Teorema della base di Hilbert e Basi di Groebner

A. Bernardi

1 marzo 2016

Alcune parti di queste note sono prese da [2] che può essere usato per completare alcune dimostrazioni o per approfondire ulteriormente l'argomento.

1 Teorema della Base di Hilbert

Teorema 1.1 (Teorema della Base di Hilbert (Basissatz))**.** *Sia A un anello Noetheriano, quindi anche $A[x]$ è un anello Noetheriano.*

Dimostrazione. Esercizio. Esistono diverse dimostrazioni di questo teorema facilmente reperibili in letteratura. Per i nostri scopi si consiglia di seguire quella di H. Sarges [1, Theorem 10.4.1] o quella di [2, Teorema 1.2]. □

Corollario 1.2. *Se A è un anello Noetheriano, allora anche $A[x_1, \ldots, x_n]$ è un anello Noetheriano.*

2 Teorema di scomposizione in fattori irriducibili in $K[x]$

Sia K un campo ed $I \subset K[x]$ un ideale.

Problema 2.1. *Esiste un algoritmo per stabilire se un polinomio $g \in K[x]$ appartiene o no ad I?*

Teorema 2.2. *Sia $f \in K[x]$ un polinomio di grado positivo e sia $c \in K^*$ il coefficiente direttore di f. Quindi esistono polinomi monici irriducibili, distinti $p_1, \ldots, p_r \in K[x]$ e interi positivi $m_1, \ldots, m_r$ tali che $f = cp_1^{m_1} \cdots p_r^{m_r}$. Inoltre se esistono altri polinomi irriducibili distinti $q_1, \ldots, q_s \in K[x]$ ed interi positivi $n_1, \ldots, n_n$ tali che $f = cq_1^{n_1} \cdots q_s^{n_s}$, allora $r = s$ e si possono permutare i $q_1^{n_1} \cdots q_s^{n_s}$ in maniera tale che $p_1 = q_1, \ldots, p_r = q_r$ e $m_1 = n_1, \ldots, m_r = n_r$.*

Dimostrazione. Esercizio. □

Teorema 2.3. *Il polinomio $(x-a) \in K[x]$ divide $f \in K[x]$ se e solo se $f(a) = 0$.*

Dimostrazione. Esercizio. □

Teorema 2.4. *$K[x]$ è un PID.*

Dimostrazione. Esercizio. □

A questo punto è chiaro che la risposta al Problema 2.1 è sì.

Corollario 2.5. *Per controllare se $p \in I \subset K[x]$ è sufficiente controllare che $p \mid f$ con $(f) = I$. Per fare questo si può usare l'algoritmo della divisione ben noto.*

Esempio 2.6. Scegliere un esempio per illustrare la situazione della divisione in $K[x]$.

3 Algoritmo della divisione in $K[x_1, \ldots, x_n]$

Un problema analogo al Problema 2.1 si può chiaramente riproporre in più di una variabile.

Problema 3.1. *Esiste un algoritmo per stabilire se un polinomio $g \in K[x_1, \ldots, x_n]$ appartiene o no ad un ideale $I \subset K[x_1, \ldots, x_n]$?*

Osservazione. Per risolvere il Problema 2.1 avevamo usato il fatto che $K[x]$ è un PID: per controllare se $g \in I \subset K[x]$ bastava controllare se il resto della divisione per f con $I = (f)$ era 0 o no.
Ora $K[x_1, \ldots, x_n]$ non è un PID. Per controllare se $g \in I \subset K[x_1, \ldots, x_n]$ vogliamo generalizzare l'algoritmo della divisione e arrivare a scrivere $g = a_1 f_1 + \cdots + a_s f_s + r$. Ma come caratterizzare gli f_i ed r?
L'idea base è la stessa del caso in una variabile: vogliamo cancellare il coefficiente direttore di f. Ma come stabilire il coefficiente direttore in $K[x_1, \ldots, x_n]$?

