Appunti di Matematica Discreta

Matteo Scarpa

Appunti del corso di Matematica Discreta fatto da Matteo Scarpa a titolo gratuito dagli appunti presi in classe per cui soggetti ad *errori e orrori*. E' stato scelto il formato pdf perchè universale. In caso di errori segnalarli a *mscarpa@dsi.uvine.it* o mandarmi un mp.

Indice

1 **5**

1.1 Teoria degli Insiemi . . . 5
1.1.1 Proprietà dell'assorbimento . . . 6
1.2 Insiemi dei Numeri . . . 6
1.2.1 Definire un insieme numerico . . . 6
1.2.2 Numeri Naturali: $\mathbb{N}$ . . . 6
1.3 Logica o Linguaggio Matematico . . . 8
1.3.1 Simbologia . . . 8
1.3.2 Risoluzione . . . 8
1.4 Relazioni . . . 8
1.4.1 Relazione di equivalenza . . . 9
1.5 Principio di Induzione . . . 9
1.6 Aritmetica Modulare . . . 9
1.6.1 Proprietà e Teoremi . . . 10
1.7 Combinatoria . . . 10
1.7.1 Principi . . . 10
1.7.2 Ordine e Ripetizione: i vari casi . . . 11

2 **13**

2.1 Spazi vettoriali . . . 13
2.1.1 Definizioni degli spazi vettoriali . . . 13
2.2 Sistemi di equazioni lineari . . . 14
2.2.1 Risoluzioni dei sistemi di equazioni lineari . . . 14
2.3 Matrici . . . 15
2.3.1 Operazioni con le matrici . . . 15
2.3.2 Prodotto di una matrice per uno scalare . . . 16
2.3.3 Proprietà dei determinanti . . . 17
2.3.4 Proprietà della caratteristica . . . 18
2.3.5 Altre definizioni legate alle matrici . . . 18
2.3.6 Matrici elementari e operazioni elementari . . . 18
2.4 Inverse e Gauss . . . 19
2.4.1 Calcolare l'inversa . . . 19
2.4.2 Metodo di elminazione di Gauss . . . 19
2.5 Spazio Vettoriale . . . 19
2.5.1 Definizioni e osservazioni legate allo spazio vettoriale . . . 20
2.5.2 Cambiare tra due basi . . . 22
2.6 Applicazioni spazi vettoriali . . . 24
2.6.1 Proprietà della allicazioni lineari . . . 25

2.6.2 Matrice associata ad una applicazione lineare 25
2.6.3 Endomorfismi 25
2.7 Esercizi svolti 31

Modulo 1

1.1 Teoria degli Insiemi

Definizione 1 (Insieme)**.** *Collezione di elelmenti finiti o infiniti*

Esempio di insieme finito

$$A = \{15; 3; 17\} \tag{1.1}$$

Esempio di insieme infinito

$$B = \{x | x \text{ è un numero pari}\} \tag{1.2}$$

In cui gli elementi appartengono o no a essi

$$2 \in \{x | x \text{ è un numero pari}\} \tag{1.3}$$
$$3 \notin \{x | x \text{ è un numero pari}\} \tag{1.4}$$

Può essere importante l'ordine in certi casi come ad esempio quando si lavora su coppie di dati

$$\{(x, y) | x, t \in \mathbb{N} \wedge x < y\} \tag{1.5}$$

In cui

$$(7; 3) \notin \{(x, y) | x, t \in \mathbb{N} \wedge x < y\} \tag{1.6}$$
$$(3; 7) \in \{(x, y) | x, t \in \mathbb{N} \wedge x < y\} \tag{1.7}$$

Esempio

$$\{x | x \text{ è multiplo di } 12\} \Rightarrow \{x | x \text{ è multiplo di } 3\} \tag{1.8}$$

Dimostrazione Sia x un multiplo di 12 allora $\exists r$ tale che $x = r * 12$

$$x = r * 4 * 3 = (r * 4) * 3 \tag{1.9}$$

quindi x è un multiplo di 3

1.1.1 Proprietà dell'assorbimento

$$A \cup (A \cap B) = A = A \cap (A \cup B) \tag{1.10}$$

1.2 Insiemi dei Numeri

Esistono vari insiemi numerici:

Gli insiemi di numeri_discreti
- $\mathbb{N}_0$ Sono i numeri naturali compreso lo zero $\{0; 1; 2; 3 \ldots\}$
- $\mathbb{N}$ Sono i numeri naturali senza lo zero $\{1; 2; 3; 4 \ldots\}$
- $\mathbb{Z}$ Sono i numeri reali $\{0; 1; 2; 3 \ldots\}$

Gli insiemi dei numeri_continui
- $\mathbb{R}$ Sono i numeri reali $\{\sqrt[2]{2}; -3; \sqrt[3]{45}; 4 \ldots\}$
- $\mathbb{C}$ Sono i numeri complessi $\{i; 3i; 24i \ldots\}$

1.2.1 Definire un insieme numerico

Per definire un insieme numerico ai bisogno di vari elementi. Per esempio cerchiamo di definire l'insieme dei numeri naturali. Si parte da un **Alfabeto** ovvero l'insieme di elementi che permutati permette di costituire tutti gli elementi dell'insieme $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}^*$. Bisogna poi definire delle regole che definiscano l'insieme numerico che vado a definire

> 0 è un numero naturale
> Se n è un numero naturale anche n+1 lo è
> Nient'altro è numero naturale

Quindi poi si definiscono le operazioni possibili.

1.2.2 Numeri Naturali: $\mathbb{N}$

Definizione dell'insieme

Si può definire come $(\mathbb{N}; +; *; 0; 1)$ in cui si ha l'insieme dei numeri, le operazioni e gli elementi neutri delle operazioni.

Proprietà della Somma

La somma in questo insieme gode delle seguenti proprietà[1]

Proprietà Associativa

$$(x + (y + z) = (x + y) + z) \tag{1.11}$$

Commutativa

$$x + y = y + x \tag{1.12}$$

[1] Per ogni proprietà considero $\forall x \quad \forall y \quad \forall z$

Elemento Neutro

$$x + 0 = x = 0 + x \tag{1.13}$$

Cancellazione della Somma

$$x + z = y + z \to x = y \tag{1.14}$$

Proprietà del Prodotto

Il prodotto in questo insieme gode delle seguenti proprietà[2]

Proprietà Associativa

$$(x * (y * z) = (x * y) * z) \tag{1.15}$$

Commutativa

$$x * y = y * x \tag{1.16}$$

Elemento Neutro

$$x * 1 = x = 1 * x \tag{1.17}$$

Anichilisce

$$x * 0 = 0 \tag{1.18}$$

Cancellazione del Prodotto

$$x * z = y * z \to x = y \tag{1.19}$$

Distribuzione del prodotto rispetto alla somma

$$x * (y + z) = (x + y) * (x + z) \tag{1.20}$$

Ordinamento parziale

Prendiamo per esempio la seguente espressione

$$x \leq y \qquad \text{se e solo se } \exists k \quad (y = x + k) \tag{1.21}$$

Se essa risponde alle seguenti tre proprietà è un **Ordinamento Parziale**[3]

Riflessiva

$$x \leq x \tag{1.22}$$

Transitiva

$$x \leq y \land y \leq z \to x \leq z \tag{1.23}$$

Antisimmetrica

$$x \leq y \land y \leq x \to x = y \tag{1.24}$$

Per cui l'espressione (1.21) NON solo è un ordinamento parziale ma vale anche la **Legge di Tricotomia**

$$\forall xy(x \leq y) \lor (y \leq x) \tag{1.25}$$

Teorema 1 (Elemento Minimo)**.** *Ogni insieme non vuoto di naturali ha un minimo elemento*

[2] Anche qui considero per ogni proprietà $\forall x \quad \forall y \quad \forall z$

[3] Sempre per $\forall x \quad \forall y \quad \forall z$

1.3 Logica o Linguaggio Matematico

La logica è il linguaggio con cui la matematica descrive il mondo e se stessa.
Esempio: Ogni numero naturale è primo si scriverà

$$\forall x \in \mathbb{N} \quad (x \in \text{Numeri Primi}) \tag{1.26}$$
$$\text{in cui} \tag{1.27}$$
$$x \in \text{Numeri Primi} \equiv (x \neq 0) \wedge (x \neq 1) \wedge (x \text{ è divisibile per 1 e } x) \wedge x|y \equiv (y = x * k) \tag{1.28}$$

In questo esempio è specificato il fatto che l'universo del discorso sono i numeri primi.

