Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE STATISTICHE
Corso in Scienze Statistiche, demografiche e Sociali

SOTTOSPAZI INVARIANTI E RETICOLI SEMIPRIMARI

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
ANDREA BRINI
Correlatore:
Chiar.mo Dott.
FRANCESCO REGONATI

Presentata da:
GIULIA GUALANDRI

Sessione I
Anno Accademico 2003/2004

Dedico questo lavoro alla mia mamma.

Introduzione

Un tema classico ed assai rilevante dell'Algebra Lineare e delle sue applicazioni alla Statistica e' lo studio della struttura della famiglia dei sottospazi di uno spazio vettoriale (di dimensione finita, a coefficienti complessi) *invarianti* rispetto all'azione di un endomorfismo assegnato.

Lo studio dei sottospazi invarianti rispetto all'azione di un endomorfismo ha una storia estremamente lunga e complessa. Come dato di fatto, questa problematica e' stata all'origine, da un lato, di teorie matematiche molto generali, quali ad esempio la *teoria delle rappresentazioni di gruppi ed algebre*, e, da un altro lato, di applicazioni assai rievanti ad altri settori scientifici quali la Statistica, la Fisica, la Chimica.

In relazione alla sua lunga storia, lo studio della struttura dei sottospazi invarianti ha stimolato l'elaborazione di metodologie assai differenti, pur se tra loro strettamente correlate od, addirittura, equivalenti.

Entrando nello specifico, le trattazioni piu' diffuse in letteratura si basano su metodi e concetti derivati essenzialmente dal formalismo dell'Algebra Lineare. In un pionieristico articolo del 1942, Reinhold Baer propose un approccio assolutamente originale e diverso, che permette di inquadrare lo studio della struttura dei sottospazi invarianti nell'ambito di una trasparente teoria di natura geometrico-reticolare, la *teoria dei reticoli semiprimari.* Il grande contributo della intuizione di Baer consiste non soltanto nel riconoscere che la teoria dei sottospazi invarianti puo' essere riguardata come caso particolare di una teoria assai piu' generale, ma, come spesso accade, nel fornire una

formalizzazione assai piu' semplice e geometrica (e, di conseguenza, molto piu' intuitiva) di quella tradizionale.

Lo scopo di questa tesi e' quello di presentare la teoria dei sottospazi invarianti rispetto ad un endomorfismo, utilizzando sia il linguaggio piu' tradizionale dell'Algebra Lineare, sia il linguaggio geometrico-reticolare dei reticoli semiprimari di Baer, cercando di sfruttarne il piu' possibile le loro sorprendenti sinergie.

Il lavoro e' organizzato come segue.

Nel primo capitolo si richiamano alcuni concetti elementari di Algebra Lineare (in dimensione finita), quali la nozione di endomorfismo e sua rappresentazione matriciale mediante la scelta di una base fissata e la nozione di sottospazio invariante rispetto ad un endomorfismo.

Nel secondo capitolo si introduce brevemente il linguaggio dei *moduli su anelli unitari* (linguaggio che Emmy Noether mostro' negli anni '30 essere equivalente al linguaggio delle *rappresentazioni di anelli*). Dopo avere sinteticamente richiamato le proprieta' dell'anello dei polinomi a coefficienti complessi $C[x]$, si introduce la struttura di $C[x]-$modulo indotta dall'azione di un endomorfismo f su uno spazio vettoriale complesso di dimensione finita. Si descrive l'equivalenza tra la nozione di $C[x]-$sottomodulo e la nozione di sottospazio $f-$invariante, e si introduce il concetto di annullatore come ideale principale di $C[x]$ e si riconosce che il suo generatore monico e' il *polinomio minimo* dell'endomorfismo f.

Il terzo capitolo e' dedicato alla presentazione dei principali concetti relativi alla teoria degli insiemi parzialmente ordinati e dei reticoli che risulteranno necessari nel seguito della trattazione. In particolare, si richiamano le nozioni di *modularita', rango* ed elementi *sup-irriducibili* ed *inf-irriducibili*.

Nel capitolo quattro, si discutono alcuni esempi significativi, basandosi sulla rappresentazione dei reticoli mediante i loro diagrammi di Hasse.

Nel capitolo cinque si inizia lo studio del reticolo dei sottospazi $f-$invarianti. Al fine di rendere piu' agevole la lettura delle parti successive, nei primi due paragrafi si studia in dettaglio la struttura di alcuni sottospazi invarianti

particolari, quali ad esempio i sottospazi invarianti generati da un singolo vettore. Il risultato principale di questo capitolo e' il cosiddetto *teorema di spezzamento*, il quale afferma che *se il polinomio minimo della restrizione dell'endomorfismo ristretto ad un sottospazio invariante e' fattorizzabile in modo non banale, allora detto sottospazio invariante si decompone canonicamente in somma diretta di sottospazi invarianti.* Questo risultato conduce in modo naturale alla caratterizzazione dei sottospazi invariante sup-irriducibili, e, grazie ad un argomento di dualita' ortogonale ad una analoga caratterizzazione dei sottospazi invarianti inf-irriducibili.

Il capitolo sei e' dedicato ad una presentazione generale della teoria dei reticoli semiprimari. In breve, questi reticoli sono reticoli modulari tali che ogni ideale principale generato da un *sup-irriducibile* risulti una *catena* e, dualmente, ogni filtro principale generato da un *inf-irriducibile* risulti una *catena.* La classe dei reticoli semiprimari risulta essere la classe naturale di reticoli nell'ambito della quale studiare da un punto di vista geometrico-sintetico la struttura dei sottospazi invarianti.

La tesi si conclude (capitolo sette) con una applicazione estremamente significativa dei concetti e dei risultati precedentemente discussi: la forma canonica di Jordan. In particolare si mostra come il sussistere di questa forma canonica e le sue principali proprieta' siano facilmente deducibili dai risultati geometrico-sintetici sui reticoli semiprimari presentati nel capitolo precedente.

Indice

Capitolo 1

Richiami di algebra lineare

1.1 Matrici ed endomorfismi

Per semplicita' di esposizione, in questa tesi tratteremo spazi vettoriali di dimensione finita sul campo C dei complessi, sebbene il lettore possa agevolmente riconoscere che una porzione consistente dei risultati esposti mantiene la sua validita' quando, in luogo del campo complesso, si considera un campo qualsiasi.

Sia V uno spazio vettoriale di dimensione finita sul campo C. Data una base $B = (v_1, ..., v_n)$ di V, per ogni vettore $v \in V$ si indica con

$$[v]_B$$

la colonna delle coordinate di v rispetto alla base B.

Definizione 1.1. Dato un endomorfismo $f : V \to V$, si definisce la matrice $[f]_B$ associata ad f rispetto alla base B come quella matrice che soddisfa l'equazione

$$[f(v)]_B = [f]_B[v]_B, \qquad \forall v \in V.$$

Osservazione 1. Si osserva che l'i-esima colonna della matrice $[f]_B$ è formata dalle componenti dell'immagine dell'i-mo vettore b_i della base B rispetto alla stessa base B.

Osservazione 2. Fissata un base B di V, la funzione, dall'algebra degli endomorfismi di V all'algebra delle matrici quadrate di ordine n con elementi in C, che ad un endomorfismo f associa la matrice $[f]_B$ è un isomorfismo d'algebra (l'inversa di tale corrispondenza associa ad una matrice A quadrata di ordine n l'endomorfismo f che manda il vettore v nel vettore di componenti $A[v]_B$ rispetto a B).

Proposizione 1.1.1. *Se due matrici rappresentano uno stesso endomorfismo f di V rispetto a due basi B_1 e B_2 di V, allora sono simili, ovvero si ha*

$$[f]_{B_1} = P^{-1}[f]_{B_2}P$$

dove P e' la matrice di passaggio dalle coordinate rispetto alla base B_2 alle coordinate rispetto alla base B_1:

$$[v]_{B_2} = P[v]_{B_1}, \qquad \forall v \in V.$$

Dimostrazione. Per definizione si ha

$$[f(v)]_{B_2} = [f]_{B_2}[v]_{B_2}, \forall v \in V;$$

passando alle coordinate rispetto alla base B_1 si ha

$$P[f(v)]_{B_1} = [f]_{B_2}P[v]_{B_1}, \forall v \in V,$$

e premoltiplicando per P^{-1} si ottiene

$$[f(v)]_{B_1} = P^{-1}[f]_{B_2}P[v]_{B_1}, \forall v \in V.$$

Quindi per definizione si ha

$$P^{-1}[f]_{B_2}P = [f]_{B_1}.$$

□

Definizione 1.2. Si definisce il polinomio caratteristico p_A di una matrice A quadrata di ordine n sul campo C come il polinomio monico di grado n dato da

$$p_A(\lambda) = det(\lambda I - A).$$

Teorema 1.1.2.

Matrici simili hanno lo stesso polinomio caratteristico:

$$A = M^{-1}BM \quad \Rightarrow \quad p_A(x) = p_B(x)$$

Osservazione 3. In generale matrici che hanno lo stesso polinomio caratteristico NON sono simili.

Esempio 1.1. La matrice A

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

e la matrice B

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

hanno lo stesso polinomio caratteristico:

$$p_A(x) = p_B(x) = x^3$$

ma non sono simili.

Ricordiamo che la valutazione di un polinomio a coefficienti in C

$$p(x) = c_n x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0$$

su una matrice A quadrata ad elementi in C e', per definizione, la matrice

$$p(A) = c_n A^n + c_{n-1}A^{n-1} + ... + c_1 A + c_0 I.$$

Teorema 1.1.3 (Teorema di Cayley-Hamilton).

