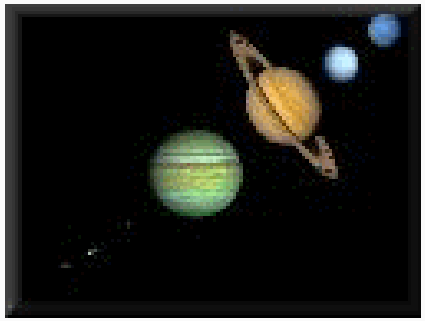


Teoria di Gröbner

Matematica e Scienze Computazionali - 2022

Luca Amata

8 luglio 2022

Dipartimento di Scienze Matematiche e Informatiche,
Scienze Fisiche e Scienze della Terra,
Università degli Studi di Messina

Indice

Introduzione

Introduzione

- I termini *algebra* e *algoritmo* vengono fatti risalire al matematico persiano **al-Khwarizmi** [5], il quale con *al-gabr* e *al-muqabalah* descriveva, rispettivamente, le trasformazioni simboliche e le riduzioni a termini comuni utilizzate per risolvere equazioni algebriche.

- Fino alla fine del XIX secolo, la manipolazione simbolica delle equazioni ha mantenuto una fondamentale importanza negli studi algebrici.

- Con l'avvento dell'algebra astratta, il cambio di paradigma ha dirottato l'interesse comune verso i sistemi formali assiomatici, oscurando il calcolo simbolico.

- Negli ultimi decenni, gli aspetti algoritmici dell'algebra sono nuovamente tornati in auge grazie, soprattutto, al rapidissimo sviluppo dei sistemi informatici e delle attività ad essi collegati.

Introduzione

- Per *sistema di computer algebra* (CAS) si intende un software che permette di manipolare automaticamente espressioni matematiche rappresentate in forma *simbolica*.

- Nasce così una nuova disciplina: la *computer algebra* (o *calcolo simbolico*), dedita allo studio di metodi per la risoluzione automatica di problemi espressi da una formulazione "matematica" tramite l'implementazione di opportuni algoritmi.

- Le applicazioni dell'algebra computazionale sono rivolte prevalentemente allo studio di proprietà di specifiche strutture e spesso anche alla produzione di esempi notevoli, esotici o controesempi.

- Si può affermare che in questi anni si stia vivendo una nuova età aurea dei metodi algoritmici nell'algebra, non soltanto come strumento accessorio, ma soprattutto come metodologia applicabile all'analisi di strutture matematiche.

Richiami algebrici

Definizioni

- Un anello commutativo con unità A è un **dominio di integrità** (ID) se non contiene divisori dello zero non nulli;
- A è un **dominio euclideo** (ED) se è possibile definire una *valutazione* $v : A \setminus \{0\} \to \mathbb{N}$ per cui valgono le seguenti:
  - $v(a) \leq v(a \cdot b)$, per ogni $a, b \in A \setminus \{0\}$;
  - per ogni $a, b \in A$, $b \neq 0$, esistono $q, r \in A$ tali che $a = q \cdot b + r$ con $r = 0$ o $v(r) < v(b)$;
- A è un **dominio ad ideali principali** (PID) se ogni suo ideale è principale, cioè generato da un solo elemento;
- A è un **dominio a fattorizzazione unica** (UFD) se ogni suo elemento si decompone in modo unico come prodotto di fattori irriducibili;
- A è **noetheriano** se:
  - vale alla condizione della catena ascendente (AAC), cioè se ogni catena ascendente di ideali $I_1 \subset I_2 \subset I_3 \subset \ldots$ è stazionaria, nel senso che esiste s tale che $I_s = I_{s+1} = I_{s+2} = \ldots$;
  - vale la condizione massimale;
  - ogni suo ideale è finitamente generato.

Risultati

Valgono le seguenti implicazioni: ED $\Longrightarrow$ PID $\Longrightarrow$ UFD.

Siano A un anello commutativo unitario e $A[x]$ l'anello dei polinomi su A. Valgono i seguenti risultati:

- Se A è un ID allora anche $A[x]$ è un ID;
- Se A è un UFD allora anche $A[x]$ è un UFD (Eulero-Gauss);
- Se A è noetheriano allora anche $A[x]$ è noetheriano (Basissatz);

Ovviamente tali risultati si estendono immediatamente all'anello dei polinomi $A[x_1, \ldots, x_n]$ con n indeterminate.

Sui campi

Siano K un campo e $K[x_1, \ldots, x_n]$ l'anello dei polinomi su K con n indeterminate. Allora:

- K è un ID, in particolare è un ED ($v(a) = 1$ per ogni $a \in K$) e quindi è un PID e un UFD;
- $K[x_1, \ldots, x_n]$ è un UFD (poiché K lo è);
- K è noetheriano (gli unici suoi ideali sono (0) e K) e quindi anche $K[x_1, \ldots, x_n]$ è noetheriano.

Osservazioni su $K[x]$

Sia K un campo e $K[x]$ l'anello dei polinomi su K. Allora $K[x]$ è un ED ($v(f) = \deg(f)$) e quindi un PID. Valgono le seguenti proprietà:

- $(f) + (g) = (\mathrm{GCD}(f, g))$;
- $(f) \cap (g) = (\mathrm{LCM}(f, g))$;
- $(f) \subseteq (g) \Leftrightarrow f \in (g) \Leftrightarrow g | f \Leftrightarrow \exists q \in K[x] : f = qg$;
- $\sqrt{(f)} = \left(\dfrac{f}{\mathrm{GCD}(f, f')} \right)$: se $f = f_1^{r_1} \cdots f_t^{r_t}$ allora $\sqrt{(f)} = (f_1 \cdots f_t)$.

  Ricordiamo che $\sqrt{(f)} = \{g \in K[x] : g^n \in (f) \text{ per qualche } n \in \mathbb{Z}^+\}$;
- Se $d = \deg(f) > 0$, il quoziente $K[x]/(f)$ è un K-spazio vettoriale di dimensione d, una cui base è $\{1, x, \ldots, x^{d-1}\}$.

Divisione in $K[x]$

- Dato $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in K[x]$, definiamo:

$$\mathrm{LT}(f) = a_n x^n, \quad \mathrm{LM}(f) = x^n \quad \text{e} \quad \mathrm{LC}(f) = a_n.$$

  Ovviamente $\deg(f) = \deg(\mathrm{LT}(f))$.

- Per effettuare la divisione di f per g si può procedere come segue:
  - se $\deg(\mathrm{LT}(f)) < \deg(\mathrm{LT}(g))$ allora $f = 0 \cdot g + f$;
  - altrimenti, $\mathrm{LT}(f)/\mathrm{LT}(g)$ è il primo monomio del quoziente parziale. Si aggiorna il valore del dividendo $f = f - \mathrm{LT}(f)/\mathrm{LT}(g)g$;
  - se $\deg(\mathrm{LT}(g)) \leq \deg(\mathrm{LT}(f))$ allora il procedimento può ripetersi, aggiornando il quoziente parziale e il dividendo;
  - il processo terminerà quando la condizione sarà falsa (ad ogni passo $\deg(\mathrm{LT}(f))$ decresce strettamente).

- L'implicazione ED $\Longrightarrow$ PID, per $K[x]$, è conseguenza dell'algoritmo di divisione. Infatti il calcolo del GCD di due polinomi (Euclide) sfrutta proprio tale algoritmo e permette di calcolare il generatore di un ideale se è noto un insieme di generatori (necessariamente in numero finito per la noetherianità).

Divisione in $K[x]$

Algoritmo di divisione con resto

$$
\begin{array}{rrrr|rr}
x^3 & +2x^2 & -9x & -4 & x^2 & -1 \\
\cline{5-6}
-x^3 & & +x & & x & +2 \\
\cline{1-3}
 & 2x^2 & -8x & -4 & & \\
 & -2x^2 & & +2 & & \\
\cline{2-4}
 & & -8x & -2 & &
\end{array}
$$

Algoritmo

Osservazione

$\mathbb{Z}[x]$ non è un dominio euclideo (non essendo a ideali principali). Ad esempio non è possibile dividere x^2 per $2x+1$. In questi casi si può procedere soltanto se $LC(b) = \pm 1$ o con quella che viene chiamata *pseudodivisione*.

Problema dell'appartenenza

Dati un ideale I e un elemento f di $K[x]$, esiste un algoritmo per decidere se $f \in I$? (Ideal Membership)

Dato $I = (g)$, basta effettuare la divisione di f per il generatore g di I. Otteniamo $f = qg + r$ con $r = 0$ o $\deg(r) < \deg(g)$ (r univocamente determinato). Ne segue che $f \in I$ se e solo se $r = 0$.

Divisione in $K[x_1, \ldots, x_n]$?

- L'anello $K[x_1, \ldots, x_n]$, $n \geq 2$, non è un ED (poiché non è un PID). Quindi non è sempre possibile effettuare la divisione fra due polinomi mantenendo le buone proprietà del caso univariato.
- In $K[x]$ la relazione $\mathbf{x^n}$ **divide** $\mathbf{x^m}$ è una relazione d'ordine totale. Per questo la successione di monomi strettamente decrescente sui gradi termina dopo un numero finito di passi (buon ordinamento).
- Tra i monomi in più variabili la relazione di divisibilità definisce invece un ordinamento parziale. Ad esempio, in $K[x, y]$, x non è divisibile per y e y non lo è per x. È necessario quindi definire alcuni ordinamenti totali su $K[x_1, \ldots, x_n]$.

Problema dell'appartenenza
Dati un ideale I e un elemento f di $K[x_1, \ldots, x_n]$, esiste un algoritmo per decidere se $f \in I$?

L'ideale I non è necessariamente principale e quindi occorre eseguire una divisione per tutti i suoi generatori $f_1, \ldots, f_k$. Si vorrebbe trovare un'espressione del tipo $\mathbf{f = q_1 f_1 + \ldots + q_k f_k + r}$ e concludere che $f \in I$ se e solo se $r = 0$. Per fare questo occorre definire un ordinamento totale fra monomi e generalizzare l'algoritmo di divisione al caso di più polinomi.

Ordinamenti monomiali

Definizioni

- Sia $\mathcal{M}_n$ l'insieme dei monomi di $K[x_1, \ldots, x_n]$. La corrispondenza

$$\mathcal{M}_n \to \mathbb{Z}_{\geq 0}^n, \text{ definita da } \quad x_1^{\alpha_1} \ldots x_n^{\alpha_n} \mapsto (\alpha_1, \ldots, \alpha_n)$$

  è un isomorfismo di monoidi (mappa logaritmica).

- Usando la notazione $\mathrm{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \ldots x_n^{\alpha_n} \in \mathcal{M}_n$, scriviamo $\mathrm{x}^{\boldsymbol{\alpha}} \cdot \mathrm{x}^{\boldsymbol{\beta}} = \mathrm{x}^{\boldsymbol{\alpha}+\boldsymbol{\beta}}$. Inoltre possiamo definire $\mathrm{mDeg}(\mathrm{x}^{\boldsymbol{\alpha}}) = \boldsymbol{\alpha}$ e $\deg(\mathrm{x}^{\boldsymbol{\alpha}}) = |\boldsymbol{\alpha}| = \sum_i \alpha_i$.

