Appunti per Geometria e Algebra Computazionale
2-3. Il Teorema di estensione e la dimostrazione del Teorema degli zeri

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

Giorgio Ottaviani

17 aprile 2020

Il problema di estensione delle soluzioni

Notiamo che dati due qualunque polinomi f, $g \in K[x, y]$, i punti di coordinate (x, y) appartenenti a $V(f, g)$ hanno la seconda coordinata che annulla ogni polinomio $q(y)$ nell'ideale di eliminazione.

È interessante chiedersi il viceversa, cioè ogni radice y_0 del polinomio generatore dell'ideale di eliminazione corrisponde a qualche $(x_0, y_0) \in V(f, g)$?Nell'esempio precedente la risposta è affermativa ma aumentando il numero delle variabili ci vogliono delle ipotesi opportune. Questo problema va sotto il nome di problema di *estensione delle soluzioni*.

Proiezione ed eliminazione

Lemma

Sia $I \subseteq K[x_1, \ldots, x_n]$ *e* I_1 *il primo ideale di eliminazione. Sia* π_1 *la proiezione sulle ultime* $(n-1)$ *indeterminate. Allora* $\pi_1(V(I)) \subseteq V(I_1)$

Dimostrazione.

Sia $(a_2, \ldots, a_n) \in \pi_1(V(I))$. Pertanto esiste $a_1 \in K$ tale che $(a_1, a_2, \ldots, a_n) \in V(I)$. Se $f \in I_1$ abbiamo $f(a_1, a_2, \ldots, a_n) = f(a_2, \ldots, a_n) = 0$ da cui $(a_2, \ldots, a_n) \in V(I_1)$ come volevamo. □

Può valere l'inclusione stretta

L'uguaglianza può non valere nell'inclusione $\pi_1(V(I)) \subseteq V(I_1)$, come è mostrato dal seguente esempio in tre variabili.

Esempio

Siano $f := xy - 1, g := xz - 1 \in K[x, y, z]$ *Eliminando la* x *troviamo* $y - z = -yg + zf$ *che è un generatore del primo ideale di eliminazione. Preso il punto di coordinate* $(y, z) = (a, a)$ *questo si estende a* $(\frac{1}{a}, a, a) \in V(f, g)$ *se* $a \neq 0$ *ma se* $a = 0$ *la soluzione non si estende! Il motivo è che il coefficiente di* x *si annulla per* $(a, a) = (0, 0)$*. Geometricamente la soluzione è andata all'infinito. In questo esempio, posto* $I = (f, g)$*, abbiamo*
$V(I) = \{(\frac{1}{a}, a, a) | a \neq 0\}$,
$\pi(V(I)) = \{(a, a) | a \neq 0\} \subsetneq \{(a, a)\} = V(I_1)$.

Il teorema di estensione

Teorema (Teorema di estensione, (Teorema fondamentale della teoria dell'eliminazione, caso affine))

Sia K un campo algebricamente chiuso. Siano

$$f_1 := g_1(x_2, \ldots, x_n)x_1^{N_1} + \ldots$$

$$\vdots$$

$$f_k := g_k(x_2, \ldots, x_n)x_1^{N_k} + \ldots$$

polinomi in $K[x_1, \ldots, x_n]$ e sia $I = (f_1, \ldots, f_k)$. Posto $I_1 := I \cap K[x_2, \ldots, x_n]$, sia $(a_2, \ldots, a_n) \in V(I_1)$ "soluzione parziale". Se $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_k)$ allora $\exists \quad a_1 \in K$ tale che $(a_1, a_2, \ldots, a_n) \in V(I)$.

La dimostrazione del teorema di estensione, I

Dimostrazione.

