

Matematica discreta

Appunti rielaborati

11/03/2009

Sid, Eleonora

Introduzione

Questi appunti si riferiscono al corso di Matematica discreta tenuto dal prof. Mainardis per il corso di Informatica presso l'Università degli studi di Udine.

Non avendo potuto frequentare il corso queste pagine sono state scritte rielaborando gli appunti dei corsi di Algebra 1 e 2 e Geometria 1 e 2 assieme a Eleonora Annigoni (neolaureata in Matematica, contattabile per lezioni al numero 329/9666124), a lei va tutta la mia gratitudine per avermi fatto apprezzare la Matematica.

L'intenzione non è stata quella di trascrivere tutte le informazioni, ma di creare un piccolo, si spera abbastanza formale, manuale utile come riferimento e al ripasso, strutturato al fine di facilitare la comprensione degli argomenti.

Per qualsiasi suggerimento, integrazione e segnalazione: sid@camminaresuimonti.org.

Sul sito <http://www.sugata.eu> potete trovare altri miei appunti inerenti il corso di laurea.



Questo/a opera è pubblicato sotto una [Licenza Creative Commons](https://creativecommons.org/licenses/by-nc/4.0/).
Se queste pagine vi sono state utili considerate di spedirmi una cartolina.
Autori: Michele Di Cosmo – Eleonora Annigoni – <http://www.sugata.eu>

Indice

Nomenclature.....	3	Omomorfismo di anelli	14
Aritmetica	3	Teorema: gli unici ideali di un campo sono banali	14
Massimo comun divisore.....	3	Spazi vettoriali.....	16
Divisione euclidea.....	3	Spazio vettoriale	16
Dimostrazione induttiva	3	Sottospazio vettoriale	16
Numeri complessi e numeri immaginari puri	3	Sottospazio generato da X	16
Algoritmo di Euclide – Esempio pratico.....	4	Sistema di generatori	17
Relazioni e insiemi	4	Vettori linearmente indipendenti	17
Relazione o corrispondenza	4	Base.....	17
Relazioni d’equivalenza	4	Base canonica (\mathcal{E}_n)	18
Relazione d’equivalenza associata	5	Dimensione di uno spazio vettoriale ($\dim V$).....	18
Relazione d’equipotenza	5	Teorema di Grassmann	18
Classe di equivalenza.....	5	Spazio quoziente.....	19
Operazioni sulle classi di equivalenza.....	5	Dimensione dello spazio quoziente	19
Insieme quoziente	5	Funzione lineare.....	20
Congruenza modulo n	5	Omomorfismo di spazi vettoriali.....	21
Insieme $\mathbb{Z}n$ o $\mathbb{Z} \equiv n$, ovvero le classi resto modulo n	5	Teorema nullità + rango.....	21
Insieme dei multipli	5	Matrici.....	21
Insieme delle parti di X	6	Matrice.....	21
Partizione	6	Matrice triangolare e matrice “a gradini”	21
Funzione	6	Matrice diagonale	22
Funzione ben definita.....	6	Complemento algebrico.....	22
Proprietà iniettiva.....	6	Operazioni di riga	22
Proprietà suriettiva.....	6	Prodotto matrice – vettore	22
Proprietà biiettiva.....	6	Prodotto matrice – matrice.....	23
Gruppi.....	7	Rango	23
Un qualcosa abeliano	7	Matrice trasposta.....	23
Semigruppoo	7	Determinante.....	23
Monoide	7	Matrice inversa	24
Gruppo	7	Sistemi lineari.....	24
Sottogruppo	8	Sistema lineare.....	25
Sottogruppo normale	8	Funzione lineare associata alla matrice	25
Classe laterale.....	8	Coordinate di un vettore.....	26
Gruppo quoziente	9	Matrice di una funzione lineare e coordinate di un vettore	26
Omomorfismo di gruppi e nucleo.....	9	Teorema di Rouché – Capelli	27
Teorema di Lagrange	10	Metodo per risolvere i sistemi lineari	27
Permutazioni	11	Autovalore e autovettore	27
Gruppo delle permutazioni su X	11	Polinomio caratteristico di una matrice.....	28
Supporto di f	11	Funzione e matrice diagonalizzabile	28
Permutazioni disgiunte.....	11	Metodo per trovare gli autovalori di una matrice e di una	29
Ciclo.....	11	funzione	29
Prodotto di cicli disgiunti.....	12	Metodo per trovare gli autovettori.....	30
Trasposizione.....	12	Metodo per trovare gli autospazi	30
Anelli.....	12	Appendice	32
Anello	12	Teoremi da sapere	32
Varietà e discendenti degli anelli.....	13	Per dimostrare che.....	32
Ideale.....	13	Approfondimenti	32
Anello quoziente	14		

Nomenclature

- 1) **Assiomi** e **definizioni** vengono da Dio.
- 2) I **teoremi** si ricavano dagli assiomi e dalle definizioni per deduzione. I **lemmi** sono dei piccoli teoremi che servono per dimostrare i veri teoremi.
- 3) I **corollari** sono conseguenze di teoremi o casi particolari di un teorema.
- 4) Le **osservazioni** sono osservazioni.

Aritmetica

Massimo comun divisore

Siano $a, b \in \mathbb{Z}$ non entrambi nulli.

$$\text{MCD}(a, b) := (a, b)$$

$(a, b) = d$ con $d > 0$ tale che

- $d|a$ e $d|b$ (d divide a e d divide b), ossia d è un divisore “comune” di a e b .
- Sia $c \in \mathbb{Z}$, se $c|a$ e $c|b \Rightarrow c|d$, ossia d è il “massimo” dei divisori comuni di a e b .

Proprietà del massimo comune divisore

Se $d = (a, b) \Rightarrow \exists x, y \in \mathbb{Z} \mid d = ax + by$.

Se $c|a$ e $c|b \Rightarrow c|ax + by \forall x, y \in \mathbb{Z}$.

a e b si dicono coprimi (primi fra loro) se $(a, b) = 1$.

Quindi a, b coprimi $\Leftrightarrow \exists x, y \in \mathbb{Z} \mid 1 = ax + by$.

Divisione euclidea

Ogni numero $a \in \mathbb{Z}$ si può dividere per un numero $n \in \mathbb{Z}$ con un resto $r \in \mathbb{Z}$:

$$a \in \mathbb{Z}, n \in \mathbb{Z} \Rightarrow \exists q \in \mathbb{Z}, r \in \mathbb{Z}, 0 \leq r < n \mid a = n \cdot q + r$$

Dimostrazione induttiva

Le dimostrazioni per induzione si suddividono in “base dell’induzione” in cui si dimostra il caso base e in “passo induttivo” in cui si dimostra la validità della tesi per gli altri valori.

Le induzioni hanno quindi senso solo in \mathbb{N} perché è il solo discreto e limitato (parte da 0).

Numeri complessi e numeri immaginari puri

La moltiplicazione, con identità $(1, 0)$, è così definita:

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

Per i numeri immaginari puri valgono le seguenti proprietà:

$$(a, b) = (\rho \cos \phi, \rho \sin \phi) = \rho(\cos \phi + i \sin \phi)$$

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a + ib)(c + id) = ac - bd + i(ad + bc)$$

$$|(a, b)| = \sqrt{a^2 + b^2} = \rho$$

Algoritmo di Euclide – Esempio pratico

$1 = 11x + 72y$. Voglio trovare l'inverso dell'elemento $11 + 72\mathbb{Z}$ nell'anello (vedi § "Anello") $\mathbb{Z}/72\mathbb{Z}$. Il suo inverso è $x + 72\mathbb{Z}$ tale che $(x + 72\mathbb{Z})(11 + 72\mathbb{Z}) = 1 + 72\mathbb{Z}$, ossia per definizione di prodotto di classi laterali (vedi § "Operazioni sulle classi di equivalenza"), $x \cdot 11 \equiv_{72} 1 \Rightarrow x \cdot 11 - 1 = 72 \cdot n$ con $n \in \mathbb{Z} \Rightarrow 1 = x \cdot 11 + 72 \cdot n$. (Vedi § "Congruenza modulo n" per il significato di \equiv_n .) L'algoritmo di Euclide permette di calcolare il valore x cercato.

$$a = 72, b = 11$$

x	y	z	q
1	0	$72 = a$	
0	1	$11 = b$	6
1	-6	6	1
-1	7	5	1
2	-13	1	5

Per calcolare i valori scrivo le prime due righe fisse, calcolo q (quoziente): quante volte ci sta l'11 nel 72. Poi calcolo x e analogamente y :

$$q = \left\lfloor \frac{z_{-1}}{z} \right\rfloor$$

$$x = x_{-2} \cdot q - x_{-1} \cdot q$$

Infatti per ogni riga vale:

$$ax + by = z$$

L'inverso è quindi $-13 + 72\mathbb{Z}$, infatti $(-13 + 72\mathbb{Z}) \cdot (11 + 72\mathbb{Z}) = (-13 \cdot 11 + 72\mathbb{Z}) = -143 + 72\mathbb{Z}$ dove $-143 \equiv_{72} 1$ quindi $-143 + 72\mathbb{Z} = 1 + 72\mathbb{Z}$.

Relazioni e insiemi

Relazione o corrispondenza

Sia \sim una relazione (o corrispondenza) fra A e B .

\sim è un sottoinsieme del prodotto cartesiano fra A e B ($\sim \subseteq A \times B$).

Relazioni d'equivalenza

Valgono le seguenti proprietà:

1. Proprietà riflessiva: ogni elemento è in relazione con se stesso: $x \sim x$.
2. Proprietà simmetrica: se $x \sim y \Rightarrow y \sim x$.
3. Proprietà transitiva: $a \sim b, b \sim c \Rightarrow a \sim c$.

Relazione d'equivalenza associata

Data una funzione f , la relazione d'equivalenza associata ad f è la relazione \sim_f così definita:

$$x \sim_f y \Leftrightarrow f(x) = f(y)$$

Relazione d'equipotenza

Due insiemi X e Y sono equipotenti, e si usa la notazione $|X| = |Y|$, se e solo se $\exists f: X \rightarrow Y$ con f biiettiva.

Questa relazione è anche una relazione d'equivalenza.

Classe di equivalenza

La classe di equivalenza di \sim con rappresentante x è definita così:

$$[x]_{\sim} := \{y \in X | x \sim y\}$$

Con \sim relazione d'equivalenza.

La classe “prende” solo gli elementi che sono in relazione con il rappresentante.

Operazioni sulle classi di equivalenza

$[a]_m + [b]_m = [a + b]_m$ per definizione.

$[a]_m \cdot [b]_m = [a \cdot b]_m$ per definizione.

Insieme quoziente

Data una relazione d'equivalenza su un insieme X , si definisce l'insieme quoziente come l'insieme di tutte le classi di equivalenza: X/\sim .

