Algebra Computazionale

Alessio Borzì

Indice

Basi di Gröbner

1.1 Introduzione

Siano k un campo, $x_1, x_2, \dots, x_n$ n indeterminate su k. Indichiamo con

$$T^n = \{x_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} : \beta_i \in \mathbb{N}, i = 1, \dots, n\}$$

l'insieme dei **monomi** di $k[x_1, \dots, x_n]$.

Definizione 1.1.1. *Dato $F \subseteq k[x_1, \dots, x_n]$ poniamo*

$$V(F) = \{P \in k^n : f(P) = 0 \quad \forall f \in F\} \subseteq k^n.$$

*L'insieme $V(F)$ è detto **varietà algebrica affine**.*

Osserviamo che se $I = \langle F \rangle = \{\sum_{i=1}^n a_i f_i : a_i \in k[x_1, \dots, x_n], f_i \in F\}$ è l'ideale generato da F allora

$$V(F) = V(I).$$

Dato che $k[x_1, \dots, x_n]$ è noetheriano allora ogni suo ideale è finitamente generato. Pertanto ogni varietà algebrica affine è l'insieme dei punti di k^n che soddisfano un numero finito di equazioni polinomiali

$$f_i(x_1, \dots, x_n) = 0 \quad (i = 1, \dots, m).$$

Proposizione 1.1.2.

1. $I \subseteq \mathscr{I}(V(I))$
2. $I \subseteq J \Rightarrow V(I) \supseteq V(J)$
3. $V(\mathscr{I}(V(I))) = V(I)$
4. $V(1) = \emptyset$, $V(0) = \mathbb{A}^n(k)$.
5. $V\left(\sum_{\lambda\in\Lambda} I_\lambda\right) = \bigcap_{\lambda\in\Lambda} V(I_\lambda)$
6. $V(IJ) = V(I \cap J) = V(I) \cup V(J)$

1. $X \subseteq V(\mathscr{I}(X))$
2. $X \subseteq Y \Rightarrow \mathscr{I}(X) \supseteq \mathscr{I}(Y)$
3. $\mathscr{I}(V(\mathscr{I}(X))) = \mathscr{I}(X)$
4. $\mathscr{I}(\mathbb{A}^n(k)) = (0), \mathscr{I}(\emptyset) = k[\,\underline{x}\,]$
5. $\mathscr{I}(\bigcup_{\lambda\in\Lambda} X_\lambda) = \bigcap_{\lambda\in\Lambda} \mathscr{I}(X_\lambda)$
6. $\mathscr{I}(X \cap Y) \supseteq \mathscr{I}(X) + \mathscr{I}(Y)$

A ogni polinomio $f \in k[x_1, \dots, x_n]$ possiamo associare la sua funzione polinomiale corrispondente (detta anche **funzione di valutazione**) $f : k^n \to k$ definita con la legge $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$. Questa associazione è iniettiva solamente nel caso k infinito.

Infatti se k è un campo finito in generale possono esserci polinomi che originano la stessa funzione polinomiale (ad esempio $k = \mathbb{Z}_2$ in cui $f(x) = x(x+1)$ dà luogo alla funzione nulla).

Osserviamo che un ideale $I \trianglelefteq k[x_1, \ldots, x_n]$ può avere insiemi di generatori di cardinalità diversa. Ad esempio

$$(x, y) = (x, x + y) = (x + xy, x^2, y^2, y + xy).$$

Definizione 1.1.3. *Dati $f, g \in k[x_1, \ldots, x_n]$, il* ***massimo comune divisore*** *di f e g è il polinomio $\mathrm{MCD}(f, g) = d$ tale che*

1. *$d|f$, $d|g$*
2. *Se $h|f$ e $h|g$ allora $h|d$*
3. *$lc(d) = 1$*

Analogamente si definisce ***minimo comune multiplo*** *di f e g il polinomio $\mathrm{mcm}(f, g) = l$ tale che*

1. *$f|l$, $g|l$*
2. *Se $f|h$ e $g|h$ allora $l|h$*
3. *$lc(l) = 1$*

L'esistenza del massimo comune divisore e del minimo comune multiplo è garantita dal fatto che $k[x_1, \ldots, x_n]$ è un UFD. Inoltre risulta $fg = \mathrm{MCD}(f, g) \cdot \mathrm{mcm}(f, g)$.

1.2 Ordinamenti monomiali

Adottiamo la seguente notazione per i monomi

$$x_1^{\beta_1} x_2^{\beta_2} \ldots x_n^{\beta_n} = x^\beta \quad \text{dove } \beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n.$$

Definizione 1.2.1. *Per* ***ordinamento monomiale*** *$<$ su T^n intendiamo un ordinamento totale su T^n tale che*

1. *$1 < x^\beta$ per ogni $x^\beta \in T^n \setminus \{1\}$.*
2. *$x^\alpha < x^\beta \Rightarrow x^\alpha x^\gamma < x^\beta x^\gamma$ per ogni $x^\gamma \in T^n$.*

Vediamo tre esempi di ordinamenti monomiali.

1. L'**ordinamento lessicografico** $<_{lex}$ con $x_1 > x_2 > \ldots > x_n$, dove, dati $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$,

$$x^\alpha < x^\beta \Leftrightarrow \alpha_1 = \beta_1, \ldots, \alpha_{k-1} = \beta_{k-1}, \alpha_k < \beta_k \text{ per qualche } k = 1 \ldots n.$$

2. L'**ordinamento lessicografico graduato** $<_{deglex}$ con $x_1 > x_2 > \ldots > x_n$, dove, dati $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$,

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{oppure} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i, \; x^\alpha <_{lex} x^\beta. \end{cases}$$

3. L'**ordinamento lessicografico graduato inverso** $<_{degrevlex}$ con $x_1 > x_2 > \ldots > x_n$, dove, dati $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$,

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{oppure} \\ \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i, \; \alpha_n = \beta_n, \ldots, \alpha_{k+1} = \beta_{k+1}, \alpha_k > \beta_k \text{ per qualche } k = 1 \ldots n. \end{cases}$$

Proposizione 1.2.2. *Se $x^\alpha | x^\beta$ allora $x^\alpha \leq x^\beta$, dove $\leq$ è un qualsiasi ordinamento monomiale su T^n.*

Dimostrazione. Per ipotesi esiste $x^\gamma \in T^n$ tale che $x^\beta = x^\gamma x^\alpha$. Adesso

$$x^\gamma \geq 1 \Rightarrow x^\gamma x^\alpha \geq x^\alpha \Rightarrow x^\beta \geq x^\alpha.$$ □

Teorema 1.2.3. *Ogni ordinamento monomiale è un buon ordinamento.*

Dimostrazione. Supponiamo per assurdo che esista una catena discendente

$$x^{\alpha_1} > x^{\alpha_2} > x^{\alpha_3} > \ldots$$

Proviamo che la seguente catena ascendente di ideali di $k[x_1, \ldots, x_n]$

$$(x^{\alpha_1}) \subseteq (x^{\alpha_1}, x^{\alpha_2}) \subseteq \ldots$$

non può essere stazionaria, contraddicendo il teorema della base di Hilbert.
Infatti se fosse $x^{\alpha_{i+1}} \in (x^{\alpha_1}, \ldots, x^{\alpha_i})$ allora

$$x^{\alpha_i} = \sum_{j=1}^{i} u_j x^{\alpha_j}.$$

Adesso dato che $x^{\alpha_{i+1}}$ è un monomio allora la somma del secondo membro deve dare luogo a un monomio, ne segue che $x^{\alpha_{i+1}}$ deve essere divisibile per uno degli $u_j x^{\alpha_j}$. Dalla proposizione precedente segue che $x^{\alpha_j} \leq x^{\alpha_{i+1}}$, assurdo. Ciò conclude la dimostrazione. □

Definizione 1.2.4. *Sia $<$ un ordinamento monomiale, $f = c_1 x^{\alpha_1} + \ldots + c_k x^{\alpha_k} \in k[x_1, \ldots, x_n]$ con $\alpha_i \in \mathbb{N}^n$ e $c_i \in k$ e supponiamo che $x^{\alpha_j} \leq x^{\alpha_1} \, \forall j \in \{1, \ldots, n\}$. Diamo le seguenti definizioni:*

$$\begin{array}{ll} lm(f) = x^{\alpha_1} & \textbf{\textit{leading monomial}} \\ lc(f) = c_1 & \textbf{\textit{leading coefficient}} \\ lt(f) = c_1 x^{\alpha_1} & \textbf{\textit{leading term}} \end{array}$$

Dalla definizione segue subito che se $f, g \in k[x_1, x_2, \ldots, x_n]$ allora

$$\begin{array}{rcl} lm(f \cdot g) & = & lm(f) \cdot lm(g) \\ lc(f \cdot g) & = & lc(f) \cdot lc(g) \\ lt(f \cdot g) & = & lt(f) \cdot lt(g) \end{array}$$

1.3 Algoritmo di divisione in $k[x_1, \ldots, x_n]$

Fissiamo un ordinamento monomiale $<$.

Definizione 1.3.1. *Siano $f, g \in k[x_1, \ldots, x_n]$ con $g \neq \underline{0}$. Diciamo che f si* ***riduce*** *a h modulo g e scriveremo $f \xrightarrow{g} h$ se $lt(g)$ divide un termine non nullo X di f e $h = f - \frac{X}{lt(g)} g$.*

Definizione 1.3.2. *Siano $f, h, f_1, \ldots, f_k \in k[x_1, \ldots, x_n]$ con $f_i \neq \underline{0}$ per $i = 1, \ldots, k$ e sia $F = \{f_1, \ldots, f_k\}$. Diciamo che f si* ***riduce*** *a h modulo F e scriviamo $f \xrightarrow{F}_+ h$ se esiste una sequenza di indici $i_1, i_2, \ldots, i_t \in \{1, \ldots, k\}$ e polinomi $h_1, \ldots, h_{t-1} \in k[x_1, \ldots, x_n]$ tali che*

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \ldots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Definizione 1.3.3. *Un polinomi f è detto* ***ridotto*** *rispetto a un insieme di polinomi non nulli $F = \{f_1, \ldots, f_k\}$ se $f = \underline{0}$ oppure nessun termine di f è divisibile per alcun leading term di un polinomio in F. In altri termini se non si riduce modulo F.*
Se $f \xrightarrow{F}_+ r$ e r è ridotto rispetto a F allora r è un ***resto*** *di f rispetto a F.*

Fissato un ordinamento monomiale $<$ e dati $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ con $f_i \neq 0$ descriviamo un algoritmo (detto **algoritmo di divisione**) tramite il quale otteniamo dei polinomio quozienti $u_1, \ldots, u_s \in k[x_1, \ldots, x_n]$ e un polinomio resto $r \in k[x_1, \ldots, x_s]$ ridotto rispetto a $F = \{f_1, \ldots, f_s\}$ tali che[1]

$$f = u_1 f_1 + \ldots + u_s f_s + r,$$
$$lm(f) = \max\{lm(u_1 f_1), \ldots, lm(u_s f_s), lm(r)\}.$$

Data: $f \in k[x_1, \ldots, x_n]$, $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n] \setminus \{\underline{0}\}$
Result: $r, u_1, \ldots, u_s \in k[x_1, \ldots, x_n]$ tali che r è ridotto rispetto a F e
$f = u_1 f_1 + \ldots + u_s f_s + r$
Initialization: $u_1 := 0, \ldots, u_s := 0$, $r := 0$, $h := f$
while $h \neq 0$ **do**
  Scegli un termine X di h;
  if *esiste i tale che $lt(f_i)$ divide X* **then**
    $u_i := u_i + \frac{X}{lt(f_i)}$;
    $h := h - \frac{X}{lt(f_i)} f_i$;
  else
    $r := r + X$;
    $h := h - X$;
  end
end

Osserviamo che il precedente algoritmo di divisione non è deterministico. In particolare l'output non è unico. Per rendere l'algoritmo deterministico possiamo decidere di scegliere $X = lt(h)$ e i ogni volta il minimo possibile.

