Appunti per Geometria e Algebra Computazionale 3-5. Decomposizione primaria. Molteplicità delle soluzioni.

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

Giorgio Ottaviani

29 maggio 2020

Decomposizione primaria e definizione di molteplicità

Sia $I \subset K[x_1, \ldots, x_n]$,dove $K = \mathbb{R}$ oppure $\mathbb{C}$, un ideale zero-dimensionale.
In questa sezione assegneremo una molteplicità a ogni punto $p_i \in V(I)$, analogamente a quanto avviene per le radici di un polinomio in una variabile, in modo che la somma delle molteplicità di tutte le soluzioni sia uguale alla dimensione di $K[x_1, \ldots, x_n]/I$

Sia M_i l'ideale massimale dei polinomi che si annullano in $p_i = ((p_i)_1, \ldots, (p_i)_n)$. L'ideale M_i è generato dai polinomi $x_j - (p_i)_j$. Con un piccolo abuso di notazione, indicheremo con M_i anche la sua immagine nel quoziente $\mathbb{C}[x_1, \ldots, x_n]/I$, che è ancora un ideale massimale.

Ideale radicale di un numero finito di punti.

Lemma

(i) $V(M_1 \cap \ldots \cap M_k) = p_1 \cup \ldots \cup p_k$.
(ii) Sia $V(I) = \{p_1, \ldots p_k\}$. *Vale* $\sqrt{I} = M_1 \cap \ldots \cap M_k$.
Questo significa che $g \in \sqrt{I}$ *se e solo se* $g(p_i) = 0$ *per* $i = 1, \ldots, k$. *In particolare, per ogni elemento del quoziente* $g \in \mathbb{C}[x_1, \ldots, x_n]/I$, *la valutazione* $g(p_i) \in \mathbb{C}$ *è ben definita e non dipende dal rappresentante.*

Dimostrazione.

(i) è elementare e segue dalle proprietà della topologia di Zariski. Per provare (ii), se $f \in \sqrt{I}$ allora esiste $m > 0$ tale che $f^m(p_i) = 0$, da cui $f(p_i) = 0$ e quindi $f \in M_1 \cap \ldots \cap M_k$. Viceversa, per il teorema degli zeri, $\sqrt{I} = I(V(I)) = I(p_1 \cup \ldots \cup p_k) = I(V(M_1 \cap \ldots \cap M_k)) = \sqrt{M_1 \cap \ldots \cap M_k} \supset M_1 \cap \ldots \cap M_k$.

Il polinomio h che prende valori distinti sui punti

Lemma

Dato $V(I) = \{p_1, \dots p_k\} \subset \mathbb{C}^n$, esiste un polinomio $h(x)$ tale che $h(p_i)$ siano distinti (si veda la Figura alla slide seguente). Se I è generato da polinomi a coefficienti reali, allora $h(x)$ puo' essere scelto a coefficienti reali. In tale caso, per ogni coppia di punti complessi coniugati $\{p, \overline{p}\}$, abbiamo $h(\overline{p}) = \overline{h(p)}$.

Dimostrazione.

Il prodotto scalare euclideo si può estendere (algebricamente) a $\mathbb{C}^n$ ponendo $(z_1, \dots, z_n) \cdot (w_1, \dots, w_n) = \sum_{i=1}^{n} z_i w_i$, $\forall (z_1, \dots, z_n), (w_1, \dots, w_n) \in \mathbb{C}^n$. E' sufficiente scegliere un vettore $H = (h_1, \dots, h_n)$ tale che il prodotto scalare euclideo $H \cdot (p_i - p_j) \neq 0 \ \forall i \neq j$. Questo è possibile perché $(p_i - p_j)$ sono un numero finito di vettori. Allora $h(x) = \sum_{i=1}^{n} h_i x_i$ soddisfa la condizione richiesta. □