Ordinamenti monomiali
Un ordinamento monomiale in $K[\mathrm{x}]$ è una relazione $\geq$ definita su $\mathcal{M}_n$ tale che valgano le seguenti:

- $\geq$ è un ordinamento totale, cioè ogni coppia di monomi è confrontabile;
- $\geq$ è compatibile con la moltiplicazione, cioè per ogni $\mathrm{x}^{\boldsymbol{\alpha}}, \mathrm{x}^{\boldsymbol{\beta}}, \mathrm{x}^{\boldsymbol{\gamma}}$ con $\mathrm{x}^{\boldsymbol{\alpha}} \geq \mathrm{x}^{\boldsymbol{\beta}}$ vale $\mathrm{x}^{\boldsymbol{\alpha}}\mathrm{x}^{\boldsymbol{\gamma}} \geq \mathrm{x}^{\boldsymbol{\beta}}\mathrm{x}^{\boldsymbol{\gamma}}$ (e conversa);
- $\geq$ è un buon ordinamento, cioè ogni sottoinsieme di $\mathcal{M}_n$ ha minimo.

Ordinamenti "notevoli"

Proprietà
Sia $\geq$ un ordinamento monomiale totale in $\mathcal{M}_n$, compatibile con il prodotto. Le seguenti sono equivalenti:

- $\geq$ è un buon ordinamento;
- $1 \leq \mathtt{x}^{\alpha}$ per ogni $\mathtt{x}^{\alpha} \in \mathcal{M}_n$;
- Se $\mathtt{x}^{\alpha}$ divide $\mathtt{x}^{\beta}$ allora in un qualunque ordinamento monomiale si ha $\mathtt{x}^{\alpha} \leq \mathtt{x}^{\beta}$.

Esempio
Dalle proprietà segue che in $K[x]$ esiste un unico ordinamento monomiale, quello per "grado": $1 < x < x^2 < \cdots < x^k < \cdots$

Lessicografico (Lex in $\mathcal{M}_n$ e $\mathbb{Z}^n_{\geq 0}$)
Dati $\mathtt{x}^{\alpha}, \mathtt{x}^{\beta} \in \mathcal{M}_n$, si definisce $\mathtt{x}^{\alpha} \geq_{\mathrm{Lex}} \mathtt{x}^{\beta}$ se $\alpha = \beta$ oppure se esiste r tale che $\alpha_i = \beta_i$ per ogni $i < r$ e $\alpha_r > \beta_r$. Equivalentemente, $\mathtt{x}^{\alpha} \geq_{\mathrm{Lex}} \mathtt{x}^{\beta}$ se $\alpha = \beta$ oppure se la prima entrata non nulla da sinistra di $\alpha - \beta$ è positiva.

Osservazione
L'ordinamento $\geq_{\mathrm{Lex}}$ induce le disuguaglianze: $x_1 >_{\mathrm{Lex}} x_2 >_{\mathrm{Lex}} \ldots >_{\mathrm{Lex}} x_n$. Permutando l'ordine delle variabili, si ottengono $n!$ diversi ordinamenti Lex.

Ordinamenti "notevoli"

Lessicografico graduato (GLex)
Dati $\mathrm{x}^\alpha, \mathrm{x}^\beta \in \mathcal{M}_n$, si definisce $\mathrm{x}^\alpha \geq_{\mathrm{GLex}} \mathrm{x}^\beta$ se $|\alpha| > |\beta|$ oppure se $|\alpha| = |\beta|$ e $\mathrm{x}^\alpha \geq_{\mathrm{Lex}} \mathrm{x}^\beta$.

Osservazione
Usando $\geq$ Lex, fra due monomi di $\mathcal{M}_n$ possono esistere infiniti monomi: $x_1 >_{\mathrm{Lex}} \cdots >_{\mathrm{Lex}} x_2^k >_{\mathrm{Lex}} \cdots >_{\mathrm{Lex}} x_2 >_{\mathrm{Lex}} 1$.
Usando $\geq_{\mathrm{GLex}}$ si verifica che esistono al più un numero finito di monomi fra due fissati. Infatti, il numero di monomi di grado d in $\mathcal{M}_n$ è $\binom{n+d-1}{d}$.
Vedremo che Lex è utile per eliminare variabili, mentre GRevLex è ottimale per il calcolo delle *sizigie*.

Lessicografico inverso graduato (GRevLex)
Dati $\mathrm{x}^\alpha, \mathrm{x}^\beta \in \mathcal{M}_n$, si definisce $\mathrm{x}^\alpha \geq_{\mathrm{GRevLex}} \mathrm{x}^\beta$ se $|\alpha| > |\beta|$ oppure se $|\alpha| = |\beta|$ e la prima entrata non nulla da destra di $\alpha - \beta$ è negativa.

Esempi

In $K[x, y]$ $\quad x^2y >_{\mathrm{Lex}} xy^2, \quad x^2y >_{\mathrm{GRevLex}} xy^2.$

In $K[x, y, z]$ $\quad x^2yz^2 >_{\mathrm{Lex}} xy^3z, \quad x^2yz^2 <_{\mathrm{GRevLex}} xy^3z.$

Ordinamenti tramite matrici

- Siano $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ e A una matrice $n \times n$ a entrate intere di rango massimo. Si definisce $\alpha \geq_A \beta$ se $A\alpha^t \geq_{\text{Lex}} A\beta^t$.
- $\geq_A$ è un ordinamento monomiale su $\mathcal{M}_n$ se e solo se la prima entrata non nulla di ogni colonna di A è positiva.
- Qualsiasi ordinamento monomiale può essere indotto tramite una matrice con le proprietà sopra descritte (Mora-Robbiano).
  Si osservi che matrici distinte possono indurre lo stesso ordinamento.

Esempi

- La matrice identica I_n definisce l'ordinamento Lex in $\mathcal{M}_n$.
- La matrice mostrata a fianco rappresenta l'ordinamento GLex in $\mathcal{M}_n$. Si osservi che la prima entrata della generica immagine coincide con il grado del monomio.

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

- Quale matrice rappresenta GRevLex?
- Costruire una funzione che, data un'opportuna matrice, ordini una lista di monomi indipendentemente dall'ordinamento dell'anello in uso.

Ordinamenti pesati

- Sia $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{R}^n$ un vettore "generico", cioè tale che nessun ω_i sia combinazione lineare a coefficienti interi degli altri ω_j.
  Dati $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, si definisce $\alpha \geq_\omega \beta$ se $\alpha \cdot \omega \geq \beta \cdot \omega$ (scalare).
- Se $\omega_i > 0$, per $i = 1, \ldots, n$, allora $\geq_\omega$ è un ordinamento monomiale.
- Se $\omega \in \mathbb{Z}^n_{\geq 0}$, allora $\geq_\omega$ è un ordinamento parziale. Considerato un ordinamento monomiale $\geq_\mu$, la relazione $\alpha \geq_{\omega\mu} \beta$ definita da $\alpha >_\omega \beta$ oppure $\alpha =_\omega \beta$ ($\alpha \cdot \omega = \beta \cdot \omega$) e $\alpha \geq_\mu \beta$ è un ordinamento monomiale.
- Sia $\omega = (\omega_1, \ldots, \omega_i, 0, \ldots, 0) = (1, \ldots, 1, 0, \ldots, 0)$, l'ordinamento monomiale $\geq_{\omega\text{GRevLex}}$, è detto **ordinamento di eliminazione** delle prime i variabili di $K[x_1, \ldots, x_n]$.
- Costruire la funzione `ordina` con pesi e matrice e applicarla.

Esempi

In $K[x_1, \ldots, x_5]$ con $\omega = (1, 1, 0, 0, 0)$ si ha:

	μ = GLex	μ = GRevLex
$>_\mu$	$x_3x_4^2 > x_1x_4 > x_2x_3 > x_2x_5$	$x_3x_4^2 > x_2x_3 > x_1x_4 > x_2x_5$
$>_{\omega\mu}$	$x_1x_4 > x_2x_3 > x_2x_5 > x_3x_4^2$	$x_2x_3 > x_1x_4 > x_2x_5 > x_3x_4^2$

Algoritmo di divisione

Definizioni in $K[x_1, \ldots, x_n]$

- Dato l'anello $K[x_1, \ldots, x_n]$, sia fissato un ordinamento monomiale $\geq$ su $\mathcal{M}_n$. Preso un polinomio $f \in K[\mathtt{x}]$, scriveremo:

$$f(\mathtt{x}) = a_1 \mathtt{x}^{\alpha_1} + a_2 \mathtt{x}^{\alpha_2} + \cdots + a_r \mathtt{x}^{\alpha_r},$$

  con $\mathtt{x}^{\alpha_1} > \mathtt{x}^{\alpha_2} > \cdots > \mathtt{x}^{\alpha_r}$.

- Il **multigrado** di f, $\mathrm{mDeg}(f) = \alpha_1$, è la n-pla massima tra quelle corrispondenti ai termini di f con l'ordinamento monomiale prescelto.
- Il **termine iniziale** di f, $\mathrm{LT}(f) = a_1 \mathtt{x}^{\alpha_1}$, è il maggiore fra i termini di f, cioè il termine con multigrado massimo. Analogamente, il monomio e il coefficiente iniziali, $\mathrm{LM}(f) = \mathtt{x}^{\alpha_1}$ e $\mathrm{LC}(f) = a_1$, sono rispettivamente il monomio e il coefficiente del termine iniziale di f.
- Osserviamo che presi $f, g \in K[\mathtt{x}]$, si ha $\mathrm{LT}(fg) = \mathrm{LT}(f)\mathrm{LT}(g)$, come anche per LM e LC. Inoltre $\mathrm{LM}(f+g) \leq \max\{\mathrm{LM}(f), \mathrm{LM}(g)\}$ e vale l'uguaglianza quando $\mathrm{LM}(f) \neq \mathrm{LM}(g)$.

Divisione in $K[x_1, \ldots, x_n]$

- Vogliamo definire la divisione di un polinomio f per un insieme di polinomi $\{f_1, \ldots, f_s\}$. Lo scopo è quello di ottenere la seguente scrittura:

$$f = q_1 f_1 + \cdots + q_s f_s + r.$$

  Analogamente al caso dei polinomi in una variabile, si richiede che $r = 0$ o che $\mathrm{LT}(r)$ non sia divisibile per nessuno degli $\mathrm{LT}(f_i)$.

- Si procede nel modo seguente:
  - Provare a dividere $\mathrm{LT}(f)$ per $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, nell'ordine, e se l'operazione è possibile all'indice i aggiungere $\mathrm{LT}(f)/\mathrm{LT}(f_i)$ all'i-esimo quoziente e sottrarre $(\mathrm{LT}(f)/\mathrm{LT}(f_i))f_i$ da f;
  - Se non è stato possibile dividere $\mathrm{LT}(f)$ per nessuno tra gli $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$, allora aggiungere $\mathrm{LT}(f)$ al resto r e sottrarre $\mathrm{LT}(f)$ da f;
  - Se il dividendo f è non nullo, ripetere il processo.

- Osserviamo che l'algoritmo ha sempre termine, poiché ad ogni passo il multigrado di f decresce strettamente (ordinamento monomiale).

Algoritmo

Divisione in $K[x_1, \ldots, x_n]$

Sia $K[x, y]$ dotato di ordinamento Lex con $x > y$. Dividere il polinomio $f = x^2y + xy^2 + y^2$ per la coppia $\{f_1 = xy - 1,\ f_2 = y^2 - 1\}$.

