CAPITOLO VI. SOLUZIONI DI SISTEMI ED IDEALI

Questo capitolo è dedicato a richiami e anticipazioni.

1. VARIETÀ ALGEBRICHE AFFINI. VARIETÀ di un IDEALE

In maniera un po' semplicistica identifichiamo lo spazio affine di dimensione n sul campo k con l'insieme delle n-uple ordinate: $k^n = \{(c_1, \ldots, c_n), c_i \in k\}$.
Ogni polinomio $f \in \mathsf{A} = k[x_1, \ldots, x_n]$ può essere pensato come una funzione f: $k^n \to k$. Ci chiediamo in quali punti di k^n tale funzione si annulla. Si è già visto che, se k è infinito, tale funzione è identicamente nulla su k^n se e solo se è il polinomio nullo; ogni altro polinomio si annulla su un sottoinsieme più piccolo di k^n. Un siffatto sottoinsieme viene detto varietà algebrica affine. Più in generale,

DEFINIZIONE 1.1 Dato un insieme $\{f_1, \ldots, f_s\}$ di polinomi di A l'insieme

$$V(f_1, \ldots, f_s) = \{(c_1, \ldots, c_n) \in k^n \mid f_i(c_1, \ldots, c_n) = 0 \text{ per ogni } i=1,2,\ldots,s\}$$

delle soluzioni del sistema di equazioni algebriche:

$$f_1(x_1, \ldots, x_n) = 0, f_2(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0$$

è detto ***varietà algebrica affine*** definita da $f_1, \ldots, f_s$.

ESEMPI 1.2 Ci sono varietà algebriche affini vuote (o se si preferisce l'insieme vuoto è una varietà affine), ad esempio $V(x, x-1)$: infatti in qualunque campo lo zero è distinto dall'unità. Ci sono anche varietà affini che risultano vuote o non vuote a seconda del campo su cui si costruisce lo spazio affine: ad esempio $V(x^2+1)$ è vuota in $k^1=\mathbf{R}$, mentre è formata da due punti in $k^1=\mathbf{C}$.
Ci sono poi sottoinsiemi di k^n che non sono varietà algebriche affini (anzi sono la maggior parte): ad esempio $X=\{c \in \mathbf{R} \text{ con } c \neq 0\}$. Infatti se un polinomio si annulla su un insieme infinito di numeri reali è necessariamente il polinomio nullo, ma tra le soluzioni della corrispondente equazione algebrica c'è anche $c=0$, contro la descrizione di X [(1)].

Notiamo che, per definizione,

$$V(f_1, \ldots, f_s) = V(f_1) \cap \ldots \cap V(f_s).$$

Fin qui sembra che una varietà algebrica affine sia strettamente correlata con l'insieme dei polinomi di cui costituisce l'insieme degli zeri. In realtà è ovvio che se f è un polinomio dell'ideale $\langle f_1, \ldots, f_s \rangle$ ed $(c_1, \ldots, c_n)$ un punto di $V(f_1, \ldots, f_s)$ si ha $f(c_1, \ldots, c_n) = 0$, cioè

(*) se f appartiene a $\langle f_1, \ldots, f_s \rangle$, $V(f)$ contiene $V(f_1, \ldots, f_s)$.

Supponiamo allora che si abbia $\langle g_1, \ldots, g_t \rangle = \langle f_1, \ldots, f_s \rangle$. Per il ragionamento appena fatto ogni $V(g_i)$ contiene $V(f_1, \ldots, f_s)$, cioè $V(g_1, \ldots, g_t) = V(g_1) \cap \ldots \cap V(g_t) \supseteq V(f_1, \ldots, f_s)$. Il ragionamento simmetrico porta a concludere che $V(g_1, \ldots, g_t) = V(f_1, \ldots, f_s)$.
Quindi, non essendo importante la base scelta, si può a buon diritto parlare di ***varietà algebrica affine definita dall'ideale*** $\langle f_1, \ldots, f_s \rangle$.

Queste considerazioni hanno una ricaduta concreta: cercare le soluzioni di un sistema di equazioni algebriche significa cercare la varietà algebrica affine definita dai corrispondenti polinomi, ma visto che la varietà dipende esclusivamente dall'ideale generato da tali polinomi, si può sostituire al loro insieme una qualunque altra base (comoda) dell'ideale.

---

(1) Attenzione: X sarebbe stata una varietà se avessimo considerato uno spazio affine, invece che sul campo reale, su un campo finito.

Possiamo notare infine che ogni ideale I di $\mathbf{A}$ ha base finita (teorema della base di Hilbert) e quindi ad ogni ideale I è associata una varietà algebrica affine $V(\mathrm{I})$ che chiameremo ***varietà dell'ideale*** I.

In questo modo si definisce una corrispondenza

$$V\text{: Ideali di } \mathbf{A} \;\rightarrow\; \text{Varietà algebriche affini}$$

che trasforma il reticolo degli ideali in quello delle varietà come illustrato dalle seguenti

PROPRIETÀ 1.3 Per ogni ideale I si ha $(0) \subseteq \mathrm{I} \subseteq \mathbf{A}$; corrispondentemente

a) $V(0) = k^n$, e $V(\mathbf{A}) = \varnothing$, poiché $\mathbf{A}$ contiene il polinomio 1.

b) Siano I e J due ideali di $\mathbf{A}$. $\mathrm{J} \subseteq \mathrm{I}$ implica $V(\mathrm{J}) \supseteq V(\mathrm{I})$: basta applicare (*) agli elementi di una base di J, pensando $\mathrm{I} = \langle f_1, \ldots, f_s \rangle$.

c) Dati due ideali $\mathrm{I} = \langle f_1, \ldots, f_s \rangle$ e $\mathrm{J} = \langle g_1, \ldots, g_t \rangle$, risulta

