

TEOREMA DI CAYLEY-HAMILTON, TRIANGOLAZIONE, FORMA CANONICA DI JORDAN

Le ultime lezioni del corso sono andate via molto rapidamente, e alcune dimostrazioni non sono state chiarissime. Riassumo, in modo stringatissimo, tutto in questi appunti.

1. SPAZI VETTORIALI QUOZIENTE

A lezione ho introdotto il concetto di spazio vettoriale quoziente V/U attraverso quello di sottospazio affine di giacitura $U \subset V$. La definizione più tradizionale, sebbene equivalente, definisce gli elementi di V/U attraverso il concetto di congruenza modulo il sottospazio vettoriale U . Per una questione di completezza, riporto in queste note anche la definizione più comune.

1.1. Relazioni di equivalenza. Una relazione \sim su un insieme X è una *relazione di equivalenza* se è

- **riflessiva:** $x \sim x$ per ogni x ;
- **simmetrica:** $x \sim y$ ogni volta che $y \sim x$;
- **transitiva:** se $x \sim y$ e $y \sim z$ allora anche $x \sim z$.

Si dice che x e y sono \sim -equivalenti se $x \sim y$. Se x è un elemento dell'insieme X , la sua *classe di equivalenza* è il sottoinsieme $[x] = \{y \in X \mid y \sim x\}$. Per la riflessività, $[x]$ contiene sicuramente almeno l'elemento x . Inoltre, per simmetria e transitività, tutti gli elementi di $[x]$ sono \sim -equivalenti tra loro.

Lemma 1.1. Sia \sim una relazione di equivalenza sull'insieme X e $a, b \in X$. Sono affermazioni equivalenti:

- (1) $a \sim b$;
- (2) $a \in [b]$;
- (3) $[a] = [b]$.

Dimostrazione. (1) \iff (2) per definizione di classe di equivalenza. (2) \implies (3): se $x \in [a]$, allora $x \sim a$; poiché $a \in [b]$, allora $a \sim b$. Per transitività, si ha $x \sim b$, cioè $x \in [b]$. Viceversa, se $x \in [b]$, allora $x \sim b$; poiché $a \sim b$, allora anche $b \sim a$ per simmetria, e quindi $x \sim a$, cioè $x \in [a]$. (3) \implies (2) segue da $a \in [a]$. \square

Osservazione 1.2. Se $[a] \cap [b] \neq \emptyset$, sia $x \in [a] \cap [b]$. Allora $[a] = [x] = [b]$. Questo mostra che classi di equivalenza distinte devono essere disgiunte. Poiché $x \in [x]$, questo mostra che ogni relazione di equivalenza su X lo ripartisce nell'unione disgiunta delle corrispondenti classi di equivalenza.

E' importante osservare che ogni elemento di X appartiene ad una ed una sola classe di equivalenza: la proprietà di appartenere alla stessa classe di \sim -equivalenza è precisamente la relazione \sim .

1.2. Congruenza modulo un sottospazio. Sia V uno spazio vettoriale, ed U un suo sottospazio vettoriale. Diremo che $\mathbf{v}, \mathbf{v}' \in V$ sono congruenti modulo U , o in maniera più compatta

$$\mathbf{v} \equiv \mathbf{v}' \pmod{U},$$

se la differenza $\mathbf{v} - \mathbf{v}'$ appartiene a U . In altre parole, $\mathbf{v} \equiv \mathbf{v}' \pmod{U}$ se e solo se $\mathbf{v}' = \mathbf{v} + \mathbf{u}$ per qualche $\mathbf{u} \in U$. Mostrare come la congruenza modulo U sia una relazione di equivalenza è un facile esercizio – che mi aspetto svolgiate. Convincetevi, ad esempio, che la classe di equivalenza di 0 contiene tutti e soli gli elementi di U , e che

$$[\mathbf{v}]_U = \{\mathbf{v} + \mathbf{u} \mid \mathbf{u} \in U\} =: \mathbf{v} + U,$$

dove riconosciamo $\mathbf{v} + U$ come il sottospazio affine di V che contiene \mathbf{v} e ha giacitura uguale ad U . Quando non c'è rischio di confusione, userò la notazione $[v]$ invece della ridondante ma più precisa $[v]_U$.

Possiamo usare le operazioni di V per definire una struttura di spazio vettoriale sull'insieme delle classi di equivalenza, nel seguente modo:

$$[\mathbf{v}] + [\mathbf{v}'] = [\mathbf{v} + \mathbf{v}'], \quad \lambda[\mathbf{v}] = [\lambda\mathbf{v}].$$

L'unica cosa da controllare è che queste operazioni siano *ben definite*, cioè che la classe di equivalenza del risultato dipenda soltanto dalla classe di equivalenza degli addendi, e non dalla scelta dei rappresentanti.

Ad esempio, \mathbf{v} non è l'unico elemento di $[v]$, così come \mathbf{v}' non è l'unico elemento di $[v']$. Tuttavia, in qualsiasi modo scegliamo $\bar{\mathbf{v}} \in [v], \bar{\mathbf{v}}' \in [v']$ avremo che $\bar{\mathbf{v}} = \mathbf{v} + \mathbf{u}, \bar{\mathbf{v}}' = \mathbf{v}' + \mathbf{u}'$, con $\mathbf{u}, \mathbf{u}' \in U$. Pertanto $(\bar{\mathbf{v}} + \bar{\mathbf{v}}') = (\mathbf{v} + \mathbf{v}') + (\mathbf{u} + \mathbf{u}')$, e $(\mathbf{u} + \mathbf{u}')$ appartiene al sottospazio vettoriale U in quanto somma di due suoi elementi: in altre parole sommando un elemento equivalente a \mathbf{v} con un elemento equivalente a \mathbf{v}' si ottiene un elemento equivalente a $\mathbf{v} + \mathbf{v}'$. In modo perfettamente analogo si vede che è ben definita la moltiplicazione per uno scalare $\lambda[\mathbf{v}] = [\lambda\mathbf{v}]$.

Verificata la buona definizione delle operazioni, le proprietà di spazio vettoriale (commutatività, associatività della somma, esistenza dello 0 e dell'inverso additivo, distributività del prodotto rispetto alla somma, ecc...) seguono tutte facilmente dalle analoghe proprietà per le operazioni dello spazio vettoriale V . L'insieme delle classi di equivalenza di elementi di V modulo il sottospazio U , munito delle naturali operazioni di somma e prodotto per uno scalare, possiede quindi una struttura di spazio vettoriale, che si chiama *spazio vettoriale quoziente di V per U* e si indica con V/U .

1.3. Il teorema di omomorfismo. L'applicazione che associa ad ogni elemento di V la sua classe di equivalenza modulo U è lineare (mostratelo!) e definisce la *proiezione naturale*

$$\pi_U : V \rightarrow V/U.$$

Il nucleo di π è dato da tutti quegli elementi $\mathbf{v} \in V$ tali che $[\mathbf{v}] = [0]$: abbiamo già visto che gli elementi congruenti allo zero modulo U sono tutti e soli quelli che appartengono ad U , perciò $\ker \pi_U = U$. D'altronde la proiezione π_U è chiaramente suriettiva, poiché per definizione $[\mathbf{v}] = \pi_U(\mathbf{v})$. Il Teorema del rango ci garantisce che, se V ha dimensione finita,

$$\dim \ker \pi_U + \dim \operatorname{Im} \pi_U = \dim V.$$

In questo caso, otteniamo l'importante conseguenza

$$\dim V/U = \dim V - \dim U.$$

In effetti abbiamo visto a lezione che per costruire una base di V/U basta scegliere una base $(\mathbf{u}_1, \dots, \mathbf{u}_k)$ di U e completarla ad una base $(\mathbf{u}_1, \dots, \mathbf{u}_k, \mathbf{v}_1, \dots, \mathbf{v}_l)$ di V . Gli elementi $([\mathbf{v}_1], \dots, [\mathbf{v}_l])$ saranno allora una base di V/U . Il teorema di omomorfismo al quale siamo interessati enuncia il seguente risultato:

Teorema 1.3. *Sia $T : V \rightarrow W$ un'applicazione lineare, $U \subset V$ un sottospazio. Allora esiste un'applicazione lineare $\bar{T} : V/U \rightarrow W$ tale che $T = \bar{T} \circ \pi$ se e solo se $U \subset \ker T$. In tal caso \bar{T} è univocamente determinata.*

Dimostrazione. Una delle implicazioni (il "solo se") è facile: se $T = \bar{T} \circ \pi$, allora chiaramente $U = \ker \pi \subset \ker T$. Vediamo quindi l'altra implicazione.