Algoritmo di divisione con resto

$$
\begin{array}{rrrrrrr|l}
x^2y & +xy^2 & & +y^2 & & & & f_1 = xy - 1 \\
-x^2y & & +x & & & & & f_2 = y^2 - 1 \\
\hline
 & xy^2 & +x & +y^2 & & & & q_1 = x + y \\
 & -xy^2 & & & +y & & & q_2 = 1 \\
\hline
 & & x & +y^2 & +y & & & r = x + y + 1 \\
 & & & y^2 & +y & & & \\
 & & & -y^2 & & +1 & & \\
\hline
 & & & & y & +1 & & \\
 & & & & & 1 & &
\end{array}
$$

Il risultato ottenuto è quindi $f = q_1 f_1 + q_2 f_2 + r$:

$$x^2y + xy^2 + y^2 = (x + y)(xy - 1) + (1)(y^2 - 1) + (x + y + 1);$$

Divisione in $K[x_1, \ldots, x_n]$

Sia $K[x, y]$ dotato di ordinamento Lex con $x > y$. Dividere il polinomio $f = x^2y + xy^2 + y^2$ per la coppia $\{f_2 = y^2 - 1,\ f_1 = xy - 1\}$.

Algoritmo di divisione con resto

$$
\begin{array}{rrrrrr|l}
x^2y & +xy^2 & & +y^2 & & f_2 = y^2 - 1 \\
-x^2y & & +x & & & f_1 = xy - 1 \\
\hline
 & xy^2 & +x & +y^2 & & q_2 = x + 1 \\
 & -xy^2 & +x & & & q_1 = x \\
\hline
 & & 2x & +y^2 & & r = 2x + 1 \\
 & & & y^2 & & \\
 & & & -y^2 & +1 & \\
\hline
 & & & & 1 &
\end{array}
$$

Il risultato ottenuto è quindi $f = q_2 f_2 + q_1 f_1 + r$:

$$x^2y + xy^2 + y^2 = (x + 1)(y^2 - 1) + (x)(xy - 1) + (2x + 1);$$

Divisione in $K[x_1, \ldots, x_n]$

Abbiamo osservato che, nell'esecuzione dell'algoritmo, l'ordine dei polinomi divisori risulta essere di fondamentale importanza. In ogni caso valgono i seguenti:

Risultati
Sia fissato un ordinamento monomiale in $K[\mathtt{x}]$ e siano $f, f_1, \ldots, f_s \in K[\mathtt{x}]$, allora esistono $q_1, \ldots, q_s, r \in K[\mathtt{x}]$ tali che:

- $f = q_1 f_1 + \cdots + q_s f_s + r$;
- nessun termine di r è divisibile per $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$;
- se $q_i f_i \neq 0$ vale $\mathrm{mDeg}(f) \geq \mathrm{mDeg}(q_i f_i)$.

In più esiste un algoritmo che determina $q_1, \ldots, q_s, r$.

Problema dell'appartenenza
Possiamo a questo punto stabilire se dato un ideale I e un elemento f di $K[x_1, \ldots, x_n]$, esiste un algoritmo per decidere se $f \in I$?

Divisione in $K[x_1, \ldots, x_n]$

Osservazioni

Con gli strumenti di cui attualmente disponiamo, possiamo solo affermare che la condizione "resto della divisione di f per $\{f_1, \ldots, f_s\}$ uguale a 0" è una condizione sufficiente ma non necessaria affinché $f \in (f_1, \ldots, f_s)$.
Ciò è in contrasto con quanto accade per i polinomi in una variabile. Si ovvierà a questo inconveniente definendo un opportuno insieme di generatori per l'ideale $(f_1, \ldots, f_s)$, dipendente da un ordinamento monomiale.

Esempi

- Dati $f = xy^2 - x$, $f_1 = xy + 1$ e $f_2 = y^2 - 1$ in $K[x, y]$, con Lex:

$$f/\{f_1, f_2\} \longrightarrow xy^2 - x = y(xy + 1) + 0(y^2 - 1) - x - y;$$
$$f/\{f_2, f_1\} \longrightarrow xy^2 - x = 0(xy + 1) + x(y^2 - 1) + 0.$$

- Dato $f = x^2y^2 + y^2 + 2$ in $K[x, y]$, con GRevLex:

$f_1 = xy^2 - 1;$ $f_2 = y^2 + 1;$	$f/\{f_1, f_2\} \longrightarrow f = xf_1 + f_2 + x + 1;$ $f/\{f_2, f_1\} \longrightarrow f = 0f_1 + (x^2 + 1)f_2 - x^2 + 1.$
$g_1 = x + 1;$ $g_2 = y^2 + 1;$	$f/\{g_1, g_2\} \longrightarrow f = (xy^2 - y^2)g_1 + 2g_2 + 0;$ $f/\{g_2, g_1\} \longrightarrow f = (-x + 1)g_1 + (x^2 + 1)g_2 + 0.$

Ideali monomiali

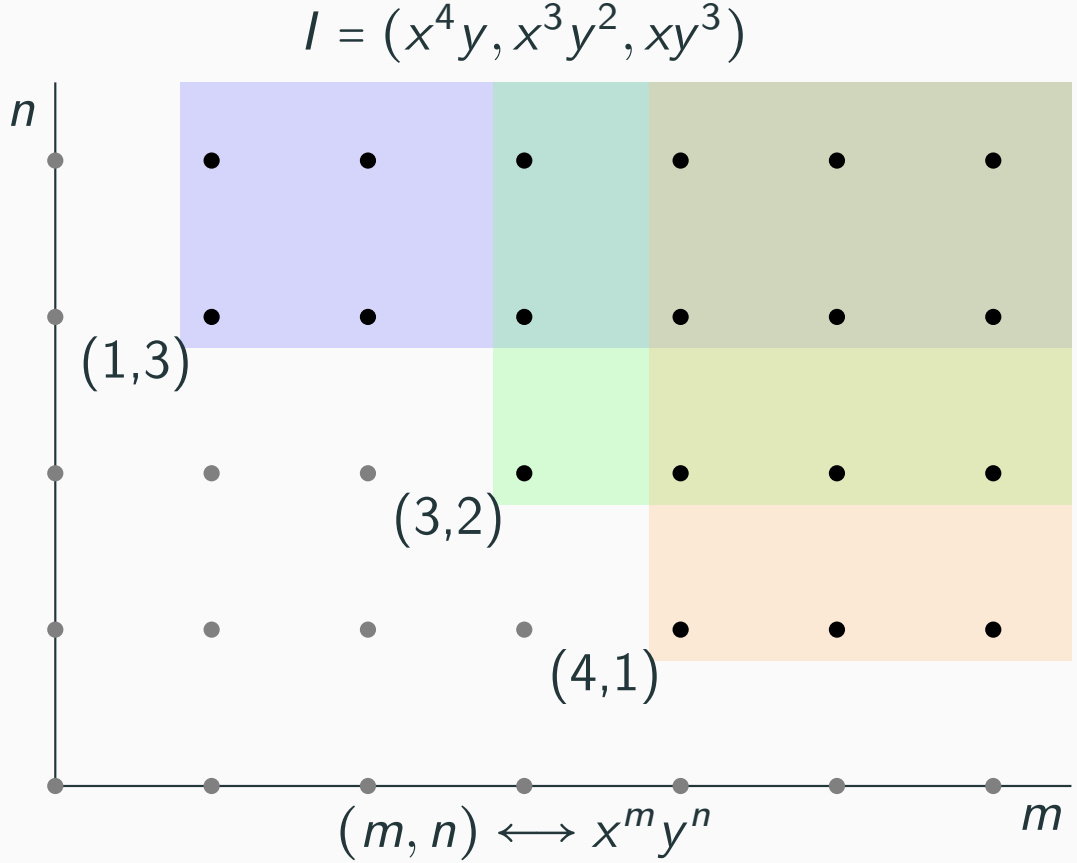
Definizioni

- Un ideale I dell'anello $K[\mathtt{x}]$ si dice **monomiale** se esiste un insieme di generatori formato da monomi.
- Un ideale monomiale I può essere visto come lo spazio vettoriale su K generato da tutti i monomi di I.
- Sia $I \subset K[\mathtt{x}]$ un ideale monomiale e $f = \sum_{i=1}^{r} a_i u_i \in K[\mathtt{x}]$ un polinomio non nullo. Allora $f \in I$ se e solo se $u_i \in I$ per ogni $i = 1, \ldots, r$. Definendo $\mathrm{supp}(f) = \{u_i\}_{i \in [r]}$: $f \in I$ se e solo se $\mathrm{supp}(f) \subset I$.
- Sia I un ideale di $K[\mathtt{x}]$. Le seguenti condizioni sono equivalenti:
  - I è un ideale monomiale;
  - Per ogni $f \in K[\mathtt{x}]$ vale: $f \in I$ se e solo $\mathrm{supp}(f) \subset I$;
  - I è generato da un numero finito di monomi.

Esempio
L'ideale $I = (xyz, y^2, x^2yz + 3xy^2)$ di $K[x, y, z]$ è monomiale. Infatti $x^2yz = x(xyz)$ e $3xy^2 = 3x(y^2)$ appartengono a I (così la loro somma). Quindi $I = (xyz, y^2)$.

Lemma di Dickson

È possibile identificare ogni ideale monomiale di $K[x_1, \ldots, x_n]$ con un opportuno sottoinsieme di $\mathbb{Z}_{\geq 0}^n$. Questa osservazione permette una dimostrazione diretta del lemma di Dickson, indipendentemente dal teorema della base di Hilbert [2].



Proprietà

- Dato un ideale monomiale $I \in K[\mathtt{x}]$, $I = (\mathtt{x}^{\boldsymbol{\alpha}_1}, \ldots, \mathtt{x}^{\boldsymbol{\alpha}_r})$, vale il seguente criterio di appartenenza:

$$\mathtt{x}^{\boldsymbol{\beta}} \in I \text{ se e solo se } \mathtt{x}^{\boldsymbol{\alpha}_j} \mid \mathtt{x}^{\boldsymbol{\beta}} \text{ per qualche } j \in \{1, \ldots, r\}.$$

- Un ideale monomiale I possiede un unico insieme minimale di generatori. Tale insieme può essere indicato con $G(I)$.
- L'anello dei polinomi $K[x_1, \ldots, x_n]$ è un UFD, quindi è possibile calcolare GCD e LCM fra due elementi non nulli. In particolare, dati due monomi $\mathtt{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} + \cdots + x_n^{\alpha_n}$ e $\mathtt{x}^{\boldsymbol{\beta}} = x_1^{\beta_1} + \cdots + x_n^{\beta_n}$ si ha che:

$$\mathtt{x}^{\boldsymbol{\gamma}} = \mathrm{LCM}(\mathtt{x}^{\boldsymbol{\alpha}}, \mathtt{x}^{\boldsymbol{\beta}}), \text{ con } \gamma_i = \max\{\alpha_i, \beta_i\}, \text{ per } i \in [n];$$
$$\mathtt{x}^{\boldsymbol{\delta}} = \mathrm{GCD}(\mathtt{x}^{\boldsymbol{\alpha}}, \mathtt{x}^{\boldsymbol{\beta}}), \text{ con } \delta_i = \min\{\alpha_i, \beta_i\}, \text{ per } i \in [n].$$

Osservazioni

Siano I e J due ideali monomiali di $K[\mathrm{x}]$, con $G(I) = \{\mathrm{x}^{\alpha_1}, \ldots, \mathrm{x}^{\alpha_r}\}$ e $G(J) = \{\mathrm{x}^{\beta_1}, \ldots, \mathrm{x}^{\beta_s}\}$. Valgono le seguenti proprietà:

- $I + J = \left(\mathrm{x}^{\alpha_1}, \ldots, \mathrm{x}^{\alpha_r}, \mathrm{x}^{\beta_1}, \ldots, \mathrm{x}^{\beta_s}\right)$;
- $IJ = \left(\mathrm{x}^{\alpha_i}\mathrm{x}^{\beta_j} \ : \ i \in [r] \text{ e } j \in [s]\right)$;
- $I \cap J = \left(\mathrm{LCM}(\mathrm{x}^{\alpha_i}, \mathrm{x}^{\beta_j}) \ : \ i \in [r] \text{ e } j \in [s]\right)$;
- $\sqrt{I} = (\sqrt{\mathrm{x}^{\alpha_1}}, \ldots, \sqrt{\mathrm{x}^{\alpha_r}})$, dove $\sqrt{\mathrm{x}^{\alpha_i}} = x_{i_1} \cdots x_{i_t}$ con $\alpha_{i_1}, \ldots, \alpha_{i_t} \neq 0$;
- $I : J = \bigcap_{j=1}^{s} I : (\mathrm{x}^{\beta_j})$, e $G(I : (\mathrm{x}^{\beta_j})) \subseteq \left\{ \dfrac{\mathrm{x}^{\alpha_i}}{\mathrm{GCD}(\mathrm{x}^{\alpha_i}, \mathrm{x}^{\beta_j})} \ : \ i \in [r] \right\}$.

