Appunti per Geometria e Algebra Computazionale 3-4. Ideali zero-dimensionali. Diagonalizzazione simultanea. Matrici compagne in più variabili

Corso di Laurea in Matematica, Università di Firenze, 2019/20

Giorgio Ottaviani

23 maggio 2020

Una base del quoziente

Il seguente risultato è una conseguenza dell'additività della forma normale rispetto a un ideale.

Teorema

Sia $I \subset K[x_1, \ldots, x_n]$ *un ideale, fissiamo un ordine monomiale e sia* $S =< x^\alpha | x^\alpha \notin LT(I) >$ *sottospazio (su* K*) di* $K[x_1, \ldots, x_n]$*. Allora* $K[x_1, \ldots, x_n]/I \simeq S$ *come spazi vettoriali su* K*.*

Una base del quoziente, la dimostrazione, I

Dimostrazione.

Sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner per I. Indichiamo con $[f] \in K[x_1, \ldots, x_n]/I$ gli elementi del quoziente ($f \in K[x_1, \ldots, x_n]$) e definiamo $\phi : K[x_1, \ldots, x_n]/I \to S$ data da $\phi([f]) = \overline{f}^G$ (resto della divisione per G, che abbiamo indicato anche come $f \ \% \ I$, forma normale di f rispetto a I). Se $f = \sum h_i g_i + r$ è la divisione poniamo quindi $\phi([f]) = r$. ϕ è ben definito perché se $f - f' \in I$ abbiamo $f = \sum h_i g_i + r, f' = \sum h'_i g_i + r'$ (divisioni per G) e quindi $r - r' \in I$. Pertanto se $r \neq r'$ abbiamo $LT(r - r')$ divisibile per qualche $LT(g_j)$ (per definizione di base di Gröbner) in contraddizione con l'algoritmo di divisione. ϕ è suriettiva perchè se $x^\alpha \in S$ abbiamo $\phi([x^\alpha]) = x^\alpha$. Inoltre se $\overline{f}^G = \overline{f'}^G$ è ovvio che $f - f' \in I$, quindi ϕ è iniettiva. E' facile verificare che $\phi(k[f]) = k\phi([f])$. $\square$

Una base del quoziente, la dimostrazione, II

Dimostrazione.

Rimane da far vedere che ϕ conserva la somma. Infatti se $f = g + r, f' = g' + r'$ dove nessun termine di r, r' appartiene a $LT(I)$ segue che $f + f' = (g + g') + (r + r')$ dove nessun termine di $(r + r')$ appartiene a $LT(I)$. Per le proprietà della forma normale rispetto a I segue $\phi([f]) + \phi([f']) = \phi([f + f'])$. $\square$

Ideali zero-dimensionali

Teorema (Caratterizzazione degli ideali zero-dimensionali)

Sia $K = \mathbb{R}$ oppure $K = \mathbb{C}$ e $I \subset K[x_1, \ldots, x_n]$ un ideale. Sono equivalenti:

- *i) $V_{\mathbb{C}}(I)$ è finito*
- *ii) $\forall i = 1, \ldots, n$ $\exists m_i \geq 0$ tale che ${x_i}^{m_i} \in LT(I)$*
- *iii) lo spazio vettoriale $K[x_1, \ldots, x_n]/I (\simeq S$ vedi teor. 0.1) ha dimensione finita*

Dimostrazione.

- $i) \Rightarrow ii)$ Se $V_{\mathbb{C}}(I) = \emptyset$ abbiamo $1 \in LT(I)$ dal teorema degli zeri e basta porre $m_i = 0$. Se $V_{\mathbb{C}}(I) \neq \emptyset$ siano $\{a_j\}_{j \in J(i)}$ tutte le i-esime coordinate dei punti di $V_{\mathbb{C}}(I)$. Posto $f_i = \prod_{j \in J(i)} (x_i - a_j)$ abbiamo

  $f_i \in I(V_{\mathbb{C}}(I)) = \sqrt{I}$ dal teorema degli zeri.