- $V(\mathrm{I}+\mathrm{J}) = V(\mathrm{I}) \cap V(\mathrm{J})$, poiché una base di I+J è data da $\{f_1, \ldots, f_s, g_1, \ldots, g_t\}$;
- $V(\mathrm{I} \cap \mathrm{J}) = V(\mathrm{I} \cdot \mathrm{J}) = V(\mathrm{I}) \cup V(\mathrm{J})$, ove I·J è l'ideale generato dai prodotti $f_i g_j$ $(i = 1, \ldots, s; j = 1, \ldots, t)$ dei generatori dei due ideali (detto ***ideale prodotto*** di I e J [(2)]).
  Infatti, da $\mathrm{I} \cdot \mathrm{J} \subseteq \mathrm{I} \cap \mathrm{J} \subseteq \mathrm{I}$ e $\mathrm{I} \cdot \mathrm{J} \subseteq \mathrm{I} \cap \mathrm{J} \subseteq \mathrm{J}$ si deduce $V(\mathrm{I} \cdot \mathrm{J}) \supseteq V(\mathrm{I} \cap \mathrm{J}) \supseteq V(\mathrm{I}) \cup V(\mathrm{J})$.
  Viceversa, se $(c_1, \ldots, c_n) \in V(\mathrm{I} \cdot \mathrm{J})$ o $f_i(c_1, \ldots, c_n) = 0$ per tutti gli i e allora $(c_1, \ldots, c_n) \in V(\mathrm{I})$ oppure per un certo i risulta $f_i(c_1, \ldots, c_n) \neq 0$; in tal caso, dovendo essere $f_i g_j(c_1, \ldots, c_n) = 0$ per ogni j, deve risultare $g_j(c_1, \ldots, c_n) = 0$ per ogni indice j e quindi $(c_1, \ldots, c_n) \in V(\mathrm{J})$ per cui $V(\mathrm{I}) \cup V(\mathrm{J}) \supseteq V(\mathrm{I} \cdot \mathrm{J})$.
  Dunque $V(\mathrm{I}) \cup V(\mathrm{J}) \supseteq V(\mathrm{I} \cdot \mathrm{J}) \supseteq V(\mathrm{I} \cap \mathrm{J}) \supseteq V(\mathrm{I}) \cup V(\mathrm{J})$: che è la tesi.

2. IDEALE DI UNA VARIETÀ

Sia X un sottoinsieme di k^n. L'insieme $\{f \in \mathbf{A} \mid f(c_1, \ldots, c_n) = 0 \;\forall\; (c_1, \ldots, c_n) \in \mathrm{X}\}$ dei polinomi di $\mathbf{A}$ che si annullano su tutti i punti di X è un ideale di $\mathbf{A}$: esso sarà denotato con $I(\mathrm{X})$.
Se X è una varietà algebrica affine V si dirà che

$$I(\mathrm{V}) = \{f \in \mathbf{A} \mid f(c_1, \ldots, c_n) = 0 \text{ per tutti i punti } (c_1, \ldots, c_n) \in \mathrm{V}\}$$

è l'***ideale della varietà*** V.

ESEMPI 2.1

i) Se $\mathrm{V} = \{(0,0)\} \subseteq k^2$, allora $I(\mathrm{V}) = \langle x, y \rangle$. Infatti un polinomio $a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \ldots$ si annulla in $x = 0$ e $y = 0$ se e solo se $a_{00} = 0$ e in questo caso il polinomio si riscrive come $x(a_{10} + a_{20}x + a_{11}y + \ldots) + y(a_{01} + a_{02}y + \ldots)$, cioè il polinomio sta in $\langle x, y \rangle$.

ii) Se $\mathrm{V} = k^n$ e k è infinito: $I(k^n) = (0)$. Ma se k non è infinito la cosa non è vera: ad esempio in $k^1 = \mathbf{Z}_2$, si ha $I(k^1) = \langle x(x+1) \rangle$.

Anche in questo caso resta definita una corrispondenza

$$I\text{: Varietà algebriche affini} \;\rightarrow\; \text{Ideali di } \mathbf{A}$$

che trasforma il reticolo delle varietà in quello degli ideali come illustrato dalle seguenti

PROPRIETÀ 2.2 Per ogni varietà V si ha $\varnothing \subseteq \mathrm{V} \subseteq k^n$; corrispondentemente

a) $I(\varnothing) = \mathbf{A}$.

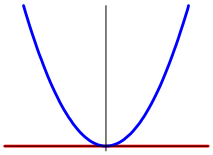
b) Siano V, W due varietà algebriche affini: $\mathrm{V} \subseteq \mathrm{W}$ implica $I(\mathrm{V}) \supseteq I(\mathrm{W})$.
Infatti ogni polinomio f che si annulla su tutti i punti di W si annulla in particolare sui punti di V.
Più in generale, dati due insiemi X e Y, $\mathrm{X} \subseteq \mathrm{Y}$ implica $I(\mathrm{X}) \supseteq I(\mathrm{Y})$.

---

(2) Attenzione: l'ideale prodotto non coincide con l'intersezione. Basta osservare che se $\mathrm{I} = \mathrm{J} = \langle x \rangle$ si ha ovviamente $\mathrm{I} \cap \mathrm{J} = \mathrm{I}$, mentre $\mathrm{I} \cdot \mathrm{J} = \langle x^2 \rangle$, oppure ricordare che (vedi Capitolo V § 12) il generatore dell'intersezione di due ideali principali è il mcm (che in generale non coincide con il prodotto) dei loro generatori.

c) Siano V, W due varietà algebriche affini: $I(V \cup W) = I(V) \cap I(W)$.
Infatti $I(V \cup W) \subseteq I(V) \cap I(W)$, per la parte **(b)**; viceversa se f si annulla sui punti di V e su quelli di W si annulla sui punti di $V \cup W$.

d) $I(V \cap W) \supseteq I(V) + I(W)$, per la parte **(b),** ma non è vero in generale che sia $I(V \cap W) = I(V) + I(W)$.



Ad esempio consideriamo in k^2 le due varietà $V=V(y)$ e $W=V(x^2-y)$ (che in figura rappresentiamo per comodità come varietà di $\mathbf{R}^2$). Risulta $I(V) = \langle y \rangle$ e $I(W) = \langle x^2 - y \rangle$ e quindi

$$I(V) + I(W) = \langle x^2 - y, y \rangle = \langle x^2, y \rangle;$$

ma essendo $V \cap W = \{(0,0)\}$, l'ideale $I(V \cap W)$ è $\langle x, y \rangle$.

Vediamo quali legami ci sono tra le due corrispondenze V e I.