Data una matrice A quadrata ad elementi in C, la valutazione del polinomio caratteristico di A sulla stessa matrice A è la matrice nulla:

$$p_A(A) = \boldsymbol{O}$$

1.2 Sottospazi invarianti

Definizione 1.3. Un sottospazio W di V si dice invariante rispetto ad un endomorfismo f di V, o più brevemente f-invariante, se f trasforma vettori di W in vettori di W:

$$f(W) \subseteq W.$$

Osservazione 4. Dalla linearità di f e dalle proprietà di chiusura di W segue che W è f-invariante se e solo se f trasforma vettori di una *base* di W in vettori di W. Per verificare quindi che un sottospazio sia f-invariante ci si può limitare a considerare i trasformati dei vettori di una base del sottospazio W.

Sia $f : C^n \to C^n$ un endomorfismo di C^n. Dato un sottospazio W f-invariante, si può restringere il dominio di f a W, ottenendo l'endomorfismo ristretto

$$f|_W : W \to W.$$

Osservazione 5. Una qualunque base $B_1 = (w_1, w_2, ..., w_p)$ di W, si può estendere fino ad ottenere una base B di C^n:

$$B = (w_1, w_2, ..., w_p, w_{p+1}, ..., w_{n-1}, w_n)$$

Così le immagini dei primi p vettori della base B saranno combinazioni lineari solo dei primi p vettori di B, quindi le componenti rispetto ai restanti $n-p$ vettori saranno tutte nulle.

Pertanto la matrice rappresentativa di f rispetto alla nuova base B risulterà triangolare a blocchi:

$$[f]_B = \begin{pmatrix} P & Q \\ 0 & R \end{pmatrix}$$

dove 0 è un blocco nullo e

$$P = [f|_W]_{B_1}$$

è la matrice rappresentativa della restrizione di f al sottospazio W rispetto alla base B_1.

Siano W e Z due sottospazi entrambi f-invarianti tali che

$$C^n = W \oplus Z$$

Date due basi $B_1 = (v_1, ..., v_p)$ e $B_2 = (v_{p+1}, ..., v_n)$ rispettivamente di W e di Z, la loro unione $B = (v_1, ..., v_n)$ è una base di C^n.

La matrice rappresentativa di f rispetto alla base B sarà diagonale a blocchi: infatti le prime p colonne della matrice rappresentativa di f rispetto alla base B sono combinazioni lineari solo dei primi p vettori di B e le restanti $n-p$ colonne sono combinazioni lineari solo degli ultimi $n-p$ vettori di B.

$$[f]_B = \begin{pmatrix} P & 0 \\ 0 & Q \end{pmatrix}$$

dove $P = [f|_W]_{B_1}$ e $Q = [f|_Z]_{B_2}$

Data una matrice A quadrata di ordine n a coefficienti complessi, indichiamo con f_A l'endomorformismo di C^n, definito da

$$f_A(x) = Ax, \qquad \forall x \in C^n,$$

la cui matrice rappresentativa rispetto alla base canonica $\widetilde{B} = (e_1, e_2, ..., e_n)$ è la matrice A, avendo identificato x con la matrice colonna $[x]_{\widetilde{B}}$.

Definizione 1.4. Un sottospazio $W \subseteq C^n$ si dice A-invariante se è f_A-invariante.

Osservazione 6. I sottospazi A-invarianti potranno avere dimensione 0,1,2...,n L'unico sottospazio di dimensione 0 è lo spazio nullo e l'unico sottospazio di dimensione n è l'intero spazio C^n.

Osservazione 7. Studiare i sottospazi A-invarianti di dimensione 1 equivale a studiare gli autovettori di A. I sottospazi A-invarianti di dimensione 1 sono tutti e soli quelli generati da esattamente un autovettore (non nullo) di A.

Infatti un sottospazio unidimensionale W ha una base costuita da un solo vettore non nullo w. Quindi W è A-invariante se e solo se $f(w) \in W$; questo si traduce col fatto che Aw si possa scrivere come combinazione lineare del solo vettore w che genera W, cioè che sia un suo multiplo:

$$Aw = \lambda w, \qquad \lambda \in C,$$

il che significa che w è un *autovettore* di A.

Osservazione 8. Un sottospazio $W \subseteq C^n$ avente base $(w_1, w_2, ..., w_r)$ è A-invariante se Aw_i (per $i = 1, ..., r$) si può scrivere come combinazione lineare dei vettori $(w_1, w_2, ..., w_r)$.

In termini matriciali se indichiamo con B_W la matrice costituita dalle colonne $w_1, w_2, ..., w_r$ si ha che

$$AB_W = B_W\Lambda$$

dove Λ è la matrice rappresentativa della restrizione di f_A a W rispetto alla base $(w_1, w_2, ..., w_r)$.

Si noti che questa formula si può applicare anche nei casi di $r = 1$, in cui la matrice Λ ha un solo elemento ($\Lambda = [\lambda]$) ed r=n in cui la matrice Λ rappresenta l'endomorfismo f_A rispetto alla base $(w_1, w_2, ..., w_n)$.

Capitolo 2

Richiami sui Moduli

2.1 Anelli unitari

Definizione 2.1. Si dice *anello unitario* un insieme A munito di due operazioni interne $+$, $\cdot$ e dotato di un elemento $1 \in A$ tali che valgano gli assiomi:

1. $(A, +)$ è un gruppo abeliano;
2. $a \cdot (a_1 + a_2) = a \cdot a_1 + a \cdot a_2$;
3. $(a_1 + a_2) \cdot a = a_1 \cdot a + a_2 \cdot a$;
4. $(a_1 a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$;
5. $1 \cdot a = a$

per ogni $a, a_1, a_2, a_3 \in A$

Definizione 2.2. In un anello A un sottoinsieme non vuoto I si dice *ideale* di A se

- $(x_1, x_2 \in I) \Rightarrow (x_1 + x_2 \in I)$
- $(x \in I, a \in A) \Rightarrow (a \cdot x \in I, x \cdot a \in A)$

2.2 Anello $C[x]$

L'insieme $C[x]$ dei polinomi in una variabile a coefficienti nel campo C dei complessi è un anello commutativo unitario rispetto alle usuali operazioni di somma e prodotto tra polinomi.

Definizione 2.3. Il grado di un polinomio non nullo f, indicato con $deg(f)$, è il massimo esponente della potenza della variabile x che compare in f con coefficiente diverso da 0; il grado di un polinomio nullo e' -1.

Proposizione 2.2.1. *Comunque dati $f, g \in C[x]$, con $g \neq 0$, esistono e sono unici $q, r \in C[x]$, che vengono detti rispettivamente quoziente e resto della divisione di f per g, tali che*

$f = qg + r$ *, con* $deg(r) < deg(g)$

Dimostrazione. L'esistenza è determinata dal ben noto algoritmo della divisione tra polinomi con resto.

Per quanto concerne l'unicità se fosse $f = q_1 g + r_1$ e $f = q_2 g + r_2$ allora

$0 = (q_1 - q_2)g + r_1 - r_2$ da cui $(q_1 - q_2)g = r_2 - r_1$ siccome $deg(r_1) < deg(g)$ e $deg(r_2) < deg(g)$ l'unica possibilità è che $q_1 = q_2$ e di conseguenza $r_1 = r_2$. □

Per ogni polinomio $g \in C[x]$, l'insieme

$$\{fg, f \in C[x]\}$$

dei multipli di g e' un ideale di $C[x]$, il piu' piccolo ideale di $C[x]$ contenente g. Questo ideale viene detto *ideale principale generato da g*, e viene indicato con

$$< g > .$$

Teorema 2.2.2. *Ogni ideale dell'anello $C[x]$ è principale.*

Dimostrazione. L'enunciato e' chiaramente vero per l'ideale nullo $\{0\}$ di $C[x]$. Dato $I \neq \{0\}$, ideale non nullo di $C[x]$, si prenda fra i polinomi non nulli di I un polinomio $g_0 \in I$ di grado *minimo*.

Ora prendiamo un generico polinomio $p \in I$, per il teorema 2.1.1 esistono $q, r \in C[x]$ tali che

$$p = qg_0 + r,$$

con $\deg(r) < \deg(g_0)$.

Per ipotesi $p \in I$ quindi $qg_0 \in I$ perché multiplo di g_0, ne segue che $r \in I$; ma g_0 è un polinomio di grado *minimo* fra i polinomi non nulli di I, quindi l'unico polinomio nell'ideale I che soddisfi la disequazione $\deg(r) < \deg(g_0)$ è il polinomio nullo. Quindi

$$p = qg_0$$

cioè ogni polinomio $p \in I$ è multiplo di g_0:

$$I =< g_0 >= \{fg_0, f \in C[x]\}$$

□

Osservazione 9. Dato $I \neq \{0\}$, ideale non nullo di $C[x]$, esiste uno ed un solo polinomio monico (cioè con coefficiente della potenza più alta pari a 1) $g_0 \in I$ tale che $I =< g_0 >$. Si ha cosi' una corrispondenza biunivoca fra ideali non nulli di $C[x]$ e polinomi monici di $C[x]$.

2.3 Modulo su un anello

La definizione di modulo su un anello è una generalizzazione di quella di spazio vettoriale su un campo: l'unica differenza è che non è richiesto che l'insieme degli scalari sia un campo, ma è sufficiente che sia un anello.

