Appunti di Algebra Lineare

Lorenzo Baloci e Andrea Vianello*

13 giugno 2007

Indice

*E-Mail: lorenzo@xelon.it - andrea@xelon.it

1 Definizioni

1.1 Gruppo

Sia G un insieme non vuoto. G si dice *gruppo* se G è dotato di una operazione $\cdot : G \times G \to G$ che gode delle seguenti proprietà:

1. associatività $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in G$
2. $\exists$ un elemento neutro rispetto all'operazione
3. ogni elemento di G è invertibile rispetto all'operazione

n.b. l'elemento neutro è unico e $\forall a \in G$ l'inverso è unico e si denota con a^{-1}, si noti che anche solo una parte di un insieme può essere un gruppo

1.1.1 Semigruppo

Un insieme non vuoto munito di una operazione binaria chiusa $\cdot : A \times A \to A$ associativa è detto *semigruppo*

1.1.2 Gruppo abeliano (commutativo)

Un gruppo si dice *abeliano* (o *commutativo*) se $a \cdot b = b \cdot a$ $\forall a, b \in G$.

1.1.3 Sottogruppo

Se G è un gruppo e $H \subseteq G$, H si dice un *sottogruppo* di G se la stessa operzione definita in G rende H un gruppo.
Questo significa che se $\cdot : G \times G \to G$ allora $\cdot : H \times H \to H$, quindi il sottoinsieme deve essere chiuso rispetto all'operazione (ad esempio i numeri pari sono un sottogruppo di $(\mathbb{Z}, +)$ mentre i dispari non lo sono perchè la somma di due è un pari!).
Per verificare che $H \subseteq G$ è un sottogruppo di G bisogna verificare che:

- $\forall a, b \in H$ $a \cdot b \in H$
- $\forall a \in H$ $a^{-1} \in H$

1.2 Anello

Un insieme è detto *anello* se è non vuoto, è dotato di due operazioni dette somma e prodotto. Rispetto la somma è un gruppo abeliano e rispetto il prodotto è un semigruppo e vale la proprietà distributiva del prodotto rispetto la somma.

1.2.1 Anello commutativo

Un anello è detto commutativo se è commutativo anche rispetto al prodotto.

1.2.2 Anello unitario

L'anello è *unitario* oppure con unità se ha un elemento neutro 1 per il prodotto. Poiché gli anelli più studiati sono in gran parte unitari, alcuni autori chiamano semplicemente anello un anello unitario.

1.2.3 Sottoanello

Sia A un anello e $S \subseteq A$, S è *sottoanello* di A se le stesse operazioni definite su A rendono S un anello.

1.3 Campo

Un anello commutativo in cui ogni elemento non nullo ha un inverso è detto *campo*. In altre parole vale che:

- $(K, +)$ è un gruppo abeliano con elemento neutro 0
- $(K/\{0\}, \cdot)$ è un gruppo abeliano con elemento neutro 1
- la moltiplicazione è distributiva rispetto alla somma

1.4 Spazio vettoriale

Sia V un insieme non vuoto. V si dice uno *spazio vettoriale* su $\mathbb{R}$ se:

1. è un gruppo abelliano $(V, +)$ con elemento neutro 0_V
2. è dotato di una operazione esterna da $\mathbb{R} \times V \to V$ che ad ogni coppia (r, v) associa un elemento di V indicato con rv e che verifica:
   (a) $r(sv) = (rs)v$ (associativa)
   (b) $(r + s)v = rv + sv$ (distributiva)
   (c) $r(u + v) = ru + rv$ (distributiva)
   (d) $1v = v$ (elemento neutro)

dove $r, s \in \mathbb{R}, v, u \in V$
Se prendiamo quindi v,$w \in V$, $r \in \mathbb{R}$ se V è spazio vettoriale allora:

- $(v + w) \in V$
- $rv \in V$

1.4.1 Sottospazio vettoriale

Sia V uno spazio vettoriale e $U \subseteq V$, U è *sottospazio vettoriale* di V se le stesse operazioni definite su V rendono U uno spazio vettoriale.