ESEMPIO 2.3 Se $V = V(y - x^2, z - x^3)$ e k è infinito, allora $I(V) = \langle y - x^2, z - x^3 \rangle$.
Infatti dividendo $f \in I(V)$ per $(y - x^2, z - x^3)$ (che è una base di Gröbner rispetto a LEX con $y>z>x$) risulta $f = (y - x^2)\, p + (z - x^3)\, q + r$ ove il resto r dipende esclusivamente da x: ora questo resto è nullo poiché tra i punti di V ci sono sicuramente quelli della forma (t, t^2, t^3) e $f(t, t^2, t^3) = r(t) = 0$ per ogni $t \in k$ implica che r è il polinomio nullo.

Il caso prospettato da questo esempio non è però generale. Cioè non è sempre vero che $I(V(I)) = I$: ad esempio $V(\langle x^2, y \rangle) = (0,0)$ e quindi $I(V(\langle x^2, y \rangle)) = \langle x, y \rangle$. In generale si può dire che

OSSERVAZIONI 2.4

a) $I(V(I)) \supseteq I$: infatti per definizione di $V(I)$ i polinomi di I si annullano su $V(I)$.

b) $V(I(V)) = V$: l'inclusione $\supseteq$ vale per definizione; viceversa se $V = V(f_1, \ldots, f_s) = V(I)$ si ha, per **(a)** $I(V(I)) \supseteq I$ e quindi, per la proprietà **1.3 (b)**, $V(I(V(I))) \subseteq V(I) = V$.

c) $I(V(I(V))) = I(V)$ e $V(I(V(I))) = V(I)$: entrambe le uguaglianze si desumono da $V(I(V)) = V$, la prima calcolando l'ideale delle due varietà, la seconda sostituendo $V=V(I)$.

d) Date due varietà algebriche affini V, W si ha $V \subseteq W$ se e solo se $I(V) \supseteq I(W)$.
Un'implicazione è stata provata nelle proprietà **2.2 (b)**; viceversa se $I(V) \supseteq I(W)$ per la proprietà **1.3 (b)** risulta $V(I(V)) \subseteq V(I(W))$ inoltre per **(b)** $V(I(V)) = V$ e analogamente su W: quindi $V \subseteq W$.

Invece, non essendo sempre vero che $I(V(I)) = I$, non si può affermare che se $V(I) \supseteq V(J)$ allora $I \subseteq J$: lo si può verificare sugli ideali $I = \langle x^2, y \rangle$ e $J = \langle x, y^2 \rangle$ che hanno la stessa varietà affine.

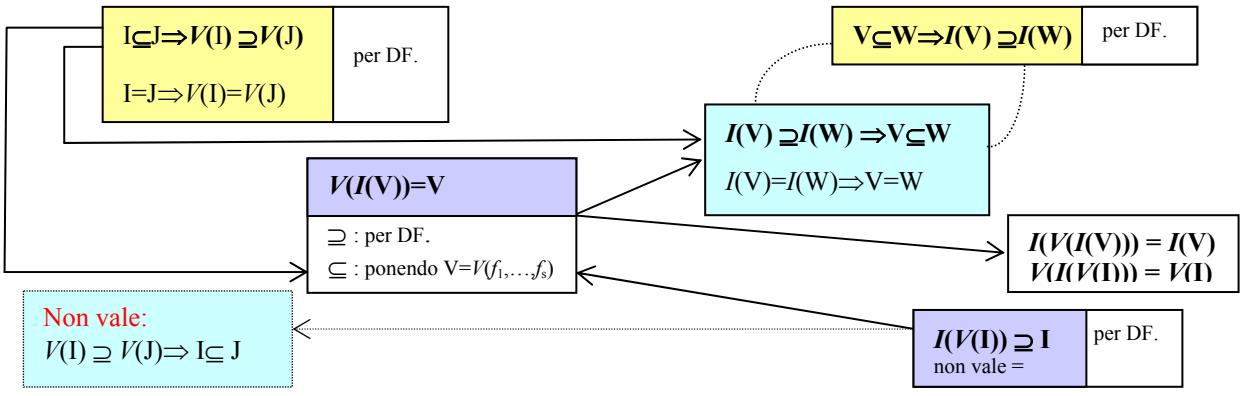
In totale quindi ci sono due corrispondenze, con comportamento non del tutto simmetrico

V: Ideali di $\mathbb{A} \rightarrow$ Varietà algebriche affini

I: Varietà algebriche affini $\rightarrow$ Ideali di $\mathbb{A}$

che danno una traduzione geometrica dei concetti algebrici e viceversa.

MAPPA LOGICA DELLE PROPRIETÀ FINORA ESPOSTE
(in caselle di ugual colore: proprietà dello stesso genere relative alle due corrispondenze).



Abbiamo osservato nel primo paragrafo che ci sono sottoinsiemi X di k^n che non sono varietà algebriche (affini).

DEFINIZIONE 2.5 *Si dice* ***chiusura di Zariski*** *di un sottoinsieme* X *di* k^n *la più piccola varietà algebrica affine di* k^n *che contiene* X.

È interessante osservare che proprio le due corrispondenze appena introdotte permettono di costruire la chiusura di Zariski di X. Vale infatti la seguente

OSSERVAZIONE 2.6 *La varietà affine* $V = V(I(X))$ *dell'ideale*

$$I(X) = \{f \in \mathbf{A} \mid f(c_1, \ldots, c_n) = 0 \ \forall \ (c_1, \ldots, c_n) \in X\}$$

è la più piccola varietà affine contenente X. *Inoltre l'ideale* $I(V)$ *di tale varietà coincide con* $I(X)$.

Infatti, se W è una varietà contenente X, l'ideale $I(X)$ dei polinomi che si annullano su X contiene $I(W)$ e quindi $V(I(X))$ è contenuta in $V(I(W)) = W$: ciò prova che $V = V(I(X))$ è la chiusura di Zariski di X.
Invece si vede che $I(V) = I(X)$, notando che, per la proprietà 2.2 (b), $I(X) \supseteq I(V)$ e viceversa, per l'osservazione 2.4 (a), $I(X) \subseteq I(V(I(X))) = I(V)$.