Definizione 2.4. Un gruppo abeliano $(M, +)$ si dice *Modulo* su un anello (unitario) A, o più brevemente un A-modulo

se è data un'operazione esterna:

$$\cdot : A \times M \to M$$

tale che valgano gli assiomi:

1. $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$
2. $(a_1 + a_2) \cdot m = a_1 \cdot m + a_2 \cdot m$
3. $(a_1 a_2) \cdot m = a_1 \cdot (a_2 \cdot m)$
4. $1 \cdot m = m$

2.4 Struttura di $C[x]$-modulo indotta da un endomorfismo f

Definizione 2.5. Sia $f : C^n \to C^n$ un endomorfismo di C^n. Per ogni polinomio in una variabile a coefficienti complessi

$$q(x) = c_0 x^0 + c_1 x + c_2 x^2 + ... + c_n x^n,$$

si pone:

$$q(f) = c_0 f^0 + c_1 f + c_2 f^2 + ... + c_n f^n,$$

e si definisce un'azione di $C[x]$ su C^n ponendo:

$$q(x) \cdot v = (q(f))(v), \qquad \forall v \in V.$$

Osservazione 10. Con tale operazione esterna su C^n, visto come un gruppo abeliano rispetto all'addizione usuale, si ottiene una struttura di $C[x]$-modulo su C^n; le verifiche sono quasi immediate.

2.5 Sottomoduli e sottospazi invarianti

Definizione 2.6. Un sottomodulo di un $\mathcal{A}$-modulo M è un sottinsieme non vuoto $S \subseteq M$ chiuso rispetto alle operazioni di somma e di moltiplicazione esterna.

Osservazione 11. Sia $f : C^n \to C^n$ un endomorfismo di C^n. Un sottomodulo S di C^n, riguardato come $C[x]$-modulo tramite f, dev'essere chiuso rispetto alla somma e alla moltiplicazione esterna rispetto agli scalari di $C[x]$, che sono polinomi. In particolare dev'essere chiuso rispetto alla moltiplicazione per polinomi di grado 0, che si possono pensare come scalari di C; quindi S dev'essere un sottospazio vettoriale di C^n. In più dev'essere chiuso rispetto alla moltiplicazione esterna per il polinomio x, quindi

$$v \in S \Rightarrow xv = fv \in S$$

cioè S è f-invariante.

Viceversa, un sottospazio f-invariante S di C^n e' è un sottomodulo di C^n visto come $C[x]$-modulo tramite f. Infatti, applicando più volte la definizione di f-invarianza, si ha:

$$v \in S \Rightarrow fv \in S \Rightarrow f^2v \in S \Rightarrow ... \Rightarrow f^nv \in S;$$

quindi anche

$$(c_0 + c_1x + c_2x^2 + ... + c_nx^n)v = c_0v + c_1fv + c_2f^2v + ... + c_nf^nv \in S$$

in quanto combinazione lineare di vettori del sottospazio S.

2.6 Annullatore e polinomio minimo

Definizione 2.7. Dato un modulo M su un anello $\mathcal{A}$ e un sottinsieme $H \subseteq M$, l' *Annullatore di H* è l'insieme degli scalari che mandano ogni elemento

v di H in 0:

$$Ann(H) = \{a \in \mathcal{A} : \quad av = 0, \forall v \in H\}.$$

Proposizione 2.6.1. *L'annullatore di un sottinsieme di un modulo M su un anello commutativo $\mathcal{A}$ e' un ideale di $\mathcal{A}$.*

Ora, dato un endomorfismo f di C^n, riguardiamo C^n come $C[x]$-modulo tramite f, e consideriamo l'ideale $Ann(C^n)$. Per il teorema di Cayley-Hamilton il polinomio caratteristico $p_f(x)$ di f appartiene ad $Ann(C^n)$, dunque $Ann(C^n) \neq \{0\}$. Essendo $C[x]$ un dominio ad ideali principali, $Ann(C^n)$ sarà generato da un solo polinomio. Tale polinomio è definito a meno di uno scalare non nullo ed ha grado *minimo* tra i polinomi non nulli di $Ann(C^n)$.

Definizione 2.8. Si definisce *polinomio minimo* di un endomorfismo f di C^n, e si indica con $m_f(x)$, l'unico polinomio che genera $Ann(C^n)$ ed ha coefficiente direttore uguale ad 1, cioè è *monico*.

$$< m_f(x) >= Ann(C^n)$$

Proposizione 2.6.2. *Il poliniomio minimo di un endomorfismo f divide il polinomio caratteristico di f:*

$$m_f |\ p_f.$$

Dimostrazione. Per il teorema di Cayley-Hamilton il polinomio caratteristico $p_f(x)$ di f appartiene ad $Ann(C^n)$. Tutti gli elementi di $Ann(C^n)$, essendo $Ann(C^n)$ generato dal solo polinomio $m_f(x)$, sono multipli di $m_f(x)$, in particolare $m_f(x)$ divide $p_f(x)$.

□

Capitolo 3

Reticoli di lunghezza finita

3.1 Insiemi parzialmente ordinati e reticoli

Definizione 3.1.

Un insieme L si dice *parzialmente ordinato* se è definita in esso una relazione $\leq$ che soddisfi le seguenti proprietà: per ogni $x, y, z \in L$

- $x \leq x$ (Riflessiva)
- $(x \leq y \ , \ y \leq x) \Rightarrow x = y$ (Antisimmetrica)
- $(x \leq y \ , \ y \leq z) \Rightarrow x \leq z$ (Transitiva)

L'insieme L si chiama *totalmente ordinato* o *catena* se vale anche la proprietà: per ogni $x, y \in L$

- $x \leq y$ o $y \leq x$ (Confrontabilità)

Se $x \leq y$ ed $y \neq x$ allora scriveremo semplicemente $x < y$.

La nozione gerarchica di superiore immediato, detta relazione di *copertura* si può definire come segue.

Definizione 3.2. In un insieme parzialmente ordinato L si dice che x *copre* y se si ha

$y < x$ e non esiste alcun $z \in L$ tale che $y < z < x$.

Definizione 3.3. La *lunghezza* di una catena finita è il numero dei suoi elementi diminuito di uno.

Definizione 3.4. Un insieme parzialmente ordinato L si dice *di lunghezza finita* se l'insieme delle lunghezze delle *catene* di L è limitato.

D'ora in avanti, qunado si parlerà di un insieme parzialmente ordinato, lo si intenderà di lunghezza finita.

Definizione 3.5. Dati due elementi x, y in un insieme parzialmente ordinato L, si dice che un elemento $z \in L$ è estremo superiore (o *sup*) tra x ed y se

- $x \leq z$, $y \leq z$;
- per ogni $t \in L$ tale che $x \leq t$ e $y \leq t$, si ha $z \leq t$

Si verifica che se esite un estremo superiore tra x ed y, questo è unico. Esso viene indicato con

$$x \vee y$$

Analogamente si definisce il concetto di estremo inferiore (o inf) tra x ed y come un elemento $z \in L$ tale che

- $x \geq z$, $y \geq z$;
- per ogni $t \in L$ tale che $x \geq t$ e $y \geq t$, si ha $z \geq t$.

Si verifica che se esite un estremo inferiore di x ed y, questo è unico. Esso viene indicato con

$$x \wedge y$$

Definizione 3.6. Si definisce *reticolo* un insieme L parzialmente ordinato dove, comunque dati due elementi $x, y \in L$, esiste sempre, in L, il loro estremo superiore $x \vee y$ ed estremo inferiore $x \wedge y$.

Esempio 3.1. L'insieme dei sottospazi di uno spazio vettoriale ordinati per inclusione forma un reticolo, dove le operazioni reticolari $\vee$ ed $\wedge$ sono, rispettivamente, le operazioni di somma $+$ ed intersezione $\cap$ tra sottospazi.

Proposizione 3.1.1.

In ogni reticolo (di lunghezza finita) esistono sempre, e sono unici, massimo e minimo assoluto, indicati rispettivamente con 1 e 0. Per ogni $x \in L$ valgono

- $x \wedge 0 = 0; x \vee 0 = x;$
- $x \wedge 1 = x; x \vee 1 = 1.$

Definizione 3.7. Dati due elementi x, y in un retcolo L, si dice che y è *complemento* di x se

$$x \vee y = 1, \quad e \quad x \wedge y = 0$$

Esempio 3.2. Nel reticolo dei sottospazi di C^n ogni sottospazio W ammette complemento, ad esempio il suo complemento ortogonale $W^{\perp}$.

Proposizione 3.1.2. *In un reticolo L, le operazioni di $\vee$ ed $\wedge$ godono delle seguenti proprietà: per ogni $x, y, z \in L$*

1. $x \wedge x = x \vee x = x$ *(Idempotenza)*
2. $x \wedge y = y \wedge x;\ x \vee y = y \vee x$ *(Commutatività)*
3. $x \wedge (y \wedge z) = (x \wedge y) \wedge z; x \vee (y \vee z) = (x \vee y) \vee z$ *(Associatività)*
4. $x \wedge (y \vee x) = x \vee (y \wedge z) = x.$ *(Assorbimento)*
5. $y \leq z \Rightarrow x \wedge y \leq x \wedge z, x \vee y \leq x \vee z.$ *(Monotonia di $\wedge$ e $\vee$)*

3.2 Modularità

In generale, nei reticoli sussiste la relazione

$$x \leq z \Rightarrow x \vee (y \wedge z) \leq (x \vee y) \wedge z,$$

detta disequazione modulare.

Definizione 3.8. Un reticolo L è *modulare* se, per ogni $x, y, z \in L$ è soddisfatta l'uguaglianza

$$x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z.$$

Esempio 3.3. Si dimostra che i sottospazi di uno spazio vettoriale, ordinati per inclusione, formano un reticolo modulare.