  Quindi $\exists \quad k_i : {f_i}^{k_i} \in I$ e $LT({f_i}^{k_i}) =: {x_i}^{m_i} \in LT(I)$ come volevamo.

$\square$

Caratterizzazione degli ideali zero-dimensionali, conclusione della dimostrazione

Dimostrazione.

- $ii) \Rightarrow iii)$ Se $x^\alpha \in S =< x^\alpha | x^\alpha \notin LT(I) >$ (l'uguaglianza per il teorema sulla base del quoziente) deve essere $\alpha_i \leq m_i - 1$. Quindi $dimS \leq \prod_{i=1}^n m_i$.
- $iii) \Rightarrow i)$ Per ipotesi gli elementi $[1], [x_1], [{x_1}^2], \dots, [{x_1}^n], \dots$sono linearmente dipendenti, quindi $\exists \quad c_j \in J$ tali che $\sum c_j {x_1}^j \in I$. In particolare i punti di $V_\mathbb{C}(I)$ possono avere solo un numero finito di coordinate differenti al primo indice (le radici del polinomio precedente). Il ragionamento si ripete anche per gli altri indici.

$\square$

Criterio effettivo per stabilire se un ideale è zero-dimensionale

La condizione ii) del teorema precedente di caratterizzazione dà un algoritmo per stabilire se l'insieme delle soluzioni di un sistema di polinomi è finito, una volta calcolata una base di Gröbner. In caso affermativo la dimostrazione mostra anche che il numero delle soluzioni è limitato da $\prod_{i=1}^{n} m_i$ (se ci fossero $\prod_{i=1}^{n} m_i + 1$ soluzioni potrei costruire $\prod_{i=1}^{n} m_i + 1$ polinomi ciascuno dei quali si annulla in tutti i punti escluso uno, e questi polinomi sarebbero indipendenti in $K[x_1, \ldots, x_n]/I$).

Definizione

Un ideale che soddisfa una delle condizioni equivalenti del Teorema di caratterizzazione degli ideali zero-dimensionali si dice zero-dimensionale.

Esercizio sugli ideali zero-dimensionali

Esercizio

Nei casi seguenti determinare quando $V(I)$ è finito e limitare il numero dei punti di $V(I)$.

1. $I \subset \mathbb{C}[x, y, z]$ *con base di Gröbner data da* (x^2y, y^3z, z^5, xz)
2. $I \subset \mathbb{C}[x, y, z]$*con base di Gröbner data da* $(x^2, xy, y^3, yz^{10}, z^7)$
3. $I \subset \mathbb{C}[x_1, x_2, x_3, x_4]$ *con base di Gröbner data da* $(x_1^2, x_2^2, x_3^2, x_1x_4, x_2x_4, x_3x_4)$

Risposta: $V(I)$ è finito solo nel caso ii) ed il numero di punti è≤ 42.

Diagonalizzazione simultanea di più matrici

Teorema (Diagonalizzazione simultanea)

(i) Siano $A, B\colon V \to V$ due endomorfismi diagonalizzabili. Allora esiste una base di autovettori comuni a A e B se e solo se $AB = BA$.
(ii) Siano $A_1, \dots A_n\colon V \to V$ endomorfismi diagonalizzabili. Allora esiste una base di autovettori comuni a A_i per $i = 1, \dots, n$ se e solo se $A_iA_j = A_jA_i$ per ogni i, j.

Diagonalizzazione simultanea di più matrici, dimostrazione di (i)

Dimostrazione.