SISTEMI DI EQUAZIONI ALGEBRICHE

I problemi legati alla soluzione dei sistemi di equazioni algebriche si possono vedere come le generalizzazioni di analoghi problemi incontrati in algebra lineare a proposito della soluzione di sistemi di equazioni lineari. Essi sono:

i) (CONSISTENZA) il sistema

$$f_1(x_1, \ldots, x_n) = 0, f_2(x_1, \ldots, x_n) = 0, \ \ldots \ , f_s(x_1, \ldots, x_n) = 0$$

ha soluzione? Cioè, la varietà algebrica $V(f_1, \ldots, f_s)$ è non vuota? La risposta dipende anche dal campo su cui si lavora.

ii) (FINITEZZA) il sistema ha un numero finito di soluzioni? Cioè, la varietà algebrica $V(f_1, \ldots, f_s)$ è costituita da un insieme finito di punti? È possibile stimare quanti sono? E come si calcolano?

iii) (DIMENSIONE) se le soluzioni non sono in numero finito, quanto è grande l'insieme delle soluzioni? È possibile definire un concetto di dimensione di una varietà algebrica analogo a quello di dimensione di spazio delle soluzioni noto dall'algebra lineare? È possibile (o comunque che cosa significa) esprimere parametricamente le soluzioni?

iv) (DETERMINAZIONE SOLUZIONI) se le soluzioni ci sono, come si calcolano?

Si arriverà alla soluzione di questi problemi in due passaggi:

- la teoria dell'eliminazione ci darà un metodo per "calcolare" le soluzioni (e strumenti teorici da usare successivamente)
- il Nullstellensatz darà risposte al problema della consistenza e della stima del numero di soluzioni.

In termini di soluzioni di sistemi, il fatto che $V(I) = V(J)$ non implichi $I = J$ può essere interpretato così:
le soluzioni di un sistema possono essere soluzioni anche di un sistema diverso e di un sistema più restrittivo (con "più" equazioni).

Diamo un'idea di come funziona il metodo di eliminazione delle incognite ed estensione delle soluzioni su qualche esempio: la corrispondente teoria sarà oggetto del capitolo VII.

ESEMPIO 3.1 Cerchiamo le soluzioni di

$$\begin{cases} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{cases}.$$

Spontaneamente sottrarremmo la seconda equazione dalla prima ottenendo un'equazione in y e nella seconda sostituiremmo z al posto di x pervenendo al sistema

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

in cui la prima equazione contiene solo l'incognita y, la seconda contiene la y e la z e la terza potrebbe anche contenere tutte e 3 le incognite. Risolta la prima equazione: $y = \frac{-1 \pm \sqrt{5}}{2}$, la seconda si risolve sostituendo: $z = \pm\frac{1}{2}\sqrt{-1 \pm \sqrt{5}}$ e la terza pure. Così in $\mathbf{C}^3$ si trovano le quattro soluzioni

$$\left(\frac{1}{2}\sqrt{-1+\sqrt{5}}, \frac{-1+\sqrt{5}}{2}, \frac{1}{2}\sqrt{-1+\sqrt{5}}\right), \left(-\frac{1}{2}\sqrt{-1+\sqrt{5}}, \frac{-1+\sqrt{5}}{2}, -\frac{1}{2}\sqrt{-1+\sqrt{5}}\right)$$
$$\left(\frac{1}{2}\sqrt{-1-\sqrt{5}}, \frac{-1-\sqrt{5}}{2}, \frac{1}{2}\sqrt{-1-\sqrt{5}}\right), \left(-\frac{1}{2}\sqrt{-1-\sqrt{5}}, \frac{-1-\sqrt{5}}{2}, -\frac{1}{2}\sqrt{-1-\sqrt{5}}\right).$$

Quanto abbiamo fatto corrisponde a:

- introdurre in $\mathbf{C}[x, y, z]$ l'ordinamento LEX con $x > z > y$
- trovare una base di Gröbner dell'ideale $I = \langle x^2 + y^2 + z^2 - 1,\ x^2 + z^2 - y,\ x - z \rangle$. Abbiamo verificato che questa operazione restituisce una base, $\{x - z,\ 2z^2 - y,\ y^2 + y - 1\}$, in cui da un certo punto in poi manca la prima incognita e da un altro punto in poi manca la seconda: si esprime questo fatto dicendo che l'ordinamento LEX è un ordinamento di eliminazione. [3] Ciò permette di
- risolvere il sistema partendo dall'equazione nella sola ultima incognita; sostituire ogni soluzione c_3 di tale equazione nell'equazione contenente solo le ultime due incognite, ottenendo, per ogni soluzione sostituita, un'equazione nella sola penultima incognita, ciascuna eventuale soluzione c_2 del quale va aggregata a c_3 formando la coppia (c_2, c_3) e così via estendendo.

Geometricamente abbiamo ricondotto il problema di trovare l'intersezione di 3 superficie di $\mathbf{C}^3$ (una sfera, un paraboloide ellittico e un piano) a un problema in dimensione 1; poi abbiamo esteso queste soluzioni in dimensione 2, leggendo $y = \frac{-1 \pm \sqrt{5}}{2}$ come le equazioni di due rette in $\mathbf{C}^2$ da intersecare con la parabola $2z^2 - y = 0$; infine abbiamo esteso queste soluzioni in dimensione 3, leggendo ad esempio

$$y = \frac{-1+\sqrt{5}}{2}, \quad z = \frac{1}{2}\sqrt{-1+\sqrt{5}}$$

come le equazioni di una retta in $\mathbf{C}^3$ da intersecare con il piano $x - z = 0$.

In generale la strategia di eliminazione non è così immediata: ma si può sempre far riferimento all'ordinamento LEX per eliminare via via le variabili. I problemi più grossi vengono posti dal passo di estensione, poiché può succedere che una soluzione non possa essere estesa alla dimensione superiore in quanto in contrasto con le equazioni delle varietà che ivi si dovrebbero intersecare.

---

[3] Verificare che se si usa sempre l'ordinamento LEX ma con $x>y>z$ la base diventa $\{x - z, y - 2z^2, 4z^4 + 2z^2 - 1\}$: questo mette in evidenza già dalla prima equazione la differenza di soluzione tra campo complesso e campo reale.

