Appunti per Geometria e Algebra Computazionale
2. Ideale dei LeadTerm e basi di Gröbner

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

Giorgio Ottaviani

14 marzo 2020

Criterio di appartenenza di un polinomio a un ideale monomiale

Lemma

Sia I un ideale monomiale. Sono equivalenti

- *i) $f \in I$*
- *ii) ogni termine di f appartiene a I.*

Dimostrazione.

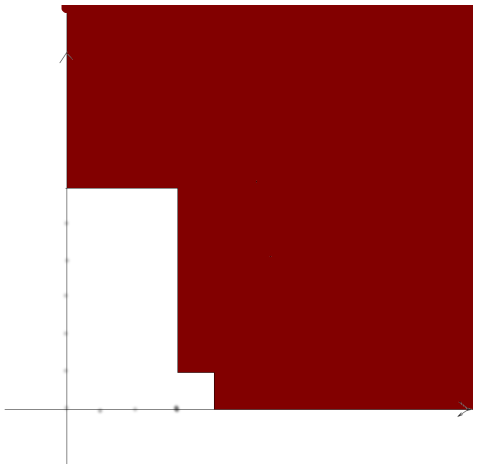
ii) $\Rightarrow$ i) è banale. Per provare i) $\Rightarrow$ ii) scriviamo $f = \sum_i f_i$ (ogni f_i è un termine)$= \sum_j g_j m_j$ (ogni m_j è un monomio in I).
A secondo membro ogni termine appartiene a I, quindi questo è vero anche a primo membro che è ottenuto cancellando tra loro alcuni termini a secondo membro. □

Ideali monomiali come sottoinsiemi di $\mathbb{Z}^n_{\geq 0}$

Corollario

Due ideali monomiali sono uguali se e solo se contengono gli stessi monomi.

Il corollario precedente permette quindi di identificare gli ideali monomiali con dei sottoinsiemi di $\mathbb{Z}^n_{\geq 0}$. Ad esempio l' ideale monomiale (x^4, x^3y, y^6) in $K[x, y]$ corrisponde alla regione seguente:



Basi minimali di ideali monomiali

Definizione

Un insieme di monomi B si dice una base minimale per un ideale monomiale I se

1. *i monomi di B generano I*
2. *nessun monomio di B è divisibile per qualche altro monomio di B.*

Esistenza e unicità di basi minimali

Proposizione

Sia I un ideale monomiale. Allora esiste una unica base minimale per I.

Dimostrazione.

Per l'esistenza di una base minimale si prende un insieme di generatori ed si eliminano successivamente i monomi divisi da qualcun altro. Per l'unicità prendiamo due basi minimali. Dal criterio di appartenenza di un monomio a un ideale monomiale, ogni monomio x^α della prima base è divisibile per un monomio della seconda base, che a sua volta è divisibile per un monomio della prima base, che per la minimalità può essere solo x^α. Segue che ogni monomio della prima base à uguale a un monomio della seconda e viceversa, da cui le due basi sono uguali. □

Ideale dei LeadTerm

Definizione

Sia I un ideale di $K[x_1, \ldots, x_n]$ e sia fissato un ordine monomiale. $LT(I)$ è l'ideale (monomiale) generato da tutti i termini $LT(f)$ dove $f \in I$. In formula

$$LT(I) := \langle LT(f) | f \in I \rangle$$

Il comando corrispondente in Macaulay2 è $\mathrm{leadTerm(I)}$*, con l'algoritmo di Buchberger del §3 vedremo come calcolare $LT(I)$.*

Basi di Gröbner

Osservazione Se $I = (g_1, \dots g_k)$ allora
$LT(I) \supseteq (LT(g_1), \dots, LT(g_k))$ ma può valere l'inclusione stretta come mostra il seguente

Esempio

Sia $I = (x^2 + y, x^2 - y) \subset K[x, y]$ *con un qualunque ordine monomiale graduato. Allora* $y \in I$ *da cui* $y \in LT(I)$ *mentre* $y \notin (LT(x^2 + y), LT(x^2 - y)) = (x^2)$

L'osservazione precedente motiva la seguente

Definizione

Un insieme $(g_1, \dots, g_k)$ *di elementi di* I *si dice una* *base di Gröbner* *per* I *se*

$$LT(I) = (LT(g_1), \dots, LT(g_k))$$

Esistenza di basi di Gröbner (non costruttiva)

Proposizione

Ogni ideale di $K[x_1, \ldots, x_n]$, con un ordine monomiale fissato, ammette una base di Gröbner.