1.5 Combinazione lineare

Dati dei vettori $v_1, ..., v_n$ di uno spazio vettoriale V, si dice loro *combinazione lineare* ogni vettore $r_1v_1 + ... + r_nv_n$ dove $r_1, ..., r_n$ sono numeri reali qualsiasi; i numeri $r_1, ..., r_n$ vengono chiamati coefficienti della combinazione lineare.

1.6 Dipendenza lineare

I vettori $v_1, ..., v_n$ si dicono *linearmente indipendenti* se l'unico modo per ottenere 0_V come combinazione lineare è quello di prendere tutti gli scalari uguali a 0, cioè se l'uguaglianza $r_1v_1 + ... + r_nv_n = 0_V$ implica $r_1 = ... = r_n = 0$
I vettori si dicono *linearmente dipendenti* in caso contrario, cioè quando esistono dei numeri che non sono tutti 0 e tali che $r_1v_1 + ... + r_nv_n = 0_V$.

1.7 Generatori

I vettori $v_1, ..., v_n$ si dicono *generatori dello spazio vettoriale* V se ogni vettore di V è loro combinazione lineare.

1.8 Base

I vettori $v_1, ..., v_n$ sono una *base* dello spazio vettoriale V se sono linearmente indipendenti e generatori (n.b. la dimensione della base è quindi il minimo numero di vettori necessari per generare tutto lo spazio).
In uno spazio di dimensione n, le basi sono composte da n vettori.

1.8.1 Cambio di base

Esercizio:
$\mathbb{B}$,$\mathbb{C} \in \mathbb{R}^3$

$$\mathbb{B} = (1,2,1),(0,1,2),(0,3,5) \qquad \mathbb{C} = (1,0,0),(0,1,0),(0,0,1)$$

Determinare le matrici di cambiamento di base nelle due direzioni.
Soluzione:
$\mathbb{B} \to \mathbb{C}$:
Troviamo le immagini della base $\mathbb{B}$ con coordinate in $\mathbb{C}$:

$$(1,2,1) = x(1,0,0) + y(0,1,0) + z(0,0,1) \Rightarrow x = 1, y = 2, z = 1$$

$$(0,1,2) = x(1,0,0) + y(0,1,0) + z(0,0,1) \Rightarrow x = 0, y = 1, z = 2$$

$$(0,3,5) = x(1,0,0) + y(0,1,0) + z(0,0,1) \Rightarrow x = 0, y = 3, z = 5$$

La matrice associata sarà quindi:

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 3 \\ 1 & 2 & 5 \end{pmatrix}$$

$\mathbb{C} \to \mathbb{B}$:
Avendo la matrice D, la matrice di cambiamento di base $\mathbb{C} \to \mathbb{B}$ sarà D^{-1}.

1.9 Dimensione di uno spazio vettoriale

Dato uno spazio vettoriale V finitamente generato e non banale, si chiama *dimensione di* V e si indica con $dimV$, il numero dei vettori di una base di V.
La dimensione dello spazio banale si pone uguale a 0.
La *dimensione* di uno spazio vettoriale indica il numero di coordinate di cui ha bisogno un vettore per essere definito. Ad esempio se V è uno spazio vettoriale su $\mathbb{R}$ di dimensione n allora $V \simeq \mathbb{R}^n$ (è isomorfo), $\exists\, \varphi : V \to \mathbb{R}^n$

1.10 Somma

Dati due sottospazi U e W di uno spazio vettoriale V, il minimo sottospazio che contiene l'insieme $U \cup W$ lo chiamiamo *sottospazio somma* di U e W ed anzichè indicarlo con $< U \cup W >$ gli riserviamo un nuovo simbolo: $U + W$

1.10.1 Somma diretta

Se U e W che verificano almeno una di queste condizioni:

1. $U \cap W = 0_V$
2. per ogni $v \in U + W$ esistono un unico $u \in U$ ed un unico $w \in W$ t.c $V = U + W$
3. $dim(U + W) = dimU + dimW$
4. unendo una base di U e una di W si ottiene una base di $U + W$

allora la somma di $U + W$ si dice *diretta* e si indica con $U \oplus W$.