1.3.1 Simbologia

La logica usa sostanzialmente 2 simboli:

and $\wedge$ che unisce 2 enunciati $A \wedge B$
or $\vee$ unisce due enunciati $A \vee B$
non $\neg$ nega l'elemento che segue $\neg A$

E il loro valore di verità è

$A \wedge B$ è vero se e solo se A e B sono entrambi veri
$A \vee B$ è falso se e solo se A e B sono entrambi falsi
$\neg A$ è vero se e solo se A è falso

Teorema 2 (De Morgan)**.**

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B \tag{1.29a}$$
$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B \tag{1.29b}$$

1.3.2 Risoluzione

Per dimostrare la verità non basta un esempio, bisogna usare le proprietà
per dimostrare che vale sempre

Questa frase spiega in modo generale come bisogna comportarsi per dimostrare la verità di una affermazione. In particolare abbiamo che bisogna fare:

$A \wedge B$ Provo prima A e poi provo B
$A \rightarrow B$ A lo do per vero quindi dimostro B
$\forall x \quad f(x) \rightarrow \quad g(x)$ Basta controllare B: se vero è vera altrimenti è falsa

1.4 Relazioni

Metodo per collegare più elelmenti di uno stesso insieme che abbiano tutti la stessa caratteristica/e: prendendo l'insieme degli alunni in un aula gli elementi x e y sono in relazione sse hanno la stessa età. In questo caso avere la stessa età è una relazione.

1.4.1 Relazione di equivalenza

Una relazione R è di equivalenza se verifica le proprietà riflessiva, simmetrica e transitiva

Riflessiva

$$xRx \tag{1.30}$$

Transitiva

$$xRy \land yRz \to xRz \tag{1.31}$$

Simmetrica

$$xRy \land yRx \to x \neq y \tag{1.32}$$

1.5 Principio di Induzione

Tra i più importanti argomenti del corso e dell'informatica, il principio di induzione ti permette di dimostrare molti teoremi e le funzioni ricorsive.

$$\forall P \quad (P(0) \land \forall x(P(x) \to P(x+1)) \to \forall x P(x)) \tag{1.33}$$

Se si riesce a dimostrare per i 2 casi possibili ovvero per il caso base P(0) e nel caso induttivo $P(x) \to P(x+1)$ è sempre verificato. Per cui bisogna prima verificare P(0) che per il 99% è elementare. È il passo induttivo quello più problematico; personalmente partendo dal caso $P(x+1)$ utilizzo operazioni elementari fino a riportarlo al caso $P(x) + P(1)$ o viceversa.

1.6 Aritmetica Modulare

Viene anche chiamata aritmetica dell'orologio ed è stata inventata da Gauss nel quale i numeri si avvolgono su se stessi. Ad esempio possiamo calcolare il resto delle dvisione in 2 interi

$$r \equiv k \bmod n \tag{1.34}$$

$$\text{se e solo se } n \text{ divide } (r-k)$$

Esempio

$$7 \equiv 2 \bmod 57 - 2 = 55|5 \tag{1.35}$$

$$4 + 4 = 3 \tag{1.36a}$$
$$4 + 3 = 2 \tag{1.36b}$$

I due esempi (1.36) sono in mod4

Inverso

$$\forall x \quad x \text{ ammette un inverso se e solo se x ed n sono coprimi} \tag{1.37}$$

MCD o **M**inimo **C**omun **D**ivisore

$$d = \text{MCD}(x, n) \quad \text{se e solo se} \quad rx + sn = d \tag{1.38}$$

che si risolve

$$n = q_1 * x + r_1 \tag{1.39}$$
$$x = q_2 * r_1 + r_2 \tag{1.40}$$
$$\dots \tag{1.41}$$
$$r_{n-2} = q_n * r_{n-1} + r_n \tag{1.42}$$
$$r_{n_1} = r_n * q + 0 \tag{1.43}$$

In cui il valore di r_n corrisponde al MCD

1.6.1 Proprietà e Teoremi

Tutte le proprietà che valgono per gli interi valgono anche per i resti

Teorema 3 (Fermat)**.** *Se n è numero primo allora $r^{n-1} \equiv 1 \bmod n$ purchè r non sia divisibile per n*

Teorema 4 (Eulero)**.**

$$y^{\phi(x)} \equiv 1 \bmod n \quad \textit{se } y \textit{ è coprimo con } n \tag{1.44}$$

Teorema 5 (Fermat)**.**

$$x^{P-1} \equiv 1 \bmod P \quad \textit{con } P \textit{ numero Primo} \wedge \quad \forall x \textit{ non divisibili per } P \tag{1.45}$$

Teorema 6 (Fermat versione di Gauss)**.**

$$\underset{\mathbb{N}\to\mathbb{N}}{\phi(n)} \qquad \textit{Funzione di Eulero} \tag{1.46}$$

Numero di interi tra 1 e n-1 (compresi) che sono coprmi con n

Teorema 7 (Funzione moltiplicativa)**.** *Data ϕ che è una funzione moltiplicativa allora vale*

$$\phi(k * r) = \phi(k) * \phi(r) \quad k \textit{ ed } r \textit{ sono coprimi} \tag{1.47}$$

1.7 Combinatoria

1.7.1 Principi

Principio Moltiplicativo Risponde alla domanda 'Quante targhe si possono fare con 2 lettere dell'alfabeto inglese seguite da 3 cifre e poi ancora 2 lettere dell'alfabeto inglese?' che corrisponde al prodotto delle cardinalità:

$$|A| = n \qquad |B| = k \qquad n * k \tag{1.48}$$

Principio 1 (Principio additivo)**.**

$$|A| = n \qquad |B| = k \qquad |A \cup B| = n + k \quad \textit{sse} \quad A \cap B = \varnothing \tag{1.49}$$

che di fatto corrisponde a

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{1.50}$$

nel caso $|A \cup B|$ e

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \tag{1.51}$$

nel caso $|A \cup B \cup C|$

1.7.2 Ordine e Ripetizione: i vari casi

Disposizione Semplice

Ovvero ordine senza ripetizione. In un insieme A di cardinalità n è una sequenza di k elementi di A tutti distinti tra loro

$$Dn, k = \frac{n!}{(n-k)!} \tag{1.52}$$

Combinazione Semplice

Ovvero senza ripetizione e senza ordine. In un insieme A di n elementi è uguale al numero di sottoinsiemi di A di cardinalità k

$$Cn, k = \frac{Dn, k}{k!} = \frac{n!}{k!(n-k)!} = \left(\begin{array}{c} n \\ k \end{array} \right) \tag{1.53}$$

Combinazione con ripetizione

Senza ordine e con ripetizione

$$Cn, k = \left(\begin{array}{c} n+k-1 \\ k \end{array} \right) = \frac{(n+k-1)!}{k!(n-1)!} \tag{1.54}$$

Modulo 2

2.1 Spazi vettoriali

Un enupla ordinata di numeri reali $v = (a_i, \ldots, a_n)$ si possono eseguire queste operazioni:

- Prodotto enupla per numero $k * v = (k * a_i, \ldots, k * a_n)$ con $k \in \mathbb{R}$
- Somma enupla con enupla $v + u = (a_1 + b_1, \ldots, a_n + b_n)$ con $v = (a_1 + \ldots, a_n)$ $u = (b_1, \ldots, b_n)$

2.1.1 Definizioni degli spazi vettoriali

Definizione Un gruppo abeliano è un insieme dotato di operazione di somma che gode delle seguenti proprietà

Indichiamo con g l'elemento generico dell'insieme

- $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$
- Esiste un elemento neutro detto 0 tale che $g + 0 = g \quad \forall g \in G$
- Ogni elemento $g \in G$ è dotato di un opposto ovvero un elemento $-g$ tale che $g + (-g) = (-g) + g = 0$

Per definizione godono anche delle proprietà di

- Il numeto neutro è unico
- L'opposto di g è unico

Definizione Uno spazio vettoriale V su $\mathbb{R}$ è un inisieme $\neq \varnothing$ i cui elementi sono detti vettori dotato delle seguenti proprietà

- V è dotato dell'operazione di somma (solitamente indicata con $+$) rispetto alla quale è gruppo abeliano
- V è dotato di una operazione detta moltiplicazione a scalari

Denotiamo con $K^n = \{(a_1, \ldots, a_n) | a \in \mathbb{R}\}$ lo spazio vettoriale su $\mathbb{R}$ rispettto alle operazioni di somma e di prodotto per scalare

Definizione Se V e W sono spazi vettoriali, una applicazione $f : V \to W$ è detta applicazione lineare se

- $f(v + v') = f(v) + f(v') \qquad \forall v, v' \in V$
- $f(k * v) = k * f(v) \qquad \forall k \in \mathbb{R}, v \in V$

Definizione Se $A = (a_{i,j})$ è una matrice quadrata di ordine n, la matrice quadrata ottenuta da A cancellando la i-esima riga e la j-esima colonna è una matrice quadrata di ordine $n - 1$ detta la matrice aggiunta di a_1

2.2 Sistemi di equazioni lineari

Un equazione lineare è un' equazione del tipo $a_1x_1 + \cdots + a_nx_n = b$ ove $a_1, \ldots, a_n, b$ sono numeri e $x_1, \ldots, x_n$ sono incognite. Un sistema di equazioni lineari è un sistema del tipo