Congruenza modulo n

$a \equiv_n b$ oppure $a \equiv b \pmod{n}$ significa n divide $a - b$, ovvero

$$a - b = n \cdot t \text{ con } t \in \mathbb{Z}$$

\equiv_n è una relazione d'equivalenza su \mathbb{Z} .

Insieme \mathbb{Z}_n o \mathbb{Z}_{\equiv_n} , ovvero le classi resto modulo n

$$\mathbb{Z}_n := \mathbb{Z}_{\equiv_n} := \{\bar{x} | x \in \mathbb{Z}\} := \{[x]_{\equiv_n} | x \in \mathbb{Z}\} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

Ad esempio $\mathbb{Z}_{17} = \{\bar{0}, \dots, \bar{16}\}$, ovvero i resti della divisione di ogni \mathbb{Z} per 17.

Insieme dei multipli

Usando la notazione additiva, l'insieme dei multipli di a è:

$$a\mathbb{Z} = \langle a \rangle := \{a \cdot n | n \in \mathbb{Z}\}$$

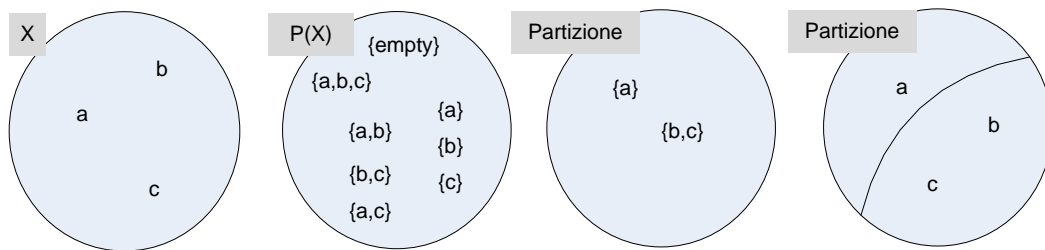
Insieme delle parti di X

$\mathcal{P}(X)$ è l'insieme di tutti i possibili sottoinsiemi di X compreso \emptyset e X .

Partizione

Una partizione è un sottoinsieme di $\mathcal{P}(X)$. Formalmente la partizione di un insieme è una famiglia $\mathcal{A} = \{A_i : i \in I\}$ di sottoinsiemi di X tale che:

- P1) Ogni sottoinsieme non contiene elementi che compaiono in altri sottoinsiemi: $\forall i \neq j A_i \cap A_j = \emptyset$.
- P2) Ci sono tutti gli elementi: $\bigcup_{i \in I} A_i = X$.
- P3) Nessun sottoinsieme è vuoto: $\emptyset \neq A_i \forall A_i \in \mathcal{A}$.



Funzione

Una funzione $f: X \rightarrow Y$ è una relazione fra X e Y dove ogni elemento del codominio è immagine tramite f al più di un elemento del dominio.

Ovvero una funzione $f: X \rightarrow Y$ è una relazione di X in Y tale che:

- F1) $\forall x \in X \exists y \in Y | y = f(x)$ (sottointeso nella praticità delle dimostrazioni)
- F2) $x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$ (ovvero se $f(x) = y \wedge f(x) = y' \Rightarrow y = y'$)

Funzione ben definita

E' una funzione della quale ho verificato che il codominio è quello che ho scritto essere (F1). Si usa dire nelle dimostrazioni.

Per verificare che è effettivamente una funzione si verifica F2.

Proprietà iniettiva

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Proprietà suriettiva

$$\forall y \in Y \exists x \in X | f(x) = y$$

Proprietà biiettiva

Funzione che gode della proprietà iniettiva e suriettiva.

E' abbastanza intuitivo che se una funzione è biettiva è anche invertibile (f^{-1}) (uso sia la proprietà iniettiva che suriettiva per dimostrarlo).

Gruppi

Un qualcosa abeliano

Un qualcosa che gode della proprietà commutativa: $a \cdot b = b \cdot a$.

Semigrupp

(X, \cdot) con X insieme e \cdot operazione.

Gode della proprietà associativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. E' stabile per definizione.

Nei semigrupp gli elevamenti a potenza x^n con x semigrupp $(X, *)$ "eseguono" $*$ n volte su x .

Il semigrupp con cui lavoriamo solitamente è $(\mathbb{Z}, +)$ e useremo la notazione additiva in quanto l'operazione è l'addizione (moltiplicazione per ripetere l'operazione). Nel caso in cui lavorassimo con la moltiplicazione useremmo la notazione moltiplicativa (potenza per ripetere l'operazione).

$n \cdot x$ con x semigrupp sono multipli, non prodotti, e sono definiti $n \cdot x := (n - 1) \cdot x + x$ dove $+$ è l'operazione del semigrupp in notazione additiva. In notazione moltiplicativa dovrei scrivere $x^n := x^{n-1} \cdot x$ con $n > 0$ e $x^1 := x$.

Monoide

$(X, \cdot, 1_X)$ con X insieme, \cdot operazione e 1_X elemento neutro di X .

Semigrupp con elemento neutro destro e sinistro (che sono uguali in quanto associativo): $e_d = e_s = e$.

L'elemento neutro viene identificato con 0_X o 1_X a seconda della notazione usata (additiva o moltiplicativa).

Da notare che un elemento elevato alla 0, ovvero x^0 viene definito solo per i monoidi (nei semigrupp era definito x^n con $n > 0$) poiché serve l'elemento neutro per definirlo: $x^0 = 1_X$.

Gruppo

Monoide con elemento inverso destro e sinistro (che sono uguali in quanto associativo): $a_s \cdot a = e = a \cdot a_d$.

L'elevamento a potenza -1 di più elementi di un gruppo si definisce così:

$$(a \cdot b \cdot c)^{-1} = c^{-1} \cdot b^{-1} \cdot a^{-1}$$

Prodotto diretto di gruppi

Siano H e G gruppi.

$$H \times G = \{(h, g) | h \in H, g \in G\} \Rightarrow |H \times G| = |H| \cdot |G|$$

$$(H \times G, \cdot) = (h_1, g_1) \cdot (h_2, g_2) := (h_1 h_2, g_1 g_2)$$

dove $(H \times G, \cdot)$ è un gruppo.

Sottogruppo

H è un sottogruppo se

S0) Sottoinsieme non vuoto di G : $H \subseteq G$ con $H \neq \emptyset$.

S1) E' stabile: $(x \cdot y) \in H \forall x, y \in H$.

S2) Contiene gli inversi di tutti gli elementi: $\forall a \in H, a^{-1} \in H$.

Come conseguenza H è un gruppo (corollario).

Indicherò H sottogruppo di G con $H \leq G$.

Negli esercizi solitamente si usa la definizione costruttiva di sottogruppo per dimostrare che un sottoinsieme di G è un sottogruppo:

$$H \leq G \Leftrightarrow x^{-1}y \in H \forall x, y \in H$$

Sottogruppi di $(\mathbb{Z}, +)$

Una proprietà particolare di $(\mathbb{Z}, +)$ è che i suoi sottogruppi sono tutti e soli gli insiemi $a\mathbb{Z}$ (insieme dei multipli).

Sottogruppo normale

$$K \leq G$$

$$xK = Kx \forall x \in G \Rightarrow H \text{ normale in } G$$

Indicherò H normale in G con $H \trianglelefteq G$.

Per stabilire se un sottogruppo K è normale posso anche usare questa definizione costruttiva:

$$K \leq G$$

$$\forall x \in G, \forall k \in K, x^{-1} \cdot k \cdot x \in K \Leftrightarrow K \trianglelefteq G$$

Si noti che i sottogruppi dei gruppi abeliani sono tutti normali poiché:

$$x \in G, h \in H$$

$$xh = hx \Rightarrow xH = Hx$$

Classe laterale

Sia G un gruppo e $H \leq G$,

$$x \sim_H y \Leftrightarrow x^{-1} \cdot y \in H$$

$$x \sim'_H y \Leftrightarrow x \cdot y^{-1} \in H$$

una classe laterale sinistra di H in G è così definita: $Hg := [g]_{\sim_H} = \{y \in G | g \sim_H y\} = \{y \in G | g^{-1} \cdot y \in H\}$

una classe laterale destra di H in G è così definita: $gH := [g]_{\sim'_H} = \{y \in G | g \sim'_H y\} = \{y \in G | g \cdot y^{-1} \in H\}$

Inoltre, sapendo che $[x]_{\sim_H} = \{y \in G | g \sim_H y\}$ si dimostra che $[x]_{\sim_H} = xH$:

$$\begin{aligned}
 [x]_{\sim_H} &= \{y \in G \mid x^{-1} \cdot y \in H\} \\
 &= \{y \in G \mid x^{-1} \cdot y = h \in H\} \\
 &= \{y \in G \mid y = xh \text{ con } h \in H\} \\
 &=: xH
 \end{aligned}$$

Si noti che $Hg \subseteq G$ e $gH \subseteq G$.

Gruppo quoziente

Sia G gruppo. $N \trianglelefteq G$.

Il gruppo quoziente è così definito:

$$G/N := G/\sim_N = G/\sim'_N \text{ poiché normale.}$$

Quindi $G/N = \{gN = Ng \mid g \in G\}$.

Definisco l'operazione \times :

$$\begin{aligned}
 G/N \times G/N &\rightarrow G/N \\
 (xN, yN) &\mapsto xyN \\
 xN \cdot yN &\stackrel{\text{def}}{=} xyN
 \end{aligned}$$

$(G/N, \cdot)$ è un gruppo e si chiama gruppo quoziente di G su N .

L'elemento neutro è $1 \cdot N$, ovvero N :

$$\begin{aligned}
 (xN) \cdot (1N) &= (x \cdot 1)N = xN \\
 (1N) \cdot (xN) &= (1 \cdot x)N = xN
 \end{aligned}$$

L'inverso di xN è $x^{-1}N$.

Esempio

I sottogruppi di $(\mathbb{Z}, +)$ sono $n\mathbb{Z}$ (teorema).

$$\begin{aligned}
 \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} &\stackrel{\text{div.euclidea}}{\implies} \mathbb{Z}/n\mathbb{Z} = \{(n \cdot q + r) + n\mathbb{Z} \mid q \in \mathbb{Z}, r \in \mathbb{Z}, 0 \leq r < n\} \implies \\
 \implies \mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \mid r \in \mathbb{Z}, 0 \leq r < n\} &\stackrel{0 \leq r < n}{\implies} \mathbb{Z}/n\mathbb{Z} \text{ ha } n \text{ elementi} \implies \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \bar{n}\}
 \end{aligned}$$

dove $a + n\mathbb{Z}$ è una classe laterale.

$$\{[g]_{\equiv_n} \mid g \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\} = \mathbb{Z}/n\mathbb{Z} = \{[g]_n\} = \mathbb{Z}_n.$$

Omomorfismo di gruppi e nucleo

Siano G, G' gruppi.