1.11 Proprietà della dimensione

Siano U, W sottospazi finitamente generati in V:

1. $dimU + dimW = dim(U + W) + dimU \cap dimW$ (teorema di Grassmann)
2. $dim(V \times W) = dimV + dimW$
3. $dim(V/U) = dimV - dimU$

1.12 Funzioni lineari

Dati due spazi vettoriali V e W, una funzione $L : V \to W$ si dice *lineare* se per ogni $v, u \in V, r \in \mathbb{R}$ vale:

1. $L(v + u) = L(v) + L(u)$
2. $L(rv) = rL(v)$

(n.b. Sinonimo di funzione lineare è il termine *omomorfismo* di spazi vettoriali, mentre se V e W coincidono è detto *endomorfismo*).
Sia $L : V \to W$ una funzione lineare tra due spazi vettoriali:

- L trasforma famiglie di vettori indipendenti in famiglie di vettori indipendenti $\Leftrightarrow$
- la controimmagine del vettore 0_W è costituita dal solo 0_V $\Leftrightarrow$
- L è iniettiva

Esercizio:

$$f(x, y) = (x - y, x + y + 1, 0)$$

Soluzione:

$$f(x + x', y + y') = (x + x' - y - y', x + x' + y + y' + 1, 0) \tag{1}$$

$$\begin{aligned} f(x, y) + f(x', y') &= (x - y, x + y + 1, 0) + (x' - y', x' + y' + 1, 0) \\ &= (x + x' - y - y', x + x' + y + y' + 2, 0) \end{aligned} \tag{2}$$

La (1) e la (2) non sono equivalenti quindi la funzione non è lineare.

Esercizio:

$$f(x, y) = (x - y, x + y)$$

Soluzione:

$$f(\alpha x + \beta x', \alpha y + \beta y') = (\alpha x + \beta x', \alpha x + \beta x' + \alpha y + \beta y') \tag{3}$$

$$\begin{aligned} f(x,y) + f(x',y') &= \alpha(x, x+y) + \beta(x', x'+y') \\ &= (\alpha x, \alpha x + \alpha y) + (\beta x', \beta x' + \beta y') \\ &= (\alpha x + \beta x', \alpha x + \beta x' + \alpha y + \beta y') \end{aligned} \tag{4}$$

La (3) e la (4) sono equivalenti quindi la funzione è lineare.

1.13 Kernel

Sia $L : V \rightarrow W$ una funzione lineare. La controimmagine di 0_W si chiama *kernel* di L e si indica con $K(L)$.

Inoltre se $L(v) = w$ (cioè v è un vettore qualsiasi della controimmagine di w), la controimmagine di w è l'insieme $v + K(L)$.

1.14 Isomorfismo

Un *isomorfismo* è una funzione lineare iniettiva e suriettiva; un endomorfismo biiettivo (cioè un endomorfismo che sia anche isomorfismo) è detto *automorfismo*.

1.15 Teorema delle dimensioni

Sia $L : V \rightarrow W$ una funzione lineare e V abbia dimensione finita, allora sussiste la seguente uguaglianza:
$dimV = dim(K(L)) + dim(Im(L))$

1.16 Autovettore, autovalore e autospazio

Sia V uno spazio vettoriale su un campo K e $f : V^n \rightarrow V^n$.
Se v è un vettore non nullo in V e λ è uno scalare qualsiasi tali che:

$$f(v) = \lambda v$$

allora v è un *autovettore* della trasformazione f, e λ è il suo *autovalore*. Poiché f è lineare, se v è un autovettore con autovalore λ, allora ogni multiplo non nullo di v è anch'esso un autovettore con lo stesso autovalore λ:

$$v_2 = \alpha v_1 \Rightarrow f(v_2) = f(\alpha v_1) = \alpha f(v_1) = \alpha \lambda_1 v_1 = \lambda_1 v_2$$