(i) Sia $\{v_1, \dots v_n\}$ una base comune di autovettori. Allora $Av_i = \lambda_i v_i$ e $Bv_i = \mu_i v_i$. Quindi $ABv_i = \lambda_i \mu_i v_i = BAv_i$. Quindi AB e BA assumono gli stessi valori su una base di V e pertanto sono uguali. Viceversa siano $V_{\lambda_i} = \ker(A - \lambda_i I)$ gli autospazi di A. Se $v \in V_{\lambda_i}$ allora $A(Bv) = B(Av) = B(\lambda_i v) = \lambda_i(Bv)$, da cui $Bv \in V_{\lambda_i}$. Quindi $B(V_{\lambda_i}) \subseteq V_{\lambda_i}$, cioè gli autospazi di A sono B-invarianti. Pertanto il polinomio caratteristico di B si fattorizza come prodotto dei polinomi caratteristici di $B_{|V_{\lambda_i}}$ e quindi gli autovalori di $B_{|V_{\lambda_i}}$ sono tutti in K. Inoltre il polinomio minimo di $B_{|V_{\lambda_i}}$ divide il polinomio minimo di B, siccome quest'ultimo per ipotesi non ha fattori ripetuti, neanche il polinomio minimo di $B_{|V_{\lambda_i}}$ ha fattori ripetuti e pertanto $B_{|V_{\lambda_i}}$ è diagonalizzabile. Mettendo insieme le basi di autovettori per $B_{|V_{\lambda_i}}$, si ottiene una base di autovettori comuni a A e B. $\square$

Diagonalizzazione simultanea di più matrici, dimostrazione di (ii)

Dimostrazione.

(ii) Se abbiamo una base comune di autovettori l'argomento è lo stesso del punto (i). Viceversa, possiamo ragionare per induzione su n. Se V_i sono gli autospazi di A_n, abbiamo come nel punto (i) che $A_j(V_i) \subseteq V_i$ per ogni i, j. Il ragionamento del punto (i) mostra che, per ogni i, gli $n-1$ endomorfismi $A_{j|V_i}$ per $j = 1, \ldots, n-1$ commutano a due a due e sono diagonalizzabili e quindi hanno una base di autovettori comuni su V_i. Mettendo insieme queste basi di autovettori comuni, si ottiene una base di autovettori comuni a tutti gli A_i.

$\square$

Diagonalizzazione simultanea con una matrice che ha autovalori distinti

Proposizione (Diagonalizzazione simultanea con una matrice che ha autovalori distinti)

Siano A_i per $i = 1, \dots, n$ endomorfismi tali che $A_i A_j = A_j A_i$ per ogni i, j. Sia A_1 diagonalizzabile con autovalori distinti. Allora ogni A_i è diagonalizzabile e tutti gli A_i hanno una base comune di autovettori.

Dimostrazione.

Per ipotesi, gli autospazi di A_1 $V_{\lambda_i} = \ker(A_1 - \lambda_i I)$ hanno dimensione uno. Come nella dimostrazione precedente abbiamo $A_j(V_{\lambda_i}) \subset V_{\lambda_i}$, e questo vuol dire che i generatori di V_{λ_i} sono autovettori anche per A_j. Pertanto A_j è diagonalizzabile e gli autovettori trovati sono comuni a tutti gli A_j. $\square$ $\square$

Triangolarizzazione simultanea

Proposizione (Matrici che commutano hanno autovettore comune)

Siano A_i per $i = 1, \ldots, n$ endomorfismi tali che $A_iA_j = A_jA_i$ per ogni i, j. Esiste un autovettore (complesso) comune a A_i.

Dimostrazione.

Sia λ_1 un autovalore di A_1. Allora $V_1 = \ker(A_1 - \lambda_1 I)$ è A_2-invariante, pertanto A_2 ha un autovettore su V_1 con autovalore λ_2 e $V_2 = \bigcap_{i=1}^{2} \ker(A_i - \lambda_i I) \neq 0$. Analogamente, V_2 è A_3-invariante, per cui esiste λ_3 tale che $V_3 = \bigcap_{i=1}^{3} \ker(A_i - \lambda_i I) \neq 0$. Proseguendo in questo modo, si trova $V_n = \bigcap_{i=1}^{n} \ker(A_i - \lambda_i I) \neq 0$, e ogni vettore non nullo in V_n è un autovettore comune a A_i. $\square$ $\square$

Dalla Proposizione precedente segue che un sottospazio di endomorfismi che commutano può essere ridotto (simultaneamente) a forma triangolare.

