi quantistici aperti e ci soffermiamo su alcuni esempi in casi semplici.

Capitolo 1

Prerequisiti di Teoria dei Gruppi

In questo capitolo si sviluppano alcuni strumenti elementari di Teoria dei Gruppi, quindi definizioni di base, esempi e risultati elementari come ad esempio il Teorema di Lagrange e il Primo Teorema di Omomorfismo. Successivamente ci si concentra sui gruppi di permutazioni S_n e si mostrano alcuni risultati elementari su di essi.
Per i contenuti di questo capitolo, dove non esplicitamente indicato diversamente, si rimanda a [Cat96], in cui si possono trovare eventuali approfondimenti.

1.1 Gruppi: Definizioni, Esempi e Nozioni di Base

In questa sezione daremo la definizione di gruppo e vedremo alcune loro proprietà elementari.

Definizione 1.1.1. *Un gruppo è una coppia $(G, *)$ dove G è un insieme e $*$ è un operazione cioè:*

$$* : G \times G \to G$$

$$(g_1, g_2) \mapsto g_1 * g_2$$

e l'operazione soddisfa i seguenti assiomi:

1. *$(g_1 * (g_2 * g_3)) = ((g_1 * g_2) * g_3)$ per ogni $g_1, g_2, g_3 \in G$ (Proprietà Associativa)*
2. *esiste $\epsilon \in G$ tale che $g * \epsilon = \epsilon * g = g$ per ogni $g \in G$ (Esistenza dell'elemento neutro)*
3. *per ogni $g \in G$ esiste $\tilde{g}$ tale che: $g * \tilde{g} = \tilde{g} * g = \epsilon$ (Esistenza dell'inverso)*

Diremo inoltre che un gruppo è abeliano se e solo se soddisfa la seguente proprietà:

$$g_1 * g_2 = g_2 * g_1 \quad \textit{(Proprietà commutativa)}$$

Per ogni $g_1, g_2 \in G$.

Vediamo alcuni esempi:

Esempio 1.1.1. *1. Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ con la somma definita nella solita maniera sono dei gruppi abeliani, dove l'inverso è l'opposto.*

2. $(\mathbb{N}, +)$ *non è un gruppo perché non ci sono gli inversi.*

3. $(\mathbb{R}, \cdot)$ *non è un gruppo perché* 0 *non ha un inverso.*

4. *Se A è un insieme indichiamo con S_A l'insieme delle biezioni da A in A. Allora S_A con la composizione di funzioni come operazione è un gruppo non abeliano se A ha almeno tre elementi.*

Definizione 1.1.2. *Sia $(G, *)$ un gruppo, sia $H \subseteq G$ un sottoinsieme. Diremo che H è un sottogruppo di G (e useremo la notazione $H \leq G$) se e solo se $(H, *_{|H \times H})$ è un gruppo a sua volta, equivalentemente:*

1. *H è chiuso rispetto a $*$. Cioè per ogni $g_1, g_2 \in H$ si ha $g_1 * g_2 \in H$.*

2. *per ogni $h \in H$, l'elemento $\tilde{h} \in H$.*

Dai due punti sopra segue immediatamente che se H è un sottogruppo $\epsilon \in H$.

Vediamo anche qui alcuni esempi:

Esempio 1.1.2. 1. *Consideriamo $(\mathbb{Z}, +)$. Allora $H = \{$interi pari$\}$ è un sottogruppo. Gli interi dispari non formano un sottogruppo in quanto* 0 *non è dispari.*

2. *Sia $\mathbb{R}^* := \mathbb{R} - \{0\}$ e $\mathbb{R}^{>0} := \{x \in \mathbb{R} \mid x \geq 0\}$. La coppia $(\mathbb{R}^*, \cdot)$ è un gruppo e $H = \mathbb{R}^{>0}$ è un suo sottogruppo.*

Definizione 1.1.3. *Siano $(G, \cdot)$ e $(H, *)$ due gruppi. Una funzione:*

$$f : G \to H$$

è un omomorfismo di gruppi se e solo se per ogni $g_1, g_2 \in G$ si ha:

$$f(g_1 \cdot g_2) = f(g_1) * f(g_2)$$

Esempio 1.1.3. *$f : \mathbb{R} \to \mathbb{R}^*$ data da $f(x) = e^x$ è un omomorfismo fra i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}^*, \cdot)$.*

Da ora utilizzeremo la notazione moltiplicativa $g_1 \cdot g_2 := g_1 g_2$ per ogni gruppo, tenendo sempre però ben presente che l'operazione può essere diversa da gruppo a gruppo, e indicheremo, a meno che non crei confusione, un gruppo $(G, *)$, semplicemente con G. Indicheremo inoltre con g^{-1} l'inverso di g e porremo: $\underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ volte}} := g^n$.
Si può verificare che valgono le usuali proprietà delle potenze.

Definizione 1.1.4. *Siano G, H due gruppi. Sia $f : G \to H$ un omomorfismo di gruppi. Definiamo:* $\ker(f) = \{g \in G : f(g) = \epsilon_H\}$ *e* $\mathrm{im}(f) = \{f(g) \in H : g \in G\}$. *Si mostra facilmente che sono sottogruppi di G e H rispettivamente.*

Esempio 1.1.4. *Consideriamo $(\mathbb{Z}, +)$ e $(\mathbb{C}^*, \cdot)$. Sia $f : \mathbb{Z} \to \mathbb{C}^*$ definita come: $f(n) = i^n$. Questo è un omomorfismo di gruppi e si ha* $\mathrm{im}(f) = \{1, i, -1, -i\}$ *e* $\ker(f) = 4\mathbb{Z} = \{4n : n \in \mathbb{Z}\}$.

Vediamo ora i primi risultati sui gruppi.

Proposizione 1.1.1. *Sia G un gruppo. Se $g, h, l \in G$ allora $h = l$ se e solo se $gh = gl$ e $hg = lg$.*

Dimostrazione. $\Rightarrow$) Si ha che $gh = gh$, ma $h = l$ quindi $gh = gl$. Analogamente si mostra $hg = lg$.
$\Leftarrow$) $gh = gl$ quindi per il punto precedente $g^{-1}gh = g^{-1}gl$ quindi $h = l$. □

Proposizione 1.1.2. *L'elemento neutro e l'inverso di un elemento sono unici.*

Dimostrazione. Se l'elemento neutro non è unico allora esistono ϵ_1, ϵ_2 neutri quindi $g\epsilon_1 = g\epsilon_2 = g$ quindi per la Proposizione 1.1.1 $\epsilon_1 = \epsilon_2$. Analogamente si mostra che l'inverso di un elemento è unico. □

Spesso ci riferiremo alla cardinalità di un gruppo con il termine ordine.

Lemma 1.1.1. *Sia G un gruppo finito. Allora $H \subseteq G$ è un sottogruppo se e solo se è chiuso rispetto all'operazione.*

Dimostrazione. $\Leftarrow$) Per definizione.
$\Rightarrow$) Sia $\mathbb{N}^{>0} := \{n \in \mathbb{N} \mid n > 0\}$ e sia $h \in H$. Per ipotesi $a^n \in H$ per ogni $n \in \mathbb{N}^{>0}$. Per il principio dei cassetti [1], essendo H finito, esistono $r, s \in \mathbb{N}^{>0}$ tali che $r > s$ e $h^r = h^s$ quindi $h^{r-s} = \epsilon$ e $r - s > 0$ quindi h^{r-s-1} è l'inverso di h. □

Definizione 1.1.5. *Sia G un gruppo e $g \in G$. L'ordine di g (che indicheremo con $o(g)$) è il più piccolo $n \in \mathbb{N}^{>0}$ tale che $g^n = \epsilon$. Se tale n non esiste poniamo $o(g) = \infty$.*

Lemma 1.1.2. *Se $f : G \to H$ è un omomorfismo di gruppi allora $f(\epsilon_G) = \epsilon_H$*

Dimostrazione. si ha:

$$f(g\epsilon_G) = f(g)f(\epsilon_G) = f(g)$$

e

$$f(\epsilon_G g) = f(\epsilon_G)f(g) = f(g)$$

Quindi per la definizione di elemento neutro $f(\epsilon_G) = \epsilon_H$. □

Definizione 1.1.6. *Siano G, H gruppi. $f : G \to H$ si dice isomorfismo di gruppi se e solo se è un omomorfismo di gruppi ed è un applicazione bigettiva.*
Due gruppi G, H si dicono isomorfi se e solo se esiste un isomorfismo tra di essi, in tal caso si scrive: $G \cong H$

Si mostra facilmente che se f è un isomorfismo, l'inversa è a sua volta un isomorfismo.

Esempio 1.1.5. *Consideriamo: $f : \mathbb{R} \to \mathbb{R}^{>0}$ data da $f(x) = e^x$. Tale applicazione è un isomorfismo fra $(\mathbb{R}, +)$ e $(\mathbb{R}^{>0}, \cdot)$.*

Iniziamo adesso ad introdurre alcune costruzioni di base che si possono fare a partire da gruppi dati.

[1] Il principio dei cassetti afferma che se un insieme A infinito è unione di un numero finito di insiemi: $A = A_1 \cup \cdots \cup A_n$ allora almeno uno degli A_i è infinito.

Definizione 1.1.7. *Siano G, H due gruppi allora definiamo il loro prodotto diretto come l'insieme $G \times H$ con l'operazione definita componente per componente.*

Per definizione è immediato vedere che le proiezioni canoniche sui fattori del prodotto sono degli omomorfismi di gruppi.
Notiamo prima di procedere che l'intersezione di sottogruppi di un gruppo G è ancora un gruppo, detto ciò diamo la seguente definizione:

Definizione 1.1.8. *Sia G un gruppo e $X \subseteq G$ un sottoinsieme. Indichiamo con $\langle X \rangle$ il sottogruppo di G, dato dall'intersezione di tutti i sottogruppi di G contenenti X (Tale famiglia è non vuota perché c'è G). Chiamiamo $\langle X \rangle$ sottogruppo di G generato da X.*

Proposizione 1.1.3. *Sia G un gruppo e $X \subseteq G$. Si ha che $\langle X \rangle = \{g_1^{a_1} g_2^{a_2} \dots g_k^{a_k} : g_i \in X, k \in \mathbb{N}^{>0}, a_i \in \mathbb{Z}\}$*

Dimostrazione. Essendo $\langle X \rangle$ un sottogruppo è chiaro che $\{g_1^{a_1} g_2^{a_2} \dots g_k^{a_k} : g_i \in X, k \in \mathbb{N}^{>0}, a_i \in \mathbb{Z}\} \subseteq \langle X \rangle$. D'altro canto, $\{g_1^{a_1} g_2^{a_2} \dots g_k^{a_k} : g_i \in X, k \in \mathbb{N}^{>0}, a_i \in \mathbb{Z}\}$ è per costruzione un sottogruppo di G contente X quindi $\langle X \rangle \subseteq \{g_1^{a_1} g_2^{a_2} \dots g_k^{a_k} : g_i \in X, k \in \mathbb{N}^{>0}, a_i \in \mathbb{Z}\}$ □

Definizione 1.1.9. *Diremo che un gruppo G è ciclico se e solo se è generato da un solo elemento.*

Esempio 1.1.6. $\mathbb{Z} = \langle 1 \rangle$ *dunque è ciclico.*

Vogliamo iniziare a parlare di quozienti di gruppi.

Definizione 1.1.10. *Sia G un gruppo e $H \leq G$. Sia $g \in G$. L'insieme $gH = \{gh : h \in H\}$ è detta classe laterale sinistra (o semplicemente laterale sinistro) di H.*

Esempio 1.1.7. *Sia $G = \mathbb{Z}$ con l'addizione come operazione. Sia $H = n\mathbb{Z} = \{nm : m \in \mathbb{Z}\}$, allora $kH = \{k + h : h \in n\mathbb{Z}\} = \{m : m \equiv k \pmod{n}\}$.*
Dove $m \equiv k \pmod{n}$ se e solo se $m - k$ è un multiplo di n.

Lemma 1.1.3. *Sia G un gruppo e $H \leq G$ allora:*

1. *I laterali sinistri formano una partizione di G e definiscono dunque la relazione di equivalenza di appartenere allo stesso laterale.*

2. *Ciascun laterale ha la stessa cardinalità di H.*

Dimostrazione. 1. $g \in gH$ quindi i laterali sono non vuoti e la loro unione al variare di $g \in G$ ci dà G.
Mostriamo che se due laterali hanno almeno un elemento in comune allora coincidono.
Sia $x \in g_1H \cap g_2H$ con $g_1, g_2 \in G$. Esistono allora h_1, h_2 tali che: $x = g_1h_1 = g_2h_2$ quindi $g_1 = g_2h_1h_2^{-1}$. Dunque se $l \in g_1H$ allora $l = g_1h$ per qualche $h \in H$ ma allora $l = g_2(h_1h_2^{-1}h)$ quindi $l \in g_2H$. Quindi $g_1H \subseteq g_2H$. Analogamente si mostra che $g_2H \subseteq g_1H$.

2. Notiamo che l'applicazione:

$$H \to gH$$

$$h \mapsto gh$$

è una biezione, infatti è suriettiva per definizione ed è iniettiva per la Proposizione 1.1.1.

□

In modo analogo a quanto fatto sopra si definiscono i laterali destri Hg, certamente per i laterali destri vale quanto visto per i laterali sinistri con una dimostrazione analoga.

Corollario 1.1.1 (**Teorema di Lagrange**). *Se G è un gruppo finito e $H \leq G$ allora l'ordine di H divide G, $|H| \mid |G|$.*

Dimostrazione. Segue immediatamente dal Lemma 1.1.3 □

Definizione 1.1.11. *Sia G un gruppo e $H \leq G$. Diremo che H è un sottogruppo normale, e lo indicheremo con $H \trianglelefteq G$, se e solo se laterali destri e sinistri coincidono.*

Esempio 1.1.8. *1. Se G è abeliano tutti i sottogruppi sono normali.*

2. Se l'ordine di H è metà di quello di G allora, essendoci come laterali solo H e $G - H$, H è normale.

Notiamo che $N \trianglelefteq G$ se e solo se per ogni $g \in G$ si ha che $gNg^{-1} = N$ cioè se per ogni $n \in N$ e $g \in G$ si ha: $gng^{-1} \in N$.

Proposizione 1.1.4. *Siano G, H due gruppi e $f : G \to H$ un omomorfismo di gruppi. Si ha che $ker(f) \trianglelefteq G$.*

Dimostrazione. Se $n \in ker(f)$ allora per ogni $g \in G$ si ha $gng^{-1} \in ker(f)$. Infatti:

$$f(gng^{-1}) = f(g)\epsilon_H f(g)^{-1} = \epsilon_H$$

□

Notiamo che se $H \leq G$ allora $x, y \in G$ sono nello stesso laterale destro se e solo se $xy^{-1} \in H$. Infatti se $xy^{-1} \in H$ allora $x \in Hy$ quindi sono nello stesso laterale. Viceversa se x, y sono nello stesso laterale destro allora $x, y \in Hg$ per qualche $g \in G$ quindi $x = h_1 g$ e $y = h_2 g$ e $xy^{-1} = h_1 g g^{-1} h_2 \in H$.
Quindi la relazione di equivalenza di appartenere allo stesso laterale destro di H si può riformulare ponendo:

$$x \sim y \quad \text{se e solo se} \quad xy^{-1} \in H.$$

Definizione 1.1.12. *Sia G un gruppo e sia $\sim$ una relazione di equivalenza su G. Diremo che la relazione $\sim$ è compatibile se e solo se per ogni $x, y, x', y' \in G$ tali che $x \sim x'$ e $y \sim y'$ si ha: $xy \sim x'y'$. Cioè l'operazione: $[x] \cdot [y] = [xy]$ è ben definita. In particolare $G/\sim$ è un gruppo con l'operazione definita sopra.*

Teorema 1.1.1. *Sia G un gruppo, allora:*

1. *Se $N \trianglelefteq G$, allora la relazione di appartenere allo stesso laterale è compatibile.*
2. *Se $\sim$ è una relazione di equivalenza compatibile allora $[\epsilon]$ è un sottogruppo normale di G e $x \sim y$ se e solo se $xy^{-1} \in [\epsilon]$.*

Dimostrazione. Rimandiamo a [Cat96] □

Questo teorema ci dice che le relazioni di equivalenza compatibili sono e sole le relazioni date dall'appartenenza ad uno stesso laterale di un qualche sottogruppo normale.

Definizione 1.1.13. *Sia G un gruppo e $N \trianglelefteq G$. Definiamo il gruppo:*

$$G/N = \{\textit{laterali di } N\}$$

con l'operazione data da:

$$(g_1N)(g_2N) := g_1g_2N$$

Tale operazione è ben definita essendo N normale.

Sulla base delle osservazioni di prima posto $x \sim y$ se e solo se $xy^{-1} \in N$ si ha che $G/N \cong G/\sim$ mediante l'omomorfismo: $gN \mapsto [g]$. Vediamo ora un Teorema fondamentale.

Teorema 1.1.2. *Siano G, H gruppi e sia $f : G \to H$ un omomorfismo di gruppi. Sia $N \trianglelefteq G$ tale che $N \subseteq \ker(f)$. Allora esiste un unico omomorfismo $\overline{f} : G/N \to H$ che faccia commutare il seguente diagramma (cioè tale che $f = \overline{f}\pi$):*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ G/N & & \end{array}$$

Dimostrazione. Intanto l'applicazione $\overline{f}(gN) = f(g)$ è ben definita in quanto se $gN = g'N$ si ha che g, g' sono nello stesso laterale quindi $gg'^{-1} \in N \subseteq \ker(f)$ quindi $f(g) = f(g')$, inoltre $\overline{f}$ è l'unica applicazione che fa commutare il diagramma sopra. Per definizione di $\overline{f}$ e dell'operazione di G/N si ha che $\overline{f}$ è anche un omomorfismo. □

Corollario 1.1.2 (**Primo Teorema di Omomorfismo**)**.** *Siano G, H gruppi e sia $f : G \to H$ un omomorfismo di gruppi. Allora si ha che:*

$$G/\ker(f) \cong \mathrm{im}(f)$$

Dimostrazione. Intanto l'applicazione $f : G \to im(f)$ è ben definita e suriettiva. Dunque per il Teorema 1.1.2 esiste un unico omomorfismo $\overline{f}$ che fa commutare il seguente diagramma:

$$\begin{array}{ccc} G & \xrightarrow{f} & \mathrm{im}(f) \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{f}} & \\ G/\ker(f) & & \end{array}$$

Siccome $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$ si ha che $\overline{f}$ è suriettiva.
Se $\overline{f}(g_1\ker(f)) = \overline{f}(g_2\ker(f))$ allora $f(g_1) = f(g_2)$ quindi $g_1g_2^{-1} \in \ker(f)$ quindi $g_1\ker(f) = g_2\ker(f)$ dunque $\overline{f}$ è anche iniettiva. □

Vediamo alcuni esempi.

Esempio 1.1.9. *1. Consideriamo $(\mathbb{Z}, +)$. Prendiamo come sottogruppo normale $n\mathbb{Z}$. Il gruppo quoziente $(\mathbb{Z}/n\mathbb{Z}, +)$ ha come elementi (usando l'isomorfismo con l'insieme quoziente per la relazione: $x \sim y$ se e solo se $x \equiv y \pmod{n}$):*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$$

e l'operazione è definita come: $[n] + [m] = [n+m]$.

2. Indichiamo con C_4 il gruppo $(\{1, i, -1, -i\}, \cdot)$. Per quanto visto nell'Esempio 1.1.4 e il Corollario 1.1.1 si ha che:

$$\mathbb{Z}/4\mathbb{Z} \cong C_4$$

Introduciamo ora alcuni concetti che ci torneranno utili in seguito.