Proviamo adesso che l'algoritmo di divisione descritto si ferma.

[1] La seconda condizione ci dice che non ci sono cancellazioni tra i leading terms dei polinomi elencati.

Lemma 1.3.4. *Sia T un albero con la proprietà che ogni vertice V ha solo un numero finito di vertici figli. Supponiamo che T non contiene nessun cammino*[2] *infinito che parte dalla radice. Allora T ha un numero finito di vertici.*

Dimostrazione. Per assurdo supponiamo che T abbia un numero infinito di vertici. Consideriamo la radice V_0. Essa ha un numero finito di vertici figli. Per ipotesi almeno uno di essi, diciamo V_1, deve avere infiniti vertici sotto di lui. Adesso supponiamo di aver costruito V_n, similmente a prima poniamo V_{n+1} uguale a un vertice figlio di V_n con infiniti vertici sotto di lui. In questo modo abbiamo costruito per induzione un cammino infinito che parte dalla radice V_0, assurdo. $\square$

Teorema 1.3.5. *Dati $f \in k[x_1, \dots, x_n]$, $F = \{f_1, \dots, f_s\} \subseteq k[x_1, \dots, x_n] \setminus \{\underline{0}\}$, l'algoritmo di divisione si ferma producendo polinomi quoziente $u_1, \dots, u_s \in k[x_1, \dots, x_n]$ e un polinomio resto $r \in k[x_1, \dots, x_s]$ ridotto rispetto a $F = \{f_1, \dots, f_s\}$ tali che*

$$\begin{gathered} f = u_1 f_1 + \ldots + u_s f_s + r, \\ lm(f) = \max\{lm(u_1 f_1), \dots, lm(u_s f_s), lm(r)\}. \end{gathered}$$

Dimostrazione. Prima di procedere col dimostrare il teorema, osserviamo che se scegliessimo di volta in volta $X = lt(h)$, dopo ogni ciclo while il polinomio h avrà leading term strettamente minore, pertanto, dato che ogni ordinamento monomiale è un buon ordinamento, l'algoritmo termina.
Nel caso generale, supponiamo dapprima che f sia costituito da un solo termine. Sia X_i il valore di X all'i-esima iterazione. Consideriamo il grafo formato dagli indici i, collegando l'indice i all'indice j quando X_j è stato introdotto in h durante il processo che ha utilizzato X_i. Dalla costruzione si ha che ogni indice ha un solo genitore, quindi il grafo che consideriamo è un albero. Osserviamo che se $\{i, j\}$ è un segmento del grafo allora $X_j < X_i$. Essendo $<$ un buon ordinamento ogni cammino che parte dalla radice è finito. La tesi segue dal lemma precedente.
Se f non è un termine allora basta considerare la foresta di alberi formati da ogni singolo termine di f e aggiungere un nodo fittizio che abbia come figli le radici dei vari alberi.
Adesso la prima condizione segue dalla definizione dell'algoritmo. Per dimostrare la seconda condizione, cioè che

$$lm(f) = \max\{lm(u_1 f_1), \dots, lm(u_s f_s), lm(r)\},$$

notiamo innanzitutto che durante l'esecuzione dell'algoritmo $lt(h)$ non auementa mai, infatti nel passo di divisione i termini che aggiungiamo sono minori o uguali (rispetto all'ordinamento monomiale) di

$$lt\left(\frac{X}{lt(f_i)} f_i\right) = lt\left(\frac{X}{lt(f_i)}\right) lt(f_i) = \frac{X}{lt(f_i)} lt(f_i) = X \leq lt(h).$$

Se siamo nel passo del resto rimuoviamo un termine di h, quindi il nuovo leading term è minore o uguale del vecchio. In questo modo $lm(u_i f_i)$ non potrà mai essere più grande di $lt(h)$. $\square$

[2]con cammino intendiamo una successione di vertici in cui ogni vertice è figlio del vertice precedente.

Osservazione 1.3.6. *Dati* $f \in k[x_1, \ldots, x_n]$*,* $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n] \setminus \{\underline{0}\}$*, con l'algoritmo di divisione otteniamo*

$$f = u_1 f_1 + \ldots + u_s f_s + r.$$

Pertanto se $r = 0$ *allora* $f \in \langle f_1, \ldots, f_s \rangle$*. In generale il viceversa non vale.*

1.4 Basi di Gröbner

Definizione 1.4.1. *Sia* I *un ideale di polinomi. Un insieme* $G = \{g_1, \ldots, g_t\}$ *è detto* ***base di Gröbner*** *(o* ***base standard****) per* I *se*

$$\forall f \in I \setminus \{\underline{0}\}, \exists i \in \{1, \ldots, t\} : lm(g_i) | lm(f).$$

In particolare se G è una base di Gröbner per I allora nessun polinomio $f \in I \setminus \{\underline{0}\}$ è ridotto rispetto a G.

Definizione 1.4.2. *Sia* $S \subseteq k[x_1, \ldots, x_n]$*, l'****ideale dei leading terms*** *di* S *è l'ideale*

$$Lt(S) = \langle lt(s) : s \in S \rangle \subseteq k[x_1, \ldots, x_n].$$

Teorema 1.4.3. *Siano* $I \subseteq k[x_1, \ldots, x_n]$ *un ideale e* $G = \{g_1, \ldots, g_t\} \subseteq I$*, sono equivalenti*

1. G *è una base di Gröbner per* I*;*
2. $f \in I \Leftrightarrow f \xrightarrow{G}_+ \underline{0}$*;*
3. $f \in I \Leftrightarrow f = \sum_{i=1}^{t} h_i g_i$ *con* $lm(f) = \max\{lm(h_1 g_1), \ldots, lm(h_t g_t)\}$*;*
4. $Lt(G) = Lt(I)$*.*

Dimostrazione.

(1) $\Rightarrow$ (2) Sia $f \in k[x_1, \ldots, x_n]$, dall'algoritmo di divisione sappiamo che f si riduce a un polinomio $r \in k[x_1, \ldots, x_n]$ ridotto rispetto a G. Se $f \in I$ allora $r \in I$, pertanto, dato che G è una base di Gröbner per I, deve aversi $r = \underline{0}$. Viceversa se $r = \underline{0}$ allora $f \in I$.

(2) $\Rightarrow$ (3) Supponiamo che $f \in I$, dall'algoritmo di divisione f si riduce a $r \in I$ ridotto rispetto a G, quindi, applicando l'ipotesi su r deve aversi $r = \underline{0}$. Adesso la tesi segue dalle ipotesi dell'algoritmo di divisione. Il Viceversa è ovvio.

(3) $\Rightarrow$ (4) $G \subseteq I \Rightarrow Lt(G) \subseteq Lt(I)$. Viceversa se $f \in I$ allora per ipotesi

$$lm(f) = \max\{lm(h_1)lm(g_1), \ldots, lm(h_t)lm(g_t)\} \in Lt(G),$$

pertanto $Lt(I) \subseteq Lt(G)$.

(4) $\Rightarrow$ (1) Sia $f \in I$, allora $lt(f) \in Lt(I) = Lt(G)$ quindi

$$lt(f) = \sum_{i=1}^{t} h_i lt(g_i),$$

pertanto, dato che il primo membro è un termine, $lm(f)$ sarà divisibile per qualche $lm(g_i)$. □

Corollario 1.4.4. *Se $G = \{g_1, \ldots, g_t\}$ è una base di Gröbner per un ideale I allora $I = \langle G \rangle$.*

Dimostrazione. Sia $f \in I$, dal punto 3 del teorema precedente abbiamo che $f \in \langle G \rangle$. L'inclusione inversa è ovvia. □

Lemma 1.4.5 (Lemma di Dickson)**.** *Sia S un insieme di termini non nulli e $I = \langle S \rangle$. Sia $f \in k[x_1, \ldots, x_n]$ allora*

$$f \in I \Leftrightarrow \text{ per ogni termine } X \text{ di } f, \text{ esiste } Y \in S \text{ tale che } Y|X.$$

Inoltre esiste un insieme finito $S_0 \subseteq S$ tale che $I = \langle S_0 \rangle$.

Dimostrazione. Risulta $f \in I$ se e solo se $f = \sum_{i=1}^{k} h_i X_i$ con $h_i \in k[x_1, \ldots, x_n]$ e $X_i \in S$ se e solo se ogni termine X di f è divisibile per qualche termine $Y \in S$.
Adesso, dal teorema della base di Hilbert sappiamo che $I = \langle f_1, \ldots, f_t \rangle$, inoltre

$$f_i = \sum_{j=1}^{k_i} h_{ij} X_{ij} \quad \text{con } h_{ij} \in k[x_1, \ldots, x_n], X_{ij} \in S$$

quindi $I = \langle X_{ij} \rangle$. □

Corollario 1.4.6. *Ogni ideale I di $k[x_1, \ldots, x_n]$ ha una base di Gröbner.*

Dimostrazione. Dal lemma precedente sappiamo che, considerando l'ideale $Lt(I) = \langle lt(f) : f \in I \rangle$, esistono $g_1, \ldots, g_t \in I$ tali che $Lt(I) = \langle lt(g_1), \ldots, lt(g_t) \rangle$, allora posto $G = \{g_1, \ldots, g_t\}$ si ha $Lt(I) = Lt(G)$, quindi G è una base di Gröbner per I. □

Diremo che $G \subseteq k[x_1, \ldots, x_n]$ è una base di Gröbner se lo è per $\langle G \rangle$.

Teorema 1.4.7. *Sia $G = \{g_1, \ldots, g_t\} \subseteq k[x_1, \ldots, x_n] \setminus \{\underline{0}\}$, risulta*

$$G \text{ è base di Gröbner} \iff \begin{array}{l} \text{per ogni } f \in k[x_1, \ldots, x_n] \text{ il resto} \\ \text{della divisione di } f \text{ per } G \text{ è unico.} \end{array}$$

Dimostrazione.

$\Rightarrow$ Supponiamo che f si riduca a due polinomi r_1 e r_2 ridotti rispetto a G. La differenza $r_1 - r_2$ è ridotta rispetto a G, inoltre $r_1 - r_2 = (f - r_1) - (f - r_2) \in \langle G \rangle$, pertanto dal fatto che G è una base di Gröbner deve aversi $r_1 - r_2 = \underline{0} \Rightarrow r_1 = r_2$.

$\Leftarrow$ Proviamo il punto 2 del Teorema 1.4.3. Se $f \xrightarrow{G}_+ \underline{0}$ allora $f \in \langle G \rangle$. Viceversa sia $f \in \langle G \rangle$ e supponiamo che $f \xrightarrow{G}_+ r$ con r ridotto rispetto a G. Proviamo che, dati $X \in T^n$ e $c \in k \setminus \{0\}$, si ha $f - cXg_i \xrightarrow{G}_+ r$. Sia $d \in k$ il coefficiente del termine $Xlt(g_i)$ in f (nel caso in cui f non possieda tale termine porremo $d = 0$). Distinguiamo vari casi.