$\varphi: G \rightarrow G'$ è un omomorfismo di gruppi se

$$\varphi(g_1 \cdot_G g_2) = \varphi(g_1) \cdot_{G'} \varphi(g_2) \quad \forall g_1, g_2 \in G$$

Se φ è biettiva, φ si dice isomorfismo.

Gli omomorfismi di gruppi godono delle seguenti proprietà:

- $\varphi(1_G) = 1_{G'}$
- $\varphi(x^{-1}) = \varphi(x)^{-1}$

○ $\varphi(x^n) = \varphi(x)^n$

L'insieme degli omomorfismi si dice:

$$\text{hom}(G, G') := \{\varphi: G \rightarrow G' \mid \varphi \text{ omorfismo}\}$$

Il nucleo di φ è così definito:

$$\ker(\varphi) := \{g \in G \mid \varphi(g) = 1_H\} = \varphi^{-1}(1_H) \subseteq G$$

Si noti che $\ker \varphi \trianglelefteq G$.

Si noti anche che φ iniettiva $\Leftrightarrow \ker(\varphi) = \{1_G\}$.

Teorema di Lagrange

Lemma: $|xH| = |Hx| = |H|$

Il numero di elementi di una classe laterale destra coincide con il numero di quelli della classe laterale sinistra: $|xH| = |Hx| = |H| \forall x \in G$ con $H \leq G$. Per dimostrare questo lemma è sufficiente definire una funzione biiettiva (vedi § "Relazione d'equipotenza"):

$$\varphi: H \rightarrow Hx, h \mapsto hx$$

φ è ben definita per costruzione, iniettiva (dimostrabile) e suriettiva per costruzione. In modo analogo si definisce una biiezione sulla classe laterale sinistra.

Lemma: $|\mathcal{S}| = |\mathcal{D}|$

Il numero di classi laterali destre coincide con il numero di classi laterali sinistre: $|\{xH : x \in G\}| = |\{Hx : x \in G\}|$. Per dimostrare questo lemma è sufficiente definire una funzione biiettiva (vedi § "Relazione d'equipotenza"):

$$\varphi: \mathcal{S} \rightarrow \mathcal{D}, xH \mapsto Hx^{-1}$$

Per dimostrare che φ è ben definita devo dimostrare che $xH = yH \Rightarrow Hx^{-1} = Hy^{-1}$. Dimostriamo i \Leftrightarrow così dimostriamo sia che è una funzione (ben definita) che è iniettiva:

$$xH = yH \Leftrightarrow y \in xH \Leftrightarrow y = xh \Leftrightarrow x^{-1}y = h \Leftrightarrow x^{-1} = hy^{-1} \Leftrightarrow x^{-1} \in Hy^{-1} \Leftrightarrow Hx^{-1} = Hy^{-1}$$

φ è suriettiva perché $Hy = H(y^{-1})^{-1} = \varphi(y^{-1}H)$.

Notazione: Indice di H in G

Sia l'indice di H in G così definito:

$$[G: H] := |\mathcal{S}| = |\mathcal{D}| = |\{Hg : g \in G\}| = |\{Hg_1, \dots, Hg_n\}|$$

Teorema di Lagrange

Ipotesi: G finito $\Rightarrow |H| < \infty$.

Tesi: $|G| = [G: H] \cdot |H|$.

$[G: H] = |\mathcal{S}| = m < \infty$ perché $\mathcal{S} \subseteq \mathcal{P}(G)$

$\mathcal{S} = \{x_1H, x_2H, \dots, x_mH\} \xrightarrow{\mathcal{S} \text{ partizione di } G} G = \bigcup_{i=1, \dots, m} x_iH$. Notare che l'unione è disgiunta perché partizione.
 $\Rightarrow |G| = \sum_{i=1}^m |x_iH| = \sum_{i=1}^m |H|$ a causa del lemma visto sopra.
 $= m \cdot |H| = [G:H] \cdot |H|$

I sottogruppi hanno cardinalità che divide $|G|$: $|H|$ divide $|G|$ (corollario).

Permutazioni

Gruppo delle permutazioni su X

Sia X un insieme $\neq \emptyset$.

$S_X := \{f \text{ biettiva} | f: X \rightarrow X\}$

(S_X, \circ) è un gruppo (non abeliano) dove \circ è la composizione di funzioni.

L'elemento neutro è $1_{S_X} := id$. = funzione identità

$\forall f \in S_X$, l'inverso di f è $f^{-1} \in S_X$.

(S_X, \circ) viene chiamato il gruppo delle permutazioni su S_X .

Supporto di f

Supporto di $f = \text{supp } f := \{x \in X | f(x) \neq x\}$.

La notazione per una permutazione è

$$f = \begin{pmatrix} 1 & \dots & n \\ f(1) & \dots & f(n) \end{pmatrix} \text{ se } f \in S_X \text{ con } |X| = n.$$

Permutazioni disgiunte

Due permutazioni f e g si dicono disgiunte se $\text{supp } g \cap \text{supp } f = \emptyset$.

Ciclo

Un ciclo di lunghezza d è una permutazione $f \in S_X$ tale che

$\text{supp } f = \{a_1, \dots, a_d\}$

$f(a_i) = a_{i+1} \forall 1 \leq i \leq d-1$

$f(a_d) = a_1$

Se f è un ciclo, denotiamo f nel modo seguente:

$$f = (a_1 \dots a_d)$$

Esempi

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \text{supp } \sigma = \{2,3\}, \sigma = (2 \ 3)$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 7 & 5 & 1 & 6 \end{pmatrix}, \text{supp } f = \{1,3,4,6,7\}, f = (1 \ 3 \ 4 \ 7 \ 6)$$

Prodotto di cicli disgiunti

Si noti che ogni permutazione di S_X si scrive in modo unico come prodotto di cicli disgiunti.

Esempio

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix}, f = (1 \ 2), g = (3 \ 4), h = (5 \ 6), \sigma = f \circ g \circ h \text{ poiché disgiunte.}$$

Trasposizione

Un ciclo di lunghezza 2 si chiama trasposizione.

Ogni ciclo si può scrivere come prodotti di trasposizioni (non disgiunte), infatti

$$\begin{aligned} (a_1 \ \dots \ a_d) &= \\ &= (a_1 \ a_d) \cdot (a_1 \ a_{d-1}) \cdot \dots \cdot (a_1 \ a_2) = \\ &= (a_d \ a_1) \cdot (a_d \ a_2) \cdot \dots \cdot (a_d \ a_{d-1}). \end{aligned}$$

Ogni permutazione si può scrivere come prodotto di trasposizioni (non disgiunte).

Esempio

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 9 & 3 & 4 & 8 & 1 & 5 & 7 \end{pmatrix}$$

$\sigma = (1 \ 2 \ 6 \ 8 \ 5 \ 4 \ 3 \ 9 \ 7)$ come prodotto di cicli disgiunti.

$\sigma = (1 \ 7) \cdot (1 \ 9) \cdot (1 \ 3) \cdot (1 \ 4) \cdot (1 \ 5) \cdot (1 \ 8) \cdot (1 \ 6) \cdot (1 \ 2)$ come prodotto di trasposizioni.

Anelli

Anello

Un anello è una terna $(A, +, \cdot)$ dove A è un insieme e $+$ e \cdot sono operazioni binarie su A che verificano le seguenti proprietà:

- A1) La coppia $(A, +)$ è un gruppo abeliano con elemento neutro 0 .
- A2) L'operazione \cdot è associativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- A3) Vale la proprietà distributiva.

Divisori dello zero

Un "divisore sinistro dello 0" è un $a \in A, a \neq 0 \mid \exists b \neq 0, b \in A, a \cdot b = 0$.

Analogamente viene definito il "divisore destro dello 0".

In \mathbb{Z}_n è facile trovarne esempi:

Siano $a, b \in \mathbb{Z}_6, a = \bar{3}, b = \bar{2}$, infatti $\bar{3} \cdot \bar{2} = \overline{3 \cdot 2} = \bar{6} = \bar{0}$.

Prodotto diretto di anelli

Siano A e B anelli. Prendo i gruppi abeliani $(A, +)$ e $(B, +)$ e considero il prodotto diretto $A \times B$.

Su $A \times B$ definisco \cdot nel modo seguente:

$$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$$

con $a, a' \in A, b, b' \in B$.

$(A \times B, +, \cdot, (0_A, 0_B))$ è un anello chiamato prodotto diretto di A e B .

Se A e B sono anelli unitari allora $(1_A, 1_B)$ è l'unità di $A \times B$.

Varietà e discendenti degli anelli

Un **anello unitario** (o **anello con identità**) possiede l'elemento neutro per l'operazione \cdot .

Un **anello commutativo** gode della proprietà commutativa sull'operazione \cdot .

Un **anello integro** è un anello unitario privo di divisori destri e sinistri dello zero.

Un **dominio [di integrità]** è un anello integro commutativo:

$\forall a, b, a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ (come in $\mathbb{N}, \mathbb{Z}, \mathbb{R}$).

Un **corpo**, o **anello con divisore**, è un anello unitario dove tutti gli elementi non nulli sono invertibili.

Un **campo** è un corpo commutativo, ovvero un anello unitario in cui vale la proprietà commutativa ed esiste l'inverso di ogni elemento diverso da zero.

Ogni campo è un dominio di integrità (teorema).

Esempio

Un esempio di anello commutativo unitario che non è un dominio è

$$\mathbb{Z}_6: \bar{2} \cdot \bar{3} = \bar{6} = \bar{0} \quad \text{ma } \bar{2} \neq \bar{0} \neq \bar{3}$$

$$(\mathbb{Z} \times \mathbb{Z}, +, \cdot): (a, b) + (c, d) = (a + c, b + d) \Rightarrow (a, b) \cdot (c, d) = (a \cdot c, b \cdot d) \Rightarrow (1, 0)(0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$$

Esempio

Un esempio di anello commutativo con identità con un ideale non banale (vedi § "Ideale") è \mathbb{Z} anello,

$n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ ideale:

$ab \in I \forall a \in A, b \in I \Rightarrow n \cdot rz \in n\mathbb{Z}$ poiché.

La dimostrazione sull'ideale destro non serve poiché l'anello \mathbb{Z} è commutativo.

Ideale

Sia A un anello, $I \subseteq A$.

I si dice

- ideale sinistro se $I \leq (A, +), a \cdot b \in I \quad \forall a \in A, b \in I$.
- ideale destro se $I \leq (A, +), b \cdot a \in I \quad \forall a \in A, b \in I$.
- ideale [bilatero] se è sia ideale destro che sinistro.

$\{0\}, A$ sono gli ideali bilateri banali di A .

Anello quoziente

Sia $(A, +, \cdot)$ anello. Sia I un ideale bilatero di A .

Considero il gruppo $(A, +)$. So che $I \trianglelefteq (A, +)$, quindi posso fare il gruppo quoziente $(A/I, +)$.