Definizione 1.1.14. *Sia G un gruppo e $h \in G$. Definiamo $C_h : G \to G$ data da: $g \mapsto hgh^{-1}$.*
Chiameremo tale applicazione coniugio per l'elemento h.

Proposizione 1.1.5. *Si ha che:*

1. *$C_{h_1} \circ C_{h_2} = C_{h_1 h_2}$*
2. *C_h è un automorfismo di G.*

Dimostrazione. 1. $(C_{h_1} \circ C_{h_2}) = h_1 h_2 g h_2^{-1} h_1^{-1} = h_1 h_2 g (h_1 h_2)^{-1} = C_{h_1 h_2}(g)$

2. per il punto precedente C_h è una biezione. Mostriamo che è un omomorfismo:

$$C_h(g_1 g_2) = h g_1 g_2 h^{-1} = h g_1 h^{-1} h g_2 h^{-1} = C_h(g_1) c_h(g_2).$$

□

Esempio 1.1.10. *1. Sia G un gruppo abeliano. Vale $C_h(g) = g$ per ogni $g \in G$.*

2. Sia $G = GL_n(K)$ e sia $M_2 = C_B(M_1)$. Questo vuol dire che le matrici M_1 ed M_2 sono simili.

Definizione 1.1.15. *Sia G un gruppo. Diremo che $g_1, g_2 \in G$ sono coniugati se e solo se esiste $h \in G$ tale che $g_2 = C_h(g_1)$.*

Si vede immediatamente che la relazione di essere coniugati è una relazione di equivalenza. Le classi di equivalenza sono dette classi di coniugio.

1.2 Gruppo Simmetrico S_n

Definizione 1.2.1. *Poniamo $S_n = S_{\{1,\dots,n\}}$ con $S_{\{1,\dots,n\}}$ definito come nell'Esempio 1.1.1. Consideriamo il gruppo: $(S_n, \circ)$ dove $\circ$ è la composizione di funzioni. Tale gruppo è noto come gruppo Simmetrico. I suoi elementi sono detti permutazioni.*

Si ha immediatamente che $|S_n| = n!$ Iniziamo a dare alcune definizioni sulle permutazioni e ad introdurre un po' di notazione.

Definizione 1.2.2. *Sia $\sigma \in S_n$ e $i \in \{1, \dots, n\}$. Definiamo l'orbita di i come:*

$$\theta_{\sigma(i)} = \{i, \sigma(i), \dots, \sigma^n(i) \dots\}$$

Naturalmente essendo $\theta_{\sigma(i)} \subseteq \{1, \dots, n\}$, le orbite sono insiemi finiti.

Proposizione 1.2.1. *Sia $\sigma \in S_n$. Le orbite di σ formano una partizione di $\{1, \dots, n\}$.*

Dimostrazione. Siano $i, j, k \in \{1, \dots, n\}$ tali che: $k \in \theta_{\sigma(i)} \cap \theta_{\sigma(j)}$. Allora applicando ripetutamente σ a k possiamo ottenere tutti gli elementi di $\theta_{\sigma(i)}$ e di $\theta_{\sigma(j)}$.Infatti, sempre per il principio dei cassetti, esistono $l, l' \in \mathbb{N}^{>0}$ tale che $\sigma^l(k) = i$ e $\sigma^{l'}(k) = j$. Quindi $\theta_{\sigma(i)} = \theta_{\sigma(j)}$. Dunque le orbite sono a due a due disgiunte e facendo l'unione delle orbite al variare di $i \in \{1, \dots, n\}$ otteniamo tutto $\{1, \dots, n\}$. □

Diremo che un orbita è banale se contiene un solo elemento. Tali elementi per definizione sono fissati da σ.

Definizione 1.2.3. *Una permutazione $\sigma \in S_n$ è detta ciclo se e solo se ha un unica orbita non banale. In tal caso se i è un elemento dell'orbita non banale poniamo $\sigma := (i, \sigma(i), \dots, \sigma^n(i), \dots)$ in quanto così la permutazione è completamente definita visto che gli elementi che non compaiono nella notazione sono fissati.*

Certamente data una qualsiasi permutazione $\sigma \in S_n$ possiamo associare alle sue orbite non banali dei cicli σ_i. Essendo le orbite disgiunte a due a due per ogni coppia di cicli di σ si ha: $\sigma_i\sigma_j = \sigma_j\sigma_i$. Visto che la permutazione σ è completamente definita dalle sue orbite si ha il seguente risultato:

Proposizione 1.2.2. *Ogni $\sigma \in S_n$ è prodotto di cicli che commutano fra loro.*

Dimostrazione. Segue dall'osservazione sopra. □

Le orbite sono finite quindi si ha anche che ogni σ è prodotto di un numero finito di cicli che commutano.
Vediamo un esempio:

Esempio 1.2.1. *Sia $\sigma \in S_8$ data da: $\sigma = (1, 3, 7, 4)(2, 6)$. Allora si ha che:*
$\sigma(1) = 3$; $\sigma(2) = 6$; $\sigma(3) = 7$; $\sigma(4) = 1$; $\sigma(5) = 5$; $\sigma(6) = 2$; $\sigma(7) = 4$; $\sigma(8) = 8$.

Esempio 1.2.2. *Definiamo $\sigma \in S_8$ come:*
$\sigma(1) = 2$; $\sigma(2) = 5$; $\sigma(3) = 6$; $\sigma(4) = 4$; $\sigma(5) = 7$; $\sigma(6) = 3$; $\sigma(7) = 1$; $\sigma(8) = 8$. *Da cui si ha la seguente decomposizione in cicli: $\sigma = (1, 2, 5, 7)(3, 6)$.*

La lunghezza di un ciclo è definita come la cardinalità della sua orbita non banale.

Definizione 1.2.4. *Una trasposizione è un ciclo di lunghezza due.*

Teorema 1.2.1. *Ogni permutazione è prodotto di trasposizioni.*

Dimostrazione. Per la Proposizione 1.2.2 è sufficiente mostrare la tesi per i cicli.
Sia $(i_1, \dots, i_k)$ un ciclo. Allora si verifica che:

$$(i_1, i_2, \dots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \dots (i_1, i_2)$$

□

Definizione 1.2.5. *Diremo che $\sigma \in S_n$ è pari (dispari) se e solo se è prodotto di un numero pari (dispari) di permutazioni.*

A priori non sappiamo se esistono permutazioni sia pari che dispari, vediamo che non è così.
Partiamo definendo per ogni $\sigma \in S_n$ l'applicazione f_σ che dato un polinomio in n variabili $p(x_1, \dots, x_n)$ restituisce il polinomio $p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.
Poniamo ora $p := \prod_{1 \le i < j \le n}(x_i - x_j)$ e mostriamo il seguente lemma:

Lemma 1.2.1. *Sia $\tau \in S_n$ la trasposizione (i, j). Allora $f_\tau(p) = -p$*

Dimostrazione. Guardiamo cosa succede ad ogni singolo termine:

1. i fattori senza i, j rimangono invariati.
2. i fattori $(x_h - x_i)(x_h - x_j)$ con $h < i$ si scambiano senza cambiare segno
3. i fattori $(x_i - x_h)(x_j - x_h)$ con $j < h$ si scambiano senza cambiare segno
4. i fattori $(x_i - x_h)(x_h - x_j)$ con $i < h < j$ si scambiano cambiando entrambi di segno quindi complessivamente il segno non cambia.

L'unico fattore rimanente è $(x_i - x_j)$ che cambia di segno. □

Teorema 1.2.2. *Una permutazione non può essere sia pari che dispari.*

Dimostrazione. Sia $p \neq 0$ come definito sopra. Se esistesse $\sigma \in S_n$ sia pari che dispari si avrebbe per il precedente lemma: $p = -p$ quindi $p = 0$ ma ciò è assurdo. □

Definizione 1.2.6. *L'applicazione* $\operatorname{sgn} : S_n \to \mathbb{C}$ *definita come segue:*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{se } \sigma \text{ è pari,} \\ -1 & \text{se } \sigma \text{ è dispari.} \end{cases}$$

è detta applicazione segno, è ben definita per il precedente teorema e definisce un omomorfismo di gruppi fra $(S_n, \circ)$ e $(\mathbb{C}, \cdot)$.

Si ha che im(sgn) = $\{1, -1\}$ e ker(sgn) = {permutazioni pari}. Dunque per quanto visto nella sezione precedente si ha che l'insieme delle permutazioni pari forma un sottogruppo normale, noto come gruppo alterno, che si indica con A_n. Inoltre per il primo teorema di omomorfismo (Corollario 1.1.2) sappiamo che ci sono solo due laterali di A_n da cui concludiamo che $|A_n| = n!/2$.
Vogliamo ora indagare le classi di coniugio di S_n.

Lemma 1.2.2. *Sia $\sigma \in S_n$ data da $\sigma = (i_1, \dots, i_k)$ e sia $\tau \in S_n$ qualsiasi. Allora si ha che $C_\tau(\sigma) = (\tau(i_1), \dots, \tau(i_k))$. Viceversa, se due cicli hanno la stessa lunghezza allora sono coniugati.*

Dimostrazione. Rimandiamo a [Cat96] □

Vogliamo ora togliere la condizione di avere cicli per guardare alle permutazioni generiche.

Definizione 1.2.7. *Sia $n \in \mathbb{N}^{>0}$. Una partizione di n è una successione $\lambda = (\lambda_1, \dots, \lambda_k)$ con $\lambda_1 \geq \lambda_2 \geq \dots$ tale che: $\sum_i \lambda_i = n$. Se λ è una partizione di n scriveremo: $\lambda \vdash n$.*

Definizione 1.2.8. *Diremo che $\sigma \in S_n$ ha struttura ciclica $\lambda = (\lambda_1, \dots, \lambda_k)$ con $\lambda \vdash n$ se e solo se le sue orbite hanno cardinalità: $\lambda_1, \dots, \lambda_2$.*

Veniamo adesso al teorema che ci interessa:

Teorema 1.2.3. *Due elementi $\sigma_1, \sigma_2 \in S_n$ sono coniugati se e solo se hanno la stessa struttura ciclica. Dunque le classi di coniugio di S_n sono in biezione con le partizioni di n.*

Dimostrazione. Sia $\sigma_1 = \sigma_{1_{i_1}} \dots \sigma_{1_{i_r}}$ la sua scomposizione in cicli e sia $\sigma_2 = \sigma_{2_{i_1}} \dots \sigma_{2_{i_r}}$ la scomposizione in cicli di σ_2.
$\Rightarrow$) Si ha che esiste $\tau \in S_n$ tale che $C_\tau(\sigma_1) = \sigma_2$. Essendo C_τ un automorfismo si ha: $C_\tau(\sigma_1) = C_\tau(\sigma_{1_{i_1}}) \cdots C_\tau(\sigma_{1_{i_r}})$. Per il Lemma 1.2.2, dunque le due permutazioni hanno la stessa struttura ciclica.
$\Leftarrow$) Sia: $\sigma_1 = (a_{11}, \dots, a_{1k_1}) \dots (a_{r1}, \dots, a_{rk_r})$. Allora per ipotesi si ha che

$$\sigma_2 = (b_{11}, \dots, b_{1k_1}) \dots (b_{r1}, \dots, b_{rk_r})$$

in quanto hanno la stessa struttura ciclica. Allora si verifica che posto $\tau(a_{ij}) = b_{ij}$ e che lascia fissi gli altri elementi si ha $C_\tau(\sigma_1) = \sigma_2$. □

Capitolo 2

Teoria Generale

In questo capitolo iniziamo a sviluppare la teoria generale delle rappresentazioni delle algebre associative studiando gli A-moduli. Vedremo alcuni risultati importanti come ad esempio il Lemma di Schur e il Teorema di Jordan-Hölder che ci prepareranno allo studio di una classe molto importante di algebre e moduli ovvero quelli semisemplici. Riconduciamo poi le rappresentazioni di gruppi alle rappresentazioni dell'algebra associata e useremo questo fatto per dimostrare il teorema di Maschke il quale ci dirà che una vasta gamma di algebre associate a gruppi finiti sono in realtà semisemplici e useremo questo fatto per dare una prima classificazione delle rappresentazioni di gruppi finiti. Questo capitolo si conclude con alcune nozioni sui prodotti tensoriali e rappresentazioni indotte utili per lo studio delle rappresentazioni dei gruppi simmetrici.
Per i contenuti di questo capitolo, dove non esplicitamente indicato diversamente, si rimanda a [Kar18], in cui si possono trovare eventuali approfondimenti.

2.1 K-Algebre

Per le definizioni e i risultati di base riguardanti la teoria degli anelli e dei campi rimandiamo a [Her10]. Diamo ora la definizione di K-algebra associativa.

Definizione 2.1.1. *Sia K un campo. A si dice K-algebra associativa se e solo se valgono le seguenti condizioni:*

1. *A è un Anello Unitario con $0_A \neq 1_A$.*
2. *A è un K-Spazio Vettoriale*
3. *Per ogni $\lambda \in K$ e $a, b \in A$ si ha:*

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

L'algebra si dirà finito dimensionale se A è uno spazio vettoriale finito dimensionale.
L'algebra si dirà commutativa se A è un anello commutativo.

Vediamo ora alcuni esempi.

Esempio 2.1.1. 1. *Un campo K è una K-algebra di dimensione 1.*

2. *Il campo $\mathbb{C}$ è una $\mathbb{R}$-algebra di dimensione 2, in quanto $\mathbb{C}$ è un $\mathbb{R}$-Spazio Vettoriale di dimensione 2 ed è un campo. La proprietà* 3. *della Definizione 2.1.1 è soddisfatta in quanto $\mathbb{R} \subset \mathbb{C}$.*

Notiamo che se A è una K-algebra e $\mathcal{B}$ è una base allora per linearità è sufficiente conoscere i prodotti bb', al variare di $b, b' \in \mathcal{B}$, per conoscere tutti i prodotti.

Esempio 2.1.2. 1. *$M_n(K)$ ovvero lo spazio delle matrici quadrate di ordine n a coefficienti nel campo K è una K-algebra di dimensione n^2 con la somma e il prodotto per scalare soliti e il prodotto riga per colonna.*
Le matrici E_{ij} con 1 nell'entrata (i,j) e 0 altrove costituiscono una base per $M_n(K)$ e si può verificare che:
$$E_{ij}E_{kl} = \delta_{jk}E_{il}.$$

2. *$K[X]$ cioè lo spazio dei polinomi in una variabile a coefficenti in K costituisce una K-algebra di dimensione infinita.*

3. *Sia V un K-Spazio Vettoriale, allora:*
$$\mathrm{End}_K(V) = \{\alpha : V \to V \mid \alpha \quad \textit{lineare}\}$$
è una K-algebra con prodotto per scalare e somma puntuali e prodotto composizione di funzioni.

Introduciamo ora un importante algebra per il seguito.

Definizione 2.1.2. *Sia G un gruppo e K un campo. Allora l'algebra gruppo, KG è lo Spazio vettoriale generato da G, cioè l'insieme delle combinazioni lineari formali di elementi di G con coefficienti in K. Vediamo come sono definite le operazioni. La somma è:*
$$\sum_{i=1}^{n} a_i g_i + \sum_{j=1}^{m} b_j g_j = \sum_{i=0}^{max(n,m)} (a_i + b_i) g_i$$
il prodotto per scalare è:
$$\lambda \sum_{i=1}^{n} a_i g_i = \sum_{i=1}^{n} \lambda a_i g_i$$
Il prodotto è l'estensione lineare del prodotto di G.

Si verifica che con le operazioni sopra definite KG è una K-algebra.
Introduciamo ora un altro po' di concetti utili.

Definizione 2.1.3. *Sia A una K-algebra. $B \subseteq A$ è una K-sottoalgebra di A se e solo se è a sua volta una K-algebra ovvero se e solo se:*

1. *è un sottoanello unitario*

2. *è un K-sottospazio vettoriale di A.*

Esempio 2.1.3. 1. *$T_n(K)$, cioè l'insieme delle matrici triangolari superiori di ordine n, è una sottoalgebra di $M_n(K)$.*

2. *$D_n(K)$, cioè l'insieme delle matrici di ordine n diagonali, è una sottoalgebra di $M_n(K)$*

3. *Sia G un gruppo e $H \leq G$ un sottogruppo, allora: KH è una sottoalgebra di KG.*

Definizione 2.1.4. *Sia A una K-algebra e sia $I \subseteq A$ tale che $(I, +)$ è un sottogruppo. Se per ogni $x \in I$ e $a \in A$ si ha:*

1. *$ax \in I$ allora I si dice ideale sinistro*

2. *$xa \in I$ allora I si dice ideale destro*

3. *se valgono entrambe le proprietà sopra I si dice ideale bilatero.*

Notiamo che se I ideale è una sottoalgebra allora coincide con l'algebra in quanto $1_A \in I$.

Esempio 2.1.4. 1. *Ogni algebra A ha come ideali A e $\{0_A\}$ detti ideali banali.*

2. *Sia $z \in A$. $Az = \{az \mid a \in A\}$ è un ideale sinistro che indicheremo con (z) e chiameremo ideale sinistro generato da z.*

3. *Si può mostrare che gli unici ideali bilateri di $M_n(K)$ sono quelli banali.*

Richiamiamo la notazione della Definizione 1.1.13: Se I è un ideale bilatero della K-algebra A allora A/I è l'insieme dei laterali di I. Essendo A un gruppo abeliano I è normale quindi A/I è un gruppo con l'operazione data da:

$$(a + I) + (b + I) = (a + b + I)$$

Si può mostrare in modo analogo a quanto fatto per i gruppi che A/I è una K-algebra con il seguente prodotto:

$$(a + I)(b + I) = (ab + I)$$

e con il prodotto per scalare dato da:

$$\lambda(a + I) = (\lambda a + I)$$

con $\lambda \in K$. Si può anche mostrare sempre in analogia con quanto visto per i gruppi il corrispettivo del Teorema 1.1.1, ragione per la quale A/I è anche detta algebra quoziente. Introduciamo ora i morfismi di algebre.

Definizione 2.1.5. *Siano A, B due K-algebre. L'applicazione $\phi : A \to B$ è un omomorfismo (o morfismo) d'algebre se e solo se:*

1. *ϕ è K-lineare*

2. *ϕ è un morfismo di anelli unitari.*

Diremo che ϕ è un isomorfismo e scriveremo in tal caso $A \cong B$ se e solo se è biunivoca. Si vede immediatemente che se ϕ è un isomorfismo allora anche ϕ^{-1} lo è.

Per linearità si ha che è sufficente conoscere un morfismo di K-algebre su una base per averla definita su tutta l'algebra. Vediamo alcuni esempi:

Esempio 2.1.5. *1. Per ogni $a \in A$ esiste ed è unico il morfismo di K-algebre di valutazione $\phi_a : K[X] \to A$ che manda: $\sum_i \lambda_i X^i \mapsto \sum_i \lambda_i a^i$.*

2. $\pi : A \to A/I$ la proiezione canonica al quoziente è un morfismo di K-algebre.

3. Definiamo il prodotto diretto delle K-algebre A_1, A_2 ponendo come insieme $A_1 \times A_2$ e operazioni definite componente per componente. Le proiezioni canoniche sono morfismi di K-algebre.

Esempio 2.1.6. *Un fatto molto importante a cui faremo spesso riferimento è che se A è una K-algebra allora il morfismo:*

$$\phi : K \to A$$

$$\lambda \mapsto \lambda 1_A$$

è iniettivo e dunque in A vi è una copia isomorfa a K.