- Se $d = 0$ allora riduciamo $f - cXg_i$ tramite g_i, da cui $f - cXg_i \xrightarrow{g_i} f \xrightarrow{G}_+ r \Rightarrow f - cXg_i \xrightarrow{G}_+ r$.
- Se $d = c \neq 0$ riduciamo f tramite g_i, da cui $f \xrightarrow{g_i} f - cXg_i \xrightarrow{G}_+ r'$ con r' ridotto, quindi $f \xrightarrow{G}_+ r'$, dall'unicità del resto segue $r' = r$, pertanto $f - cXg_i \xrightarrow{G}_+ r$.
- Se $0 \neq d \neq c$ allora f e $f - cXg_i$ si riducono a $f - dXg_i$ mediante i termini rispettivamente dXg_i e $(d - c)Xg_i$. Risulta

$$\begin{array}{rcccl} f & \xrightarrow{g_i} & f - dXg_i & \xrightarrow{G}_+ & r' \\ f - cXg_i & \xrightarrow{g_i} & f - dXg_i & \xrightarrow{G}_+ & r' \end{array}$$

  con r' ridotto rispetto a G. Pertanto $f \xrightarrow{G}_+ r'$, dall'unicità del resto $r' = r$ e quindi si ha anche $f - cXg_i \xrightarrow{G}_+ r$.

Adesso, dato che $f \in \langle G \rangle$ scriviamo

$$f = \sum_{i=1}^{t} h_i g_i = \sum_v c_v X_v g_{i_v},$$

iterando più volte quanto appena dimostrato risulta $\underline{0} = f - \sum_v c_v X_v g_{i_v} \xrightarrow{G}_+ r$ allora $r = \underline{0}$ $\square$.

Osserviamo che anche se il resto della divisione è unico, i quozienti possono non essere unici (nel caso in cui l'insieme di generatori non è minimale).

1.5 S-polinomio

Definizione 1.5.1. *Siano $f, g \in k[x_1, \ldots, x_n] \setminus \{\underline{0}\}$ e sia $L = mcm(lm(f), lm(g))$, il polinomio*

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

*è detto **S-polinomio** di f e g.*

Lemma 1.5.2. *Siano $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ con $lm(f_i) = X \neq \underline{0}$ per $i = 1, \ldots, s$. Sia $f = \sum_{i=1}^{s} c_i f_i$ con $c_i \in k$. Se $lm(f) < X$ allora f è combinazione lineare a coefficienti in k di $S(f_i, f_j)$ con $1 \leq i \leq j \leq s$.*

Dimostrazione. Poniamo $f_i = a_i X + g_i$, con $a_i \in k$. Per ipotesi $\sum_{i=1}^{s} c_i a_i = 0$, inoltre risulta
$$S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j,$$
pertanto si ha

$$\begin{aligned} f = c_1 f_1 + c_2 f_2 + \ldots c_s f_s &= c_1 a_1 \left(\frac{1}{a_1} f_1 \right) + c_2 a_2 \left(\frac{1}{a_2} f_2 \right) + \ldots + c_s a_s \left(\frac{1}{a_s} f_s \right) = \\ &= c_1 a_1 \left(\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) + (c_1 a_1 + c_2 a_2) \left(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3 \right) + \ldots + \\ &+ (c_1 a_1 + \ldots + c_{s-1} a_{s-1}) \left(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s \right) + (c_1 a_1 + \ldots + c_s a_s) \left(\frac{1}{a_s} f_s \right) = \\ &= b_1 S(f_1, f_2) + b_2 S(f_2, f_3) + \ldots + b_{s-1} S(f_{s-1}, f_s), \end{aligned}$$

con $b_i = c_1 a_1 + \ldots + a_i c_i \in k$ $(b_s = 0)$. □

Teorema 1.5.3 (Buchberger)**.** *Sia* $G = \{g_1, \ldots, g_t\} \subseteq k[x_1, \ldots, x_n] \setminus \{\underline{0}\}$,

$$G \text{ è base di Gröbner} \iff S(g_i, g_j) \xrightarrow{G}_{+} \underline{0} \text{ per ogni } i \neq j.$$

Dimostrazione.

- $\Rightarrow$ Segue da $S(g_i, g_j) \in \langle G \rangle$.
- $\Leftarrow$ Proviamo il punto 3 tel Teorema 1.4.3. Se $f = \sum_{i=1}^{t} h_i g_i$ allora ovviamente $f \in \langle G \rangle$. Viceversa sia $f \in \langle G \rangle$, scriviamo f come combinazione dei g_i
$$f = \sum_{i=1}^{t} h_i g_i$$
in modo che $X = \max\{lm(h_i g_i) : i = 1, \ldots, t\}$ sia minimo ($>$ è un buon ordinamento). Se $X = lm(f)$ la tesi è acquisita. Altrimenti supponiamo per assurdo che $X > lm(f)$. Sia $S = \{i : lm(h_i) lm(g_i) = X\}$, per gli indici $i \in S$ sceriviamo $lt(h_i) = c_i X_i$, dove X_i sono monomi. Scriviamo
$$f = \sum_{i \in S} lt(h_i) g_i + \sum_{i \in S} (h_i - lt(h_i)) g_i + \sum_{i \notin S} h_i g_i. \tag{1.1}$$
Poniamo
$$g = \sum_{i \in S} lt(h_i) g_i = \sum_{i \in S} c_i X_i g_i = \sum_{i \in S} c_i f_i$$
dove $f_i = X_i g_i = lm(h_i) g_i$. Per definizione, per ogni $i \in S$ risulta $lm(f_i) = lm(h_i) lm(g_i) = X$, inoltre $lm(g) \leq lm(f) < X$ (poiché f è somma di g e termini più piccoli di $lt(g)$). Possiamo applicare il lemma precedente a g, pertanto esistono $d_{ij} \in k$ tali che
$$g = \sum_{\substack{i,j \in S \\ i \neq j}} d_{ij} S(f_i, f_j) = \sum_{\substack{i,j \in S \\ i \neq j}} d_{ij} S(X_i g_i, X_j g_j).$$

Poiché $X = lm(X_i g_i) = lm(X_j g_j) = LCD(lm(X_i g_i), lm(X_j g_j))$ allora

$$S(X_i g_i, X_j g_j) = \frac{X}{lt(X_i g_i)} X_i g_i - \frac{X}{lt(X_j g_j)} X_j g_j = \frac{X}{lt(g_i)} g_i - \frac{X}{lt(g_j)} g_j =$$
$$= \frac{X}{X_{ij}} \left(\frac{X_{ij}}{lt(g_i)} g_i - \frac{X_{ij}}{lt(g_j)} g_j \right) = \frac{X}{X_{ij}} S(g_i, g_j),$$

dove $X_{ij} = LCD(lm(g_i), lm(g_j))$. Per ipotesi $S(g_i, g_j) \xrightarrow{G}_+ \underline{0}$, pertanto, in base alla relazione precedente, $S(X_i g_i, X_j g_j) \xrightarrow{G}_+ \underline{0}$. Dall'algoritmo di divisione (che possiamo effettuare con le stesse divisioni della riduzione $S(X_i g_i, X_j g_j) \xrightarrow{G}_+ \underline{0}$) sappiamo che

$$S(X_i g_i, X_j g_j) = \sum_{v=1}^{t} h_{ijv} g_v \quad \text{con} \quad lm(S(X_i g_i, X_j g_j)) = \max\{lm(h_{ijv} g_v)\}. \tag{1.2}$$

Inoltre scriviamo

$$S(X_i g_i, X_j g_j) = \frac{X}{lt(X_i g_i)} X_i g_i - \frac{X}{lt(X_j g_j)} X_j g_j = \frac{1}{lc(X_i g_i)} X_i g_i - \frac{1}{lc(X_j g_j)} X_j g_j,$$

pertanto i termini di $S(X_i g_i, X_j g_j)$ sono minori di X, da cui $lm(S(X_i g_i, X_j g_j)) < X$. Da ciò, scrivendo g come combinazione degli $S(X_i g_i, X_j g_j)$ e sostituendo come in 1.2, seguirebbe che possiamo trovare una scrittura del tipo 1.1 che contraddice la minimalità di X, assurdo. $\square$.

Il precedente teorema suggerisce un algoritmo (detto **algoritmo di Buchberger**) per ottenere una base di Gröbner di un ideale I da una base data.

Data: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n] \setminus \{\underline{0}\}$
Result: $G = \{f_1, \ldots, f_k\}$ base di Gröbner per $I = \langle F \rangle$ $(k \geq s)$
Initialization: $G := \{f_1, f_2, \ldots, f_s\}$, $t := s$
while $S(f_i, f_j) \xrightarrow{G}_+ h \neq \underline{0}$ *per qualche* $i, j \leq t$ **do**
    $f_{t+1} := S(f_i, f_j)$;
    Aggiungi f_{t+1} a G ;
    $t := t + 1$;
end

Teorema 1.5.4. *Dato $F = \{f_1, \ldots, f_s\}$ l'algoritmo di Buchberger si ferma restituendoci una base di Gröbner per $I = \langle F \rangle$.*

Dimostrazione. Per assurdo, supponiamo che l'algoritmo non si fermi. Indichiamo con G_i l'insieme G al passo i. Se l'algoritmo non si ferma otteniamo la catena di insiemi

$$G_1 \subsetneq G_2 \subsetneq G_3 \subsetneq \ldots$$

Dato che al passo $i+1$ aggiungiamo all'insieme G_{i+1} l'S-polinomio di due elementi di G_i, alla precedente catena corrisponde la catena di ideali monomiali

$$Lt(G_1) \subsetneq Lt(G_2) \subsetneq Lt(G_3) \subsetneq \ldots$$

contro il teorema della base di Hilbert.
Inoltren tutti gli S-polinomi di G si riducono al polinomio nullo e da $F \subseteq G \subseteq I$ segue $I = \langle F \rangle = \langle G \rangle$, pertanto dal teorema di Buchberger G è una base di Gröbner per I. $\square$

1.6 Base di Gröbner ridotta

Definizione 1.6.1. *Una base di Gröbner $G = \{g_1, \dots, g_t\}$ è detta* ***minimale*** *se*

- $lc(g_i) = 1$
- $lm(g_i) \nmid lm(g_j)$ *per* $i \neq j$.

Di immediata dimostrazione è il seguente

Lemma 1.6.2. *Se $G = \{g_1, \dots, g_t\}$ è una base di Gröbner per I e $lm(g_i)|lm(g_j)$ per qualche $i \neq j$ allora anche $G \setminus \{g_j\}$ è una base di Gröbner.*

Corollario 1.6.3. *Sia $G = \{g_1, \dots, g_t\}$ una base di Gröbner per I. Per ottenere una base minimale da G basta eliminare tutti i g_i tali che esiste $j \neq i$ con $lm(g_j)|lm(g_i)$, e poi dividere i rimanenti g_i per $lc(g_i)$.*

Proposizione 1.6.4. *Se $G = \{g_1, \dots, g_t\}$ e $F = \{f_1, \dots, f_s\}$ sono due basi di Gröbner minimali per I allora $t = s$ e, a meno di riordinamento degli indici, risulta $lm(f_i) = lm(g_i)$.*

Dimostrazione. Per ipotesi $f_1 \in I$, quindi $lm(g_i)|lm(f_1)$ per qualche i. A meno di riordinamento degli indici possiamo suppore che $i = 1$. Adesso $g_1 \in I$, allora $lm(f_j)|lm(g_1) \Rightarrow lm(f_j)|lm(f_1)$, da cui necessariamente $j = 1$, pertanto $lm(g_1) = lm(f_1)$. Adesso supponiamo $s \leq t$, ripetiamo lo stesso ragionamento per $f_2, \dots, f_s$ ottenendo $lm(g_i) = lm(f_i)$ e $s = t$. Per provare l'ultima asserzione, supponiamo per assurdo $s < t$, allora $g_{s+1} \in I$, da cui $lm(g_i) = lm(f_i)|lm(g_{s+1})$ per qualche i, contro la minimalità di G. □

Definizione 1.6.5. *Una base di Gröbner $G = \{g_1, \dots, g_t\}$ è detta* ***ridotta*** *se per ogni $i \in \{1, \dots, t\}$*

- $lc(g_i) = 1$
- g_i *è ridotto rispetto a* $G \setminus \{g_i\}$

Ogni base di Gröbner ridotta è minimale.