Più in generale, gli autovettori aventi lo stesso autovalore λ, insieme al vettore nullo, formano un sottospazio di V^n chiamato l'*autospazio relativo all'autovalore* λ. Sia f_λ l'autospazio:

$$f_\lambda(x) = f(x) - \lambda i(x)$$

Attraverso λ posso trasformare una qualsiasi funzione in una funzione con dimensione del kernel diversa da 0 in quanto:

$$f(v_1) - \lambda_1 i(v_1) = \lambda_1 v_1 - \lambda_1 v_1 = 0_V$$

Avendo $f(x) \to A$

$$f_t(x) \to A - tI$$

se t è un autovalore allora: $p(t) = \det(A - tI) = 0$

Se come base della matrice scelgo una base costituita da autovettori posso usarla per ottenere sempre una matrice diagonale. Una matrice è *diagonalizzabile* se posso trovare una matrice H tale che $HDH^{-1} = B$; per fare ciò è necessario che esista una base di autovettori, ovvero se e solo se la moltiplicità geometrica di ogni autospazio corrisponde a quella algebrica del suo autovalore, dove la moltiplicità geometrica è la dimensione del autospazio mentre la moltiplicità algebrica è il numero di volte che l'autovalore è soluzione di $p(t)$.

Esercizio:

$$A = \begin{pmatrix} -10 & 1 & 3 \\ 0 & 0 & 0 \\ -10 & 1 & 3 \end{pmatrix}$$

- Trovare gli autovalori e la loro moltiplicità algebrica n.
- Trovare gli autospazi e la loro moltiplicità geometrica m.

Soluzione:

Troviamo gli autovalori:

$$A_t = \begin{pmatrix} -10-t & 1 & 3 \\ 0 & 0-t & 0 \\ -10 & 1 & 3-t \end{pmatrix}$$

$$\begin{aligned} \det(A_t) &= -t \det \begin{pmatrix} -10-t & 3 \\ -10 & 3-t \end{pmatrix} \\ &= -t((-10-t)(3-t)+30) \\ &= -t(t^2+7t) \\ &= -t^2(t+7) \end{aligned}$$

$-t^2(t+7)$ si annulla due volte per $t=0$ e una volta per $t=-7$:
$\lambda_1 = 0$, $n_1 = 2$
$\lambda_2 = -7$, $n_2 = 1$

Troviamo gli autospazi:
autospazio$_{\lambda_1}$:

$$\begin{pmatrix} -10 & 1 & 3 \\ 0 & 0 & 0 \\ -10 & 1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda_1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0 \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{cases} -10x + y + 3z = 0 \\ 0 = 0 \\ -10x + y + 3z = 0 \end{cases} \Rightarrow \begin{cases} y = 10x - 3z \\ x = \alpha \\ z = \beta \end{cases}$$

Un suo vettore avrà quindi forma: $(\alpha, 10\alpha - 3\beta, \beta)$
autospazio$_{\lambda_1}$ $=< (1, 10, 0), (0, -3, 1) >$ e $m_1 = 2$ autospazio$_{\lambda_2}$:

$$\begin{pmatrix} -10 & 1 & 3 \\ 0 & 0 & 0 \\ -10 & 1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \lambda_2 \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -7 \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -7x \\ -7y \\ -7z \end{pmatrix}$$

$$\begin{cases} -10x + y + 3z = -7x \\ 0 = -7y \\ -10x + y + 3z = -7z \end{cases} \Rightarrow \begin{cases} y = 0 \\ 3x = 3z \\ -10x = -10z \end{cases} \Rightarrow \begin{cases} y = 0 \\ x = \alpha \\ z = \alpha \end{cases}$$

Un suo vettore avrà quindi forma: $(\alpha, 0, \alpha)$
autospazio$_{\lambda_2}$ $=< (1, 0, 1) >$ e $m_2 = 1$

1.17 Teorema di Rouché-Capelli

Un sistema di equazioni lineari:

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \vdots & \vdots \quad \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{cases}$$

può essere descritto tramite una matrice:

$$(A|b) = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} & b_m \end{array}\right)$$

detta matrice *associata al sistema*; essa è ottenuta dalla giustapposizione della matrice dei coefficienti e di un'ulteriore colonna detta *colonna dei termini noti*. Le matrici A e $(A|b)$ sono dette rispettivamente *incompleta* (o *dei coefficienti*) e *completa*.

