TEORIA DELLE MATRICI INVERTIBILI E DEL RANGO: ALGEBRA LINEARE 2010-11

M.M. 16 NOVEMBRE 2010

Notazione: $\mathbb{K}$ è un campo, $\mathbb{K}^n$ e $\mathbb{K}^{\times n}$ sono rispettivamente gli spazi vettoriali dei vettori colonna e riga ad n coordinate.

1. Matrici invertibili

Date due matrici $A \in M_{n,m}(\mathbb{K}), B \in M_{m,l}(\mathbb{K})$ osserviamo che ogni vettore colonna del prodotto AB è una combinazione lineare dei vettori colonna di A: più precisamente la i-esima colonna di AB è la combinazione lineare delle colonne di A con coefficienti le coordinate dell'i-esimo vettore colonna di B. Similmente ogni riga di AB è combinazione lineare delle righe di B. Da questo ne deduciamo che:

(1) Date due matrici $A \in M_{n,m}(\mathbb{K}), D \in M_{n,l}(\mathbb{K})$, esiste una matrice $B \in M_{m,l}(\mathbb{K})$ tale che $AB = D$ se e solo se ogni colonna di D è combinazione lineare delle colonne di A.
(2) Date due matrici $A \in M_{n,m}(\mathbb{K}), D \in M_{l,m}(\mathbb{K})$, esiste una matrice $C \in M_{l,n}(\mathbb{K})$ tale che $CA = D$ se e solo se ogni riga di D è combinazione lineare delle righe di A.

Le precedenti considerazioni per $C = I$ la matrice identità ci danno il seguente risultato.

Lemma 1.1. *Sia $A \in M_{n,m}$. Allora:*

(1) *Esiste $B \in M_{m,n}$ tale che $AB = I$ se e solo se le colonne di A generano $\mathbb{K}^n$ (e quindi $m \geq n$).*
(2) *Esiste $C \in M_{m,n}$ tale che $CA = I$ se e solo se le righe di A generano $\mathbb{K}^{\times m}$ (e quindi $m \leq n$).*

Se esistono B e C come sopra, allora sono uniche e vale $n = m$, $B = C$.

Dimostrazione. Basta osservare che sia i vettori colonna che i vettori riga della matrice identità sono un insieme di generatori. Se esistono B e C allora

$$C = CI = C(AB) = (CA)B = IB = B.$$

Inoltre se $A\hat{B} = I$ allora, $C = CI = C(AB) = (CA)\hat{B} = I\hat{B} = \hat{B}$ e quindi $B = \hat{B}$. In modo del tutto simile si prova l'unicità di C. □

Definizione 1.2. Una matrice quadrata $A \in M_{n,n}(\mathbb{K})$ si dice **invertibile** se esiste una matrice $A^{-1} \in M_{n,n}(\mathbb{K})$, tale che

$$A^{-1}A = AA^{-1} = I.$$

Abbiamo visto che la matrice A^{-1} se esiste è unica ed è invertibile con inversa $(A^{-1})^{-1} = A$. Se A è invertibile, allora anche A^T è invertibile con inversa $(A^T)^{-1} = (A^{-1})^T$: infatti

$$(A^{-1})^T A^T = (AA^{-1})^T = I^T = I, \qquad A^T(A^{-1})^T = (A^{-1}A)^T = I^T = I.$$

Se $A, B \in M_{n,n}(\mathbb{K})$ sono invertibili, allora anche AB è invertibile e vale $(AB)^{-1} = B^{-1}A^{-1}$.

Teorema 1.3. *Siano $A, B \in M_{n,n}(\mathbb{K})$ tali che $AB = I$. Allora A e B sono invertibili e $B = A^{-1}$, $A = B^{-1}$.*

Dimostrazione. Mostriamo che i vettori colonna di B sono linearmente indipendenti e quindi una base di $\mathbb{K}^n$. A tal fine è sufficiente mostrare che, dato $v \in \mathbb{K}^n$ vale $Bv = 0$ se e solo se $v = 0$. Se $Bv = 0$ allora $0 = A0 = A(Bv) = Iv = v$ e quindi $v = 0$. Dunque esiste $C \in M_{n,n}(\mathbb{K})$ tale che $BC = I$. Ragionando come sopra $A = A(BC) = (AB)C = C$ e quindi B è invertibile con $B^{-1} = A$. Passando alle trasposte si ottiene $B^T A^T = I$, dunque A^T è invertibile con inversa $(A^T)^{-1} = B^T$ e, per quanto visto sopra anche $A = (A^T)^T$ è invertibile con inversa $(B^T)^T = B$. □