Corollario 1.6.6. *Sia $G = \{g_1, \dots, g_t\}$ una base di Gröbner minimale per I. Consideriamo il seguente processo di riduzione*

$$\begin{array}{ll} g_1 \xrightarrow{H_1}_+ h_1 & \text{con } h_1 \text{ ridotto rispetto a } H_1 = \{g_2, \dots, g_t\}, \\ g_2 \xrightarrow{H_1}_+ h_2 & \text{con } h_2 \text{ ridotto rispetto a } H_2 = \{h_1, g_3, \dots, g_t\}, \\ & \vdots \\ g_1 \xrightarrow{H_1}_+ h_t & \text{con } h_t \text{ ridotto rispetto a } H_t = \{h_1, \dots, h_{t-1}\}. \end{array}$$

Allora $H = \{h_1, \dots, h_t\}$ è una base di Gröbner ridotta per I.

Dimostrazione. Dato che G è una base minimale si ha $lm(h_i) = lm(g_i)$, quindi H è una base di Gröbner minimale per I. Infine poiché la riduzione di g_i per H_i è fatta utilizzando i termini $lm(h_1) = lm(g_1), \dots, lm(h_{i-1}) = lm(g_{i-1}), lm(g_{i+1}), \dots, lm(g_t)$, ne segue che H è ridotta. □

Teorema 1.6.7. *Fissato un ordinamento monomiale, ogni ideale I di $k[x_1, \dots, x_n]$ ha un unica base di Gröbner ridotta.*

Dimostrazione. Siano $G = \{g_1, \dots, g_t\}$ e $H = \{h_1, \dots, h_t\}$ due basi di Gröbner ridotte. In base a una proposizione precedente possiamo supporre $lm(g_i) = lm(h_i)$. Per assurdo supponiamo che $g_i \neq h_i$. Consideriamo la differenza $g_i - h_i \in I$, per ipotesi esiste j tale che $lm(g_j) = lm(h_j)|lm(g_i - h_i)$, ovviamente $j \neq i$ dato che $lm(g_i - h_i) < lm(g_i) = lm(h_i)$. Otteniamo che $lm(g_j) = lm(h_j)$ divide qualche termine di g_i oppure di h_j, il che contraddice il fatto che G e H sono ridotte, assurdo. □

1.7 Lo spazio vettoriale $\frac{k[x_1,\dots,x_n]}{I}$

Vogliamo trovare una base del k-spazio vettoriale $\frac{k[x_1,\dots,x_n]}{I}$.

Definizione 1.7.1. *Siano $G = \{g_1, \dots, g_n\}$ una base di Gröbner per l'ideale I e $f \in k[x_1, \dots, x_n]$. Il polinomio $r \in k[x_1, \dots, x_n]$ ridotto rispetto a G, tale che $f \xrightarrow{G}_+ r$, è detto **forma normale** di f rispetto a G, ed è denotato con $N_G(f)$.*

Osservazione 1.7.2. *Dall'algoritmo di divisione si ha che $f \equiv N_G(f) \pmod I$ per ogni $f \in k[x_1, \dots, x_n]$*

Lemma 1.7.3. *Sia G una base di Gröbner per I e siano $r, f \in k[x_1, \dots, x_n]$ con r ridotto rispetto a G. Se $f - r \in I$ allora $f \xrightarrow{G}_+ r$.*

Dimostrazione. Risulta $N_G(f) \equiv f \equiv r \pmod I$, quindi $N_G(f) - r \in I$ ridotto rispetto a G, pertanto $N_G(f) - r$ deve essere il polinomio nullo, cioè $N_G(f) = r$. □

Proposizione 1.7.4. *Siano $f, g \in k[x_1, \dots, x_n]$, allora*

$$f \equiv g \pmod I \Longleftrightarrow N_G(f) = N_G(g).$$

Perciò $\{N_G(f) : f \in k[x_1, \dots, x_n]\}$ è un insieme di rappresentanti dei laterali in $\frac{k[x_1,\dots,x_n]}{I}$. Inoltre la mappa $N_G : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$, con $f \mapsto N_G(F)$, è k-lineare.

Dimostrazione. Dall'osservazione precedente se $N_G(f) = N_G(g)$ allora $f \equiv N_G(f) = N_G(g) \equiv g \pmod I$. Viceversa se $f \equiv g \pmod I$ allora $N_G(f) \equiv N_G(g) \pmod I$, cioè $N_G(f) - N_G(g) \in I$; quest'ultimo è un polinomio ridotto rispetto a G, pertanto deve essere il polinomio nullo, cioè $N_G(f) = N_G(g)$. Adesso siano $c_1, c_2 \in k$ e $f_1, f_2 \in k[x_1, \dots, x_n]$, risulta

$$c_1 f_1 + c_2 f_2 - (c_1 N_G(f_1) + c_2 N_G(f_2)) = c_1(f_1 - N_G(f_1)) + c_2(f_2 - N_G(f_2)) \in I,$$

ma $c_1 N_G(f_1) + c_2 N_G(f_2)$ è ridotto rispetto a G, pertanto dal lemma precedente

$$N_G(c_1 f_1 + c_2 f_2) = c_1 N_G(f_1) + c_2 N_G(f_2).$$ □

Proposizione 1.7.5. *Sia $G = \{g_1, \dots, g_t\}$ una base di Gröbner per I. Una base per il k-spazio vettoriale $\frac{k[x_1,\dots,x_n]}{I}$ consiste dei laterali di tutti i monomi non nulli $X \in T^n$ ridotti rispetto a G.*

Dimostrazione. Sia $f \in k[x_1, \ldots, x_n]$, allora $f + I = N_G(f) + I$ e $N_G(f)$ è combianzione k-lineare di monomi ridotti rispetto a G. Ciò prova che i laterali di monomi ridotti formano un insieme di generatori del k-spazio vettoriale $\frac{k[x_1,\ldots,x_n]}{I}$. Infine tali laterali sono linearmente indipendenti, poiché ogni combinazione lineare di polinomi ridotti è ancora un polinomio ridotto e se $r \in I$ ridotto allora $r = \underline{0}$. □

Osservazione 1.7.6. *Un polinomio $f \in k[x_1, \ldots, x_n]$ è invertibile nel quoziente $\frac{k[x_1,\ldots,x_n]}{I}$ se e solo se $(f, I) = (1)$.*

Siano $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ un ideale e $G = \{g_1, \ldots, g_t\}$ una base di Gröbner ridotta per I. Il teorema degli zeri di Hilbert debole ci dice che $V_{\overline{k}}(I) = \emptyset \Leftrightarrow G = \{1\}$.

Teorema 1.7.7. *Sono equivalenti*

1. $|V_{\overline{k}}(I)| < \infty$
2. *Per ogni $i \in \{1, \ldots, n\}$, esiste $j \in \{1, \ldots, t\}$ tale che $lm(g_j) = x_i^{v_i}$, per qualche v_i*
3. $\dim_k \left(\frac{k[x_1,\ldots,x_n]}{I} \right) < \infty$

Dimostrazione.

(1) ⇒ (2) Se $V_{\overline{k}}(I) = \emptyset$ allora $G = \{1\}$, quindi $v_i = 0$ per ogni $i \in \{1, \ldots, n\}$. Supponiamo che $V_{\overline{k}}(I) \neq \emptyset$, fissato $i \in \{1, \ldots, n\}$ siano a_{ij} con $j = 1, \ldots, l$ le i-esime coordinate distinte dei punti di $V_{\overline{k}}(I)$ (dato che le prendiamo distinte, in generale si potrebbero avere ripetizioni, quindi l dipende da i). Per ogni $j = 1, \ldots, l$, sia $f_j \in k[x_i]$ monico tale che $f_j(a_{ij}) = 0$, e sia $f = f_1 \cdot \ldots \cdot f_l \in k[x_i] \subseteq k[x_1, \ldots, x_n]$. Per ogni $(\alpha_1, \ldots, \alpha_n) \in V_{\overline{k}}(I)$, $f(\alpha_1, \ldots, \alpha_n) = f_1(\alpha_1, \ldots, \alpha_n) \cdot \ldots \cdot f_l(\alpha_1, \ldots, \alpha_n) = f_1(\alpha_i) \cdot \ldots \cdot f_l(\alpha_i) = 0$, in quanto $\alpha_i = a_{ij}$ per qualche j, quindi $f_j(\alpha_i) = 0$. Pertanto $f \in \mathscr{I}(V_{\overline{k}}(I)) = \sqrt{I}$, da cui $f^m \in I$ per qualche $m \in \mathbb{N}$, ma dato che f è monico si ha che $lm(f^m) = x_i^{m'}$ per qualche $m' \in \mathbb{N}$, quindi esiste j tale che $lm(g_j) | x_i^{m'}$ pertanto $lm(g_j) = x_i^{v_i}$.

(2) ⇒ (3) Una k-base per $\frac{k[x_1,\ldots,x_n]}{I}$ è l'insieme dei laterali di monomi ridotti rispetto a G. Dall'ipotesi sappiamo che tali monomi sono in numero finito.

(3) ⇒ (1) Sia $i \in \{1, \ldots, n\}$, consideriamo i laterali

$$1 + I, x_i + I, x_i^2 + I, \ldots, x_i^k + I, \ldots$$

essi sono linearmente dipendenti per ipotesi, quindi esistono $m \in \mathbb{N}$ e $c_j \in k$ non tutti nulli tali che $p(x_i) = \sum_{j=0}^m c_j x_i^j \in I$. Sia adesso $P = (\alpha_1, \ldots, \alpha_n) \in V_{\overline{k}}(I)$, allora $p(P) = p(\alpha_i) = 0$, pertanto la i-esima coordinata di un qualsiasi punto di $V_{\overline{k}}(I)$ è radice del polinomio p, ma p ha un un numero finito di radici. Dall'arbitrarietà di i segue che $V_{\overline{k}}(I)$ è finito.

□

Definizione 1.7.8. *Un ideale $I \subsetneq k[x_1, \ldots, x_n]$ che soddisfa una delle precedenti condizioni equivalenti è detto* ***zerodimensionale****.*

Corollario 1.7.9. *Sia I un ideale zerodimensionale e $G = \{g_1, \ldots, g_t\}$ la base di Gröbner ridotta per I rispetto a $>_{lex}$ con $x_n > x_{n-1} > \ldots > x_1$. È possibile ordinare $g_1, \ldots, g_t$ in modo tale che*

$$\begin{array}{ll} g_1 \in k[x_1] & \\ g_2 \in k[x_1, x_2] & lm(g_2) = x_2^{a_2} \\ g_3 \in k[x_1, x_2, x_3] & lm(g_3) = x_3^{a_3} \\ \vdots & \\ g_n \in k[x_1, x_2, \ldots, x_n] & lm(g_n) = x_n^{a_n} \end{array}$$

Dimostrazione. Dalla (2) del teorema precedente, a meno di riordinamento degli indici si ha che $lm(g_j) = x_j^{a_j}$. Dato che è $x_n > x_{n-1} > \ldots > x_1$ allora $g_j \in k[x_1, \ldots, x_j]$. □

Teorema 1.7.10. *Sia $I = (f_1, \ldots, f_s)$ un ideale di $k[x_1, \ldots, x_n]$, allora*

$$f \in \sqrt{I} \Longleftrightarrow (I, 1 - wf) = k[x_1, \ldots, x_n, w].$$

Dimostrazione.