Gli elementi $a_{1,1}, \ldots, a_[m, n]$ si definiscono *coefficienti* mentre $b_1, \ldots, b_m$ è la *colonna dei termini noti*

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n = b_2 \\ \ldots \\ a_{m,1}x_1 + \ldots + a_{m,n}x_n = b_m \end{cases} \tag{2.1}$$

Una soluzione del sistema è una enupla $(s_1, \ldots, s_n)$ di numeri tali che sostituiti alle incognite rendono le equazioni delle identità

Definizione Un sistema di equazioni lineare si dice sistema omogeneo se la colonna dei termini noti è fatta di 0. Ovviamente il sistema omogeneo ha sempre una soluzione chiamata soluzione banale che è la soluzione $(0, \ldots, 0)$

Definizione Una matrice scala per righe è una matrice che risponde a tutte queste proprietà

1. Il primo elemento non nullo di ciascuna riga di A è 1. Tale elemento è detto *pivot*
2. Il primo elemento non nullo a sinistra della $i + 1$ esima riga è posto a destra del primo elemento non nullo della riga precedente
3. Gli elementi al di sopra di un pivot sono zero

Osservazione Data una matrice A_i la sua forma a scala per righe A' è unicamente sdefinita anche se la sequenza di operazioni elementari che uso per trasferire A in A' non è unico

2.2.1 Risoluzioni dei sistemi di equazioni lineari

Le soluzioni si ottengono dando un valore arbitrario alle incognite corrispondenti alle colonne in cui non ci sono pivot.

Teorema Sia $M' = (A'|B')$ una matrice scalal per righe. Allora il sistema di equazioni lineare $AX = B$ ammette soluzioni se e solo se la colonna B non contiene pivot. In tal caso può essere associato un valore arbitrario all'incognita X_i se la i-esima colonna non contiene pivot.

Teorema Ogni sistema $AX = 0$ di equazioni lineari omogenee in n incognite con m equazioni con $m > n$ ammette a meno una soluzione non banale.

Teorema Una matrice A quadrata:

- Può essere ridotta alla matrice identica mediante una sequenza di operazioni elementari
- È il prodotto di matrici elementari
- È invertibile
- Il sistema di equazioni lineari omogenee $AX = 0$ ha solo la soluzione banale

2.3 Matrici

Una matrice è una struttura di questo tipo

Matrice con m righe e n colonne è una matrice di tipo o dimensione m,n

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ a_{2,1} & \dots & a_{2,n} \\ \dots & \dots & \dots \\ a_{m,1} & \dots & a_{m,n} \end{bmatrix} \tag{2.2}$$

Una matrice di tipo m, n ha $m * n$ elementi.

Definizione Due matrici sono uguali se sono dello stesso tipo e se $a_{i,j} = b_{i,j}$ $\forall i$ e $\forall j$

$A = (a_{i,j})$ e $B = (b_{i,j})$

2.3.1 Operazioni con le matrici

Somma di due matrici

Date due matrici A e B entrambe di tipo m, n si può definire una matrice somma $A + B$ come

$$\text{Se} \quad A = (a_{i,j}) \quad B = (b_{i,j}) \quad C = (c_{i,j}) = (a_{i,j} + b_{i,j})^1 \tag{2.3}$$

La somma tra matrici ha le seguenti proprietà:

- Matrice Nulla tale che $A + 0 = A \quad \forall A$[2]
- Associativa $(A + B) + c = A + (B + C)$
- Elemento Opposto $\forall A \quad A + (-A) = 0$
- Commutativa $A + B = B + A$

[2]Matrice Nulla=Tutti gli elementi sono 0

Prodotto righe per colonne di matrici

Supponendo di avere $A = (a_{iy})$ di tipo (m, n) e $B = (b_{yk})$ di tipo (n, r) $C = A * B$ viene definito nel modo seguente[3]

$$C_{ij} = \sum_{s=1}^{n} a_{is} * b_{sj} \qquad \forall i \quad 1 \leq i \leq m \quad \forall j \quad 1 \leq j \leq r \tag{2.4}$$

Proprietà del prodotto righe per colonne di matrici

- $A * (v + v') = A * v + A * v'$ [4]
- $A * (k * v) = k * (A * v)$

$M_{mn}(K)$Insieme di tutte le matrici a m righe e n colonne con elementi appartenenti all'insieme K. Una matrice A si dice quadrata di ordine n se è di tipo (n, n).

L'insieme delle matrici quadrate di ordine n a elementi reali si indica con $M_n(\mathbb{R})$. In tal caso il prodotto righe per colonne di due matrici quadrate di ordine n è ancora una matrice quadrata di ordine n. Si possono in oltre osservare alcune differernze nelle proprietà del prodotto in $M_n(\mathbb{R})$ rispetto al prodotto tra numeri reali:

- Non è commutativa $A * B \neq B * A$
- Non vale la legge di cancellazione del prodotto

Comunque esistono alcune somiglianze:

- Associativa $(A * B) * C = A * (B * C)$
- Esiste una matrice Identità di ordine n che fa le veci del numero 1 per la moltiplicazione semplice $A * I = I * A = A$
- Proprietà distributiva
  - a destra $A * (B + C) = A * B + A * C$
  - a sinistra $(B + C) * A = B * A + C * A$

2.3.2 Prodotto di una matrice per uno scalare

con $i = 1 \ldots m$ e con $j = 1 \ldots n$

Avendo A di tipo (m, n), $k \in \mathbb{R}$ e $A = (a_{ij})$ allora

$$k * A = (k * a_{ij}) \tag{2.5}$$

Proprietà della moltiplicazione per uno scalare

- $h, u \in \mathbb{R}$, A di tipo (m, n) $\qquad h(u * A) = (h * u)(A)$
- $(h + n) * A = h * A + n * A$
- $h * (A * B) = (h * A) * B = A(h * B)$

[3] Il numero di righe di A deve essere il numero di colonne di B altrimenti non è definita

[4] A è una matrice di tipo (m, n) e $v = \begin{pmatrix} a_1 \\ \ldots \\ a_n \end{pmatrix}$

Definizione Una matrice quadrata A si dice simmetrica se $a_{ij} = a_{ji} \quad \forall i, j$

Definizione Se $A = (a_{ij})$ con $i = 1 \dots m$ e $j = 1\dot{n}$ e $A^T = (b_{ij})$ ove $b_{ij} = a_{ji}$
Alcuni casi particolari delle matrici trasposte

$$(A + B)^t = A^t + B^t \tag{2.6}$$

$$(A * B)^t = B^t * A^t \tag{2.7}$$

$$(A^t)^t = A \tag{2.8}$$

Ogni sistema lineare si può riportare alla forma

$$Ax = B \Leftrightarrow \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + \cdots + a_{2,n}x_n = b_2 \\ \dots \quad \dots \quad \dots \quad \dots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_m \end{cases} \quad a_{i,j} \in \mathbb{R} \quad x_i\text{Incognita} \tag{2.9}$$

in cui

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \dots & \dots & \dots \\ a_{m,1} & \dots & a_{m,n} \end{bmatrix} \qquad B = \begin{bmatrix} b_1 \\ \dots \\ b_m \end{bmatrix} \qquad X = \begin{bmatrix} x_1 \\ \dots \\ x_n \end{bmatrix} \tag{2.10}$$

La matrice A si dice incompleta associata al sistema. La matrice $(A|B)$ di tipo $(m, n+1)$ si dice matrice completa associata al sistema. La scrittura $AX = B$ si dice forma compatta

Determinante di matrice quadrata

Il determinante è definibile solamente per le matrici quadrate. In modo induttivo lo si definisce come

- Se $n = 1 \qquad A = (a)$ poniamo Det$A = a$ ovvero $D(A) = a$ ove D sta per determinante
- Se a è una matrice quadrata di ordine n poniamo $D(A) = \sum_{j=1}^{n} -1^{i+j} a_{i,j} D(A_{i,j})$

2.3.3 Proprietà dei determinanti

Queste proprietà valgono solo per matrici $A \in M_n(\mathbb{R})$

Denotiamo con A_i la riga i. Per le colonne A^j per la colonna j

1. Se A ha una riga o una colonna fatta interamente di zero allora $Det(A) = 0$
2. Ogni riga e ogni colonna di A sono elementi di $\mathbb{R}^n$. Sono $A_1, \dots, A_p$ elementi di $\mathbb{R}^n$ e $\lambda_1, \dots, \lambda_P \in \mathbb{R}$ allora una combinazione lineare [5] di $A_1, \dots, A_p$ è l'elemento di $\mathbb{R} \quad \lambda_1 A_1 + \cdots + \lambda_p A_p$

[5] $A_1, \dots, A_p$ si dicono *Linearmente indipendenti* se dati $\lambda_1, \dots, \lambda_P \in \mathbb{R}$ tali che $\mathbb{R} \quad \lambda_1 A_1 + \cdots + \lambda_p A_p = (0, \dots, 0)$ ne segue che $\lambda_1 = \cdots = \lambda_p = 0$ altrimenti si dice che sono *Linearmente dipendenti. Se $A_1, \dots, A_p$ sono elementi di $\mathbb{R}$ linearmente indipendenti, almeno uno di essi è combinazione lineare degli altri*