Affiché \bar{T} soddisfi la proprietà richiesta, deve essere $\bar{T}([\mathbf{v}]) = T(\mathbf{v})$ per ogni $\mathbf{v} \in V$: questo definisce univocamente \bar{T} ; dobbiamo quindi solo verificare che questa definizione sia ben posta. Osserviamo che elementi di V equivalenti modulo U sono mandati da \bar{T} nella stessa immagine, dal momento che

$$T(\mathbf{v} + \mathbf{u}) = T(\mathbf{v}) + T(\mathbf{u}) = T(\mathbf{v}) + 0 = T(\mathbf{v}),$$

se $\mathbf{u} \in U \subset \ker T$, quindi l'applicazione \bar{T} è ben definita. La linearità è adesso di facile dimostrazione. \square

Il caso che più ci interesserà in seguito è quello in cui l'endomorfismo $T : V \rightarrow V$ soddisfa $T(U) \subset U$: il sottospazio $U \subset V$ è cioè T -invariante. In questa situazione, T definisce per composizione un'applicazione lineare $\pi_U \circ T : V \rightarrow V/U$ il cui nucleo contiene U . Ma allora, per il teorema di omomorfismo, rimane ben definita un'applicazione lineare $\tilde{T} = \overline{\pi_U \circ T} : V/U \rightarrow V/U$. Nel seguito, spesso indicheremo l'applicazione indotta da T sul quoziente semplicemente con $T : V/U \rightarrow V/U$. L'applicazione \tilde{T} è detta *applicazione indotta da T sul quoziente V/U* : in termini più espliciti, si ha

$$\tilde{T}([\mathbf{v}]) = [T(\mathbf{v})],$$

oppure $\tilde{T}(\mathbf{v} + U) = T(\mathbf{v}) + U$, come abbiamo scritto spesso a lezione.

Esercizi del § 1.

- Mostrare che la proiezione canonica $\pi_U : V \rightarrow V/U$ è un'applicazione lineare, e che il suo nucleo coincide con U .
- Sia $T : V \rightarrow W$ un'applicazione lineare, e $U \subset W$ un sottospazio vettoriale. Mostrare che $\{\mathbf{v} \in V \mid T(\mathbf{v}) \in U\}$ è un sottospazio vettoriale di V .
- Sia $(\mathbf{u}_1, \dots, \mathbf{u}_k)$ una base di U . Mostrare che $[\mathbf{v}_1], \dots, [\mathbf{v}_l] \in V/U$ sono linearmente indipendenti se e solo se $\mathbf{v}_1, \dots, \mathbf{v}_l, \mathbf{u}_1, \dots, \mathbf{u}_k$ sono linearmente indipendenti in V . In questo caso $\mathbf{v}_1, \dots, \mathbf{v}_l$ si dicono anche *linearmente indipendenti modulo U* .
- Sia $V = \mathbb{R}^3$ e $U \subset V$ il sottospazio generato da $(1, 2, -3)$. Dire se i vettori $(1, 1, 1)$ e $(2, -1, 3)$ sono linearmente dipendenti o indipendenti modulo U .
- Sia V lo spazio vettoriale delle matrici complesse 3×3 e D il sottospazio delle matrici diagonali. Stabilire se le matrici

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 6 \\ 4 & 6 & 8 \\ 6 & 8 & -1 \end{pmatrix}$$

siano o meno linearmente indipendenti modulo D .

- f) Siano V, V' spazi vettoriali e $U \subset V$ un sottospazio vettoriale. Mostrare che ogni applicazione lineare $T : V \rightarrow V'$ definisce univocamente un'applicazione lineare $\tilde{T} : V/U \rightarrow V'/T(U)$ tale che $\pi_{T(U)} \circ T = \tilde{T} \circ \pi_U$.
- g) Sia $T : V \rightarrow V$ un'applicazione lineare, ed U un sottospazio vettoriale T -invariante di V , ovvero un sottospazio tale che $T(U) \subset U$. Scegliamo una base $\mathfrak{B} = (\mathbf{u}_1, \dots, \mathbf{u}_l, \mathbf{v}_1, \dots, \mathbf{v}_k)$ di V nella quale i primi l elementi costituiscano una base di U . Allora $\tilde{\mathfrak{B}} = ([\mathbf{v}_1], \dots, [\mathbf{v}_k])$ è una base di V/U , la matrice di T nella base $\tilde{\mathfrak{B}}$ è triangolare a blocchi, cioè della forma:

$$\begin{pmatrix} a_{11} & \dots & a_{1l} & b_{11} & \dots & b_{1k} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{l1} & \dots & a_{ll} & b_{l1} & \dots & b_{lk} \\ 0 & \dots & 0 & c_{11} & \dots & c_{1k} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & c_{k1} & \dots & c_{kk} \end{pmatrix},$$

e allora quella di $\tilde{T} = \overline{\pi_U \circ T}$ si ricava come segue:

$$\begin{pmatrix} c_{11} & \dots & c_{1k} \\ \vdots & & \vdots \\ c_{k1} & \dots & c_{kk} \end{pmatrix}.$$

Mostrare inoltre che ogni base $\tilde{\mathfrak{B}}$ di V/U si ottiene da una base \mathfrak{B} di V nella maniera appena descritta, e che la scelta della base $(\mathbf{u}_1, \dots, \mathbf{u}_l)$ di U può essere fatta in modo arbitrario.

- h) Siano V uno spazio vettoriale, $T : V \rightarrow V$ un'applicazione lineare ed U un sottospazio T -invariante di V . Mostrare che il polinomio caratteristico di T è il prodotto dei polinomi caratteristici della restrizione $T|_U$ e della proiezione al quoziente $\tilde{T} = \overline{\pi_U \circ T}$.
- i) Siano T ed S endomorfismi di uno spazio vettoriale V di dimensione finita. Mostrare che TS e ST hanno lo stesso polinomio caratteristico. [Sugg.: nel caso in cui uno degli endomorfismi sia invertibile, TS ed ST sono coniugate... Il caso generale è invece più difficile, ma provateci!]

2. TRIANGOLAZIONE DI ENDOMORFISMI COMPLESSI

Il risultato di triangolazione che dimostro in questo paragrafo non è di per sé fondamentale. E' tuttavia un utile strumento per la dimostrazione di tutta una serie di risultati, dal Teorema di Cayley-Hamilton al Teorema spettrale, che illustrano in maniera evidente la struttura degli endomorfismi di uno spazio vettoriale complesso di dimensione finita. In tutto ciò che segue, il campo scelto per gli scalari è sempre \mathbb{C} e quindi tutti gli spazi vettoriali sono complessi; tuttavia, se decidete di utilizzare un qualsiasi campo algebricamente chiuso i risultati si estendono facilmente.

2.1. Il Teorema fondamentale dell'algebra. I numeri complessi sono stati introdotti per permettere l'estrazione della radice quadrata di numeri negativi, e rendere possibile così la risoluzione di qualsiasi equazione di secondo grado a coefficienti reali.

E' tuttavia in linea di principio ipotizzabile che per risolvere equazioni a coefficienti reali di grado più alto, o anche solamente per risolvere equazioni di secondo grado a coefficienti complessi, sia nuovamente necessario estendere l'insieme dei numeri necessari a campi sempre più grandi. Questo non succede, come mostra il seguente risultato, detto *Teorema fondamentale dell'algebra*.

Teorema 2.1. Ogni polinomio non costante $p(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$, $a_n \neq 0$, $n \geq 1$ a coefficienti complessi ammette almeno una radice complessa. In particolare, ogni polinomio a coefficienti complessi si spezza nel prodotto di polinomi complessi di grado 1.

Dimostrazione. Vedrete la dimostrazione di questo fatto quando farete un po' di omologia OPPURE di Teoria di Galois OPPURE di funzioni oморfe: esistono anche dimostrazioni del tutto elementari, ma personalmente non le trovo illuminanti. E' comunque il caso di osservare che la seconda affermazione segue dalla prima applicando ripetutamente il metodo di Ruffini per la divisione tra polinomi. \square

Se il polinomio complesso $p(z)$ ammette la fattorizzazione in fattori lineari

$$p(z) = a_n (z - \alpha_1)^{n_1} \dots (z - \alpha_h)^{n_h},$$

con gli $\alpha_j \in \mathbb{C}$ tutti distinti, allora le radici complesse di $p(z)$ sono tutti e soli i numeri α_j , $1 \leq j \leq h$, e n_j è la molteplicità algebrica della radice α_j . In particolare, il numero delle radici di p , ognuna contata con la sua molteplicità, è uguale al grado di p .

2.2. Esistenza di autovettori. Se T è un endomorfismo dello spazio vettoriale V , un elemento $0 \neq \mathbf{u} \in V$ è autovettore di T se $T(\mathbf{u})$ è un multiplo di \mathbf{u} , cioè se esiste uno scalare λ tale che $T(\mathbf{u}) = \lambda \mathbf{u}$.

E' facile costruire esempi di endomorfismi che non possiedono autovettori: l'operatore di shift a destra delle successioni a valori in un campo \mathbb{K} :

$$S(a_0, a_1, a_2, \dots) = (0, a_0, a_1, a_2, \dots)$$

non possiede mai autovettori. Più semplicemente, la rotazione del piano reale \mathbb{R}^2 di un angolo $\theta \neq 0, \pi$ fissa solo l'origine, e non possiede quindi autovettori reali. La sua *complettizzazione* – l'endomorfismo di \mathbb{C}^2 che possiede la stessa matrice – ammette tuttavia autovettori complessi, e questo è un caso particolare di un fenomeno del tutto generale.