Teorema 2.1.1. *Sia K un campo e A, B due K-algebre. Sia $\phi : A \to B$ un morfismo di K-algebre. Allora valgono le seguenti:*

1. $\ker(\phi)$ *è un ideale bilatero.*

2. *se $I \subseteq \ker(\phi)$ allora esiste un unico morfismo di K-algebre $\overline{\phi}$ che fa commutare il seguente diagramma:*

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\phi}} & \\ A/I & & \end{array}$$

3. $A/\ker(\phi) \cong \mathrm{im}(\phi)$

Dimostrazione. La dimostrazione è analoga a quella del Teorema 1.1.2 □

Esempio 2.1.7. *1. Sia: $\phi : \mathbb{R}[X] \to \mathbb{C}$ data dalla valutazione in i. Certamente si ha che $(X^2+1) \subseteq \ker(\phi)$ ma X^2+1 è irriducibile in $\mathbb{R}[X]$ quindi (X^2+1) è massimale e dunque $\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$.*

2. Sia G un gruppo ciclico di ordine n generato da g cioè: $G = \{\epsilon, g, g^2, \ldots, g^{n-1}\}$. Consideriamo:

$$\phi : K[X] \to KG$$

$$f \mapsto f(g)$$

Certamente $(X^n-1) \subseteq \ker(\phi)$ ed essendo $\dim(KG) = n$, per ragioni di dimensione $(X^n-1) = \ker(\phi)$ e quindi:

$$K[X]/(X^n-1) \cong KG.$$

2.2 Moduli e Rappresentazioni

In questa sezione vediamo alune proprietà generali degli R-moduli che definiamo di seguito.

Definizione 2.2.1. *Sia R un anello unitario ed $(M,+)$ un gruppo abeliano. M si dice R-modulo sinistro se e solo se è definita un applicazione:*

$$\cdot : R \times M \to M$$

$$(r, m) \mapsto r \cdot m$$

che soddisfa le seguenti proprietà per ogni $r, s \in R$ e ogni $m, n \in M$

1. $r \cdot (m+n) = r \cdot m + r \cdot n$
2. $(r+s) \cdot m = (r \cdot m + s \cdot m)$
3. $r \cdot (s \cdot m) = (rs) \cdot m$
4. $1_R \cdot m = m$

Notiamo alcune cose importanti. Innanzitutto definire una struttura di R-modulo sinistro su un gruppo abeliano M è equivalente a definire un morfismo di anelli unitari fra R ed $\mathrm{End}(M) = \{\alpha \mid \alpha : M \to M \quad \text{ed è un morfismo di gruppi}\}$ Dove $\mathrm{End}(M)$ è un anello unitario con la somma data dalla somma di funzioni e prodotto dato dalla composizione di funzioni. In effetti dato un R-modulo sinistro M se consideriamo

$$\phi : R \to \mathrm{End}(M)$$

$$r \mapsto r \cdot m$$

l'assioma 1 ci dice che tale applicazione è ben definita mentre gli altri ci dicono che è un morfismo di anelli unitari. Vicecersa se si ha un morfismo di anelli unitari:

$$\phi : R \to \mathrm{End}(M)$$

$$r \mapsto \phi_r$$

allora M ha una struttura naturale di R-modulo sinistro data dall'operazione:

$$r \cdot m = \phi_r(m)$$

che soddisfa tutti gli assiomi di R-modulo per definizione. In analogia si possono definire i moduli destri per cui valgono le stesse considerazioni. Noi considereremo da ora moduli sinistri e dunque lo lasceremo sottinteso.
Vediamo alcuni esempi.

Esempio 2.2.1.

1. *Se R è un campo allora M è per definizione un K-spazio vettoriale. La nozione di modulo generalizza dunque quella di spazio vettoriale.*
2. *Sia $R = \mathbb{Z}$. Ogni gruppo abeliano è un R-modulo con l'azione data da: $n \cdot m := \underbrace{m + m \cdots + m}_{n \text{ volte}}$; $(-n) \cdot m := -(n \cdot m)$ e $0_{\mathbb{Z}} \cdot m := 0_M$.*

3. *Sia I un ideale di R allora I è un R-modulo con l'azione data dalla moltiplicazione a sinistra. In particolare R si può sempre vedere come R-modulo per tale azione.*

4. *Sia $\phi : R \to S$ un morfismo di anelli unitari allora se M è un S-modulo è anche un R-modulo con azione data da:*

$$r \cdot m = \phi(r) \cdot m$$

In particolare se R è un sottoanello di S ed M è un S-modulo è anche un R-modulo, infatti è sufficiente prendere come ϕ l'inclusione di R in S.

L'ultimo esempio ci dice in particolare che se M è un A-modulo con A una K-algebra allora è anche un K-modulo (come ϕ consideriamo il morfismo dell'Esempio 2.1.6) ovvero un K-spazio vettoriale. Quando ci concentreremo dunque sui moduli di algebre indicheremo il modulo con V. In tal caso essendo V uno spazio vettoriale saremo in grado di valutare molte proprietà guardando solo una sua base.

Definizione 2.2.2. *Sia R un Anello Unitario e sia M un R-modulo. Un R-sottomodulo U di M è un sottoinsieme che sia sottogruppo di M e sia chiuso rispetto all'azione di R ovvero per ogni $u \in U$ e $r \in R$ si ha: $r \cdot u \in U$*

Esempio 2.2.2.

1. *Se $R = K$ un campo allora i sottomoduli sono i sottospazi vettoriali.*

2. *Se $R = A$ una K-algebra allora i sottomoduli sono sottospazi vettoriali chiusi per l'azione di A. Vediamo ad esempio K^n come $M_n(K)$-modulo con azione data dal prodotto riga per colonna a sinistra. Sia U un suo sottomodulo non nullo allora preso $u \in U$ non nullo consideriamo una sua coordinata u_j non nulla. Allora si ha: $(u_j)^{-1}E_{ij} \cdot u$ è l'i-esimo vettore della base canonica dunque per chiusura $U = K^n$. Ciò ci dice che K^n come $M_n(K)$-modulo ha solo sottomoduli banali cioè $\{0_{K^n}\}$ e K^n. Ciò ci dice anche che la nozione di sottomodulo è più restrittiva di quella di sottospazio vettoriale.*

3. *Se consideriamo R come R-modulo nel modo naturale visto negli esempi precedenti allora i sottomoduli sono gli ideali sinistri.*

4. *Se U, V sono sottomoduli di M allora $U \cap V$ è un sottomodulo di M.*

Definizione 2.2.3.

1. *Dati M_1, M_2 due R-moduli si può dotare $M_1 \times M_2$ della struttura di R-modulo con azione componente per componente.*

2. *Dati U, V sottomoduli di M possiamo definire:*

$$U + V = \{u + v : u \in U \quad e \quad v \in V\}$$

Questo è un sottomodulo di M. Se $U \cap V = \{0\}$ si scrive $U \oplus V$.

Si mostra in analogia con il caso degli Spazi Vettoriali che $x \in U \oplus V$ allora $x = u + v$ in modo unico. Ciò garantisce che vi sia un isomorfismo fra $U \oplus V$ e $U \times V$ dato da:

$$x = u + v \mapsto (u, v).$$

Consideriamo ora un sottomodulo U dell'R-modulo M. Essendo M un gruppo abeliano ed U un sottogruppo si ha che come già visto che l'insieme dei laterali M/U ha la struttura di gruppo. Si può mostrare con metodi analoghi a quelli visti per i gruppi che l'azione: $r \cdot (m + U) = (r \cdot m + U)$ è ben definita dunque M/U si può dotare della struttura di R-modulo. Inoltre, sempre in analogia con quanto visto per i gruppi, vale un analogo del Teorema 1.1.1 pertanto l'R-modulo M/U è anche detto modulo quoziente.

Definizione 2.2.4. *Siano M, N R-moduli. Si dice che $\phi : M \to N$ è un omomorfismo o morfismo di moduli se e solo se per ogni $m, m_1, m_2 \in M$ e $r \in R$ si ha:*

1. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$
2. $\phi(r \cdot m) = r \cdot \phi(m)$

Anche in questo caso diremo che ϕ è un isomorfismo se e solo se è bigettiva, in tal caso anche ϕ^{-1} è un isomorfismo. Diremo che M, N sono degli R-moduli isomorfi se e solo se esiste un isomorfismo fra di essi, in tal caso scriveremo $M \cong N$.
Notiamo anche che se $\phi : V \to W$ è un morfismo di A-moduli con A una K-algebra allora ϕ è anche un applicazione lineare infatti: $\phi(\lambda v) = \phi(\lambda 1_A \cdot v) = \lambda\phi(v)$. Nel caso in cui $R = A$ è una K-algebra la condizione 2 della Definizione 2.2.4 si può verificare solo per gli elementi di una base.

Esempio 2.2.3.
1. *Sia U un R-sottomodulo di M. Allora $\pi : M \to M/U$ la proiezione canonica al quoziente è un morfismo di R-moduli.*
2. *Sia M un R- modulo, allora l'applicazione:*

$$\phi_m : R \to M$$

$$r \to r \cdot m$$

con $m \in M$ fissato, è un morfismo di R-moduli.

Si definiscono nella solita maniera $\ker(\phi)$ e $\mathrm{im}(\phi)$ e si ha che sono sottomoduli.

Teorema 2.2.1. *Siano M, N R- moduli e $\phi : M \to N$ un morfismo fra di essi. Valgono allora le seguenti:*

1. $M/\ker(\phi) \cong \mathrm{im}(\phi)$
2. *Siano U, V sottomoduli di M. Si ha:*

$$U/(U \cap V) \cong (U + V)/V$$

3. *Siano $U \subseteq V$ sottomoduli di M allora: V/U è un sottomodulo di M/U e*

$$\frac{M/U}{V/U} \cong M/V$$

Dimostrazione. Per la dimostrazione si veda a [Kar18, Theorem 2.24]. □

Enunciamo ora alcuni risultati che ci torneranno utili poi.

Proposizione 2.2.1. *Siano M, N R-moduli e $\phi : M \to N$ un morfismo di R-moduli. Sia $W \subseteq N$ un sottomodulo. Allora la controimmagine $\phi^{-1}(W)$ è un sottomodulo di M che contiene* $\ker(\phi)$.

Dimostrazione. Per la dimostrazione si veda a [Kar18, Proposition 2.26] □

Consideriamo ora U sottomodulo di M e sia $\pi : M \to M/U$. La proiezione canonica al quoziente. Sia W un sottomodulo di M/U. Poniamo $\overline{W} = \pi^{-1}(W)$. Dalla precedente proposizione sappiamo che $\overline{W}$ è un sottomodulo di M e contiene U.

Teorema 2.2.2. *Sia M un R-modulo e U un R-sottomodulo allora l'applicazione $W \mapsto \overline{W}$ dà una biezione che preserva l'ordine dato dall'inclusione fra i sottomoduli di M/U e i sottomoduli di M che contengono U.*

Dimostrazione. Per la dimostrazione si veda a [Kar18, Theorem 2.28] □

Introduciamo ora la nozione di rappresentazione

Definizione 2.2.5. *Sia K un campo e A una K-algebra.*

1. *Una rappresentazione di A su K è una coppia (V, θ) con V K-spazio vettoriale e $\theta : A \to \mathrm{End}_K(V)$ un morfismo d'algebre.*

2. *Una rappresentazione matriciale di A è una coppia (K^n, θ) con $\theta : A \to M_n(K)$ morfismo d'algebre.*

Certamente le due nozione coincidono in dimensione finita a meno di scegliere una base.

Sulla base di quanto osservato all'inizio di questa sezione si ha che la nozione di A-modulo e la nozione di rappresentazione di A si equivalgono.

Esempio 2.2.4. *In termini di rappresentazioni intendere una K-algebra come A-modulo mediante l'azione di moltiplicazione a sinistra equivale a definire la seguente rappresentazione nota come rappresentazione regolare:*

$$\theta : A \to \mathrm{End}_K(A)$$

$$a \mapsto l_a$$

Dove l_a è l'endomorfismo dato da: $x \mapsto ax$

Definizione 2.2.6. *Siano (V_1, θ_1) e (V_2, θ_2) rappresentazioni su K della K-algebra A. Esse si diranno equivalenti se e solo se esiste un isomorfismo di Spazi Vettoriali: $\psi : V_1 \to V_2$ tale che:*

$$\theta_1(a) = \psi^{-1} \circ \theta_2(a) \circ \psi$$

per ogni $a \in A$. Nel caso di rappresentazioni matriciali la condizione è equivalente a richiedere che le diverse matrici associate ad ogni elemento di A siano simultaneamente simili mediante la stessa matrice.

Proposizione 2.2.2. *Sia A una K-algebra e siano $(V_1, \theta_1), (V_2, \theta_2)$ due K-rappresentazioni. Si ha che le due rappresentazioni sono equivalenti se e solo se V_1 e V_2 dotati della struttura di A-modulo con azione specificata dalle due rispettive rappresentazioni sono isomorfi come A-moduli.*

Dimostrazione. $\Rightarrow$) Se le due rappresentazioni sono equivalenti si ha $\psi : V_1 \to V_2$ lineare tale che:

$$\psi(a \cdot v) = \psi(\theta_1(a)(v)) = \theta_2(a)\psi(v) = a \cdot \psi(v).$$

Cioè ψ è un isomorfismo di moduli.
$\Leftarrow$) Sia $\psi : V_1 \to V_2$ un isomorfismo di A-moduli. Allora è certamente un isomorfismo di K-Spazi Vettoriali e si ha che:

$$(\psi \circ \theta_1(a))(v) = \psi(a \cdot v) = a \cdot \psi(v) = (\theta_2(a) \circ \psi)(v)$$

per ogni $v \in V$ ma allora si ha:

$$\psi \circ \theta_1 = \theta_2 \circ \psi$$

ovvero:

$$\theta_1 = \psi^{-1} \circ \theta \circ \psi$$

□

Utilizzeremo dunque da qui il concetto di rappresentazione di una K-algebra A e A-modulo interscambiabilmente in base a quale risulta più comodo.

2.3 Moduli Irriducibili e Algebre Semisemplici

Da adesso ci concentreremo su moduli di algebre, dunque indicheremo sempre con A una K-algebra e con V un A-modulo.

Definizione 2.3.1. *L'A-modulo $V \neq 0$ si dice irriducibile se e solo se ha solo sottomoduli banali.*

Esempio 2.3.1.
1. *Ogni A-modulo di $\dim_K = 1$ è irriducibile, infatti ogni sottomodulo non nullo ha dimensione 1 e quindi coincide col modulo stesso.*
2. *Abbiamo già notato nell'Esempio 2.2.2 il fatto che K^n visto come $M_n(K)$-modulo è irriducibile, quindi ci sono irriducibili di ogni dimensione.*

Lemma 2.3.1. *Sia V un A-modulo non nullo. Allora V è irriducibile se e solo se per ogni $v \in V$ non nullo si ha: $Av = V$, con $Av = \{av \mid a \in A\}$.*

Dimostrazione. $\Rightarrow$) Se V è irriducibile allora essendo Av un sottomodulo non nullo si ha $Av = V$.
$\Leftarrow$) Sia U un sottomodulo non nullo di V. Sia $u \in U$ non nullo allora: $Au \subseteq U$ essendo un sottomodulo ma $Au = V$ quindi $V = U$. □

Per il Teorema 2.2.2 si ha che se U è un sottomodulo massimale (rispetto all'inclusione) di V il quoziente V/U è irriducibile. Dunque visto che ogni K-algebra ammette almeno un A-modulo (rappresentazione regolare vista nell'Esempio 2.2.4) si ha che esistono A-moduli irriducibili [1]. Introduciamo ora una nozione molto utile.

[1] Per il Lemma di Zorn esiste un sottomodulo massimale rispetto all'inclusione.

Definizione 2.3.2. *Sia V un A-modulo. Una serie di composizione per V è una catena finita di A-Sottomoduli:*

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

tale che i fattori

$$V_i/V_{i-1}$$

per ogni $i \in \{0, \ldots, n\}$ sono irriducibili. I sottomoduli V_i sono detti termini. I quozienti V_i/V_{i-1} sono detti fattori di composizione.

Esempio 2.3.2. *1. Se V ha una serie di composizione i suoi termini la ereditano.*

2. *Sia $A = M_n(K)$ considerato come A-modulo con la rappresentazione regolare. Siano C_i i sottomoduli dati dalle matrici con tutti 0 fuori dalla i-esima colonna. Si ha che $C_i \cong K^n$ per ogni i dunque i C_i sono irriducibili per l'Esempio 2.3.1. Inoltre si ha che $C_1 \oplus C_2 \oplus \cdots \oplus C_n = M_n(K)$. Dunque:*

$$0 \subset C_1 \subset C_1 \oplus C_2 \subset \cdots \subset C_1 \oplus \cdots \oplus C_n$$

è una serie di composizione infatti usando il Teorema 2.2.1 si ha:

$$C_1 \oplus \cdots \oplus C_k / C_1 \oplus \cdots \oplus C_{k-1} \cong C_k / C_k \cap C_1 \oplus \cdots \oplus C_{k-1} \cong C_k.$$

3. *Sia V un K-spazio vettoriale di dimensione infinita. Per ragioni di dimensione i sottospazi vettoriali di dimensione* 1 *sono irriducibili, d'altro canto se un sottospazio vettoriale ha dimensione maggiore di* 1 *ammette sottspazio non banale dato da* $\mathrm{span}(v)$ *con v qualsiasi vettore non nullo del sottospazio. Dunque gli unici irriducibili in questo caso sono i sottospazi vettoriali di dimensione* 1*. Non si può dunque mai costruire una serie di composizione perché nessuna catena finita che soddisfi l'ipotesi che i fattori di composizione siano irriducibili può avere come ultimo termine V. Dunque non tutti i moduli hanno una serie di composizione.*

Lemma 2.3.2. *Se V è un A-modulo di dimensione finita ammette serie di composizione.*

Dimostrazione. La dimostrazione si fa per induzione sulla dimensione:
Per il passo base abbiamo che se V ha dimensione 1 è irriducibile per l'Esempio 2.3.1 e dunque ammette serie di composizione data da:

$$0 = V_0 \subset V_1 = V.$$

Per il passo induttivo assumiamo che ogni A-modulo di dimensione $< n$ ammette serie di composizione. Assumiamo ora che V abbia dimensione n. Se è irriducibile si conclude come prima altrimenti V ammette sottomodulo non nullo. Prendiamo quello di dimensione massima, esso sarà massimale dunque V/U sarà irriducibile. Ora per ipotesi $\dim_K(U) < \dim_K(V)$ quindi per ipotesi induttiva U ammette serie di composizione:

$$0 \subset U_1 \subset \cdots \subset U_k = U$$

allora per l'osservazione precedente la seguente è una serie di composizione per V:

$$0 \subset U_1 \subset \cdots \subset U_k = U \subset V$$

□

Proposizione 2.3.1. *Sia V un A-modulo. Se V ammette una serie di composizione anche U sottomodulo di V la ammette.*

Dimostrazione. Sia $0 \subset V_1 \subset \cdots \subset V_n = V$ una serie di composizione per V. Consideriamo:

$$0 \subset V_1 \cap U \subset \cdots \subset V_n \cap U = U$$

dove vi possono essere delle ripetizioni.
Se valutiamo $V_i \cap U/V_{i-1} \cap U = V_i \cap U/(V_i \cap U) \cap V_{i-1}$ in quanto $V_{i-1} \subset V_i$ e usando il Teorema 2.2.1 si ha:

$$V_i \cap U/(V_i \cap U) \cap V_{i-1} \cong V_{i-1} + (V_i \cap U)/V_{i-1} \subseteq V_i/V_j$$

quindi $V_i \cap U/V_{i-1} \cap U$ è irriducibile o nullo. Se eliminiamo le ripetizioni abbiamo una serie di composizione. □

Siano

$$0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

$$0 = W_0 \subset W_1 \subset \cdots \subset W_m = V$$

due serie di composizione per V. Esse si diranno equivalenti se e solo se $n = m$ ed esiste $\sigma \in S_n$ tale che $V_i/V_{i-1} \cong W_{\sigma(i)}/W_{\sigma(i)-1}$ per ogni $i = 0, \ldots, n$.