3. Sia $A = (A_1, \ldots, A_i, \ldots, A_n)$ con $A_i = \lambda B_i + \mu C_i \quad B_i, C_i \in \mathbb{R}^n \quad \lambda, \mu \in \mathbb{R}$. Questo si può riassumere con il determinante è 'lineare' rispetto alle righe e rispetto alle colonne
4. Se scambio tra di loro due righe o due colonne di A allora il determinante cambia di segno
5. Se A ha due righe o due colonne uguali allora $D(A) = 0$
6. Se ad una riga di A aggiungo una combinazione lineare delle altre righe il determinante non cambia
7. Se le righe o le colonne di A sono linearmente dipendenti, allora $D(A) = 0$

Caratteristica di una matrice $A \in M_{p*q}(\mathbb{R})$

Sia $n \geq p \quad n \leq q$ un minore B di A di ordine n è la matrice quadrata di ordine n che si ottiene da A scegliendo n righe e n colonne di A che stanno in queste n righe e n colonne. Diciamo che A ha caratteristica (o rango) n se esiste un minore B di A di ordine n tale che $D(B) \neq 0$

2.3.4 Proprietà della caratteristica

Avendo una matrice A appartenente a $M_{p*q}(\mathbb{R})$ allora

1. Il massimo numero di righe linearmente indipendente come elementi di $(R)^p$ coincide con la caratteristica
2. Il massimo numero di colonne linearmente indipendente come elementi di $(R)^p$ coincide con la caratteristica

Ne segue che il massimo numero di colonne linearmenti indipendenti è uguale al massimo numero di righe linearmente indipenenti che a sua volta è uguale alla caratteristica della matrice.

2.3.5 Altre definizioni legate alle matrici

Definizione Una matrice $A \in M_n(\mathbb{R})$ si dice invertibile se esiste una matrice $B \in M_n(\mathbb{R})$ tale che $AB = BA = I_n$

Il prodotto di due matrici A e B è invertibile e l'inversa di AB è la matrice $B^- A^-$

Osservazione Sia $AX = B$ un sistema in p equazioni e in q incognite e sia B una matrice invertibile di ordine p. Allora il sistema $AX = B$ e il sistema $(CA)X = CB$ hanno esattamente le stesse soluzioni

2.3.6 Matrici elementari e operazioni elementari

Esistono sostanzialmente tre tipi di matrici elementari:

1. Matrice I_n in cui uno 0 è sostituito da un altro valore a
2. Matrice I_n in cui due 1 sono scambiati con due 0
3. Matrice I_n in cui un 1 è sostituito con un altro valore c

Applicando il prodotto tra matrici tra una matrice $A \in M_{p*q}(\mathbb{R})$ e una di queste matrici elementari si ottiene una di queste operazioni elementari:

1. La somma della i-esima riga di A con la j-esima moltiplicata per l'elemento a (1 matrice elementare)
2. Scambiare tra loro le righe i-esima e j-esima (2 matrice elementare)
3. Moltiplicare la i-esima riga per c (3 matrice elementare)

2.4 Inverse e Gauss

2.4.1 Calcolare l'inversa

La matrice inversa di A definita A^{-1} si ottiene partendo dalla matrice

$$(A|I_n) \tag{2.11}$$

ed eseguendo solo operazioni elementari si ottiene

$$(I_n|E_k \dots E_1) = (I_n|A^{-1}) \tag{2.12}$$

Questo è possibile solo se la matrice di partenza A ha il determinante uguale a 0.

2.4.2 Metodo di elminazione di Gauss

Data una matrice A tramite una sequenza di operazioni elementari a sinistra (equivalente a moltiplicae a sinistra per una sequenza di matrici elementari) possiamo trasformarla in una matrice A detta a scala per righe di A o Col A.

Usando il metodo di eliminazione di Gausssi possono fare tre cose:

1. Calcolo della matrice inversa di una matrice invertibile
2. Risoluzione del sistema di equazioni lineari
3. Calcolare il rango di una matrice

2.5 Spazio Vettoriale

Definizione Un insieme non vuoto G è detto *gruppo abeliano* se dotato di una operazione $G * G \to G$ detta usualmente somma e denotata con il simbolo $+$ e che gode delle seguenti proprietà

- *Associativa* $(a + b) + c = a + (b + c) \quad \forall a, b, c \in G$
- *Commutativa* $a + b = b + a \quad \forall a, b \in G$
- Esiste in G un elemento detto neutro per la somma e si denota con 0 di G tale che $a + 0 = a \quad \forall a \in G$
- $\forall a \in G$ esiste un elemento detto opposto di a tale che $a + (-a) = 0_g$

Notiamo che l'elemento neutro è necessariamente unico e così anche l'opposto di un elemento a

Definizione Lo *spazio vettoriale* V nel campo $\mathbb{R}$ è un gruppo abeliano dotato anche di una seconda operazione, detta moltiplicazione per scalari definita in questo modo $\mathbb{R} * V \to V$ $(r, v) \to rv$ e che gode delle seguenti proprietà

- $a * (b * v) = (a * b) * v \qquad \forall a, b \in \mathbb{R} \quad v \in V$
- $(a + b) * v = a * v + b * v \qquad \forall a, b \in \mathbb{R} \quad v \in V$
- $a * (v_1 + v_2) = a * v_1 + a * v_2 \qquad \forall a \in \mathbb{R} \quad v_1, v_2 \in V$
- $1 * v = v \qquad \forall v \in V$

2.5.1 Definizioni e osservazioni legate allo spazio vettoriale

Definizione Lo 0 di V è detto vettore nullo

Osservazione

1. $a0_v = 0_v \qquad a \in \mathbb{R}$
2. $0v = 0_v \qquad 0 \in \mathbb{R}, v \in V$
3. $(-1) * v = -v \qquad v \in V$

Definizione Dato $v_1, \ldots, v_n \in V$ il vettore $a_1v_1 + \ldots, a_nv_n$ sia una combinazione lineare di $v_1, \ldots, v_n \in V$ allora $a_i \in \mathbb{R}$ si dicono *coefficenti* della combinazione lineare

Definizione I vettori $v_1, \ldots, v_n$ si dicono linearmente dipendenti se esiste una combinazione lineare con tutti i coefficienti nulli $a_1v_1 + \cdots + a_nv_n = 0_v$ diversa da $a_i = 0$. Altrimenti sono linearmente indipendenti

Definizione V si dice *generato dal generatore* $v_1, \ldots, v_n \in V$ se ogni $v \in V$ è combinazione lineare di $v_1, \ldots, v_n$

Definizione Un insieme $v_1, \ldots, v_n$ di vettori linearmente indipendenti che generano V si dice *base di V*

NB Non tutti gli spazi vettoriali hanno un numero finito di generatori. Ci occuperemo solo degli spazi vettoriali con numero finito di generatori altrimenti non si possono usare le matrici

Definizione La *base canonica* di $V = \mathbb{R}^n$ è la base fatta dai vettori $(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)$ in cui n è il numero di elementi per enupla

Osservazione I coefficienti $a_1, \ldots, a_n$ di una combinazione lineare dei vettori di una base sono determinati univocamente da v e dalla base scelta

Definizione Sottospazio di uno spazio vettoriale V è un sottoinsieme di questo spazio vettoriale $W \subseteq V$ se

- $\forall w_1, w_2 \in W \to w_1 + w_2 \in W$
- $\forall a \in \mathbb{R} \quad \forall w \in W \quad a * w \in W$

Definizione L'equazione di un piano in $\mathbb{R}^3$ passante per l'origine è sottospazio vettoriale di $\mathbb{R}^3$

Definizione L'equazione di una retta in $\mathbb{R}^2$ passante per l'origine è sottospazio vettoriale di $\mathbb{R}^2$

Esempio Sia $AX = 0$ un sistema di m equazioni in n incognite.

$$A = \begin{matrix} a_{1,1} & \dots & a_{1,m} \\ \dots & \dots & \dots \\ a_{n,1} & \dots & a_{n,m} \end{matrix}$$

L'insieme delle soluzioni del sistema è un sottospazio vettoriale di $\mathbb{R}^n$.

In generale le soluzioni di un sistema $AX = B$ non sono di m equazioni in n incognite *NON* è un sottospazio di $\mathbb{R}^n$ Infatti se S_1 e S_2 sono due soluzioni allora $S_1 + S_2$ non è una soluzione. Infatti $A(S_1 + S_2) = AS_1 + aS_2 = B + B = 2B \neq B$

Se V sottospazio vettoriale su $\mathbb{R}$. Siano $v_1, \dots, v_p \in V$ vogliamo considerare il sottospazio vettoriale di V generato da $v_1, \dots, v_p \in V$.