Corollario 1.4. *Per una matrice quadrata A le seguenti condizioni sono equivalenti:*

(1) *A è invertibile.*
(2) *Le colonne di A sono linearmente indipendenti.*
(3) *Le righe di A sono linearmente indipendenti.*

Dimostrazione. La condizione che le colonne siano indipendenti equivale al fatto che sono generatori, che a sua volta equivale all'esistenza di una matrice B tale che $AB = I$. Passando alla matrice trasposta otteniamo l'analogo risultato per le righe. □

Se F è un campo che contiene $\mathbb{K}$, si ha $M_{n,n}(\mathbb{K}) \subset M_{n,n}(F)$: se $A \in M_{n,n}(\mathbb{K})$ è invertibile come matrice a coefficienti in $\mathbb{K}$ allora $A^{-1} \in M_{n,n}(F)$ e quindi A è invertibile come matrice a coefficienti in F. Viceversa se A è invertibile come matrice a coefficienti in F, allora le colonne sono linearmente indipendenti su F ed a maggior ragione sono linearmente indipendenti su $\mathbb{K}$. Dunque **l'invertibilità di una matrice quadrata non dipende dal campo nel quale i coefficienti sono considerati.**

Esempio 1.5 (La matrice di Vandermonde)**.** Dati n numeri $a_1, \ldots, a_n$, la **matrice di Vandermonde** associata è la matrice $n \times n$

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$$

Dimostriamo che *la matrice V è invertibile se e solo se i numeri a_i sono distinti.* Se $a_i = a_j$ per qualche coppia di indici $i \neq j$, allora le colonne di V non sono linearmente indipendenti e quindi V non è invertibile. Se V non è invertibile, allora le righe di V sono linearmente dipendenti, ossia esiste un vettore riga non nullo $(c_1, \ldots, c_n)$ tale che $(c_1, \ldots, c_n)V = 0$. Questo significa che per ogni $i = 1, \ldots, n$ vale

$$c_1 + c_2 a_i + \cdots + c_n a_i^{n-1} = 0$$

e dunque che $a_1, \ldots, a_n$ sono radici del polinomio $p(t) = c_1 + c_2 t + \cdots + c_n t^{n-1}$ che, avendo grado $\leq n-1$, possiede al più $n-1$ radici distinte. Dunque $a_i = a_j$ per qualche coppia di indici $i \neq j$.

2. Iperpiani di $\mathbb{K}^n$

Ricordiamo che un **iperpiano** di uno spazio vettoriale di dimensione n è un sottospazio vettoriale di dimensione $n-1$.

Dato un vettore riga $w = (w_1, \ldots, w_n) \in \mathbb{K}^{\times n}$ definiamo

$$H_w = \{x \in \mathbb{K}^n \mid w \cdot x = 0 \text{ (prodotto riga per colonna)}\},$$

ossia

$$H_w = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid w_1 x_1 + \cdots + w_n x_n = 0 \right\}.$$

Teorema 2.1. *Nelle notazioni precedenti se $w \neq 0$ allora H_w è un iperpiano di $\mathbb{K}^n$. Ogni iperpiano di $\mathbb{K}^n$ è uguale a H_w per qualche $w \neq 0$.*

Dimostrazione. La dimostrazione che H_w è un sottospazio vettoriale è facile ed è lasciata per esercizio. Sia $e_1, \ldots, e_n$ la base canonica di $\mathbb{K}^n$ e supponiamo, per fissare le idee che $w_1 \neq 0$, allora gli $n-1$ vettori

$$v_i = e_i - \frac{w_i}{w_1} e_1, \qquad i = 2, \ldots, n$$

apartengono ad H_w e sono linearmente indipendenti (esercizio: perché?) e quindi $\dim H_w \geq n-1$ d'altra parte $e_1 \notin H_w$ e quindi $H_w \neq \mathbb{K}^n$, $\dim H_w < n$.

