

Lezione 17

Cenni sulle basi di Gröbner.

Nella lezione precedente abbiamo visto che gli ideali monomiali sono particolarmente facili da maneggiare ai fini della determinazione delle decomposizioni primarie e delle dimensioni dei relativi anelli quozienti. Questi problemi, per gli ideali di tipo più generale, non possono essere risolti in maniera altrettanto diretta. Esiste, tuttavia, un modo per associare, ad ogni ideale di polinomi a coefficienti in campo, un ideale monomiale che ha molte proprietà in comune con esso, tra cui la dimensione.

Come nelle ultime lezioni, faremo sempre riferimento, salvo avviso contrario, all'anello dei polinomi a coefficienti nel campo K nelle indeterminate x_1, \dots, x_n .

Definizione 17.1 Sia $M = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid (\alpha_1, \dots, \alpha_n) \in \mathbf{N}^n\}$. Si dice *ordine monomiale* ogni ordinamento totale \leq su M rispetto al quale ogni sottoinsieme non vuoto di M ha un elemento minimo e tale che, per ogni $(\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n), (\gamma_1, \dots, \gamma_n) \in \mathbf{N}^n$

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} < x_1^{\beta_1} \cdots x_n^{\beta_n} \implies x_1^{\alpha_1} \cdots x_n^{\alpha_n} \cdot x_1^{\gamma_1} \cdots x_n^{\gamma_n} < x_1^{\beta_1} \cdots x_n^{\beta_n} \cdot x_1^{\gamma_1} \cdots x_n^{\gamma_n} \quad (1)$$

Nota La condizione (1) esprime la compatibilità dell'ordinamento monomiale rispetto al prodotto. Segue che, nel caso di una sola indeterminata, l'unico ordine monomiale è quello indotto dalla relazione di divisibilità (equivalentemente: dall'ordinamento rispetto al grado).

Esempio 17.2 Un esempio di ordine monomiale è il cosiddetto *ordine lessicografico*, definito come segue: si pone

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} < x_1^{\beta_1} \cdots x_n^{\beta_n}$$

se, in corrispondenza del minimo indice i tale che $\alpha_i \neq \beta_i$, si ha che $\alpha_i - \beta_i < 0$. Si ha, ad esempio:

$$1 < x_2 < x_1 < x_1 x_2 < x_1 x_2 x_3 < x_1 x_2 x_3^2 < x_1^2$$

Definizione 17.3 Dati un ordine monomiale \leq su $K[x_1, \dots, x_n]$ ed un polinomio non costante $f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, si dice *monomio direttore* di $f(x_1, \dots, x_n)$ rispetto all'ordine \leq il massimo tra i monomi di $f(x_1, \dots, x_n)$.

Nota Il termine inglese, più frequentemente usato, è *leading term*, che corrisponde alla notazione $LT_{\leq}(f)$ (o $LT(f)$ qualora si sottintenda l'ordine monomiale). I risultati generali che enunceremo sono validi, in realtà, per ogni ordine monomiale.

Nel seguito, supporremo fissato, nell'anello dei polinomi $K[x_1, \dots, x_n]$, l'ordine lessicografico.

Esempio 17.4 Sia $f(x_1, x_2) = x_1^4 + x_1^3 - x_1^2 x_2 + x_2^7$. Allora $LT(f) = x_1^4$.

Definizione 17.5 Dato un ideale proprio non nullo I di $K[x_1, \dots, x_n]$, si dice *ideale iniziale* $\text{in}(I)$ di I l'ideale generato dai monomi direttori degli elementi non nulli di I .

L'ideale $\text{in}(I)$ è un ideale monomiale, ed è fortemente legato all'ideale I . Infatti:

Proposizione 17.6 Sia I un ideale proprio non nullo di $K[x_1, \dots, x_n]$. Allora $\dim K[x_1, \dots, x_n]/I = \dim K[x_1, \dots, x_n]/\text{in}(I)$.