Definizione 3.9. Dato un reticolo L ed un suo sottoinsieme L_1, si dice che L_1 è un *sottoreticolo* di L se per ogni $x, y \in L_1$ si ha che anche $x \vee y \in L_1$ e $x \wedge y \in L_1$.

Osservazione 12. Si noti che in generale un sottoinsieme parzialmente ordinato di un reticolo L che risulti essere un reticolo NON è un sottoreticolo di L.

Osservazione 13. Nel passaggio a sottoreticoli, poiché le operazioni sono conservate, la modularità si conserva, cioè ogni sottoreticolo di un reticolo modulare è modulare.

Esempio 3.4. L'insieme dei sottospazi di C^n invarianti rispetto ad un endomorfismo di C^n è un sottoreticolo del reticolo modulare di tutti i sottospazi di C^n, quindi è modulare.

3.3 Rango

Definizione 3.10. In un reticolo, una catena avente un massimo a ed un minimo b si dice catena tra a e b. Una catena tra a e b si dice *massimale* se non è contenuta propriamente in alcuna catena tra a e b.

Definizione 3.11. In un reticolo L, in cui comunque dati due elementi a e b, le catene massimali tra a e b hanno tutte la medesima lunghezza, dato un elemento $x \in L$ si dice *rango* di x, indicato con $\rho(x)$, la lunghezza di una catena massimale da 0 a x.

Teorema 3.3.1. *Un reticolo L è modulare se e solo se L è dotato di rango e presi comunque due elementi x ed y sussiste la seguente relazione, detta identità di Grassmann:*

$$\rho(x) + \rho(y) = \rho(x \vee y) + \rho(x \wedge y)$$

3.4 Sup-irriducibili ed inf-irriducibili

Definizione 3.12. In un reticolo L un elemento $p > 0$ si dice *sup-irriducibile* se

$$p = x_1 \vee x_2 \Rightarrow p = x_1 \ o \ p = x_2,$$

cioè se p non si può scrivere come estremo superiore di due elementi diversi da p stesso. Dualmente si definiscono gli elementi *inf-irriducibili*.

Osservazione 14. In un reticolo L un elemento è sup-irriducibile se e solo se copre un solo elemento.

Osservazione 15. Dualmente in un reticolo L un elemento è inf-irriducibile se e solo se è coperto da un solo elemento.

Teorema 3.4.1. *In un reticolo L ogni elemento $x \in L$ si può scrivere come sup (inf) di un numero finito di elementi sup-irriducibili (inf-irriducibili).*

Esempio 3.5. Nel reticolo dei sottospazi di C^n ogni sottospazio è esprimibile come estremo superiore di sottospazi monodimensionali e come estremo inferiore di iperpiani di dimensione $n - 1$.

Capitolo 4

Esempi

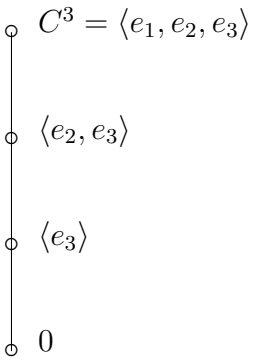
Per un reticolo (o anche insieme parzialmente ordinato) L di lunghezza finita si può dare una rappresentazione grafica della copertura, detta *diagramma di Hasse*. Basta rappresentare ogni elemento di L con un cerchietto, mettendo a più in alto di b se $b < a$ e disegnare un segmento discendente da x ad y se e soltanto se x copre y.

Nelle pagine seguenti si possono vedere i diagrammi di Hasse dei reticoli dei sottospazi di C^3 invarianti rispetto ad alcune matrici di ordine 3. In realta', i reticoli che rappresentiamo sono, a meno di isomorfismi, *tutti* i reticoli di sottospazi invarianti di C^3.

Esempio 4.1. Ciascuna matrice della forma

$$A = \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}, \quad \lambda \in C$$

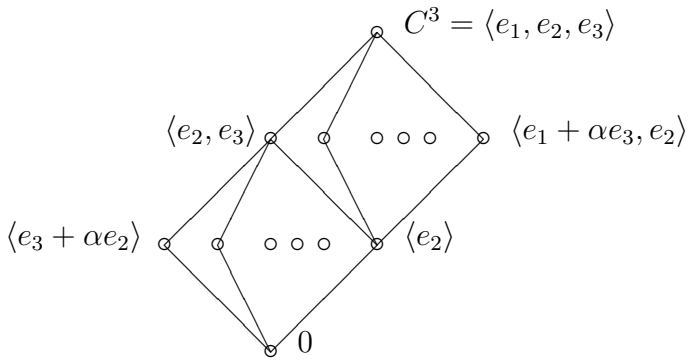
ha come reticolo dei sottospazi invarianti la catena:



Esempio 4.2. Ciascuna matrice della forma

$$B = \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}, \quad \lambda \in C$$

ha come reticolo dei sottospazi invarianti:



Di seguito riportiamo, per ogni sottospazio B-invariante, la matrice che rappresenta la restrizione dell'operatore B a tale sottospazio, rispetto alla

base usata per descrivere il sottospazio stesso.

$$\begin{array}{ll} < e_2 > & (\lambda) \\ < e_3 + \alpha e_2 > & (\lambda) \\ < e_2, e_3 > & \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \\ < e_1 + \alpha e_3, e_2 > & \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix} \end{array}$$

Esempio 4.3. Ciascuna matrice scalare

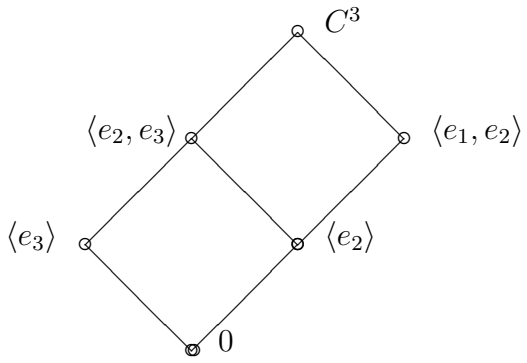
$$C = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} = \lambda I_3, \quad \lambda \in C,$$

ha come reticolo dei sottospazi invarianti l'intero reticolo dei sottospazi di C^3 (non rappresentabile con un diagramma di Hasse).

Esempio 4.4. Ciascuna matrice della forma

$$D = \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix}, \quad \lambda, \mu \in C, \lambda \neq \mu,$$

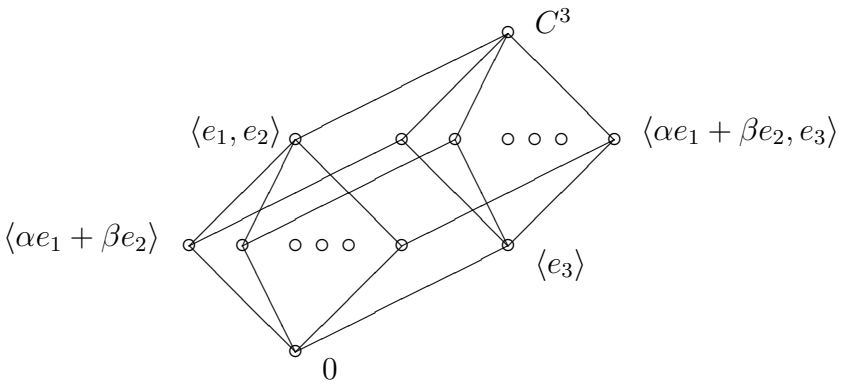
ha come reticolo dei sottospazi invarianti



Esempio 4.5. Ciascuna matrice diagonale

$$E = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix} \quad \lambda, \mu \in C, \lambda \neq \mu,$$

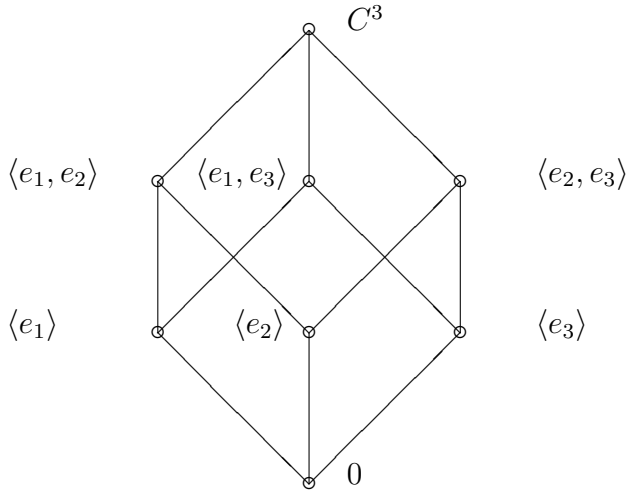
ha come reticolo dei sottospazi invarianti



Esempio 4.6. Ciascuna matrice diagonale

$$F = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{pmatrix}, \quad \lambda, \mu, \nu \in C,$$

con elementi diagonali a due a due distinti, ha come reticolo dei sottospazi invarianti



Capitolo 5

Reticolo dei sottospazi f-invarianti

5.1 Sottospazio f-invariante generato da un vettore

Data una trasformazione lineare $f : C^n \to C^n$ e un vettore $v \in C^n$, ci possiamo chiedere quale sia il più piccolo sottospazio f-invariante che contenga il vettore v, detto *sottospazio f-invariante generato da v*, ed indicato con $< v >_f$.

Tale sottospazio contiene certamente v, essendo f-invariante dovrà contenere le immagini successive di v, cioè $f(v)$, $f^2(v)$ e così via; essendo un sottospazio dovrà contenere anche tutte le combinazioni lineari di tali vettori; essendo il più piccolo dovrà essere il sottospazio generato dalle potenze di f applicate ad v.