Su $(A/I, +)$ definisco l'operazione \cdot in questo modo:

$$(x + I) \cdot (y + I) = xy + I$$

Dunque $(A/I, +, \cdot)$ risulta un anello, detto anello quoziente.

L'elemento neutro è $1 + I$.

Un esempio particolare di anello quoziente è $(\mathbb{Z}/m\mathbb{Z}, +, \cdot) = (\mathbb{Z}_m, +, \cdot)$.

Omomorfismo di anelli

Siano A, B due anelli.

$\varphi: A \rightarrow B$ è un omomorfismo se

$$\begin{aligned}\varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \quad \forall a \in A, b \in B \\ \varphi(a + b) &= \varphi(a) + \varphi(b) \quad \forall a \in A, b \in B\end{aligned}$$

Se φ è biettiva si dice isomorfismo.

L'insieme degli omomorfismi si dice:

$$\text{hom}(G, H) := \{\varphi: G \rightarrow H \mid \varphi \text{ omorfismo}\}$$

Il nucleo di φ è così definito:

$$\ker(\varphi) = \{a \in A \mid \varphi(a) = 0_B\}$$

Si noti che φ iniettiva $\Leftrightarrow \ker(\varphi) = \{0_A\}$.

Gli omomorfismi di anelli godono delle seguenti proprietà:

- $\varphi(0_A) = 0_B$
- $\ker(\varphi)$ è un ideale bilatero di A .

Teorema: gli unici ideali di un campo sono banali

$$\mathbf{1_R \in I \Rightarrow I = R}$$

Sia R anello unitario, I ideale di R .

Tesi: $1_R \in I \Rightarrow I = R$.

$I \subseteq R$ è vera per definizione.

$I \supseteq R$: Sia $r \in R$.

$$r \cdot 1_R \in I = r$$

$$1_R \cdot r \in I = r.$$

$u \in I \Rightarrow I = R$

R anello unitario

I ideale di R

Se I contiene un elemento invertibile $\Rightarrow I = R$.

Suppongo che I sia ideale destro. L'ipotesi diventa $b \cdot a \in I \forall a \in R, b \in I$.

I contiene un elemento invertibile $:= u$.

$1_R \in I \Rightarrow I = R$.

$u \in I$ per ipotesi $\Rightarrow u^{-1} \in R \Rightarrow u \cdot u^{-1} \in I \Rightarrow 1_R \in I \Rightarrow I = R$.

Gli unici ideali di un campo sono banali

Sia I ideale di C con C campo.

Tesi: $I \neq \{1_C\} \Rightarrow I = C$.

$\exists x \neq 1_C \mid x \in I$

$I \subseteq C$ perché tutti gli elementi sono invertibili $\Rightarrow x$ invertibile (perché $x \in I$) $\Rightarrow I = R$.

Spazi vettoriali

Spazio vettoriale

Sia $(V, +)$ un gruppo abeliano, \mathbb{K} un campo, che solitamente è generico o $(\mathbb{R}, +, \cdot)$ o $(\mathbb{C}, +, \cdot)$.

Sia $\sigma: \mathbb{K} \times V \rightarrow V$ una funzione

$$(k, v) \mapsto k \cdot v$$

tale che, $\forall k_1, k_2 \in \mathbb{K}, v_1, v_2 \in V$, vale:

- $(k_1 + k_2) \cdot v = k_1 \cdot v + k_2 \cdot v$
- $k \cdot (v_1 + v_2) = k \cdot v_1 + k \cdot v_2$
- $(k_1 \cdot k_2) \cdot v = k_1 \cdot (k_2 \cdot v)$
- $1_{\mathbb{K}} \cdot v_1 = v_1$

La tripla $(V, +, \sigma)$ si dice spazio vettoriale sul campo $\mathbb{K} = V$ s. v. su \mathbb{K} .

Gli elementi di V si dicono vettori.

Gli elementi di \mathbb{K} si dicono scalari.

Si noti che uno spazio vettoriale contiene lo 0.

Si noti che se V s. v. su \mathbb{K} ,

0_V l'elemento neutro di V , chiamato vettore nullo,

$0_{\mathbb{K}}$ l'elemento neutro di \mathbb{K} , allora:

- $k \cdot 0_V = 0_V$
- $0_{\mathbb{K}} \cdot v = 0_V$
- $(-k) \cdot v = -(k \cdot v) = k \cdot (-v)$
- $k \cdot v = 0_V \Leftrightarrow k = 0_{\mathbb{K}} \vee v = 0_V$

Sottospazio vettoriale

Un sottospazio vettoriale è un sottoinsieme W tale che

- SSV1) $(W, +) \leq (V, +)$ nel senso di sottogruppo
- SSV2) $\forall k \in \mathbb{K}, \forall w \in W \Rightarrow k \cdot w \in W$

Si noti che $0_V \in W$ in quanto $W \leq V$.

Identificherò un sottospazio vettoriale con $W < V$ (questa notazione viene usata solo in questi appunti).

Si noti che come conseguenza W s. v. su \mathbb{K} .

Si noti che se V s. v. su \mathbb{K} , $W < V, U < V \Rightarrow (W \cap U) < V$.

Si noti che, visto che uno spazio vettoriale deve contenere 0, se V s. v. su \mathbb{K} , $W < V$, $W \setminus V$ non può essere uno spazio vettoriale poiché non contiene lo 0.

Sottospazio generato da X

Sia $X \subseteq V$, il sottospazio generato da X è così definito:

$$\langle X \rangle := \bigcap_{\substack{W \leq V \\ W \ni X}} W$$

Ovvero faccio l'intersezione per avere il più piccolo dei sottospazi poiché il più piccolo è contenuto in tutti i sottospazi possibili.

Osserviamo infatti che $\langle X \rangle$ è il più piccolo sottospazio di V contenente X . Vedi ad esempio “Figura 1) Es. $\langle X \rangle$ in \mathcal{R}^2 ” dove il vettore è $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ e la retta è $\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rangle$.

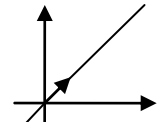


Figura 1) Es. $\langle X \rangle$ in \mathcal{R}^2

Notiamo che se

$X = \{v_1, v_2, \dots, v_n\} \subseteq V \Rightarrow \langle X \rangle = \langle v_1, v_2, \dots, v_n \rangle = \{a_1 v_1 + a_2 v_2 + \dots + a_n v_n \mid a_1, a_2, \dots, a_n \in \mathbb{K}\}$,
 ovvero l'insieme delle combinazioni lineari dei vettori di X .

Sistema di generatori

Sia V s. v. su \mathbb{K} , $X = \{v_1, v_2, \dots, v_n\} \subseteq V$, allora se vale

$$\langle X \rangle = \langle \{v_1, v_2, \dots, v_n\} \rangle = V$$

si dice che $X = \{v_1, \dots, v_n\}$ è un sistema di generatori di V .

Osserviamo quindi che

$$\begin{aligned} \langle v_1, \dots, v_n \rangle = \{ \alpha_1 v_1 + \dots + \alpha_n v_n \mid \alpha_1, \dots, \alpha_n \in K \} = V &\Leftrightarrow \\ \forall v \in V \exists \alpha_1, \dots, \alpha_n \in K \mid v = \alpha_1 v_1 + \dots + \alpha_n v_n & \end{aligned}$$

ovvero che ogni vettore di V è combinazione lineare a coefficienti in \mathbb{K} dei vettori di $X = \{v_1, v_2, \dots, v_n\} \subseteq V$, ovvero che con X posso generare tutti i vettori di V .

Vettori linearmente indipendenti

Sia V s. v. su \mathbb{K} .

Siano v_1, \dots, v_n vettori di V .

v_1, \dots, v_n si dicono linearmente indipendenti se

$$\begin{aligned} \forall a_1, \dots, a_n \in \mathbb{K} \text{ si ha} \\ a_1 v_1 + \dots + a_n v_n = 0_V \Rightarrow a_1 = \dots = a_n = 0 \end{aligned}$$

Altrimenti si dicono linearmente dipendenti quando non sono linearmente indipendenti, ossia quando

$$\exists a_1, \dots, a_n \in \mathbb{K} \text{ non tutti } = 0_{\mathbb{K}} \mid a_1 v_1 + \dots + a_n v_n = 0_V$$

Base

Sia V s. v. su \mathbb{K} e $X = \{v_1, \dots, v_n\} \subseteq V$.

X si dice base di V se

B1) $\langle X \rangle = V$, ossia X è un sistema di generatori di V .

B2) v_1, \dots, v_n linearmente indipendenti, ovvero tolgo i vettori che non mi servono.

Le basi si indicano con le lettere corsive maiuscole.

Esempio

$\mathcal{A} := \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \right\}$ non è una base perché i suoi vettori non sono linearmente indipendenti,

infatti $\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$ è combinazione lineare degli altri, in particolare $2 \cdot e_1 + 0 \cdot e_2 + 0 \cdot e_3 = 0$, quindi se voglio

formare una base lo tolgo perché non serve.

Teorema di completamento della base

Sia V s. v. su \mathbb{K} di dimensione finita, $\dim V = n$ (vedi § “Dimensione di uno spazio vettoriale (**dim** V)”)

Siano w_1, \dots, w_k vettori linearmente indipendenti di V , con $k \leq n$.

Sono possibili due casi:

- a) $k = n \Rightarrow w_1, \dots, w_k$ è una base di V ,
oppure
- b) $\exists w_{k+1}, \dots, w_n$ vettori di V tali che $w_1, \dots, w_k, w_{k+1}, \dots, w_n$ è una base di V .

Base canonica (\mathcal{E}_n)

Siano

$$\begin{aligned} e_1 &= \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ \boxed{1} & & & & & \end{pmatrix} \\ e_2 &= \begin{pmatrix} 0 & 1 & \dots & \dots & \dots & 0 \\ & \boxed{1} & & & & \end{pmatrix} \\ e_i &= \begin{pmatrix} 0 & \dots & \dots & 1 & \dots & 0 \\ & & & \boxed{1} & & \end{pmatrix} \\ e_n &= \begin{pmatrix} 0 & \dots & \dots & \dots & \dots & 1 \\ & & & & & \boxed{1} \end{pmatrix} \end{aligned}$$

$\mathcal{E}_n := \{e_1, \dots, e_n\}$ è un sistema di generatori per $\mathbb{K}^n := \underbrace{\mathbb{K} \cdot \mathbb{K} \cdot \dots \cdot \mathbb{K}}_n$ ed è detta base canonica.

Dimensione di uno spazio vettoriale (**dim** V)

Sia V s. v. su \mathbb{K} , sia $\mathcal{B} = \{v_1, \dots, v_n\}$ una base di V .

Si dice che V ha dimensione n e si scrive $\dim V = n$.

Se ne deduce che tutte le basi di un determinato spazio hanno la stessa cardinalità.

Teorema di Grassmann

Sia V s. v. su \mathbb{K} , $\dim(V) < \infty$, $U \leq V$, $W \leq V$.