  Ricordiamo che $I : J = \{f \in K[\mathrm{x}] \ : \ fg \in I \text{ per ogni } g \in J\}$;
- Il quoziente $K[\mathrm{x}]/I$ è generato, come spazio vettoriale su K, dalle classi i cui rappresentanti sono i monomi che non appartengono a I.

Ideale iniziale

Sia I un ideale di $K[\mathtt{x}]$ e sia fissato un ordinamento monomiale.

- L'**ideale iniziale** di I, $\mathrm{LT}(I)$ o $\mathrm{in}(I)$, è definito dall'ideale monomiale

$$\mathrm{LT}(I) = (\mathrm{LT}(f) \ : \ f \in I),$$

  cioè l'ideale generato dai leading term di tutti i polinomi di I.

- Sia $\mathrm{LT}(I) = (\mathtt{x}^{\alpha_1}, \ldots, \mathtt{x}^{\alpha_r})$ e siano $f_1, \ldots, f_r \in I$ tali che $\mathrm{LT}(f_i) = \mathtt{x}^{\alpha_i}$ per $i \in [r]$. Allora $I = (f_1, \ldots, f_r)$.

Osservazione
Se $I = (f_1, \ldots f_r)$ allora sicuramente $(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r)) \subset \mathrm{LT}(I)$. In generale può valere l'inclusione stretta come mostra il seguente esempio.

Sia $I = \left(x^2 + y, x^2 - y\right) \subset K[x, y]$ con un qualunque ordinamento monomiale graduato. Osserviamo che $y \in I$ e quindi $y \in \mathrm{LT}(I)$, ma $y \notin \left(\mathrm{LT}(x^2 + y), \mathrm{LT}(x^2 - y)\right) = \left(x^2\right)$.

Basi di Gröbner

Definizioni e proprietà

Sia I un ideale di $K[\mathrm{x}]$, con un ordinamento monomiale fissato.

☆ Un insieme di elementi $\{g_1, \ldots, g_s\} \subset I$ si dice una **base di Gröbner** (o *base standard* o *G-base*) per I se

$$\mathrm{LT}(I) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$$

- Ogni ideale non nullo di $K[\mathrm{x}]$ ammette una base di Gröbner. Aggiungendo ad essa polinomi di I, si ottiene ancora una base di Gröbner.
- Una base di Gröbner per I costituisce un insieme di generatori per I.
- Un base di Gröbner per I, $\{g_1, \ldots, g_s\}$, si dice **minimale** se $\mathrm{LT}(g_i)$ non divide $\mathrm{LT}(g_j)$, per $i \in [s]$ e $j \neq i$. Spesso si richiede inoltre che i generatori siano monici ($\mathrm{LC}(g_i) = 1$).
- Un base di Gröbner per I, $\{g_1, \ldots, g_s\}$, si dice **ridotta** se $\mathrm{LT}(g_i)$ non divide alcun monomio di $\mathrm{supp}(g_j)$, per $i \in [s]$ e $j \neq i$. Spesso si richiede inoltre che i generatori siano monici ($\mathrm{LC}(g_i) = 1$).
- Ogni ideale non nullo di $K[\mathrm{x}]$, fissato un ordinamento monomiale, ammette un'unica base di Gröbner ridotta.

Esempio

Sia $I = \left(x^2 + y^2, xy\right) \subset K[x, y]$ con l'ordinamento Lex. Cerchiamo un base di Gröbner per I facendo qualche osservazione:

- Tutti i monomi di grado 3 appartengono ad I (e quindi anche a $\mathrm{LT}(I)$):

$$x^3 = x(x^2 + y^2) - y(xy); \quad x^2y = x(xy);$$
$$y^3 = y(x^2 + y^2) - x(xy); \quad xy^2 = y(xy).$$

  Quindi tutti i polinomi omogenei di grado 3 appartengono a $\mathrm{LT}(I)$.

- Poiché ogni monomio di grado ≥ 3 è divisibile per un monomio di grado 3, allora questi appartengono a I e quindi a $\mathrm{LT}(I)$.
- Anche x^2 e xy appartengono a $\mathrm{LT}(I)$ e devono appartenere ad un qualunque insieme di generatori di $\mathrm{LT}(I)$.
- Infine notiamo che $y^3 \notin (x^2, xy)$ e quindi sono necessari almeno tre elementi per una base di Gröbner.
- Una tale base è quindi $\{y^3, x^2 + y^2, xy\}$.

Divisione in $K[\mathtt{x}]$ e G-basi

Sia I un ideale di $K[\mathtt{x}]$, con un ordinamento monomiale fissato.

Teorema di unicità
Sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner per l'ideale I e sia $f \in K[\mathtt{x}]$. Allora esiste unico $r \in K[\mathtt{x}]$ tale che:

- $f = g + r$ per un opportuno $g \in I$;
- nessun termine di r è divisibile per qualche $\mathrm{LT}(g_i)$;

In particolare r è il resto della divisione di f per G.

Osservazioni

- Il resto della divisione di f per una base di Gröbner di I si indica con $f \bmod I$, $\mathrm{NF}(f)$ (forma normale) o $\overline{f}^{G}$ (G-riduzione).
- Il resto della divisione di un polinomio f per una base di Gröbner di I dipende soltanto da I e dall'ordinamento monomiale fissato. Non dipende né dalla base scelta $\left(\overline{f}^{G} = \overline{f}^{G'}\right)$ né dall'ordine dei divisori.
- Osserviamo che i quozienti delle divisione non sono unici; l'unicità del resto nella divisione è il massimo che si riesce ad ottenere.

Problema dell'appartenenza

Ideal membership
Sia I un ideale di $K[\mathtt{x}]$, con ordinamento monomiale fissato. Allora $f \in I$ se e solo se il resto della divisione di f per una base di Gröbner di I è zero, cioè $f \bmod I = 0$, $\mathrm{NF}(f) = 0$ o $\overline{f}^{G} = 0$.

Esercizi

1. In $K[\mathtt{x}]$, dotato di Lex, dividere xy per $x+z$, $y-z$. Ripetere invertendo i divisori.
2. Sia $I = (f_1, f_2, f_3) \subset K[x, y, z]$ dove $f_1 = xy^2 - xz + y$, $f_2 = xy - z^2$ e $f_3 = x - yz^4$. Trovare un polinomio $f \in I$ tale che $\mathrm{LT}(f) \notin (\mathrm{LT}(f_1), \mathrm{LT}(f_2), \mathrm{LT}(f_3))$, utilizzando gli ordinamenti GRevLex e Lex.
3. Sia $B = \{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$. Provare che B non è una base di Gröbner per l'ideale (B), rispetto all'ordinamento GRevLex.
4. Sia $I \subset K[\mathtt{x}]$ 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.

Codice

Costruzione di una base di Gröbner

- Siano f, g polinomi di $K[\mathtt{x}]$, con ordinamento monomiale fissato, e sia $\mathtt{x}^{\gamma} = \mathrm{LCM}\left(\mathrm{LM}(f), \mathrm{LM}(g)\right)$. Si definisce S-polinomio (o S-coppia):

$$S(f,g) = \frac{\mathtt{x}^{\gamma}}{\mathrm{LT}(f)} f - \frac{\mathtt{x}^{\gamma}}{\mathrm{LT}(g)} g$$

- Notiamo che in $S(f,g)$ i termini di multigrado $\boldsymbol{\gamma}$ si cancellano mentre tutti gli altri termini hanno multigrado $< \boldsymbol{\gamma}$: $\mathrm{mDeg}(S(f,g)) < \boldsymbol{\gamma}$.

- Un impedimento a che $F = \{f_1, \ldots, f_r\}$ sia una base di Gröbner è che

$$\mathrm{LT}\left(S(f_i, f_j)\right) \notin \left(\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_r)\right) = \left(\mathrm{LT}(F)\right).$$

- Supponiamo di avere una cancellazione tra i LT di un insieme di polinomi f_i, cioè una combinazione $\sum_{i=1}^{t} c_i \mathtt{x}^{\alpha_i} f_i$ con $c_i \in K$, $\alpha_i + \mathrm{mDeg}(f_i) = \delta$ (se $c_i \neq 0$) e $\mathrm{mDeg}\left(\sum c_i \mathtt{x}^{\alpha_i} f_i\right) < \delta$. Allora, posto $\mathtt{x}^{\gamma_{jk}} = \mathrm{LCM}\left(\mathrm{LT}(f_j), \mathrm{LT}(f_k)\right)$, esistono c_{jk} tali che:

$$\sum_{i=1}^{t} c_i \mathtt{x}^{\alpha_i} f_i = \sum_{j,k=1}^{t} c_{jk} \mathtt{x}^{\delta - \gamma_{jk}} S(f_j, f_k).$$

Criterio di Buchberger (1965)

Sia I un ideale di $K[\mathrm{x}]$, con ordinamento monomiale fissato, generato da $G = \{g_1, \ldots, g_t\}$. L'insieme G è una base di Gröbner per I se e solo se per ogni coppia (i, j), con $i \neq j$, il resto della divisione di $S(g_i, g_j)$ mod $G = 0$.

