Appunti per Geometria e Algebra Computazionale 4. Il teorema di eliminazione e le sue prime applicazioni

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

Giorgio Ottaviani

24 marzo 2020

il k-esimo ideale di eliminazione

Definizione

Sia I un ideale di $K[x_1, \ldots, x_n]$, si pone

$$I_k := I \cap K[x_{k+1}, \ldots, x_n]$$

I_k contiene le "conseguenze" dei polinomi di I che coinvolgono solo le variabili $x_{k+1}, \ldots, x_n$.

Il teorema di eliminazione

Teorema (di eliminazione.)

Sia I un ideale di $K[x_1, \ldots, x_n]$. Sia G una base di Gröbner per I rispetto a Lex. Allora $G_k := G \cap K[x_{k+1}, \ldots, x_n]$ è una base di Gröbner per I_k.

Dimostrazione.

Riordiniamo gli elementi di $G = \{g_1, \ldots, g_m\}$ in modo che i primi r elementi $\{g_1, \ldots, g_r\}$ formino G_k. Facciamo vedere che $\{g_1, \ldots, g_r\}$ generano I_k. Dato $f \in I_k$, abbiamo che il resto della divisione di f per G è zero. Notiamo che $LT(g_{r+1}), \ldots, LT(g_m)$ contengono termini dove compare qualche $x_1, \ldots, x_k$ e quindi hanno multigrado maggiore (per Lex) di ogni monomio di f. Pertanto $g_{r+1}, \ldots g_m$ non entrano in gioco nella divisione di f per G e risulta $f = \sum_{i=1}^{r} a_i g_i$ come volevamo. Questo prova che $\{g_1, \ldots, g_r\}$ generano I_k. □

Seconda parte della dimostrazione del teorema di eliminazione

Dimostrazione.

Usiamo il criterio di Buchberger per provare che $\{g_1, \ldots, g_r\}$ è una base di Gröbner per I_k. Se $1 \leq j, k \leq r$ abbiamo $S(g_j, g_k) \in I_k$. Per quanto visto sopra la divisione di $S(g_j, g_k)$ per G coincide con la divisione per G_k, quindi il resto della divisione è zero come volevamo. □

Esercizi

1. Provare che se $I = (x - y, x^2 + y^3) \subset K[x, y]$ allora $I_1 = (y^3 + y^2)$.
2. Provare che se $= (-x^3 + y, x^2y - z) \subset K[x, y, z]$ allora $I_1 = (y^5 - z^3)$ e $I_2 = 0$.

Intersezione di due ideali

Vediamo adesso un algoritmo che permette di calcolare i generatori di $(f_1, \ldots, f_r) \cap (g_1, \ldots, g_s)$. Questo problema non è banale perché nel caso $(f) \cap I$ contiene il problema di appartenenza "$f \in I$?".
Infatti $f \in I \iff (f) \cap I = (f)$.
Siano I, J due ideali di $K[x_1, \ldots, x_n]$. Definiamo tI come l'ideale di $K[x_1, \ldots, x_n, t]$ generato da tf con $f \in I$. Analogamente si puó definire $(1-t)J$. Vale la

Proposizione

[L'intersezione tra ideali si riconduce ad una eliminazione]

$$I \cap J = [tI + (1-t)J] \cap K[x_1, \ldots, x_n]$$

Dimostrazione del calcolo dell'intersezione tra due ideali

Dimostrazione.

- $\subset$ è ovvia scrivendo $f = tf + (1-t)f$
- $\supset$ Sia $f(x) \in [tI + (1-t)J] \cap K[x_1, \ldots, x_n]$. Pertanto $f(x) = g(x,t) + h(x,t)$ con $g \in tI$ e $h \in (1-t)J$. In particolare

$$g(x,0) = 0 \text{ da cui } f(x) = h(x,0) \in J$$

$$h(x,1) = 0 \text{ da cui } f(x) = g(x,1) \in I$$

Quindi $f \in I \cap J$ come volevamo.

Algoritmo per calcolare l'intersezione tra due ideali

La proposizione precedente dà un algoritmo per calcolare l'intersezione di due ideali. Infatti se $I = (f_1, \ldots, f_r)$ e $J = (g_1, \ldots, g_s)$ allora si può trovare una base di Gröbner (e quindi un insieme di generatori) di $I \cap J$ eliminando t da

$$(tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s)$$

utilizzando il teorema di eliminazione.

Massimo comun divisore e minimo comune multiplo tra polinomi

Il minimo comune multiplo tra due polinomi f e g si può trovare come il generatore dell'ideale intersezione $(f) \cap (g)$. Un algoritmo per calcolarlo segue quindi dall'algoritmo per l'intersezione tra due ideali, che a sua volta segue dall'eliminazione.
Siccome $M.C.D.(f,g) = \frac{fg}{m.c.m.(f,g)}$, abbiamo anche un algoritmo per calcolare il *MCD*. *MCD* e *mcm* possono essere trovati in M2 con i comandi $\gcd(f_1, \ldots, f_k)$ e $\mathrm{lcm}(f_1, \ldots, f_k)$, applicabili anche a più di due polinomi.