Possiamo assumere (rinumerando eventualmente $f_1, \ldots, f_k$) che $g_1(a_2, \ldots, a_n) \neq 0$. Introduciamo delle nuove indeterminate $u_2, \ldots, u_k$ e consideriamo

$$Res(f_1, u_2 f_2 + \ldots + u_k f_k, x_1) = A f_1 + B(u_2 f_2 + \ldots + u_k f_k) = \sum h_\alpha u^\alpha$$

dove $u^\alpha = u_2^{\alpha_2} \ldots u_k^{\alpha_k}$ $\quad A, B \in K[u_2, \ldots, u_k, x_1, \ldots, x_n]$ $h_\alpha \in K[x_2, \ldots, x_n]$. Sviluppando l'ultima uguaglianza si ottiene $h_\alpha \in I_1$ e quindi $h_\alpha(a_2, \ldots, a_n) = 0 \quad \forall \alpha$. Sostituendo eventualmente f_2 con $\tilde{f}_2 := f_2 + x_1^N f_1$ $(N \gg 0)$ possiamo supporre che $g_2(a_2, \ldots, a_n) \neq 0$ e che f_2 ha grado in x_1 maggiore di $f_3, \ldots, f_n$. □

La dimostrazione del teorema di estensione, II

Dimostrazione.

Lavoriamo adesso in $K[x_1, u_2, \ldots, u_k]$ sostituendo $(x_2, \ldots, x_n) = (a_2, \ldots, a_n)$. Allora

$$Res(f_1, u_2 f_2 + \ldots + u_k f_k, x_1)_{|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)} = 0 \qquad (0.1)$$

Siccome i leading term in x_1 di f_1 e di $u_2 f_2 + \ldots + u_k f_k$ non si annullano quando sostituisco $(x_2, \ldots, x_n) = (a_2, \ldots, a_n)$ possiamo dire che il risultante precedente coincide con il risultante tra $f_{1|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)}$ e $u_2 f_2 + \ldots + u_k f_{k|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)}$ nell'anello $K[x_1, u_2, \ldots, u_k]$. Per le proprietà del risultante segue che $f_1(x_1, a_2, \ldots, a_n)$ e $(u_2 f_2 + \ldots + u_k f_k)_{|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)}$ in $K[x_1, u_2, \ldots, u_k]$ hanno a comune un fattore F di grado positivo in x_1. Siccome $F | f_1(x_1, a_2, \ldots, a_n)$ abbiamo $F \in K[x_1]$ e quindi F divide anche $f_2(x_1, a_2, \ldots, a_n), \ldots, f_k(x_1, a_2, \ldots, a_n)$. Per ipotesi $K = \overline{K}$, quindi esiste $a_1 \in K$ tale che $F(a_1) = 0$ da cui $f_i(a_1, a_2, \ldots, a_n) = 0$ e quindi $(a_1, a_2, \ldots, a_n) \in V(I)$ c.v.d. □

Il Nullstellensatz debole

Vediamo ora come utilizzare il teorema di estensione per provare il teorema degli zeri di Hilbert .
Come passo intermedio, importante di per sé, si prova che il teorema degli zeri equivale ad una versione "debole" (qui il teorema di estensione ancora non interviene). La versione debole segue poi facilmente dal teorema di estensione.

Teorema

Nullstellensatz debole. Sia K un campo algebricamente chiuso e I un ideale di $K[x_1, \ldots, x_n]$. Abbiamo

$$V(I) = \emptyset \Longleftrightarrow I = K[x_1, \ldots, x_n]$$

Il Nullstellensatz equivale alla versione debole, I

Proposizione

$$\textit{Nullstellensatz} \iff \textit{Nullstellensatz debole}$$

Dimostrazione.

- " $\Longrightarrow$ " Sia $V(I) = \emptyset$, allora per il Nullstellensatz $\sqrt{I} = (1)$ da cui $I = (1)$. Il viceversa è evidente.
- " $\Longleftarrow$ " Sia $f \in I(V(f_1, \ldots, f_s))$. Vogliamo provare che esiste m tale che $f^m \in (f_1, \ldots, f_s)$. Sia $\tilde{I} := (f_1, \ldots, f_s, 1 - yf) \subset K[x_1, \ldots x_n, y]$ (*Rabinowitsch trick*). Affermiamo che $V(\tilde{I}) = \emptyset$. Se per assurdo esiste $P_0 := (a_1, \ldots, a_n, y_0) \in V(\tilde{I})$ allora in particolare $f_i(a_1, \ldots, a_n) = 0$, e quindi $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ da cui $f(a_1, \ldots, a_n) = 0$. Pertanto $1 - yf$ vale 1 nel punto P_0 e questa è una contraddizione.

Il Nullstellensatz equivale alla versione debole, II

Dimostrazione.