Teorema 2.2. *Ogni endomorfismo T di uno spazio vettoriale complesso di dimensione finita (non nulla) V possiede almeno un autovettore.*

Dimostrazione. Se $\lambda \in \mathbb{C}$, i λ -autovettori di T sono gli elementi non nulli dell'autospazio $V(\lambda) = \ker(\lambda \text{id} - T)$. Pertanto ne esistono esattamente quando l'applicazione lineare¹ $\lambda \text{id} - T$ è non iniettiva.

Controllare l'iniettività di un endomorfismo di uno spazio vettoriale di dimensione finita è però molto facile: è sufficiente calcolare il suo determinante² e verificare se sia o meno uguale a zero. L'endomorfismo è iniettivo nel caso il determinante sia diverso da zero, e non iniettivo (o singolare) altrimenti.

Affinché λ sia un autovalore di T deve quindi valere $\det(\lambda \text{id} - T) = 0$. Sappiamo bene che se $\dim V = n$, allora $\det(x \text{id} - T)$ è un polinomio – detto *polinomio caratteristico* – di grado n in x . Per il Teorema fondamentale dell'algebra, $\det(x \text{id} - T) = 0$ ammetterà almeno una radice, cioè un autovalore di T , al quale corrisponderà un autovettore non nullo. \square

Osservazione 2.3. Un endomorfismo di uno spazio vettoriale V di dimensione zero non ammette autovettori, semplicemente perché in questo caso V non contiene elementi non nulli.

2.3. Forma triangolare e bandiere invarianti. Possiamo a questo punto dimostrare che ogni endomorfismo di uno spazio vettoriale complesso di dimensione finita è triangolabile: è possibile cioè trovare una base nella quale la matrice che rappresenta l'endomorfismo sia triangolare superiore. La dimostrazione è per induzione, ed utilizza il concetto di spazio vettoriale quoziente, quindi prestate un minimo di attenzione e cercate di comprenderla bene.

Teorema 2.4. *Sia V uno spazio vettoriale di dimensione finita, T un suo endomorfismo. Allora è sempre possibile trovare una base \mathfrak{B} di V tale che ${}_{\mathfrak{B}}[T]_{\mathfrak{B}}$ sia triangolare superiore, cioè:*

$${}_{\mathfrak{B}}[T]_{\mathfrak{B}} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}.$$

Dimostrazione. Per induzione sulla $\dim V$, il caso $\dim V = 1$ essendo ovvio³. Sia $\mathbf{u} \in V$ un autovettore di T di autovalore λ ; allora il sottospazio vettoriale $U \subset V$ generato da \mathbf{u} è T -invariante, e T induce un endomorfismo \tilde{T} dello spazio vettoriale quoziente V/U che ha dimensione inferiore a quella di V . Per ipotesi induttiva, \tilde{T} si triangolarizza in una base $([\mathbf{v}_1], \dots, [\mathbf{v}_n])$ di V/U . Ma allora, per l'esercizio 1.g), $(\mathbf{u}, \mathbf{v}_1, \dots, \mathbf{v}_n)$ è una base di V in cui T è triangolare superiore. \square

La proposizione che segue mostra quale proprietà di una base garantisce che T ne sia triangolata.

Proposizione 2.5. *Sia $\mathfrak{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ una base di V ; allora \mathfrak{B} triangolarizza T se e solo se il sottospazio $V_h = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_h \rangle$ è T -invariante per ogni $1 \leq h \leq n$.*

Dimostrazione. T è triangolare nella base \mathfrak{B} se e solo se $T(\mathbf{v}_h) \in V_h$ per ogni $1 \leq h \leq n$. Per la definizione dei sottospazi V_h , questo accade se e solo se $T(V_h) \subset V_h$. \square

La successione di sottospazi V_h costruita a partire da una base \mathfrak{B} è detta *bandiera associata a \mathfrak{B}* . Più in generale una bandiera di uno spazio vettoriale V di dimensione n è una successione di sottospazi

$$V_1 \subset V_2 \subset \dots \subset V_n,$$

con la proprietà che $\dim V_i = i$. Chiaramente $V_n = V$, ed ogni bandiera è associata a qualche base.

¹A lezione c'è stato un proliferare di $(-1)^n$ nel polinomio caratteristico perché abbiamo sempre considerato $T - \lambda \text{id}$. Se invece riformuliamo tutto in termini di $\lambda \text{id} - T$, i segni scompaiono e viviamo più felici.

²Cioè il determinante della matrice ${}_{\mathfrak{B}}[\lambda \text{id} - T]_{\mathfrak{B}}$ associata a T utilizzando sia in partenza che in arrivo la stessa base \mathfrak{B} , che per il Teorema di Binet non dipende (il determinante, non la matrice!) dalla scelta di \mathfrak{B} .

³E, in fondo, anche il caso $\dim V = 0$: una matrice è triangolare superiore se tutti i suoi coefficienti al di sotto della diagonale principale sono nulli. Non avendo una matrice 0×0 coefficienti, non ne ha nemmeno al di sotto della diagonale principale, e quindi non possono essere non nulli.

Osservazione 2.6. Ogni manipolazione di una base $\mathfrak{B} = (\mathbf{v}_1, \dots, \mathbf{v}_n)$ che non ne alteri la successione sopra definita di sottospazi V_h non altera la triangolarità della matrice che rappresenta T .

Esercizi del § 2.

- a) Trovare tutte le soluzioni complesse delle equazioni $z^2 = i$ e di $z^3 = 11 + 2i$. Verificare che il numero delle soluzioni, contate con le loro molteplicità, è rispettivamente due e tre.
- b) Se \mathbb{K} è un campo, indichiamo con $\mathbb{K}^{\mathbb{N}}$ il \mathbb{K} -spazio vettoriale delle successioni $(a_n)_{n \in \mathbb{N}}$ a valori in \mathbb{K} . Verificare che l'operatore di shift $S : \mathbb{K}^{\mathbb{N}} \rightarrow \mathbb{K}^{\mathbb{N}}$ definito da

$$S(a_0, a_1, a_2, \dots) = (0, a_0, a_1, a_2, \dots)$$

è \mathbb{K} -lineare, e mostrare che non possiede autovettori, indipendentemente dalla scelta di \mathbb{K} .

- c) Determinare autovalori e autovettori dell'applicazione lineare $R_\theta : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ di matrice

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

- d) Verificare che se T è un endomorfismo di uno spazio vettoriale V di dimensione finita, allora $\det T = \det_{\mathfrak{B}}[T]_{\mathfrak{B}}$ è indipendente dalla scelta della base \mathfrak{B} di V . Dedurre che il polinomio caratteristico di T è definito a prescindere dalla scelta di una base.
- e) Se M è una matrice 2×2 complessa tale che $M^3 = 0$, allora $M^2 = 0$.
- f) Calcolare gli autovalori di una⁴ matrice triangolare superiore.
- g) Un'endomorfismo T è nilpotente se $T^N = 0$ per qualche $N > 0$. Mostrare che se V è uno spazio vettoriale di dimensione finita, e $T \in \text{End}(V)$ è nilpotente, allora esiste una base \mathfrak{B} di V in cui la matrice associata a T è *triangolare superiore stretta*, cioè triangolare superiore con tutti zeri sulla diagonale principale. Dedurre che se $\dim V = n$, allora $T^n = 0$.
- h) L'operazione di derivazione D definisce un endomorfismo dello spazio vettoriale dei polinomi complessi di grado ≤ 3 . Mostrare che D è nilpotente, determinare una base in cui la sua matrice sia triangolare superiore, e verificare che $D^4 = 0$, ma che $D^3 \neq 0$.
- i) Sia V uno spazio vettoriale di dimensione finita, T un suo endomorfismo nilpotente. Allora gli autovalori di T sono tutti nulli, e $\alpha \text{id} - T$ è invertibile per ogni $0 \neq \alpha \in \mathbb{C}$. In particolare, il polinomio caratteristico di $\alpha \text{id} - T$ è $(x - \alpha)^{\dim V}$.
- j) Sia V uno spazio vettoriale di dimensione finita. Mostrare che comunque sia fissata una bandiera $\mathcal{F} : V_1 \subset \dots \subset V_n$ di V è possibile trovare una base \mathfrak{B} alla quale \mathcal{F} sia associata.
- k) Siano V_1 il sottospazio vettoriale di \mathbb{R}^3 generato da $(1, 2, 3)$ e V_2 quello di equazione cartesiana $x - 2y + z = 0$. Verificare che $V_1 \subset V_2$ e quindi che $V_1 \subset V_2 \subset V_3 = \mathbb{R}^3$ è una bandiera. Determinare una base di \mathbb{R}^3 alla quale tale bandiera sia associata.
- l) Sia V uno spazio vettoriale complesso di dimensione finita, T, S endomorfismi di V . Mostrare che se T ed S commutano, cioè se $T \circ S = S \circ T$, allora esiste una base \mathfrak{B} di V che triangolarizza sia T che S : si dice che \mathfrak{B} **triangolarizza simultaneamente** i due endomorfismi.
[Sugg.: è sufficiente far vedere che esiste un autovettore simultaneo di T ed S . Mostrate allora che ciascun autospatio di T è S -stabile...]
- m) Mostrare che l'ortonormalizzazione di Gram-Schmidt non altera la bandiera. Dedurre che ogni endomorfismo di uno spazio vettoriale complesso – sul quale sia definito un prodotto scalare Hermitiano definito positivo – di dimensione finita possiede una base **ortonormale** nella quale la matrice associata all'endomorfismo è triangolare. [NB: se avete visto l'ortonormalizzazione di Gram-Schmidt solo nel caso reale, considerate il caso in cui lo spazio vettoriale sia reale, così come anche gli autovalori dell'endomorfismo, ed il prodotto scalare sia simmetrico e definito positivo. Se non avete visto l'ortonormalizzazione di Gram-Schmidt neanche nel caso reale, aspettate di vederla prima di affrontare questo esercizio.]