Tesi:

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$$

Dimostrazione:

Sia x_1, \dots, x_k una base di $(U \cap W)$.

Per il teorema di completamento della base $\exists u_1, \dots, u_t$ vettori $| x_1, \dots, x_k, u_1, \dots, u_t$ sia una base di U .

Analogamente $\exists w_1, \dots, w_s$ vettori $| x_1, \dots, x_k, w_1, \dots, w_s$ sia una base di W .

Per ora abbiamo $\dim(U \cap W) = k$, $\dim(U) = k + t$, $\dim(W) = k + s$.

La tesi diventa: $\dim(U + W) = (k + t) + (k + s) - k = k + t + s$.

Noi dimostreremo che $\mathcal{B} = \{x_1, \dots, x_k, u_1, \dots, u_t, w_1, \dots, w_s\}$ è una base di $U + W$.

a) Dimostriamo che generano $U + W$: $\langle \mathcal{B} \rangle = U + W$.

i. $\langle \mathcal{B} \rangle \subseteq U + W$

$\langle \mathcal{B} \rangle =$

$$= \left\{ \underbrace{a_1 \cdot x_1 + \dots + a_k \cdot x_k}_{\in U \cap W} + \underbrace{b_1 \cdot u_1 + \dots + b_t \cdot u_t}_{\in U} + \underbrace{c_1 \cdot w_1 + \dots + c_s \cdot w_s}_{\in W} \mid \begin{array}{l} a_1, \dots, a_k \in K \\ b_1, \dots, b_t \in K \\ c_1, \dots, c_s \in K \end{array} \right\}$$

$\Rightarrow \langle \mathcal{B} \rangle \subseteq U + W$

ii. $\langle \mathcal{B} \rangle \supseteq U + W$

Siano $u \in U, w \in W$.

Considero $(u + w) \in (U + W)$ e voglio dimostrare che $u + w \in \langle \mathcal{B} \rangle$.

$u \in U \Rightarrow \exists a_1, \dots, a_k, b_1, \dots, b_t \in \mathbb{K} \mid u = \sum_{i=1}^k a_i x_i + \sum_{i=1}^t b_i u_i$

$w \in W \Rightarrow \exists c_1, \dots, c_k, d_1, \dots, d_s \in \mathbb{K} \mid w = \sum_{i=1}^k c_i x_i + \sum_{i=1}^s d_i w_i$

Quindi $u + w = \sum_{i=1}^k (a_i + c_i) x_i + \sum_{i=1}^t b_i u_i + \sum_{i=1}^s d_i w_i$

b) Dimostriamo che i vettori di \mathcal{B} sono linearmente indipendenti.

$\sum_{i=1}^k a_i x_i + \sum_{i=1}^t b_i u_i + \sum_{i=1}^s c_i w_i = 0 \Rightarrow$ voglio dimostrare che i coefficienti sono uguali a 0.

$\sum_{i=1}^k a_i x_i + \sum_{i=1}^t b_i u_i = - \underbrace{\sum_{i=1}^s c_i w_i}_{\in W} \Rightarrow$

$\underbrace{\sum_{i=1}^k a_i x_i + \sum_{i=1}^t b_i u_i}_{\in U} \in W$

$\sum_{i=1}^k a_i x_i + \sum_{i=1}^t b_i u_i \in U \cap W \Rightarrow$

$\exists d_1, \dots, d_k \in \mathbb{K} \mid \sum_{i=1}^k a_i x_i + \sum_{i=1}^t b_i u_i = \sum_{i=1}^k d_i x_i \Rightarrow$

$\sum_{i=1}^k (a_i - d_i) x_i + \sum_{i=1}^t b_i u_i = 0 \xRightarrow{x_1, \dots, x_k, u_1, \dots, u_t \text{ è una base di } U}$

$b_i = 0 \forall i = 1, \dots, t$

Sostituendo b_i con la combinazione lineare di \mathcal{B} si ottiene:

$\sum_{i=1}^k a_i x_i + \sum_{i=1}^s c_i w_i = 0 \xRightarrow{x_1, \dots, x_k, w_1, \dots, w_s \text{ base di } W} \begin{array}{l} a_i = 0 \forall i = 1, \dots, k, \\ c_i = 0 \forall i = 1, \dots, s. \end{array}$

Spazio quoziente

Sia V s. v. su $\mathbb{K}, W \leq V$.

Lo spazio quoziente è così definito: $V/W \stackrel{\text{def.}}{=} \{v + W \mid v \in V\}$.

L'operazione "prodotto per uno scalare" è così definita:

$$k(v + W) = kv + W$$

V/W risulta quindi uno spazio vettoriale.

Dimensione dello spazio quoziente

Sia uno spazio quoziente di V su W con V s. v. su \mathbb{K} e $W \leq V$.

$$\dim V/W = \dim V - \dim W$$

Dimostrazione:

Sia $\{w_1, \dots, w_k\}$ base di W .

Sia $\{w_1, \dots, w_k, v_{k+1}, \dots, v_n\}$ base di V per il teorema di completamento della base.

$$\Rightarrow \dim V/W = n - k.$$

Voglio quindi dimostrare che $\mathcal{A} = \{v_{k+1} + W, \dots, v_n + W\}$ è base di V/W .

B1) Tesi: $\langle \mathcal{A} \rangle = V/W$

Sia $v + W \in V/W$.

$$v + W = \underbrace{a_1 w_1 + \dots + a_k w_k}_{\in W} + a_{k+1} w_{k+1} + \dots + a_n v_n + W \Rightarrow$$

$\Rightarrow \in$ alla classe laterale

$$\Rightarrow v + W = a_{k+1} v_{k+1} + \dots + a_n v_n + W \Rightarrow$$

$$\xrightarrow{\text{proprietà}} v + W = a_{k+1} (v_{k+1} + W) + \dots + a_n (v_n + W).$$

classi laterali

B2) Tesi: vettori linearmente indipendenti

Sia $v + W \in V/W$

$$a_1 w_1 + W + \dots + a_k w_k + W + a_{k+1} w_{k+1} + W + \dots + a_n v_n + W = 0 \Rightarrow$$

$$\underbrace{a_1 w_1 + \dots + a_k w_k + \dots + a_n v_n}_{\text{base di } V \Rightarrow \text{coefficienti}=0} + W = 0 \Rightarrow \text{lin.ind.}$$

base di $V \Rightarrow$ coefficienti=0

Funzione lineare

Siano V, W s. v. su \mathbb{K} .

Una funzione $f: V \rightarrow W$ si dice lineare se:

$$\text{FL1)} \quad f(v_1 + v_2) = f(v_1) + f(v_2)$$

$$\text{FL2)} \quad \forall k \in \mathbb{K}, \forall v \in V, f(k \cdot v) = k \cdot f(v)$$

Si noti che f si “comporta bene” rispetto alle combinazioni lineari:

$$f(a_1 v_1 + \dots + a_n v_n) = a_1 \cdot f(v_1) + \dots + a_n \cdot f(v_n).$$

Si noti quindi che tutte le funzioni lineari “passano” per lo 0 (segue da FL2).

Il nucleo di f viene così definito:

$$\ker f := f^{-1}(0_W) = \{v \in V | f(v) = 0_W\}$$

Si noti quindi che $\ker f \subseteq V$.

Si noti che

$$f \text{ iniettiva} \Leftrightarrow \ker f = \{0_V\}$$

Infatti:

$$\boxed{\Rightarrow} \quad |\ker f| \stackrel{\text{def. ker}}{=} |f^{-1}(0_W)| \stackrel{f \text{ iniettiva}}{=} 1 \stackrel{f \text{ lineare}}{\Rightarrow} \text{poiché } f(0_V) = 0_W \Rightarrow \ker f = \{0_V\}$$

$$\boxed{\Leftarrow} \quad \text{Ipotesi: } \ker f = \{0_V\}, \text{ la tesi è } f \text{ iniettiva, ovvero } f(v_1) = f(v_2) \Rightarrow v_1 = v_2:$$

$$f(v_1) = f(v_2) \Rightarrow 0_W = f(v_1) - f(v_2) \stackrel{f \text{ lineare}}{\Rightarrow} f(v_1 - v_2) = 0_W \Rightarrow$$

$$v_1 - v_2 \in \ker f \Rightarrow v_1 - v_2 = 0_V \Rightarrow v_1 = v_2$$

Omomorfismo di spazi vettoriali

Un omomorfismo di spazi vettoriali corrisponde ad una funzione lineare.

Un isomorfismo fra spazi vettoriali è una funzione lineare biettiva.

Teorema nullità + rango

Siano W s. v. su \mathbb{K} , V s. v. su \mathbb{K} , $\dim V < \infty$, $\dim W < \infty$, $f: V \rightarrow W$ funz. lineare \Rightarrow
 $\dim(V) = \dim(\ker f) + \dim(\text{Im } f)$

Sia $\mathcal{B} = \{v_1, \dots, v_k\}$ una base di $\ker f$.

$\ker f \subseteq V \xrightarrow{\text{Teor. compl. base}} \mathcal{B}' \supseteq \mathcal{B} \Rightarrow \exists v_{k+1}, \dots, v_n \mid \mathcal{B}' = \left\{ \underbrace{v_1, \dots, v_k}_{\text{base di } \ker f}, \underbrace{v_{k+1}, \dots, v_n}_{\in V} \right\}$ base di V .

La tesi quindi diventa $n = k + \dim(\text{Im } f) \Rightarrow$ dimostriamo che $\{f(v_{k+1}), \dots, f(v_n)\}$ è una base di $\text{Im } f$.

1. Dimostriamo che genera: $\langle f(v_{k+1}), \dots, f(v_n) \rangle = \text{Im } f$:

Sia $w \in \text{Im } f \Rightarrow \exists v \in V \mid w = f(v)$.

$\langle \mathcal{B}' \rangle = V \Rightarrow \exists a_1, \dots, a_k, a_{k+1}, \dots, a_n \in \mathbb{K} \mid v = a_1 v_1 + \dots + a_k v_k + a_{k+1} v_{k+1} + \dots + a_n v_n \Rightarrow$

Ma allora $w = f(v) = \underbrace{a_1 f(v_1) + \dots + a_k f(v_k)}_{\{v_1, \dots, v_k\} = \mathcal{B} \subseteq \ker f} + a_{k+1} f(v_{k+1}) + \dots + a_n f(v_n) \Rightarrow$

$\Rightarrow w = f(v) = 0 + a_{k+1} f(v_{k+1}) + \dots + a_n f(v_n)$.