Per il Nullstellensatz debole segue $\tilde{I} = K[x_1, \dots x_n, y]$, da cui

$$1 = \sum p_i(x_1, \dots, x_n, y) f_i + q(x_1, \dots, x_n, y)(1 - yf)$$

Sostituendo $y = 1/f$ abbiamo

$$1 = \sum p_i(x_1, \dots, x_n, \frac{1}{f}) f_i$$

I termini della somma a secondo membro sono funzioni razionali aventi a denominatore qualche potenza di f. Raccogliendo sotto un unico denominatore si ottiene:

$$f^m = \sum \tilde{p}_i(x_1, \dots, x_n) f_i$$

come volevamo. □

Esercizio

Esercizio

Sia $J = \left(x^2 + y^2 - 1, y - 1\right) \subset \mathbb{R}[x, y]$. *Trovare* $f \in I(V(J))$ *tale che* $f \notin J$.

Dimostrazione del Nullstellensatz debole, I

Se $n = 1$ il teorema è vero perché K é algebricamente chiuso, quindi ragioniamo per induzione su n.Se $V(I) = V((f_1, \ldots, f_k)) = \emptyset$ vogliamo provare che $(f_1, \ldots, f_k) = (1)$. Possiamo assumere che

$$f_i(x_1, \ldots, x_n) = c_i x_1^{N_i} + \ldots$$

con $c_i \neq 0$. Infatti consideriamo l'automorfismo ϕ di $K[x_1, \ldots, x_n]$ definito da

$$x_1 \mapsto x_1$$

$$x_2 \mapsto x_2 + a_2 x_1$$

$$\vdots$$

$$x_n \mapsto x_n + a_n x_1$$

con $a_2, \ldots, a_n$ da determinare (l'inversa di ϕ si ottiene cambiando i segni precedenti da $+$ a $-$). Abbiamo $V(\phi(f_1), \ldots, \phi(f_k)) = \emptyset$ perché $\phi(f)(x_1, \ldots, x_n) = f(\phi(x_1), \ldots, \phi(x_n))$ ed ovviamente:

$$I = (1) \Longleftrightarrow \phi(I) = (1)$$

Dimostrazione del Nullstellensatz debole, II

Sia $\phi(x^\alpha) = g_\alpha(a_2, \ldots, a_n)x_1^{\sum \alpha_i} + \ldots$ (termini di grado inferiore in x_1), dove $g_\alpha = x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, e quindi se $f_i = c_i(x_2, \ldots, x_n)x_1^{N_i} + \ldots$ (termini di grado inferiore in x_1), segue $\phi(f_i) = c_i(a_2, \ldots, a_n)x_1^{N_i} + \ldots$. Basta quindi scegliere $a_2, \ldots, a_n$ in modo che $c_i(a_2, \ldots, a_n) \neq 0$ per qualche i (ad esempio $i = 1$). Adesso possiamo applicare il teorema di estensione. Se fosse $V(I_1) \neq \emptyset$ avrei anche $V(I) \neq \emptyset$ che è una contraddizione.Quindi $V(I_1) = \emptyset$ e per l'ipotesi induttiva $1 \in I_1 \subset I$. □

La dimostrazione del teorema degli zeri è così completa !

L'ideale (1)

Lemma

La base di Gröbner dell'ideale (1) *contiene* $\{1\}$ *per ogni ordinamento monomiale.*

Dimostrazione.

Dalle proprietà degli ordini monomiali, segue subito che $LT(1) = (1)$. Inoltre se un polinomio f ha 1 come leading term, siccome 1 è minore di qualunque monomio, segue che $f = 1$. Pertanto una base di Groebner per tutto l'anello (1) deve contenere l'elemento 1. □

L'algoritmo di consistenza

Dal Nullstellensatz (debole) segue in particolare

Teorema

[Algoritmo di consistenza.] Siano $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ con K algebricamente chiuso. Vale:

$$\textit{Il sistema } f_i(x_1, \ldots, x_n) = 0 \textit{ ha una soluzione} \iff \textit{La base di Gröbner dell'ideale } (f_1, \ldots, f_s) \textit{ non contiene } \{1\}$$

Gli ideali massimali di $K[x_1, \ldots, x_n]$

Teorema

Sia K algebricamente chiuso. Gli ideali massimali di $K[x_1, \ldots, x_n]$ sono tutti e soli quelli della forma $(x_1 - a_1, \ldots, x_n - a_n)$

Dimostrazione.