⇒ Per assurdo $(a_1, \ldots, a_n, b) \in V_{\overline{k}}(I, 1-wf) \neq \emptyset$ allora $f_i(a_1, \ldots, a_n) = 0$ per ogni $i \in \{1, \ldots, s\}$ e $1 - bf(a_1, \ldots, a_n) = 0$, ma $f \in \sqrt{I} = \mathscr{I}(V_{\overline{k}}(I))$, quindi $f(a_1, \ldots, a_n) = 0$, assurdo. Pertanto $V_{\overline{k}}(I, 1 - wf) = \emptyset \Leftrightarrow (I, 1 - wf) = k[x_1, \ldots, x_n, w]$.

⇐ Dal momento che $1 \in (I, 1 - wf)$ allora

$$1 = \sum_{i=1}^{s} h_i f_i + (1 - wf)h \quad h_i, h \in k[x_1, \ldots, x_n, w].$$

Adesso sia $(a_1, \ldots, a_n) \in V_{\overline{k}}(I)$, si ha

$$1 = (1 - wf(a_1, \ldots, a_n))h(a_1, \ldots, a_n, w),$$

se per assurdo $f(a_1, \ldots, a_n) \neq 0$ allora sostituendo alla precedente $w = f(a_1, \ldots, a_n)^{-1}$ otteniamo $1 = 0$, assurdo. Quindi $f(a_1, \ldots, a_n) = 0$, cioè $f \in \mathscr{I}(V_{\overline{k}}(I)) = \sqrt{I}$. □

In base al teorema precedente $f \in \sqrt{I} \Longleftrightarrow (I, 1 - wf)$ ha base di Gröbner $\{1\}$.

1.8 Eliminazione

Teorema 1.8.1. *Siano I un ideale di $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ e $>_{lex}$ con $x_i > y_j$ per ogni i, j. Se G è una base di Gröbner per I allora $G \cap k[y_1, \ldots, y_s]$ è una base di Gröbner per $I \cap k[y_1, \ldots, y_m]$ (che è detto **ideale di eliminazione**).*

Dimostrazione. Prima di tutto osserviamo che $G \cap k[y_1, \ldots, y_m] \subseteq I \cap k[y_1, \ldots, y_m]$. Sia adesso $f \in I \cap k[y_1, \ldots, y_m]$ non nullo, allora esiste i tale che $lm(g_i)|lm(f)$, da cui $g_i \in G \cap k[y_1, \ldots, y_m]$. □

Proposizione 1.8.2. *Siano I e J due ideali di $k[x_1, \ldots, x_n]$ e w una variabile su k. Allora*

$$I \cap J = (wI, (1 - w)J) \cap k[x_1, \ldots, x_n].$$

Dimostrazione.

- $\subseteq$ Sia $f \in I \cap J$ allora $f = wf + (1-w)f \in (wI, (1-w)J) \cap k[x_1, \dots, x_n]$.
- $\supseteq$ Sia $f \in (wI, (1-w)J) \cap k[x_1, \dots, x_n]$, allora esistono $g \in I$ e $h \in J$ tali che $f = wg + (1-w)h$, da cui

  $$f = wg + (1-w)h = h + w(g-h) \in k[x_1, \dots, x_n],$$

  pertanto $g - h = 0 \Rightarrow g = h = f \in I \cap J$.

$\square$

Lemma 1.8.3. *Siano $f, g \in k[x_1, \dots, x_n] \setminus \{\underline{0}\}$, se $l = \operatorname{mcm}(f, g)$, si ha $(f) \cap (g) = (l)$.*

Dimostrazione. Se $h \in (f) \cap (g)$ allora $f|h$ e $g|h$, quindi $l|h$, cioè $h \in (l)$, quindi $(f) \cap (g) \subseteq (l)$. Viceversa, dato che $f|l$ e $g|l$ allora $l \in (f) \cap (g)$, cioè $(l) \subseteq (f) \cap (g)$. $\square$

Lemma 1.8.4. *Siano $I = (f_1, \dots, f_s)$ e J due ideali di $k[x_1, \dots, x_n]$, allora*

$$(J : I) = \bigcap_{i=1}^{s} (J : f_i).$$

Dimostrazione. $g \in (J : I)$ se e solo se $gI \subseteq J$ se e solo se per ogni i si ha $gf_i \in J$ se e solo se $g \in \bigcap_{i=1}^{s} (J : f_i)$. $\square$

Lemma 1.8.5. $(J : f) = \frac{1}{f}(J \cap (f))$.

1.9 Mappe polinomiali

Consideriamo un omomorfismo di anelli $\phi : k[y_1, \dots, y_m] \to k[x_1, \dots, x_n]$ che sia anche un'applicazione lineare di k-spazi vettoriali, cioè un omomorfismo di k-algebre. Tale mappa è univocamente determinata da $\phi(y_i)$ per ogni $i \in \{1, \dots, m\}$. Infatti per ogni $h \in k[y_1, \dots, y_m]$ con $h(y_1, \dots, y_m) = \sum_v c_v y_1^{v_1} \dots y_m^{v_m}$, dove $v = (v_1, \dots, v_m)$, si ha

$$\phi(h(y_1, \dots, y_m)) = \sum_v c_v \phi(y_1)^{v_1} \dots \phi(y_m)^{v_m} = h(\phi(y_1), \dots, \phi(y_m)).$$

Se poniamo $\phi(y_i) = f_i \in k[x_1, \dots, x_n]$ risulta $\operatorname{Im} \phi = k[f_1, \dots, f_m]$, da cui otteniamo il seguente isomorfismo di k-algebre

$$\frac{k[y_1, \dots, y_m]}{\ker \phi} \simeq k[f_1, \dots, f_m], \quad g + \ker \phi \mapsto \phi(g).$$

Osserviamo che $h \in \ker \phi \Leftrightarrow \phi(h) = 0 \Leftrightarrow h(f_1, \dots, f_m) = 0$, infatti il nucleo di ϕ è detto ideale delle relazioni tra $f_1, \dots, f_m$.

Lemma 1.9.1. *Siano R un anello commutativo unitario e $a_1, \dots, a_n, b_1, \dots, b_n \in R$. Allora*

$$a_1 \dots a_n - b_1 \dots b_n \in (a_1 - b_1, \dots, a_n - b_n)$$

Dimostrazione. Procediamo per induzione su n. Ovviamente $a_1 - b_1 \in (a_1 - b_1)$. Per il passo induttivo, risulta

$$a_1 \dots a_n - b_1 \dots b_n = a_1(a_2 \dots a_n - b_2 \dots b_n) + b_2 \dots b_m(a_1 - b_1) \in (a_1 - b_1, \dots, a_n - b_n).$$

□

Proposizione 1.9.2. *Sia* $J = (y_1 - f_1, \dots, y_n - f_n) \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$, *con le notazioni precedenti si ha* $\ker \phi = J \cap k[y_1, \dots, y_m]$.

Dimostrazione.

$\subseteq$ Sia $g \in \ker \phi$, $g = \sum_v c_v y_1^{v_1} \dots y_m^{v_m}$ con $c_v \in k$, $v = (v_1, \dots, v_m)$. Poiché $g(f_1, \dots, f_m) = 0$ allora, in base al lemma precedente, si ha

$$g = g(y_1, \dots, y_m) - g(f_1, \dots, f_m) = \sum_v c_v(y_1^{v_1} \dots y_m^{v_m} - f_1^{v_1} \dots f_m^{v_m}) \in J \cap k[y_1, \dots, y_m]$$

$\supseteq$ Sia $g \in J \cap k[y_1, \dots, y_m]$, allora $g = \sum_{i=1}^m (y_i - f_i) h_i$ con $h_i \in k[y_1, \dots, y_m, x_1, \dots, x_n]$, da cui $\phi(g) = 0 \Rightarrow g \in \ker \phi$. □

In base alla proposizione precedente, per calcolare una base di Gröbner per $\ker \phi$ basta calcolare una base di Gröbner G per J rispetto a $>_{lex}$, $x > y$ allora la base di Gröbner cercata sarà $G \cap k[y_1, \dots, y_n]$.

Proposizione 1.9.3. *Sia J come nella proposizione precedente e sia G una base di Gröbner per J rispetto a $>_{lex}$ con $x > y$, allora*

$$f \in k[x_1, \dots, x_m] \cap \operatorname{Im} \phi \Longleftrightarrow \exists h \in k[y_1, \dots, y_m] : f \xrightarrow{G}_+ h,$$

in questo caso $f = \phi(h)$.

Dimostrazione.

$\Rightarrow$ Sia $f \in k[x_1, \dots, x_n] \cap \operatorname{Im} \phi$, allora $f = g(f_1, \dots, f_m)$ con $g \in k[y_1, \dots, y_m]$. Dal lemma precedente abbiamo

$$f(x_1, \dots, x_n) - g(y_1, \dots, y_m) = g(f_1, \dots, f_m) - g(y_1, \dots, y_m) \in J$$

pertanto $N_G(f) = N_G(g) = h$, ma $g \in k[y_1, \dots, y_m]$ da cui $N_G(g) \in k[y_1, \dots, y_m]$. Dunque $f \xrightarrow{G}_+ h \in k[y_1, \dots, y_m]$.

$\Leftarrow$ Per ipotesi $f(x_1, \dots, x_n) - h(y_1, \dots, y_m) = \sum_{i=1}^n (y_i - f_i) h_i \in J$, quindi $f(x_1, \dots, x_n) - h(f_1, \dots, f_m) = 0 \Rightarrow f(x_1, \dots, x_n) = h(f_1, \dots, f_m) = \phi(h)$. □

Corollario 1.9.4. *Con la stessa notazione della proposizione precedente, se* $f \in k[x_1, \dots, x_n]$ *allora* $f \in \operatorname{Im} \phi \Leftrightarrow N_G(f) \in k[y_1, \dots, y_m]$.

Dimostrazione.

$\Rightarrow$ Se $f \in \operatorname{Im} \phi$ allora $f \xrightarrow{G}_+ h \in k[y_1, \dots, y_m]$, quindi $N_G(f) = N_G(h) \in k[y_1, \dots, y_m]$.

$\Leftarrow$ Segue dalla proposizione precedente.

$\square$

Proposizione 1.9.5. *Sia $J = (y_1 - f_1, \dots, y_m - f_m) \subseteq k[y_1 \dots, y_m, x_1, \dots, x_n]$ e sia G la base di Gröbner ridotta per J rispetto a $>_{lex}$ con $x > y$. Allora*

$$\phi \text{ è suriettiva} \iff \forall i \in \{1, \dots, n\}, \exists g_i \in G : g_i = x_i - h_i \text{ con } h_i \in k[y_1, \dots, y_m]$$

Dimostrazione.

- $\Rightarrow$ Possiamo supporre $x_n > x_{n-1} > \dots > x_1$. Sia $i \in \{1, \dots, n\}$, dato che $x_i \in \operatorname{Im}\phi$ allora $x_i \xrightarrow{G}_+ h_i' \in k[y_1, \dots, y_m]$, da cui $x_i - h_i' \in J$, quindi esiste $g_j \in G$ tale che $lm(g_j) | lm(x_i - h_i') = x_i$. A meno di riordinamento degli indici, possiamo supporre $j = i$, quindi $g_i = x_i - h_i$ con $h_i \in k[y_1, \dots, y_m]$.