2. Dimostriamo che $f(v_{k+1}), \dots, f(v_n)$ sono linearmente indipendenti:

$$a_{k+1} f(v_{k+1}) + \dots + a_n f(v_n) = 0 \Rightarrow f \left(\underbrace{a_{k+1} \cdot v_{k+1} + \dots + a_n \cdot v_n}_{\in \ker(f) \text{ perché } f(\dots) = 0} \right) = 0$$

$\langle \mathcal{B} \rangle = \ker f \Rightarrow \exists a_1, \dots, a_k \in \mathbb{K} \mid a_{k+1} \cdot v_{k+1} + \dots + a_n v_n = a_1 v_1 + \dots + a_k v_k \Rightarrow$

$\Rightarrow \underbrace{a_{k+1} \cdot v_{k+1} + \dots + a_n v_n - a_1 v_1 - \dots - a_k v_k}_{v_1, \dots, v_n \text{ base di } V \Rightarrow \text{linearmente indipendenti}} = 0 \xrightarrow{\mathcal{B}' \text{ base di } V} \Rightarrow$

\Rightarrow i coefficienti sono nulli. In particolare a_{k+1}, \dots, a_n sono nulli.

Matrici

Matrice

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M(m, n, \mathbb{K})$$

Le righe sono $\begin{pmatrix} a_{11} \\ \vdots \\ a_{1n} \end{pmatrix}, \dots, \begin{pmatrix} a_{m1} \\ \vdots \\ a_{mn} \end{pmatrix} \in \mathbb{K}^n$ e sappiamo che \mathbb{K}^n s. v. su \mathbb{K} .

Le colonne sono $\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} \in \mathbb{K}^m$ dove \mathbb{K}^m s. v. su \mathbb{K} .

Matrice triangolare e matrice “a gradini”

Una matrice $A \in M(m, n, \mathbb{K})$ si dice triangolare superiore se:

$$A = \begin{pmatrix} a_{11} & \cdots & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & a_{mn} \end{pmatrix}$$

Una matrice $B \in M(m, n, \mathbb{K})$ si dice triangolare inferiore se:

$$B = \begin{pmatrix} a_{11} & 0 & \cdots & \cdots & 0 \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ a_{m1} & \cdots & \cdots & \cdots & a_{mn} \end{pmatrix}$$

Una matrice a gradini è una matrice triangolare superiore.

Matrice diagonale

Una matrice $A \in M(m, n, \mathbb{K})$ si dice diagonale se:

$$A = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_{mn} \end{pmatrix}$$

Complemento algebrico

Sia $A \in M(m, n, \mathbb{K})$.

Il complemento algebrico di A_{ij} è la matrice che ottengo togliendo da A la riga i e la colonna j .

Operazioni di riga

E' possibile ottenere una matrice A' equivalente ad A eseguendo le seguenti operazioni:

1. Scambiare le righe
2. Moltiplicare una riga per uno scalare
3. Sommare (o sottrarre) una riga ad un'altra

Due matrici equivalenti $A \sim A'$ hanno lo stesso rango perché $\langle A \rangle = \langle A' \rangle$ dove con $\langle A \rangle$ intendo lo spazio generato dalle colonne, o equivalentemente lo spazio generato dalle righe di A , poiché si dimostra che sono uguali.

Prodotto matrice - vettore

Il prodotto fra una matrice ed un vettore è così definito:

$$\underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{m \times n} \cdot \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_{n \times 1} = \underbrace{\begin{pmatrix} a_{11}b_1 + \cdots + a_{1n}b_n \\ \vdots \\ a_{m1}b_1 + \cdots + a_{mn}b_n \end{pmatrix}}_{m \times 1}$$

Si noti quindi che la matrice identità risulta essere:

$$I_n = \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & & 1 \end{pmatrix}}_{n \times n}$$

Prodotto matrice – matrice

Due matrici $A \in M(n, m, \mathbb{K})$ e $B \in M(m, n, \mathbb{K})$ sono moltiplicabili solo se il numero delle colonne di A è uguale al numero delle righe di B , ovvero gli “interni” delle dimensioni delle matrici che moltiplico devono essere uguali.

La matrice risultante avrà dimensione pari a righe di $A \times$ colonne di B , ossia gli “esterni” delle dimensioni che moltiplico.

$$\underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{m \times n} \cdot \underbrace{\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}}_{n \times m} = \underbrace{\begin{pmatrix} a_{11}b_{11} + \cdots + a_{1n}b_{n1} & \cdots & a_{11}b_{1n} + \cdots + a_{1n}b_{nn} \\ \vdots & \ddots & \vdots \\ a_{m1}b_{11} + \cdots + a_{mn}b_{n1} & \cdots & a_{m1}b_{1n} + \cdots + a_{mn}b_{nn} \end{pmatrix}}_{m \times m}$$

Rango

Il rango di una matrice M è la dimensione dello spazio generato dalle righe o dalle colonne:

$$\text{rg } M = \dim \left\langle \underbrace{\begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1n} \end{pmatrix}, \dots, \begin{pmatrix} a_{m1} \\ a_{m2} \\ \vdots \\ a_{mn} \end{pmatrix}}_{\langle \mathbb{K}^n \rangle} \right\rangle = \dim \left\langle \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} \right\rangle$$

In verità questo è un teorema che segue dalla definizione, che non si è vista durante il corso.

Inoltre posso fare operazioni di riga per rendere M a gradini, ovvero triangolare superiore.

In questo modo rendo le righe che sono combinazioni lineari di altre uguali a 0.

A questo punto il rango è il numero di righe diverse da 0.

Matrice trasposta

Una matrice trasposta è una matrice con righe e colonne scambiate:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \rightarrow \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix} \quad \text{Ad esempio: } \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$$

Determinante

Sia $CA(A)$ il complemento algebrico di a .

$$\text{Sia } A \in M(n, n, \mathbb{K}), A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

Si sceglie una riga o una colonna (preferibilmente con molti 0).

Scegliendo ad esempio la prima riga, $\det(A) = a_{11} \cdot \det CA(a_{11}) - a_{12} \cdot \det CA(a_{12}) + \dots - a_{1n} \cdot \det CA(a_{1n})$, dove si mette il segno + al primo elemento della riga (o colonna), - al secondo e così via.

Esempio: determinante matrice 3×3

Ad esempio:

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} := \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \cdot \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \cdot \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}.$$

Esempio: determinante matrice 2×2

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} := a_{11} \cdot a_{22} - a_{12} \cdot a_{21}.$$

Matrice inversa

Sia \mathbb{K} un campo, $A \in M(n, n, \mathbb{K})$. Si noti che la matrice deve essere quadrata.

A si dice invertibile se $\exists B \in M(n, n, \mathbb{K}) \mid A \cdot B = B \cdot A = I_n$.

Si noti che A invertibile $\Leftrightarrow \det(A) \neq 0$.

Per calcolare l'inversa della matrice $A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ si usa questa procedura:

1. Calcolo $\det(A)$. Se è 0, non è invertibile.

$$\det(A) = \det \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = 1 \cdot \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} - 0 \cdot \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} + 1 \cdot \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} = 1 + 2 - 1 = 2$$

2. Calcolo la matrice dei determinanti dei complementi algebrici.

$$A' = \begin{pmatrix} \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} \\ \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \\ \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} & \begin{vmatrix} 1 & 1 \\ 2 & 0 \end{vmatrix} & \begin{vmatrix} 1 & 0 \\ 2 & 1 \end{vmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \\ -1 & -2 & 1 \end{pmatrix}$$

3. Traspongo la matrice.

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

4. Distribuisco i segni a scacchiera.

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

5. Divido ciascun elemento per il determinante di A .

$$A^{-1} = \begin{pmatrix} 1/2 & 1/2 & -1/2 \\ -1 & 0 & 1 \\ 1/2 & -1/2 & 1/2 \end{pmatrix}$$

Sistemi lineari

Sistema lineare

Un sistema lineare con m equazioni ed n incognite (x_1, \dots, x_n) è così definito:

$$\mathcal{S}: \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases} \text{ con } a_{ij} \in \mathbb{R} \forall i = 1, \dots, m, \forall j = 1, \dots, n \\ \text{con } b_i \in \mathbb{R} \forall i = 1, \dots, m$$

\mathcal{S} si dice omogeneo se $b_1 = b_2 = \dots = b_m = 0$, ovvero i termini noti sono uguali a 0.

Il sistema omogeneo associato ad \mathcal{S} è il sistema \mathcal{S} con $b_1 = b_2 = \dots = b_m$ posti = 0.

L'insieme delle possibili matrici valorizzate è definito così:

$$M(m, n, \mathbb{K}) := \{ \text{matrici di } m \text{ righe, } n \text{ colonne, a coefficienti in } \mathbb{K} \}$$

Il sistema \mathcal{S} si rappresenta con:

$$A \in M(m, n, \mathbb{K}), A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \text{ che è la matrice associata al sistema}$$

$$B \in M(m, 1, \mathbb{K}), B := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \text{ che è la colonna dei termini noti}$$

$$X \in M(n, 1, \mathbb{K}), X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^n, \text{ che è il vettore delle incognite}$$

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ è la soluzione di } \mathcal{S} \stackrel{\text{def}}{\Leftrightarrow} A \cdot X = B$$

$$(A \ B) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix} \text{ è detta "matrice completa del sistema".}$$

L'insieme delle soluzioni del sistema è così definito:

$$\text{sol}(\mathcal{S}) := \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \text{sono verificate tutte le equazioni del sistema}\} \text{ con } \text{sol}(\mathcal{S}) \subset \mathbb{R}^n$$

Si noti che se il sistema \mathcal{O} è omogeneo, le sue soluzioni sono sottospazi di \mathbb{K}^n s. v. su \mathbb{K} :

$$\text{sol}(\mathcal{O}) < \mathbb{K}^n \text{ s. v. su } \mathbb{K}$$

Si noti che se $\det(A) = 0$, la matrice non ha rango massimo e quindi i vettori della matrice sono linearmente dipendenti.

Al contrario, se $\det(A) \neq 0$, la matrice ha rango massimo e quindi i vettori della matrice (le righe o le colonne) sono linearmente indipendenti.