I coefficienti del sistema lineare (e quindi delle matrici) sono elementi di un campo K , quale ad esempio quello dei numeri reali $\mathbb{R}$ o complessi $\mathbb{C}$. Indichiamo con $\mathrm{rk}(M)$ il rango di una matrice M. L'enunciato del teorema di Rouché-Capelli è il seguente:

Esistono soluzioni per il sistema se e solo se il rango della matrice completa è uguale al rango della matrice incompleta.

Se esistono soluzioni, queste formano un sottospazio affine di K^n di dimensione $n - \mathrm{rk}(A)$. In particolare, se il campo K è infinito abbiamo:

- se $\mathrm{rk}(A) = n$ allora la soluzione è unica,
- altrimenti ci sono infinite soluzioni

1.18 Regola di Cramer

Un sistema di equazioni lineari può essere rappresentato usando la moltiplicazione fra matrici come:

$$Ax = c$$

dove A è una matrice e x, c sono due vettori. Se A è una matrice quadrata (cioè il numero di incognite del sistema è pari al numero di equazioni) ed è anche invertibile, il teorema di Rouché-Capelli asserisce che il sistema ha esattamente una soluzione.

In questo caso, la regola di Cramer fornisce un algoritmo per calcolare la soluzione $(x_1, \ldots, x_n)$ usando il determinante nel modo seguente:

$$x_i = \frac{\det(A_i)}{\det(A)}$$

dove A_i è la matrice formata sostituendo la i-esima colonna di A con il vettore c. Notiamo che la condizione di invertibilità di A garantisce che il denominatore $\det(A)$ sia diverso da zero, e quindi che l'espressione descritta abbia sempre senso.

1.19 Matrici

1.19.1 Ordine

Si chiama *matrice* di *ordine* $m \times n$ a coefficienti in $\mathbb{R}$, una funzione che ad ogni coppia di numeri naturali (i, j) con $i \leq m, j \leq n$ associa un numero reale.

1.19.2 Rango

Il *rango* di una matrice $A_{m \times n}$ può essere definito nei seguenti modi equivalenti:

- il massimo numero di colonne linearmente indipendenti
- il massimo numero di righe linearmente indipendenti
- la dimensione del sottospazio di K^m generato dalle colonne di A
- la dimensione del sottospazio di K^n generato dalle righe A
- il massimo ordine di un minore invertibile di A

Si noti che:

- solo la matrice nulla ha rango 0
- il rango di A è uguale al rango della sua *trasposta*
- il rango di A è minore-uguale sia di m che di n

È importante ricordare che il ragno di una matrice non cambia quando su di essa vengono effettuate delle *operazioni elementari* e che corrisponde alla dimensione dell'immagine di una funzione lineare con dominio lo spazio vettoriale.

1.19.3 Determinante

Il *determinante* è una funzione che associa ad ogni matrice quadrata A uno scalare, generalmente indicato come $det(A)$.

1.19.4 Invertibilità

Una matrice quadrata $A_{n \times n}$ è detta *invertibile* se esiste una matrice $B_{n \times n}$ tale che: $AB = BA = I_n$, B è quindi univocamente determinata da A ed è chiamata l'*inversa* di A e indicata con A^{-1}.
Si noti che, le seguenti definizioni sono equivalenti e caratterizzano una matrice A invertibile:

- la matrice non è *singolare*, ossia il suo *determinante* non è nullo
- il suo rango è n
- le sue colonne sono linearmente indipendenti
- le sue righe sono linearmente indipendenti

- la matrice è trasformabile nella matrice identità o in una matrice con n pivot

Interessante è anche il seguente teorema:
Sia $AX = B$ un sistema di equazioni lineari e sia M una matrice invertibile. Allora i sistemi $(MA)X = MB$ e $AX = B$ sono equivalenti, cioè hanno le stesse soluzioni.
Inoltre, il prodotto di due matrici invertibili è anch'esso invertibile.