Esempio di polinomio h che prende valori distinti su 4 punti

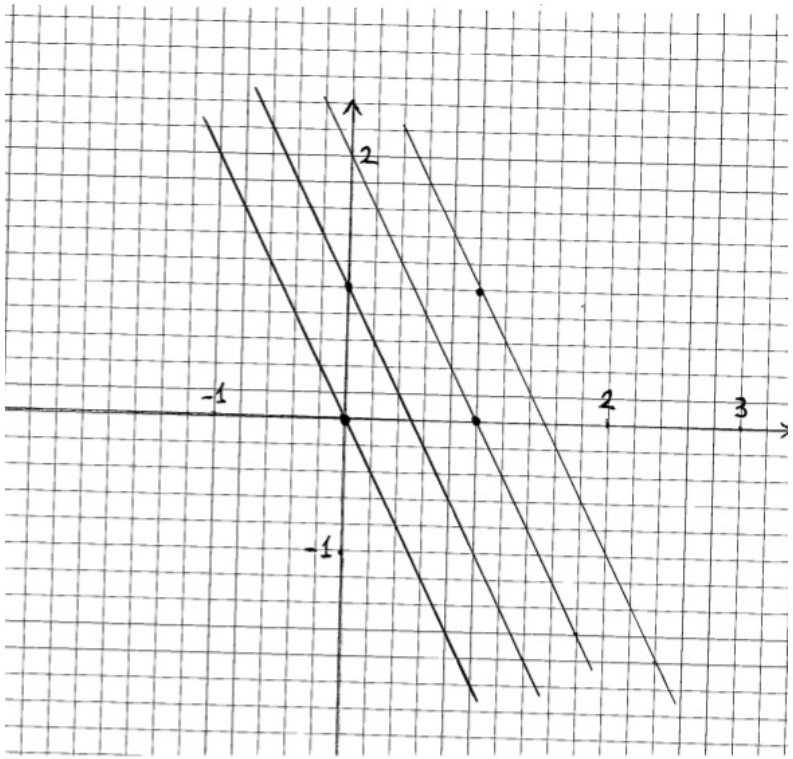

Figura: In figura i quattro punti $p_1 = (0, 0)$, $p_2 = (1, 0)$, $p_3 = (0, 1)$, $p_4 = (1, 1)$ corrispondono a $V(I)$ dove $I = (x(x-1), y(y-1))$. Posto $h(x, y) = 2x + y$, il fascio di rette parallele $h(x, y) = \lambda$ incontra $V(I)$ per i 4 valori $\lambda = h(p_i)$. I quattro autovalori di $M_{h(x)}$ sono $h(p_i)$. Ciascun punto ha molteplicità 1. In questo caso, M_x e M_y non hanno autovalori distinti (quali sono?).

Gli elementi invertibili dell'anello quoziente

Lemma

Sia $V(I) = \{p_1, \dots p_k\}$. *Un elemento del quoziente* $g \in \mathbb{C}[x_1, \dots, x_n]/I$ *è invertibile se e solo se* $g(p_i) \neq 0 \ \forall i$.

Dimostrazione.

Se g è invertibile, segue immediatamente che $g(p_i) \neq 0$. Viceversa, supponiamo $g(p_i) \neq 0 \ \forall i$. Abbiamo visto che esiste $h(x)$ tale che $h(p_i)$ sono distinti. Definiamo $g'(x) = \sum_{i=1}^{k} \frac{1}{g(p_i)} \prod_{j \neq i} \frac{h(x)-h(p_j)}{h(p_i)-h(p_j)}$, che soddisfa le uguaglianze $g(p_i)g'(p_i) = 1 \ \forall i$. Per il Lemma iniziale (ii) abbiamo $1 - gg' \in \sqrt{I}$, da cui esiste $m > 0$ tale che $(1 - gg')^m \in I$. Espandendo la potenza m-esima e raccogliendo i termini che contengono g, si trova $\tilde{g}$ tale che $1 - \tilde{g}g \in I$, da cui g è invertibile nel quoziente , come volevamo. □

Gli autovalori di M_h corrispondono ai valori assunti da h.

Lemma

Sia $V(I) = \{p_1, \dots p_k\} \subset \mathbb{C}^n$, *e sia* $h(x) \in \mathbb{C}[x_1, \dots, x_n]$. *Gli autovalori di* $M_{h(x)} \colon \mathbb{C}[x_1, \dots, x_n]/I \to \mathbb{C}[x_1, \dots, x_n]/I$ *coincidono con i valori* $h(p_i) \in \mathbb{C}$.

Dimostrazione.

Sia λ l' autovalore di $M_{h(x)}$ corrispondente all'autovettore $v(x)$. Allora $(h(x) - \lambda)\, v(x) \in I$. Affermiamo che $h(p_i) = \lambda$ per qualche i. Se per assurdo $h(p_i) - \lambda \neq 0 \ \forall i$, allora $h(x) - \lambda$ è invertibile per il Lemma 0.3. Quindi $v(x) \in I$, che è una contraddizione perché gli autovettori sono non nulli.
Viceversa, proviamo che $h(p_i)$ è un autovalore di $M_{h(x)}$. Sia $q(t)$ il polinomio minimo di $M_{h(x)}$. Allora $0 = q(M_{h(x)}) = M_{q(h(x))}$.
Quindi $q(h(x)) \in I$, da cui, valutando in p_i, $q(h(p_i)) = 0$, pertanto $h(p_i)$ è un autovalore. □

Gli autovalori di M_{x_i} sono le coordinate i-esime dei punti p_i.

Osservazione

Applicando il Lemma precedente alle matrici M_{x_i} si ottiene che le coordinate i-esime dei punti di $V(I)$ coincidono con gli autovalori di M_{x_i}. Questa è già un'informazione importante per calcolare i punti di $V(I)$, ma richiede lavoro supplementare per stabilire quali coordinate corrispondono allo stesso punto. Un metodo più efficiente è descritto dalla proposizione che vedremo in GAC3-6.