3. IL TEOREMA DI CAYLEY-HAMILTON

3.1. Annullatore di un endomorfismo. Sia V uno spazio vettoriale, e T un endomorfismo di V . Dal momento che gli spazi vettoriali di partenza ed arrivo di T coincidono, ha senso considerare la composizione di T con se stesso, che possiamo indicare con $T^2 = T \circ T$. Allo stesso modo, possiamo definire $T^3 = T \circ T \circ T$, ed in generale $T^{n+1} = T^n \circ T$.

Se vogliamo definire T^0 in modo che $T^0 T^n = T^n T^0 = T^n$, una scelta naturale è quella di porre $T^0 = \text{id}$, cosa che faremo. L'insieme $\text{End}(V)$ degli endomorfismi di V è esso stesso uno spazio vettoriale, nel quale la composizione è chiaramente distributiva rispetto alla somma. Ha senso quindi considerare

⁴Si scrive "una" ma si legge "ogni"!

espressioni polinomiali in un endomorfismo: ad esempio, il polinomio $p(x) = x^2 + 3x - 5$ calcolato sull'endomorfismo T restituisce l'endomorfismo $T^2 + 3T - 5\text{id}$, che calcolato su un vettore $\mathbf{v} \in V$ dà come risultato $T(T(\mathbf{v})) + 3T(\mathbf{v}) - 5\mathbf{v}$. In ciò che segue, V è uno spazio vettoriale di dimensione finita.

Proposizione 3.1. *Ogni endomorfismo T di V è annullato da qualche polinomio $p(x) \neq 0$.*

Dimostrazione. $\text{End}(V)$ è uno spazio vettoriale di dimensione $(\dim V)^2$. Pertanto, un insieme di elementi di $\text{End}(V)$ di cardinalità superiore a $\dim \text{End}(V)$, comunque scelto, sarà linearmente dipendente.

Gli elementi $\text{id}, T, T^2, \dots, T^k$ saranno quindi linearmente dipendenti per k sufficientemente grande, ed esisterà di conseguenza una relazione lineare tra di loro, e quindi un'espressione polinomiale non banale in T uguale a 0. \square

Ogni polinomio $p(x)$ tale che $p(T) = 0$ si dice *annullare* T , e l'insieme di tutti i polinomi che annullano T è il suo *annullatore*. L'annullatore contiene sempre il polinomio costante 0, ma abbiamo mostrato che deve contenere necessariamente almeno un polinomio non nullo – di grado minore o uguale a $(\dim V)^2$. Sapere che un endomorfismo è annullato da un polinomio è solitamente un'informazione molto forte: abbiamo visto a lezione come un endomorfismo uguale al proprio quadrato ($P^2 = P$) sia sempre diagonalizzabile, e possa sempre essere descritto come operatore di proiezione su un sottospazio opportunamente individuato. Allo stesso modo gli operatori a quadrato identico ($T^2 = \text{id}$) sono sempre operatori di simmetria – non necessariamente ortogonale – rispetto a qualche sottospazio.

E' ragionevole supporre che il polinomio (monico) di grado minimo tra quelli contenuti nell'annullatore di T ne descriva molte delle proprietà algebro-geometriche, ed è quindi un concetto interessante da studiare. Tale polinomio è detto *polinomio minimo di T* e la seguente osservazione ne mette in evidenza un'importante caratteristica.

Lemma 3.2. *Sia $p(x)$ di grado minimo tra i polinomi (non identicamente nulli) che annullano T . Se $a(T) = 0$, allora $p(x)$ divide $a(x)$.*

Dimostrazione. Sia $a(x) = p(x)q(x) + r(x)$ la divisione con resto tra polinomi; il grado di $r(x)$ è strettamente inferiore a quello di $p(x)$. Calcolando entrambi i membri su T si ottiene $0 = a(T) = p(T)q(T) + r(T) = r(T)$. Allora $r(x)$ è un polinomio che annulla T di grado inferiore a quello di $p(x)$. Per minimalità del grado di $p(x)$, deve essere $r(x) = 0$, da cui $a(x)$ è un multiplo di $p(x)$. \square

I polinomi di grado minimo che annullano T sono perciò uguali a meno di moltiplicazione per una costante. E' uso comune imporre che il polinomio minimo sia monico, cioè che il suo primo coefficiente sia 1.

3.2. Teorema di Cayley-Hamilton per endomorfismi complessi. Sia $p(x)$ un polinomio che annulla $T \in \text{End}(V)$, λ un autovalore di T e $\mathbf{u} \neq 0$ un corrispondente autovettore; allora $T(\mathbf{u}) = \lambda\mathbf{u}$ e quindi $T^n(\mathbf{u}) = \lambda^n\mathbf{u}$. Dal momento che $p(T) = 0$ avremo $0 = p(T)\mathbf{u} = p(\lambda)\mathbf{u}$ e quindi $p(\lambda) = 0$: ne segue che ogni autovalore è radice di ogni polinomio che annulla T , ed in particolare del polinomio minimo.

Conosciamo già un polinomio le cui radici sono gli autovalori di T : il polinomio caratteristico $p_T(x) = \det(x\text{id} - T)$. Il Teorema di Cayley-Hamilton afferma che questo polinomio annulla sempre l'endomorfismo che lo definisce. Quella che segue è la dimostrazione più elementare che conosco di questo fatto:

Teorema 3.3. *Se T è un endomorfismo di V , allora $p_T(T) = 0$.*

Dimostrazione. Dimostriamo l'enunciato per induzione sulla dimensione di V . Per $\dim V = 1$ l'enunciato è ovvio⁵. Per $\dim V > 1$, osserviamo che V ha sicuramente dei sottospazi U che sono T -invarianti e non banali: basta ad esempio prendere la retta generata da un autovettore (abbiamo visto nel Teorema 2.2 che T possiede almeno un autovettore). L'endomorfismo T induce i due endomorfismi

$$T|_U: U \rightarrow U \quad \text{e} \quad \tilde{T}: V/U \rightarrow V/U$$

e sappiamo dall'esercizio 1.h) che

$$p_T(x) = p_{T|_U}(x) p_{\tilde{T}}(x)$$

Poiché U è non banale, si ha $\dim U < \dim V$ e $\dim V/U < \dim V$, dunque dall'ipotesi induttiva

$$p_{T|_U}(T|_U) = 0 \quad \text{e} \quad p_{\tilde{T}}(\tilde{T}) = 0.$$

Si ha $p_{\tilde{T}}(\tilde{T}) = \widetilde{p_{T|_U}(T)}$ dunque $p_{\tilde{T}}(\tilde{T}) = 0$ equivale a $\text{Im}(p_{T|_U}(T)) \subset U$ (convincetevi di questo fatto). Ma allora

$$p_{T|_U}(T)|_{\text{Im}(p_{T|_U}(T))} = p_{T|_U}(T)|_U = p_{T|_U}(T|_U) = 0$$

⁵E anche se $\dim V = 0$, in quando l'unico endomorfismo di uno spazio vettoriale di dimensione 0 è quello nullo.

e dunque

$$p_T(T) = p_{T|_U}(T) p_{\tilde{T}}(T) = 0.$$

□

Corollario 3.4. *Il polinomio minimo di ogni endomorfismo T di V divide sempre il suo polinomio caratteristico. In particolare $\lambda \in \mathbb{C}$ è radice del polinomio minimo se e solo se è un autovalore di T se e solo se è radice del polinomio caratteristico.*

3.3. Caso generale. La dimostrazione del Teorema di Cayley-Hamilton che abbiamo appena dato si traduce in termini matriciali, ed è valida quindi anche per endomorfismi di uno spazio vettoriale reale di dimensione finita. In effetti, in questo caso è sufficiente dimostrare l'enunciato per matrici reali, che sono a maggior ragione complesse, e possiamo quindi ridurci al caso già trattato.

In generale, la dimostrazione precedentemente riportata funziona per ogni campo algebricamente chiuso. Un risultato classico di teoria dei campi mostra che, cosiccome \mathbb{R} è contenuto in \mathbb{C} , ogni campo è contenuto in un campo algebricamente chiuso opportunamente scelto. Pertanto, anche se la dimostrazione utilizza proprietà di chiusura algebrica, l'enunciato rimane valido su qualsiasi campo.