Abbiamo $\frac{K[x_1,\ldots,x_n]}{(x_1-a_1,\ldots,x_n-a_n)} \simeq K$ e quindi $(x_1 - a_1, \ldots, x_n - a_n)$ è massimale, e coincide con l'ideale $I(p)$ dei polinomi che si annullano in $p = (a_1, \ldots, a_n)$. Viceversa sia I un ideale massimale. Dal Nullstellensatz debole abbiamo che esiste $(a_1, \ldots, a_n) \in V(I)$. Pertanto

$$I \subset I(V(I)) \subset I(a_1, \ldots a_n) = (x_1 - a_1, \ldots x_n - a_n)$$

e per la massimalità vale l'uguaglianza. □

Gli ideali massimali del quoziente $K[x_1, \ldots, x_n]/I(V)$

Corollario

Sia K algebricamente chiuso e sia $V \subset K^n$ una varietá algebrica affine. Allora gli ideali massimali di $K[x_1, \ldots, x_n]/I(V)$ sono tutti e soli quelli della forma $(x_1 - a_1, \ldots, x_n - a_n)$ con $(a_1, \ldots, a_n) \in V$.

Dimostrazione.

É sufficiente osservare che gli ideali di $K[x_1, \ldots, x_n]/I(V)$ sono in corrispondenza biunivoca con gli ideali di $K[x_1, \ldots, x_n]$ che contengono $I(V)$ e che
$I(V) \subset (x_1 - a_1, \ldots x_n - a_n) \Longleftrightarrow (a_1, \ldots, a_n) \in V$. □

Esercizi

1. Si consideri il sistema di equazioni

$$x^2 + 2y^2 = 3$$
$$x^2 + xy + y^2 = 3$$

Se I è l'ideale generato da queste equazioni, si trovino generatori per $I \cap K[x]$ e $I \cap K[y]$. Si trovino tutte le soluzioni del sistema se $K = \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$.

2. Come nell'esercizio 1. per il sistema

$$x^2 + 2y^2 = 2$$
$$x^2 + xy + y^2 = 2$$

3. Trovare generatori per gli ideali di eliminazione I_1 e I_2 dove I è l'ideale generato da

$$\begin{cases} x^2 + y^2 + z^2 = 4 \\ x^2 + 2y^2 = 5 \\ xz = 1 \end{cases}$$

Esercizi

4. Si consideri il sistema di equazioni

$$x^5 + \frac{1}{x^5} = y$$

$$x + \frac{1}{x} = z$$

Sia I l'ideale in $\mathbb{C}[x, y, z]$ determinato da queste equazioni.

- a. Trovare una base per $I_1 \subset \mathbb{C}[y, z]$ e provare che $I_2 = 0$.
- b. Usare il teorema di estensione **??** per provare che ogni soluzione parziale $c \in V(I_2) = \mathbb{C}$ estende ad una soluzione $(x_0, y_0, c) \in V(I)$.
- c.Quali soluzioni parziali $(y, z) \in V(I_1) \subset \mathbb{R}^2$ si estendono a soluzioni in $V(I) \subset \mathbb{R}^3$? Confrontare la risposta con quanto affermato dal teorema di estensione.
- d. Guardando z come "parametro", risolvere il sistema con x, y funzioni razionali di z e trovare così una parametrizzazione di $V(I)$.

Esercizi

5. Siano f, $g \in \mathbb{C}[x, y]$. Questo esercizio è una guida per provare che

   $V(f, g)$ è infinito $\iff$ f e g hanno un fattore a comune non co

   - a. Provare che se f è non costante allora $V(f)$ è infinito (ridursi al teorema fondamentale dell'algebra in una variabile) .
   - b. Provare $\Longleftarrow$ utilizzando il punto a.
   - c. Provare $\Longrightarrow$ mostrando che se f e g non hanno fattori non costanti a comune allora $Res(f, g, x)$ e $Res(f, g, y)$ sono entrambi non nulli.