Teorema 2.3.1 (**Teorema di Jordan-Hölder**)**.** *Se un A-modulo V ammette serie di composizione, sono tutte equivalenti*

Dimostrazione. Per la dimostrazione si veda a [Kar18, Theorem 3.11]. □

Questo Teorema di fatto ci dice che i fattori di composizione di un modulo dipendono solo dal modulo stesso e ci permette anche di dare la seguente definizione:

Definizione 2.3.3. *Sia V un A-modulo, indichiamo con $l(V)$ la lunghezza di V che definiamo come la lunghezza di una qualsiasi serie di composizione per V, se la ammette. Se non la ammette poniamo $l(V) = \infty$.*

Per il Teorema di Jordan-Hölder tale definizione è ben posta.

Proposizione 2.3.2. *Sia V un A-modulo di lunghezza finita e U un suo sottomodulo, allora valgono i seguenti risultati:*

1. *V/U ammette serie di composizione*
2. *Esiste una serie di composizione con U come termine e $l(V) = l(U) + l(V/U)$.*
3. *$l(U) \leq l(V)$ e se $U \neq V$ allora $l(U) < l(V)$*

Dimostrazione. Per la dimostrazione rimandiamo a [Kar18, Proposition 3.17]. □

Abbiamo visto nell'Esempio 2.2.3 che il seguente è un morfismo di moduli.

$$\phi_v : A \to V$$

$$a \mapsto av$$

con v fissato. Il kernel di tale applicazione è $\mathrm{Ann}_A(v) = \{a \in A : av = 0\}$ dunque si ha che: $A/\mathrm{Ann}_A(v) \cong Av$. Usando dunque il Lemma 2.3.1 si ha il seguente:

Lemma 2.3.3. *Sia S un A-modulo irriducibile, allora per ogni $s \in S - \{0\}$ si ha $S \cong A/\mathrm{Ann}_A(S)$.*

Veniamo dunque ad uno dei teoremi importanti di questa sezione.

Teorema 2.3.2. *Sia A una K-algebra che ammetta serie di composizione come A-modulo regolare. Allora ogni A-modulo irriducibile compare come fattore di composizione.*

Dimostrazione. Per il lemma precedente se S è un A-irriducibile è isomorfo A/I per qualche sottomodulo I di A. Ma per la Proposizione 2.3.2 esiste una serie di composizione con I come termine; essendo A/I irriducibile, I è massimale, ma allora è il penultimo termine della serie di composizione e quindi A/I è un termine della serie di composizione. Per il teorema di Jordan-Holder si conclude. □

Dunque se conosciamo una serie di composizione per l'algebra A conosciamo tutti i suoi irriducibili, in particolare questi sono in numero finito.

Esempio 2.3.3. *Abbiamo visto una serie di composizione per l'algebra $M_n(K)$ nell'Esempio 2.3.2. Concludiamo che a meno di isomorfismo l'unico $M_n(K)$-modulo irriducibile è K^n.*

Teorema 2.3.3. *Sia $A = A_1 \times \cdots \times A_n$ una K-algebra. Gli A-moduli irriducibili sono gli A_i-moduli irriducibili visti come A-moduli.*

Dimostrazione. Per la dimostrazione si rimanda a [Kar18, Corollary 3.31]. □

Esempio 2.3.4. *Sia $A = M_{n_1}(K) \times \cdots \times M_{n_r}(K)$. Allora A ha r moduli irriducibili ovvero i K^{n_i}.*

Teorema 2.3.4 (**Lemma di Schur**)**.** *Siano S, T A-moduli irriducibili. Sia $\phi : S \to T$ un morfismo di moduli. Allora si ha:*

1. *$\phi = 0$ oppure ϕ è un isomorfismo.*
2. *se $S = T$ finito dimensionali e K è algebricamente chiuso allora $\phi = \lambda \mathrm{id}_S$*

Dimostrazione.

1. Sia $\ker(\phi)$ che $\mathrm{im}(\phi)$ sono sottomoduli, da cui si conclude.
2. $\phi : S \to S$ ammette autovalore λ essendo il campo algebricamente chiuso quindi esiste $v \in S$ tale che: $\phi(v) = \lambda \mathrm{id}_S$. Dunque $\phi - \lambda \mathrm{id}_S$ ha kernel non banale e dunque per la prima parte si conclude.

□

Introduciamo ora la fondamentale nozione di semisemplicità.

Definizione 2.3.4. *Sia V un A-modulo non nullo. V è detto semisemplice se e solo se è somma diretta di sottomoduli irriducibili. Cioè esistono sottomoduli irriducibili S_i con $i \in I$ tale che:*

$$V = \bigoplus_{i \in I} S_i.$$

Vediamo alcuni esempi:

Esempio 2.3.5. *1. Ogni modulo irriducibile è semisemplice.*

2. *Se $A = K$ allora dire che V è semisemplice è equivalente a dire che ammette una base, in tal senso la nozione di semisemplicità generalizza la nozione di base di uno spazio vettoriale.*

3. *Abbiamo visto che l'algebra $M_n(K) = C_1 \oplus \cdots \oplus C_n$. Dunque $M_n(K)$ è semisemplice.*

Enunciamo di seguito due risultati importanti.

Teorema 2.3.5. *Sia V un A-modulo, allora le seguenti condizioni sono equivalenti:*

1. *Ogni sottomodulo U di V ammette complemento, ovvero esiste C sottomodulo tale che:*
$$V = U \oplus C$$

2. *V è semisemplice*

3. *V è somma di sottomoduli irriducibili.*

Dimostrazione. Per la dimostrazione si rimanda a [Kar18, Theorem 4.3] □

Proposizione 2.3.3. *Sia A una K-algebra, valgono le seguenti:*

1. *Sia $\phi : S \to V$ un morfismo di moduli con S irriducibile, allora ϕ è nulla o $\mathrm{im}(\phi)$ è irriducibile ed isomorfa ad S.*

2. *Sia $\phi : V \to W$ un isomorfismo di moduli, allora V è semisemplice se e solo se W lo è.*

3. *Tutti i sottomoduli e i quozienti di moduli semisemplici sono semisemplici.*

4. *Se $(V_i)_{i \in I}$ è una famiglia di A-moduli non nulli allora $\bigoplus_{i \in I} V_i$ è semisemplice se e solo se ogni V_i lo è.*

Dimostrazione. Per la dimostrazione rimandiamo a [Kar18, Corollary 4.7]. □

Definizione 2.3.5. *Una K-algebra A si dice semisemplice se e solo se lo è come A-modulo regolare.*

Abbiamo già visto che ad esempio $M_n(K)$ è semisemplice.
Osserviamo che se A è semisemplice allora è somma diretta di un numero finito di sottomoduli irriducibili. Infatti per definizione: si ha $A = \bigoplus_{i \in I} S_i$ e si ha $1_A \in A$ quindi esistono $i_1, \ldots, i_k$ tali che $1_A \in \sum_{j=1}^{k} S_{i_k}$ ma $A = A1_A$ quindi $A \subseteq \sum_{j=1}^{k} S_{i_k}$ ma allora $A = \sum_{j=1}^{k} S_{i_k}$. In particolare A ha una serie di composizione data da:

$$0 \subset S_{i_1} \subset S_{i_1} \oplus S_{i_2} \subset \cdots \subset A$$

dunque in particolare gli irriducibili che compaiono nella somma diretta sono tutti e soli gli A-moduli irriducibili a meno di isomorfismo.
Vediamo ora la seguente fondamentale proposizione:

Proposizione 2.3.4. *Sia A una K-algebra allora le seguenti sono equivalenti:*

1. *A è semisemplice*
2. *Ogni A-modulo non nullo è semisemplice.*

Dimostrazione. $2 \Rightarrow 1)$ è immediato. $1 \Rightarrow 2)$ Sia V un qualsiasi A-modulo non nullo. Sia $\{v_i \in V : i \in I\}$ una base di V.
Consideriamo: $\bigoplus_{i\in I} A$ cioè mettiamo insieme tante copie di A quanti indici in I e definiamo:

$$\psi : \bigoplus_i A \to V$$

$$(a_i)_{i\in I} \mapsto \sum_i a_i v_i$$

Tale applicazione è ben definita perché $\bigoplus_i A$ contiene tuple con al più un numero finito di elementi non nulli. Essendo $\{v_i\}$ una base ψ è suriettiva quindi per il Teorema 2.2.1 si ha $V \cong \bigoplus_i A/\ker(\psi)$. Ma allora per la Proposizione 2.3.3 V è semisemplice. □

Vale il seguente fatto.

Proposizione 2.3.5. *Siano A, B K-algebre. Allora:*

1. *$\phi : A \to B$ un morfismo di algebre suriettivo, allora A è semisemplice se e solo se B lo è.*
2. *Se $A \cong B$ allora A è semisemplice se e solo se B lo è.*
3. *Ogni algebra quoziente di A semisemplice è ancora semisemplice.*

Dimostrazione. Per la dimostrazione rimandiamo a [Kar18, Corollary 4.12]. □

Concludiamo ora la seguente sezione con il seguente corollario.

Corollario 2.3.1. *Siano $A_1, \dots, A_r$ K-algebre e sia $A = A_1 \times \cdots \times A_r$. Allora A è semisemplice se e solo se ogni A_i lo è.*

Dimostrazione. $\Rightarrow$) $\pi_i : A \to A_i$ è suriettiva quindi per la proposizione precedente si conclude.
$\Leftarrow$) Sia $\epsilon_i = (0, \dots, 1_{A_i}, \dots, 0)$ e $M_i := \epsilon_i M$ che si possono vedere come A_i-moduli dunque sono semisemplici. A questo punto si può mostrare che sono semisemplici anche come A-moduli da cui $M = M_1 \oplus \cdots \oplus M_r$ è semisemplice. Si conclude poi in quanto è immediato l'isomorfismo fra M e A. □

2.4 Rappresentazioni di Gruppi e Teorema di Maschke

Introduciamo in questa sezione la nozione di rappresentazione di un gruppo. Richiamiamo che KG è l'algebra gruppo introdotta nella Definizione 2.1.2.

Definizione 2.4.1. *Sia G un gruppo. Una K-rappresentazione di G è un morfismo di gruppi $\rho : G \to \mathrm{GL}(V)$ dove V è un K-spazio vettoriale.*
Una K-rappresentazione matriciale è un morfismo: $\rho : G \to \mathrm{GL}_n(K)$.

Vogliamo mostrare che dare una rappresentazione per l'algebra gruppo di G su K è equivalente a dare una K-rappresentazione del gruppo.

Proposizione 2.4.1. *Sia G un gruppo e K un campo.*

1. *Ogni $\rho : G \to \mathrm{GL}(V)$ si estende a $\theta_\rho : KG \to \mathrm{End}_K(V)$ dove θ_ρ è data da:*

$$\sum_g \alpha_g g \mapsto \sum_g \alpha_g \rho(g)$$

2. *data $\theta : KG \to \mathrm{End}_K(V)$, la sua restrizione a G è una K-rappresentazione di G.*

Dimostrazione. 1. θ_ρ è lineare per costruzione. Per verificare che si preserva il prodotto è sufficiente valutarlo sulla base data da G:

$$\theta_\rho(ab) = \rho(ab) = \rho(a)\rho(b) = \theta_\rho(a)\theta_\rho(b)$$

per ogni $a, b \in G$.

2. θ è un morfismo di algebre e la sua restrizione a G risulta essere un morfismo di gruppi.

□

Dunque studiare le K-rappresentazioni di un gruppo G è equivalente a studiare i KG-moduli.

Lemma 2.4.1. *Sia G un gruppo finito e K un campo, siano M, N KG-moduli e $f : M \to N$ mappa K-lineare. Definiamo:*

$$T(f) : M \to N$$

$$m \mapsto \sum_{x \in G} x f(x^{-1} m)$$

si ha che $T(f)$ è un morfismo di KG-moduli.

Dimostrazione. La linearità deriva dalla proprietà distributiva e dalla linearità di f. Verifichiamo su una base che l'azione di G commuta con $T(f)$. Sia dunque $y \in G$, allora si ha per ogni $m \in M$:

$$T(f)(ym) = \sum_{x \in G} x f(x^{-1} y m) = \sum_{x \in G} y(y^{-1}x) f((y^{-1}x)^{-1} m)$$

y è fisso mentre x varia su tutto G ma allora y^{-1} varia su tutto G quindi posto $y^{-1}x = \overline{x}$ si ha:

$$T(f)(ym) = \sum_{\overline{x} \in G} y\overline{x} f(\overline{x}^{-1} m) = yT(f)(m)$$

□

Lemma 2.4.2. *Sia A una K-Algebra e siano M, N, N' A-moduli non nulli. Siano:*

$$j : N \to M$$

$$\pi : M \to N'$$

morfismi di A-moduli tali che $\pi \circ j$ sia un isomorfismo.
Si ha allora che j è iniettiva, π è suriettiva e si ha:

$$M = \mathrm{im}(j) \oplus \ker(\pi).$$

Dimostrazione. Mostriamo che $\mathrm{im}(j) \cap \ker(\pi) = 0$.
Sia $w \in \mathrm{im}(j) \cap \ker(\pi)$. Allora per ipotesi $w = j(n)$ con $n \in N$ e $\pi(w) = 0$ ovvero $\pi(j(n)) = 0$ ma $\pi \circ j$ è un isomorfismo quindi $w = 0$.
Mostriamo ora che $M = \mathrm{im}(j) + \ker(\pi)$.
Sia $\phi : N' \to N$ l'inversa di $\pi \circ j$. Allora $\pi \circ j \circ \phi = id_{N'}$. Sia $w \in M$. Si ha chiaramente che:

$$w = (j \circ \phi \circ \pi)(w) + (w - (j \circ \phi \circ \pi)(w))$$

Il primo termine è nell'immagine di j. Per il secondo si ha:

$$\pi(w - (j \circ \phi \circ \pi)(w)) = \pi(w) - (\pi \circ j \circ \phi\pi)(w) = \pi(w) - \pi(w) = 0.$$

Dunque si conclude. □

Siamo ora in grado di dimostrare il fondamentale teorema di Maschke.

Teorema 2.4.1 (**Teorema dei Maschke**)**.** *Sia K un Campo e G un gruppo finito, allora l'algebra gruppo KG è semisemplice se e solo se* $\mathrm{char}(K) \nmid |G|$

Dimostrazione. $\Leftarrow$) Sia W un sottomodulo di KG. Mostriamo che ammette complementare. Come K-Sottospazio vettoriale sicuramente esiste V sottospazio tale che $W \oplus V = KG$. Sia f il proiettore su W e poniamo $\gamma : KG \to W$ definita da:

$$\gamma := \frac{1}{|G|} T(f).$$

Tale applicazione è ben definita perché $\mathrm{char}(K) \nmid |G|$ ed è un morfismo di moduli per il Lemma 2.4.1.
Usiamo ora il Lemma 2.4.2 con $M = KG$ e $N = N' = W$, con $\pi = \gamma$ e j l'inclusione di W in KG.
Mostriamo che $\gamma \circ j = id_W$ e quindi è un isomorfismo:

$$(\gamma \circ j)(w) = \gamma(w) = \frac{1}{|G|} \sum_{g \in G} g f(g^{-1} w)$$

Essendo W un sottomodulo si ha $g^{-1}w \in W$ quindi essendo f il proiettore su W si ha $f(g^{-1}w) = g^{-1}w$ e quindi:

$$\gamma(w) = w.$$

Posto $C = ker(\gamma)$ si conclude:

$$KG = W \oplus C$$

$\Rightarrow$) Sia KG semisemplice e sia $w = \sum_{g\in G} g \in KG$. Si ha che $xw = w$ per ogni $x \in G$ da cui si ha che: $U = \text{span}(w)$ è un sottomodulo. Per semisemplicità esiste un sottomodulo C tale che $KG = U \oplus C$.
Siano $u \in U$, $c \in C$ tali che $1_{KG} = u + c$. Si deve avere $u \neq 0$ altrimenti $KG = KGc \subseteq C \neq KG$ essendo U non nullo. Dunque $u = \lambda w$ con $\lambda \in K$. Si ha ora:

$$w^2 = (\sum_{g\in G} g)w = g_1 w + \cdots + g_n w = w + \cdots + w = |G|w$$

Ma ora:

$$w = w1_{KG} = w\lambda w + wc$$

Ma $wc \in U \cap C = 0$ quindi $w - w\lambda w = 0$, perciò $w\lambda w = \lambda w^2 = \lambda|G|w$ quindi $w = \lambda|G|w$ con $w \neq 0$ quindi deve essere che $|G| \neq 0$ in K ovvero:

$$\text{char}(K) \nmid |G|.$$

□

Enunciamo ora un teorema estremamente utile per classificazione delle algebre semisemplici.

Teorema 2.4.2 (**Teorema di Artin-Wedderburn**). *Sia A una K-algebra semisemplice con K algebricamente chiuso. Si ha allora che:*

$$A \cong M_{n_1}(K) \times \cdots \times M_{n_r}(K).$$

Tale decomposizione è detta decomposizione di Artin-Wedderburn. In particolare ci sono r A-moduli irriducibili di dimensioni: $n_1, \ldots, n_r$.

Dimostrazione. Per la dimostrazione si rimanda a [Kar18, Corollary 5.11]. □

Vediamo alcune conseguenze di questo teorema e del teorema di Maschke. Mettiamoci nel caso in cui $K = \mathbb{C}$ quindi di caratteristica 0 (che quindi soddisfa le ipotesi del teorema di Maschke) e algebricamente chiuso. Sia $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$ la sua decomposizione di Artin-Wedderburn.

Teorema 2.4.3. *Sia G un gruppo finito allora si ha:*

1. *L'algebra $\mathbb{C}G$ ha k $\mathbb{C}G$-moduli irriducibili di dimensione: $n_1, \ldots, n_k$.*
2. *$|G| = \sum_{i=1}^{k} n_i^2$*
3. *G è Abeliano se e solo se tutti i $\mathbb{C}G$-irriducibili sono di dimensione 1.*

Dimostrazione.
1. Segue dal Teorema 2.4.2.
2. Segue dal fatto che $\mathbb{C}G$ ha dimensione $|G|$.
3. Segue dal fatto che $M_n(K)$ è abeliano se e solo se $n = 1$.

□

Vediamo ora in che modo possiamo ottenere informazioni sulla decomposizione di Artin-Wedderburn a partire dal gruppo dato.
Dato un gruppo G definiamo il commutatore come: $[x, y] = xyx^{-1}y^{-1}$. Sia G' il sottogruppo di G generato da elementi della forma $[x, y]$. Valgono i seguenti fatti per i quali rimandiamo a [Her10].

1. $G' \trianglelefteq G$
2. se G/G' è abeliano e se G/N è abeliano allora $G' \subseteq N$.

Vediamo ora il seguente risultato:

Corollario 2.4.1. *Sia G finito allora il numero di $\mathbb{C}G$-moduli irriducibili di dimensione 1 è dato da $|G/G'|$.*

Dimostrazione. Sia V un $\mathbb{C}G$-modulo di dimensione 1. Allora mostriamo che G' vi agisce banalmente; sia $n \in G'$ tale che $n = [x, y]$. Esistono $\alpha, \beta \in \mathbb{C}$ tali che:

$$x \cdot v = \alpha v \quad y \cdot v = \beta v$$

Dove con il punto si indica l'azione del gruppo e senza il prodotto per scalare. Allora si ha che $n \cdot v = \alpha\beta\alpha^{-1}\beta^{-1}v = v$. Perché $\mathbb{C}$ è un campo.
Per i Teoremi di Omomorfismo 2.2.1 si ha che i $\mathbb{C}G$-moduli di dimensione 1 sono in biezione con i $\mathbb{C}G/G'$-moduli di dimensione 1. Ma, essendo G/G' abeliano, per Teorema 2.4.3 segue che tutti gli irriducibili hanno dimensione 1 e che, quindi, $|G/G'| = \frac{|G|}{|G'|}$ è uguale al numero di irriducibili di dimensione 1. □

Sia C una classe di coniugio di G gruppo finito. Poniamo $\overline{c} = \sum_{g \in C} g \in KG$. Definiamo ora il centro di un algebra A come: $Z(A) := \{x \in A \mid xa = ax \quad \forall a \in A\}$. Si vede facilmente che $Z(A)$ è un sottospazio vettoriale di A.