Senza voler scomodare l'esistenza di una chiusura algebrica di ciascun campo, si può procedere nel seguente modo:

- Mostrare, come avete fatto in uno dei fogli di esercizi, che se M è una matrice compagna allora $p_M(M) = 0$.
- Mostrare che, comunque preso $\mathbf{v} \in V$, che esiste un massimo valore di $k \in \mathbb{N}$ tale che $\mathbf{v}, T(\mathbf{v}), \dots, T^k(\mathbf{v})$ siano linearmente indipendenti (ad esempio, se \mathbf{v} è un autovettore tale massimo valore è 0). In effetti, se $k > \dim V$, allora tali elementi sono necessariamente linearmente dipendenti.
- Trovato tale k , mostrare che $U = \text{span}(\mathbf{v}, T(\mathbf{v}), \dots, T^k(\mathbf{v}))$ è un sottospazio T -invariante di V e che la matrice associata all'endomorfismo $T|_U \in \text{End}(U)$ nella base $\mathbf{v}, T(\mathbf{v}), \dots, T^k(\mathbf{v})$ è una matrice compagna.
- Usare il fatto che $p_T(x) = p_{T|_U}(x) p_{\tilde{T}}(x)$ e procedere per induzione come già fatto precedentemente.

Esercizi del § 3.

- a) Mostrare che ogni endomorfismo annullato da un polinomio di grado uno è un multiplo dell'identità.
- b) Un'endomorfismo di uno spazio vettoriale di dimensione n è nilpotente se e solo se il suo polinomio caratteristico è x^n .
- c) Mostrare che, nella dimostrazione del Teorema 3.3, $p_{\tilde{T}}(\tilde{T}) = \widetilde{p_{\tilde{T}}(T)}$.
- d) Mostrare che, nella dimostrazione del Teorema 3.3, $p_{\tilde{T}}(\tilde{T}) = 0$ equivale a $\text{Im}(p_{\tilde{T}}(T)) \subset U$.
- e) Fornire una traduzione tra la dimostrazione del Teorema di Cayley-Hamilton data a lezione e quella presentata in questi appunti.
- f) Il polinomio minimo ed il polinomio caratteristico coincidono per una matrice 2×2 che non è multipla dell'identità.
- g) Il polinomio minimo di una matrice diagonale a blocchi è il minimo comune multiplo dei polinomi minimi dei vari blocchi.
- h) Siano $\lambda_1, \dots, \lambda_h$ gli autovalori (distinti) di una matrice diagonale. Allora il suo polinomio minimo è $(x - \lambda_1) \dots (x - \lambda_h)$. In particolare, il polinomio minimo di un endomorfismo diagonalizzabile non ha radici multiple: è *libero da quadrati*.
- i) Calcolare il polinomio minimo delle matrici

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

- j) Calcolare il polinomio minimo delle matrici

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

- k) Calcolare il polinomio minimo delle matrici

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & -1 \\ 0 & 3 & 0 \\ 1 & 1 & 3 \end{pmatrix}.$$

- l) Mostrare che il polinomio minimo di una matrice M è uguale a quello della sua trasposta.

4. DECOMPOSIZIONE DI JORDAN

Due matrici diagonalizzabili sono simili se e solo se possiedono gli stessi autovalori, contati con la loro molteplicità. Il problema di stabilire se matrici non diagonalizzabili siano simili è più complesso⁶, e richiede strumenti più sofisticati. Una risposta completa a questo problema è data dalla forma canonica di Jordan, che garantisce, per ogni endomorfismo di uno spazio vettoriale di dimensione finita, una base in cui la matrice associata sia diagonale a blocchi con blocchi triangolari di struttura particolarmente semplice: una tale matrice è detta *in forma canonica di Jordan*. Due matrici $A, B \in \text{Mat}_{n \times n}(\mathbb{C})$ saranno allora simili esattamente quando gli endomorfismi $L_A, L_B \in \text{End}(\mathbb{C}^n)$ avranno la stessa forma canonica di Jordan, che può essere determinata calcolando in maniera elementare gli autovalori degli endomorfismi, insieme ad alcuni invarianti numerici associati a ciascun autovalore.

Sappiamo già che un endomorfismo diagonalizzabile decompone lo spazio vettoriale sul quale agisce in somma diretta dei suoi autospazi. Questa decomposizione non può sussistere nel caso di un endomorfismo non diagonalizzabile: la somma degli autospazi sarà certamente diretta, ma non coinciderà con l'intero spazio vettoriale.

Agli autospazi è però possibile sostituire una nozione più generale, detta *autospazio generalizzato*, che permettono di decomporre V in somma diretta anche quando $T \in \text{End}(V)$ non è diagonalizzabile. Gli autospazi generalizzati di un endomorfismo T sono T -invarianti, e la matrice corrispondente risulta decomposta in una forma diagonale a blocchi nella quale ogni blocco è somma di una matrice nilpotente e di un multiplo dell'identità. Questa decomposizione è detta di Dunford (ad esempio, negli appunti di Manetti) ma anche *decomposizione di Jordan astratta*. La forma canonica di Jordan ne segue da uno studio più attento della struttura dell'addendo nilpotente.

4.1. Somme dirette di sottospazi vettoriali. Sia V uno spazio vettoriale, $U_1, \dots, U_n \subset V$ sottospazi vettoriali. Si dice che la somma dei sottospazi $U_i, i = 1, \dots, n$ è diretta se:

$$(4.1) \quad \text{ogni volta che } \mathbf{u}_1 + \dots + \mathbf{u}_n = 0 \text{ con } \mathbf{u}_i \in U_i \text{ per } i = 1, \dots, n, \text{ si ha } \mathbf{u}_1 = \dots = \mathbf{u}_n = 0.$$

Se inoltre $U_1 + \dots + U_n = V$, allora si dice che V è somma diretta dei sottospazi $U_i, i = 1, \dots, n$, e si scrive $V = U_1 \oplus \dots \oplus U_n$.

Proposizione 4.1. Se V è somma diretta interna dei suoi sottospazi U_1, \dots, U_n , allora ogni elemento $\mathbf{v} \in V$ si esprime in modo unico come somma $\mathbf{v} = \mathbf{u}_1 + \dots + \mathbf{u}_n$ con $\mathbf{u}_i \in U_i$. In particolare l'applicazione $\phi : U_1 \times \dots \times U_n \rightarrow V$ definita da $(\mathbf{u}_1, \dots, \mathbf{u}_n) \mapsto \mathbf{u}_1 + \dots + \mathbf{u}_n$ è un isomorfismo di spazi vettoriali.

Dimostrazione. La possibilità di decomporre \mathbf{v} in somma di elementi contenuti nei sottospazi U_i segue da $U_1 + \dots + U_n = V$. L'unicità segue facilmente da (4.1). L'esistenza e l'unicità della decomposizione garantiscono la suriettività e l'iniettività dell'applicazione ϕ , la cui linearità è chiara per definizione. \square

In seguito, avremo bisogno di un criterio di decomposizione diretta.

Lemma 4.2. Siano U_1, \dots, U_n sottospazi di V . Allora da due qualsiasi delle seguenti affermazioni:

- $U_1 + \dots + U_n = V$;
- $\dim U_1 + \dots + \dim U_i = \dim V$;
- ogni volta che $\mathbf{u}_1 + \dots + \mathbf{u}_n = 0$ con $\mathbf{u}_i \in U_i$ per $i = 1, \dots, n$, si ha $\mathbf{u}_1 = \dots = \mathbf{u}_n = 0$;

segue la terza. In particolare, V è somma diretta degli U_i non appena due qualsiasi delle affermazioni precedenti siano soddisfatte.

Dimostrazione. La prima e la terza proprietà costituiscono la definizione di somma diretta. In tal caso V è isomorfo al prodotto cartesiano degli U_i , e quindi $\dim V = \dim U_1 + \dots + \dim U_n$.

Supponiamo ora vere la prima e la seconda affermazione. Se \mathfrak{B}_i è una base di U_i , l'unione $\mathfrak{B} = \mathfrak{B}_1 \cup \dots \cup \mathfrak{B}_n$ è un insieme di generatori di V di cardinalità $\dim V$ ed è pertanto una base. Se $\mathbf{u}_1 + \dots + \mathbf{u}_n = 0$ con $\mathbf{u}_i \in U_i$, esprimiamo ciascun \mathbf{u}_i come combinazione lineare della base \mathfrak{B}_i : l'espressione ottenuta è una combinazione lineare degli elementi di \mathfrak{B} , che costituiscono una base. Tutti i coefficienti sono pertanto nulli, e così anche gli elementi \mathbf{u}_i .

Per concludere, supponiamo che siano valide le ultime due affermazioni. Fissiamo nuovamente una base \mathfrak{B}_i in ogni sottospazio U_i . La terza affermazione garantisce l'indipendenza lineare degli elementi dell'unione \mathfrak{B} , la cui cardinalità è $\dim V$. \mathfrak{B} è pertanto una base, ed i sottospazi U_i generano V . \square

⁶Hahaha!!