Osservazioni

- Dato $f \in I$, la tesi è $\mathrm{LT}(f) \in (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s))$. Si ha $f = \sum h_i g_i$ e $\mathrm{mDeg}(f) \leq \max\{m_i\}$, dove $m_i = \mathrm{mDeg}(h_i g_i)$.
  Sia δ il multigrado del monomio direttore che appare il minor numero di volte tra tutte le espressioni $\sum h_i g_i$ con m_i massimo.
- Se $\mathrm{mDeg}(f) = \delta$ abbiamo la tesi.
- Se fosse $\mathrm{mDeg}(f) < \delta$ avremmo:
  $$f = \sum h_i g_i = \sum_{m_i = \delta} \mathrm{LT}(h_i) g_i + \sum_{m_i = \delta} (h_i - \mathrm{LT}(h_i))\, g_i + \sum_{m_i < \delta} h_i g_i,$$
  con i monomi di multigrado δ solo nella prima sommatoria, quindi solo in essa si trovano le cancellazioni di δ. Scriviamo queste come combinazione degli S-polinomi G-ridotti $S(g_j, g_k) = \sum a_{ijk} g_i$.
  Poiché $\mathrm{mDeg}(a_{ijk} g_i) \leq \mathrm{mDeg}(S(g_j, g_k))$, allora non esiste alcun monomio di multigrado δ $\lightning$

Algoritmo di Buchberger

Il criterio di Buchberger suggerisce un algoritmo per costruire una base di Gröbner. Sia $F = \{f_1, \ldots, f_r\}$ un insieme di generatori dell'ideale $I \subset K[\mathtt{x}]$. Indichiamo con f mod F il resto della divisione di f per F.

- Si aggiungono ad F tutti gli elementi $S(f_i, f_j)$ mod F;
- si ripete questa operazione col nuovo insieme F;
- così facendo si ottiene una catena ascendente di ideali monomiali data, ad ogni passo, da $(\mathrm{LT}(F))$. Per noetherianità tale catena è stazionaria e questo implica che, dopo un numero finito di passi, si verifica $S(f_i, f_j)$ mod $F = 0$, per ogni $i \neq j$;
- l'algoritmo ha termine quando, in un blocco di operazioni, non viene fatta alcuna aggiunta all'insieme F;
- al termine, per Buchberger, F è una base di Gröbner.

Algoritmo

Minimalizzazione e riduzione di G-basi

Sia I un ideale non nullo di $K[\mathtt{x}]$, con ordinamento monomiale fissato. Se G è una base di Gröbner per I, allora è possibile estrarre da essa una G-base minimale G' e la G-base ridotta G''.

Osserviamo che se per $g \in G$ vale che $\mathrm{LT}(g) \in (\mathrm{LT}(G \setminus \{g\}))$, allora $G \setminus \{g\}$ è ancora una base di Gröbner per I.

Minimalizzazione
Per ottenere una G-base minimale da G basta eliminare tutti i polinomi il cui LT è multiplo di quello di qualche altro polinomio di G. Cioè per ogni $g \in G$ se $\mathrm{LT}(g) \notin \mathrm{LT}(G \setminus \{g\})$ allora consideriamo $G' = G' \cup \{g\}$. Al termine del processo G' sarà una G-base minimale per I.

Riduzione
Per ottenere la G-base ridotta a partire da una base minimale G' basta sostituire ad ogni suo polinomio il resto della divisione di esso per i rimanenti polinomi. Cioè per ogni $g \in G'$ poniamo $g' = g \bmod (G' \setminus \{g\})$ e consideriamo $G' = (G' \setminus \{g\}) \cup \{g'\}$. Al termine del processo G' sarà la G-base ridotta per I.

Esempio

Siano $K[x,y]$, con ordinamento GLex, $F = \{x^3 - 2xy, x^2y - 2y^2 + x\} = \{f_1, f_2\}$ e $J = (\mathrm{LT}(f_1), \mathrm{LT}(f_2)) = (x^3, x^2y)$. Utilizzando l'algoritmo di Buchberger costruiamo una base di Gröbner per $I = (F)$.

- $f_3 = S(f_1, f_2) = -x^2$, $\mathrm{LT}(f_3) \notin J$, quindi $F = \{f_1, f_2, f_3\}$.
- $f_4 = S(f_1, f_3) = -2xy$ e $f_5 = S(f_2, f_3) = -2y^2 + x$, $\mathrm{LT}(f_4), \mathrm{LT}(f_5) \notin J$, quindi $F = \{f_1, f_2, f_3, f_4, f_5\}$.
- Si verifica che $S(f_i, f_j) \bmod F = 0$ per $i, j \in [5]$, $i \neq j$. Per Buchberger l'algoritmo ha fine.
- Quindi $F = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$ è una base di Gröbner per I.
- F non è minimale. Per renderla tale bisogna eliminare quei polinomi il cui LT è multiplo di quello di qualche altro polinomio. Quindi $x^3 - 2xy$ e $x^2y - 2y^2 + x$ possono essere eliminati per la presenza di $-x^2$.
- Una base di Gröbner minimale è $G = \left\{x^2, xy, y^2 - \frac{1}{2}x\right\}$. In questo caso G è anche ridotta.

Variazioni Buchberger

Sia dato l'anello $K[\mathtt{x}]$, con ordinamento monomiale fissato.

- Dati $f \in K[\mathtt{x}]$ e l'insieme $F = \{f_1, \ldots, f_r\}$, si dice che f si riduce a zero modulo F, $f \xrightarrow{F} 0$, se esistono $a_i \in K[\mathtt{x}]$ tali che $f = a_1 f_1 + \cdots + a_r f_r$, con $\mathrm{LT}(f) \geq \mathrm{LT}(a_i f_i)$ quando $a_i f_i \neq 0$.
- Osserviamo che $f \bmod F = 0$ implica $f \xrightarrow{F} 0$, ma non vale il converso.

☆ Sia I l'ideale generato da $G = \{g_1, \ldots, g_s\}$. G è una base di Gröbner per I se e solo se per ogni coppia (i, j), con $i \neq j$, si ha $S(g_i, g_j) \xrightarrow{G} 0$.

- Siano $f_i, f_j \in F$ tali che $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) = \mathrm{LT}(f_i)\mathrm{LT}(f_j)$, cioè hanno monomi iniziali coprimi, allora $S(f_i, f_j) \xrightarrow{F} 0$.
- Questi risultati affermano che nell'algoritmo di Buchberger ci si pùo limitare alla verifica che $S(f_i, f_j) \xrightarrow{F} 0$ soltanto nei casi in cui $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) \neq \mathrm{LT}(f_i)\mathrm{LT}(f_j)$.

Osservazioni

Sia I un ideale non nullo di $K[\mathtt{x}]$, con ordinamento monomiale fissato. Abbiamo visto che è sempre possibile trovare la base di Gröbner ridotta per I. In particolare, per definizione, una qualsiasi G-base permette di calcolare immediatamente l'ideale iniziale $\mathrm{LT}(I)$.

Uguaglianza fra ideali
Sia J un ideale non nullo di $K[\mathtt{x}]$. Valgono le seguenti:

- $I = J$ se e solo se hanno la stessa base di Gröbner ridotta;
- Se $I \subseteq J$, allora $I = J$ se e solo se $\mathrm{LT}(I) = \mathrm{LT}(J)$.

Quozienti

- Nel quoziente $K[\mathtt{x}]/I$ i monomi $\{\mathtt{x}^{\boldsymbol{\alpha}} \in \mathcal{M}_n \ : \ \mathtt{x}^{\boldsymbol{\alpha}} \notin \mathrm{LT}(I)\}$ sono tutti distinti e costituiscono una base di $K[\mathtt{x}]/I$ come K-spazio vettoriale;
- I K-spazi vettoriali $K[\mathtt{x}]/I$ e $K[\mathtt{x}]/\mathrm{LT}(I)$ sono isomorfi. Un isomorfismo è dato da $f + I \mapsto (f \bmod G) + \mathrm{LT}(I)$, per una qualsiasi base di Gröbner per I.

Altre applicazioni

Problema dell'eliminazione

Definizioni

- Sia I un ideale di $K[x_1, \ldots, x_n]$. Eliminare le variabili $x_1, \ldots, x_k$ da I significa determinare l'ideale $I \cap K[x_{k+1}, \ldots, x_n]$ (proiezione).
- $I_k = I \cap K[x_{k+1}, \ldots, x_n]$ è detto k-esimo **ideale di eliminazione** di I. Osserviamo che I_{k+1} è il primo ideale di eliminazione di I_k.

Risultati

Sia fissato un ordinamento di eliminazione delle variabili $x_1, \ldots, x_k$.

- Per ogni polinomio $f \in K[\mathtt{x}]$ risulta che $f \in K[x_{k+1}, \ldots, x_n]$ se e solo se $\mathrm{LT}(f) \in K[x_{k+1}, \ldots, x_n]$.
- Se G è una base di Gröbner per I, allora $G_k = G \cap K[x_{k+1}, \ldots, x_n]$ è una base di Gröbner per I_k (rispetto alla restrizione dell'ordinamento).
- Quindi, per eliminare le indeterminate $x_1, \ldots, x_k$ dall'ideale I, bisogna dapprima calcolare una base di Gröbner G per I rispetto ad un opportuno ordinamento di eliminazione. Infine basta selezionare da G tutti i polinomi in cui compaiono esclusivamente le indeterminate $x_{k+1}, \ldots, x_n$ per ottenere G_k e generare così I_k.

Risoluzione di un sistema polinomiale

$$\begin{cases} f_1 = x^2 + y + z - 1 = 0 \\ f_2 = x + y^2 + z - 1 = 0 \\ f_3 = x + y + z^2 - 1 = 0. \end{cases}$$

Sia $I \subset \mathbb{R}[x, y, z]$ l'ideale generato da $\{f_1, f_2, f_3\}$ e sia fissato in $\mathbb{R}[x, y, z]$ l'ordinamento Lex, con $x > y > z$.

- Calcolando una base di Gröbner per I si ottiene $\{g_1, g_2, g_3, g_4\}$ con

$$g_1 = z^6 - 4z^4 + 4z^3 - z^2, \quad g_2 = 2yz^2 + z^4 - z^2,$$
$$g_3 = y^2 - y - z^2 + z, \quad g_4 = x + y + z^2 - 1.$$

- Per l'eliminazione si ha $I_1 = I \cap \mathbb{R}[y, z] = (g_1, g_2, g_3)$ e $I_2 = I \cap \mathbb{R}[z] = (g_1)$. Infatti g_1 è un polinomio nella sola indeterminata z.
- Fattorizzando g_1 si ottiene $g_1 = z^2(z-1)^2(z^2 + 2z - 1)$ e quindi le quattro radici distinte $\left\{0, 1, -1 \pm \sqrt{2}\right\} = \{0, 1, a, b\}$ in $\mathbb{R}$.
- Da g_2 e g_3 si ottengono i seguenti punti di $\mathbb{R}^2$:

$$\{(0,0), (1,0), (0,1), (a,a), (b,b)\}.$$

- Sostituendo le coppie in g_4 si ottengono i cinque punti di $\mathbb{R}^3$:

$$\{(1,0,0), (0,1,0), (0,0,1), (a,a,a), (b,b,b)\}.$$

Operazioni fra ideali in $K[\mathtt{x}]$

Siano I e J due ideali di $K[\mathtt{x}]$, con $G(I) = \{f_1, \ldots, f_r\}$ e $G(J) = \{g_1, \ldots, g_s\}$.
Si ha che: $I + J = (f_1, \ldots, f_r, g_1, \ldots, g_s)$ e $IJ = (f_i g_j \ : \ i \in [r] \text{ e } j \in [s])$.

Intersezione di Ideali

- Osserviamo che il caso $(f) \cap I$ "contiene" il problema dell'appartenenza ($f \in I$?). Infatti $f \in I$ se e solo se $(f) \cap I = (f)$.
- Dato un polinomio $h \in K[t]$, indichiamo con hI l'ideale in $K[\mathtt{x}, t]$ generato da $\{hf \ : \ f \in I\}$. Conoscendo i generatori di I, si ha che $hI = (hf_1, \ldots, hf_r)$.