Proposizione 2.4.2. *Sia G finito e K un campo. Allora $\overline{c}$ al variare delle classi di coniugio formano una K-base del centro $Z(KG)$.*

Dimostrazione. Intanto per ogni $x \in G$ si ha, essendo C classe di coniugio:

$$x\overline{c}x^{-1} = \sum_{g \in C} xgx^{-1} = \sum_{y \in C} y = \overline{c}$$

quindi $x\overline{c} = \overline{c}x$ e sta dunque in $Z(KG)$. Ogni g sta in un'unica classe di coniugio da cui segue che i $\overline{c}$ sono linearmente indipendenti. Mostriamo che generano il centro.
Sia $w \in Z(KG)$ allora si ha che $w = \sum_{x \in G} \alpha_x x$ in quanto G è base di KG. Essendo w nel centro si ha che $w = gwg^{-1}$ e quindi:

$$w = \sum_{x \in G} \alpha_x gxg^{-1} = \sum_{y \in G} \alpha_{g^{-1}yg} y.$$

Essendo le somme su tutto G confrontando i coefficienti si ottiene che $\alpha_x = \alpha_{g^{-1}xg}$ quindi i coefficienti sono costanti sulle classi di coniugio e quindi raccogliendo si ha:

$$w = \sum_{C} \alpha_c \overline{c}.$$

□

Teorema 2.4.4. *Sia G un gruppo finito e $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$ la sua decomposizione di Artin-Wedderburn. Allora k è uguale al numero delle classi di coniugio.*

Dimostrazione. Il centro di $\mathbb{C}G$ ha dimensione data dal numero di classi di coniugio come visto nella proposizione precedente. Sapendo che $Z(M_n(K)) = \{\lambda id : \lambda \in K\}$ (quindi ha dimensione 1) si ha che il centro di $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$ ha dimensione k da cui la tesi. □

Esempio 2.4.1. *Notiamo intanto che ogni gruppo G ha una K-rappresentazione banale data dal morfismo che manda tutti gli elementi del gruppo nel identità del campo K. Tale rappresentazione ha dimensione* 1. *Inoltre con la Definizione 1.2.6 abbiamo (per definizione di K-rappresentazione) un altra rappresentazione di dimensione* 1 *su $\mathbb{C}$ che chiamiamo rappresentazione segno. Dato che $|S_3| = 6$, usando il Teorema 2.4.3 si conclude che ci sono tre $\mathbb{C}S_3$-moduli irriducibili a meno di isomorfismo che hanno dimensione rispettivamente* $1, 1, 2$.

2.5 Prodotto Tensoriale, Rappresentazioni Ristrette ed Indotte

Introduciamo in questa sezione il prodotto tensoriale fra spazi vettoriali.
Diamo la seguente definizione preliminare:

Definizione 2.5.1. *Siano V, U, W dei K-spazi vettoriali. Sia*

$$\phi : V \times U \to W$$

una funzione. Diremo che ϕ è bilineare se e solo se è lineare su entrambi i fattori.

Consideriamo ora, conservando le notazioni della definizione precedente, un altro spazio vettoriale X. Consideriamo il seguente diagramma commutativo:

$$\begin{array}{ccc} X & \xrightarrow{f} & W \\ {\scriptstyle\phi}\uparrow & \nearrow_{\overline{f}} & \\ V \times U & & \end{array}$$

dove ϕ è bilineare e f è lineare. Si vede facilmente che sotto queste ipotesi $\overline{f} = f \circ \phi$ è bilineare. A questo punto è naturale chiedersi se esiste uno spazio vettoriale X che permetta di fattorizzare nel modo descritto sopra tutte le funzioni bilineari da $V \times U$ a W in modo unico. Tale spazio esiste ed è il prodotto tensoriale $V \otimes_K U$ che indicheremo anche con $V \otimes U$ se non ci sono ambiguità sul campo. Fissiamo dunque il campo K e consideriamo come X lo spazio vettoriale generato dai simboli $v \otimes u$ con $v \in V$ e $u \in U$. Consideriamo adesso il sottospazio vettoriale di X generato da: $(v_1+v_2)\otimes u - v_1 \otimes u - v_2 \otimes u$, $v \otimes (u_1 \otimes u_2) - v \otimes u_1 - v \otimes u_2$, $(\lambda v) \otimes u - \lambda(v \otimes u)$ ed infine $v \otimes (\lambda u) - \lambda(v \otimes u)$ al variare di $v_1, v_2, v \in V$, $u_1, u_2, u \in U$ e $\lambda \in K$. Indichiamo tale sottospazio con Y.

Definizione 2.5.2. *Definiamo il prodotto tensoriale di due spazi vettoriali V, U sul campo K come:*

$$V \otimes_K U := X/Y$$

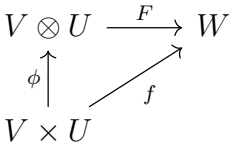
Mostriamo adesso il seguente teorema.

Teorema 2.5.1. *Siano V, U, W K-spazi vettoriali. Sia*

$$\phi : V \times U \to V \otimes U$$

$$(v, u) \mapsto v \otimes u$$

e sia $f : V \times U \to W$ un applicazione bilineare. Allora esiste un unica applicazione lineare $F : V \otimes U \to W$ che fa commutare il seguente diagramma:



Dimostrazione. Intanto per definizione di $V \otimes U$ l'applicazione ϕ è bilineare.
Definiamo F su un insieme di generatori:

$$F(v \otimes u) = f(v, u)$$

Essendo definita su un insieme di generatori tale applicazione si estende per linearità a tutto $V \otimes U$ ed è ben definita essendo f lineare e ϕ bilineare. Inoltre è chiaro che faccia commutare il diagramma sopra. Per l'unicità si rimanda a [Eti+11]. □

Si può mostrare che se $\{v_i \mid i \in I\}$ è una base di V e $\{u_j \mid j \in J\}$ è una base di U allora: $\{v_i \otimes u_j \mid i \in I, j \in J\}$. Diamo ora una definizione utile:

Definizione 2.5.3. *Siano V, U K-spazi vettoriali, diremo che $x \in V \otimes_K U$ è decomponibile se e solo se esistono $v \in V$ e $u \in U$ tali che $x = v \otimes u$.*

Si vede facilmente che non tutti gli elementi di $V \otimes_K U$ sono decomponibili, tali elementi sono detti indecomponibili.
Torniamo adesso ai moduli, in particolare al caso di KG-moduli con G un gruppo. Se $H \leq G$ abbiamo visto nell'Esempio 2.1.3 che KH è una sottoalgebra di KG dotato dunque di un morfismo di inclusione. Pertanto se V è un KG-modulo, possiamo ottenere un KH-modulo semplicemente restringendo l'azione a KH. Tale operazione sulle rappresentazioni prende il nome di restrizione. Siamo interessati alla costruzione inversa che prende il nome di induzione. Vogliamo cioè dato un KH-modulo W ottenere un KG-modulo. In particolare vorremmo una costruzione che soddisfi una proprietà universale simile a quella vista per il prodotto tensoriale. Partiamo dunque costruendo il prodotto: $KG \otimes_K W$ e definiamo una struttura di KG-modulo con la seguente azione:

$$x \cdot (g \otimes w) := xg \otimes w$$

con $x, g \in G$ e $w \in W$.
Poniamo ora $H = \text{span}\{gh \otimes w - g \otimes hw \mid g \in G, h \in H, w \in W\}$. Definiamo il modulo indotto come $KG \otimes_H W := (KG \otimes_K W)/H$ e introduciamo la notazione:

$$g \otimes_H w := g \otimes w + H.$$

Sia ora T un insieme di rappresentati del quoziente (di insiemi) G/H, ovvero tale che $G = \bigsqcup_{t\in T} tH$. Si può vedere ([Kar18]) che se W è finito dimensionale e $\{w_1, \dots, w_m\}$ è una sua base allora:

$$\{t \otimes_H w_i \mid t \in T, i = 1, \dots, m\}$$

è una base di $KG \otimes_H W$. Vediamo ora anche il seguente fatto:

Proposizione 2.5.1. *Sia K un campo, G un gruppo finito e $H \leq G$ allora se W è un KH-modulo finito dimensionale si ha che è isomorfo al sottomodulo $W_1 := \mathrm{span}\{1 \otimes_H w_i \mid i = 1, \dots, m\}$ ristretto ad un KH-modulo, dove $\{w_1, \dots, w_m\}$ è una base di W.*

Dimostrazione. Per la dimostrazione si rimanda a [Kar18, Lemma 8.14] □

Vogliamo mostrare che tale costruzione soddisfa davvero una proprietà universale simile a quella del Teorema 2.5.1

Teorema 2.5.2. *Sia K un campo, G un gruppo finito e $H \leq G$. Sia W un KH-modulo finito dimensionale e M un qualsiasi KG-modulo.*
Consideriamo:

$$\phi : W \to KG \otimes_H W$$

$$w \mapsto 1 \otimes w$$

e sia $f : W \to M$ un morfismo di KH-moduli dove consideriamo la restrizione di M a KH-modulo. Allora esiste un unico morfismo di KG-moduli

$$F : KG \otimes_H W \to M$$

che fa commutare il seguente diagramma:

$$\begin{array}{ccc} KG \otimes_H W & \xrightarrow{F} & M \\ {\scriptstyle\phi}\uparrow & \nearrow_{f} & \\ W & & \end{array}$$

Dimostrazione. Intanto ϕ è un morfismo di KH-moduli (considerando $KG \otimes_H W$ ristretto ad un KH-modulo). Infatti

$$\phi(h \cdot w) = 1 \otimes_H hw = h \otimes w = h \cdot \phi(w).$$

Definiamo ora F su una base come: $F(t \otimes_H w_i) = t \cdot f(w_i)$. In questo modo F risulta essere un morfismo di KG-moduli ed è l'unico che fa commutare il diagramma. □

Vediamo ora un caso particolare che però ci sarà utile in seguito.

Definizione 2.5.4. *Sia G un gruppo e K un campo. La K-rappresentazione banale è il morfismo di gruppi:*

$$\phi : G \to \mathrm{GL}(K)$$

$$g \mapsto \mathrm{Id}_K$$

Naturalmente tale rappresentazione dà luogo ad un KG-modulo di dimensione 1 che chiameremo nel seguito modulo banale.
Consideriamo ora la seguente situazione: sia G un gruppo finito e $H \leq G$. Sia poi $\mathcal{H} = \{g_1H, \ldots, g_kH\}$ un insieme completo di laterali. Indichiamo $K\mathcal{H}$ il K-spazio vettoriale generato da $\mathcal{H}$ come base. Possiamo dotarlo della struttura di KG-modulo con l'azione:

$$g \cdot (g_iH) = gg_iH$$

Vogliamo mostrare che questo è in realtà un caso particolare di induzione.

Teorema 2.5.3. *Sia G un gruppo finito, K un campo e $H \leq G$. Sia $W = K$ il KH-modulo banale. Allora si ha che:*

$$KG \otimes_H K \cong K\mathcal{H}$$

come KG-moduli.

Dimostrazione. Una base di $KG \otimes_H K$ è data da: $\{g_1 \otimes_H 1, \ldots, g_k \otimes 1\}$ allora l'applicazione $g_i \otimes_H 1 \mapsto g_iH$ dà l'isomorfismo di moduli cercato infatti: $gg_i \in G$ quindi si trova in unico laterale g_jH cioè $gg_i = g_jh$ per qualche $j = 1, \ldots, k$ e $h \in H$. Quindi: $g \cdot (g_i \otimes_H 1) = gg_i \otimes_H 1 = g_j \otimes h \cdot 1 = g_j \otimes 1$. Analogamente si mostra che $g \cdot (g_iH) = g_jH$ da cui si conclude. □

Capitolo 3

Rappresentazioni Irriducibili del Gruppo Simmetrico S_n

In questo capitolo giungiamo al risultato centrale della tesi ovvero arriviamo ad individuare i $\mathbb{C}S_n$-moduli irriducibili cosa che permette in questo caso di poter classificare tutti i $\mathbb{C}S_n$-moduli, daremo anche una descrizione concreta di questi moduli utilizzando i diagrammi di Ferrer.
Per i contenuti di questo capitolo, dove non esplicitamente indicato diversamente, si rimanda a [Sag01], in cui si possono trovare eventuali approfondimenti.

3.1 Sottogruppi di Young, Tableaux, Tabloidi

L'obbiettivo di questa sezione è introdurre i $\mathbb{C}S_n$-moduli M^λ (Definizione 2.2.1). Introduciamo prima un po' di notazioni e definizioni per quanto riguarda le partizioni (Definizione 1.2.7).
Introduciamo la notazione $|\lambda| = \sum_{i=1}^{l} \lambda_i$, quindi se $\lambda \vdash n$ si ha $|\lambda| = n$. Possiamo visualizzare le partizioni nella maniera seguente:

Definizione 3.1.1. *Sia $\lambda = (\lambda_1, \ldots, \lambda_l) \vdash n$. Il diagramma di Ferrer o forma di λ è un array di n punti disposti in l righe allineate a sinistra, con λ_i punti nella riga i, per $1 \leq i \leq l$.*

Diremo che il punto che si trova sulla riga i e sulla colonna j ha coordinate (i, j). Possiamo anche usare delle celle al posto dei punti. Ad esempio la partizione $\lambda = (3, 3, 1)$ ha come diagrammi di Ferrer i seguenti:

Ricordiamo che se T è un insieme, indichiamo con S_T l'insieme delle biezioni da T in T 1.1.1. Siamo ora in grado di definire i sottogruppi di Young.

Definizione 3.1.2. *Sia $\lambda = (\lambda_1, \ldots, \lambda_l) \vdash n$. Il corrispondente sottogruppo di Young di S_n è:*

$$S_\lambda = S_{\{1,\ldots,\lambda_1\}} \times S_{\{\lambda_1+1,\ldots,\lambda_1+\lambda_2\}} \times \cdots \times S_{\{n-\lambda_l+1,\ldots,n\}}$$

Vogliamo ora mostrare che questo è effettivamente isomorfo ad un sottogruppo di S_n

Proposizione 3.1.1. *Sia $\lambda = (\lambda_1, \dots, \lambda_l) \vdash n$. Allora il sottogruppo di Young S_λ è un sottogruppo di S_n.*

Dimostrazione. Notiamo intanto che $S_{\{\lambda_1+\dots+\lambda_i+1,\dots,\lambda_1+\dots+\lambda_{i+1}\}}$ per ogni $i = 1, \dots, l$ è un sottoinsieme di S_n. La composizione di due sue permutazioni è ancora una permutazione in esso. Pertanto tale sottoinsieme è chiuso rispetto al prodotto di S_n ed essendo finito è un sottogruppo per il Lemma 1.1.1.
Consideriamo ora l'insieme:

$$H = S_{\{1,\dots,\lambda_1\}} S_{\{\lambda_1+1,\dots,\lambda_1+\lambda_2\}} \dots S_{\{n-\lambda_l+1,\dots,n\}} = \{\pi_1\pi_2 \dots \pi_l : \pi_1 \in S_{\{1,\dots,\lambda_1\}} \dots, \pi_l \in S_{\{n-\lambda_l+1,\dots,n\}}\}$$

I singoli termini di tale prodotto commutano in quanto agiscono su insiemi disgiunti. Ciò garantisce il fatto che tale sottoinsieme sia un sottogruppo.
Si mostra facilmente sfruttando la commutatività che la mappa:

$$\phi : S_\lambda \to H$$

$$(\pi_1, \dots, \pi_l) \mapsto \pi_1 \dots \pi_l$$

è un isomorfismo di Gruppi. □

Noi sappiamo per il Teorema 2.4.3 che ci sono tanti $\mathbb{C}S_n$-moduli irriducili quante le classi di cogniugio di S_n ovvero tanti quanti le partizioni di n, come visto nel Teorema 1.2.3. Pertanto l'idea è partire dai sottogruppi di Young e dalla loro rappresentazione banale ed indurla ad un $\mathbb{C}S_n$-modulo. introduciamo la seguente notazione per indicare l'induzione della rappresentazione banale di S_λ a un $\mathbb{C}S_n$-modulo: $1 \uparrow_{S_\lambda}^{S_n}$. Una volta ottenute queste rappresentazioni vogliamo cercare al loro interno l'irriducibile associato alla partizione λ. Richiamiamo che se l'insieme $\{\pi_1 S_\lambda, \dots, \pi_k S_\lambda\}$ è un insieme completo di laterali allora lo spazio vettoriale $V^\lambda = \mathbb{C}\{\pi_1 S_\lambda, \dots, \pi_k S_\lambda\}$ con l'azione di S_n data da: $\pi \cdot (\pi_i S_\lambda) = (\pi\pi_i)S_\lambda$ diventa un $\mathbb{C}$ S_n-modulo isomorfo a $1 \uparrow_{S_\lambda}^{S_n}$ come visto nel Teorema 2.5.3. Vogliamo adesso dare una descrizione più concreta del modulo V^λ introducendo i tableaux ed i tabloidi.

Definizione 3.1.3. *sia $\lambda \vdash n$. Un tableau di Young di forma λ, è un array t ottenuto sostituendo i punti del diagramma di Ferrer di λ con i numeri $1, \dots, n$ bigettivamente.*

Indicheremo con $t_{i,j}$ l'entrata (i, j) del tableau t. Un tableau di Young di forma λ viene anche denotato con t^λ. Alternativamente scriveremo $sh(t) = \lambda$. Chiaramente per ogni $\lambda \vdash n$ ci sono $n!$ tableaux. Vediamo un esempio per capire meglio.

Esempio 3.1.1. *Sia $\lambda = (2, 1)$ allora i possibili tableaux di forma λ sono:*

$$\begin{array}{cc} 1 & 2 \\ 3 & \end{array} \qquad \begin{array}{cc} 2 & 1 \\ 3 & \end{array} \qquad \begin{array}{cc} 1 & 3 \\ 2 & \end{array} \qquad \begin{array}{cc} 3 & 1 \\ 2 & \end{array} \qquad \begin{array}{cc} 2 & 3 \\ 1 & \end{array} \qquad \begin{array}{cc} 3 & 2 \\ 1 & \end{array}$$

Definizione 3.1.4. *Sia $\lambda \vdash n$, due λ-tableaux t_1, t_2 si diranno equivalenti per righe, e in tal caso scriveremo $t_1 \sim t_2$, se e solo se le righe corrispondenti dei due tableaux hanno gli stessi elementi.*

Proposizione 3.1.2. *La relazione introdotta fra λ-tableaux di essere equivalenti per righe è una relazione di equivalenza.*

Dimostrazione. Siano t_1, t_2, t_3 dei λ-tableaux. Certamente ogni λ-tableaux ha in ogni riga gli stessi elementi di se stesso, analogamente se $t_1 \sim t_2, t_1$ e t_2 hanno gli stessi elementi sulle righe corrispondenti quindi si ha anche $t_2 \sim t_1$. Infine, se $t_1 \sim t_2$ e $t_2 \sim t_3$ allora t_1 ha su ogni riga corrispondente gli stessi numeri di t_2 che ha gli stessi numeri su ogni riga corrispondente di t_3 quindi anche t_1 e t_3 hanno su ogni riga corrispondente gli stessi numeri pertanto $t_1 \sim t_3$. Ciò conclude la dimostrazione. □

Definizione 3.1.5. *Un tabloide di forma λ o λ-tabloide è:*

$$\{t\} = \{t_1 : t_1 \sim t\}$$

con $sh(t) = \lambda$.
Per rappresentare un tabloide separeremo le righe del diagramma di Ferrer di un suo rappresentante con delle linee.