Riepilogo sugli ideali primari

Ricordiamo che un ideale J si dice *primario* se $fg \in J$ implica $f \in J$ oppure $g^m \in J$ per qualche $m > 0$. Per gli ideali valgono le implicazioni

$$\text{massimale} \Longrightarrow \text{primo} \Longrightarrow \text{primario}.$$

e ciascuna delle implicazioni precedenti è stretta. Se J è primario allora $\sqrt{J}$ è primo, ma il viceversa è falso. Però se $\sqrt{J}$ è massimale allora J è primario.
Segue immediatamente dalla definizione che il radicale di un ideale primario è primo.

Decomposizione primaria di un ideale zero-dimensionale. Versione con somma diretta

Teorema (Decomposizione primaria, somma diretta)

Sia $V(I) = \{p_1, \ldots, p_k\}$. *Sia* $h(x) \in \mathbb{C}[x_1, \ldots, x_n]$ *tale che* $h(p_i)$ *siano distinti (si veda il Lemma precedente).*
Considero per $i = 1, \ldots, k$ *le applicazioni lineari*

$$M_{h(x)-h(p_i)} \colon \mathbb{C}[x_1, \ldots, x_n]/I \to \mathbb{C}[x_1, \ldots, x_n]/I$$

Posto $A_i := \ker \left[M_{h(x)-h(p_i)}\right]^{\infty}$ *, abbiamo la decomposizione diretta di sottoalgebre*

$$\mathbb{C}[x_1, \ldots, x_n]/I = \oplus_{i=1}^{k} A_i. \tag{0.1}$$

Se $v(x) \in A_i$ *allora* $v(p_j) = 0 \ \forall j \neq i$. *Ogni sottoalgebra* A_i *ha un elemento unità* e_i, *che soddisfa le proprietà* $e_i^2 = e_i$, $e_i e_j = 0$ *per* $i \neq j$. *Inoltre, valutando in* p_j, $e_i(p_j) = \delta_{ij}$. *Gli elementi* $g \in A_i$ *sono invertibili in* A_i *se e solo se* $g(p_i) \neq 0$.

Dimostrazione della decomp. primaria con $\oplus$

Dimostrazione.

La somma diretta segue dalla decomposizione in autospazi generalizzati dell'Algebra Lineare. E' facile verificare dalla definizione che A_i è un ideale. Se $v(x) \in A_i$ allora esiste n_i tale che $(h(x) - h(p_i))^{n_i} v(x) \in I$, da cui valutando per $x = p_j$ segue $v(p_j) = 0$. L'unità e_i di ogni sottoalgebra A_i proviene dalla decomposizione in somma diretta $1 = \sum_{i=1}^{k} e_i$, risolubile dividendo 1 per i generatori di ciascuna A_i (aggiungendo eventualmente i generatori di I), si può applicare il comando *"quotientRemainder"* di M2. L'elemento e_i funge da unità in A_i perché, preso $a_i \in A_i \subset \mathbb{C}[x_1, \ldots, x_n]/I$, moltiplicando per 1 abbiamo $a_i = 1 \cdot a_i = \sum_{j=1}^{k} e_j a_i = e_i a_i$.

Se $i \neq j$, abbiamo $e_i e_j \in A_i \cap A_j = 0$, da cui $1 = 1^2 = \sum_{i=1}^{k} e_i^2$ e per l'unicità della decomposizione $e_i^2 = e_i$. L'affermazione sull'invertibilità segue applicando il Lemma sugli elementi invertibili del quoziente al caso $k = 1$ in cui $V(I)$ contiene un solo punto. $\square$

Decomposizione primaria di un ideale zero-dimensionale. Versione con intersezione

Teorema (Decomposizione primaria, intersezione)

Posto $J_i = \oplus_{j \neq i} A_j$, *ideale di* $\mathbb{C}[x_1, \ldots, x_n]/I$, *la sua retroimmagine* $\tilde{J}_i \subset \mathbb{C}[x_1, \ldots, x_n]$ *è un ideale primario, tale che* $\sqrt{\tilde{J}_i} = M_i$, $A_i = \mathbb{C}[x_1, \ldots, x_n]/(\tilde{J}_i)$,

$$\cap_{i=1}^{n} \tilde{J}_i = I. \tag{0.2}$$

L' intersezione (0.2) si dice la decomposizione primaria di I.
Notiamo che e_i *corrisponde alla classe di* 1 *modulo* $\tilde{J}_i$.

Dimostrazione della decomp. primaria con intersezione

Dimostrazione.