☆ Vale l'uguaglianza: $I \cap J = [tI + (1-t)J] \cap K[\mathtt{x}]$.

- Quindi per calcolare $I \cap J$ si può trovare una base di Gröbner di $(tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s)$ per poi eliminare la t.
- L'intersezione di due ideali principali di $K[\mathtt{x}]$ è un ideale principale e $(f) \cap (g) = \mathrm{LCM}(f, g)$.

Esercizio
Dati gli ideali $I = (x^2y + y - 1, xz)$ e $J = (x + yz + 1, z^2)$, calcolare l'intersezione $I \cap J$ utilizzando le basi di Gröbner.

Osservazioni

Algoritmo per il GCD **in** $K[\mathbf{x}]$

- Il **minimo comune multiplo** tra due polinomi f e g di $K[\mathrm{x}]$ si può trovare come il generatore dell'ideale intersezione $(f) \cap (g)$.
- Quindi il **massimo comune divisore** fra i due polinomi è dato da $\mathrm{GCD}(f, g) = \frac{fg}{\mathrm{LCM}(f,g)}$.

Problema del radical membership in $K[\mathbf{x}]$

- Sia I un ideale di $K[\mathrm{x}]$, con $G(I) = \{f_1, \ldots, f_r\}$. Si consideri l'ideale $J = (f_1, \ldots, f_r, 1 - tf)$ in $K[\mathrm{x}, t]$.
- Sia $f \in K[\mathrm{x}]$, allora $f \in \sqrt{I}$ se e solo se $1 \in J$, cioè se e solo se la G-base ridotta di J è $\{1\}$ rispetto ad un qualunque ordinamento.

Problema di consistenza (o compatibilità)

- Sia $F = \{f_1, \ldots, f_r\} \subset K[\mathrm{x}]$ con $K = \overline{K}$. Il sistema $f_i = 0$, per $i \in [r]$, ammette soluzioni se e solo se l'ideale $I = (F)$ è proprio, cioè ha G-base ridotta diversa da $\{1\}$ (Hilbertnullstellensatz).
- Se $K \neq \overline{K}$ vale solo che se I è improprio, il sistema è incompatibile.

Colon fra ideali in $K[\mathbf{x}]$

Proprietà

- Siano $\{I_i\}_{i\in[r]}$ e $\{J_j\}_{j\in[s]}$ due famiglie di ideali di $K[\mathbf{x}]$. Allora:
$$\left(\bigcap_{i=1}^{r} I_i : J\right) = \bigcap_{i=1}^{r} (I_i : J); \qquad \left(I : \sum_{j=1}^{s} J_j\right) = \bigcap_{j=1}^{s} (I : J_j).$$
- Se $J = (g_1) + \cdots + (g_s)$, allora $(I : J) = \bigcap_{j=1}^{s} (I : (g_j))$.
- Se $\{h_1, \ldots, h_q\}$ è un sistema di generatori di $I \cap (g)$, con $g \in K[\mathbf{x}]$, allora $\left\{\frac{h_1}{g}, \ldots, \frac{h_q}{g}\right\}$ è un sistema di generatori di $(I : (g))$.

Algoritmo

Siano I e J ideali di $K[\mathbf{x}]$, con $G(I) = \{f_1, \ldots, f_r\}$ e $G(J) = \{g_1, \ldots, g_s\}$.

- Per ogni indice j calcolare una base di Gröbner G_j per l'ideale $I \cap (g_j)$;
- per ogni indice j dividere ogni elemento di G_j per g_j ottenendo un insieme di generatori di $(I : (g_j))$;
- Infine calcolando le intersezioni $(I : (g_1)) \cap (I : (g_2)) = (I : (g_1, g_2))$, $(I : (g_1, g_2)) \cap (I : (g_3)) = (I : (g_1, g_2, g_3))$, ..., $(I : (g_1, \ldots, g_{s-1})) \cap (I : (g_s)) = (I : J)$ si ottiene il risultato.

Radicale di un ideale in $K[\mathbf{x}]$

Così non funziona!

- Per verificare se un ideale $I = (f_1, \ldots, f_2) \in K[\mathbf{x}]$ è radicale non si può usare il radical membership $f_i \in \sqrt{I}$, per $i \in [r]$.
- Per costruire $\sqrt{I}$, non si può calcolare una base di Gröbner per I e considerare $\sqrt{g}$, per ogni $g \in G$.

Quando funziona?

- Se $I = (f) \subset K[\mathbf{x}]$ è principale e $f = f_1^{e_1} \cdots f_r^{e_r}$ allora $\sqrt{I} = (f_1 \cdots f_r)$.
- Se $I = (f) \subset K[\mathbf{x}]$, con K perfetto, è principale allora $\sqrt{I} = (f_{\text{red}})$, dove $f_{\text{red}} = \frac{f}{\text{GCD}(f, \partial_{x_1} f, \ldots, \partial_{x_n} f)}$.
- Se $I \subset K[\mathbf{x}]$ è un ideale zero-dimensionale, K perfetto, allora $\sqrt{I} = I + (q_{1\,\text{red}}, \ldots, q_{n\,\text{red}})$, con $(q_i) = I \cap K[x_i]$ e $(q_{i\,\text{red}}) = \sqrt{I \cap K[x_i]}$.

  Ricordiamo che un ideale si dice zero-dimensionale se $K[\mathbf{x}]/I$ ha K-dimensione finita, o equivalentemente se $x_i^{m_i} \in \text{LT}(I)$ per ogni $i \in [n]$ e qualche $m_i > 0$, cioè $x_i^{m_i} = \text{LT}(g)$ per un g di una G-base per I.

Sizigie

Definizioni

- Sia $K[\mathtt{x}]^r = K[\mathtt{x}] \oplus \cdots \oplus K[\mathtt{x}]$ il $K[\mathtt{x}]$-modulo libero di dimensione r, con base $\{e_1, \ldots, e_r\}$. Un monomio di $K[\mathtt{x}]^r$ è un elemento del tipo $\mathtt{x}^\alpha e_i$, con $\mathtt{x}^\alpha \in \mathcal{M}_n$ e $i \in [r]$. Quindi un generico elemento $f \in K[\mathtt{x}]^r$ si scrive come $f = f_1 e_1 + \cdots + f_r e_r$, con $f_i \in K[\mathtt{x}]$.
- Sia fissato su $K[\mathtt{x}]$ un ordinamento monomiale $\geq$ e sia $e_1 > \cdots > e_r$. È possibile estendere $\geq$ ad un ordinamento monomiale sul modulo libero $K[\mathtt{x}]^r$ in due modi distinti:

  TOP: $\mathtt{x}^\alpha e_i \geq_{\mathrm{TOP}} \mathtt{x}^\beta e_j$ se e solo se $\mathtt{x}^\alpha \geq \mathtt{x}^\beta$ oppure $\mathtt{x}^\alpha = \mathtt{x}^\beta$ e $i < j$;

  POT: $\mathtt{x}^\alpha e_i \geq_{\mathrm{POT}} \mathtt{x}^\beta e_j$ se e solo se $i < j$ oppure $i = j$ e $\mathtt{x}^\alpha \geq \mathtt{x}^\beta$;
- Si estendono in maniera naturale le definizioni di monomio, termine e coefficiente iniziale per $f \in K[\mathtt{x}]^r$: $\mathrm{LT}(f)$, $\mathrm{LM}(f)$ e $\mathrm{LC}(f)$.
- Dato un sottomodulo $M \in K[\mathtt{x}]^r$, il **modulo iniziale** di M, rispetto ad un ordinamento monomiale fissato, è $\mathrm{LT}(M) = \langle \mathrm{LT}(f) \ : \ f \in M \rangle$.
- Una base di Gröbner del modulo M è un insieme $G = \{g_1, \ldots, g_s\} \subset K[\mathtt{x}]^r$ tale che $\mathrm{LT}(M) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(G) \rangle$.

Definizioni

- Dati due monomi $\mathtt{x}^{\alpha} e_i$, $\mathtt{x}^{\beta} e_j$ di $K[\mathtt{x}]^r$, diciamo che $\mathtt{x}^{\alpha} e_i$ divide $\mathtt{x}^{\beta} e_j$ se e solo se $i = j$ e $\mathtt{x}^{\alpha}$ divide $\mathtt{x}^{\beta}$. Quindi se $i = j$ è possibile definire LCM e GCD dei due monomi.
- È quindi possibile estendere l'algoritmo di divisione in $K[\mathtt{x}]^r$.
- Disporre di una base di Gröbner per il sottomodulo $M \subset K[\mathtt{x}]^r$ significa risolvere il problema dell'appartenenza: $f \in K[\mathtt{x}]^r$, $f \in M$?

☆ Sia $F = \{f_1, \ldots, f_r\}$ una r-upla ordinata di polinomi di $K[\mathtt{x}]$. Si definisce **sizigia** tra i polinomi f_i una r-upla di polinomi $S = (h_1, \ldots, h_r)$ tali che $h_1 f_1 + \cdots + h_r f_r = 0$. È possibile identificare la sizigia $(h_1, \ldots, h_r)$ con l'elemento $\sum_{i=1}^{r} h_i e_i$ del modulo libero $K[\mathtt{x}]^r$.

- L'insieme di tutte le sizigie della r-upla F, indicato con $\mathrm{Syz}(F) = \mathrm{Syz}(f_1, \ldots, f_r)$, è un sottomodulo di $K[\mathtt{x}]^r$.

Modulo delle sizigie

Sia $F = \{f_1, \ldots, f_r\}$ una r-upla ordinata di polinomi di $K[\mathtt{x}]$.

- Il modulo delle sizigie $\mathrm{Syz}(F) \subset K[\mathtt{x}]^r$ è finitamente generato.
- $\mathrm{Syz}(F)$ è il nucleo dell'omomorfismo di $K[\mathtt{x}]$-moduli

  $$\varphi_F : K[\mathtt{x}]^r \to K[\mathtt{x}] \text{ definito da } (a_1, \ldots, a_r) \mapsto a_1 f_1 + \cdots + a_r f_r,$$

  tramite il quale si ottiene la sequenza esatta corta

  $$0 \longrightarrow \mathrm{Syz}(F) \longrightarrow K[\mathtt{x}]^r \xrightarrow{\varphi} (F) \longrightarrow 0.$$

- È possibile definire gli S-vettori (associati agli S-polinomi) a partire da una coppia di polinomi di F, (f_i, f_j):

  $$S_{ij} = \frac{\mathtt{x}^\gamma}{\mathrm{LT}(f_i)} e_i - \frac{\mathtt{x}^\gamma}{\mathrm{LT}(f_j)} e_j,$$

  dove $\mathtt{x}^\gamma = \mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$. S_{ij} è una sizigia fra $\mathrm{LT}(f_i)$ e $\mathrm{LT}(f_j)$.

Variazioni Buchberger (da capo)

Sia $F = \{f_1, \ldots, f_r\}$ una r-upla ordinata di polinomi di $K[\mathtt{x}]$. Indichiamo con $\mathrm{S}(F) = \mathrm{Syz}(\mathrm{LT}(F))$ il modulo delle sizigie dei monomi iniziali di F.