ESEMPIO 3.2 Risolvendo il sistema dato dalle due equazioni: $xy = 1$, $xz = 1$ con il metodo di eliminazione (LEX con $x > y > z$) si trova la base di Gröbner $\{xy - 1, y - z\}$. Ora $V(y - z)$ in $\mathbf{C}^2$ è costituito da tutte le coppie (c, c), con c complesso. Ma la soluzione che nasce ponendo $c = 0$ non può essere estesa a $\mathbf{C}^3$ poiché l'equazione $x \cdot 0 = 1$ non ha soluzione; in termini geometrici: l'asse x ($y = z = 0$) non interseca la varietà $V(xy - 1)$.

Si può utilmente guardare (Cox, Cap. II, §8 esempio 3) anche l'esempio relativo alla soluzione del sistema

$$\begin{aligned} 3x^2 + 2yz - 2xt &= 0 \\ 2xz - 2yt &= 0 \\ 2xy - 2z - 2zt &= 0 \\ x^2 + y^2 + z^2 - 1 &= 0 \end{aligned}$$

che mostra come la base di Gröbner che nasce dal processo di eliminazione è spesso molto brutta.
Su questo esempio si può anche fare qualche conto sul numero di soluzioni (vedi prossimo paragrafo).

3. SUL NUMERO DI SOLUZIONI DI UN SISTEMA

Vedremo che il fatto che un sistema algebrico

$$f_1(x_1, \ldots, x_n) = 0, f_2(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0$$

non abbia un insieme infinito di soluzioni è legato al fatto che al di fuori dall'ideale dei LT dei polinomi di $I = \langle f_1, \ldots, f_s \rangle$ rimanga solo un numero finito di monomi.

Proveremo infatti, utilizzando il Nullstellensatz (debole e di Hilbert, vedi Capitolo VIII) e quindi ipotizzando che k sia un campo algebricamente chiuso, che:
la varietà affine $V = V(I)$ di k^n è finita (cioè il sistema ha un numero finito di soluzioni o non ha soluzioni) se e solo se, detta G una base di Gröbner di I (rispetto a un ordinamento monomiale arbitrario ma fissato), per ogni $i \in \{1, 2, \ldots, n\}$ esiste una potenza $x_i^{m_i}$ appartenente all'insieme dei LT di G e in tal caso il numero di punti di V è al massimo $m_1 \cdot \ldots \cdot m_n$.

Si noti che questo enunciato costituisce una generalizzazione di quanto noto per i sistemi lineari, che hanno un numero finito di soluzioni se e solo se la varietà affine è costituita da un solo punto; ciò si verifica se e solo se, una volta passati alla base di Gröbner ridotta (rispetto a LEX) dell'ideale (cioè al sistema ridotto di Gauss) ci sono tante equazioni quante incognite e quindi ogni generatore presenta come LT una diversa incognita (in questo caso l'esponente è 1).

Per giungere al risultato è opportuno cercare un modo conveniente di rappresentare gli elementi dell'anello quoziente $\mathbf{A}/I$ ove I è un ideale dell'anello dei polinomi $\mathbf{A}$.
Sappiamo che un polinomio f appartiene a I se e solo se, detta G una base di Gröbner di I (rispetto a un ordinamento monomiale arbitrario) si ha $f^G = 0$.
In particolare se $LT(f)$ non appartiene a $\langle LT(G) \rangle$, cioè non è divisibile per il LT di alcuno dei polinomi della base di Gröbner G, sicuramente f non appartiene a I.

ESEMPIO 3.1 Sia $I = \langle xz - y^2, x^3 - z^2 \rangle$. La corrispondente base G (rispetto a grLEX $x > y > z$) è $\{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}$. Il polinomio $f = -4x^2y^2z^2 + y^6 + 3z^5 = -4z^2(x^2y^2 - z^3) + (y^6 - z^5)$ sta in I, mentre il polinomio $f = -x^2y + z$ non appartiene a I poiché $-x^2y$ non è divisibile per xz né per x^3 né per x^2y^2 né per xy^4 né per y^6.

L'algoritmo per stabilire se un polinomio appartiene ad I può essere utilizzato per

- stabilire se una differenza di polinomi $f - g$ appartiene ad I,

cioè

- stabilire se i due laterali $f + \mathrm{I}$ e $g + \mathrm{I}$ coincidono,

vale a dire

- identificare rappresentanti diversi di uno stesso elemento $f + \mathrm{I}$ dell'anello quoziente $\mathbf{A}/\mathrm{I}$

e quindi

- trovare un rappresentante privilegiato per ciascun elemento di $\mathbf{A}/\mathrm{I}$.

Infatti, detta G una base di Gröbner di I (rispetto a un ordinamento monomiale arbitrario ma fissato), *ogni elemento* $f + \mathrm{I}$ *di* $\mathbf{A}/\mathrm{I}$ *può essere rappresentato* come $f^{\mathrm{G}} + \mathrm{I}$, ove f^{G} è il resto di f nella divisione per G, cioè *mediante un polinomio che è combinazione k-lineare di monomi che non stanno nell'ideale* $\langle \mathrm{LT}(\mathrm{I}) \rangle$. D'altra parte, *due polinomi* r *ed* r' *di questo tipo, aventi almeno un coefficiente diverso, rappresentano due diversi elementi di* $\mathbf{A}/\mathrm{I}$, *poiché* $r - r'$ *non appartiene a* I.

PROPOSIZIONE 3.2 *La corrispondenza* φ *tra* $\mathbf{A}/\mathrm{I}$ *e l'insieme* S *dei polinomi che sono combinazione k-lineare di monomi non appartenenti a* $\langle \mathrm{LT}(\mathrm{I}) \rangle$ *definita da* $\varphi(f + \mathrm{I}) = f^{\mathrm{G}}$ *è un isomorfismo di spazi vettoriali su k. Questa corrispondenza è anche un isomorfismo di anelli, pur di definire in* S *il prodotto* $*$ *come* $f^{\mathrm{G}} * g^{\mathrm{G}} = (f^{\mathrm{G}} \cdot g^{\mathrm{G}})^{\mathrm{G}}$.