- $\Leftarrow$ Se $x_i - h_i \in G$ allora $x_i \xrightarrow{G}_+ h_i \in k[y_1, \dots, y_m]$, quindi dalla proposizione precedente si ha $x_i \in \operatorname{Im}\phi$. $\square$

Definizione 1.9.6. *Una k-algebra è detta **affine** se è isomorfa a $\frac{k[x_1, \dots, x_n]}{I}$ per qualche ideale I di $k[x_1, \dots, x_n]$.*

Siano $L \subseteq k[y_1, \dots, y_m]$ e $I \subseteq k[x_1, \dots, x_n]$ ideali e sia

$$\phi : \frac{k[y_1, \dots, y_m]}{L} \to \frac{k[x_1, \dots, x_n]}{I} \quad \text{definita con } y_i + L \mapsto f_i + I.$$

Osserviamo che ϕ è ben definita se e solo se, posto $L = (g_1, \dots, g_t)$, allora risulta $g_i(f_1, \dots, f_m) \in I$. Infatti se ϕ è ben definita allora $g_i \in L \Rightarrow g_i(f_1, \dots, f_m) \in I$. Viceversa, se $h + L = h' + L$ allora $h - h' \in L$, quindi $h - h' = \sum_{i=1}^t h_i g_i$, da cui

$$h(f_1, \dots, f_m) - h'(f_1, \dots, f_m) = \sum_{i=1}^t h_i(f_1, \dots, f_m) g_i(f_1, \dots, f_m) \in I,$$

ossia $h(f_1, \dots, f_m) + I = h'(f_1, \dots, f_m) + I \Rightarrow \phi(h + L) = \phi(h' + L)$.

Teorema 1.9.7. *Sia $J = (I, y_1 - f_1, \dots, y_m - f_m) \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$, sotto queste ipotesi, se $J \cap k[y_1, \dots, y_m] = (f_1', \dots, f_t')$ allora $\ker\phi = (f_1' + L, \dots, f_t' + L)$.*

Dimostrazione.

- $\subseteq$ Sia $f' \in \ker\phi$, quindi $\phi(f' + L) = \underline{0}_{\frac{k[x_1, \dots, x_n]}{I}}$, da cui $f'(f_1, \dots, f_m) \in I$. Poniamo $f'(y_1, \dots, y_m) = \sum_v c_v y_1^{v_1} \dots y_m^{v_m}$ con $c_v \in k$, $v = (v_1, \dots, v_m)$. Risulta

$$\begin{aligned} f'(y_1, \dots, y_m) &= \big(f'(y_1, \dots, y_m) - f'(f_1, \dots, y_m)\big) + f'(f_1, \dots, f_m) = \\ &= \underbrace{\sum_v c_v (y_1^{v_1} \dots y_m^{v_m} - f_1^{v_1} \dots f_m^{v_m})}_{\in J} + \underbrace{f'(f_1, \dots, f_m)}_{\in I} \in J \cap k[y_1, \dots, y_m]. \end{aligned}$$

$\supseteq$ Sia $f' \in J \cap k[y_1, \dots, y_m]$, allora possiamo scrivere

$$f'(y_1, \dots, y_m) = \sum_{i=1}^{m} (y_i - f_i(x_1, \dots, x_n))h_i + \sum_v a_v u_v,$$

dove $a_v, h_i \in k[y_1, \dots, y_m, x_1, \dots, x_n], u_v \in I$. Si ha

$$\phi(f' + L) = f'(f_1, \dots, f_m) + I = \sum_v a_v(f_1, \dots, f_m, x_1, \dots, x_n)u_v + I = I,$$

pertanto $f' + L \in \ker \phi$. $\square$

Teorema 1.9.8. *Siano $J = (I, y_1 - f_1, \dots, y_m - f_m) \subseteq k[y_1, \dots, y_m, x_1, \dots, x_n]$, G una base di Gröbner per J rispetto a $>_{lex}$ con $x > y$ e $f \in k[x_1, \dots, x_n]$, allora*

$$f + I \in \operatorname{Im} \phi \Leftrightarrow f \xrightarrow{G}_+ h \in k[y_1, \dots, y_m],$$

in tal caso $f + I = \phi(h + L) = h(f_1, \dots, f_m) + L$

Dimostrazione.

$\Rightarrow$ Per ipotesi esiste $g \in k[y_1, \dots, y_m]$ tale che $g(f_1, \dots, f_m) + I = \phi(g + L) = f + I$ da cui $f - g(f_1, \dots, f_m) \in I$. Risulta

$$\begin{gathered} f(x_1, \dots, x_n) - g(y_1, \dots, y_m) = \\ = \big(f(x_1, \dots, x_n) - g(f_1, \dots, f_m)\big) + \big(g(f_1, \dots, f_m) - g(y_1, \dots, y_m)\big) \in J \end{gathered}$$

da cui $N_G(f) = N_G(g) = h$, e dato che $g \in k[y_1, \dots, y_m]$ si ha $N_G(g) \in k[y_1, \dots, y_m]$. Dunque $f \xrightarrow{G}_+ h \in k[y_1, \dots, y_m]$.

$\Leftarrow$ Per ipotesi $f \xrightarrow{G}_+ h \in k[y_1, \dots, y_m]$, quindi $f - h \in J$, da cui

$$f - h = \sum_{i=1}^{m} (y_i - f_i)h_i + \sum_v a_v u_v$$

da cui $f + I = h(f_1, \dots, f_m) + I = \phi(h + L)$. $\square$

Corollario 1.9.9. $f + I \in \operatorname{Im} \phi \Longleftrightarrow N_G(f) \in k[y_1, \dots, y_m]$.

Proposizione 1.9.10. *Sia G una base di Gröbner ridotta di J rispetto a $>_{lex}$ con $x > y$. Allora ϕ è suriettaiva se e solo se per ogni $i \in \{1, \dots, m\}$ esiste $g_i = x_i - h_i \in G$ con $h_i \in k[y_1, \dots, y_m]$*

Dimostrazione. Simile alla dimostrazione della Proposizione 1.9.5. $\square$

Abbreviamo $V_{\overline{k}}(I)$ con $V(I)$. Consideriamo le proiezioni $\pi : \overline{k}^{m+n} \to \overline{k}^m$, con $\pi(a_1, \dots, a_m, b_1, \dots, b_n) = (a_1, \dots, a_m)$.

Proposizione 1.9.11. *Se $S \subseteq \overline{k}^n$ allora $V(\mathscr{I}(S))$ è la più piccola varietà contenente S detta* ***chiusura*** *di Zariski di S.*

Dimostrazione. Sia $W = V(J) \subseteq \overline{k}^n$, allora

$$S \subseteq W \Rightarrow \mathscr{I}(S) \supseteq \mathscr{I}(W) \Rightarrow V(\mathscr{I}(S)) \subseteq V(\mathscr{I}(W)) = W. \qquad \square$$

Proposizione 1.9.12. *Se $V, W \subseteq \overline{k}^n$, allora $\mathscr{I}(V \setminus W) = (\mathscr{I}(V) : \mathscr{I}(W))$.*

Dimostrazione. Risulta

$$f \in \mathscr{I}(V \backslash W) \Leftrightarrow f(P) = 0 \quad \forall P \in V \backslash W \Leftrightarrow \forall g \in \mathscr{I}(W) \quad fg \in \mathscr{I}(V) \Leftrightarrow f \in (\mathscr{I}(V) : \mathscr{I}(W))$$

$\square$

Teorema 1.9.13. *Sia $I \subseteq k[y_1, \ldots, y_m, x_1, \ldots, x_n]$. La chiusura di Zariski di $\pi(V(I))$ è $V(I \cap k[y_1, \ldots, y_m])$, cioè*

$$V\Bigg(\mathscr{I}\Big(\pi\big(V(I)\big)\Big)\Bigg) = V(I \cap k[y_1, \ldots, y_m]).$$

Dimostrazione. Poniamo $V = V(I)$ e $I_y = I \cap k[y_1, \ldots, y_m]$.

- $\subseteq$ Basta verificare che $\pi(V) \subseteq V(I_y)$. Sia $P = (a_1, \ldots, a_m, b_1, \ldots, b_n) \in V$, $\pi(P) = (a_1, \ldots, a_m) \in \pi(V)$. Se $f \in I_y$ allora $0 = f(a_1, \ldots, a_n, b_1, \ldots, b_m) = f(a_1, \ldots, a_m)$, da cui $\pi(P) \in V(I_y)$.

- $\supseteq$ Proviamo che $\mathscr{I}(\pi(V)) \subseteq \sqrt{I_y}$. Siano $f \in \mathscr{I}(\pi(V))$ e $(a_1, \ldots, a_m, b_1, \ldots, b_n) \in V$, allora, vedendo $f \in k[y_1, \ldots, y_m, x_1, \ldots, x_n]$, si ha

  $$f(a_1, \ldots, a_m, b_1, \ldots, b_n) = f(a_1, \ldots, a_m) = 0.$$

  Da cui $f \in \mathscr{I}(V(I)) = \sqrt{I}$, quindi esiste $k \in \mathbb{N}$ tale che $f^k \in I$, ma $f \in k[y_1, \ldots, y_m]$, da cui $f^k \in I_y$, cioè $f \in \sqrt{I_y}$. Infine da $\mathscr{I}(\pi(V)) \subseteq \sqrt{I_y}$ segue $V(\mathscr{I}(\pi(V))) \supseteq V(\sqrt{I_y}) = V(I_y)$. $\square$

Sia $\varphi : \overline{k}^n \to \overline{k}^m$ data da $\varphi(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n))$ con $f_i \in k[x_1, \ldots, x_n]$. L'immagine $\operatorname{Im} \varphi \subseteq \overline{k}^m$ è parametrizzata dai polinomi f_i

$$\begin{cases} y_1 = f_1(x_1, \ldots, x_n) \\ \vdots \\ y_m = f_m(x_1, \ldots, x_n) \end{cases}$$

Queste equazioni definiscono una varietà $\mathcal{V} = V(y_1 - f_1, \ldots, y_m - f_m) \subseteq \overline{k}^{m+n}$. La varietà $\mathcal{V}$ è il grafico di φ, infatti risulta

$$\mathcal{V} = \left\{ \big(a_1, \ldots, a_n, f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)\big) : (a_1, \ldots, a_n) \in \overline{k}^n \right\}.$$

In generale, non sempre le equazioni parametriche definiscono una varietà. Per calcolare la chiusura di Zariski di $\operatorname{Im} \varphi$ basta applicare il teorema precedente a $\mathcal{V}$. Infatti si ha $\operatorname{Im} \varphi = \pi(\mathcal{V})$, dove $\pi(x_1, \ldots, x_n, f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)) = (f_1, \ldots, f_m)$. È sufficiente quindi calcolare una base di Gröbner per $I = (y_1 - f_1, \ldots, y_m - f_m) \subseteq$

$k[y_1, \dots, y_m, x_1, \dots, x_n]$ rispetto a $>_{lex}$ con $x > y$; i polinomi di G nella sola y sono i polinomi cercati.

Più in generale siano $V \subseteq \overline{k}^n$, $W \subseteq \overline{k}^m$ due varietà, e consideriamo la mappa di polinomi $\alpha : V \to W$ con $(a_1, \dots, a_n) \mapsto (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n))$ con $f_i \in k[x_1, \dots, x_n]$. Questa mappa tra varità genera un omomorfismo tra k-algebre affini

$$\alpha^* : \frac{k[y_1, \dots, y_m]}{\mathscr{I}(W)} \to \frac{k[x_1, \dots, x_n]}{\mathscr{I}(V)} \quad \text{con } y_i + \mathscr{I}(W) \mapsto f_i + \mathscr{I}(V).$$

Osserviamo che α^* è ben definita. Infatti per ogni $(a_1, \dots, a_n) \in V$ e per ogni $g \in \mathscr{I}(W)$ si ha $\alpha(a_1, \dots, a_n) \in W$, da cui

$$0 = g(\alpha(a_1, \dots, a_n)) = g(f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)),$$

pertanto $g(f_1, \dots, f_m) \in \mathscr{I}(V)$.