Dimostrazione: vedi [BH], Theorem 4.1.3, Corollary 4.2.4 ed il commento successivo. \square

È dunque importante, dal punto di vista pratico, poter calcolare l'ideale iniziale di un ideale di polinomi. Osserviamo preliminarmente che, dati i polinomi non costanti $f_1, \dots, f_r \in K[x_1, \dots, x_n]$, si ha

$$(\text{LT}(f_1), \dots, \text{LT}(f_r)) \subset \text{in}(f_1, \dots, f_r),$$

inclusione, che però, in generale, è stretta, come mostra il prossimo

Esempio 17.7 Siano $f_1 = x_1^2 + 2x_1x_2^2, f_2 = x_1x_2 + 2x_2^3 - 1 \in K[x_1, x_2]$ e sia $I = (f_1, f_2)$. Allora $\text{LT}(f_1) = x_1^2$ e $\text{LT}(f_2) = x_1x_2$. Inoltre $x_2f_1 - x_1f_2 = x_1 \in I$, quindi $x_1 \in \text{in}(I)$. Però, evidentemente, $x_1 \notin (x_1^2, x_1x_2)$. Dunque $(\text{LT}(f_1), \text{LT}(f_2)) \neq \text{in}(f_1, f_2)$.

Nell'esempio precedente, i monomi direttori dei generatori f_1, f_2 dell'ideale I non sono sufficienti a generare tutti i monomi direttori dei polinomi di I . Occorre dunque ampliare opportunamente l'insieme dei generatori di I .

Definizione 17.8 Si dice *base di Gröbner* (o *base standard*) di un ideale I proprio non nullo di $K[x_1, \dots, x_n]$ ogni insieme $\{f_1, \dots, f_r\} \subset I$ tale che $(\text{LT}(f_1), \dots, \text{LT}(f_r)) = \text{in}(I)$.

Si dimostra che

Proposizione 17.9 Sia I un ideale proprio non nullo di $K[x_1, \dots, x_n]$. Allora I ammette una base di Gröbner. Inoltre ogni base di Gröbner è un sistema di generatori per I .

Dimostrazione: vedi [BH], pag. 156 e seguente. \square

Osservazione 17.10 Se esiste una base di Gröbner, esiste anche una base di Gröbner finita: questa è una conseguenza del fatto che l'anello $K[x_1, \dots, x_n]$ è noetheriano. Ciò consente, in particolare, di costruire una base di Gröbner con un numero finito di passi. Esiste, in effetti, un procedimento algoritmico generale (detto *algoritmo di Buchberger*) per calcolare una base di Gröbner di un ideale proprio e non nullo di $K[x_1, \dots, x_n]$ rispetto a qualsiasi ordine monomiale. I passi fondamentali sono i seguenti:

1. il calcolo dell'*S-polinomio* $S(f, g)$ di due polinomi f, g : se a e b sono i coefficienti dei monomi direttori di f e g rispettivamente e $m = \text{mcm}(\text{LT}(f), \text{LT}(g))$, si pone

$$S(f, g) = \begin{cases} b \frac{m}{\text{LT}(f)} f - a \frac{m}{\text{LT}(g)} g & \text{se } \text{MCD}(\text{LT}(f), \text{LT}(g)) \neq 1 \\ 0 & \text{altrimenti} \end{cases}.$$

Questo è un polinomio avente monomio direttore minore di m .

Tramite la ripetuta applicazione del passo 1 (e di una sua variante) si ottiene

- la riduzione di un polinomio f modulo un insieme di polinomi $\{f_1, \dots, f_r\}$: il polinomio cercato è un polinomio h tale che $\text{LT}(f_i)$ non divide alcuno dei monomi di h , per ogni $i = 1, \dots, r$, e per il quale si ha

$$f = \sum_{i=1}^r h_i f_i + h, \quad \text{ove, per ogni } i = 1, \dots, r, \quad h_i = 0 \text{ oppure } \text{LT}(h_i f_i) \leq \text{LT}(f).$$

Il polinomio h si dice in *forma normale*. Se f stesso è in forma normale, allora f si dice *ridotto* modulo $\{f_1, \dots, f_r\}$.