Dimostrazione Osserviamo che, per come è definito, S è uno spazio vettoriale su k, rispetto all'ordinaria somma di polinomi e al loro prodotto per un elemento di k [(4)]. Circa la corrispondenza φ: $\mathbf{A}/\mathrm{I} \to \mathrm{S}$, si è appena visto che è biunivoca. Inoltre se $f + \mathrm{I} = f^{\mathrm{G}} + \mathrm{I}$ e $g + \mathrm{I} = g^{\mathrm{G}} + \mathrm{I}$ sono elementi di $\mathbf{A}/\mathrm{I}$ e a, b elementi di k

$$a(f^{\mathrm{G}} + \mathrm{I}) + b(g^{\mathrm{G}} + \mathrm{I}) = (af^{\mathrm{G}} + bg^{\mathrm{G}}) + \mathrm{I} = (af + bg)^{\mathrm{G}} + \mathrm{I}$$

dato che nessuno dei termini che compaiono in $(af^{\mathrm{G}} + bg^{\mathrm{G}})$ è divisibile per uno dei LT dei polinomi di I. Ciò prova che φ è un isomorfismo di spazi vettoriali; che lo sia anche di anelli è insito nella definizione del prodotto $*$. C.V.D.

È ovvio che *i monomi* $\boldsymbol{x}^{\alpha}$ *che non stanno in* $\langle \mathrm{LT}(\mathrm{I}) \rangle$ *costituiscono una base per il k-spazio vettoriale* S e quindi i loro corrispondenti $\boldsymbol{x}^{\alpha} + \mathrm{I}$ in $\mathbf{A}/\mathrm{I}$ costituiscono un insieme linearmente indipendente che genera l'intero k-spazio vettoriale $\mathbf{A}/\mathrm{I}$: dunque l'insieme dei monomi che non stanno in $\langle \mathrm{LT}(\mathrm{I}) \rangle$ ha cardinalità pari alla dimensione $\dim_k(\mathbf{A}/\mathrm{I})$ del k-spazio vettoriale $\mathbf{A}/\mathrm{I}$. Poiché $\dim_k(\mathbf{A}/\mathrm{I})$ è un attributo intrinseco dello spazio vettoriale, se ne deduce una conseguenza sorprendente: *se i monomi che non stanno in* $\langle \mathrm{LT}(\mathrm{I}) \rangle$ *sono in numero finito*, *tale numero non dipende dall'ordinamento monomiale scelto*.

---

(4) Invece (S, +, $*$) è un anello: che sia commutativo con unità coincidente con quella di $\mathbf{A}$ è ovvio. Inoltre, se f, g, h stanno in S, esistono i, j, i', j' in I tali che:

$$(f \cdot g) \cdot h = [(f \cdot g)^{\mathrm{G}} + i] \cdot h = (f \cdot g)^{\mathrm{G}} \cdot h + i \cdot h = [(f \cdot g)^{\mathrm{G}} \cdot h]^{\mathrm{G}} + j + i \cdot h$$

$$f \cdot (g \cdot h) = f \cdot [(g \cdot h)^{\mathrm{G}} + i'] = f \cdot (g \cdot h)^{\mathrm{G}} + f \cdot i' = [f \cdot (g \cdot h)^{\mathrm{G}}]^{\mathrm{G}} + j' + f \cdot i'$$

e, visto che $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ appartiene ad entrambi i laterali $[(f \cdot g)^{\mathrm{G}} \cdot h]^{\mathrm{G}} + \mathrm{I}$ e $[f \cdot (g \cdot h)^{\mathrm{G}}]^{\mathrm{G}} + \mathrm{I}$, i polinomi di S ad essi associati, cioè $[(f \cdot g)^{\mathrm{G}} \cdot h]^{\mathrm{G}}$ e $[f \cdot (g \cdot h)^{\mathrm{G}}]^{\mathrm{G}}$, devono coincidere. Quindi

$$(f * g) * h = [(f \cdot g)^{\mathrm{G}} \cdot h]^{\mathrm{G}} = [f \cdot (g \cdot h)^{\mathrm{G}}]^{\mathrm{G}} = f * (g * h),$$

cioè vale la proprietà associativa. Analogamente, esistono i, i', j' in I tali che:

$$(f + g) \cdot h = [(f + g) \cdot h]^{\mathrm{G}} + i$$

$$(f \cdot h) + (g \cdot h) = [(f \cdot h)^{\mathrm{G}} + i'] + [(g \cdot h)^{\mathrm{G}} + j'] = (f \cdot h)^{\mathrm{G}} + (g \cdot h)^{\mathrm{G}} + i' + j'$$

e, visto che $(f + g) \cdot h = (f \cdot h) + (g \cdot h)$ appartiene ad entrambi i laterali $[(f + g) \cdot h]^{\mathrm{G}} + \mathrm{I}$ e $(f \cdot h)^{\mathrm{G}} + (g \cdot h)^{\mathrm{G}} + \mathrm{I}$, i polinomi di S ad essi associati, cioè $[(f + g) \cdot h]^{\mathrm{G}}$ e $(f \cdot h)^{\mathrm{G}} + (g \cdot h)^{\mathrm{G}}$, devono coincidere. Quindi

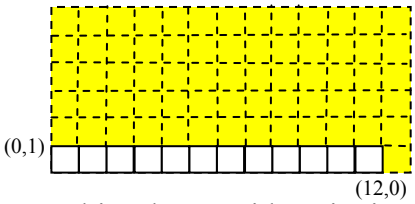
$$(f + g) * h = [(f + g) \cdot h]^{\mathrm{G}} = (f \cdot h)^{\mathrm{G}} + (g \cdot h)^{\mathrm{G}} = (f * h) + (g * h),$$

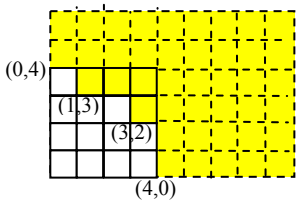
cioè vale la proprietà distributiva.

Ad esempio, l'ideale $I = \langle xy^3 - x^2, x^3y^2 - y\rangle$ di $k[x, y]$ rispetto a

- LEX ($y > x$) ha base di Gröbner $\langle y - x^7, x^{12} - x^2\rangle$ e quindi $\langle LT(I)\rangle = \langle y, x^{12}\rangle$
  mentre rispetto a
- grLEX ($x > y$) ha base di Gröbner $\langle x^4 - y^2, xy^3 - x^2, y^4 - xy, x^3y^2 - y\rangle$ e quindi $\langle LT(I)\rangle = \langle x^4, xy^3, y^4, x^3y^2\rangle$

ma in entrambi i casi i monomi che non appartengono a $\langle LT(I)\rangle$ sono 12, come è evidente dalle due rappresentazioni grafiche dei multigradi dei LT generatori in $\mathbf{N}^2$:





Applichiamo subito le considerazioni sulla dimensione dello spazio vettoriale quoziente per dimostrare l'ultima implicazione del teorema di finitezza che segue.