Definizione 3.2. Un *ordine monomiale* su $K[x_1, \ldots, x_n]$ è una relazione " $>$ " su $\mathbb{Z}^n_{\geq 0}$, o equivalentemente, ogni relazione sull'insieme dei monomi x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$ che soddisfa:

1. " $>$ " è un *ordine totale* su $\mathbb{Z}^n_{\geq 0}$ (i.e. per ogni coppia di monomi x^α, x^β, esattamente una delle seguenti è vera $x^\alpha > x^\beta$, $x^\beta > x^\alpha$, $x^\alpha = x^\beta$);
2. Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, allora $\alpha + \gamma > \beta + \gamma$;
3. " $>$ " è un *buon ordinamento* (i.e. ogni sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$ ammette il minimo per " $>$ ").

Esempio 3.3 (Ordine Lessicografico)**.** Siano $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Si dice che $\alpha >_{lex} \beta$ se nel vettore differenza $\alpha - \beta \in \mathbb{Z}^n$ la prima entrata di sinistra non nulla è positiva. Scriveremo $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.

Esercizio 1. Mostrare che l'ordine lessicografico è un ordine monomiale.

Esempio 3.4 (Ordine Lessicografico Graduato)**.** Siano $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Diciamo che $\alpha >_{grlex} \beta$ se $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$ o $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$.

Esercizio 2. Mostrare che l'ordine lessicografico graduato è un ordine monomiale.

Esempio 3.5 (Ordine lessicografico graduato inverso)**.** Siano $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Diciamo che $\alpha >_{degrevlex} \beta$ se $|\alpha| > |\beta|$ o $|\alpha| = |\beta|$ e il primo coefficiente non nullo da destra in $\alpha - \beta$ è non negativo.

Esercizio 3. Mostrare che l'ordine lessicografico graduato inverso è un ordine monomiale.

Definizione 3.6. Sia $f = \sum_\alpha a_\alpha x^\alpha \neq 0$, $f \in K[x_1, \ldots, x_n]$ e sia " $>$ " un ordine monomiale. Si danno le seguenti definizioni:

- Il multigrado di f è $multideg(f) = \max_>\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}$;
- Il coefficiente direttore di f è:
$$LC(f) = a_{multideg(f)} \in K;$$
- Il monomio direttore di f è:
$$LM(f) = x^{multideg(f)};$$
- Il termine direttore di f è:
$$LT(f) = LC(f) \cdot LM(f).$$

Esercizio 4. Scrivere $multideg(f)$, $LC(f)$, $LM(f)$ e $LT(f)$ per $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$ per LEX, GRLEX e DEGREVLEX.

Algoritmo della divisione in $K[x_1, \ldots, x_n]$

Fissiamo un ordine monomiale " $>$ " su $\mathbb{Z}^n_{\geq 0}$ e sia $F = (f_1, \ldots, f_s)$ una s-upla ordinata di polinomi in $K[x_1, \ldots, x_n]$. Allora ogni polinomio f può essere scritto come $f = a_1f_1 + \cdots + a_sf_s + r$ con $a_i, r \in K[x_1, \ldots, x_n]$ e o $r = 0$ o r è una combinazione lineare a coefficienti in K di monomi nessuno dei quali è divisibile per alcun $LT(f_1), \ldots, LT(f_s)$. Inoltre se $a_if_i \neq 0$ si ha che $multideg(f) \geq multideg(a_if_i)$.

Osservazione. NON si parla di unicità della decomposizione o del resto.

Vediamo come funziona questo algoritmo.

- Poniamo $p := f$ (resto ausiliario);
- Dividiamo $LT(p)$ successivamente per $LT(f_1), \ldots, LT(f_s)$ e quando è possibile aggiungiamo $LT(p)/LT(f_i)$ all'i-esimo quoziente e sottraiamo $f_i \frac{LT(p)}{LT(f_i)}$ dal resto ausiliario p. Quando $LT(p)$ non è divisibile per nessuno tra $LT(f_1), \ldots, LT(f_s)$ allora aggiungiamo $LT(p)$ al resto e continuiamo con $p - LT(p)$ al posto di p.