Matrici compagne in più variabili

Sia $I = (f_1, \ldots, f_k)$ un ideale zero dimensionale di $K[x_1, \ldots, x_n]$, dove $K = \mathbb{R}$ oppure $\mathbb{C}$. Questo significa che il sistema $f_1 = \ldots = f_k = 0$ ha un numero finito di soluzioni pari a d (contate con la relativa molteplicità), il quoziente $K[x_1, \ldots, x_n]/I$ ha dimensione d ed è generato dalle classi $[x^\alpha]$ di monomi non contenuti in $LT(I)$. Per ogni $f \in K[x_1, \ldots, x_n]/I$, calcolando con Macaulay2 $f\%I$, si ottiene l'espressione di f in questa base.
La moltiplicazione per x_i induce un'applicazione lineare

$$R \xrightarrow{M_{x_i}} R$$

$$[g] \mapsto [gx_i]$$

le matrici di M_{x_i} rispetto alla base $\{[x^\alpha] | x^\alpha \notin LT(I)\}$ si dicono *matrici compagne* di I. Nel caso di una variabile, la diagonalizzazione di M_x giocava un ruolo fondamentale. Nel caso di più variabili, è la diagonalizzazione simultanea delle M_{x_i} che entra in gioco.

Proposizione

$\forall h(x), k(x) \in K[x_1, \ldots, x_n]$ vale che
(i) $M_{h(x)} + M_{k(x)} = M_{h(x)+k(x)}$
(ii) $M_{ah(x)} = aM_{h(x)} \quad \forall a \in K$
(iii) $M_{h(x)} \cdot M_{k(x)} = M_{k(x)} \cdot M_{h(x)} = M_{h(x)k(x)}$
(iv) $M_{h(x_1,\ldots,x_n)} = h(M_{x_1}, \ldots, M_{x_n})$.

Dimostrazione.

(i), (ii) e (iii) sono immediate dalla definizione. Per provare (iv) supponiamo dapprima $h = x_j^i$. □

Proprietà elementari delle matrici compagne in più variabili, la dimostrazione.

Dimostrazione.

Allora $M_{x_j^i} = \left(M_{x_j}\right)^i$ come diretta applicazione di (iii).
In generale, se $h(x) = \sum a_\alpha x^\alpha$ allora, utilizzando anche (i)-(iii),

$$M_{h(x_1,\ldots,x_n)} = M_{\sum a_\alpha x^\alpha} = \sum a_\alpha M_{x^\alpha} =$$

$$= \sum a_\alpha \left(M_{x_1}\right)^{\alpha_1} \ldots \left(M_{x_n}\right)^{\alpha_n} = h(M_{x_1}, \ldots, M_{x_n})$$

$\square$

$\square$

Autovettori e autovalori di $p(A)$.

Lemma (Autovettori e autovalori di $p(A)$)

Se v è autovettore di A con autovalore λ e $p(x) \in K[x]$ è un polinomio allora

$$p(A)v = p(\lambda)v$$

cioè v è autovettore di $p(A)$ con autovalore $p(\lambda)$.

Dimostrazione.

Da $Av = \lambda v$ segue $A^k v = \lambda^k v$ per ogni $k \geq 0$. Quindi, se $p(x) = \sum_{i=0}^{d} a_i x^i$ abbiamo
$p(A)v = \sum_{i=0}^{d} a_i A^i v = \sum_{i=0}^{d} a_i \lambda^i v = p(\lambda)v$ $\square$ $\square$

Autovettori e autovalori delle matrici compagne in più variabili.

Lemma (Autovettori e autovalori delle matrici compagne in più variabili.)

Se $M_{x_i}v = \lambda_i v$ *e* $p \in K[x_1, \ldots, x_n]$ *allora*

$$p(M_{x_1}, \ldots, M_{x_n})v = p(\lambda_1, \ldots, \lambda_n)v$$

Dimostrazione.

È l'analogo multidimensionale del Lemma precedente su autovettori e autovalori di $p(A)$. $\square$