TEOREMA 3.3 *Sia k un campo algebricamente chiuso e* $V = V(I)$ *una varietà algebrica affine di* k^n. *Sono equivalenti le condizioni*:

i) *la varietà affine* $V = V(I)$ *di* k^n *è finita*

ii) *comunque si fissi l'ordinamento monomiale in* $k[x_1,\ldots, x_n]$, *per ogni* $i \in \{1, 2, \ldots, n\}$ *esiste una potenza* $x_i^{m_i}$ *appartenente a* $\langle LT(I)\rangle$

iii) *lo spazio vettoriale* S *ha dimensione finita*

iv) *lo spazio vettoriale* $k[x_1,\ldots, x_n]/I$ *ha dimensione finita.*

Dimostrazione L'equivalenza di (iii) e (iv) dipende dal fatto che i due spazi vettoriali sono isomorfi. Resta quindi da provare (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) e (iv) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii) Per dimostrare questa implicazione è necessaria l'ipotesi k algebricamente chiuso!
Dimostriamo l'affermazione in due passi. Se V è vuota, per il Nullstellensatz debole, l'ideale I contiene l'unità di $k[x_1,\ldots, x_n]$; ma $1 = x_i^0$ per ogni $i \in \{1, 2, \ldots, n\}$ e quindi vale la condizione (ii).
Se V non è vuota ed è formata da h punti, $\mathbf{c}_1 = (c_{11},\ldots, c_{1n})$, … , $\mathbf{c}_h = (c_{h1},\ldots, c_{hn})$, per ogni $i \in \{1, 2, \ldots, n\}$ consideriamo il polinomio $f = (x_i - c_{1i}) \cdot \ldots \cdot (x_i - c_{hi})$. Esso si annulla in tutti i punti di V e quindi per il Nullstellensatz di Hilbert esiste una sua potenza intera f^{r_i} che appartiene a I; d'altra parte, in qualunque ordinamento, $LT(f) = x_i^h$ e quindi $\langle LT(I)\rangle$ contiene $LT(f^{r_i}) = x_i^{hr_i}$.

(ii) $\Rightarrow$ (iii) Se, per ogni $i \in \{1, 2, \ldots, n\}$, $x_i^{m_i}$ è la più piccola potenza di x_i che appartiene a $\langle LT(I)\rangle$, in ogni monomio $x_1^{\alpha_1}x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ non appartenente a $\langle LT(I)\rangle$ l'indeterminata x_i deve comparire con grado inferiore a m_i: quindi le n-uple ordinate $(\alpha_1,\ldots, \alpha_n)$ di esponenti che corrispondono ai monomi base dello spazio vettoriale S possono essere scelte in al più $m_1 \cdot \ldots \cdot m_n$ modi diversi.

(iv) $\Rightarrow$ (i) Consideriamo una delle indeterminate, x_i, e l'insieme $\{x_i^j + I, j \in \mathbf{N}\}$ dei laterali di I mediante le sue potenze. Se $\boldsymbol{A}/I = k[x_1, \ldots, x_n]/I$ ha dimensione finita, tale insieme è dipendente, in quanto formato da infiniti elementi e quindi lo zero I dello spazio vettoriale $\boldsymbol{A}/I$ può essere scritto come una combinazione lineare finita di tali laterali, cioè esistono $r + 1$ coefficienti non tutti nulli $a_0, a_1, \ldots, a_r$ in k tali che $I = a_0(x_i^0 + I) + a_1(x_i^1 + I) + \ldots + a_r(x_i^r + I) = (a_0 + a_1 x_i + \ldots + a_r x_i^r) + I$, cioè tali che $f_i(x_i) = a_0 + a_1 x_i + \ldots + a_r x_i^r \in I$: dunque, per ogni $i \in \{1, 2, \ldots, n\}$, $V(I)$ è contenuto in $V(f_i(x_i))$. D'altra parte, essendo f_i un polinomio non nullo in una sola indeterminata, l'equazione $f_i(x_i) = 0$ ha un numero finito di soluzioni (eventualmente nessuna) $x_i = c_{i1}, \ldots, x_i = c_{ih_i}$, che in k^n rappresentano altrettanti iperpiani che sono gli unici della forma $x_i = costante$ sui quali si possono trovare i punti di $V(I)$: questo significa che per i punti di $V(I)$ ci sono al massimo h_1 scelte per la

prima coordinata, h_2 scelte per la seconda coordinata, …, h_n scelte per l'ultima coordinata. Ne consegue che V(I) è finito. C.V.D.
Più concretamente:

COROLLARIO 3.4 *Siano k un campo algebricamente chiuso,* V=V(I) *una varietà algebrica affine di* k^n *e* G *una base di Gröbner ridotta di* I *rispetto a un ordinamento monomiale* σ *fissato in* $k[x_1, \ldots, x_n]$. *La varietà affine* V = V(I) *di* k^n *è finita se e solo se tra i* LT *della base* G *c'è almeno una potenza* $x_1^{r_1}, \ldots, x_n^{r_n}$ *per ciascuna delle n indeterminate.*
In particolare, se V(I) *è finita ogni base di Gröbner di* I *contiene almeno n polinomi.*

Dimostrazione Se tra i LT della base G c'è almeno una potenza $x_1^{r_1}, \ldots, x_n^{r_n}$ per ciascuna delle n indeterminate è soddisfatta la condizione (ii) del teorema 3.3; viceversa, se vale tale condizione, per ogni $i \in \{1, 2, \ldots, n\}$ deve esistere in G un polinomio il cui LT, dividendo $x_i^{m_i}$, ha forma $x_i^{r_i}$ con $r_i \leq m_i$. È poi ovvio che, se il numero di polinomi di G è inferiore a n, LT(G) è composto da un numero insufficiente di monomi e quindi sicuramente V(I) non è finita. C.V.D.