L'algoritmo ha termine quando il resto ausiliario diventa nullo. Questo accade sempre perché il multigrado del resto ausiliario p decresce strettamente e l'ordine monomiale scelto è un buon ordinamento.

Esercizio 5. Testare questo algoritmo nei seguenti casi con l'ordine lessicografico con $x > y$:

1. $f = xy^2 + 1$ e $f_1 = xy + 1$ e $f_2 = y + 1$.
2. $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. Questo punto può essere svolto in due modi:
   (a) Dividendo due volte per f_1 e una volta per f_2,
   (b) Oppure dividendo una volta per f_1 e due volte per f_2

Concludere la non unicità della decomposizione nell'algoritmo della divisione come formulato sopra.

Esercizio 6. Sia $f = xy^2 - x$ e siano $f_1 = y^2 - 1$ e $f_2 = xy - 1$. Mostrare che $f \in (f_1, f_2)$ (banale) ma se procediamo con l'algoritmo della divisione dividendo f dapprima per f_2 si trova che il resto della divisione è diverso da zero e non più divisibile per f_1 e f_2.

Chiaramente $r = 0 \Rightarrow f \in (f_1, \ldots, f_s)$ ma è FALSO il viceversa.

4 Basi di Groebner

Definizione 4.1. Sia fissato un ordine monomiale " $>$ " su $K[x_1, \ldots, x_n]$. Sia $I \subset K[x_1, \ldots, x_n]$ un ideale. Sia $G \subset I$, $G = \{g_1, \ldots, g_s\}$ una famiglia di elementi di I. G è detta una *Base di Groebner* di I rispetto a " $>$ " se $(LT(g_1), \ldots, LT(g_s)) = (LT(I)) :=$ ideale generato dai LT degli elementi di I.

Esercizio 7. Sia $I = (g_1, g_2) \subset \mathbb{R}[x, y, z]$ con $g_1 = x - z$ e $g_2 = y + z$. Fissiamo l'ordinamento lessicografico con $x > y$. Mostrare che $\{g_1, g_2\}$ è una G-base per I.

Definizione 4.2. Un ideale si dice *monomiale* se è generato da monomi.

Una conseguenza della noetherianità di $K[x_1, \ldots, x_n]$ è il Lemma di Dickson:

Lemma 4.3 (Dickson)**.** *Ogni ideale monomiale è finitamente generato.*

Proposizione 4.4. *Sia $I \subset K[x_1, \ldots, x_n]$ un ideale. Allora*

1. *$(LT(I))$ è un ideale monomiale;*
2. *Esistono $g_1, \ldots, g_s \in I$ t.c. $(LT(I)) = (LT(g_1), \ldots, LT(g_s))$.*

Dimostrazione. Esercizio. □

Proposizione 4.5. *Sia $G = \{g_1, \ldots, g_t\}$ una G-base dell'ideale $I \subset K[x_1, \ldots, x_n]$ e sia $f \in K[x_1, \ldots, x_n]$, quindi esiste ed è UNICO $r \in K[x_1, \ldots, x_n]$ tale che*

1. *Nessun termine di r è divisibile per uno dei $LT(g_i)$;*
2. *Esiste $g \in I$ tale che $f = g + r$.*

Corollario 4.6. *Sia $G = \{g_1, \ldots, g_t\}$ una G-base dell'ideale $I \subset K[x_1, \ldots, x_n]$ e sia $f \in K[x_1, \ldots, x_n]$. Si ha che $f \in I$ SE E SOLO SE il resto della divisione di f per G è 0.*

Dimostrazione. Esercizio. Potrebbe servire il fatto che un monomio appartiene ad un ideale monomiale se è divisibile per uno dei generatori. □

Riferimenti bibliografici

[1] P.M. Cohn, Basic Algebra: Groups, Rings and Fields. Springer 2015.

[2] G. Ottaviani. Introduzione alle varietà algebriche. Un punto di vista costruttivo.
`http://web.math.unifi.it/users/ottavian/groebner/groebner.pdf`