1.19.5 Somma

Siano $A = (a_{ij})$ e $B = (b_{ij})$ due matrici di tipo $m \times n$. Si chiama *matrice somma* di A e B, e si indica con $A + B$, la matrice di tipo $m \times n$ che in posizione (i, j) ha il numero $a_{ij} + b_{ij}$.

1.19.6 Prodotto

Siano $A = (a_{ij})$ e $B = (b_{hk})$ due matrici di tipo rispettivamente $m \times n$ e $n \times r$. Si chiama matrice *prodotto* di A e B, e si indica con AB, la matrice di tipo $m \times r$ che in posizione (i, k) ha il numero $a_{i1}b_{1k} + ... + a_{in}b_{nk}$.

1.19.7 Prodotto scalare

Sia A una matrice e r un reale. Definiamo il prodotto scalare $B = rA$ come ma matrice il cui elemento generico è $b_{ij} = ra_{ij}$.

1.19.8 Operazioni elementari

Sono semplici operazioni realizzabili su di una matrice che corrispondono ad una moltiplicazione (a sinistra o a destra) per una matrice elementare. Sono utili per effettuare calcoli e portare una matrice in determinate forme.

- Sostituire la i-esima riga x_i con la riga $x_i + ax_j$
- Scambiare tra loro la riga x_i con la riga x_j
- Moltiplicare una riga per una costante c

1.19.9 Forma canonica

Una matrice $m \times n$ è in *forma canonica per righe* se le righe nulle sono tutte in basso e per quelle non nulle il primo termine diverso da 0 di ogni riga, che si chiama termine *pivot*, sta a sinistra del primo termine diverso da 0 della riga successiva.
n.b. Il rango è esattamente il numero di righe non nulle (ossia linearmente indipendenti).

1.19.10 Matrice trasposta

La *matrice trasposta* si definisce intuitivamente come una matrice in cui le colonne diventano righe e le righe diventano colonne.

$$A = \begin{pmatrix} 1 & 4 & 7 \\ 3 & 2 & 0 \\ 5 & 3 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad A^T = \begin{pmatrix} 1 & 3 & 5 & 0 \\ 4 & 2 & 3 & 1 \\ 7 & 0 & 1 & 0 \end{pmatrix}$$

1.19.11 Matrice simmetrica

Una *matrice simmetrica* è una matrice che è la *trasposta* di sé stessa. Quindi A è simmetrica se: $A^T = A$. Questo implica che A sia una matrice quadrata.

1.19.12 Matrice diagonale

Una *matrice diagonale* è una matrice quadrata in cui valori della diagonale principale possono essere diversi da 0.

$$D = \begin{pmatrix} d_1 & 0 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 & 0 \\ 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & d_{n-1} & 0 \\ 0 & 0 & 0 & 0 & d_n \end{pmatrix}$$

1.19.13 Matrice identica

La matrice diagonale con tutti i valore della diagonale uguali ad 1 è detta *matrice identica* La matrice identica è l'elemento neutro rispetto al prodotto e si indica solitamente con I.

1.19.14 Matrice triangolare

Le *matrici triangolari inferiori* sono matrici che hanno nulli tutti gli elementi al di sopra della diagonale principale, cioè della forma:

$$L = \begin{pmatrix} l_{1,1} & 0 & \dots & & 0 \\ l_{2,1} & l_{2,2} & & & \\ l_{3,1} & l_{3,2} & \ddots & & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ l_{n,1} & l_{n,2} & \dots & l_{n,m-1} & l_{n,m} \end{pmatrix}$$

Si dice invece *matrice triangolare superiore* una matrice con nulli gli elementi al di sotto della diagonale principale.