4.2. Autospazi e molteplicità geometrica. Sia V uno spazio vettoriale, T un endomorfismo di V . L'autospazio di T relativo all'autovalore $\lambda \in \mathbb{C}$ è l'insieme

$$V_\lambda = \{\mathbf{u} \in V \mid T(\mathbf{u}) = \lambda \mathbf{u}\}.$$

V_λ è il nucleo dell'endomorfismo $\lambda \text{id} - T$, ed è pertanto un sottospazio vettoriale di V .

Gli elementi non nulli di V_λ sono detti autovettori di T relativi all'autovalore λ , o più semplicemente λ -autovettori di T . $\lambda \in \mathbb{C}$ è autovalore di T quando $V_\lambda \neq 0$. Questo accade esattamente quando $\det(\lambda \text{id} - T) = 0$, cioè quando λ è radice del polinomio caratteristico.

Lemma 4.3. Siano $\lambda_i, i = 1, \dots, n$, numeri complessi distinti. Se $\mathbf{u}_i \in V_{\lambda_i}$ sono elementi tali che $\mathbf{u}_1 + \dots + \mathbf{u}_n = 0$, allora necessariamente $\mathbf{u}_1 = \dots = \mathbf{u}_n = 0$. In altre parole, la somma di autospazi distinti è sempre diretta.

Dimostrazione. Per induzione su n , il caso $n = 1$ essendo ovvio. Se $\mathbf{u}_1 + \dots + \mathbf{u}_n = 0$, applicando $\lambda_n \text{id} - T$ ad entrambi i membri si ottiene $(\lambda_n - \lambda_1)\mathbf{u}_1 + \dots + (\lambda_n - \lambda_{n-1})\mathbf{u}_{n-1} = 0$, e i $\lambda_n - \lambda_i$ sono tutti non nulli per $i = 1, \dots, n-1$. Per l'ipotesi induttiva, si ha allora $\mathbf{u}_1 = \dots = \mathbf{u}_{n-1} = 0$, da cui anche $\mathbf{u}_n = 0$. \square

Teorema 4.4. Sono affermazioni equivalenti:

- (1) T è diagonalizzabile;
- (2) la molteplicità algebrica di ogni radice λ del polinomio caratteristico di T è uguale a $\dim V_\lambda$;
- (3) V è somma diretta degli autospazi di T ;

Dimostrazione. (1) \Rightarrow (2). Se T è diagonalizzabile, sia M la matrice di T in una base \mathfrak{B} diagonalizzante. Le radici del polinomio caratteristico sono tutti e soli gli elementi sulla diagonale di M , e la molteplicità algebrica di ciascun autovalore è il numero di volte che compare sulla diagonale. Ad ogni λ sulla diagonale corrisponde un elemento di \mathfrak{B} appartenente all'autospazio V_λ , pertanto la molteplicità algebrica di λ è minore o uguale a $\dim V_\lambda$. La somma delle molteplicità algebriche degli autovalori è uguale a $\dim V$; d'altro canto, $\dim(V_{\lambda_1} + \dots + V_{\lambda_n}) = \dim V_{\lambda_1} + \dots + \dim V_{\lambda_n} \leq \dim V$. In conclusione

$$\dim V = \sum_{i=1}^n \text{molt.alg.}(\lambda_i) \leq \dim V_{\lambda_1} + \dots + \dim V_{\lambda_n} = \dim(V_{\lambda_1} + \dots + V_{\lambda_n}) \leq \dim V,$$

il che mostra che tutti i \leq sono in realtà uguaglianze, e quindi che la molteplicità algebrica di ogni autovalore è uguale alla dimensione dell'autospazio corrispondente.

(2) \Rightarrow (3). La somma degli autospazi è sempre diretta. Se la dimensione di ciascun autospazio è uguale alla molteplicità dell'autovalore corrispondente, allora la somma delle dimensioni degli autospazi è uguale a $\dim V$. Pertanto V è somma diretta degli autospazi di T .

(3) \Rightarrow (1). Sia $\lambda_1, \dots, \lambda_h$ una lista completa di autovalori distinti di T . Se \mathfrak{B}_i è una base di V_{λ_i} , allora $\mathfrak{B} = \mathfrak{B}_1 \cup \dots \cup \mathfrak{B}_h$ è una base di V costituita da autovettori di T . Pertanto \mathfrak{B} diagonalizza T . \square

4.3. Autospazi generalizzati e molteplicità algebrica. Sia V uno spazio vettoriale di dimensione finita, e T un endomorfismo di V . Se $\lambda \in \mathbb{C}$, l'autospazio generalizzato di T relativo a λ è l'insieme

$$E_\lambda = \{u \in V \mid (T - \lambda \text{id})^N(u) = 0 \text{ per } N \text{ sufficientemente grande}\}.$$

L'autospazio generalizzato E_λ contiene sempre l'autospazio V_λ ma può essere più grande. L'importanza degli autospazi generalizzati risiede nei lemmi che seguono:

Lemma 4.5. Gli autospazi generalizzati di $T \in \text{End}(V)$ sono sottospazi vettoriali T -invarianti di V .

Dimostrazione. Se $(T - \lambda \text{id})^N \mathbf{u} = 0$, allora lo stesso è vero di ogni multiplo di \mathbf{u} . Allo stesso modo, se $(T - \lambda \text{id})^N \mathbf{u} = (T - \lambda \text{id})^{N'} \mathbf{u}' = 0$, allora $(T - \lambda \text{id})^{\max(N, N')}(\mathbf{u} + \mathbf{u}') = 0$. Questo dimostra che E_λ è un sottospazio vettoriale di V .

Per quanto riguarda la T -invarianza di E_λ , si osservi che $(T - \lambda \text{id})(E_\lambda) \subset E_\lambda$. Ma allora $T = \lambda \text{id} + (T - \lambda \text{id})$, quindi se $\mathbf{u} \in E_\lambda$, allora $T(\mathbf{u}) = \lambda \mathbf{u} + (T - \lambda \text{id})(\mathbf{u}) \in E_\lambda$. \square

Lemma 4.6. La dimensione dell'autospazio generalizzato di T relativo a λ è sempre uguale alla molteplicità algebrica di λ come radice del polinomio caratteristico di T .

Dimostrazione. Completiamo una base \mathfrak{B}' di E_λ ad una base \mathfrak{B} di V . Il polinomio caratteristico di T è il prodotto dei polinomi caratteristici di $T|_{E_\lambda}$ e dell'endomorfismo indotto da T su V/E_λ . Comunque, il polinomio caratteristico di $T|_{E_\lambda}$ è $(x - \lambda)^{\dim E_\lambda}$, quindi $\dim E_\lambda$ è minore o uguale alla molteplicità algebrica di λ . Se la disuguaglianza è stretta, allora esiste un elemento non nullo $[\mathbf{u}] \in V/E_\lambda$ che è un λ -autovettore di T . In altre parole $[(T - \lambda \text{id})(\mathbf{u})] = [0]$, cioè $(T - \lambda \text{id})(\mathbf{u}) \in E_\lambda$, e quindi $(T - \lambda \text{id})^{N+1}(\mathbf{u}) = 0$, da cui $\mathbf{u} \in E_\lambda \Rightarrow [\mathbf{u}] = 0$, un assurdo. \square

4.4. Decomposizione di Jordan.

Lemma 4.7. *Siano λ, μ numeri complessi distinti. La restrizione di $(T - \mu \text{id})$ sull'autospazio generalizzato di T relativo a λ è invertibile.*

Dimostrazione. L'endomorfismo $T - \lambda \text{id}$ agisce nilpotentemente su E_λ . Inoltre possiamo decomporre $T - \mu \text{id} = (\lambda - \mu) \text{id} + (T - \lambda \text{id})$ come somma di un multiplo non nullo dell'identità e di un endomorfismo nilpotente, ed è quindi invertibile. \square

Lemma 4.8. *La somma di autospazi generalizzati è sempre diretta. Esplicitamente, se $\lambda_1, \dots, \lambda_h$ sono numeri complessi distinti, e $\mathbf{u}_1 \in V^{\lambda_1}, \dots, \mathbf{u}_h \in V^{\lambda_h}$ sono elementi tali che $\mathbf{u}_1 + \dots + \mathbf{u}_h = 0$, allora $\mathbf{u}_1 = \dots = \mathbf{u}_h = 0$.*

Dimostrazione. Per induzione su h , la base $h = 1$ dell'induzione essendo ovvia. Sia $h > 1$, e supponiamo che $\mathbf{u}_1 + \dots + \mathbf{u}_h = 0$. Applicando $(T - \lambda_h \text{id})^N$ per N sufficientemente grande, si ottiene

$$(T - \lambda_h \text{id})^N \mathbf{u}_1 + \dots + (T - \lambda_h \text{id})^N \mathbf{u}_{h-1} = 0.$$

Dall'ipotesi induttiva si ottiene che $(T - \lambda_h \text{id})^N \mathbf{u}_i = 0$ per $i = 1, \dots, h - 1$. Comunque, l'azione di $(T - \lambda_h \text{id})$ su V^{λ_i} è invertibile, quindi $\mathbf{u}_i = 0$ per $i = 1, \dots, h - 1$. Ma allora anche $\mathbf{u}_h = 0$. \square

Teorema 4.9. *Sia V uno spazio vettoriale di dimensione finita, T un suo endomorfismo. Allora V è somma diretta (interna) degli autospazi generalizzati rispetto a T . In particolare, è possibile trovare una base di V rispetto alla quale la matrice associata a T è diagonale a blocchi, e ciascun blocco è della forma $N + \lambda \text{id}$ con N nilpotente – o equivalentemente è triangolare superiore con solo λ sulla diagonale principale.*

Questi risultati illustrano con chiarezza il criterio di diagonalizzabilità dimostrato precedentemente: sussiste sempre l'inclusione $V_\lambda \subset E_\lambda$ di ciascun autospazio nel corrispondente autospazio generalizzato. Lo spazio vettoriale V si decompone sempre nella somma diretta degli autospazi generalizzati di T ; si decompone allora nella somma diretta degli autospazi di T se e soltanto se ognuna delle precedenti inclusioni è un'uguaglianza. Dal momento che $\dim V_\lambda$ e $\dim E_\lambda$ sono rispettivamente le molteplicità geometrica ed algebrica di λ , questo accade soltanto quando coincidono.