Vogliamo determinare la chiusura di Zariski di $\operatorname{Im} \alpha = \alpha(V)$.

Proposizione 1.9.14. $g \in \mathscr{I}(\alpha(V)) \Leftrightarrow g + \mathscr{I}(W) \in \ker \alpha^*$.

Dimostrazione. Risulta

$$\begin{aligned} g \in \mathscr{I}(\alpha(V)) &\Leftrightarrow \forall P \in V \quad g(\alpha(P)) = 0 \Leftrightarrow \\ \Leftrightarrow g \circ \alpha \in \mathscr{I}(V) &\Leftrightarrow \alpha^*(g + \mathscr{I}(W)) = \underline{0} \Leftrightarrow g + \mathscr{I}(W) \in \ker \alpha^*. \end{aligned}$$ □

Definizione 1.9.15. *Due varietà $V \subseteq \overline{k}^n$, $W \subseteq \overline{k}^m$ sono **isomorfe** se esistono $\alpha : V \to W$ e $\beta : W \to V$ date da polinomi a coefficienti in k tali che $\alpha \circ \beta = 1_W$ e $\beta \circ \alpha = 1_V$.*

Teorema 1.9.16. *Due varietà $V \subseteq \overline{k}^n$ e $W \subseteq \overline{k}^m$ sono isomorfe se e solo se esiste un isomorfismo tra le k-algebre affini $\frac{k[y_1,\dots,y_n]}{\mathscr{I}(W)}$ e $\frac{k[x_1,\dots,x_n]}{\mathscr{I}(V)}$.*

Dimostrazione.

$\Rightarrow$ Siano

$$\begin{aligned} &\alpha : V \to W \text{ con } \alpha(a_1, \dots, a_n) = (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n)), f_i \in k[x_1, \dots, x_n] \\ &\beta : W \to V \text{ con } \beta(b_1, \dots, b_m) = (g_1(b_1, \dots, b_m), \dots, g_n(b_1, \dots, b_m)), g_i \in k[y_1, \dots, y_m]; \end{aligned}$$

come dall'ipotesi. Tali funzioni inducono i seguenti omomorfismi di k-algebre

$$\begin{aligned} \alpha^* : \frac{k[y_1, \dots, y_m]}{\mathscr{I}(W)} \to \frac{k[x_1, \dots, x_n]}{\mathscr{I}(V)} \quad &\text{con } y_i + \mathscr{I}(W) \mapsto f_i + \mathscr{I}(V) \\ \beta^* : \frac{k[x_1, \dots, x_n]}{\mathscr{I}(V)} \to \frac{k[y_1, \dots, y_m]}{\mathscr{I}(W)} \quad &\text{con } x_i + \mathscr{I}(V) \mapsto g_i + \mathscr{I}(W). \end{aligned}$$

Per ipotesi $\beta \circ \alpha = 1_V$, quindi

$$\alpha^* \circ \beta^* = (\beta \circ \alpha)^* = (1_V)^* = 1_{\frac{k[x_1,\dots,x_n]}{\mathscr{I}(V)}}.$$

Analogamente $\beta^* \circ \alpha^* = 1_{\frac{k[y_1,\dots,y_m]}{\mathscr{I}(W)}}$, da cui α^* e β^* sono isomorfisimi.

$\Leftarrow$ Sia

$$\tau : \frac{k[y_1, \ldots, y_m]}{\mathscr{I}(W)} \to \frac{k[x_1, \ldots, x_n]}{\mathscr{I}(V)}$$

un isomorfismo di k-algebre. Poniamo

$$\tau(y_i + \mathscr{I}(W)) = f_i + \mathscr{I}(V) \quad f_i \in k[x_1, \ldots, x_n]$$
$$\tau^{-1}(x_i + \mathscr{I}(V)) = g_i + \mathscr{I}(W) \quad g_i \in k[y_1, \ldots, y_m].$$

Sia $\alpha : V \to W$ con $\alpha(a_1, \ldots, a_n) = (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n))$. Osserviamo che, poiché τ è ben definita allora lo è anche α, procediamo in modo analogo per $\beta : W \to V$. Infine si verifica facilmente che $\beta = \alpha^{-1}$.

□

1.10 Basi di Gröbner e sizigie

Poniamo $A = k[x_1, \ldots, x_n]$ e sia $I = (f_1, \ldots, f_s)$ un ideale di A. Consideriamo l'omomorfismo di A-moduli

$$\phi : A^s \to I \quad \text{con } \phi(h_1, \ldots, h_s) = \sum_{i=1}^{s} h_i f_i.$$

In questo modo risulta $I \simeq \frac{A^s}{\ker \phi}$. Il nucleo $\ker \phi$ è detto **modulo delle sizigie** della matrice $1 \times s$ $[f_1 \ldots f_s]$ denotato con $\mathrm{Syz}(f_1, \ldots, f_s)$. Un elemento $(h_1, \ldots, h_s) \in \mathrm{Syz}(f_1, \ldots, f_s)$ è detto **sizigia** di $[f_1 \ldots f_s]$, e soddisfa

$$h_1 f_1 + \ldots h_s f_s = 0.$$

Osservazione 1.10.1. *La mappa ϕ può essere vista come moltiplicazione tra matrici*

$$\phi(h_1, \ldots, h_s) = \begin{bmatrix} f_1 \ldots f_s \end{bmatrix} \cdot \begin{bmatrix} h_1 \\ \vdots \\ h_s \end{bmatrix} = \sum_{i=1}^{s} h_i f_i.$$

Se poniamo $F = [f_1 \ldots f_s]$ e $\underline{h} = [h_1 \ldots h_s]^t \in A^s$, allora $\phi(h_1, \ldots, h_s) = F \cdot \underline{h}$ e $\mathrm{Syz}(f_1, \ldots, f_s)$ è l'insieme di tutte le soluzioni $\underline{h}$ dell'equazione $F \cdot \underline{h} = 0$.

Definizione 1.10.2. *Definiamo* ***multigrado*** *del monomio $X = x_1^{v_1} x_2^{v_2} \ldots x_n^{v_n}$ il vettore $v = (v_1, \ldots, v_n) \in \mathbb{N}^n$.*

Proposizione 1.10.3. *Siano $c_1, \ldots, c_s \in k \setminus \{0\}$ e $X_1, \ldots, X_s \in A$ monomi. Per $i, j \in \{1, \ldots, s\}$ con $i \neq j$, sia $X_{ij} = \mathrm{mcm}(X_i, X_j)$, allora*

$$\mathrm{Syz}(c_1 X_1, \ldots, c_s X_s) = \left(\left\{ \frac{X_{ij}}{c_i X_i} \underline{e_i} - \frac{X_{ij}}{c_j X_j} \underline{e_j} \in A^s : 1 \leq i < j \leq s \right\} \right)$$

dove $\underline{e_i} = (0, \ldots, \underbrace{1}_{\text{posto } i}, \ldots, 0) \in A^s$.

Dimostrazione.

$\supseteq$ Basta osservare che per ogni $i \neq j$ risulta $\frac{X_{ij}}{c_i X_i} \underline{e_i} - \frac{X_{ij}}{c_j X_j} \underline{e_j} \in \mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$.

$\subseteq$ Sia $(h_1, \ldots, h_s) \in \mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$, allora

$$c_1X_1h_1 + \ldots + c_sX_sh_s = 0.$$

In particolare, la somma di tutti i monomi di un fissato multigrado $v \in \mathbb{N}^n$ è nulla. Poniamo $X = \underline{x}^v$ e sia, per ogni $i \in \{1, \ldots, n\}$, a_iY_i il termine di h_i tale che $a_i \in k$ e $Y_iX_i = X$. Basta considerare il caso $(h_1, \ldots, h_s) = (a_1Y_1, \ldots, a_sY_s)$. Risulta

$$\sum_{i=1}^{s} c_i a_i X_i Y_i = \sum_{i=1}^{s} c_i a_i X = \left(\sum_{i=1}^{s} c_i a_i \right) X = 0 \Rightarrow \sum_{i=1}^{s} c_i a_i = 0$$

da cui possiamo scrivere

$$(h_1, \ldots, h_s) = (a_1Y_1, \ldots, a_sY_s) = \sum_{i=1}^{s} a_i Y_i \underline{e_i} = \sum_{i=1}^{s} c_i a_i \frac{X}{c_i X_i} \underline{e_i} =$$

$$= c_1 a_1 \frac{X}{X_{12}} \left(\frac{X_{12}}{c_1 X_1} \underline{e_1} - \frac{X_{12}}{c_2 X_2} \underline{e_2} \right) + (c_1a_1 + c_2a_2) \frac{X}{X_{23}} \left(\frac{X_{23}}{c_2 X_2} \underline{e_2} - \frac{X_{23}}{c_3 X_3} \underline{e_3} \right) + \ldots +$$
$$+ (c_1a_1 + \ldots + c_{s-1}a_{s_1}) \frac{X}{X_{s-1\,s}} \left(\frac{X_{s-1\,s}}{c_{s-1} X_{s-1}} \underline{e_{s-1}} - \frac{X_{s-1\,s}}{c_s X_s} \underline{e_s} \right). \qquad \square$$

Osservazione 1.10.4. *La sizigia* $\frac{X_{ij}}{c_i X_i} \underline{e_i} - \frac{X_{ij}}{c_j X_j} \underline{e_j}$ *di* $[lt(f_1) \ldots lt(f_s)]$ *dà luogo all'S-polinomio* $S(f_i, f_j)$*, infatti*

$$[f_1 \ldots f_s] \cdot \left(\frac{X_{ij}}{c_i X_i} \underline{e_i} - \frac{X_{ij}}{c_j X_j} \underline{e_j} \right) = \frac{X_{ij}}{c_i X_i} f_i - \frac{X_{ij}}{c_j X_j} f_j = S(f_i, f_j).$$

Definizione 1.10.5. *Siano* $X_1, \ldots, X_s, X$ *monomi e* $c_1, \ldots, c_s \in k \setminus \{0\}$ *. Diciamo che una sizigia* $\underline{h} = (h_1, \ldots, h_s) \in \mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$ *è **omogenea di grado*** X *se ogni* $h_i \neq \underline{0}$ *è un termine non nullo e* $X_i lm(h_i) = X$ *per ogni* $i \in \{1, \ldots, s\}$*. Diciamo che* $\underline{h} \in \mathrm{Syz}(c_1X_1, \ldots, c_sX_s)$ *è **omogenea** se è omogenea di grado* X *per qualche* $X \in T^n$*.*

Ad esempio, l'insieme dei generatori della proposizione precedente è un insieme finito di sizigie omogenee.

Teorema 1.10.6. *Sia* $G = \{g_1, \ldots, g_t\}$ *un insieme di polinomi non nulli in* A *e sia* $\mathcal{B}$ *un insieme omogeneo di generatori di* $\mathrm{Syz}(lt(g_1), \ldots, lt(g_t))$*. Allora* G *è una base di Gröbner se e solo se per ogni* $(h_1, \ldots, h_t) \in \mathcal{B}$ *si ha* $h_1g_1 + \ldots + h_tg_t \xrightarrow{G}_+ \underline{0}$.

Dimostrazione.

$\Rightarrow$ Se G è una base di Gröbner allora sappiamo che $h_1g_1 + \ldots + h_tg_t \xrightarrow{G}_+ \underline{0}$ in quanto $h_1g_1 + \ldots + h_tg_t \in \langle G \rangle$.