Il sottospazio f-invariante *generato da v* risulta essere:

$$< v >_f = < v, f(v), f^2(v), ..., f^{n-1}(v) >$$

Infatti per il teorema di Cayley-Hamilton il polinomio caratteristico di un endomorfismo f è un polinomio annullatore di f: se il polinomio caratteristico di f è:

$$p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + ... + a_1\lambda + a_0\lambda^0$$

allora

$$f^n + a_{n-1}f^{n-1} + ... + a_1 f + a_0 f^0 = 0.$$

Questo comporta che f^n e le potenze successive di f si possono scrivere come combinazione lineare delle potenze di f di grado inferiore ad n.

Siccome il polinomio *minimo* è il polinomio monico annullatore di f di grado minimo, allora si ha che

$$< v >_f = < v, f(v), f^2(v), ..., f^{k-1}(v) >$$

dove k è il grado del polinomio minimo.

Inoltre, i vettori $v, f(v), f^2(v), ..., f^{k-1}(v)$ formano una base di $< v >_f$.

Proposizione 5.1.1. *Ciascun sottospazio W sup-irriducibile nel reticolo dei sottospazi f-invarianti è generato da un solo vettore, cioè esiste un vettore $v \in C^n$ tale che*

$$< v >_f = W$$

Dimostrazione. Il sottospazio W, essendo sup-irriducibile nel reticolo dei sottospazi f-invarianti coprirà un solo sottospazio f-invariante W_0. Preso un elemento $v \in W \setminus W_0$ si consideri il sottospazio $< v >_f$ generato da v. Si ha che $< v >_f \subseteq W$ ma $< v >_f \nsubseteq W_0$, quindi

$$< v >_f = W.$$

□

Teorema 5.1.2. *Sia W un sottospazio f-invariante generato da un solo vettore v:*

$$W =< v >_f,$$

allora il polinomio caratteristico e quello minimo di $f|_W$ coincidono:

$$p_{f|_W}(x) = m_{f|_W}(x)$$

Dimostrazione. Sia p il minimo intero positivo tale che $f^p(v)$ si possa scrivere come combinazione lineare delle immagini precedenti di v:

$$f^p(v) = c_0v + c_1f(v) + c_2f^2(v) + ... + c_pf^p(v) \qquad (*)$$

ovvero

$$f^p(v) - c_{p-1}f^{n-1}(v) - ... - c_1f(v) - c_0v = 0.$$

Allora $\{v, f(v), f^2(v), ..., f^{p-1}(v)\}$ è una *base* di $< v >_f$.

Il polinomio

$$x^p - c_{p-1}x^{p-1} - ... - c_1x - c_0$$

appartiene ad $Ann(W)$, in quanto $.(f^p - c_{p-1}f^{n-1} - ... - c_1f - c_0)v = 0$

Tale polinomio inoltre, per come è stato costruito è un polinomio monico di grado minimo in $Ann(W$, quindi esso è il polinomio minimo $m_{f|_W}$ di $f|_W$. Siccome il grado del polinomio caratteristico $p_{f|_W}$ è p e $m_{f|_W}$ divide $p_{f|_W}$, allora necessariamente $p_{f|_W} = m_{f|_W}$. □

Corollario 5.1.3. *Le restrizioni di f ai sottospazi W sup-irriducibili nel reticolo dei sottospazi f-invarianti hanno uguale polinomio caratteristico e polinomio minimo. $p_{f|_W}(x) = m_{f|_W}(x)$*

Dimostrazione. W, essendo sup-irriducibile sar‘a generato da un solo elemento v:

$$< v >_f= W.$$

Per il teorema precedente, si ha $p_{f|_W}(x) = m_{f|_W}(x)$ □

5.2 Catene

Oltre ai sottospazi f-invarianti banali $\{0\}$ e C^n ne esistono altri piuttosto semplici: i nuclei e le immagini di potenze di f. [1]

Il sottospazio Nucleo o Ker di f è per definizione:

$$Kerf = \{v \in C^n \mid f(v) = 0\}.$$

Siccome $f(v) = 0$ per ogni $v \in Kerf$ e $0 \in Kerf$, il sottospazio $Kerf$ è f-invariante.

Il sottospazio Immagine di f è per definizione:

$$Imf = \{f(v) \mid v \in C^n\}.$$

Per ogni $v \in C^n$ la sua immagine $f(v)$ appartiene ad Imf , quindi $f(Imf) \subseteq Imf$, cioè Imf è f-invariante. .

Più in generale i sottospazi $Kerf^m$, con $m = 0, 1, 2, ...$ sono f-invarianti:

$$v \in Kerf^m \Leftrightarrow f^m(v) = 0 \Rightarrow f^m(f(v)) = f(f^m(v)) = 0 \Rightarrow f(v) \in Kerf^m.$$

Analogamente i sottospazi Imf^m, con $m = 0, 1, 2, ...$ sono f-invarianti:

$$v = f^m(w) \in Imf^m \Rightarrow f(v) = f(f^m(w)) = f^m(f(w)) \Rightarrow f(v) \in Imf^m.$$

Inoltre si noti che

$$\{0\} = Kerf^0 \subseteq Kerf \subseteq Kerf^2 \subseteq ..... \subseteq Kerf^{m-1} \subseteq Kerf^m \subseteq \dots$$

$$C^n = Imf^0 \supseteq Imf \supseteq Imf^2 \supseteq ..... \supseteq Imf^{m-1} \supseteq Imf^m \supseteq \cdots$$

[1] Tra le potenze si considera anche f^0 che si pone per definizione uguale alla trasformazione identica I

Osservazione 16. Le inclusioni sono strette fino ad un certo indice $i \leq n$, poi sono tutte uguaglianze:

$$\{0\} = Kerf^0 \subset Kerf \subset Kerf^2 \subset ..... \subset Kerf^{i-1} \subset Kerf^i = Kerf^{i+1} = \dots$$

infatti

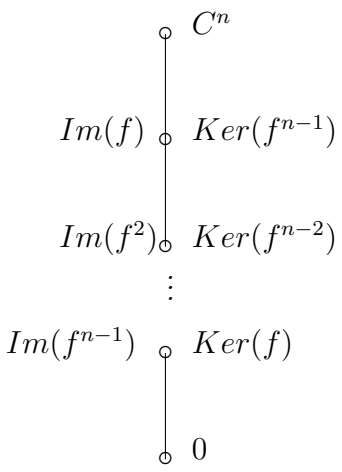
$$Ker\ f^i = Ker\ f^{i+1} \implies (\ f^{i+1}(x) = 0 \Rightarrow f^i(x) = 0,\ \forall x \in C^n) \Rightarrow$$

$$(f^{i+2}(x) = 0 \Rightarrow f^{i+1}(x) = 0,\ \forall x \in C^n) \Rightarrow Ker\ f^{i+1} = Ker\ f^{i+2}.$$

Da ciò segue che tutti i nuclei delle potenze successive ad i saranno uguali a $Kerf^i$.

Un discorso analogo si può fare per le immagini successive di f.

Proposizione 5.2.1. *Sia $f : C^n \to C^n$ un endomorfismo nihilpotente di indice n, cioe' tale che $f^n = 0$ e $f^{n-1} \neq 0$. Allora il reticolo dei sottospazi f-invarianti di C^n e' la catena*



Dimostrazione. Sappiamo che tra i sottospazi invarianti ci sono $Kerf^0, Kerf, ...Kerf^n$.

Inoltre

$$\{0\} = Kerf^0 \subseteq Kerf \subseteq Kerf^2 \subseteq ..... \subseteq Kerf^{n-1} \subseteq Kerf^n \ = \ C^n$$

Le inclusioni sono strette. Infatti se fosse $Kerf^1 = Kerf^{i+1}$ per un certo $i < n$, allora $Kerf^{n-1} = Kerf^n = C^n$, cioè $f^{n-1} = 0$ contro l'ipotesi.

Quindi si ha che

$$\{0\} = Kerf^0 \subset Kerf \subset Kerf^2 \subset ..... \subset Kerf^{n-1} \subset Kerf^n \ = \ C^n$$

e

$$dim(Kerf^i) = i \ \ per \ i = 0, 1, .., n$$

Con passaggi analoghi si mostra che:

$$\{0\} = Im \ f^n \subset Im \ f^{n-1} \subset ... \subset Im \ f^2 \subset Im \ f \subset Im \ f^0 \ = \ C^n.$$

e

$$dim \ Im \ f^i = n - i \ \ per \ i = 0, 1, .., n$$

Inoltre

$$v = f^i(w) \in Im \ f^i \ \ \Rightarrow \ \ (f^{n-i}(v) = f^n(w) = 0) \ \Rightarrow \ v \in Kerf^{n-i}$$

quindi

$$Im \ f^i \subseteq Ker \ f^{n-i},$$

per parità di dimensioni si ha

$$Im \ f^i = Ker \ f^{n-i}.$$

Mostriamo ora che questi sono tutti i sottospazi f-invarianti.

Prendiamo un generico sottospazio W f-invariante.

Sia dim $W = h \quad (1 \leq h \leq n)$ allora

$$p_{f|_W} = x^h,$$

poiché $p_{f|_W} \mid p_f = x^n$ e $deg\ p_{f|_W} = dim\ W = h$.

Ora $m_{f|_W}$ è un divisore di $p_{f|_W} = x^h$, perciò

$$m_{f|_W} = x^{h-i} \qquad (i = 0, 1, ..., h - i)$$

Ne segue che $(f|_W)^{h-i} = 0$, cioè $W \subseteq Ker\ f^{h-i}$, ma dim $Ker\ f^{h-i} = h - i$; siccome dim $W = h$, l'unica possibilità è $i = 0$ e di conseguenza $W = Ker\ f^{n-i}$.