Vediamo anche qui un esempio con la partizione dell'Esempio 3.1.1.

Esempio 3.1.2. *consideriamo:*

$$t = \begin{array}{cc} 1 & 2 \\ 3 & \end{array}$$

allora si ha che:

$$\{t\} = \left\{ \begin{array}{cc} 1 & 2 \\ 3 & \end{array}, \begin{array}{cc} 2 & 1 \\ 3 & \end{array} \right\} = \begin{array}{|cc|} \hline 1 & 2 \\ \hline 3 & \\ \cline{1-1} \end{array}$$

Se $\lambda = (\lambda_1, \ldots, \lambda_l) \vdash n$ allora ogni tabloide contiene $\lambda_1! \ldots \lambda_l! := \lambda!$ tableaux. Quindi il numero di λ-tabloidi è $n!/\lambda!$. Vogliamo ora definire un'azione di S_n sui tableaux e sui tabloidi. Sia $\pi \in S_n$e $t = (t_{i,j})$ un λ-tableaux con $\lambda \vdash n$ allora poniamo:

$$\pi \cdot t = (\pi(t_{i,j}))$$

quindi ad esempio:

$$(1,2,3) \begin{array}{cc} 1 & 2 \\ 3 & \end{array} = \begin{array}{cc} 2 & 3 \\ 1 & \end{array}$$

Lemma 3.1.1. *Sia $\lambda \vdash n$, sia $\{t\}$ un λ -tabloide, e sia $\pi \in S_n$ allora l'azione:*

$$\pi \cdot \{t\} = \{\pi t\}$$

è ben definita.

Dimostrazione. Bisogna mostrare che se $\{t\} = \{t'\}$ allora $\{\pi t\} = \{\pi t'\}$. Se π permuta solo elementi nelle righe allora $\{\pi t\} = \{t\}$ e $\{\pi t'\} = \{t'\}$ quindi abbiamo quello che vogliamo. Assumiamo ora che π scambi i numeri a, b che si trovano rispettivamente sulle righe i_1, i_2 di $\{t\}$ e $\{t'\}$ (ciò ha senso perché hanno le righe corrispondenti con gli stessi numeri) allora per definizione la permutazione manderà a nella riga i_2 di entrambi e b nella riga i_1. Quindi i due tableaux rimangono equivalenti visto che ciò vale per ogni coppia di numeri che vengono scambiati fra due righe distinte. □

Consideriamo ora lo spazio vettoriale:

$$M^\lambda = \mathbb{C}\{\{t_1\}, \ldots, \{t_k\}\}$$

dove i $\{t_i\}$ formano un insieme completo di λ-tabloidi con $\lambda \vdash n$. Grazie al Lemma 3.1.1 possiamo dotare M^λ della struttura di $\mathbb{C}S_n$-modulo con l'azione definita sempre nel Lemma 3.1.1. Tali moduli sono detti moduli di permutazione corrispondenti a λ.
Vediamo alcuni esempi per capire meglio di cosa si tratta.

Esempio 3.1.3. *Sia $\lambda = (n)$ allora l'unico tabloide è:*

1	2	...	n

pertanto $M^\lambda \cong \mathbb{C}$ con azione banale cioè in tal caso M^λ è la rappresentazione banale.

Esempio 3.1.4. *Consideriamo $\lambda = (1, 1, \ldots, 1) = (1^n)$. In questo caso in ogni classe di equivalenza $\{t\}$ vi è un solo tableau che si può identificare mediante una permutazione di S_n. L'azione in tal caso dunque corrisponde alla moltiplicazione a sinistra pertanto si ha:*

$$M^{(1^n)} \cong \mathbb{C}S_n$$

dove $\mathbb{C}S_n$è visto come $\mathbb{C}S_n$-modulo su se stesso mediante moltiplicazione a sinistra cioè la rappresentazione regolare.

Esempio 3.1.5. *Consideriamo $\lambda = (n-1, 1)$. Qui ogni tabloide è identificato in modo univoco dal numero in posizione $(2, 1)$ pertanto si ha che:*

$$M^\lambda \cong \mathbb{C}^n$$

con azione data dalla permutazione degli elementi della base.

Proposizione 3.1.3. *Se $\lambda \vdash n$, allora M^λ è ciclico, cioè esiste un λ-tabloide $\{t\}$ tale che $M^\lambda = \mathbb{C}S_n\{t\}$. Inoltre si ha che M^λ è generato da un qualsiasi λ-tabloide. Infine si ha $\dim_{\mathbb{C}}(M^\lambda) = n!/\lambda!$*

Dimostrazione. La considerazione sulla dimensione deriva dal fatto che i λ-tabloidi sono $n!/\lambda!$ come già osservato. Si ha invece che è ciclico perché ogni talboide si può ottenere da un altro mediante una qualche permutazione. □

Proviamo ora a capire meglio qual è il rapporto fra il modulo V^λ ed M^λ. Definiamo prima di tutto il seguente λ-tabloide:

$$\{t^\lambda\} = \begin{array}{|c|c|c|} \hline 1 & ... & \lambda_1 \\ \hline \lambda_1 + 1 & ... & \lambda_1 + \lambda_2 \\ \hline \vdots & \vdots & \vdots \\ \hline n - \lambda_l + 1 & ... & n \\ \hline \end{array}$$

Vediamo ora il seguente teorema.

Teorema 3.1.1. *Sia $\lambda = (\lambda_1, \ldots, \lambda_l) \vdash n$. Allora $V^\lambda \cong M^\lambda$ come $\mathbb{C}S_n$-moduli.*

Dimostrazione. Notiamo innanzitutto che per il Teorema di Lagrange 1.1.1 la dimensione di V^λ è $n!/\lambda!$. Notiamo poi che l'azione di S_λ lascia invariato il tabloide $\{t^\lambda\}$ e se $\pi \in S_n$ lascia invariato $\{t^\lambda\}$, per costruzione, $\pi \in S_\lambda$.
Consideriamo ora l' insieme completo di laterali $\{\pi_1 S_\lambda, \dots, \pi_k S_\lambda\}$ base di V^λ e assumiamo senza perdità di generalità che $\pi_1 S_\lambda = S_\lambda$ quindi che $\pi_1 \in S_\lambda$ allora i π_i con $i \neq 1$ non stanno in S_λ e dunque la loro azione non lascia invariato il tabloide $\{t^\lambda\}$.
Siano ora $\pi_i \neq \pi_j$, se la loro azione su $\{t^\lambda\}$ fosse uguale allora si avrebbe: $\pi_i\{t^\lambda\} = \pi_j\{t^\lambda\}$ quindi $\pi_j^{-1}\pi_i\{t^\lambda\} = \{t^\lambda\}$ cioè $\pi_j^{-1}\pi_i \in S_\lambda$ quindi sono nello stesso laterale ma ciò è assurdo perché $\pi_i S_\lambda \neq \pi_j S_\lambda$ quindi $\pi_i\{t^\lambda\} \neq \pi_j\{t^\lambda\}$ per ogni $\pi_i \neq \pi_j$ dunque per ragioni di cardinalità i $\pi_i\{t^\lambda\}$ con $i = 1, \dots, k$ formano un insieme completo di λ-tabloidi.
Se definiamo quindi la funzione:

$$\phi : V^\lambda \to M^\lambda \quad \text{come} \quad \phi(\pi_i S_\lambda) = \pi_i\{t^\lambda\}$$

e prendiamo la sua estensione lineare: per ragioni di dimensione è un isomorfismo di spazi vettoriali.
Manca solo mostrare che è anche un omomorfismo di moduli. Valutiamolo sulla base individuata sopra; sia $\pi \in S_n$ allora $\pi \cdot (\pi_i S_\lambda) = \pi\pi_i S_\lambda$ ma $\pi\pi_i \in S_n$ quindi esiste un unico laterale a cui appartiene e quindi esistono π_j per qualche $j = 1, \dots, k$ e $\pi' \in S_\lambda$ tali che $\pi\pi_i = \pi_j\pi'$ quindi si ha che:

$$\phi(\pi\pi_i S_\lambda) = \pi_j\{t^\lambda\} = \pi_j\pi'\{t^\lambda\} = \pi\pi_i\{t^\lambda\} = \pi\phi(\pi_i S_\lambda)$$

dove abbiamo usato il fatto che essendo $\pi' \in S_\lambda$, lascia invariato $\{t^\lambda\}$.
Ciò conclude la dimostrazione. □

Dunque M^λ non è altro che l'induzione della rappresentazione banale di S_λ.

3.2 Relazioni d'Ordine e Dominanza

In questa sezione introdurremo un ordine per le partizioni di n.

Definizione 3.2.1. *Sia A un insieme, diremo che è un insieme ordinato se dotato di una relazione $\leq$ che soddisfa le seguenti proprietà:*

1. *$a \leq a$*
2. *Se $a \leq b$ e $b \leq a$ allora $a = b$*
3. *Se $a \leq b$ e $b \leq c$ allora $a \leq c$*

Per ogni $a, b, c \in A$. Scriveremo anche $b \geq a$ al posto di $a \leq b$. Scriveremo $a < b$ con il significato di $a \leq b$ e $a \neq b$. Se per ogni $a, b \in A$ si ha $a \leq b$ oppure $b \leq a$ diremo che $\leq$ è un ordine totale e $(A, \leq)$ è un insieme totalmente ordinato. Se $(A, \leq)$ è un insieme ordinato e vi sono $a, b \in A$ per cui non vale nè $a \leq b$ nè $b \leq a$ allora a, b si dicono incomparabili.

Diamo ora la definizione a cui siamo interessati.

Definizione 3.2.2. *Siano $\lambda = (\lambda_1 \ldots, \lambda_l)$ e $\mu = (\mu_1, \ldots, \mu_m)$ partizioni di n. Diremo che λ domina μ, scritto $\lambda \trianglerighteq \mu$, se:*

$$\lambda_1 + \cdots + \lambda_i \geq \mu_1 + \cdots + \mu_i$$

per ogni $i \geq 1$. Se $i > l$ (rispettivamente, $i > m$), allora poniamo $\lambda_i = 0$ (rispettivamente $\mu_i = 0$).

Mostriamo che questo è effettivamente un ordine per le partizioni.

Proposizione 3.2.1. *La relazione di dominanza introdotta nella Definione 3.2.2 è una relazione d'ordine sulle partizioni di n.*

Dimostrazione. Sicuramente se $\lambda \vdash n$ allora $\lambda \trianglerighteq \lambda$.
Se abbiamo $\lambda, \mu \vdash n$ e si ha $\lambda \trianglerighteq \mu$ e $\mu \trianglerighteq \lambda$ allora si ha che per ogni indice i: $\lambda_1 + \cdots + \lambda_i \geq \mu_1 + \cdots + \mu_i$ e $\lambda_1 + \cdots + \lambda_i \leq \mu_1 + \cdots + \mu_i$ cioè $\lambda_1 + \cdots + \lambda_i = \mu_1 + \cdots + \mu_i$ ovvero $l = m$ e $\lambda_i = \mu_i$ per ogni indice i.
Infine siano $\lambda, \mu, \nu \vdash n$ se $\lambda \trianglerighteq \mu$ e $\nu \trianglerighteq \lambda$ allora si ha che per ogni indice i: $\lambda_1 + \cdots + \lambda_i \geq \mu_1 + \cdots + \mu_i$ e $\nu_1 + \cdots + \nu_i \geq \lambda_1 + \cdots + \lambda_i$ cioè per ogni indice i: $\nu_1 + \cdots + \nu_i \geq \mu_1 + \cdots + \mu_i$ ovvero $\nu \trianglerighteq \mu$. □

Esempio 3.2.1. *Sia $n = 6$ si ha che $(3,3) \trianglerighteq (2,2,1,1)$ perché $3 \geq 2, 3+3 \geq 2+2$, etc. Tuttavia $(3,3)$ e $(4,1,1)$ sono incomparabili in quanto $3 \leq 4$, ma $3+3 \geq 4+1$.*

Definizione 3.2.3. *Se $(A, \leq)$ è un insieme ordinato e $b, c \in A$, allora diremo che b è coperto da c (oppure c copre b), scritto $b \prec c$ (o $c \succ b$), se $b < c$ e non esiste $d \in A$ tale che $b < d < c$.*

Mostriamo ora il seguente fondamentale lemma.

Lemma 3.2.1. *Siano t^λ e s^μ dei tableaux di forma λ e μ rispettivamente. Se, per ogni indice i, gli elementi della riga i di s^μ sono tutti su colonne diverse di t^λ, allora $\lambda \trianglerighteq \mu$.*

Dimostrazione. Non siamo interessati a quale tableux stiamo usando in quanto ci interessa solo la relazione fra partizioni, dunuqe per ipotesi possiamo ordinare le entrate di ogni colonna di t^λ in modo che gli elementi sulle righe $1, 2, \ldots, i$ di s^μ siano nelle prime i righe di t^λ. Quindi:

$$\begin{aligned} \lambda_1 + \cdots + \lambda_i = &\quad \text{numero di elementi nelle prime i righe di } t^\lambda \\ \geq &\quad \text{numero di elementi di } s^\mu \text{ nelle prime i righe di } t^\lambda \\ = &\ \mu_1 + \cdots + \mu_i. \end{aligned}$$

□

3.3 Moduli di Specht

Introdurremo in questa sezione quelli che mostreremo essere i $\mathbb{C}S_n$-moduli irriducibili. Iniziamo con alcune definizioni:

Definizione 3.3.1. *Si assuma che tableau t abbia righe $R_1, \ldots, R_l$ e colonne $C_1, \ldots, C_k$ allora:*

$$R_t = S_{R_1} \times \cdots \times S_{R_l}$$

e

$$C_t = S_{C_1} \times \cdots \times S_{C_k}$$

sono gli stabilizzatori-riga e gli stablizzatori-colonna di t, rispettivamente.

Con una dimostrazione analoga a quella della Proposzione 3.1.1 si ha che R_t e C_t sono sottogruppi di S_n.

Esempio 3.3.1. *Sia:*

$$t = \begin{array}{ccc} 4 & 1 & 2 \\ 3 & 5 & \end{array}$$

allora:

$$R_t = S_{\{1,2,4\}} \times S_{\{3,5\}}$$

e

$$C_t = S_{\{3,4\}} \times S_{\{1,5\}} \times S_{\{2\}}.$$

Si noti che $\{t\} = R_t t$. Inoltre a tali sottogruppi possiamo associare certi elementi di $\mathbb{C}S_n$. In generale infatti dato $H \subseteq S_n$, possiamo definire i seguenti elementi:

$$H^+ = \sum_{\pi \in H} \pi$$

e

$$H^- = \sum_{\pi \in H} \operatorname{sgn}(\pi)\pi$$

Poniamo

$$k_t := C_t^-$$

Si noti che sempre per la Proposizione 3.1.1 se t ha colonne $C_1, \ldots, C_k$, allora si ha:

$$k_t = k_{C_1} k_{C_2} \ldots k_{C_k}$$

Definizione 3.3.2. *Se t è un tableau, allora il politabloide associato è*

$$e_t = k_t\{t\}.$$

Vediamo meglio con un esempio.

Esempio 3.3.2. *Consideriamo il tabloide t dell'Esempio 3.3.1, si ha:*

$$k_t = (\epsilon - (3,4))(\epsilon - (1,5))$$

e quindi:

$$e_t = \begin{array}{|ccc|} \hline 4 & 1 & 2 \\ \hline 3 & 5 & \\ \cline{1-2} \end{array} \; - \; \begin{array}{|ccc|} \hline 3 & 1 & 2 \\ \hline 4 & 5 & \\ \cline{1-2} \end{array} \; - \; \begin{array}{|ccc|} \hline 4 & 5 & 2 \\ \hline 3 & 1 & \\ \cline{1-2} \end{array} \; + \; \begin{array}{|ccc|} \hline 3 & 5 & 2 \\ \hline 4 & 1 & \\ \cline{1-2} \end{array}$$

Il seguente lemma ci dice cosa succede ai vari oggetti appena definiti passando da t a πt.

Lemma 3.3.1. *Sia t un tableau e $\pi \in S_n$. Allora si ha:*

1. $R_{\pi t} = \pi R_t \pi^{-1}$
2. $C_{\pi t} = \pi C_t \pi^{-1}$
3. $k_{\pi t} = \pi k_t \pi^{-1}$
4. $e_{\pi t} = \pi e_t$.

Dimostrazione. Dimostriamo solo 1. in quanto 2. e 3. sono analoghi.
Sia $\sigma \in R_{\pi t}$ per definizione ciò è vero se e solo se si ha che $\sigma\{\pi t\} = \{\pi t\}$ visto che agiamo solo dentro le righe. Ma per come abbiamo definito l'azione sui tabloidi ciò è equivalente a: $\pi^{-1}\sigma\pi\{t\} = \{t\}$ ovvero $\pi^{-1}\sigma\pi \in R_t$ ma ciò è equivalente a $\sigma \in \pi R_t \pi^{-1}$.
Mostriamo ora 4. Si ha:

$$e_{\pi t} = k_{\pi t}\{\pi t\} = \pi k_t \pi^{-1}\{\pi t\} = \pi k_t\{t\} = \pi e_t.$$

In particolare 4. ci dice che ogni politabloide si ottiene da una qualche permutazione di un politabloide fissato. □

Siamo finalmente in grado di definire i moduli di Specht.

Definizione 3.3.3. *Per ogni $\lambda \vdash n$, il corrispondente modulo di Specht, S^λ, è il sottomodulo di M^λ generato dai politabloidi e_t dove t ha forma λ.*

Proposizione 3.3.1. *Gli S^λ sono moduli ciclici generati da un qualsiasi politabloide.*

Dimostrazione. Segue immediatamente dal Lemma 3.3.1. □

Vediamo ora in dettaglio alcuni esempi.