6. Sia K algebricamente chiuso e siano $y_1, \ldots, y_k$ tutte le radici di $Res(f, g, x)$ e $x_1, \ldots, x_s$ tutte le radici di $Res(f, g, y)$. Provare che tutte le soluzioni del sistema $\begin{cases} f = 0 \\ g = 0 \end{cases}$ sono contenute tra le (x_i, y_j) per $i = 1, \ldots s$, $j = 1, \ldots, k$ (è sufficiente quindi eseguire un numero finito di verifiche per conoscere tutte le soluzioni)

Il Teorema di chiusura

Teorema

Teorema di chiusura (Interpretazione geometrica dell'eliminazione). Sia $V = V(I) \subset K^n$ una varietà algebrica affine e sia K algebricamente chiuso. Sia $K^n \xrightarrow{\pi_t} K^{n-t}$ la proiezione sulle ultime $n - t$ coordinate. Allora

$$V(I_t) = \overline{\pi_t(V)}$$

Dimostrazione.

Intanto notiamo che $\pi_t(V) \subset V(I_t)$. Infatti sia $(a_1, \ldots, a_n) \in V$ e quindi $(a_{t+1}, \ldots, a_n) \in \pi_t(V)$. Se $f \in I_t$ abbiamo $f(a_{t+1}, \ldots, a_n) = f(a_1, \ldots, a_n) = 0$ e quindi

$$(a_{t+1}, \ldots, a_n) \in V(I_t)$$

Pertanto $V(I_t) \supset \overline{\pi_t(V)}$. □

Dimostrazione del teorema di chiusura

Dimostrazione.

Per l'inclusione opposta è sufficiente provare che

$$I(\pi_t(V)) \subset \sqrt{I_t} \tag{0.2}$$

Se (0.2) è vera allora abbiamo
$V(I_t) = V(\sqrt{I_t}) \subset V(I(\pi_t(V))) = \overline{\pi_t(V)}$ (vedi la prop. **??**) come volevamo.
Per provare (0.2) prendiamo
$f \in I(\pi_t(V)) \subset K[x_{t+1}, \ldots, x_n] \subset K[x_1, \ldots, x_n]$. Quindi se $(a_{t+1}, \ldots, a_n) \in \pi_t(V)$ abbiamo $f(a_{t+1}, \ldots, a_n) = 0$. Pertanto $f \in I(V)$ e per il Nullstellensatz $f \in \sqrt{I}$, cioè $\exists\ n$ tale che $f^n \in I \cap K[x_{t+1}, \ldots, x_n] = I_t$, cioè $f \in \sqrt{I_t}$. □

Le ipotesi del teorema di chiusura

Osservazione Per verificare che l'ipotesi K algebricamente chiuso è necessaria nel teorema di chiusura è sufficiente considerare $I = (x^2 + y^2, 2x^2 + y^2 + 1) \subset \mathbb{R}[x, y]$. Eliminando la x abbiamo $V(I_1) = \{-1, 1\} \subset \mathbb{R}$ mentre $\pi_1(V) = \emptyset$

Criterio di appartenenza al radicale

Possiamo risolvere adesso facilmente il problema di appartenenza di un elemento al radicale $\sqrt{I}$ di un ideale I di $K[x_1, \ldots, x_n]$.

Teorema

Sia $I = (f_1, \ldots, f_s)$ *un ideale di* $K[x_1, \ldots, x_n]$. *Allora*

$$f \in \sqrt{I} \iff 1 \in (f_1, \ldots, f_s, 1 - yf) \subset K[x_1, \ldots, x_n, y]$$

Dimostrazione.

- "$\Longleftarrow$" è stata essenzialmente già vista con il Rabinowitsch trick. Se abbiamo $1 = \sum p_i(x, y) f_i + g(x, y)(1 - yf)$ ponendo $y = \frac{1}{f}$ e semplificando i denominatori si ottiene la tesi.
- "$\Longrightarrow$" Sia $f^m \in I \subset \tilde{I} := (f_1, \ldots, f_s, 1 - yf)$. Per definizione abbiamo anche $1 - yf \in \tilde{I}$. Pertanto

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \ldots + y^{m-1} f^{m-1}) \in \tilde{I}$$

Eliminazione ed estensione

Il seguente diagramma schematizza come si possono trovare alcune soluzioni di un sistema generico di m equazioni polinomiali in n variabili (con $m \geq n$) se ad ogni passo sono verificate le ipotesi del teorema di estensione.