□

Proposizione 5.2.2. *Date due trasformazioni $f, g : C^n \to C^n$ ed un sottospazio M che sia contemporaneamente f-invariante e g-invariante, si ha che M è invariante per qualsiasi combinazione lineare $\alpha f + \beta g$ di f e g (con $\alpha, \beta \in C$).*

Dimostrazione. Per ogni $x \in M$ abbiamo,

$$(\alpha f + \beta g)x = \alpha(fx) + \beta(gx) \in M,$$

in quanto combinazione lineare di due elementi di M. □

Un caso particolare si ha quando $\alpha = 1$ e g è la trasformazione identica I (tutti i sottospazi sono I-invarianti):

Proposizione 5.2.3. *Ogni sottospazio invariante rispetto a una trsformazione f è anche invariante anche rispetto ad una trsformazione del tipo $(f - \lambda I)$ e viceversa. Sarà quindi equivalente studiare i sottospazi invarianti rispetto a f o rispetto a $f - \lambda I$.*

Dalle considerazioni precedenti segue la

Proposizione 5.2.4. *Sia $f : C^n \to C^n$ una trasformazione con polinomio minimo del tipo*

$$m_f = (x - \lambda)^n, \quad \lambda \in C.$$

Allora il reticolo dei sottospazi f-invarianti e' una catena.

5.3 Teorema di spezzamento

L'insieme dei polinomi monici a coefficienti complessi ordinati per divisibilità è un reticolo in cui

$\varphi \vee \gamma = m.c.m.(\varphi, \gamma)$ (m.c.m = minimo comune multiplo)

$\varphi \wedge \gamma = M.C.D.(\varphi, \gamma)$ (M.C.D = massimo comun divisore).

Ad ogni polinomio monico φ possiamo associare l'ideale $< \varphi >$ generato da φ e viceversa per ogni ideale di $C[x]$ possiamo associare il suo polinomio generatore monico.

L'insieme degli ideali di $C[x]$ ordinati per inclusione è un reticolo in cui

$< \varphi > \vee < \gamma > = < \varphi > + < \gamma >$

$< \varphi > \wedge < \gamma > = < \varphi > \cap < \gamma >$

Questi due reticoli sono anti-isomorfi, nel senso che

$$\varphi | \gamma \Leftrightarrow < \gamma > \subseteq < \varphi >,$$

$$\varphi \vee \gamma = \kappa \Leftrightarrow < \varphi > \wedge < \gamma > = < \kappa >$$

$$\varphi \wedge \gamma = \kappa \Leftrightarrow < \varphi > \vee < \gamma > = < \kappa >$$

Teorema 5.3.1. *Dato un modulo M su $C[x]$ con $Ann(M) = < \mu >$, se $\mu = \varphi \cdot \gamma$, dove φ e γ sono primi tra loro, allora M si puo' scrivere come*

$$M = N \oplus P,$$

con $Ann(P) =< \varphi >$ *e* $Ann(N) =< \gamma >$.

Dimostrazione. Innanzitutto poniamo

$$N =< \varphi > M, \quad P =< \gamma > M,$$

e mostriamo che N e P sono sottomoduli di M tali che

$$M = N \oplus P.$$

I polinomi φ e γ sono primi tra di loro, cioe' il loro M.C.D. è il polinomio 1; quindi $< 1 >=< \varphi > + < \gamma >$ e

$$1 = a\varphi + b\gamma,$$

per opportuni $a, b \in C[x]$. Osserviamo inoltre che

$$\varphi = a\varphi^2 + b\varphi\gamma = a\varphi^2 + b\mu.$$

Ora, per ogni $v \in M$ si ha:

$$v = 1v = (a\varphi + b\gamma)v = a\varphi v + b\gamma v$$

dove $a\varphi v \in N, b\gamma v \in P$, cioè

$$M = N + P.$$

Inoltre, se $v \in N \cap P$ cioè $v = \varphi v_1 = \gamma v_2$ con $v_1, v_2 \in M$, allora

$$v = \varphi v_1 = a\varphi^2 v_1 + b\mu v_1 = a\varphi^2 v_1 = a\varphi\gamma v_2 = a\mu v_2 = 0.$$

Perciò

$$N \cap P = \{0\}.$$

Infine mostriamo che

$$Ann(N) =< \gamma > \quad , \quad Ann(P) =< \varphi > .$$

Infatti γ è un polinomio di grado minimo rispetto a tutti i polinomi che annullano $\varphi \cdot v$ per ogni $v \in M$: se per assurdo fosse l con $deg(l) < deg(\gamma)$, allora si avrebbe che $Ann(M) =< \varphi \cdot l >$ con $deg(\varphi \cdot l) < deg(\mu)$ contro le ipotesi. Analogamente si mostra che $Ann(P) =< \varphi >$.

□

Nelle ipotesi del teorema, si può poi dimostrare che ogni sottomodulo di M si può scrivere in modo unico come $N_1 \oplus P_1$, dove $N_1 \subseteq N$ e $P_1 \subseteq P$.

Il reticolo dei sottomoduli di M si può quindi ottenere come *prodotto diretto* tra i reticoli dei sottomoduli di N e P:

$$L(M) = L(N) \times L(P).$$

Ricordiamo la

Definizione 5.1. Il prodotto diretto dei reticoli L_1, L_2 è il prodotto cartesiano

$$L_1 \times L_2 = \{(x_1, x_2), \quad x_1 \in L_1, \quad x_2 \in L_2\},$$

munito dell'ordine parziale

$$(x_1, x_2) \leq (x_1', x_2') \;\Leftrightarrow\; x_1 \leq x_1',\ e\ x_2 \leq x_2';$$

gli estremi superiori ed inferiori in $L_1 \times L_2$ risultano essere

$$(x_1, x_2) \vee (y_1, y_2) = (x_1 \vee y_1, x_2 \vee y_2),$$

$$(x_1, x_2) \wedge (y_1, y_2) = (x_1 \wedge y_1, x_2 \wedge y_2).$$

5.4 Complemento ortogonale e principio di dualità

Definizione 5.2. Il prodotto interno (canonico) $\langle x, y \rangle$ di due vettori $x = (x_1, x_2, ..., x_n)$ e $y = (y_1, y_2, ..., y_n) \in C^n$ e' definito come

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_i}.$$

Definizione 5.3. Dato un sottospazio $W \subseteq C^n$, si definisce il complemento ortogonale $W^\perp$ di W come l'insieme dei vettori di C^n ortogonali a tutti i vettori di W, cioè

$$W^\perp = \{z \in C^n : w \in W \Rightarrow \langle w, z\rangle = 0\}.$$

Si può mostrare che $W^\perp$ è un *sottospazio* di C^n ed è un complemento di W:

$$W \oplus W^\perp = C^n.$$

Osservazione 17. L'operatore $^\perp$ è un *antimorfismo* del reticolo dei sottospazi di C^n:

$V \subseteq W \Rightarrow V^\perp \supseteq W^\perp$;
$(V \cap W)^\perp = V^\perp + W^\perp$;
$(V + W)^\perp = V^\perp \cap W^\perp$;
$(V^\perp)^\perp = V$.

Definizione 5.4. L'endomorfismo *aggiunto* f^* di un endomorfismo $f : C^n \to C^n$ e' l'endomorfismo di C^n definito dalle relazioni
$\langle fx, y\rangle = \langle x, f^*y\rangle$ per ogni $x, y \in C^n$.

La definizione e' ben posta, in quanto si mostra che l'aggiunto di un endomorfismo esiste sempre ed è unico.

L'operatore di aggiunzione gode delle seguenti proprieta':
$(f + g)^* = f^* + g^*, \quad (\alpha f)^* = \overline{\alpha} f^*,$
$(fg)^* = g^* f^*, \quad (f^*)^* = f,$
$(f^*)^* = f.$

Se consideriamo la matrice rappresentativa di un endomorfismo f rispetto alla base canonica $(e_1, e_2, ...e_n)$ e quella rappresentativa di f^* rispetto alla

stessa base, si ha che la seconda è la matrice coniugata della trasposta della prima:

$$[f] = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & & . \\ . & . & & . \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$$[f^*] = \begin{pmatrix} \overline{a}_{11} & \overline{a}_{21} & \dots & \overline{a}_{n1} \\ \overline{a}_{12} & \overline{a}_{22} & \dots & \overline{a}_{n2} \\ . & . & & . \\ . & . & & . \\ \overline{a}_{1n} & \overline{a}_{2n} & \dots & \overline{a}_{nn} \end{pmatrix}$$

Teorema 5.4.1. *Sia $f : C^n \to C^n$ un endomorfismo di C^n. Un sottospazio $W \subseteq C^n$ è f-invariante se e solo se il suo complemento ortogonale $W^\perp$ è f^*-invariante.*

Dimostrazione. Sia $W \subseteq C^n$ un sottospazio f-invariante. Allora, per ogni $z \in W^\perp$ si ha

$$\langle w, f^* z \rangle = \langle fw, z \rangle = 0,$$

per ogni $w \in W$, cioe' $f^* z \in W^\perp$. Cio' significa che il sottospazio $W^\perp$ è f^*-invariante. La verifica del viceversa e' analoga. □

Osservazione 18. L'operatore $^\perp$ è un *antimorfismo* dal reticolo dei sottospazi f-invarianti al reticolo dei sottospazi f^*-invarianti.