Consideriamo

$$W = \{a_1 v_1 + \dots + a_p + v_p | a \in \mathbb{R}\}$$

cioè l'insieme delle combinazioni lineari di vettori $v_1, \dots, v_p \in V$. Allora W è un sottospazio di V $W \leq V$ detto sottospazio generato da $v_1, \dots, v_p \in V$. W è il più piccolo sottospasio di V che contiene $v_1, \dots, v_p$

Proprietà

- Se $W_1, W_2 \leq V$ $\quad$ $W_1 \cap W_2$ è un sottospazio di V
- In generale $W_1 \cup W_2$ non è sottospazio di V
- In generale $W_1 + W_2 = \{w_1 + w_2 | w_1 \in W_1, w_2 \in W_2\}$ è sottospazio di V

Teorema Due qualsiasi basi di uno spazio vettoriale V hanno lo stesso numero di vettori che viene chiamato *dimensione* di V o $\dim(V)$

Lemma Sia V uno spazio vettoriale e $(a_1, \dots, a_n)$ una sua base. Sia $v_1, \dots, v_p$ un insieme di vettori linearmente indipendenti di V con $p \leq n$. Allora è possibile scegliere $n - p$ vettori della base data, siano $e_{i1}, \dots, e_{in-p}$ tali che $(v_1, \dots, v_p, e_{i1}, \dots, e_i n - p$ è una base di V

Corollario Se V è uno spazio vettoriale ed $e_1, \dots, e_n$ è una base di V un insieme di $v_1, \dots, v_n$ di vettori linearmente indipendenti formano una base di V

Lemma Sia V uno psazio vettoriale $(e_1, \dots, e_n)$ una base di V Se $v_1, \dots, v_p$ sono vettori di V con $p > n$ allora $n_1, \dots, n_p$ sono linearmente dipendenti

Teorema Un sottoinsieme di un insieme di vettori linearmente indipendenti è ancora un insieme di vettori linearmente indipendenti

Come facciamo a generare una base di V

Supponiamo che V ha un numero finito di $e_1, \dots, e_m$ di genenratori. Poniamo sapere $e_i \neq 0_v$. Un singolo e_i è un insieme di vettori linearmente indipendenti. Allora ho due possibilità

1. $e_1, \dots, e_m$ sono linearmente indipendenti e ne consegue che sono linearmente indipendenti
2. Sono linearmente dipendenti quindi esiste una compinazione lineare in cui almeno una degli $a_i \neq 0$

Supponendo che a_m allora $v_m = -1(a_1e_1 + \cdots + a_{m-1}e_{m-1})$ allora v_m è una combinazione lòineare dei primi $m-1$ vettori quindi V è generato da $e_1, \dots, e_{m-1}$. Applico lo stesso procedimento a $e_1, \dots, e_{m-1}$ che è ancora un insieme di generatori di V. Ripetendo il procedimento alla fine troverò un sottoinsieme di $e_1, \dots, e_m$ che è ancora un insieme di generatori di V ed è anche un insieme di vettori linearmente indipendenti quindi è una base

2.5.2 Cambiare tra due basi

V spazio vettoriale su $\mathbb{R}$, $(e_1, \dots, e_n)$ base di V e $(e'_1, \dots, e'_n)$ base di V. Se $v \in V$

$$v = b_1e_1 + \cdots + b_ne_nv = b'_1e'_1 + \cdots + b'_ne'_n$$

Che relazione c'è tra le coordinate v rispetto a $(e'_1, \dots, e'_n)$?
Scriviamo

$$v = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix} \begin{pmatrix} b_1 \\ \dots \\ b_n \end{pmatrix}$$

Poniamo

$$(e) = \begin{pmatrix} e_1 & \dots & e_n \end{pmatrix} (b) = \begin{pmatrix} b_1 \\ \dots \\ b_n \end{pmatrix}$$

Ne consegue che

$$v = (e)(b)v = (e')(b')$$

Calcolando così le coordinate dei vettori della base nuova rispetto a quelli della base vecchia

$$e'_1 = c_{1,1}e_1 \dots c_{n,1}e_n \dots e'_n = c_{1,n}e_1 \dots c_{n,n}e_n$$

Generando così la matrice N

$$N = \begin{pmatrix} c_{1,1} & \dots & c_{1,n} \\ \dots & \dots & \dots \\ c_{n,1} & \dots & c_{n,n} \end{pmatrix}$$

N è detta matrice di passaggio dalla base $(e_1, \dots, e_n) = (e)$ alla base $(e'_1, \dots, e'_n) = (e')$

Teorema La matrice N è invertibile se V è spazio vettoriale su $\mathbb{R}$ di dimensione n. (e) (e') due basi di V. Sia N la matrice di passaggio da (e) ed (e'). Allora N è invertibile e la sua inversa N^{-1} è la matrice di passaggio di (e') e (e).

Dimostrazione

$$(e') = (e)N$$

Sia N' la matrice di passaggio da (e') ad $()e'$

$$(e) = (e') = N'$$

Ne segue che

$$(e) = (e')N' = (e)NN'$$

Se chiamiamo $NN' = (b_{i,j})$

$$e_1 = (e_1, \dots, e_n)NN' \Rightarrow NN' = (I_n) \Rightarrow N$$

è invertibile e N' è la sua inversa

Teorema Sia V spazio vettoirale su $\mathbb{R}$ di dimensione n (e) e (e') due basi di V. N la matrice di passaggio da (e) a (e'). Siano (b) e (b) le coordinate di un vettore $v \in V$. Allora $(b') = N^{-1}(b)$ e analogamente $(b) = N(b')$

Dimostrazione

$$(e') = (e) = N \tag{2.13}$$
$$(e) = (e')N^{-1} \tag{2.14}$$
$$v = (e)(b) = (e')(b') \tag{2.15}$$
$$(e')(b') = (e)(b) = ((e')N^{-1})(b) = (e')(N^{-1}(b)) \Rightarrow (b') = N^{-1}(b) \tag{2.16}$$

Esempio

$$V = \mathbb{R}^3[x] \tag{2.17}$$
$$(e) = (1, x, x^2) \tag{2.18}$$
$$(e') = (1 + x, 1 + x + x^2, 1 + 2x) \tag{2.19}$$
$$N = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix} \qquad N^{-1} = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \tag{2.20}$$
$$p(x) = a_0 + a_1 x + a_2 x^2 \tag{2.21}$$
$$(b) = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \tag{2.22}$$
$$(b') = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} * \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \tag{2.23}$$

Teorema Sia V uno spazio vettoriale su $\mathbb{R}$ e $()e_!, \dots, e_n$ una base di V. Sia $v_1 \dots v_q$ con $q < n$ un insieme di vettori V. Allora $v_1 \dots v_q$ sono linearmente indipendenti se e solo se le matrici M le cui colonne sono le coordinate de vettori $v_1 \dots v_q$ rispetto alla base $(e_1, \dots, e_n)$(M sarà una matrice a n righe e q colonne) ha caratteristica q.

Teorema V sottospazio vettoriale su $\mathbb{R}$ e $U, W \leq V$
dim $u \leq$ dim V dim $W \leq$ dim V Supponendo che

$$dimU = n \tag{2.24}$$
$$dimW = m \tag{2.25}$$
$$dimU \cap W = r \tag{2.26}$$
$$\Rightarrow dimU + W = n + m - r \tag{2.27}$$

$U \cap W$ contiene sempre il vettore nullo. Se $U \cap W = \{0\}$ diciamo che le dim $(U \cap W) = 0$. In tal caso le formule delle dimensioni è dim$(U \oplus W)$. In tal caso si dice che U e W sono in somma diretta.

U e W sono in somma diretta se e solo se ogni vettore di $U + W$ si può scrivere in uno ed uno solo modo come somma di un vettore di U e di uno di W. In generale non è detto che $u = u'$ e $w = w'$

Supponiamo che ogni $u + w$ si possa scrivere in un solo modo come somma di un vettore di U e di uno di W. Sia $z \in U \cap W$

$$u + z \in Uw - z \in Wu + z + w - z = u + w \Rightarrow z = 0$$

Viceversa su $U \cap W = 0$ allora

$$u + w = u' + w' \Rightarrow u - u' = w' - w \in U \cap W = \{0\} \tag{2.28}$$
$$\Rightarrow u - u' = w - w' = 0 \tag{2.29}$$
$$\Rightarrow u = u' \tag{2.30}$$
$$w = w' \tag{2.31}$$

Se $U \leq V$ allora esiste $W \leq V$ tale che $V = U \oplus W$. Un tale W si dice supplemento di U in V.