- Gli S-vettori S_{ij} tra i polinomi di F generano il modulo delle sizigie di $\mathrm{LT}(F)$, cioè $\mathrm{S}(F) = \langle S_{ij} \ : \ i < j \rangle$.
- Ogni elemento $(h_1, \ldots, h_r) \in \mathrm{S}(F)$ si scrive in maniera unica come somma di elementi "omogenei" (cioè con $\mathrm{mDeg}(h_i) + \mathrm{mDeg}(f_i) = \alpha$ per $i \in [r]$). Sia $\mathcal{S}$ un insieme di generatori omogenei.
- Esiste un criterio per ottenere un insieme minimale di generatori di $\mathrm{S}(F)$ a partire da $\mathcal{S}$. Siano $f_i, f_j, f_k \in F$ tali che $\mathrm{LT}(f_k)$ divida $\mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$; se $S_{ik}, S_{jk} \in \mathcal{S}$ allora $\mathcal{S} \setminus \{S_{ij}\}$ genera $\mathrm{S}(F)$.

☆ Sia I l'ideale generato da $G = \{g_1, \ldots, g_s\}$. G è una base di Gröbner per I se e solo se per ogni elemento $S = (h_1, \ldots, h_s)$ della base omogenea $\mathcal{S}$ risulta $S \cdot G = \sum_{i=1}^{s} h_i g_i \xrightarrow{G} 0$.

- Tale criterio migliora l'efficienza dell'algoritmo di Buchberger per il calcolo della base di Gröbner di un ideale I di $K[\mathtt{x}]$.

Ulteriori risultati

Le seguenti proposizioni sono equivalenti:
Sia I un ideale non nullo di $K[\mathrm{x}]$.

- $G = \{g_1, \ldots, g_s\}$ è una base di Gröbner per I;
- $\mathrm{S}(G) = \langle \mathrm{LT}(G) \rangle$;
- $\mathrm{S}(G) = \mathrm{LT}(\mathrm{Syz}(G))$;
- Ogni elemento in $\mathrm{S}(G)$ si "solleva" ad un elemento di $\mathrm{Syz}(G)$;

Teorema di Schreyer
Sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner per l'ideale I di $K[\mathrm{x}]$.

- Per Buchberger si ha che $S(g_i, g_j) \bmod G = 0$, per $i < j$. Dividendo si ha quindi $S(g_i, g_j) = \sum_{k=1}^{s} a_{ijk} g_k$, con $a_{ijk} \in K[\mathrm{x}]$ e $\mathrm{LT}(a_{ijk} g_k) \leq \mathrm{LT}(S(g_i, g_j))$ per ogni k. Si definiscono, con x^γ non nullo:

$$s_{ij} = \frac{\mathrm{x}^\gamma}{\mathrm{LT}(g_i)} e_i - \frac{\mathrm{x}^\gamma}{\mathrm{LT}(g_j)} e_j - a_{ij1} e_1 - \cdots - a_{ijs} e_s.$$

- L'insieme $\{s_{ij} \ : \ 1 \leq i, j \leq s\}$ genera $\mathrm{Syz}(G)$ come $K[\mathrm{x}]$-modulo. Sono una G-base rispetto all'ordinamento $\mathrm{x}^\alpha e_i \geq \mathrm{x}^\beta e_j$ se e solo se $\mathrm{LT}(\mathrm{x}^\alpha g_i) \geq \mathrm{LT}(\mathrm{x}^\beta g_j)$ oppure $\mathrm{LT}(\mathrm{x}^\alpha g_i) = \mathrm{LT}(\mathrm{x}^\beta g_j)$ e $i < j$.

Risoluzioni libere

Sia M un $K[\mathtt{x}]$-modulo finitamente generato: $M = \langle m_1, \ldots, m_r \rangle$.

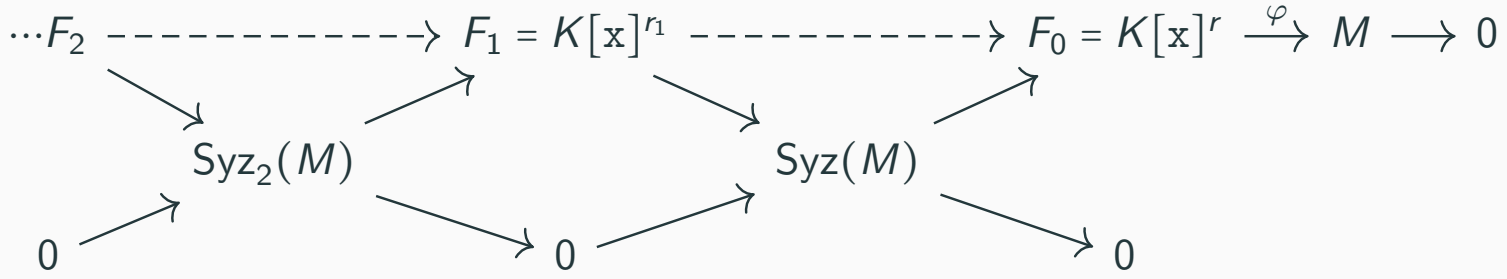
- Esiste un omomorfismo suriettivo di $K[\mathtt{x}]$-moduli

$$\varphi : K[\mathtt{x}]^r \to M \text{ tale che } e_1 \mapsto m_i, \text{ per } i \in [r].$$

- Il nucleo di φ è il modulo delle (prime) sizigie di M: $\mathrm{Syz}(M) = \mathrm{Syz}(m_1, \ldots, m_r) = \ker \varphi$. Osserviamo che $\ker \varphi = \langle 0 \rangle$ se e solo se M è un modulo libero.
- Se $M_1 = \mathrm{Syz}(M) \neq \langle 0 \rangle$, allora è finitamente generato per la noetherianità di $K[\mathtt{x}]^r$ e quindi esiste un omomorfismo suriettivo di $K[\mathtt{x}]$-moduli $\varphi_1 : K[\mathtt{x}]^{r_1} \to M_1$ costruito analogamente al caso precedente.
- Il nucleo di φ_1 è il modulo delle seconde sizigie di M: $\mathrm{Syz}_2(M) = \ker \varphi_1$. Se tale nucleo non è nullo, il processo può continuare.
- Si costruisce così una successione di moduli. È inoltre possibile considerare, eventualmente, i moduli liberi che contengono i moduli delle sizigie calcolati.

Risoluzioni libere

- Si ottiene così una successione esatta detta **risoluzione libera** di M:



- La lunghezza di una risoluzione libera finita di un modulo M è p se:

$$0 \longrightarrow F_p \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

Teorema delle sizigie di Hilbert
Ogni $K[x_1, \ldots, x_n]$-modulo finitamente generato possiede una risoluzione libera finita di lunghezza al più n.

Esempio

Dato l'ideale $I = (x^3, xy, y^5)$ di $S = K[x, y]$, costruire una risoluzione libera di S/I.

- Si pone $F_0 = S$. Osserviamo che x^3, xy e y^5 sono generatori, rispettivamente di grado 3, 2 e 5, del nucleo di $S \to S/I$. Quindi $Syz(S/I) \subset F_1 = S^3 = S(-3) \oplus S(-2) \oplus S(-5)$, ottenendo:

$$\cdots F_1 = S^3 \longrightarrow F_0 = S \xrightarrow{\pi} S/I \longrightarrow 0$$

- Ripetendo il procedimento e calcolando le sizigie di $\mathrm{Syz}(S/I)$ si ottiene il modulo $\mathrm{Syz}_2(S/I) \subset F_2 = S^2 = S(-4) \oplus S(-6)$ e quindi

$$\cdots F_2 = S^2 \longrightarrow F_1 = S^3 \longrightarrow F_0 = S \xrightarrow{\pi} S/I \longrightarrow 0$$

- Infine, calcolando il modulo delle sizigie di $\mathrm{Syz}_2(S/I)$ si ottiene il modulo nullo. Questo pone fine all'algoritmo (d'altronde $n = 2$) e si ottiene la risoluzione libera:

$$0 \longrightarrow F_2 = S^2 \longrightarrow F_1 = S^3 \longrightarrow F_0 = S \xrightarrow{\pi} S/I \longrightarrow 0$$

Codice

Bibliografia

Bibliografia i

[1] W. Adams and P. Loustaunau.
An Introduction to Gröbner Bases, volume 3.
American Mathematical Society, USA, 1994.

[2] D. A. Cox, J. Little, and D. Oshea.
Ideals, Varieties, and Algorithms.
Undergraduate Texts in Mathematics. Springer, 4 edition, 2015.

[3] J. H. Davenport, Y. Siret, and E. Tournier.
Computer Algebra: Systems and Algorithms for Algebraic Computation (2th ed.).
Academic Press Ltd., GBR, 1993.

[4] R. Fröberg.
An introduction to Gröbner bases.
In *Pure and applied mathematics*. John Wiley & Sons Inc, 1997.

Bibliografia ii

[5] J. Grabmeier, E. Kaltofen, and V. Weispfenning, editors.
Computer Algebra Handbook.
Springer-Verlag, Berlin, Heidelberg, 2003.

[6] D. R. Grayson and M. E. Stillman.
Macaulay2, a software system for research in algebraic geometry.
Available at `http://www.math.uiuc.edu/Macaulay2/`, 2020.

[7] M. Kreuzer and L. Robbiano.
Computational Commutative Algebra 1.
Springer-Verlag, 2000.

[8] J. von zur Gathen and J. Gerhard.
Modern Computer Algebra.
Cambridge University Press, 3 edition, 2013.

Algoritmo di divisione fra polinomi in un dominio euclideo $K[x]$

Algorithm 1: Divisione fra polinomi

Input: Polinomi a, b
Output: Polinomi q, r
begin
    $q \leftarrow 0$;
    $r \leftarrow a$;
    while $r \neq 0$ *and* $\deg(\mathrm{LT}(b)) \leq \deg(\mathrm{LT}(r))$ **do**
        $q \leftarrow q + \mathrm{LT}(r)/\mathrm{LT}(b)$;
        $r \leftarrow r - \mathrm{LT}(r)/\mathrm{LT}(b) * b$;
    end
    return $\{q, r\}$;
end

Indietro

```
i1 :  matLex := n -> (
      id_(ZZ^n)
      )
o1 =  -*Function[stdio:256:13-257:8]*-
o1 :  FunctionClosure
i2 :  matGLex := n -> (
      A=matLex n;
      matrix {toList(n:1)} || A^{0..n-2}
      )
o2 =  -*Function[stdio:259:14-261:31]*-
o2 :  FunctionClosure
i3 :  matGRevLex := n -> (
      A=matLex n;
      B=A^{0..n-2};
      C=B_{n-1};
      for i from 1 to n-1 do C=C | (-1)*B_{n-1-i};
      matrix {toList(n:1)} || C
      )
o3 =  -*Function[stdio:1:17-9:25]*-
o3 :  FunctionClosure
```