Il risultato che segue è noto come decomposizione di Dunford o decomposizione di Jordan astratta.

Corollario 4.10. *Sia V uno spazio vettoriale di dimensione finita, T un suo endomorfismo. Allora è possibile trovare un endomorfismo D diagonalizzabile ed uno N nilpotente tali che $DN = ND$ e $T = D + N$.*

Dimostrazione. Una volta fissata una base di V in cui la matrice M di T sia diagonale a blocchi con blocchi triangolari superiori con autovalori tutti uguali, è sufficiente scegliere D in modo che la sua matrice sia la parte diagonale di M , ed $N = T - D$. Allora D è chiaramente diagonalizzabile; la matrice di N è triangolare superiore stretta ed N è pertanto nilpotente; inoltre D ed N commutano dal momento che, blocco per blocco, D è rappresentato da multipli dell'identità. \square

Si può mostrare che D ed N possono essere ottenuti da espressioni polinomiali in T .

Corollario 4.11. *Sia V uno spazio vettoriale di dimensione finita, T un suo endomorfismo. Allora T è diagonalizzabile se e solo se il polinomio minimo di T non ha radici multiple.*

Dimostrazione. Sappiamo già che se T è diagonalizzabile, il suo polinomio minimo non ha radici multiple. Supponiamo viceversa che il polinomio minimo di T non abbia radici multiple. La decomposizione in somma diretta di autospazi generalizzati che abbiamo appena mostrato permette di associare a T una matrice diagonale a blocchi in cui ogni blocco è triangolare superiore con un autovalore λ di T sulla diagonale. Il polinomio minimo $p(x)$ di tale blocco è della forma $(x - \lambda)^n$ e divide il polinomio minimo di T che non ha radici multiple. Pertanto $p(x) = x - \lambda$ e il blocco è diagonale. Ma se ogni blocco di una matrice diagonale a blocchi è diagonale, la matrice è complessivamente diagonale. \square

Esercizi del § 4.

- Se V è uno spazio vettoriale di dimensione finita, e $T \in \text{End}(V)$ è tale che per ogni $\mathbf{u} \in V$ esista $N \in \mathbb{N}$ con la proprietà che $(T - \lambda \text{id})^N(\mathbf{u}) = 0$, allora un'opportuna potenza di $T - \lambda \text{id}$ si annulla: in altre parole, $T - \lambda \text{id}$ è un endomorfismo nilpotente.
- Mostrare con un esempio che è possibile trovare uno spazio vettoriale (di dimensione infinita) V e un endomorfismo T tali che per ogni $\mathbf{u} \in V$ esista $N \in \mathbb{N}$ tale che $T^N(\mathbf{u}) = 0$ ma nessuna potenza di T sia l'endomorfismo nullo. In altre parole, T è localmente nilpotente, ma non è nilpotente.
- Un endomorfismo P si dice proiettore se $P^2 = P$. Mostrare che ogni proiettore di uno spazio vettoriale di dimensione finita è diagonalizzabile, e può avere solo 0 ed 1 come autovalori.
- Anche nel caso in cui V abbia dimensione infinita, gli autospazi di un proiettore $P \in \text{End}(V)$ decompongono V in somma diretta.

- e) Se $T \in \text{End}(V)$ soddisfa $T^n = \text{id}$, allora T è diagonalizzabile.
 f) Mostrare che se un endomorfismo $T \in \text{End}(V)$ soddisfa un polinomio non nullo, allora V si decompone in somma diretta degli autospazi generalizzati di T anche quando V non ha dimensione finita. [Sugg.: mostrare che ogni elemento $v \in V$ è contenuto in un sottospazio T -invariante di dimensione finita.]

5. FORMA CANONICA DI JORDAN

L'enunciato preciso che dimostreremo è il seguente:

Teorema 5.1. Ogni endomorfismo di uno spazio vettoriale di dimensione finita ammette una base nella quale la matrice corrispondente è diagonale a blocchi, con blocchi quadrati con λ sulla diagonale principale ed 1 sulla sopradiagonale, cioè della forma

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & & 0 & \lambda & 1 & 0 \\ 0 & & & 0 & \lambda & 1 \\ 0 & \dots & & \dots & 0 & \lambda \end{pmatrix}$$

5.1. Forma di Jordan per endomorfismi nilpotenti. Se l'endomorfismo T è nilpotente, allora i blocchi del teorema precedente hanno tutti $\lambda = 0$.

Definizione 5.2. Sia T un endomorfismo nilpotente di uno spazio vettoriale di dimensione finita V . Un insieme di generatori di Jordan per T è un insieme finito $\mathbf{v}^1, \dots, \mathbf{v}^n$ di elementi di V con la proprietà che gli elementi **NON NULLI** della forma $T^k \mathbf{v}^j$, dove $k \in \mathbb{N}$, $1 \leq j \leq n$, siano una base di V .

Lemma 5.3. Sia V uno spazio vettoriale, $U \subset V$ un sottospazio vettoriale. Se $[\mathbf{v}_1], \dots, [\mathbf{v}_n]$ sono elementi linearmente indipendenti di V/U , allora $\mathbf{v}_1, \dots, \mathbf{v}_n$ sono linearmente indipendenti in V .

Dimostrazione. Supponiamo che $a_1 \mathbf{v}_1 + \dots + a_n \mathbf{v}_n = 0$. Allora

$$[0] = [a_1 \mathbf{v}_1 + \dots + a_n \mathbf{v}_n] = a_1 [\mathbf{v}_1] + \dots + a_n [\mathbf{v}_n],$$

e quindi $a_1 = \dots = a_n = 0$ per lineare indipendenza di $[\mathbf{v}_1], \dots, [\mathbf{v}_n]$. \square

Lemma 5.4. Sia V uno spazio vettoriale, $T \in \text{End}(V)$. Se $[\mathbf{v}_1], \dots, [\mathbf{v}_n]$ sono elementi linearmente indipendenti di $V/\ker T$, allora $T(\mathbf{v}_1), \dots, T(\mathbf{v}_n)$ sono elementi linearmente indipendenti di V .

Dimostrazione. Se $a_1 T(\mathbf{v}_1) + \dots + a_n T(\mathbf{v}_n) = 0$, allora $T(a_1 \mathbf{v}_1 + \dots + a_n \mathbf{v}_n) = 0$ e quindi $a_1 \mathbf{v}_1 + \dots + a_n \mathbf{v}_n \in \ker T$. Pertanto

$$[0] = [a_1 \mathbf{v}_1 + \dots + a_n \mathbf{v}_n] = a_1 [\mathbf{v}_1] + \dots + a_n [\mathbf{v}_n] = 0,$$

e quindi $a_1 = \dots = a_n = 0$ per lineare indipendenza di $[\mathbf{v}_1], \dots, [\mathbf{v}_n]$. \square

Proposizione 5.5. Sia V uno spazio vettoriale di dimensione finita, $T \in \text{End}(V)$ nilpotente. Allora esiste un insieme di generatori di Jordan per T .

Dimostrazione. Per induzione sulla dimensione di V . Se $\dim V = 1$, allora $T = 0$ e ogni vettore non nullo è un insieme di generatori di Jordan per T .

Supponiamo allora che $\dim V > 1$. Poiché T è nilpotente, $\ker T \subset V$ è un sottospazio vettoriale non nullo. Se $\ker T = V$, allora $T = 0$ e ogni base di V è un insieme di generatori di Jordan per T . Se invece $\ker T \subsetneq V$, allora $\dim V/\ker T < \dim V$ e possiamo usare l'ipotesi induttiva sull'endomorfismo $\tilde{T} \in \text{End}(V/\ker T)$. Pertanto, esiste un insieme di generatori di Jordan

$$[\mathbf{v}^1], [\mathbf{v}^2], \dots, [\mathbf{v}^n]$$

per \tilde{T} . Innanzitutto, è importante osservare che $\tilde{T}^k[\mathbf{v}^i] = [T^k(\mathbf{v}^i)]$ per ogni scelta di $\mathbf{v} \in V$ e $k \in \mathbb{N}$.