Supponiamo adesso che $V \subset \mathbb{K}^n$ sia un iperpiano e scegliamo una base $v_1, \ldots, v_n$ di $\mathbb{K}^n$ tale che $v_2, \ldots, v_n \in V$. La matrice $A = (v_1, \ldots, v_n)$ che ha come vettori colonna i v_i è invertibile. Sia w il primo vettore riga della matrice A^{-1}. Dalla relazione $A^{-1}A = I$ si ricava che $w \cdot v_1 = 1$, $w \cdot v_i = 0$ per ogni $i > 1$. Dunque $v_2, \ldots, v_n \in H_w$ da cui se ne deduce che $V = H_w$. □

Lemma 2.2. *Sia $A \in M_{n,m}(\mathbb{K})$ una matrice. Allora:*

(1) *i vettori colonna generano $\mathbb{K}^n$ se e solo se i vettori riga sono linearmente indipendenti.*
(2) *i vettori riga generano $\mathbb{K}^{\times m}$ se e solo se i vettori colonna sono linearmente indipendenti.*

Dimostrazione. Dire che le righe sono linearmente indipendenti significa che l'unico vettore riga $x = (x_1, \dots, x_n)$ tale che $xA = 0$ è quello banale. Abbiamo visto che se le colonne generano, allora esiste una matrice B ale che $AB = I$ dunque se $xA = 0$ vale

$$0 = 0B = xAB - xI = x,$$

ossia $xA = 0$ implica $x = 0$ e le righe sono indipendenti. Viceversa se i vettori colonna non generano, il sottospazio da essi generato è contenuto in un iperpiano H_w per qualche $w \neq 0$; dimostriamo che $z = wA$ è il vettore riga nullo. Per ogni vettore $x \in \mathbb{K}^m$ il vettore Ax appartiene al sottospazio generato dalle colonne di A, dunque $Ax \in H_w$ e $wAx = zx = 0$. Prendendo $x = e_i$ vettori della base canonica otteniamo che

$$0 = ze_i = \text{ coordinata } i\text{-esima di } z$$

e dunque z è il vettore nullo.

Abbiamo dunque provato il primo enunciato: il secondo equivale al primo per la matrice trasposta. □

3. Rango di una matrice

Definizione 3.1. Il rango $r(A)$ di una matrice A è la dimensione del sottospazio vettoriale generato dai vettori colonna. Equivalentemente il rango è uguale al massimo numero di colonne linearmente indipendenti.

Osserviamo che per ogni matrice $A \in M_{n,m}(\mathbb{K})$ il rango $r(A)$ è sempre minore od uguale al minimo tra n ed m. Abbiamo dimostrato che una matrice quadrata $n \times n$ è invertibile se e solo se ha rango n.

Altre due semplici osservazioni:

(1) Se una matrice B è ottenuta da A eliminando una colonna, allora $r(B) \leq r(A)$. Questo è ovvio.
(2) Se una matrice C è ottenuta da A eliminando una riga, allora $r(C) \leq r(A)$. Infatti se $r(C) = r$ posso scegliere r colonne di C linearmente indipendenti e a maggior ragione le corrispondenti colonne di A sono ancora linearmente indipendenti.

Diremo che B è una sottomatrice di A se B si ottiene a partire da A eliminando alcune righe ed alcune colonne. Abbiamo visto che il rango di una sottomatrice di A è sempre minore od uguale al rango di A.

Teorema 3.2. *Il rango di una matrice $A \in M_{n,m}$ è uguale al massimo intero r tale che A possiede una sottomatrice $r \times r$ invertibile. In particolare il rango di una matrice non dipende dal campo in cui sono considerati i coefficienti.*

Dimostrazione. Sia r il rango di A. Siccome ogni sottomatrice ha rango $\leq r$ basta provare che A possiede una sottomatrice $r \times r$ invertibile. Sia $B \in M_{n,r}$ la sottomatrice ottenuta scegliendo un insieme di r colonne linearmente indipendenti. Per il Lemma 2.2 i vettori riga generano $\mathbb{K}^{\times r}$ e quindi se ne possono estrarre r linearmente indipendenti. Troviamo quindi una sottomatrice C di B quadrata di ordine r con le righe indipendenti. Dunque C è invertibile. □

Corollario 3.3. *Per ogni matrice A vale $r(A) = r(A^T)$. Dunque per ogni matrice il massimo numero di colonne indipendenti è uguale al massimo numero di righe indipendenti.*

Dimostrazione. Siccome la trasposta di una matrice invertibile è ancora invertibile, una matrice possiede una sottomatrice $r \times r$ invertibile se e solo se la sua trasposta ha la medesima proprietà. Basta quindi applicare il teorema precedente. □

Nota: per gli esercizi ed i metodi di calcolo della matrice inversa rimandiamo ad una futura dispensa.