Dimostrazione.

È sufficiente estrarre dall'insieme $\{LT(f) | f \in I\}$ un numero finito di generatori per $LT(I)$. Questo è sempre possibile per noetherianità . □

La dimostrazione precedente è non costruttiva. Buchberger sviluppó nel 1965 (nella sua tesi di dottorato) un algoritmo per calcolare effettivamente una base di Gröbner a partire da un insieme di generatori. Vedremo questo algoritmo nel Capitolo 3.

Una base di Gröbner genera

Teorema

Una base di Gröbner per I genera I.

Dimostrazione.

Sia $g_1, \ldots, g_k$ una base di Gröbner, pertanto $LT(I) = (LT(g_1), \ldots, LT(g_k))$. Se $f \in I$ allora per l'algoritmo di divisione possiamo scrivere $f = \sum a_i g_i + r$ da cui $r = f - \sum a_i g_i \in I$ ed in particolare $LT(r) \in (LT(g_1), \ldots, LT(g_k))$. Se fosse $r \neq 0$ allora dalle proprietà dell'algoritmo di divisione $LT(r)$ non è divisibile per nessuno dei $LT(g_i)$ e questa è una contraddizione con il criterio di appartenenza a un ideale monomiale. □

Un esempio di base di Gröbner, I

Esempio

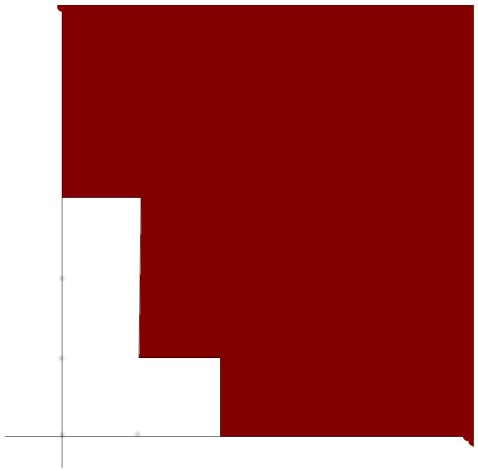
Sia $I = (x^2 + y^2, xy) \subset K[x, y]$ *con l'ordine Lex. Una base di Gröbner per* I *è costituita da almeno tre elementi. Infatti tutti i monomi di grado* 3 *appartengono ad* I *(e quindi anche a* $LT(I)$*:*

$$\begin{aligned} x^3 &= x(x^2 + y^2) - y(xy) \\ x^2y &= x(xy) \\ xy^2 &= y(xy) \\ y^3 &= y(x^2 + y^2) - x(xy). \end{aligned}$$

Siccome ogni monomio di grado ≥ 3 *é divisibile per un monomio di grado* 3*, segue che ogni monomio di grado* ≥ 3 *appartiene a* I *(e quindi anche a* $LT(I)$*. Anche* x^2 *e* xy *appartengono a* $LT(I)$ *e devono appartenere ad un qualunque insieme di generatori di* $LT(I)$*. Infine notiamo che* $y^3 \notin (x^2, xy)$ *e quindi sono necessari almeno tre elementi come asserito.*

Un esempio di base di Gröbner, II

Continuiamo con $I = \left(x^2 + y^2, xy\right) \subset K[x, y]$ con l'ordine Lex. La rappresentazione grafica di $LT(I)$ è la seguente:



Se $I = \left(x^2 + y^2, xy\right) \subset K[x, y]$ con l'ordine Lex, abbiamo che $LT(I) = (x^2, xy, y^3)$ e una base di Gröbner è $x^2 + y^2, xy, y^3$

.