Funzione lineare associata alla matrice

Sia $A \in M(m, n, \mathbb{K})$, v un vettore $\in \mathbb{K}^n$, considero la funzione lineare associata alla matrice A : ℓ_A :

$$\ell_A: \mathbb{K}^n \rightarrow \mathbb{K}^m \\ \underbrace{v}_{(n,1)} \mapsto \underbrace{A}_{(m,n,\mathbb{K})} \cdot \underbrace{v}_{(n,1)} \\ \underbrace{\hspace{10em}}_{(m,1)}$$

$$\ell_{A(v)} := A \cdot v$$

Si noti che

$$\dim(\ker \ell_A) = n - \dim(\text{Im } \ell_A) \Rightarrow \dim(\text{sol } \mathcal{S}) = n - \text{rg}(A)$$

Dimostrazione: sia $\mathcal{E}_n = \{e_1, \dots, e_n\}$ la base canonica di $\mathbb{K}^n \Rightarrow \langle \ell_A(e_1), \dots, \ell_A(e_n) \rangle = \text{Im } (\ell_A) \Rightarrow$
es.visto $\underbrace{\langle \ell_A(e_1), \dots, \ell_A(e_n) \rangle}_{\langle 1^\circ \text{ colonna}, \dots, n^\circ \text{ colonna} \rangle}$

$$\Rightarrow \dim(\text{Im } \ell_A) \underset{=\text{rg}(A)}{=} \dim(\langle 1^\circ \text{ colonna}, \dots, n^\circ \text{ colonna} \rangle) \Rightarrow$$

\Rightarrow considero il sistema lineare associato ad $A := \mathcal{S}$.

$$\text{sol}(\mathcal{S}) = \{X \in \mathbb{K}^n \mid A \cdot X = 0_{\mathbb{K}^m}\} = \ker(\ell_A).$$

Siano V, W s. v. su \mathbb{K} , $f: V \rightarrow W$ una funzione lineare, allora applicando il teorema

$$\dim(U) = \dim(\ker f) + \dim(\text{Im } f) \text{ nel caso } V = \mathbb{K}^n \text{ si ottiene: } \dim(\ker \ell_A) = n - \dim(\text{Im } \ell_A) \Rightarrow \dim(\text{sol } \mathcal{S}) = n - \text{rg}(A).$$

Coordinate di un vettore

Sia V s. v. su \mathbb{K} , \mathcal{A} base di V , $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\}$, $v \in V$.

Le coordinate del vettore v nella base \mathcal{A} sono

$$[v]_{\mathcal{A}} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \in \mathbb{K}^n \stackrel{\text{def.}}{\Leftrightarrow} v = a_1 \alpha_1 + \dots + a_n \alpha_n$$

Matrice di una funzione lineare e coordinate di un vettore

Siano V, W s. v. su \mathbb{K} ,

$f: V \rightarrow W$ funzionale lineare,

$\mathcal{A} = (\alpha_1, \dots, \alpha_n)$ base di V .

$\mathcal{B} = (\beta_1, \dots, \beta_m)$ base di W .

$M_{\mathcal{B} \mathcal{A}}$ è la matrice di f rispetto alla base \mathcal{A} e \mathcal{B} :

$$M_{\mathcal{A} \mathcal{B}}(f) \stackrel{\text{def.}}{=} ([f(v_1)]_{\mathcal{B}} \quad \dots \quad [f(v_n)]_{\mathcal{B}})$$

Ovvero $M_{\mathcal{A} \mathcal{B}}(f) = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \stackrel{\text{def.}}{\Leftrightarrow} \begin{cases} f(\alpha_1) = a_{11} \cdot \beta_1 + \dots + a_{m1} \cdot \beta_m \\ \vdots \\ f(\alpha_n) = a_{1n} \cdot \beta_1 + \dots + a_{mn} \cdot \beta_m \end{cases}$

coefficienti della
combinazione lineare

Con la notazione $M_{\mathcal{B}}(f)$ indicheremo la funzione $M_{\mathcal{B} \mathcal{B}}(f)$.

Notiamo quindi che se $f: V \rightarrow W$ funzione lineare, $\mathcal{A} = \{\alpha_1, \dots, \alpha_n\}$ base di V , allora f è completamente identificata da $f(\alpha_1), \dots, f(\alpha_n)$ perché $\forall v \in V$, v è combinazione lineare dei vettori di \mathcal{A} :

$$\text{Sia } v = a_1 \alpha_1 + \dots + a_n \alpha_n \Rightarrow \text{conosco } f(v) \text{ perché } f(v) = a_1 f(\alpha_1) + \dots + a_n f(\alpha_n)$$

Questo si collega al teorema di estensione per linearità (non trattato in questi appunti).

Teorema di Rouché – Capelli

Sia (A, B) un sistema lineare. Sia $(A \ B)$ l'unione fra A e B : $\begin{pmatrix} a & \cdots & a & b \\ \vdots & \ddots & \vdots & \vdots \\ a & \cdots & a & b \end{pmatrix}$.

$$(A, B) \text{ ha soluzione} \Leftrightarrow \text{rg}(A \ B) = \text{rg}(A)$$

Il sistema (A, B) ha soluzione \Leftrightarrow la colonna B (dei termini noti) appartiene al sottospazio generato dalle colonne di A , ossia $B \in \langle \underbrace{A^1, \dots, A^n}_{\text{colonne}} \rangle \subset \mathbb{K}^m$ dove $\underbrace{(A^1 \ \dots \ A^n)}_{\text{colonne}} = A$.

$$\begin{aligned} \text{Il sistema } \left(\underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_A, \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}}_B \right) \text{ ha soluzione} &\Leftrightarrow \\ \Leftrightarrow \exists t_1, \dots, t_n \in \mathbb{K} \mid A \cdot \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = B &\Leftrightarrow \begin{pmatrix} a_{11}t_1 + \cdots + a_{1n}t_n \\ \vdots \\ a_{m1}t_1 + \cdots + a_{mn}t_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \Leftrightarrow \\ \Leftrightarrow t_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + t_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} + \cdots + t_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} &\Leftrightarrow \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ combinazione lineare di } A \Leftrightarrow \\ \Leftrightarrow \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \langle \underbrace{A^1, \dots, A^n}_{\text{colonne di } A} \rangle &\Leftrightarrow B \in \langle A^1, \dots, A^n \rangle \Leftrightarrow \langle A^1, \dots, A^n, B \rangle = \langle A^1, \dots, A^n \rangle \Leftrightarrow \\ \Leftrightarrow \dim \langle A^1, \dots, A^n, B \rangle = \dim \langle A^1, \dots, A^n \rangle &\Leftrightarrow \text{rg}(A \ B) = \text{rg}(A). \end{aligned}$$

Metodo per risolvere i sistemi lineari

Sia A la matrice del sistema lineare e sia λ il parametro che compare nella matrice.

Sia B il vettore dei termini noti.

$$A = \begin{pmatrix} 1 - \lambda & 1 & \lambda - 1 \\ 2\lambda - 2 & 6 - 2\lambda & 2 \\ 0 & 2 - \lambda & 0 \end{pmatrix}, B = \begin{pmatrix} 3 \\ 3\lambda \\ 0 \end{pmatrix}.$$

- Calcolare il determinante di A . Il risultato che otterrà sarà ovviamente in funzione di λ .
In particolare otterremo che per $\lambda \in \{1, 2\}$ la matrice ha determinante = 0, e pertanto non ha soluzioni o ha più di una soluzione, questi due valori vengono chiamati "casi critici".
Per $\lambda \in \mathbb{R} / \{1, 2\}$, invece, $\det(A) \neq 0$ e pertanto $(A \ B)$ ha una soluzione.
Infatti A è invertibile, quindi la soluzione si ottiene moltiplicando $AX = B$ per A^{-1} a sinistra, da cui $IX = A^{-1}B$, dunque la soluzione (unica) è data da $X = A^{-1}B$.
- Per i casi critici (nel nostro caso 1 e 2) sostituisco λ nel sistema e studio il determinante

Autovalore e autovettore

Sia V s. v. su \mathbb{K} ,

$f: V \rightarrow V$ funzione lineare.

- $d \in \mathbb{K}$ si dice autovalore di f se $\exists \alpha \in V, \alpha \neq 0_V \mid f(\alpha) = d \cdot \alpha$.

- $\alpha \in V$ si dice autovettore di f se $\alpha \neq 0_V \wedge \exists d \in \mathbb{K} \mid f(\alpha) = d \cdot \alpha$.

Se $f(\alpha) = d \cdot \alpha$ si dice che d è l'autovalore relativo all'autovettore α .

Teorema

\exists una base di V tale che la matrice associata ad f sia diagonale \Leftrightarrow
 $\Leftrightarrow \exists$ una base di V i cui elementi siano autovettori di f

Osservazione

α autovettore relativo all'autovalore 0 $\Leftrightarrow f(\alpha) = 0 \cdot \alpha = 0 \Leftrightarrow \alpha \in \ker(f)$
 ma $\alpha \neq 0_V$ perché autovettore $\Leftrightarrow \ker(f) \neq \{0_V\} \Leftrightarrow f$ non è iniettiva

Teorema

Siano $\mathcal{V} = \{v_1, \dots, v_n\}$, $\mathcal{W} = \{w_1, \dots, w_n\}$ due basi di V .
 Sia $A_{\mathcal{V}\mathcal{V}}$ la matrice associata ad f rispetto alla base $\mathcal{V} \Rightarrow$
 $\Rightarrow \exists$ una matrice invertibile B tale che $A_{\mathcal{V}\mathcal{V}} = B^{-1}A_{\mathcal{W}\mathcal{W}}B$

Polinomio caratteristico di una matrice

Il polinomio caratteristico di una matrice P_A è così definito:

Sia $A \in M(n, n, \mathbb{K})$.

$$P_A := \det(A - x \cdot I_n) \in \mathbb{K}[x]$$

dove I_n è la matrice identità di dimensione n e $\mathbb{K}[x]$ è l'insieme dei polinomi con variabile x e coefficienti in \mathbb{K} .

Ad esempio se $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $P_A = \det\left(\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} - x \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \det\begin{pmatrix} 1-x & 2 \\ 3 & 4-x \end{pmatrix} = (1-x)(4-x) - 6 = x^2 - 5x - 2 \in \mathbb{R}[x]$

Funzione e matrice diagonalizzabile

Sia $f: V \rightarrow V$, f funzione lineare,
 f diagonalizzabile $\Leftrightarrow \exists \mathcal{B}$ base di $\mathbb{K}^n \mid M_{\mathcal{B}}(f)$ è diagonale.

Per trovare una matrice diagonale devo quindi trovare una base di V formata da autovettori della matrice $M_{\mathcal{B}}(f)$. Infatti sia $\mathcal{B} := (v_1, \dots, v_n)$ base di V , se v_1, \dots, v_n autovettori di $M_{\mathcal{B}}(f) \Rightarrow M_{\mathcal{B}}(f)$ è diagonale.

Teorema

Sia $f: V \rightarrow V$ funzione lineare, V s. v. su \mathbb{K} ,
 siano $\alpha_1, \dots, \alpha_r$ autovettori di f ,
 siano c_1, \dots, c_r i rispettivi autovalori.

c_1, \dots, c_r distinti $\Rightarrow \alpha_1, \dots, \alpha_r$ linearmente indipendenti

Corollario

$A \in M(n, n, \mathbb{K})$. Se A ha n autovalori distinti $(c_1, \dots, c_n) \Rightarrow A$ è diagonalizzabile, ovvero basterà prendere la base \mathcal{B} di \mathbb{K}^n formata dagli autovettori relativi agli autovalori c_1, \dots, c_n per avere che $M_{\mathcal{B}}$ è diagonale.

Esempio: Sia $A \in M(3,3, \mathbb{C})$, $A = \begin{pmatrix} 5 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & 1 & 4 \end{pmatrix}$ è diagonalizzabile?