2.6 Applicazioni spazi vettoriali

Definizione Se ho $V \Rightarrow W$ sapzio vettoriale su $\mathbb{R}$. η si dice applicazione lineare () se

1. $\eta(v_1 + v_2) = \eta(v_1) + \eta(v_2) \quad v_1, v_2 \in V$
2. $\eta(\alpha v) = \alpha\eta(v) \quad \forall \alpha \in \mathbb{R} \quad \forall v \in V$

Esempio

$$\eta : \mathbb{R}^3 \Rightarrow \mathbb{R}^2 \tag{2.32}$$
$$\eta(x, y, z) = (z, y) \tag{2.33}$$
$$\eta((x, y, z) + (x', y', z')) = \eta(x + x', y + y', z + z') \tag{2.34}$$
$$= (z + z', y + y') = (z * y) + (z' * y') = \eta(x, y, z) + \eta(x', y', z') \tag{2.35}$$

2.6.1 Proprietà della allicazioni lineari

Un'applicazione lineare ha queste proprietà

- $\eta(0_v) = 0_w$
- Se $V_1 \leq V_2 \Rightarrow \eta(V_1) = \{\eta(v_1) | v_1 \in V_1\} \leq W$
- Se $W_1 \leq W \quad \eta(W_1) \leq V$

In particolare

1. $\eta(V) \leq W$
2. $\eta^{-1}(0_W) \leq V$
3. $\eta^{-1}(0_W)$ è detto il nucleo di η e si denota con Ker η
4. Se $V \xrightarrow{\eta} W \xrightarrow{\varphi} Z$ con η, φ applicazioni lineari allora $(\varphi\eta)(v) = \varphi(\eta(v))$. Allora $\varphi\eta$ è una applicazione lineare
5. Se $\eta : V \Rightarrow W$ è biettiva e η è lineare in W_1 allora $\eta^{-1} \Rightarrow W \Rightarrow V$ è anch'essa lineare

Teorema $\eta : V \Rightarrow W$ è detta iniettiva se e solo se Ker $\eta = \{0_V\}$

2.6.2 Matrice associata ad una applicazione lineare

$\eta : V \Rightarrow W$ che è applicazione lineare. La base $(e_1, \ldots, e_q)$ di V e la base $(b_1, \ldots, b_p)$ di W. Allora

$$\begin{cases} \eta(e_1) = a_{1,1}f_1 + a_{2,1}f_2 + \cdots + ap, 1f_p \\ \ldots \\ \eta(e_q) = a_{1,q}f_1 + a_{2,q}f_2 + \cdots + ap, qf_p \end{cases} \tag{2.36}$$

$$A = \begin{pmatrix} a_{1,1} & \ldots & a_{1,q} \\ \ldots & \ldots & \ldots \\ a_{p,1} & \ldots & a_{p,q} \end{pmatrix} \tag{2.37}$$

A matrice associata ad $\eta : V \Rightarrow W$ rispetto alle basi (e) ed (f).
Se $v \in V$ allora lo possiamo scrivere come

$$v = b_1e_1 + \cdots + l_qe_q \tag{2.38}$$

$$\eta(v) = b + \eta(e_1) + \cdots + b_q\eta(e_q) = \tag{2.39}$$

$$(f_1, \ldots, f_p)A \begin{pmatrix} b_1 \\ \ldots \\ b_q \end{pmatrix} = \eta(v) \tag{2.40}$$

2.6.3 Endomorfismi

$\eta : V \to V$ Stessa base nel dominio e nel codominio. Quindi se A è la matrice associata ad η rispetto ad una data base e A' rispetto ad un altra allora $A' = P^{-1}A * P$ con P matrice di passaggio tra le due matrici

Ci concentriamo su cercare di vedere se e quando è possibile torvare una matrice associata che è diagonale.

$$a = \begin{pmatrix} \lambda_1 & \cdots \\ \cdots & \lambda_n \\ above & \end{pmatrix} \tag{2.41}$$

Definizione $\eta : V \to V \qquad v \neq 0$ si dice autovettore per η relativo all'autovalore λ. Polinomio caratteristico $\mathrm{Det}(A - (\lambda I))$ la ove λ è un incognita e I è la matrice identica.

Teorema Se AxA' sono due matrici quadrate di ordine n e $A' = P^{-1}AP$ con P matrice invertibile allora il polinomio completo di A e di A' coincidono.
$\mathrm{Det}(A' - \lambda I) = \mathrm{Det}(P^{-1}AP - \lambda I) =$
$\mathrm{Det}(P^{-1}AP - P^{-1}\lambda IP) = \mathrm{Det}(P^{-1}(A - \lambda I)P) =$
Per il teorema di Binet
$\mathrm{Det}(P^{-1}(A_\lambda I)P) = \mathrm{Det}(A - \lambda I)$
siccome $\mathrm{Det}P^{-1} = (DetP)^{-1}$
allora = Det $(A - \lambda I)$
Una matrice scalare è una matrice diagonale in cui tutti gli elelmenti della diagonale principale siano uguali.
Abbiamo visto che λ_0 è per η tale che λ_0 è una radice del polinomio caratteristico di η.

Definizione La moltiplicità di una radice λ_0 di un polinomio $P(\lambda)$ è il massimo intero positivo tale che $(\lambda - \lambda_0)$ divida $P(\lambda)$ cioè $P(\lambda) = (\lambda - \lambda_n)^{n_0} q(\lambda)$ ma $(\lambda - \lambda_0)$ non divide $P(\lambda)$

Dati due polinomi $a(\lambda), b(\lambda), b(\lambda) \neq 0$ esiste un polinomi $q(\lambda)$ e $r(\lambda)$ tali che $a(\lambda) = b(\lambda)q(\lambda) + r(\lambda)$ tale che $r(\lambda) = 0$ affinche grado di $r(\lambda)$ sia minore del grado di $b(\lambda)$. Per il teorema di Ruffini se λ_0 è radice di $p(\lambda)$ allora $(\lambda - \lambda_0)q(\lambda)$. Se λ_0 è una radice di $q(\lambda)$ allora $p(\lambda)|q(\lambda) \Rightarrow q(\lambda) = (\lambda - \lambda_0)q_1(\lambda)$
$\Rightarrow p(\lambda) = (\lambda - \lambda_0)^{n_0} q_n(\lambda)$ con λ_0 non è radice di $q_n(\lambda)$

Teorema $\eta \quad V \to V$ è diagonalizzabile se e solo secontiene una base di autovettori.

Definizione Se λ_0 è autovalore per η, l'autospazio relativo all'autovalore λ_0 è costituito dal vettore nullo e da tutti gli autovettori relativi all'autovalore λ_0. Tale autovalore n indica con $E(\lambda_0)$ ed è un sottospazio di V.

Infatti $E(\lambda_0) = \mathrm{Ker}()\eta - \lambda_0 I$
$(\eta - \lambda_0 I)(v) = \eta(v) - \lambda_0(v) \qquad v \in \mathrm{Ker}(\eta - \lambda I)$
$\Leftrightarrow (\eta - \lambda_0 I)(v) = 0$ e cioè $\eta(v) - \lambda_0 v = 0$
$\Leftrightarrow \eta(v) = \lambda_0 v \Leftrightarrow v = 0$ v è autovettore per η relatico all'autovalore λ_0. Quindi dobbiamo studiare $E(\lambda_0)$ per ogni autovalore λ_0 di η.

In generale possiamo affermare che se λ_0 è autocalore con molteplicità n_0 allora $E(\lambda_0) \leq n_0$

Teorema Sia $\eta \quad V \to V$ un endomorfismo. Sia $n = \text{Dim}V$. Siano $\lambda_0, \ldots, \lambda_q$ gli autovalori di $\eta, m_1, \ldots, m_q$ le loro molteplicità. Sia $E(\lambda_i) \quad i = 1, \ldots, q$ l'autospazio relativo all'autovalore λ_i. Allora η è diagonalizzabile se e solo se $\sum_{i=1}^{q} m_i = n$ e Dim $E(\lambda_i) = m_i$

Dimostrazione Dim $E(\lambda_i) \leq m_i$ in generale.

Se ho una base di $V \quad (e_1, \ldots, e_q, \ldots, e_n)$ in cui $e_1, \ldots, e_q$ sono autovettori. La matrice associata A che forma avrà?

$$\eta(e_1) = \lambda_1 \eta_1$$

Sia

$$\begin{pmatrix} T & C \\ & B \end{pmatrix}$$

Se $q = n$ e se T è una matrice tirangolare (superiore o inferiore)

$$\text{Def}(A - \lambda I) = (-1)^s(\lambda - a_{1,1} \ldots (\lambda - a_{ss,})Det(B - \lambda I))$$

In particolare, se A è triangolare (superiore o inferiore) allora $\text{Def}(A - \lambda I) = (-1)^s(\lambda - a_{1,1} \ldots (\lambda - a_{ss,})$. Dunque per una matrice triangolare gli autovalori coincidono con gli elementi della diagonale principale.