Indietro

```
i1 :  ordina = method(TypicalValue=>List)
o1 =  -*Function*-
o1 :  MethodFunction
i2 :  ordina(RingElement,RingElement,Matrix) := (m1,m2,A) -> (
      e1:=transpose matrix exponents m1;
      e2:=transpose matrix exponents m2;
      if flatten entries (A*e1) > flatten entries (A*e2) then {m1,m2}
         else {m2,m1}
      )
o2 =  -*Function[stdio:329:53-333:74]*-
o2 :  FunctionClosure
i3 :  ordina(List,Matrix) := (L,A) -> (
      for i to #L-2 do (
          for j to #L-2-i do (
             l=take(L,0,j-1)|ordina(L_j,L_(j+1),A)|take(L,j+2,#L-1);
          );
      );
      L
      )
o3 =  -*Function[stdio:336:30-346:1]*-
o3 :  FunctionClosure
```

```
i1 :  n=5;
i2 :  S=QQ[x_1..x_n];
i3 :  A=matLex 5;
i4 :  f=x_2*x_3+x_1*x_4+x_2*x_5+x_3*x_4^2
o4 =   x_3x_4^2+x_2x_3+x_1x_4+x_2x_5
o4 :  S
i5 :  g=x_1*x_4+x_3^3*x_4+x_2*x_4-x_2*x_5^3+x_4^5
o5 =   x_4^5+x_3^3x_4-x_2x_5^3+x_1x_4+x_2x_4
o5 :  S
i6 :  l=flatten entries monomials f
o6 =  {x_3x_4^2, x_2x_3, x_1x_4, x_2x_5}
o6 :  List
i7 :  m=flatten entries monomials g
o7 =  {x_4^5, x_3^3x_4, x_2x_5^3, x_1x_4, x_2x_4}
o7 :  List
i8 :  ordina(l,A)
o8 =  {x_1x_4, x_2x_3, x_2x_5, x_3x_4^2}
o8 :  List
i9 :  ordina(m,A)
o9 =  {x_1x_4, x_2x_4, x_2x_5^3, x_3^3x_4, x_4^5}
o9 :  List
```

```
i1 :  ordina = method(TypicalValue=>List, Options=>{Peso=>{}});
i2 :  ordina(RingElement,RingElement,Matrix) := opts -> (m1,m2,A) -> (
      e1:=transpose matrix exponents m1;
      e2:=transpose matrix exponents m2;
      p:=opts.Peso;
      if p!= then (
           p=p | toList(n-#p:0);
           A=matrix p || A^{0..n-1};
           k:=min numgens source A, numgens target A;
           if rank A < k then error "singular ordering matrix";
      );
      if flatten entries (A*e1) > flatten entries (A*e2) then {m1,m2}
         else {m2,m1}
      );
i3 :  ordina(List,Matrix) := opts -> (L,A) -> (
      for i to #L-2 do (
          for j to #L-2-i do (
             l=take(L,0,j-1)|ordina(L_j,L_(j+1),A,Peso=>opts.Peso)|take(L,j+2,#L-1);
          );
      );
      L
      );
```

```
i1 :  n=5;
i2 :  S=QQ[x_1..x_n,MonomialOrder=>{Weights=>{1,1}}];
i3 :  A=matGRevLex 5;
i4 :  f=x_2*x_3+x_1*x_4+x_2*x_5+x_3*x_4^2;
i5 :  g=x_1*x_4+x_3^3*x_4+x_2*x_4-x_2*x_5^3+x_4^5;
i6 :  l=flatten entries monomials f
o6 =  {x_2x_3, x_1x_4, x_2x_5, x_3x_4^2}
o6 :  List
i7 :  m=flatten entries monomials g
o7 =  { x_2x_5^3, x_1x_4, x_2x_4, x_4^5, x_3^3x_4}
o7 :  List
i8 :  p={1,1};
i9 :  ordina(l,A,Peso=>p)
o9 =  {x_2x_3, x_1x_4, x_2x_5, x_3x_4^2}
o9 :  List
i10 :  ordina(m,A,Peso=>p)
o10 =  { x_2x_5^3, x_1x_4, x_2x_4, x_4^5, x_3^3x_4}
o10 :  List
```

Indietro

Algoritmo di divisione in $K[\mathtt{x}]$

Algorithm 2: Divisione in $K[\mathtt{x}]$

Input: Polinomi $f, f_1, f_2, \ldots, f_s$
Output: Polinomi $q_1, q_2, \ldots, q_s, r$
begin
  $r \leftarrow 0$; $q_i \leftarrow 0$, per $1 \leq i \leq s$;
  while $f \neq 0$ **do**
    $flag \leftarrow$ `false`; $i \leftarrow 1$;
    while $i \leq s$ `and` $!flag$ **do**
      if $\mathrm{LT}(f_i)$ `divide` $\mathrm{LT}(f)$ **then**
        $q_i \leftarrow q_i + \mathrm{LT}(f)/\mathrm{LT}(f_i)$;
        $f \leftarrow f - f_i * \mathrm{LT}(f)/\mathrm{LT}(f_i)$;
        $flag \leftarrow$ `true`;
      end
      $i \leftarrow i + 1$;
    end
    if $!flag$ **then**
      $r \leftarrow r + \mathrm{LT}(f)$;
      $f \leftarrow f - \mathrm{LT}(f)$;
    end
  end
  return $\{q_1, q_2, \ldots, q_s, r\}$;
end

Indietro

Macaulay2 RESET INTERRUPT UPLOAD FILE

```
i1 :  S=QQ[x..z];
i2 :  f_1=x*y^2-x*z+y
o2 =  xy^2-xz+y
o2 :  S
i3 :  f_2=x*y-z^2
o3 =  xy-z^2
o3 :  S
i4 :  f_3=x-y*z^4
o4 =  -yz^4+x
o4 :  S
i5 :  LTg=ideal((1..3)/(i->leadTerm f_i))
o5 =  ideal(xy^2, xy, -yz^4)
o5 :  Ideal of S
i6 :  f_4=f_1-y*f_2
o6 =  yz^2-xz+y
o6 :  S
i7 :  (leadTerm f_4) % LTg
o7 =  yz^2
o7 :  S
i8 :  leadTerm ideal(f_1,f_2,f_3)
o8 =  (xy yz^2 x^2z y^3 x^3 z^4 xz^3)
o8 :  Matrix S^1 <-- S^7
```

```
i9 :  S=QQ[x..z,MonomialOrder=>Lex];
i10 :  f_1=x*y^2-x*z+y;
i11 :  f_2=x*y-z^2;
i12 :  f_3=x-y*z^4;
i13 :  LTg=ideal((1..3)/(i->leadTerm f_i))
o13 =  ideal(xy^2, xy, x)
o13 :  Ideal of S
i14 :  f_4=f_1-y*f_2
o14 =  -xz+yz^2+y
o14 :  S
i15 :  (leadTerm f_4) % LTg
o15 =  0
o15 :  S
i16 :  f_5=f_4+z*f_3
o16 =  -yz^5+yz^2+y
o16 :  S
i17 :  (leadTerm f_5) % LTg
o17 =  -yz^5
o17 :  S
i18 :  leadTerm ideal(f_1,f_2,f_3)
o18 =  (x^7 yz^5 y^2 x)
o18 :  Matrix S^1 <-- S^4
```

Indietro

Algoritmo di Buchberger

Algorithm 3: Algoritmo di Buchberger (non ottimizzato)

Input: Base $F = \{f_1, \ldots, f_r\}$
Output: Base di Gröbner $\{g_1, \ldots, g_s\}$
begin
  repeat
    $G \leftarrow F$;
    foreach $\{p, q\} \subset G,\ p \neq q$ **do**
      $rem \leftarrow S(p, q) \bmod G$;
      if $rem \neq 0$ **then**
        $F \leftarrow F \cup \{rem\}$;
      end
    end
  until $F = G$;
  return G;
end

Indietro

```
i1 :  interseca := (I,J) -> (
      S:=ring I; n=numgens S;
      R:=newRing(S,Variables=>n+1,MonomialOrder=>{Weights=>toList(n:0)|{1}});
      use R;
      R2S:=map(S,R,vars S|matrix{{0}}); S2R:=map(R,S,(vars R)_{0..n-1});
      K:=R_n* S2R I+(1-R_n)* S2R J; gK:=flatten entries gens gb K;
      int=ideal select(gK,i->(product flatten entries monomials(i) % R_n)!=0);
      R2S int
      )
i2 :  colon := (I,J) -> (
      gJ:=flatten entries mingens J; L:={};
      for g in gJ do (
          G:=gens gb intersect(I,ideal g);
          L=L | entries (G // g);
      );
      intersect(L/ideal)
      )
i3 :  radicale := I -> (
      ind=gens ring I; L:={};
      for i in ind do (
          g:=flatten entries mingens eliminate (delete(i,ind),I);
          L=L | g_0//diff(i,g_0);
      );
      I+ ideal L
      )
```

Indietro

Algoritmo di Buchberger

Algorithm 4: Algoritmo di Buchberger (alquanto ottimizzato)

Input: Base $F = \{f_1, \ldots, f_r\}$
Output: Base di Gröbner $\{g_1, \ldots, g_s\}$
begin
  $S \leftarrow \{(i,j) \ : \ 1 \leq i < j \leq r\}$;
  $G \leftarrow F$;
  while $S \neq \varnothing$ **do**
    $(i,j) \leftarrow$ first S;
    $var1 \leftarrow \mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) \neq \mathrm{LT}(f_i)\mathrm{LT}(f_j)$;
    $var2 \leftarrow \forall k \neq \{i,j\} \ : \ \mathrm{LT}(f_k) \nmid \mathrm{LCM}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$;
    $var2 \leftarrow var2$ or $\forall k \neq \{i,j\} \ : \ (i,k), (j,k) \notin S$;
    if *var*1 *and* *var*2 **then**
      $rem \leftarrow S(f_i, f_j) \bmod G$;
      if $rem \neq 0$ **then**
        $r = r + 1$; $f_r \leftarrow rem$;
        $G = G \cup \{f_r\}$;
        $S \leftarrow S \cup \{(i,r) \ : \ 1 \leq i \leq r-1\}$;
      end
    end
    $S \leftarrow S \setminus \{(i,j)\}$;
  end
  return G;
end

Indietro

Macaulay2 RESET INTERRUPT UPLOAD FILE

```
i1 :  ris := I -> (
      S:=ring I;
      F:={S^1};
      Syz:={gens I};
      i:=0;
      while Syz_i!=0 do (
           i=i+1;
           GB:=gb(Syz_(i-1),Syzygies=>true);
           Syz=Syz | {syz GB};
           F=F | {target Syz_i};
      );
      for j to i list {F_j,flatten degrees target Syz_j,Syz_j}
      )
i2 :  S=QQ[x,y];
i3 :  I=ideal(x^3, x*y, y^5);
i4 :  ris I
```

$$o4 = \left\{\left\{S^1, \{0\}, \begin{pmatrix} x^3 & xy & y^5 \end{pmatrix}\right\}, \left\{S^3, \{3, 2, 5\}, \begin{matrix}\{3\}\\\{2\}\\\{5\}\end{matrix} \begin{pmatrix} y & 0 \\ -x^2 & -y^4 \\ 0 & x \end{pmatrix}\right\}, \left\{S^2, \{4, 6\}, 0\right\}\right\}$$

```
o4 :  List
i5 :  res I
```

$$o5 = S^1 \xleftarrow{\begin{pmatrix} x & y & x^3 & y^5 \end{pmatrix}} S^3 \xleftarrow{\begin{pmatrix} -x^2 & -y^4 \\ y & 0 \\ 0 & x \end{pmatrix}} S^2 \xleftarrow{0} 0$$

$$\begin{matrix} 0 & & 1 & & 2 & & 3 \end{matrix}$$

```
o5 :  ChainComplex
```

Indietro