Esempio 3.3.3. *Sia $\lambda = (n)$. Siccome $M^{(n)}$ ha dimensione 1 è irriducibile dunque essendo che $\underline{1\ \ 2\ \ \ldots\ \ n} \in S^{(n)}$, $S^{(n)}$ è non nullo quindi si ha che $S^{(n)} = M^{(n)}$ ed è irriducibile.*

Esempio 3.3.4. *Sia $\lambda = (1^n)$ e fissiamo:*

$$t = \begin{matrix} 1 \\ 2 \\ \vdots \\ n \end{matrix}$$

Quindi:

$$k_t = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\sigma.$$

E allora per definizione $e_t = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\sigma\{t\}$. Usando ora il Lemma 3.3.1 si ha che:

$$e_{\pi t} = \pi e_t = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma)\pi\sigma\{t\}$$

Ora poniamo $\pi\sigma := \tau$ *e si ha:*

$$e_{\pi t} = \sum_{\tau \in S_n} \operatorname{sgn}(\pi^{-1}\tau)\tau\{t\} = \operatorname{sgn}(\pi^{-1}) \sum_{\tau \in S_n} \operatorname{sgn}(\tau)\tau\{t\}$$

ora usando il fatto che $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$*) si ha che:*

$$e_{\pi t} = \operatorname{sgn}(\pi) e_t$$

Cioè ogni politabloide è un multiplo scalare di e_t *e l'azione è data da* $\pi e_t = \operatorname{sgn}(\pi)e_t$*. Quindi:*

$$S^{(1^n)} = \mathbb{C}\{e_t\}$$

Con l'azione descritta sopra. Tale rappresentazione è la rappresentazione segno vista nella Definizione 1.2.6

Esempio 3.3.5. *Sia* $\lambda = (n, n-1)$*. Come visto nell'Esempio 3.1.5 possiamo identificare i tabloidi* $\{t\}$ *con l'elemento* k *in posizione* $(2,1)$ *quindi poniamo:*

$$\{t\} := \boldsymbol{k}$$

Per definizione se i *è l'elemento in posizione* $(1,1)$ *allora si ha che* $e_t = \boldsymbol{k - i}$*. Quindi* $S^{(n-1,1)}$ *è generato (a meno di riordinare la prima riga ma ciò è irrilevante visto che stiamo lavorando con i tabloidi) da:* $\boldsymbol{\{2-1, 3-1, \ldots, n-1\}}$ *cioè:*

$$S^{(n-1,1)} = \{c_1\mathbf{1} + \cdots + c_n\boldsymbol{n} : c_i \in \mathbb{C} \quad con \quad i = 1, \ldots, n, \quad c_1 + \cdots + c_n = 0\}$$

con azione data dalla permutazione degli elementi della base. Mostriamo che tale modulo è irriducibile.
Sia U *un sottomodulo non nullo di* $S^{(n-1,1)}$*. Sia* $u \in U$ *non nullo, allora a meno di permutazione possiamo assumere che* u *sia della forma* $u = (0, \ldots, u_i, \ldots, u_n)$ *con* $u_j \neq 0$ *per ogni* $j = i, i+1, \ldots, n$*. Siccome le coordinate si devono sommare a 0 ci sono almeno due entrate non nulle quindi esiste* $j > i$ *tale che* $u_j \neq 0$*. Consideriamo ora l'elemento* $u' = u - \frac{u_i}{u_j}(i,j)u$*. Certamente* $u' \in U$ *essendo* U *un sottomodulo ed inoltre l'entrata* i*-esima di* u' *è nulla quindi* u' *ha un entrata in meno di* u*. Iterando tale procedimento otteniamo, considerando che la somma delle coordinate deve essere nulla,* $(0, \ldots, -u_{n-1}, u_{n-1})$ *e a meno di permutazione e riscalamento abbiamo che i vettori della base di* $S^{(n-1,1)}$ *ovvero:* $(-1, 0, \ldots, 0, 1, 0, \ldots, 0)$ *sono in* U *pertanto* $U = S^{(n-1,1)}$ *ed è quindi un irriducibile di dimensione* $n-1$*.*

Esempio 3.3.6. *Consideriamo* S_3*. Dall'Esempio 2.4.1 sappiamo che ci sono tre* $\mathbb{C}S_3$*-moduli irriducibili (a meno di isomorfismo) di dimensioni 1, 1, 2. Dunque in questo caso* $S^{(3)}, S^{(1^3)}, S^{(2,1)}$ *costituiscono un insieme completo di* $\mathbb{C}S_3$*-moduli irriducibili.*

3.4 Teorema del Sottomodulo

In questa sezione mostriamo che i moduli S^λ costituiscono un insieme completo di $\mathbb{C}S_n$-moduli irriducili (a meno di isomorfismo).
In questa sezione quando $H \subseteq S_n$ e $H = \{\pi\}$ poniamo $\pi^- = H^-$. Introduciamo ora un prodotto interno su M^λ.

Definizione 3.4.1. *Definiamo l'applicazione* $\langle \quad , \quad \rangle : M^\lambda \times M^\lambda \to \mathbb{C}$ *nel seguente modo. Su una base:*

$$\langle \{t\}, \{s\} \rangle = \delta_{\{t\},\{s\}}.$$

Si estende poi per linearità sulla prima entrata e per antilinearità sulla seconda entrata.

Si vede facilmente che tale applicazione è non degenere ovvero: $\langle w, v \rangle = 0$ per ogni $v \in M^\lambda$ allora $w = 0$. In effetti se $\langle w, v \rangle = 0$ per ogni $v \in M^\lambda$ allora ciò è vero per i tabloidi della base ma allora per linearità e per definizione w ha tutte le coordinate nulle ed è dunque nullo.

Proposizione 3.4.1. *Il prodotto interno introdotto nella Definizione 3.4.1 è* $\mathbb{C}S_n$*-invariante, ovvero se* $a \in \mathbb{C}S_n$ *e* $v, u \in M^\lambda$ *si ha che:*

$$\langle av, aw \rangle = \langle v, w \rangle$$

Dimostrazione. Per linearità è sufficiente verificare la proprietà richiesta per una base di M^λ e per $\pi \in S_n$.
Allora si ha: $\langle \pi\{t\}, \pi\{s\} \rangle = \delta_{\pi\{t\},\pi\{s\}}$ ma π è una biezione quindi:
$\delta_{\pi\{t\},\pi\{s\}} = \delta_{\{t\},\{s\}} = \langle \{t\}, \{s\} \rangle$. □

Vediamo alcuni corollari di tale proposizione:

Corollario 3.4.1. *Siano* $v, w \in M^\lambda$ *e* $\pi \in S_n$ *allora si ha che:*

$$\langle \pi v, w \rangle = \langle v, \pi^{-1} w \rangle$$

Dimostrazione. Si ha la seguente catena di uguaglianze valide per la Proposizione 3.4.1:

$$\langle \pi v, w \rangle = \langle \pi^{-1}\pi v, \pi^{-1} w \rangle = \langle v, \pi^{-1} w \rangle.$$

□

Corollario 3.4.2. *Se* $U \subseteq M^\lambda$ *è un* $\mathbb{C}S_n$*-sottomodulo allora anche* $U^\perp$ *è un* $\mathbb{C}S_n$*-sottomodulo di* M^λ*.*

Dimostrazione. Per definizione $u \in U^\perp$ se e solo se $\langle u, v \rangle = 0$ per ogni $v \in U$. Si ha che: $\langle \pi u, v \rangle = \langle u, \pi^{-1} v \rangle$ per il Corollario 3.4.1, ma U è un sottomodulo quindi $\pi^{-1} v \in U$ e quindi:

$$\langle \pi u, v \rangle = \langle u, \pi^{-1} v \rangle = 0.$$

Cioè $\pi u \in U^\perp$. □

Siamo pronti per mostrare il lemma fondamentale di questa sezione:

Lemma 3.4.1. *Sia* $H \leq S_n$ *un sottogruppo, allora:*

1. *Se* $\pi \in H$*, allora:*

$$\pi H^- = H^- \pi = \operatorname{sgn}(\pi) H^-$$

   O in altre parole: $\pi^- H^- = H^-$*.*

2. *Per ogni* $u, v \in M^\lambda$*,*

$$\langle H^- u, v \rangle = \langle u, H^- v \rangle$$

3. *Se la trasposizione* $(b,c) \in H$*, allora possiamo fattorizzare:*

$$H^- = k(\epsilon - (b,c))$$

con $k \in \mathbb{C}S_n$*.*

4. *Se* t *è un tableau con* b, c *nella stessa riga di* t *e* $(b,c) \in H$ *allora:*

$$H^-\{t\} = 0$$

Dimostrazione. 1. La dimostrazione è analoga a quella dell'Esempio 3.3.4 per cui $\pi e_t = sgn(\pi)e_t$ ovvero (moltiplicando per $sgn(\pi)$) $\pi^- e_t = e_t$.

2. Usiamo il Corollario 3.4.1 e il fatto che $sgn(\pi) = sgn(\pi^{-1})$,

$$\langle H^- u, v\rangle = \sum_{\pi\in H}\langle sgn(\pi)\pi u, v\rangle = \sum_{\pi\in H}\langle u, sgn(\pi^{-1})\pi^{-1}v\rangle$$

ora siccome H è un sottogruppo i π^{-1} al variare di $\pi \in H$ ci danno tutti gli elementi di H quindi l'ultimo termine è: $\langle u, H^- v\rangle$.

3. Consideriamo il sottogruppo $K = \{\epsilon, (b,c)\}$, sia: $\{k_1 K, \ldots, k_m K\}$ un insieme completo di laterali. Si ha: $H = \bigsqcup_i k_i K$ e quindi: $H^- = (\sum_i k_i^-)(\epsilon - (b,c))$ come richiesto.

4. Per ipotesi, $(b,c)\{t\} = \{t\}$ quindi usando il punto precedente:

$$H^-\{t\} = k(\epsilon - (b,c))\{t\} = k(\{t\} - \{t\}) = 0.$$

□

Vediamo ora alcuni corollari di tale Lemma.

Corollario 3.4.3. *Sia* $t = t^\lambda$ *un* λ*-tableau e* $s = s^\mu$ *un* μ*-tableau, con* $\lambda, \mu \vdash n$*. Se* $k_t\{s\} \neq 0$*, allora* $\lambda \trianglerighteq \mu$*. Se* $\lambda = \mu$*, allora* $k_t\{s\} = \pm e_t$*.*

Dimostrazione. Siano b, c due elementi sulla stessa riga di s^μ. Essi non possono essere sulla stessa colonna di t^λ in quanto se così fosse $k_t = (\epsilon - (b,c))$ e $k_t\{s\} = 0$ per i punti $3, 4$ del precedente lemma. Dunque per il Lemma 3.2.1 si ha $\lambda \trianglerighteq \mu$.
Se $\lambda = \mu$ allora si ha $\{s\} = \pi\{t\}$ per qualche $\pi \in C_t$. Quindi usando il punto 1 del precedente lemma si ha:

$$k_t\{s\} = k_t\pi\{t\} = sgn(\pi)k_t\{t\} = \pm e_t.$$

□

Corollario 3.4.4. *Se* $u \in M^\mu$ *e* $sh(t) = \mu$*, allora* $k_t u$ *è un multiplo di* e_t*.*

Dimostrazione. Si ha che $u = \sum_i c_i\{s_i\}$ con s_i dei μ-tableaux. Allora per il corollario precedente, $k_t u = \sum_i \pm c_i e_t$. □

Siamo ora in grado di mostrare il teorema del sottomodulo:

Teorema 3.4.1 (**Teorema del Sottomodulo**). *Sia U un $\mathbb{C}S_n$-sottomodulo di M^μ. Allora:*

$$S^\mu \subseteq U \quad \textit{oppure} \quad U \subseteq S^{\mu\perp}.$$

Dimostrazione. Sia $u \in U$ e t un μ-tableau. Per il corollario precedente si ha che $k_t u = fe_t$ per qualche $f \in \mathbb{C}$. Ci sono due casi possibili.
Se esistono u e t tali che $f \neq 0$ allora, essendo U un sottomodulo si ha che $k_t u \in U$ cioè $fe_t \in U$ quindi essendo $f \neq 0$ si ha $e_t \in U$ ed essendo S^μ cicilco si ha: $S^\mu \subseteq U$. Se invece si ha sempre $k_t u = 0$, consideriamo $u \in U$ e dato un $\mu-$tableau t, usiamo la 2 del Lemma 3.4.1 e si ha:

$$\langle u, e_t \rangle = \langle u, k_t\{t\}\rangle = \langle k_t u, \{t\}\rangle = 0.$$

Quindi $U \subseteq S^{\mu\perp}$. □

Proposizione 3.4.2. *Sia $\theta \in Hom_{\mathbb{C}S_n}(S^\lambda, M^\mu)$ non nulla. Allora $\lambda \trianglerighteq \mu$ e se $\lambda = \mu$, allora θ è la moltiplicazione per uno scalare.*

Dimostrazione. Intanto $\theta \neq 0$ quindi esiste e_t tale che $\theta(e_t) \neq 0$. Siccome il nostro campo è $\mathbb{C}$ e il prodotto interno definito in 3.4.1 è non degenere si ha che $M^\mu = S^\mu \oplus S^{\mu\perp}$ quindi possiamo definire $\theta' : M^\lambda \to M^\mu$ come: $\theta'|_{S^\lambda} = \theta$ e $\theta'|_{S^{\lambda\perp}} = 0$. La funzione $\theta' \in \mathrm{Hom}_{\mathbb{C}S_n}(M^\lambda, M^\mu)$ per definizione di somma diretta di sottomoduli. A questo punto si ha:

$$0 \neq \theta'(e_t) = \theta'(k_t\{t\}) = k_t\theta'(\{t\}) = k_t \sum_i c_i\{s_i\}.$$

Dove s_i sono $\mu-$tableaux. Per il Corollario 3.4.3 si ha: $\lambda \trianglerighteq \mu$.
Se $\lambda = \mu$ allora usando il Corollario 3.4.4 si ha che $\theta'(e_t) = ce_t$ per qualche scalare c. Allora per ogni permutazione π. Si ha:

$$\theta'(e_{\pi t}) = \theta'(\pi e_t) = \pi\theta'(e_t) = ce_{\pi t}.$$

Quindi su una base θ' è la moltiplicazione per uno scalare quindi è la moltiplicazione per scalare. □

Teorema 3.4.2. *Gli S^λ con $\lambda \vdash n$ formano un insieme completo di $\mathbb{C}S_n$-moduli irriducibili.*

Dimostrazione. Intanto mostriamo che gli S^λ sono irriducibili. Essendo il nostro campo $\mathbb{C}$ si ha che $S^\lambda \cap S^{\lambda\perp} = 0$. Sia ora $U \subseteq S^\lambda$ un sottomodulo non nullo. Sicuramente $U \nsubseteq S^{\lambda\perp}$ quindi per il teorema del sottomodulo $S^\lambda \subseteq U$ cioè $U = S^\lambda$, quindi gli S^λ sono irriducibili.
Mostriamo che sono a due a due non isomorfi. Se $S^\lambda \cong S^\mu$ allora $Hom_{\mathbb{C}S_n}(S^\lambda, M^\mu) \neq 0$ quindi per la precedente proposizione $\lambda \trianglerighteq \mu$, analogamente si ha che $\mu \trianglerighteq \lambda$ quindi $\lambda = \mu$. Dunque gli S^λ con $\lambda \vdash n$ sono irriducibili e sono a due due non isomorfi quindi essendo tanti quante le classi di cogniugio di S_n sono una lista completa di $\mathbb{C}S_n$-irriducibili. □

Sapendo dal Teorema 2.4.1 che $\mathbb{C}S_n$ è semisemplice, il precedente teorema insieme alla Proposizione 2.3.4 ci permettono di classificare tutti i $\mathbb{C}S_n$-moduli, cioè capire dati due $\mathbb{C}S_n$-moduli V_1 e V_2, se sono isomorfi o meno. Questo si può vedere guardando se hanno la stessa decomposizione in irriducibili.

Capitolo 4

Operatori di Kraus e Gruppo Simmetrico

In questo capitolo con gli strumenti sviluppati nei precedenti capitoli usiamo le rappresentazioni dei gruppi simmetrici per ottenere delle equazioni di evoluzione dinamica per sistemi quantistici aperti e ci soffermeremo a fare alcuni esempi in casi semplici.
Per i contenuti di questo capitolo, dove non esplicitamente indicato diversamente, si rimanda a [Cat+21], in cui si possono trovare eventuali approfondimenti.

4.1 Introduzione e Preliminari

L'obiettivo di questo capitolo è lo studio di sistemi quantistici aperti, ovvero sistemi che sono liberi di interagire con l'ambiente o con altri sistemi.

In Meccanica quantistica, lo Stato di un sistema chiuso è dato da un raggio in uno spazio di Hilbert separabile [1] $\mathcal{H}$. Ovvero da una classe di vettori $[v]$ con $v \in \mathcal{H}$ rispetto alla relazione di equivalenza $v \sim \lambda v$ con $\lambda \in \mathbb{C} - \{0\}$. Adottiamo in seguito la notazione di Dirac per gli elementi di $\mathcal{H}$. Considereremo solo spazi di Hilbert finito-dimensionali di dimensione n. Un modo equivalente per descrivere un raggio in uno spazio di Hilbert è mediante il proiettore sullo stato che ci interessa:

$$\rho_v = |v\rangle\langle v|/||v||.^2$$

Tale operatore è un proiettore a traccia unitaria, autoaggiunto, definito positivo e di rango 1 che prende il nome di matrice densità. Quando uno stato può essere descritto in questo modo si dice puro.
In generale la matrice densità ci permette di trattare meglio non solo il caso puro ma anche il caso di miscele statistiche. Precisiamo meglio tale punto.
In Meccanica quantistica le probabilità intervengono su due livelli:

1. Vi è una probabilità intrinseca agli stati. Se ci limitiamo al caso finito-dimensionale sappiamo che ogni operatore autoaggiunto ammette una base ortonormale di autovettori. In Meccanica quantistica le osservabili sono rappresentati da operatori autoaggiunti. Sia $\{|u_n\rangle\}$ con $n = 1, \ldots, N$ una base ortonormale di autovettori

[1] Per la definizione si veda [CDL91].

dell'osservabile A con autovalori: $\{a_n\}$. Se viene effettuata una misura sullo stato $|\psi\rangle = \sum_n c_n|u_n\rangle$, i possibili esiti della misura sono gli autovalori e la probabilità che una misura abbia come esito a_n è $P(a_n) = \sum_k^{g_k} |c_k|^2$ dove i c_k sono i coefficienti associati agli autovettori di a_n e g_k è la molteplicità algebrica dell'autovalore. A seguito della misura lo stato viene proiettato sull'autospazio relativo ad a_n.

2. Vi può essere una probabilità non intrinseca allo stato data dalla nostra conoscenza parziale dello stato del sistema. In tal caso si dice che lo stato è in una miscela statistica in cui si può trovare in un qualche stato: $\{|\psi_1\rangle, \ldots, |\psi_k\rangle\}$ con probabilità rispettivamente: $p_1, \ldots, p_k$. In tal caso $|\psi_i\rangle$ non sono per forza ortogonali mentre per le p_i essendo delle probabilità vale: $\sum_{i=1}^k p_i = 1$ e $0 \leq p_i \leq 1$.