Forma normale rispetto a un ideale

Teorema (Forma normale di un elemento rispetto a un ideale)

Sia fissato un ordine monomiale e per l'ideale $I \subset K[x_1, \ldots, x_n]$. Sia $f \in K[x_1, \ldots, x_n]$. Allora esiste unico $r \in K[x_1, \ldots, x_n]$ tale che:

- *i) nessun termine di r appartiene a $LT(I)$.*
- *ii) esiste $g \in I$ tale che $f = g + r$.*

In particolare r è il resto della divisione di f per una base di Gröbner di I. r si dice la forma normale di f rispetto a I e dipende solo dall'ordine monomiale fissato.

Dimostrazione.

Sia $G = \{g_1, \ldots, g_t\}$ una base di Gröbner, dunque $LT(I) = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Scegliamo r come il resto della divisione di f per G, che soddisfa le due proprietà dell'enunciato.

Continuo dimostrazione per l'unicità della forma normale

Dimostrazione.

Per provare l'unicità consideriamo $f = g' + r' = g'' + r''$. Allora $r'' - r' = g' - g'' \in I$ da cui $LT(r'' - r') \in LT(I) = (LT(g_1), \ldots, LT(g_k))$. Se $r'' - r' \neq 0$ allora $LT(r'' - r')$ sarebbe divisibile per qualche $LT(g_i)$ e questo è impossibile perché nessun termine di r' o di r'' è divisibile per qualche $LT(g_i)$. □

Esercizi, I

Esercizi.

1. Sia $I = (g_1, g_2, g_3) \subset \mathbb{R}[x, y, z]$ dove $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$, $g_3 = x - yz^4$. Utilizzando Lex, dare un esempio di $g \in I$ tale che $LT(g) \notin < LT(g_1), LT(g_2), LT(g_3) >$.
2. Sia $G = \{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$. Provare che G non è una base di Gröbner per $< G >$ rispetto a GRevLex.
3. Sia $I \subset K[x_1, \ldots, x_n]$ un ideale principale. Provare che un sottoinsieme di I è una base di Gröbner per I se e solo se contiene un generatore di I.

Esercizi, II

4. Sia $I = (f)$ un ideale principale. Provare che $LT(I)$ è principale ed è generato da $LT(f)$. In questo caso il problema di appartenenza si risolve mediante la divisione per f (perché ?).
5. Provare che g divide f se e solo se la divisione di f per g dà resto zero. Questo non dipende dall' ordine monomiale scelto.
6. Calcolare la forma normale di x^2y rispetto a $I = (x^2 + y^2, xy)$ effettuando la divisione rispetto alla base di Gröbner $\{x^2 + y^2, xy, y^3\}$. Notare che i quozienti dipendono dall'ordine dei tre elementi (si provi l'ordine $\{xy, x^2 + y^2, y^3\}$.

Algoritmo di divisione e basi di Gröbner

Corollario

Quando si divide per una base di Gröbner l'algoritmo di divisione porta sempre allo stesso resto qualunque sia l'ordine dei divisori.

Di più vale

Corollario

$f \in I \iff$ *il resto della divisione di* f *con una base di Gröbner di* I *è zero*

Dimostrazione.

$\Leftarrow$ è ovvia

$\Rightarrow$ $f = f + 0$ nella forma normale. $\square$

Il corollario precedente risolve quindi il problema di appartenenza a un ideale qualunque se si conosce una base di Gröbner.

Forma normale in M2

Definizione

Scriveremo f % I per indicare la forma normale di f rispetto a I. f % I dipende solo dall'ordine monomiale, ed in particolare

$$f \in I \iff f \,\%\, I = 0$$

In Macaulay2 f % I è il resto della divisione di f per una base di Gröbner di I.

Esercizio

Sia $f = x^4y + y^3$ e $I = (x^2 + y^2, xy)$. Fissato l'ordine Lex, calcolare f % I.

Osservazione Un esercizio che vedremo (vedi eserc. 3.4 2 delle note del corso) mostra che i quozienti non sono unici: l'unicità del resto nella divisione è il massimo che si riesce ad ottenere.