Per come è definito l'ideale $\tilde{J}_i$, abbiamo $\mathbb{C}[x_1, \ldots, x_n]/\tilde{J}_i \simeq A_i$. Notiamo che $\cap_{i=1}^n J_i = 0$, da cui prendendo le retroimmagini $\cap_{i=1}^n \tilde{J}_i = I$. Valutando gli elementi unità e_i abbiamo $p_i = V(\tilde{J}_i)$, dal Nullstellensatz segue che $\sqrt{\tilde{J}_i} = M_i$, ideale massimale, segue che $\tilde{J}_i$ è primario. □

Localizzazione. Molteplicità di un punto.

Osservazione

Gli anelli A_i hanno come unico ideale massimale M_i e sono quindi anelli locali. La decomposizione (0.1) spiega l'origine del termine locale. Ogni A_i corrisponde a localizzare in un punto p_i , cioè la classe di un polinomio in A_i è influenzata soltanto dal comportamento vicino a p_i e può essere ricostruita da un opportuno sviluppo di Taylor nel punto p_i (rispetto ai monomi $\notin \tilde{J}_i$). In particolare la localizzazione di A in M_i coincide con A_i. Infatti l'elemento $e_i \notin M_i$ soddisfa $e_i A_j = 0$ per $j \neq i$ e quindi localizzando rispetto a M_i gli addendi A_j per $j \neq i$ sono identificati a zero.

Definizione

$\dim A_i$ *si dice molteplicità di p_i in I, la indicheremo con m_{p_i}, non dipende dal polinomio $h(x)$ scelto nella decomposizione primaria.*

Unicità della decomposizione primaria, I.

Il fatto che la molteplicità sia ben definita e non dipenda da $h(x)$ segue dal fatto che A_i ha una definizione intrinseca come localizzato di A rispetto a M_i. Per provare che la molteplicità non dipende da $h(x)$, con un ragionamento diretto ed elementare, prendiamo un altro polinomio $h'(x)$ che assume valori distinti sui punti p_i. Si osserva che A_i è $h'(x)$-invariante. Siccome $A_i = \mathbb{C}[x_1, \ldots, x_n]/(\tilde{J}_i)$ e $V(\tilde{J}_i) = V(\sqrt{\tilde{J}_i}) = \{p_i\}$ dal Teorema sulla decomposizione primaria, segue che l'unico autovalore di $M_{h'(x)}$ su A_i è $h'(p_i)$ per il Lemma sugli autovalori di M_h, applicato al caso $I = \tilde{J}_i$. Pertanto l' autospazio generalizzato A_i di $M_{h(x)}$ relativo all'autovalore $h(p_i)$ è contenuto nell' autospazio generalizzato A'_i di $M_{h'(x)}$ relativo all'autovalore $h'(p_i)$. Sia la somma dei A_i che quella dei A'_i sono entrambe dirette, quindi vale l'uguaglianza $A_i = A'_i$.
Come conseguenza di questo ragionamento enunciamo esplicitamente la

Unicità della decomposizione primaria, II.

Proposizione

(i) Sia $h(x)$ un polinomio che assume valori distinti sui punti p_i. Gli ideali A_i sono gli autospazi generalizzati di $M_{h(x)}$ e l'unico autovalore di $M_{h(x)}$ su A_i è $h(p_i)$.
(ii) Per ogni polinomio $k(x)$, l'unico autovalore di $M_{k(x)}$ su A_i è $k(p_i)$ (segue dal Lemma 0.4 applicato al caso $I = \tilde{J}_i$).
(iii) La sottoalgebra A_i del teorema sulla decomposizione primaria dipende solo da I.
(iv) La decomposizione primaria $I = \cap_{i=1}^{n} \tilde{J}_i$ è unica.

Esercizio

Modificando la figura precedente con i 4 punti 0.1, consideriamo $I = \big(x^2(x-1), y(y-1)\big)$. *Provare che, con le notazioni della figura,* $V(I) = \{p_1, p_2, p_3, p_4\}$, *la molteplicità di* p_1, p_3 *è* 2, *la molteplicità di* p_2, p_4 *è* 1.

Corollario

La somma delle molteplicità di ciascun p_i in I è uguale alla dimensione di $\mathbb{C}[x_1, \ldots, x_n]/I$.

Corollario

Vale $I = \sqrt{I}$ se e solo se tutti i punti hanno molteplicità 1 in I.

Dimostrazione.

Basta confrontare

$$\mathbb{C}[x_1, \ldots, x_n]/I = \oplus_{i=1}^{k} \mathbb{C}[x_1, \ldots, x_n]/\tilde{J}_i$$

con

$$\mathbb{C}[x_1, \ldots, x_n]/\sqrt{I} = \oplus_{i=1}^{k} \mathbb{C}[x_1, \ldots, x_n]/M_i,$$

dove nella seconda somma gli addendi hanno dimensione 1, si veda (ii) del primo Lemma di GAC3-5. □