Se

$$\begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \text{Det}(A - \lambda I) = \text{Def}(B - \lambda I)\text{Def}(C - \lambda I)$$

Dimostrazione Suppongo che $\text{Dim}E(\lambda I) = s > m_i$. Allora prendo una base di $E(\lambda I) \quad (e_1 \ldots e_s)$ e poi la prolungo fino ad una base di $V(e) = (e_1 \ldots e_s \ldots e_n)$. Allora $\text{Det}(A - \lambda I) = (-1)^s(\lambda - \lambda_i)^s\text{Det}(B - \lambda I)$ con $s > m_i$. Ma m è la moltiplicità di λ_i come radice del prodotto di A perchè le molteplicità di λ è il massimo numero intero tale che $(\lambda - \lambda_i)$ divide il polinomio caratteristico che è un assurdo. Quindi $\text{Dim}E(\lambda I) \leq m_i$

Teorema Autovettori relativi ad autovalori distinti sono linearmente indipendenti.

Nel caso di due autovettori v_1 e v_2 relativi agli autovalori λ_1 e λ_2 con $\lambda_1 \neq \lambda_2$. Se v_1 e v_2 sono linearmente indipendenti, allora per esempio, $v_1 = kv_2 \qquad k \in \mathbb{R}$

Definizione Somma diretta di sottospazio di uno spazio vettoriale (simboli $\oplus$) Sia V spazio vettoriale $V_1, \ldots, V_m$. Si dice che $V_1, \ldots, V_m$ sono una somma diretta se ogni vettore al sottospazio $V_1 + \cdots + V_m$ si può scrivere in uno ed un solo modo come somma $v_1 * \cdots + v_m, v_i \in V_i$. Conseguentemente si ha che se $(v_1, \ldots, v_m)$ è un insieme di vettori non tutti nulli, allora $(v_1, \ldots, v_m)$ sono linearmente indipendenti. In oltre se $r_m \text{Dim}V_i$ e $(v_{1,1}, \ldots, v_{i,r_i})$ è una base di V_i allora $(v_{1,1}, \ldots, v_{1,r+1}, v_{2,1}, \ldots, v_{2,r}, \ldots, v_{m,r_m})$ è una base di $V_1 \oplus \cdots \oplus V_m = V$

Teorema Sia $V' = E(\lambda_1) + \cdots + E(\lambda_m)$ ove $\lambda_1, \ldots, \lambda_m$ sono autovalori distinti. Allora $A' = E(\lambda_1) \oplus \cdots \oplus E(\lambda_m)$

Affinche l'andomorfismo sia diagonabilizzabile è necessario e sufficiente avere una base di autovettori. Ciò significa che $E(\lambda_1 \oplus \cdots \oplus E(\lambda_m)) = V$ cioè equvale a dire che la somma delle dimensioni equivale alla dimensioni di V. $\Sigma m_i \leq n = \text{Dim}V$ Si deve avere $\Sigma m_i = n$ e $\text{Dim}E(\lambda) = m_i$.

Esempio Se il polinomio caratteristico è $(\lambda-2)(\lambda^2+1)$ bisogna considerare il campo di esistenza. Infatti con i reali ha dimensione 2 mentre con i complessi ha dimensione 3.

Esempio

$$\eta : \mathbb{R}^3 \to \mathbb{R}^3 \eta(x_1, x_2, x_3) = (2x_3 - x_1, x_1 + 2x_2 + x_3, 2x_1 - x_3)$$

Scriviamo la matrice associata ad η rispetto alla base canonica

$$\eta(1,0,0) = (-1,1,2)\eta(0,1,0) = (0,2,0)\eta(0,0,1) = (2,1,-1)$$

$$\begin{pmatrix} -1 & 0 & 2 \\ 1 & 2 & 1 \\ 2 & 0 & -1 \end{pmatrix}$$

$$\text{Det} \begin{pmatrix} -1\lambda & 0 & 2 \\ 1 & 2-\lambda & 1 \\ 2 & 0 & -1\lambda \end{pmatrix} = (-1-\lambda)[(2-\lambda)(-1-\lambda)]-4(2-\lambda) = (-1-\lambda)^2(2-\lambda)-4(2-\lambda) = (2-\lambda)(\lambda^2+$$

Gli autovalori sono $(2, -3, 1)$

$$\mathbb{R}^3 = E(2) \oplus E(-3) \oplus E(1)$$

Dunque η è diagonalizzabile. Cerchiamo quindi una base di V fatta di autovettori, per fare questa basta prendere un autovettore non nullo da ciascun autospazio.

$$\eta - 2I$$

La matrice associata rispetto alla base canonica

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 0 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

$E(2)$ è insieme delle soluzioni del sistema

$$B \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \eta(0,1,0) = (0,0,0) \Rightarrow (0,1,0)$$

È una base di $E(2)$

$E(-3)$ =Ker$(\eta + 3I)$ =

$$B \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$(1, 0, -1)$ che è base per $E(-3)$

$(1, -2, 1)$ è una base per $E(1)$

Base di autovettori per $\mathbb{R}^3$ è per esempio $((0,1,0),(1,0,-1),(1,-2,1))$

Come faccio a trovare al matrice di cambiamento di base $P^{-1}AP$ (trovare P)?

$$P^{-1}\begin{pmatrix} -1 & 0 & 2 \\ 1 & 2 & 1 \\ 2 & 0 & -1 \end{pmatrix}P = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Se A è una matrice associata a η associata alla base canonica esistte una matricee invertibile P tale che P^{-1} è la matrice diagonale

$$A = \begin{pmatrix} -1 & 0 & 2 \\ 1 & 2 & 1 \\ 2 & 0 & -1 \end{pmatrix} \tag{2.43}$$

P è la matrice di cambiamento di base della base canonica alla base di autovettori. La base A associata ad η rispetto alla base canonica.

P è la matrice di passaggio dalla base canonica alla base di autovettori.

$$P = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & -2 \\ 0 & -1 & 1 \end{pmatrix} \tag{2.44}$$

Teorema Diagonalizzazione $\eta : V \to V$ è diagonalizzabile se e solo se tutte le radici del polinomio caratteristico sono in $\mathbb{R}$ (o in generale sul campo in cui è definito lo spazio vettoriale) e la Dim$E(\lambda_i)$ =molteplicità di λ come radice del polinomio caratteristico.[6]

In tale caso $V = E(\lambda_1) \oplus \cdots \oplus E(\lambda_q)$ con $\lambda_1, \ldots, \lambda_q$ sono le radici del polinomio caratteristico. Detto m_1 molteplicità di $\lambda_1, \ldots, n$ deve avere $\sum_{i=1}^{q} m_i = n$ =Dim$V$ =grado polinomio caratteristico.

Teorema Ogni polinomio di grado n a coefficenti complessi ha n radici (contate con la loro molteplicità) in $\mathbb{C}$

Se $\eta : V \to V$ è endomorfismo (o ventaglio), una base a bandiera per V rispetto ad η $(e_1, \ldots, e_n)$ è un base tale che , detta V, il sottospazio generato da $(e_1, \ldots, e_i)$ se ha $\eta(V_i) \leq V_i$

Teorema $\eta V \to V$ con V Dim$n$ endomorfismo . Allora η è triangonalizzabile se e solo se tutte le radici caratteristiche di η sono in $\mathbb{R}$ (o, più in generale, nel cmapo su cui è definito lo spazio vettoriale).

$(e_1, \ldots, e_i)$ Se V_i è lo spazio generato da $(e_1, \ldots, e_i)$ allora $\eta(V_i) \leq V_i$

Se $\eta : V \to V$ è un endomorfismo e λ un autovalore per η allora λ^P è un autovalore per $\eta^P = \eta \ldots \eta$ e se v è un autovettore relativo ad λ, v è un autovettore per η^P relativo a λ^P.

Allora se η è un isomorfismo allora v è un autovettore per η^{-P} relativo all'autovettore λ^{-P}.

[6] In generale una matrice triangolare ha come autovalori gli elementi della diagonale principale.