Dalle considerazioni precedenti segue il

Principio di dualita' per i reticoli di sottospazi invarianti. Una proposizione sui sottospazi f-invarianti, espressa nei termini della relazione di inclusione $\subseteq$, delle operazioni di somma $+$ e intersezione $\cap$, e delle nozioni ad esse riconducibili (come 'sup-irriducibile', 'inf-irriducibile', ...), e' vera per ogni endomorfismo f sse la proposizione duale, ottenuta invertendo l'ordine, scambiando le operazioni $+$ e $\cap$, e modificando coerentemente le nozioni ad esse riconducibili (ad esempio scambiando 'sup-irriducibile' con 'inf-irriducibile', ...) e' vera per ogni endomorfismo f.

Osservazione 19. Nel caso di matrici *hermitiane*, ossia matrici che coincidono con la propria coniugata della trasposta, si ha che $[f] = [f^*]$. Dato un qualsiasi sottospazio W è f-invariante, il suo complemento ortogonale sarà anch'esso f-invariante (poiché $f = f^*$). Quindi in questo caso ogni sottospazio f-invariante di C^n ammette complemento nel reticolo dei sottospazi f-invarianti di C^n, ovvero il reticolo dei sottospazi invarianti di C^n rispetto ad un operatore hermitiano, è *complementato.*

5.5 Sup-irriducibili ed inf-irriducibili

Teorema 5.5.1. *Sup-irriducibili vedono sotto di sé catene*

Sia $f : C^n \to C^n$ un endomorfismo di C^n. Se un sottospazio W di C^n e' sup-irriducibile nel reticolo dei sottospazi f-invarianti, allora l'intervallo $[0, W]$ è una catena.

Dimostrazione. Sappiamo che la restrizione di f ad un sottospazio f-invariante sup-irriducibile ha polinomio minimo e polinomio caratteristico uguali:

$$m_{f|w} = p_{f|w}.$$

Consideriamo ora W come sottomodulo di C^n, visto come $C[x]$-modulo via f. Sappiamo che

$$Ann(W) =< m_{f|_W} > .$$

Il polinomio minimo di $f|_W$ sarà la potenza di un polinomio primo. Infatti se fosse $m_{f|_W} = m_1 m_2$ con m_1, m_2 coprimi allora si avrebbe $W = W_1 \oplus W_2$, il che è impossibile in quanto W è sup-irriducibile.

Dunque possiamo scrivere

$$m_{f|_W} = (x - \lambda)^l, \quad \lambda \in C,$$

dove $l = dim W$.

Ora, per l'ultima proposizione del secondo paragrafo, si ha che il reticolo dei sottospazi f-invarianti di W e' una catena.

□

Dal principio di dualita' segue inoltre il

Teorema 5.5.2. *Inf-irriducibili vedono sopra di sé catene.*

Sia $f : C^n \to C^n$ un endomorfismo di C^n. Se un sottospazio W di C^n e' inf-irriducibile nel reticolo dei sottospazi f-invarianti, allora l'intervallo $[W, C^n]$ è una catena.

Capitolo 6

Reticoli semiprimari

Definizione 6.1. Un reticolo L si dice *semiprimario* se

1. L e' modulare, di rango finito;
2. per ogni sup-irriducibile $p \in L$, l'intervallo $[0, p]$ e' una catena;
3. per ogni inf-irriducibile $m \in L$, l'intervallo $[m, 1]$ e' una catena.

A parole un reticolo semiprimario è un reticolo modulare dove ogni elemento sup(inf)-irriducibile vede sotto (sopra) di sé una catena.

Si mostra che se un reticolo e' semiprimario allora sono semiprimari anche i suoi intervalli e il suo duale.

Teorema 6.0.3.
In un reticolo semiprimario L l'elemento massimo 1 si puo' scrivere come estremo superiore di un insieme indipendente di elementi sup-irriducibili, cioe' esistono $p_1, p_2, \dots p_r$ elementi sup-irriducibili di L tali che

$$1 = \bigvee_{i=1,\dots r} p_i \ , \qquad p_i \bigwedge (\vee_{j>i} p_j) = 0, \quad i = 1, \dots r.$$

Indicato con n_i il rango di p_i, si ha che il multinsieme

$$n_1, n_2, \dots, n_r$$

non dipende dalla scelta dei p_i e viene detta il tipo del reticolo L.

L' esistenza di un sistema indipendente di sup-irriducibili il cui sup sia 1 e' una conseguenza del Lemma seguente.

Lemma 6.0.4. *Ogni sup-irriducibile p di rango massimo in un reticolo semiprimario L possiede un complemento in L.*

Dimostrazione. Si osserva che esiste un inf-irriducibile $m \in L$ tale che

$$m \wedge p = 0.$$

Infatti, presi degli inf-irriducibili $m_1, \ldots, m_r$ il cui inf sia l'elemento minimo 0 di L, si ha:

$$0 = \wedge_{i=1,\ldots r} m_i = \wedge_{i=1,\ldots r}(m_i \wedge p).$$

Ora, poiche' l'intervallo $[0, p]$ e' una catena finita, deve esistere fra gli m_i un elemento m tale che $0 = m \wedge p$.

Ragionando dualmente, si prova che esiste un sup-irriducibile $p' \in L$ tale che

$$p' \vee m = 1.$$

Dalla formula di Grassmann per la funzione rango ρ, dai risultati dei passi precedenti e ricordando che p e' un sup-irriducibile di rango massimo, si ottiene la catena di disuguaglianze

$$\begin{aligned}
\rho(p) + \rho(m) &\geq \\
\rho(p') + \rho(m) &= \\
\rho(p' \wedge m) + \rho(p' \vee m) &= \\
\rho(p' \wedge m) + \rho(1) &\geq \\
\rho(0) + \rho(p \vee m) &= \\
\rho(p \wedge m) + \rho(p \vee m), &
\end{aligned}$$

il cui primo termine coincide con l'ultimo. Dunque tutte le disuguaglianze devono essere uguaglianze; si deduce che $\rho(p \vee m) = \rho(1)$, cosi' che $p \vee m = 1$. □

In un reticolo semiprimario dunque, l'elemento massimo 1 del reticolo L puo' essere scritto come:

$$1 = p_1 \vee m_1, \quad p_1 \wedge m_1 = 0,$$

dove p_1 è sup-irriducibile di rango massimo.

L'intervallo $[0, m_1]$ è un sottoreticolo ed è anch'esso semiprimario.

Quindi l'elemento massimo m_1 dell'intervallo $[0, m_1]$ puo' essere scritto come

$$m_1 = p_2 \vee m_2, \quad p_2 \wedge m_2 = 0,$$

dove p_2 è sup-irriducibile di rango massimo nell'intervallo $[0, m_1]$ è sup-irriducibile nel reticolo originario.

Iterando il processo, per la finitezza del rango di L, si ottengono dei sup-irriducibili $p_1, p_2, \ldots$ di L tali che

$$1 = \bigvee_{i=1,\ldots r} p_i \ , \qquad p_i \bigwedge (\vee_{j>i} p_j) = 0, \quad i = 1, \ldots r.$$

Capitolo 7

Forma canonica di Jordan

7.1 Blocchi di Jordan

Teorema 7.1.1. *Dato un endomorfismo $f : C^n \to C^n$ ed un sottospazio V, di dimensione r, sup-irriducibile nel reticolo dei sottospazi f-invarianti, esiste una base B di V tale che la matrice $[f|_V]_B$ è un blocco di Jordan così fatto:*

$$[f|_V]_B = \begin{pmatrix} \lambda & 0 & ... & 0 \\ 1 & \lambda & ... & 0 \\ 0 & 1 & ... & 0 \\ : & : & : & : \\ 0 & 0 & ... & \lambda \end{pmatrix}$$

Dimostrazione. Se V è sup-irriducibile allora $p_{f|_V} = m_{f|_V} = (x - \lambda)^r$ per un certo $\lambda \in C$.

Prendiamo un elemento z che appartiene a V ma non al sottospazio coperto da V e poniamo

$z_1 = z$

$\mathrm{z}_2 = (f - \lambda I)(z_1) = (f - \lambda I)^1(z)$

$\mathrm{z}_3 = (f - \lambda I)(z_2) = (f - \lambda I)^2(z)$.

$\vdots$

$\mathrm{z}_r = (f - \lambda I)(z_{r-1}) = (f - \lambda I)^{r-1}(z)$

È facile mostrare che tutti gli z_i per $i = 1, .., r$ sono linearmente indipendenti, quindi costituiscono una base di V.

La matrice rappresentativa di $f|_V$ rispetto alla base $B = (z_1, ..., z_r)$ ha come i-esima colonna le componenti di $f(z_i)$,

Per $i = 1, .., r-1$ si ha $z_{i+1} = (f - \lambda I)(z_i) = f(z_i) - \lambda z_i$, da cui

$$f(z_i) = \lambda z_i + z_{i+1}$$

. Per $i = r$ si ha $0 = (f - \lambda I)(z_r) = f(z_r) - \lambda z_r$, da cui

$$f(z_r) = \lambda z_r.$$

Quindi la forma della matrice rappresentativa è

$$[f|_V]_B = \begin{pmatrix} \lambda & 0 & ... & 0 \\ 1 & \lambda & ... & 0 \\ 0 & 1 & ... & 0 \\ : & : & : & : \\ 0 & 0 & ... & \lambda \end{pmatrix}$$

□

7.2 Forma canonica di Jordan

Teorema 7.2.1. *Dato un endomorfismo $f : C^n \to C^n$, esiste una base B di C^n tale che la matrice $[f]_B$ è una matrice a blocchi*

$$[f]_B = \begin{pmatrix} J_1 & 0 & ... & 0 \\ 0 & J_2 & ... & 0 \\ . & . & . & . \\ 0 & 0 & ... & J_p \end{pmatrix},$$

dove i blocchi J_i sono di Jordan.