Si osservi che, nell'anello dei polinomi in una sola indeterminata, per $r = 1$, il passo 2. equivale alla determinazione del resto h della divisione di f per f_1 . Si procede infine con:

- l'aggiunta di nuovi generatori: ogni polinomio non nullo h ottenuto al passo 2 si aggiunge all'insieme di generatori.

Il procedimento si ripete, per ogni nuova coppia di generatori f, g , finché nessun nuovo generatore viene più aggiunto. Si dimostra allora che l'insieme di generatori ottenuto è una base di Gröbner.

Sviluppiamo l'algoritmo di Buchberger in un caso concreto.

Esempio 17.11 Determiniamo, tramite l'algoritmo di Buchberger, una base di Gröbner dell'ideale $I = (f_1, f_2)$ dell'Esempio 17.7. Ricordiamo che abbiamo $\text{LT}(f_1) = x_1^2$ e $\text{LT}(f_2) = x_1 x_2$.

- $S(f_1, f_2) = x_2 f_1 - x_1 f_2 = x_1$;
- x_1 è ridotto modulo $\{f_1, f_2\}$; sia $f_3 = x_1$.
- Si considera $\{f_1, f_2, f_3\}$ come nuovo sistema di generatori. Si ha $\text{LT}(f_3) = x_1$.

- $S(f_1, f_3) = f_1 - x_1 f_3 = 2x_1 x_2^2$;
- $2x_1 x_2^2 - 2x_2^2 f_3 = 0 \rightarrow$ non si aggiunge nessun nuovo generatore.

- $S(f_2, f_3) = f_2 - x_2 f_3 = 2x_2^3 - 1$;
- $2x_2^3 - 1$ è ridotto modulo $\{f_1, f_2, f_3\}$; sia $f_4 = 2x_2^3 - 1$. Si ha $\text{LT}(f_4) = x_2^3$.
- Si considera $\{f_1, f_2, f_3, f_4\}$ come nuovo sistema di generatori.

1. S(f₁, f₄) = 0, S(f₃, f₄) = 0; S(f₂, f₄) = 2x₂²f₂ - x₁f₄ = 4x₂⁵ - 2x₂² + x₁;
2. x₁ + 4x₂⁵ - 2x₂² - f₃ = 4x₂⁵ - 2x₂², 4x₂⁵ - 2x₂² - 2x₂²f₄ = 0 → non si aggiunge nessun nuovo generatore.

Si dimostra che allora {f₁, f₂, f₃, f₄} è una base di Gröbner per l'ideale I. Segue che

$$\text{in}(I) = (x_1^2, x_1x_2, x_1, x_2^3) = (x_1, x_2^3).$$

Osservazione 17.12 La base di Gröbner cambia, in generale, cambiando l'ordine monomiale. In realtà, possono anche esistere diverse basi di Gröbner rispetto ad uno stesso ordine monomiale. Nell'Esercizio 17.11, ad esempio, si vede che anche {f₃, f₄} è una base di Gröbner (minimale) rispetto all'ordine lessicografico.

Come conseguenza della Proposizione 17.6 ed in base a quanto visto nell'Esercizio 14.20, si ha allora che

$$\dim K[x_1, x_2]/I = \dim K[x_1, x_2]/(x_1, x_2^3) = \dim K[x_1, x_2]/\sqrt{(x_1, x_2^3)} = \dim K[x_1, x_2]/(x_1, x_2) = 0.$$

D'altronde, la varietà V(I): x₁(x₁ + 2x₂²) = 0, x₁x₂ + 2x₂³ - 1 = 0 è l'intersezione di due curve del piano, che non hanno componenti irriducibili in comune. Quindi essa è formata da un insieme finito di punti, ed ha, pertanto, dimensione 0.

Il problema di trovare una decomposizione primaria minimale è, in generale, molto più complesso. Diversi algoritmi, che si avvalgono delle basi di Gröbner, sono stati sviluppati negli ultimi decenni.