$P_A = \det(A - x \cdot I_3) = \dots = (5 - x) \left(x^2 + \underbrace{1}_{=-i^2} \right) = (5 - x)(x + i)(x - 1) \Rightarrow P_A$ ha 3 soluzioni distinte
 \Rightarrow è diagonalizzabile poiché ha un numero massimo ($n = 3$) di autovalori distinti.

Metodo per trovare gli autovalori di una matrice e di una funzione

Per trovare gli autovalori di una matrice calcolo il polinomio caratteristico.

Sia $A \in M(m, n, \mathbb{K})$,
 $d \in \mathbb{K}$.

d autovalore di $A \stackrel{\text{def.}}{\Leftrightarrow} \exists \alpha \in \mathbb{K}^n, \alpha \neq 0 \mid f(\alpha) = d \cdot \alpha$
 quindi per le matrici vale

$$\begin{aligned} d \text{ autovalore di } A &\stackrel{\text{def.}}{\Leftrightarrow} \exists \alpha \in \mathbb{K}^n, \alpha \neq 0 \mid A \cdot \alpha = \underbrace{d}_{d \cdot I_n} \cdot \alpha \Leftrightarrow \\ &\Leftrightarrow \exists \alpha \in \mathbb{K}^n, \alpha \neq 0_{\mathbb{K}^n} \mid \underbrace{(A - d \cdot I_n)}_{\substack{:= B \in M(n, n, \mathbb{K}) \\ B \cdot \alpha = 0_{\mathbb{K}^n}}} \cdot \alpha = 0_{\mathbb{K}^n} \Leftrightarrow \\ &\Leftrightarrow A - d \cdot I_n \notin GL(n, n, \mathbb{K}) \Leftrightarrow \det(A - d \cdot I_n) = 0 \end{aligned}$$

Quindi

$$d \text{ autovalore di } A \Leftrightarrow P_A(d) = 0 \Leftrightarrow d \text{ radice di } P_A$$

ovvero gli autovalori di una matrice sono le radici del polinomio caratteristico.

Esempio di matrice senza autovalori

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in M(2,2, \mathbb{R}), \text{ quindi } P_A = \det \begin{pmatrix} -x & -1 \\ 1 & -x \end{pmatrix} = x^2 + 1$$

$\forall a \in \mathbb{R}, P_A(a) = a^2 + 1 \geq 1 \Rightarrow P_A(a) \neq 0 \stackrel{\mathbb{K}=\mathbb{R}}{\Rightarrow} P_A$ non ha radici $\Rightarrow A$ non ha autovalori.

Esempio di matrice con autovalori

$$A = \begin{pmatrix} 5 & 6 \\ -1 & 0 \end{pmatrix} \in M(2,2, \mathbb{R}), \text{ quindi}$$

$$P_A = \det(A - x \cdot I_2) = \det \left(\begin{pmatrix} 5 & 6 \\ -1 & 0 \end{pmatrix} + \begin{pmatrix} -x & 0 \\ 0 & -x \end{pmatrix} \right) = \det \begin{pmatrix} 5-x & 6 \\ -1 & -x \end{pmatrix} = ((5-x)(-x)) -$$

$$(6 \cdot (-1)) = -5x + x^2 + 6 = x^2 - 5x + 6 \Rightarrow \begin{cases} x_1 = \frac{5+1}{2} = 3 \\ x_2 = \frac{4}{2} = 2 \end{cases}$$

Quindi 3 e 2 sono gli autovalori di A .

Esempio sugli autovalori di una funzione

Sia $\mathbb{K} = \mathbb{Z}_5$, V s. v. su \mathbb{K} , $\dim(V) = 3$,

$$\mathcal{A} = \{v_1, v_2, v_3\} \text{ una base di } V$$

$f: V \rightarrow V$ una funzione lineare così definita: $v_1 \mapsto v_1, v_2 \mapsto v_1 - v_2, v_3 \mapsto 2v_1 + 2v_2 + 3v_3$.

Per determinare gli autovalori di f devo trovare gli autovalori della relativa matrice $M_{\mathcal{A}\mathcal{A}}(f) =$

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & -1 & 2 \\ 0 & 0 & 3 \end{pmatrix} \text{ (la colonna } n \text{ è il vettore } v_n \text{).}$$

Metodo per trovare gli autovettori

Una volta che ho trovato gli autovalori, posso trovare i relativi autovettori usando la definizione.

- $\beta \in \mathbb{K}^3$ autovettori di f relativi all'autovalore 3 $\Leftrightarrow M \cdot \beta = 3 \cdot \beta$

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & -1 & 2 \\ 0 & 0 & 3 \end{pmatrix} \beta = 3 \cdot \beta \Leftrightarrow \dots \Leftrightarrow \begin{cases} x_2 + 2x_3 = 3x_1 \\ x_1 - x_2 + 2x_3 = 3x_2 \\ 3x_3 = 3x_3 \end{cases} \stackrel{t \in \mathbb{K} = \mathbb{Z}_5}{\Leftrightarrow} \begin{cases} x_3 = t \\ x_2 + 2t = 3x_1 \\ x_1 - x_2 + 2t = 3x_2 \end{cases} \Leftrightarrow \dots \Leftrightarrow$$

$$\begin{cases} x_3 = t \\ x_2 = 3\left(\frac{10}{11}t\right) - 2t \\ x_1 = \frac{10}{11}t \end{cases} \stackrel{\text{siamo in } \mathbb{Z}_5}{\Leftrightarrow} \begin{cases} x_1 = 0 \\ x_2 = -2t \\ x_3 = t \end{cases} \Rightarrow \beta = \begin{pmatrix} 0 \\ -2t \\ t \end{pmatrix} \text{ con } t \in \mathbb{Z}_5$$

Introducendo t nell'autovettore relativo all'autovalore 3 indico che qualsiasi valore di x_3 va bene.

Si nota quindi che il numero di autovettori per ogni autovalore non è sempre 1.

Si ricorda che per definizione un autovettore deve essere diverso da 0_V .

Metodo per trovare gli autospazi

Sia $A \in M(m, n, \mathbb{K}), c \in \mathbb{K}, c$ autovalore di A .

$\text{Aut}(c) := \{\alpha \in \mathbb{K}^n \mid A \cdot \alpha = c \cdot \alpha\}$ è l'autospazio di A relativo a c .

Si noti che $\text{Aut}(c)$ è l'insieme degli autovettori di A relativi a c più $0_{\mathbb{K}^n}$.

Esempio di autospazio con un autovettore

$$\text{Aut}(3) = \left\{ \begin{pmatrix} 0 \\ -2t \\ t \end{pmatrix} \mid t \in \mathbb{Z}_5 \right\} = \left\{ t \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix} \mid t \in \mathbb{Z}_5 \right\} = \left\langle \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix} \right\rangle$$

Esempio di autospazio con due autovettori

Sia $A \in M(3,3, \mathbb{R}), A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix}$.

$$P_A = \det(A - x \cdot I_3) = \dots \Rightarrow \begin{cases} x_1 = 1 \\ x_2 = 2 \end{cases} \Rightarrow 1 \text{ e } 2 \text{ sono gli autovalori di } A.$$

- $M \cdot \alpha = 1 \cdot \alpha$

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \Rightarrow \dots \Rightarrow \begin{cases} x_1 = t \\ x_2 = -t \\ x_3 = -t \end{cases}$$

$$\text{Aut}(1) = \left\{ t \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \mid t \in \mathbb{R} \right\} = \left\langle \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \right\rangle$$

$$\bullet \quad M \cdot \alpha = 2 \cdot \alpha$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = 2 \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \Rightarrow \begin{cases} x_1 = 2x_1 \\ x_1 + 2x_2 = 2x_2 \\ x_1 + 2x_3 = 2x_3 \end{cases} \Rightarrow \begin{cases} x_1 = 0 \\ x_2 = x_2 \\ x_3 = x_3 \end{cases}$$

$$\text{Aut}(2) = \left\{ \begin{pmatrix} 0 \\ x_2 \\ x_3 \end{pmatrix} \mid x_2, x_3 \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} 0 \\ x_2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ x_3 \end{pmatrix} \mid x_2, x_3 \in \mathbb{R} \right\} = \left\{ x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mid x_2, x_3 \in \mathbb{R} \right\} = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

Appendice

Teoremi da sapere

I teoremi che normalmente vengono segnalati dal docente sono:

1. Lagrange
2. Grassmann
3. Rouché – Capelli
4. Nullità – Rango
5. Spazio quoziente (anche se non l'ho mai visto essere richiesto)

Per dimostrare che...

- Un elemento appartiene al \ker di una funzione lineare (es. $a \in \ker f$)
applico f all'elemento a e dimostro che fa 0: $f(a) = 0$.
- In generale, per dimostrare che due insiemi sono uguali dimostro le due inclusioni (es. $U = W$).
“ \subseteq ”: prendo un elemento di U e dimostro che sta in W ,
“ \supseteq ”: viceversa.
- Un insieme di vettori genera uno spazio vettoriale (es. $\langle v_1, \dots, v_n \rangle = V$)
prendo un elemento di V e dimostro che è combinazione lineare dei vettori v_1, \dots, v_n .
Questo equivale a dimostrare l'inclusione $V \subseteq \langle v_1, \dots, v_n \rangle$. Infatti l'altra inclusione è ovvia perché ogni combinazione lineare di elementi di V sta ancora in V .
- Un elemento appartiene all'Im di una funzione (lineare) (es. $f: V \rightarrow W$)
Tesi: $b \in \text{Im } f$, cerco un elemento $a \in V$ tale che $f(a) = b$. a lo devo proprio mostrare, e dimostrare che sta veramente in V !
- Una funzione è iniettiva
suppongo $f(a) = f(b)$ e voglio dimostrare che $a = b$ ($\forall a, b \in \text{dominio di } f$)
- Una funzione è suriettiva (come per $\text{Im } f$) (es. $f: U \rightarrow W$)
prendo un qualsiasi elemento $w \in W$ e cerco un elemento $u \in U$ tale che $f(u) = w$. Lo devo mostrare!
- Dimostrare che vale una cosa o un'altra (es. Sia I ideale di \mathbb{R} campo, dimostrare che $I = \{0\}$ oppure $I = R$)
si suppone che una delle due non valga e si dimostra che vale l'altra: suppongo $I \neq \{0\}$ e dimostro $I = R$.
- Qualcosa = \emptyset
suppongo per assurdo che sia $\neq \emptyset$ e prendo un elemento. (es. Siano $xH \neq yH$ classi laterali, dimostrare che $xH \cap yH = \emptyset$. Suppongo per assurdo $xH \cap yH \neq \emptyset \Rightarrow \exists$ un elemento $a \in xH \cap yH \Rightarrow \dots$.)

Approfondimenti

Per degli appunti più verbosi consiglio il sito di Nicola Gigante: <http://www.gigabytes.it>.