Dimostrazione. Il reticolo dei sottospazi f-invarianti di C^n è semiprimario.

Infatti, nel Capitolo 3 si e' osservato che il reticolo dei sottospazi f-invarianti di C^n e' modulare di rango finito, e nel Capitolo 5 si e' dimostrato che i sottospazi sup-(inf-)irriducibli nel reticolo dei sottospazi f-invarianti vedono sotto di se' (sopra di se') catene.

Nei reticoli semiprimari l'elemento massimo si puo' scrivere come estremo superiore di un insieme indipendente di sup-irriducibili, per il Teorema 6.01. Quindi lo spazio C^n si puo' scrivere come somma diretta

$$C^n = W_1 \oplus W_2 \oplus ... \oplus W_p,$$

di sottospazi W_i sup-irriducibili nel reticolo dei sottospazi f-invarianti di C^n.

Per ogni sottospazio W_i sup-irriducibile possiamo costruire una base B_i tale che la matrice rappresentativa $[f|_{W_i}]_{B_i}$ sia un blocco di Jordan.

Ora, la matrice $[f]_B$ rappresentativa dell'endomorfismo f rispetto alla base B di C^n ottenuta dall'unione delle basi B_i diagonale a blocchi, dove i blocchi sono di Jordan:

$$[f]_B = \begin{pmatrix} J_1 & 0 & ... & 0 \\ 0 & J_2 & ... & 0 \\ . & . & . & . \\ 0 & 0 & ... & J_p \end{pmatrix},$$

$$J_i = [f|_{W_i}]_{B_i} = \begin{pmatrix} \lambda_i & 0 & 0 & ... & 0 \\ 1 & \lambda_i & 0 & ... & 0 \\ 0 & 1 & \lambda_i & ... & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & ... & \lambda_i \end{pmatrix}.$$

7.3 Unicità

Nel paragrafo precedente abbiamo mostrato che ogni endomorfismo di C^n puo' essere rappresentato da una matrice a blocchi di Jordan. Questa matrice dipende essenzialmente solo dall'endomorfismo, nel senso che due matrici a

blocchi di Jordan che rappesentano lo stesso endomorfismo differiscono solo per l'ordine in cui compaiono i blocchi.

Per semplicità di calcolo ci limiteremo a dimostrare questo fatto nel solo caso fondamentale di operatori nihilpotenti.

Dato un endomorfismo $f : C^n \to C^n$ nihilpotente di indice l, cioè tale che $f^{l-1} \neq 0$ e $f^l = 0$, lo spazio C^n si può spezzare in somma diretta di sottospazi f-invarianti sup-irriducibili:

$$C^n = V_1 \oplus V_2 \oplus ... \oplus V_s.$$

dove le dimensioni dei sottospazi V_i sono debolmente decrescenti. Gli interi $n_i = dim V_i$ *formano una partizione dell'intero* n, cioe'

$$n_1 \geq n_2 \geq ... \geq n_s \geq 1 \qquad , \qquad n_1 + n_2 + ... + n_s = n.$$

Se indichiamo con n'_k il numero degli addendi n_i maggiori o uguali a k, risulta:

$$n'_1 \geq n'_2 \geq ... \geq n'_t \geq 1 \qquad , \qquad n'_1 + n'_2 + ... + n'_t = n$$

con $s = n'_1, t = n_1$. Gli interi n'_k formano dunque una partizione di n, che è detta *partizione coniugata* della partizione formata dagli interi n_i. Noi mostreremo che gli interi n'_k sono univocamente determinati dall'endomorfismo f attraverso le relazioni

$$n'_k = dim Ker f^k - dim Ker f^{k-1}.$$

Poichè la partizione coniugata della coniugata è la partizione originaria, si potra' concludere che gli n_i sono individuati univocamente da f.

Se indichiamo con n'_k il numero degli addendi n_i maggiori o uguali a k, risulta:

$$n'_1 \geq n'_2 \geq ... \geq n'_t \geq 1 \qquad , \qquad n'_1 + n'_2 + ... + n'_t = n$$

con $s = n'_1, t = n_1$. Gli interi n'_k formano dunque una partizione di n, che è detta *partizione coniugata* della partizione formata dagli interi n_i. Noi mostreremo che gli interi n'_k sono univocamente determinati dall'endomorfismo f attraverso le relazioni

$$n'_k = dimKerf^k - dimKerf^{k-1}.$$

Poichè la partizione coniugata della coniugata è la partizione originaria, si potra' concludere che gli n_i sono individuati univocamente da f.

Il generico $v_i \in V_i =< w_i >_f$ è del tipo

$$v_i = c_0 w_i + c_1 f w_i + c_2 f^2 w_i + ...c_{n_i-1} f^{n_i-1} w_i = p_i(f) w_i$$

con $deg(p_i) < n_i$. Quindi il generico elemento $w \in C^n$ è ottenibile come

$$w = v_1 + v_2 + ... + v_s = p_1(f)w_1 + p_2(f)w_2 + ...p_s(f)w_s.$$

Primo passo.
Se $w \in Kerf$ si ha

$$0 = f(w) = fp_1(f)w_1 + ... + fp_1s(f)w_s;$$

poichè il vettore nullo si può scrivere in modo unico come sommma di vettori dei V_i, tali addendi sono tutti nulli cioè $fp_i(f)w_i = 0$ per ogni $i = 1, ..., s$. Ne segue che:

$$0 = fp_i(f)w_i = f(c_0 + c_1 f + ...c_{n_i-1} f^{n_i-1})w_i = c_0 f w_i + c_1 f^2 w_i + ...c_{n_i-1} f^{n_i} w_i;$$

ma dato che $f^{n_i} w_i = 0$ ed i vettori $fw_i, f^2 w_i, ..., f^{n_i-1} w_i$ sono linearmente indipendenti per costruzione, i coefficienti devono essere tutti nulli tranne quello di indice $n_i - 1$ cioè $c_0 = c_1 = c_2 = ... = c_{n_i-2} = 0$.

Quindi ponendo $c_{n_i-1} = a_i$ si ha

$$w \in Kerf \Leftrightarrow w = a_1 f^{n_1-1} w_1 + a_2 f^{n_2-1} w_2 + ... + a_s f^{n_s-1} w_s;$$

essendo i vettori $f^{n_1-1}w_1, f^{n_2-1}w_2, ..., f^{n_s-1}w_s$ generatori di $Ker(f)$ che sono linearmente indipendenti, si ha:

$$dimKerf = s = n'_1.$$

Secondo passo.

Se $w \in Kerf^2$ ragionando in modo analogo si ha che i coefficienti c_i devono essere tutti nulli tranne quelli di indice $n_i - 1$ ed $n_i - 2$ e quindi:

$$w \in Kerf^2 \Leftrightarrow w = (a_1 f^{n_1-1} + b_1 f^{n_1-2})w_1 + ... + (a_s f^{n_s-1} + b_s f^{n_s-1})w_s;$$

dove per ogni $i = 1, ..., s$ avremo due vettori linearmente indipendenti se $n_i \geq 2$ ed uno solo se $n_i = 1$.

Pertanto $dimKerf^2$ è uguale alla somma tra il numero di addendi n_i maggiori o uguali ad 1 ed il numero di addendi n_i maggiori o uguali a 2.

Secondo le notazioni introdotte si ha

$$dimKerf^2 = n'_1 + n'_2 \qquad n'_2 = dimKerf^2 - dimKerf.$$

h-mo passo. Con argomenti analoghi si prova che

$$dimKerf^h = n'_1 + n'_2 + ... + n'_h \qquad n'_h = dimKerf^h - dimKerf^{h-1}.$$

Bibliografia

[1] R.Baer *A unified Theory of Projective Spaces and Finite Abelian Groups* Trans. Am. Math. Soc. 52, 283-343 (1942)

[2] Birkhoff, Garrett *Lattice theory.* Third (new) ed. American Mathematical Society (AMS). Colloquium Publications. Vol. 25. Providence, R.I.: American Mathematical Society. (1967)

[3] Cohn, P.M. *Algebra.* Vol. 1. London etc.: John Wiley & Sons. (1974)

[4] L.Giudici *Dintorni del teorema di coordinatizzazione di Von Neumann; Appendice D: Reticoli fortemente semimodulari semiprimari* Tesi di Dottorato. Universita' degli Studi di Milano. (1995)

[5] Gohberg, Israel; Lancaster, Peter; Rodman, Leiba *Invariant subspaces of matrices with applications.* Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. New York etc.: John Wiley & Sons. (1986)

[6] B.Jonsson, G.S.Monk *Representation of Primary Arguesian Lattices* Pac. J. Math. 30, 95-139 (1969)

[7] Regonati, Francesco *Introduzione ai reticoli semiprimari*, in: Appunti dal corso di Algebra Superiore tenuto all'Universita' di Bologna dal Prof. Libero Verardi (a.a. 1998/99)

[8] G.P.Tesler *Semi-Primary Lattices and Tableau Algorithms* PHD Thesis, MIT (1995)

Ringraziamenti

Vorrei ringraziare innanzitutto i professori Francesco Regonati ed Andrea Brini, che mi hanno sopportato e seguito con pazienza.

Meritano un ringraziamento inoltre mio padre ed i miei amici più stretti che mi hanno sostenuto anche nei tanti momenti di difficoltà.

Un grazie infine a tutte le persone che, data la mia sbadataggine, avrò sicuramente dimenticato di ringraziare.

Giulia Gualandri