$(\eta \dots \eta)(v) = \lambda^P v$ con v è autovettore per η^P con autovettore λ^P.
Se $\eta(v) = \lambda v$ allora $\eta^{-1}(v) = \lambda^{-1} v$. Allora λ^{-1} è autovettore per η^{-1} con autovalore v allora v è autovettore per $\eta^{-P} = (\eta^{-1})^P$ con autovalore $(\lambda^{-1})^P = \lambda^{-P}$

Teorema Sia $\eta : V \to V$ un endomorfismo Dim$V = n$. Allora esiste un intero $s \leq n$ tale che $\eta^s(v) = \eta^{s+1}(v) \qquad \forall v \in V$
Ker(η^s) =Ker(η^{s+1}).
Poniamo $U = \eta^s(V), \qquad W =Ker\eta^s$.
Allora si ha:

- $\eta|_u : U \to U$ è un isomorfismo
- $\eta(W) \leq W$
- $\eta : W \to W$ è nulopotente [7]
- $V = U \oplus W$

Dimostrazione

$$V \geq \eta(n) \geq \eta^2(v) \cdots \geq \eta^s(v) \geq \eta^{s+1}(v) \tag{2.45}$$

Siccome v ha dimensione finita esiste s tale che $\eta^s(v) = \eta^{s+1}(v)$

$$\eta|_{\eta^s(v)} \eta^s(v) \to \eta^{s+1}(v) = \eta^s(v) \Rightarrow \eta|_{\eta^s(v)} \tag{2.46}$$

Facciamo vedere che per lo stesso intero s si ha
Ker(η^s)=Ker(η^{s+1}). Sia $v \in$Ker$(\eta^s) \Rightarrow \eta^s(v) = 0 \Rightarrow \eta^{s+1}(v) = 0 \Rightarrow \eta^s(v) \in$Ker$\eta \Rightarrow$ $\eta^s(v) = 0 \Rightarrow v \in$Ker$(\eta^s) \Rightarrow$Ker$(\eta^s)$ =Ker(η^{s+1})
Allora posto $W =$Kerη^s.Allora

$$\left\{ \ \eta^s(w) = \eta^{s+1}(w) = \eta^s(\eta(w)) \quad \Rightarrow \eta(w) \subseteq \text{Ker}(\eta^s) = w \right. \tag{2.47}$$

Teorema $\eta : V \to V$ dove V di dimensione n. Allora esiste un intero $0 < s < n$ tale che se ha $\eta^s(V) = \eta^{s+1}(V)$ e Ker(η^s) =Ker(η^{s+1}). Posto $U = \eta^s(V)$ e $W =$Ker(η^s). Si ha quindi:

- $\eta|_U : U \to U$
- $\eta(W) \subseteq W$
- $\eta|_W : W \to W$ è nilpotente
- $V = U \oplus W$

Si ha

1. $V \geq \eta(V) \geq \eta(\eta(V)) \geq \dots$ perchè V ha dimensione finita: la catena ad un certo punto si ferma. Si avrà $\eta^s(V) = \eta^{s+1}(V)$.
   $\eta|_{\eta^s(V)} : \eta^s(V) \to \eta^{s+1}(V) = \eta^s(V) \Rightarrow \eta|_U : U \to U$ isomorfismo

[7] $\eta : V \to V$ si dice nulpotente se esiste s tale che $\eta^s = 0$ (funzione che manda tutto in 0)

2. W =Ker(η^s) =Ker(η^{s+1}). Sia $v \in$Ker(η^s) e quindi $\eta^s(V) = 0 \Rightarrow \eta(\eta^s(v)) = 0 \Rightarrow \eta^{s+1}(v) = 0$. Viceversa se $v \in$Ker(η^{s+1}). Allora $\eta^{s+1}(v) = 0 = \eta(\eta^s(v))$ se e solo se $\eta^s(V) = U$ e $\eta|_U$ e isomorfa. Quindi l'unico vettore di U le cui immagini tramite η è 0, è il vettore 0. Ne segue che $\eta^s(v) = 0 \Rightarrow v \in$Ker$\eta^s \Rightarrow$Ker$(\eta^s)$ =Ker(η^{s+1}). Abbiamo allora che $\eta(W) \subseteq W$. Sia $\eta^s(W) = 0$. $\eta^{s+1}(W) = 0 = \eta^s(\eta(W)) \Rightarrow \eta(W) \subseteq$Ker$\eta^s = W$ Quindi $\eta|_W : W \to W$

3. $\eta|_W : W \to W$ è nipotente. Se $w \in W \Rightarrow w \in$Ker$(\eta^s)$. $\eta^s(w) = 0 \forall w \in W \Rightarrow \eta^s|_W$ è la applicazione che manda tutto in 0 e quindi $\eta|_W$ è nulpotente.

4. $V = U \oplus W$. Sia $v \in U \cap W$; $w \in W \Rightarrow v \in$ Ker$(\eta^s) \Rightarrow \eta^s(v) = 0$, ma $v \in U$ e $\eta|_U : U \to U$ è isomorfismo. Allora $v = 0$ perchè $\eta|_U$ è isomorfismo. Allora $\eta^s : U \to U$ è isomorfiscmo e quindi $\eta^s : V \to V$ con Dim$V$ =DimKer(η^s)+Dim$\eta^s(V)$ e $V = U \oplus W$

5. Ponendo una base di V costruita da $(u_1, \ldots, u_n, w_1, \ldots, w_t)$ e $(u_1, \ldots, u_n)$ è la base di U mentre $(w_1, \ldots, w_t)$ è la base di W. Allora la matrice associata ad η rispetto a tale base sarà della forma $A00B$. A è la matrice associata ad $\eta|_U : U \to U.b$ è la matrice associata ad $\eta|_W : W \to W$.

Corollario Se $\eta : V \to V$ endomorfismo di v di dimensione n. Se η è multipotente e λ è una endomorfismo per η allora $\lambda = 0$. Viceversa se 0 è autovalore per η con molteplicità n allora η è nilpotente.

2.7 Esercizi svolti

Esercizio Consideriamo $T : \mathbb{R}^3 \to \mathbb{R}^3$ l'applicazione lineare $T(x_1, x_2, x_3) = (x_1 + x_2, x_2 + x_3, x_1 + x_3)$

1. Scrivere matrice associata a T rispetto alla base canonica di $\mathbb{R}^3$. $T(1,0,0) = (1,0,0)$ $T(0,1,0) = (1,1,0)$ $T(0,0,1) = (0,1,1)$

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \tag{2.48}$$

2. Siano $u_1 = (1,-1,0)$, $u_2 = (1,0,-1)$, $u_3 = (0,1,1)$. È una base se la matrice

$$T = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 1 \end{pmatrix} \tag{2.49}$$

   Visto che questa è una base la posso considerare come una matrice di cambiamento di base. Matrice di passaggio della vecchia base alla nuova base ha come colonne le coordinate dei vettori della vecchia base rispetto alla nuova base. T è la matrice di cambiamento di base dalla base di u_1, u_2, u_3 alla base canonica.

3. Se vogliamo scrivere la matrice A' associata a T rispetto alla base u_1, u_2, u_3.

$$A' = P^{-1}AP \tag{2.50}$$

   è la matrice di passaggio della base (e_1, e_2, e_3) alla base (u_1, u_2, u_3). La matrice T corrisponde a P^{-1}. Per trovare P ho due possibilità: trovare l'inversa di T

attraverso la riduzione scala per righe di $(T|I_3) \rightarrow (I_3|T^{-1} = P)$ oppure cerco di scrivere direttamente i vettori (e_1, e_2, e_3) come combinazione lineare dei vettori (u_1, u_2, u_3).
$e_1 = 1/2u_1 + 1/2u_2 + 1/2u_3 = (1, 0, 0)$[8]
$e_2 = -1/2u_1 + 1/2u_2 + 1/2u_3 = (0, 1, 0)$
$e_3 = 1/2u_1 - 1/2u_2 + 1/2u_3 = (0, 0, 1)$

$$P = \begin{pmatrix} 1/2 & -1/2 & 1/2 \\ 1/2 & 1/2 & -1/2 \\ 1/2 & 1/2 & 1/2 \end{pmatrix} \tag{2.51}$$

Esercizio Sia V uno spazio vetttoriale sul campo $\mathbb{R}$ e $\phi : V \rightarrow V$ una funzione linare la cui matrice associata è

$$A = \begin{pmatrix} 3 & 1 & 5 \\ 2 & 0 & 2 \\ 1 & 1 & 3 \end{pmatrix} \tag{2.52}$$

1. Verificare che sia invertibile. Altrivmenti la si renda tale cambiando una o più colonne
2. Si calcoli l'aplicazione inversa

Calcolo il determinante (si può calcolare il determinante in svariati modi; qui si usa semplicemente la formula del determinante).

$$1(2 * 3 - 2 * 1) + 1(3 * 2 - 5 * 2) = 4 + (-4) = 0 \tag{2.53}$$

Per calcolare l'inversa mi basta usare la matrice

$$\begin{pmatrix} 3 & 1 & 5 \\ 2 & 0 & 2 \\ 2 & 1 & 3 \end{pmatrix} \tag{2.54}$$

Ne calcolo l'inversa con l'algoritmo scala per righe $A|I$ e viene fuori che è

$$\begin{pmatrix} -1 & 1 & 1 \\ -1 & -\frac{1}{2} & 2 \\ 1 & -\frac{1}{2} & -1 \end{pmatrix} \tag{2.55}$$

Esercizio Si trovi l'insieme delle soluzioni del sistema lineare con coefficienti in $\mathbb{R}$

$$\begin{bmatrix} 3 & 1 & 4 \\ 2 & 0 & 2 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 3 \end{bmatrix} \tag{2.56}$$

Si tratta di uno spazio vettoriale? Perchè? $Ax = 0$ oppure Ker(A) e N(N) e la soluzione di $Ax = b$

Si consideri l'insieme M delle matrici $3x3$

[8] $e_1 = a * 1u_+ b * u_2 + c * u_3$ e così per tutti gli altri

1. Le matrici assimmetriche ($A^t = -A$) sono un sottospazio
2. Le matrici non simmetriche ($A^t \neq A$)
3. Le matrici che hanno $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ nel Kernel