Quando uno stato è descritto da una miscela statistica è detto misto ed in tal caso la matrice densità è data da:

$$\rho = \sum_{i=1}^{N} p_i \rho_i$$

dove le ρ_i sono le matrici densità degli stati puri della miscela statistica e le p_i le probabilità. In questo caso ρ è autoaggiunto, a traccia unitaria e definito positivo ma non è più un proiettore.
Quando consideriamo un sistema quantistico aperto A che interagisce con l'ambiente B si ha che lo spazio di Hilbert che rappresenta l'intero stato è dato da: $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes_\mathbb{C} \mathcal{H}_\mathcal{B}$. Siano $\{e_i^A : i \in I\}$ e $\{e_j^B : j \in J\}$ basi ortonormali di $\mathcal{H}_\mathcal{A}$ e $\mathcal{H}_\mathcal{B}$ rispettivamente, allora un generico elemento di $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ sarà dato da: $\psi_{AB} = \sum_{i\in I, j\in J} a_{ij} e_i^A \otimes e_j^B$ con $\sum |a_{ij}|^2 = 1$.
La matrice densità del sistema A è data dalla traccia parziale su B della matrice densità totale: $\rho_A = Tr_B(\rho_{\psi_{AB}}) = \sum_{j\in J} \langle e_j^B | \rho_{\psi_{AB}} | e_j^B \rangle$.
Un noto teorema ([CDL91]) ci dice che lo stato ψ_{AB} è decomponibile (Definizione 2.5.3) se e solo se ρ_A è pura.
Per un sistema quantistico chiuso, nel caso in cui l'Hamiltoniana $\mathbb{H}$ non dipenda dal tempo, l'evoluzione temporale è data dall'operatore unitario $U(t) = \exp[-i\mathbb{H}t/\hbar]$ mediante:

$$\rho(t) = U(t)\rho(t=0)U(t)^\dagger$$

con $U(t)^\dagger$ è l'aggiunto di $U(t)$. Per maggiori dettagli si veda [CDL91]
La dinamica dei sistemi aperti è generata dall'equazione di Gorini-Kossakowski-Sudarshan-Lindbland (GKLS) [Cat+21]:

$$L(\rho) = -i[\mathbb{H}, \rho] - \frac{1}{2}\sum_{j=1}^{N} \{V_j^\dagger V_j, \rho\} + \sum_{j=1}^{N} V_j \rho V_j^\dagger,$$

dove $[\cdot,\cdot]$ è il commutatore, $\{\cdot,\cdot\}$ è l'anticommutatore e le V_j sono operatori limitati arbitrari (con $N = 1, \ldots, n^2 - 1$ dove n è la dimensione di $\mathcal{H}$). Cioè la dinamica dei sistemi aperti è governata dalla seguente equazione differenziale:

$$\frac{d}{dt}\rho = L(\rho).$$

Un approccio diverso, ma equivalente, adottato in [Cat+21], è quello secondo cui la dinamica di un sistema aperto con matrice densità $\rho_A(t_0) \equiv \rho(t_0)$ è descritto dalle cosiddette

Mappe Universali Dinamiche (UDM), ovvero mappe lineari completamente positive [2] che preservano la traccia date da:

$$\varepsilon_{K([t_0,t_1])} : \rho(t_0) \to \rho(t_1) = \sum_\alpha K_\alpha(t_1,t_0)\rho(t_0)K_\alpha(t_1,t_0)^\dagger \tag{4.1}$$

data una configurazione iniziale al tempo $t = t_0$ espressa da $\rho(t_0)$. Gli operatori K_α sono detti operatori di Kraus, non dipendono dalla condizione iniziale ma solo dall'intervallo di tempo $[t_0, t_1]$. Chiameremo mappa di Kraus una qualsiasi combinazione lineare di operatori di Kraus. Inoltre per assicurare che la traccia venga preservata si deve avere:

$$\sum_\alpha K_\alpha(t_1,t_0)K_\alpha(t_1,t_0)^\dagger = \mathbf{1}.$$

Quando gli operatori dell'Equazione (4.1) dipendono solo dalla differenza $(t_1 - t_0)$ e soddisfano la legge di composizione

$$\varepsilon_{K([s,t])} \circ \varepsilon_{K([t,0])} = \varepsilon_{K([s,0])}$$

per ogni $s \geq t \geq 0$ l'equazione definisce un semigruppo a un parametro che è generato da L.
Vogliamo di seguito caratterizzare la parte non unitaria della dinamica quindi poniamo $\mathbb{H} = 0$. Notiamo che le equazioni GKLS sono invarianti per trasformazioni unitarie in quanto: $\rho(t) \to U\rho(t)U^\dagger, V_j \to UV_jU^\dagger$, per ogni j. Inoltre possiamo sempre diagonalizzare $\rho(0) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ con $\lambda_i \geq 0$ e $\lambda_1 + \cdots + \lambda_n = 1$. Dunque possiamo considerare un equazione GLKS della forma:

$$L(\rho) = -\frac{1}{2}\sum_{j=1}^{N}\{V_j^\dagger V_j, \rho\} + \sum_{j=1}^{N}(V_j\rho V_j^\dagger)$$

con ρ diagonale.
Per descrivere tale situazione prenderemo una via algebrica basata sulla teoria delle rappresentazioni di S_n.

4.2 Rappresentazioni di S_n e Mappe di Kraus

Vogliamo in questa sezione capire come associare mappe di Kraus ad elementi di $\mathbb{C}S_n$. Innanzitutto, in questa sezione lavoreremo con il $\mathbb{C}S_n$-modulo $\mathbb{C}^n$ con azione data dalla permutazione degli elementi della base canonica visto nell'Esempio 3.1.5. A tale $\mathbb{C}S_n$-modulo corrisponde la seguente rappresentazione unitaria su $\mathbb{C}$ di S_n:

$$\chi : S_n \to GL_n(\mathbb{C})$$

$$\sigma \mapsto R_\sigma$$

[2] Con completamente positivo intendiamo che la mappa $K_{[t_0,t_1]} \otimes 1_B$ è definita positiva per ogni estensione di $\mathcal{H}_A$ ad $\mathcal{H}_A \otimes \mathcal{H}_B$.

Con R_σ data da:

$$(R_\sigma)_{ij} = \begin{cases} 1 & \text{se } \sigma(j) = i. \\ 0 & \text{altrimenti.} \end{cases}$$

Sappiamo in particolare dalla Proposizione 2.3.4 e dal Teorema 2.4.1 che tale rappresentazione è semisemplice e ha come sottomodulo irriducibile quello visto nell'Esempio 3.3.5. Notiamo che se identifichiamo $\mathbb{C}^n$ con $D_n(\mathbb{C})$ l'azione di S_n è data da:

$$\sigma \cdot \mathrm{diag}(\lambda_1, \dots, \lambda_n) = \mathrm{diag}(\lambda_{\sigma(1)}, \dots, \lambda_{\sigma(n)})$$

Definiamo ora una dipendenza temporale: per ogni $\sigma \in S_n$ scegliamo delle funzioni lisce $c_\sigma(t)$ per $t \in [0, +\infty)$ e a valori in $\mathbb{C}$ e consideriamo la mappa:

$$[0, +\infty) \ni t \mapsto \sum_{\sigma \in S_n} c_\sigma(t)\sigma \in \mathbb{C}S_n$$

Se guardiamo all'operatore ottenuto mediante χ si ha che

$$\sum_{\sigma \in S_n} (c_\sigma(t)R_\sigma)(c_\sigma(t)R_\sigma)^\dagger = \sum_{\sigma \in S_n} c_\sigma(t)\overline{c_\sigma}(t)R_\sigma R_\sigma^\dagger = (\sum_{\sigma \in S_n} c_\sigma(t)\overline{c_\sigma}(t))\mathrm{Id}_n$$

Dove $\overline{c_\sigma}(t)$ è la funzione complessa coniugata. Quindi se:

$$\sum_{\sigma \in S_n} c_\sigma(t)\overline{c_\sigma}(t) = \mathbf{1} \tag{4.2}$$

dove $\mathbf{1}$ è la funzione costante uguale ad 1 si ha che $\sum_{\sigma \in S_n} c_\sigma(t)\sigma$ agisce su $D_n(\mathbb{C})$, mediante χ, come un operatore di Kraus. Serve comunque avere la completa positività e la condizione temporale.
Dato un sottogruppo S di S_n vi associamo:

$$K_S = g(t)\mathrm{Id}_n + f(t)\sum_{\sigma \in S} R_\sigma$$

dove:

$$g(t) = \sqrt{\frac{1}{|S|}(1 + (|S| - 1)e^{-t})} \quad f(t) = \sqrt{\frac{1}{|S|}(1 - e^{-t})}$$

con $|S|$ ordine del sottogruppo, si ha che K_S soddisfa la condizione (4.2). Vedremo che da origine proprio ad un operatore di Kraus. Tale operatore dà origine all'equazione di evoluzione data da:

$$F^S_{(t,0)}(\rho(0)) = \rho(t) = g^2(t)\rho(0) + f^2(t)\sum_{\sigma \in S} R_\sigma \rho(0) R_\sigma^{-1}.$$

Dati due sottogruppi S, T diremo che K_S, K_T sono equivalenti, e in tal caso scriviamo $K_S \cong K_T$, se danno origine alla stessa evoluzione temporale ovvero:

$$F^S_{(t,0)}(\rho(0)) = F^T_{(t,0)}(\rho(0))$$

per ogni $t \in [0, +\infty)$ e ogni $\rho(0) \in D_n(\mathbb{C})$. Visto che siamo interessati alle equazioni di evoluzione ci interessano le mappe di Kraus associate a sottogruppi di S_n a meno di equivalenza. In tal senso abbiamo il seguente risultato:

Proposizione 4.2.1. *Due mappe di Kraus K_S, K_T associate a due sottogruppi S, T di S_n, sono equivalenti se e solo se la partizione di $\{1, \dots, n\}$ associata alle orbite dell'azione di S, T su $\{1, \dots, n\}$ è la stessa.*

Dimostrazione. Due mappe di Kraus K_S, K_T sono equivalenti se e solo se $|S| = |T|$ e si ha:

$$\sum_{\sigma \in T} R_\sigma \rho(0) R_\sigma^{-1} = \sum_{\sigma' \in S} R_{\sigma'} \rho(0) R_{\sigma'}^{-1}.$$

Vi è dunque una biezione tra T ed S che manda σ in σ'. Siccome R_σ sono matrici di permutazione ciò è vero se e solo se le orbite dell'azione di S, T su $\{1, \dots, n\}$ sono le stesse. □

Notiamo che se $\lambda = (\lambda_1, \dots, \lambda_k) \vdash n$ e consideriamo il sottogruppo ciclico (1.1.9) generato da $\sigma = c_1 c_2 \dots c_k$ dove c_i è un qualsiasi ciclo che permuta λ_i. Per la proposizione precedente è chiaro che a meno di equivalenza possiamo guardare le mappe di Kraus associate a questi sottogruppi.
Notiamo ora anche che se S, T sono sottogruppi cogniugati allora possiamo dedurre l'evoluzione $F^T_{(t,0)}$ da $F^S_{(t,0)}$ in quanto:

1. Intanto, $|S| = |T|$ quindi $g_T(t) = g_S(t)$ e $f_T(t) = f_S(t)$
2. $\sum_{\sigma \in T} R_\sigma \rho(0) R_\sigma^{-1} = \sum_{\sigma' = \tau \sigma \tau^{-1} \in S} R_{\sigma'} \rho(0) R_{\sigma'}^{-1}$ dove $\tau \in T$.

In particolare i gruppi sopra descritti sono unici a meno di coniugio. Dunque per comprendere le varie evoluzioni dinamiche è sufficiente considerare l'azione di sottogruppi ciclici di S_n su $\mathbb{C}^n$ a meno di coniugio. Dal Teorema 1.2.3 sappiamo che il numero di tali sottogruppi è pari al numero di partizioni di n.

4.3 Azione delle Mappe di Kraus Associate ai Sottogruppi di S_n

Sia $S = \langle \sigma \rangle$ un sottogruppo ciclico di S_n, si ha:

$$K_S = K_\sigma = g(t) Id_n + f(t) \sum_{i=1}^{|\sigma|-1} R_\sigma^i$$

e

$$\rho(t) = g^2(t)\rho(0) + f^2(t) \sum_{i=1}^{|\sigma|-1} R_\sigma^i \rho(0) R_\sigma^{-i}$$

Ricordiamo che stiamo assumendo senza perdità di generalità che $\rho(0) \in D_n(\mathbb{C})$. Vogliamo ora dare un espressione esplicita per la $\rho(t)$.
Sia $\sigma = c_1 \dots c_r$ la decomposizione in cicli di σ, inclusi quelli di lunghezza 1 e con $|c_i| \geq |c_{i+1}|$. Sia $|c_i| = \mu_i$, per $i = 1, \dots, r$ e poniamo $\mu_0 = 1$. Chiaramente: $\mu_1 + \dots + \mu_r = n$. Siccome lavoriamo a meno di coniugio possiamo assumere che la permutazione sia del tipo:

$$\sigma = (1, 2, \dots, \mu_1)(\mu_1 + 1, \dots, \mu_1 + \mu_2) \dots (\sum_{j=0}^{r-1} \mu_j, \dots, n)$$

quindi:

$$c_i = (\sum_{j=0}^{i-1} \mu_j, \ldots, \sum_{j=1}^{i} \mu_j)$$

Si noti poi che $|\sigma| = \text{LCM}\{\mu_1, \ldots, \mu_r\}$, dove LCM sta per minimo comune multiplo. Se $\rho(0) = \text{diag}(\lambda_1, \ldots, \lambda_n)$ e poniamo:

$$B_i = (\frac{1}{\mu_i} \sum_{h \in c_i} \lambda_h) Id_{\mu_i}$$

per $i = 1, \ldots, r$ e indichiamo con B la matrice a blocchi: $B_1 \oplus \cdots \oplus B_r$, allora:

$$\rho_\sigma(t) = \rho(0)e^{-t} + (1 - e^{-t})B.$$

Notiamo che da ciò segue che gli autovalori di $\rho_\sigma(t)$ sono combinazioni lineari con coefficienti non negativi, di cui almeno uno non nullo, degli autovalori di $\rho(0)$. Possiamo ora formulare il seguente teorema:

Teorema 4.3.1. *L'azione associata ad ogni sottogruppo ciclico $\langle\sigma\rangle$ di S_n soddisfa due proprietà:* (1) *è completamente positiva e* (2) *soddisfa la condizione temporale.*

Dimostrazione. Per la dimostrazione si rimanda a [Cat+21]. □

Dunque le mappe K_S soddisfano le condizioni necessarie per poter parlare di Mappe di Kraus.
Usando dunque ora la formula esplicita per $\rho_\sigma(t)$ possiamo iniziare a trarre alcune conclusioni sull'orbita. Intanto:

$$\lim_{t \to \infty} \rho_\sigma(t) = B$$

Inoltre si ha che $\rho(0) - \rho_\sigma(t) = (1 - e^{-t})(\rho(0) - B)$ è una matrice diagonale e si verifica facilmente che le entrate diagonali soddisfano il sistema seguente:

$$\begin{cases} x_1 + x_2 + \cdots + x_{\mu_1} = 0 \\ x_{\mu_1+1} + x_{\mu_1+2} + \cdots + x_{\mu_1+\mu_2} = 0 \\ \vdots \\ x_{n-\mu_r} + x_{n-\mu_r+1} + \cdots + x_n = 0. \end{cases}$$

Se abbiamo degli autovalori con molteplicità maggiore di 1 valgono naturalmente i risultati visti fin'ora tuttavia ci sono meno gradi di libertà in quanto vi sono elementi di S_n che agiscono banalmente su $\rho(0)$, per avere delle azioni non banali dobbiamo guardare agli operatori che permutano autovalori distinti. Nella sezione che segue vedremo alcuni esempi di orbite in casi semplici.

4.4 Interpretazione Geometrica ed Esempi

Proviamo ad avere un po' di intuizione geometrica su quanto visto. Dati n punti $P_1, \ldots, P_n \in \mathbb{C}$ denotiamo il $(n-1)$-simplesso di vertici $P_1, \ldots, P_n$ con $\Delta^{n-1} = \Delta(P_1, \ldots, P_n) = \{\lambda_1 P_1 + \cdots + \lambda_n P_n : \lambda_i \geq 0, \lambda_1 + \cdots + \lambda_n = 1\}$. Associamo ad ogni matrice $\rho(0) =$

$\mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ l'elemento $\lambda_1 P_1 + \cdots + \lambda_n P_n \in \Delta(P_1, \ldots, P_n)$. Ogni elemento $\sigma \in S_n$ agisce sui vertici di Δ^{n-1} permutandoli e per linearità su tutto il simplesso. Dato un ciclo $c = (i_1, \ldots, i_\mu)$, denotiamo con $L(c) \subset \mathbb{C}^n$ il sottospazio generato dagli $n-1$ vettori $P_{i_1} - P_{i_j}$ con $j = 2, \ldots, \mu$. Indichiamo inoltre con $\mathrm{Bar}(c)$ il baricentro di $\Delta(P_{i_1}, \ldots, P_{i_\mu})$. Si noti che c fissa $\mathrm{Bar}(c)$.
Siccome K_σ preserva la traccia si ha che $\rho_\sigma(t)$ dà un cammino in Δ^{n-1}. Vediamo alcuni esempi.
Consideriamo come primo esempio quello di un qubit ovvero uno spazio di Hilbert di dimensione $n = 2$. Così una generica matrice densità sarà della forma:

$$\mathrm{diag}(\lambda_1, 1 - \lambda_1).$$

Posto $X = \lambda_1 - \lambda_2 \in [-1, 1]$, possiamo rappresentare il simplesso Δ^1 come il segmento generato dai due punti P_1, P_2 di coordinate $X = +1, -1$ rispettivamente. L'unico sottogruppo ciclico non banale è generato dalla permutazione:

$$\sigma : (\lambda_1, \lambda_2) \to (\lambda_2, \lambda_1).$$

Un conto diretto mostra che l'evoluzione temporale è data da:

$$\rho_\sigma(t) = \mathrm{diag}(e^{-t}\lambda_1 + (1 - e^{-t})/2, e^{-t}\lambda_2 + (1 - e^{-t})/2)$$

che tende al limite $\rho_\infty = \mathrm{diag}((\lambda_1 + \lambda_2)/2, (\lambda_1 + \lambda_2)/2)$.
Prendiamo come secondo caso $n = 3$. In generale la matrice $\rho(0) = diag(\lambda_1, \lambda_2, 1 - \lambda_1 - \lambda_2)$. Posto $X_1 = (\lambda_1 - \lambda_2)/2$ e $X_2 = (\lambda_1 + \lambda_2)/2 - 1/3$, possiamo rappresentare il simplesso Δ^2 nel piano X_1, X_2 come il triangolo equilatero di vertici: $P_1 = (1, \sqrt{3}), P_2 = (-1, \sqrt{3}), P_3 = (0, -2/\sqrt{3})$.
Abbiamo ora diversi gruppi ciclici.
Ad esempio, $S_1 : (\lambda_1, \lambda_2, \lambda_3) \mapsto (\lambda_1, \lambda_3, \lambda_2)$ cioè dove abbiamo un ciclo di lunghezza 1 e uno di lunghezza 2. Allora la matrice densità si evolve mediante un UDM F_1 come segue:

$$\rho_{F_1}(t) = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & e^{-t}\lambda_2 + (1 - e^{-t})(\lambda_2 + \lambda_3)/2 & 0 \\ 0 & 0 & e^{-t}\lambda_3 + (1 - e^{-t})(\lambda_2 + \lambda_3)/2 \end{pmatrix}$$

con orbita limite: $\rho_\infty = \mathrm{diag}(\lambda_1, (\lambda_2 + \lambda_3)/2, (\lambda_2 + \lambda_3)/2)$, l'orbita è parallela al lato P_2P_3 del triangolo. Similmente ci sono le orbite parallele ai lati P_1P_3 e P_1P_2 ottenute rispettivamente dai sottogruppi ciclici generati da: $S_2 : (\lambda_1, \lambda_2, \lambda_3) \mapsto (\lambda_3, \lambda_2, \lambda_1)$ e $S_3 : (\lambda_1, \lambda_2, \lambda_3) \mapsto (\lambda_2, \lambda_1, \lambda_3)$.
Possiamo anche considerare il sottogruppo ciclico massimale generato da $S : (\lambda_1, \lambda_2, \lambda_3) \mapsto (\lambda_3, \lambda_1, \lambda_2)$ che ci dà l'orbita:

$$\rho_F(t) = \begin{pmatrix} e^{-t}\lambda_1 + (1 - e^{-t})/3 & 0 & 0 \\ 0 & e^{-t}\lambda_2 + (1 - e^{-t})/3 & 0 \\ 0 & 0 & e^{-t}\lambda_3 + (1 - e^{-t})/3 \end{pmatrix}$$

Il cui punto limite è il baricentro del triangolo, ovvero: $\rho_\infty = \mathrm{diag}(1/3, 1/3, 1/3)$.

Bibliografia

[Cat+21] Alessia Cattabriga, Elisa Ercolessi, Riccardo Gozzi e Erika Meucci. «Kraus operators and symmetric groups». English. In: *International Journal of Geometric Methods in Modern Physics* 18 (2021), p. 13.

[Cat96] Giulia Maria Piacentini Cattaneo. *ALGEBRA: un approccio algoritmico*. Zanichelli, 1996.

[CDL91] Claude Cohen-Tannoudji, Bernard Diu e Frank Laloe. *Quantum Mechanics*. Wiley-VCH, 1991.

[Eti+11] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dimitry Vaintrob, Elena Yudovina e Slava Gerovitch. *Introduction to Representation Theory*. American Mathematical Society, 2011.

[Her10] Israel Nathan Herstein. *Algebra*. Editori Riuniti, 2010.

[Kar18] Thorsten Holm Karin Erdmann. *Algebras and Representation Theory*. Springer, 2018.

[Sag01] Bruce Eli Sagan. *The Symmetric Group Representations: Combinatorial Algorithms, and Symmetric Functions*. Springer, 2001.