$\Leftarrow$ Sia $g \in \langle G \rangle$. Tra tutte le rappresentazioni di g del tipo

$$g = u_1g_1 + \ldots + u_tg_t \tag{1.3}$$

scegliamo quella con $X = \max_{1\le i\le t}\{lm(u_i)lm(g_i)\}$ minimo. Dal teorema di caratterizzazione delle basi di Gröbner basta provare che g può essere scritto come in 1.3 con $X = lm(g)$. Per assurdo supponiamo $lm(g) < X$ e proviamo che possiamo ottenere una rappresentazione del tipo 1.3 con valore minore di X. Sia $S = \{i \in \{1,\dots,t\} : lm(u_i)lm(g_i) = X\}$, così risulta $\sum_{i\in S} lt(u_i)lt(g_i) = 0$. Poniamo $\underline{h} = \sum_{i\in S} lt(u_i)\underline{e_i} \in A^t$, si ha così $\underline{h} \in \mathrm{Syz}(lt(g_1),\dots,lt(g_t))$ e inoltre $\underline{h}$ è omogeneo di grado X. Sia $\mathcal{B} = \{\underline{h_1},\dots,\underline{h_k}\} \subseteq A^t$[3], dove per ogni $j \in \{1,\dots,k\}$ poniamo $\underline{h_j} = (h_{1j},\dots,h_{tj})$, da cui $\underline{h} = \sum_{j=1}^k a_j\underline{h_j}$, con $a_j \in A$. Essendo $\underline{h}$ sizigia omogenea di grado X, espandendo gli a_i e sommando i termini simili, possiamo supporre che a_j siano termini tali che $lm(a_j)lm(h_{ij})lm(g_j) = X$. Per ipotesi, dato che per ogni $j \in \{1,\dots,k\}$ si ha $\underline{h_j} \in \mathcal{B}$, abbiamo $\sum_{i=1}^t h_{ij}g_j \xrightarrow{G}_+ \underline{0}$. Ne segue che possiamo scrivere

$$\sum_{i=1}^{t} h_{ij}g_j = \sum_{i=1}^{t} v_{ij}g_i$$

con v_{ij} tali che

$$\max_{1\le i\le t}\{lm(v_{ij})lm(g_i)\} = lm\left(\sum_{i=1}^{t} v_{ij}g_i\right) = lm\left(\sum_{i=1}^{t} h_{ij}g_i\right) < \max\{lm(h_i)lm(g_i)\},$$

in quanto, dal momento che $\underline{h}_j \in \mathcal{B}$, risulta $\sum_{i=1}^t h_{ij}lm(g_j) = 0$. Scriviamo

$$g = u_1g_1 + \ldots + u_tg_t = \sum_{i\in S} lt(u_i)g_i + \underbrace{\sum_{i\in S}(u_i - lt(u_i))g_i + \sum_{i\notin S} u_ig_i}_{\text{termini più piccoli di } X}.$$

Per quanto scritto finora si ha

$$\sum_{i\in S} lt(u_i)g_i = [g_1\dots g_t]\cdot\underline{h} = [g_1\dots g_t]\cdot\sum_{j=1}^{k} a_j\underline{h_j} = \sum_{j=i}^{k}\sum_{i=1}^{t} a_jh_{ij}g_i = \sum_{j=1}^{k}\sum_{i=1}^{t} a_jv_{ij}g_i.$$

Poiché $\max_{i,j}\{lm(a_j)lm(v_{ij})lm(g_i)\} < \max_{i,j}\{lm(a_j)lm(h_{ij})lm(g_i)\} = X$, ne segue che possiamo scrivere g come somma di termini minori di X, assurdo. $\square$

Adesso mostreremo come calcolare $\mathrm{Syz}(f_1,\dots,f_s)$ per $f_1,\dots,f_s \in A$. Sia $\{g_1,\dots,g_t\}$ una base di Gröbner per $(f_1,\dots,f_s)$, con g_i monici. Per $i \in \{1,\dots,t\}$, poniamo $lt(g_i) = X_i$ e per $i \ne j$ poniamo $X_{ij} = \mathrm{mcm}(X_i, X_j)$. Con questa notazione si ha che

$$S(g_i,g_j) = \frac{X_{ij}}{X_i}g_i - \frac{X_{ij}}{X_j}g_j.$$

Dal teorema di caratterizzazione della base di Gröbner sappiamo che $S(g_i,g_j) \xrightarrow{G}_+ \underline{0}$, quindi $S(g_i,g_j) = \sum_{v=1}^t h_{ijv}g_v$ con $h_{ijv} \in A$ tali che

$$\max_{1\le v\le t}\{lm(h_{ijv})lm(g_v)\} = lm\left(\sum_{v=1}^{t} h_{ijv}g_v\right) = lm(S(g_i,g_j)).$$

[3] $\mathrm{Syz}(lt(g_1),\dots,lt(g_t))$ è finitamente generato in quanto A^t è noetheriano.

I polinomi h_{ijv} sono ottenuti mediante l'algoritmo di divisione. Definiamo per $i, j \in \{1, \ldots, t\}$, $i \neq j$

$$\underline{s}_{ij} = \frac{X_{ij}}{X_i}\underline{e}_i - \frac{X_{ij}}{X_j}\underline{e}_j - (h_{ij1}, \ldots, h_{ijt}) \in A^t.$$

Risulta $\underline{s}_{ij} \in \mathrm{Syz}(g_1, \ldots, g_t)$ in quanto

$$\begin{aligned}[g_1 \ldots g_t] \cdot \underline{s}_{ij} = [g_1 \ldots g_t] \cdot \left(\frac{X_{ij}}{X_i}\underline{e}_i - \frac{X_{ij}}{X_j}\underline{e}_j\right) - [g_1 \ldots g_t] \cdot (h_{ij1}, \ldots, h_{ijt}) = \\ = S(g_i, g_j) - \sum_{v=1}^{t} h_{ijv} g_v = 0\end{aligned}$$

Teorema 1.10.7. *L'insieme* $\{\underline{s}_{ij} : 1 \leq i < j \leq t\}$ *è un insieme di generatori per* $\mathrm{Syz}(g_1, \ldots, g_t)$.

Dimostrazione. Supponiamo per assurdo che esista

$$(u_1, \ldots, u_t) \in \mathrm{Syz}(g_1, \ldots, g_t) \setminus \Big(\{\underline{s}_{ij} : 1 \leq i < j \leq t\}\Big)$$

e scegliamo $(u_1, \ldots, u_t)$ in modo tale che $X = \max_{1 \leq i \leq t}\{lm(u_i) lm(g_i)\}$ sia minimo. Sia $S = \{i \in \{1, \ldots, t\} : lm(u_i) lm(g_i) = X\}$. Per ogni $i \in \{1, \ldots, t\}$ definiamo

$$Y_i = \begin{cases} 0 & i \notin S \\ lt(u_i) & i \in S \end{cases}, \quad u'_i = u_i - Y_i.$$

Osserviamo che risulta $(Y_1, \ldots, Y_t) \in \mathrm{Syz}(X_1, \ldots, X_t)$. Dalla Proposizione 1.10.3 si ha

$$(Y_1, \ldots, Y_t) = \sum_{i<j} a_{ij} \left(\frac{X_{ij}}{X_i}\underline{e}_i - \frac{X_{ij}}{X_j}\underline{e}_j\right)$$

poiché ogni coordinata del vettore a sinistra è omogenea e poiché $Y_i X_i = X$, allora possiamo supporre a_{ij} un multiplo secondo una costante di $\frac{X}{X_{ij}}$. Risulta

$$\begin{aligned}(u_1, \ldots, u_t) = (Y_1, \ldots, Y_t) + (u'_1, \ldots, u'_t) = \sum_{i<j} a_{ij} \left(\frac{X_{ij}}{X_i}\underline{e}_i - \frac{X_{ij}}{X_j}\underline{e}_j\right) + (u'_1, \ldots, u'_t) = \\ = \sum_{i<j} a_{ij}\underline{s}_{ij} + (u'_1, \ldots, u'_t) + \sum_{i<j} a_{ij}(h_{ij1}, \ldots, h_{ijt}).\end{aligned}$$

Definiamo $(l_1, \ldots, l_t) = (u'_1, \ldots, u'_t) + \sum_{i<j} a_{ij}(h_{ij1}, \ldots, h_{ijt})$. Osserviamo che

$$(l_1, \ldots, l_t) = (u_1, \ldots, u_t) - \sum_{\substack{i<j \\ i,j \in S}} a_{ij}\underline{s}_{ij} \in \mathrm{Syz}(g_1, \ldots, g_t) \setminus \Big(\{\underline{s}_{ij} : 1 \leq i < j \leq t\}\Big).$$

Inoltre $lm(l_i) lm(g_i) < X$, contraddicendo la minimalità di X, infatti

$$\begin{aligned}&lm(u'_i) lm(g_i) < lm(u_i) lm(g_i) = X \\ &lm(a_{ij}) lm(h_{ijk}) lm(g_k) \leq \frac{X}{X_{ij}} \max_{1 \leq k \leq t}\{lm(h_{ijk}) lm(g_k)\} = \frac{X}{X_{ij}} lm(S(g_i, g_j)) < X. \qquad \square\end{aligned}$$

Siano $\{f_1, \ldots, f_s\} \subseteq A$ e $\{g_1, \ldots, g_t\}$ una base di Gröbner per $\{f_1, \ldots, f_s\}$. Poniamo

$$F = [f_1 \ldots f_s] \quad G = [g_1 \ldots g_t],$$

come visto in precedenza, esistono una matrice S di dimensione $t \times s$ e una matrice T di dimensione $s \times t$ ad elementi in A tali che

$$F = G \cdot S \quad G = F \cdot T.$$

Usando l'ultimo teorema calcoliamo $\{\underline{s}_1, \ldots, \underline{s}_s\}$ di generatori per $\mathrm{Syz}(G)$, si ha

$$0 = G\underline{s}_i = FT\underline{s}_i = F(T\underline{s}_i),$$

da cui $\langle T\underline{s}_i : i \in \{1, \ldots, r\}\rangle \subseteq \mathrm{Syz}(F)$. Inoltre, se I_s denota la matrice identità $s \times s$, allora

$$F(I_s - TS) = F - FTS = F - GS = F - F = 0.$$

Pertanto le colonne $\underline{r}_1, \ldots, \underline{r}_s$ di $I_s - TS$ stanno in $\mathrm{Syz}(F)$.

Teorema 1.10.8. *Risulta* $\mathrm{Syz}(f_1, \ldots, f_s) = \langle T\underline{s}_1, \ldots, T\underline{s}_r, \underline{r}_1, \ldots, \underline{r}_s\rangle$.

Dimostrazione.

- $\supseteq$ Vista in precedenza.
- $\subseteq$ Sia $\underline{s} = (a_1, \ldots, a_s) \in \mathrm{Syz}(f_1, \ldots, f_s)$, allora $0 = F\underline{s} = GS\underline{s}$, da cui $S\underline{s} \in \mathrm{Syz}(G)$, quindi $S\underline{s} = \sum_{i=1}^r h_i\underline{s}_i$, con $h_i \in A$, da cui $TS\underline{s} = T\sum_{i=1}^r h_i\underline{s}_i = \sum_{i=1}^r h_i(T\underline{s}_i)$. Otteniamo infine

$$\underline{s} = \underline{s} - TS\underline{s} + TS\underline{s} = (I_s - TS)\underline{s} + \sum_{i=1}^r h_i(T\underline{s}_i) =$$

$$= \sum_{i=1}^s a_i\underline{r}_i + \sum_{i=1}^r h_i(T\underline{s}_i) \in \langle T\underline{s}_1, \ldots, T\underline{s}_r, \underline{r}_1, \ldots, \underline{r}_s\rangle. \qquad \square$$