Poniamo

$$k_i = \max\{k \in \mathbb{N} \mid \tilde{T}^k([\mathbf{v}^i]) \neq 0\}.$$

Gli elementi $\tilde{T}^{k_i}([\mathbf{v}^i])$, $1 \leq i \leq n$, sono linearmente indipendenti e lo sono quindi anche gli elementi $T^{k_i+1}(\mathbf{v}^i)$, $1 \leq i \leq n$, che devono appartenere tutti a $\ker T$, in quanto $\tilde{T}^{k_i+1}([\mathbf{v}^i]) = [0]$. Possiamo allora completarli ad una base di $\ker T$ aggiungendo degli elementi $\mathbf{v}^{n+1}, \dots, \mathbf{v}^r$.

Gli elementi $\mathbf{v}^1, \dots, \mathbf{v}^r$ sono allora un insieme di generatori di Jordan per T : gli elementi $T^k \mathbf{v}^j$, $1 \leq j \leq n$, $0 \leq k \leq k_j$ sono linearmente indipendenti poiché lo sono gli elementi

$$[T^k \mathbf{v}^j] = \tilde{T}^k[\mathbf{v}^j], 1 \leq j \leq n, 0 \leq k \leq k_j.$$

Il fatto che questi ultimi elementi siano una base di $V/\ker T$ ci dice inoltre che gli elementi $T^k \mathbf{v}^j$, $1 \leq j \leq n$, $0 \leq k \leq k_j$, sono una base di V modulo $\ker T$. Se aggiungiamo, a questi, gli elementi di una

qualsiasi base di $\ker T$ formeranno insieme necessariamente una base di V . Ma gli elementi $T^{k_j+1}\mathbf{v}^j$, $1 \leq j \leq n$, assieme agli elementi $\mathbf{v}^{n+1}, \dots, \mathbf{v}^r$ costituiscono appunto una base di $\ker T$, e ogni loro immagine attraverso T è nulla. \square

Il prossimo enunciato segue come corollario immediato.

Teorema 5.6. *Se $T \in \text{End}(V)$ è nilpotente, allora esiste una base*

$$(\mathbf{v}_0^1, \mathbf{v}_1^1, \dots, \mathbf{v}_{\ell_1}^1, \mathbf{v}_0^2, \dots, \mathbf{v}_{\ell_2}^2, \dots, \mathbf{v}_0^h, \dots, \mathbf{v}_{\ell_h}^h)$$

di V con la proprietà che $T(\mathbf{v}_n^i) = \mathbf{v}_{n+1}^i$ per $0 \leq n < \ell_i$, e $T(\mathbf{v}_{\ell_i}^i) = 0$.

Dimostrazione. Se $\mathbf{v}^1, \dots, \mathbf{v}^h$ è un insieme di generatori di Jordan per T , allora ponendo $\mathbf{v}_j^i = T^j(\mathbf{v}^i)$ si ottiene la base cercata. \square

L'importanza dell'enunciato appena dimostrato risiede nel fatto che il sottospazio V^i generato dai vettori \mathbf{v}_j^i , $0 \leq j \leq \ell_i$ è T -invariante, e la matrice associata alla sua base $(\mathbf{v}_{\ell_i}^i, \mathbf{v}_{\ell_i-1}^i, \dots, \mathbf{v}_1^i, \mathbf{v}_0^i)$ è un blocco di Jordan, di autovalore zero, $(\ell_i+1) \times (\ell_i+1)$. Per questi motivi, il Teorema 5.1 è valido per ogni endomorfismo nilpotente. Tuttavia, la decomposizione di uno spazio vettoriale di dimensione finita nella somma diretta di autospazi generalizzati rispetto ad un proprio endomorfismo permette di dimostrarlo nel caso generale, come segue:

Dimostrazione del Teorema 5.1. V è somma diretta degli autospazi generalizzati E_λ rispetto all'endomorfismo T , quindi T è già diagonale a blocchi, con un blocco per ogni autospazio generalizzato E_λ . L'enunciato è quindi dimostrato se lo dimostriamo per la restrizione di T ad ogni suo autospazio generalizzato. In altre parole possiamo supporre, senza perdita di generalità, che T possieda un solo autovalore λ .

Ma in tal caso $N = T - \lambda \text{id}$ è nilpotente, e possiamo applicare la Proposizione 5.2 all'endomorfismo N . Possiamo quindi trovare una base B nella quale la matrice di N sia in forma canonica di Jordan con zeri sulla diagonale. Ma allora

$${}_B[T]_{\mathfrak{B}} = {}_B[N + \lambda \text{id}]_{\mathfrak{B}} = {}_B[N]_{\mathfrak{B}} + \lambda {}_B[\text{id}]_{\mathfrak{B}} = {}_B[N]_{\mathfrak{B}} + \lambda \text{id},$$

e quindi nella stessa base la matrice di T è in forma canonica di Jordan con λ sulla diagonale. \square

Riassumo l'idea generale della dimostrazione che abbiamo appena dato: la decomposizione di V in somma diretta degli autospazi generalizzati di un endomorfismo T ci permette di trovare una base nella quale la matrice associata a T sia già diagonale a blocchi, con ciascun blocco che possiede un solo autovalore. Ciascuno di tali blocchi può essere ridotto a forma canonica di Jordan applicando la Proposizione 5.2 all'endomorfismo nilpotente che si ottiene sottraendo a (lla restrizione di) T un multiplo opportuno dell'identità.

5.2. Caratterizzazione delle classi di similitudine. *Non è ancora chiaro per quale motivo la forma canonica di Jordan debba essere utile. La sua proprietà essenziale è l'unicità: il numero ed il tipo (che è dato dall'autovalore e dalla dimensione) dei blocchi in una qualsiasi riduzione di T a forma canonica di Jordan è univocamente determinato. Questo si può vedere facilmente: se λ è un autovalore di T , i numeri $d_\lambda^i = \dim \ker(\lambda \text{id} - T)^i$ crescono col crescere di n , fino a stabilizzarsi sulla molteplicità algebrica di λ . In particolare, si osservi che $d_\lambda^0 = 0$, mentre d_λ^1 è la molteplicità geometrica di λ , e d_λ^n è la sua molteplicità algebrica quando n è la dimensione del più grande blocco di Jordan di autovalore λ . Per calcolare il numero ed il tipo dei vari blocchi di Jordan di autovalore λ è sufficiente calcolare le dimensioni di λ su una riduzione di T a forma canonica di Jordan. Con questa strategia si ottiene il seguente preciso risultato:*

Lemma 5.7. *La differenza $d_\lambda^{n+1} - d_\lambda^n$ coincide con il numero di blocchi di Jordan di autovalore λ di dimensione maggiore di n .*

Dimostrazione. È sufficiente mostrare che, su ciascun blocco di Jordan, la differenza $d_\lambda^{n+1} - d_\lambda^n$ vale zero per i blocchi fino ad $n \times n$, mentre vale 1 per quelli più grandi. \square

È a questo punto del tutto evidente come la conoscenza dei numeri di λ permetta di calcolare il numero ed il tipo dei vari blocchi di Jordan di autovalore λ , e di dimostrare come conseguenza l'unicità della forma canonica di Jordan. Ad esempio l'ultima differenza prima che le dimensioni di λ si stabilizzino sarà uguale al numero di blocchi di dimensione massima (chiamiamola n). Allo stesso modo la differenza precedente sarà la somma del numero di blocchi di dimensione n (che conosciamo) e del numero di blocchi di dimensione $n-1$ (che possiamo quindi determinare). Continuando, otterremo il numero di blocchi di Jordan di autovalore λ e dimensione k per ogni k . Questo procedimento va ovviamente ripetuto per ogni autovalore.

Corollario 5.8. *Due matrici $A, B \in \text{Mat}_{n \times n}(\mathbb{C})$ sono simili se e solo se L_A, L_B possiedono la stessa forma canonica di Jordan.*

Dimostrazione. Se L_A, L_B hanno la stessa forma canonica di Jordan, allora A, B sono simili alla stessa matrice, e sono quindi simili tra loro per transitività della relazione di similitudine. D'altro canto, matrici simili hanno lo stesso rango, e quindi i numeri $d_\lambda^i = \dim \ker(\lambda \text{id} - T)^i$ che si ricavano ponendo $T = L_A, L_B$ sono gli stessi (perché?). Ma allora L_A e L_B possiedono la stessa forma canonica di Jordan. \square

Ai matematici piace pronunciare frasi come quella che segue: un insieme completo di invarianti delle matrici $n \times n$ rispetto alla relazione di similitudine è dato dall'insieme di autovalori della matrice, insieme ai numeri $d_\lambda^i = \dim \ker(\lambda \text{id} - T)^i$, dove λ è un autovalore, e $0 \leq i \leq n$. Questo dovrebbe più o meno dire che due matrici sono simili se e solo se queste informazioni (gli autovalori e le dimensioni) coincidono per le due matrici. Dal momento che queste informazioni sono facilmente calcolabili — e dovrete sapere come — questo fornisce un metodo efficace per determinare se due matrici siano simili.