Notiamo che il corollario dice che per stabilire se un sistema ha un numero finito di soluzioni non è sempre necessario risolverlo.
Ad esempio all'ideale $I = < x^5 + y^3 + z^2 - 1, x^2 + y^3 + z - 1, x^4 + y^5 + z^6 - 1 >$ di $\mathbf{C}[x, y, z]$ è associato un sistema che ha certamente un numero finito (e non nullo) di soluzioni, poiché questa è la base di Gröbner ridotta di I rispetto a grLEX e i LT dei suoi polinomi sono x^5, y^3, z^6, cioè potenze non nulle delle tre indeterminate: questo garantisce la finitezza di V(I), mentre il fatto che I non contenga 1 implica l'esistenza di almeno una soluzione, per il Nullstellensatz debole.

OSSERVAZIONE 3.5 *Nelle ipotesi del corollario 3.4, se* σ *è l'ordinamento lessicografico,* G *una base di Gröbner ridotta di* I *e* LT(G) *contiene* $x_1^{r_1}, \ldots, x_n^{r_n}$, *il numero di punti di* V(I) *è al massimo* $r_1 \cdot \ldots \cdot r_n$.
Infatti, se uno degli esponenti è nullo, questo è l'enunciato del Nullstellensatz debole; altrimenti, avendo supposto G ridotta, se $x_1^{r_1}, \ldots, x_n^{r_n} \in$ LT(G) questi sono gli esponenti minimi con cui compaiono le indeterminate nei LT(I). Allora, applicando il procedimento di eliminazione ed estensione,

- quando si va a risolvere l'equazione[(5)] in x_n si troveranno r_n soluzioni (essendo il campo algebricamente chiuso);
- quando si sostituisce una di queste soluzioni c_n nelle equazioni del sistema contenenti solo x_n e x_{n-1} si avrà un sistema di equazioni in x_{n-1} sicuramente risolubile (come verrà dimostrato col teorema di estensione, vedi Capitolo VII), contenente almeno un'equazione di grado r_{n-1} in x_{n-1} che avrà r_{n-1} soluzioni, che però potrebbero non essere tutte soluzioni delle restanti equazioni in x_{n-1}; quindi le soluzioni parziali (c_{n-1}, c_n) ottenute a questo punto non possono essere più di $r_{n-1} \cdot r_n$;
- risalendo in questo modo fino alle equazioni in x_1 si prova il risultato.

In alcuni casi questo massimo viene effettivamente raggiunto.

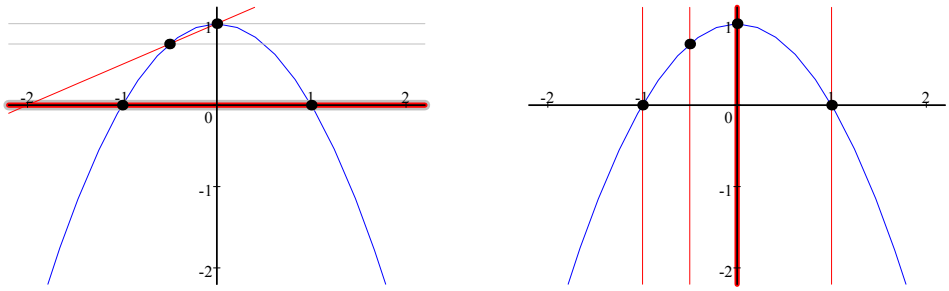
ESEMPIO 3.6 Se I è l'ideale $< x - y^7, y^{12} - y >$ di $\mathbf{C}[x, y]$, la base di Gröbner ridotta di I rispetto a LEX ($x > y$) è data dai generatori e quindi LT(G) = $\{x, y^{12}\}$. Quindi $r_1 \cdot r_2 = 12$ e la varietà V(I) di $\mathbf{C}^2$ è proprio formata da 12 punti: il punto (0,0) e gli 11 punti (c^7, c), con c radice 11-esima dell'unità.

(5) Visto che l'ordinamento è lessicografico e la base G è ridotta, non può esistere più di una equazione nell'ultima variabile x_n (la riduzione tra polinomi in x_n equivale ad applicare l'algoritmo euclideo per il calcolo del MCD).

In altri casi, no.

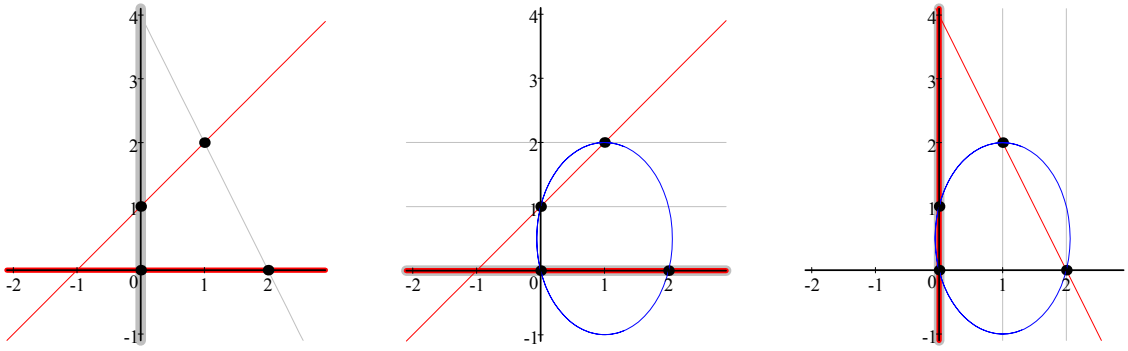
ESEMPIO 3.7 Se $I = < x^2 + y - 1, xy - 2y^2 + 2y >$, la base di Gröbner ridotta di I rispetto a LEX ($x > y$) è $G = \{x^2 + y - 1, xy - 2y^2 + 2y, 4y^3 - 7y^2 + 3y\}$ e $LM(G) = \{x^2, xy, y^3\}$. Pur essendo $r_1 \cdot r_2 = 6$, in realtà $V(I)$ è composta di soli 4 punti: (1,0), (–1,0), (0,1), (–1/2, 3/4).

Il problema non è legato alla molteplicità "algebrica" dei punti di $V(I)$ e neppure al fatto che ci siano "punti all'infinito" comuni alle due varietà che si intersecano formando $V(I)$: infatti $V(x^2 + y - 1)$ è una parabola e $V(xy - 2y^2 + 2y)$ una coppia di rette incidenti non parallele all'asse della parabola.
È invece legato al fatto che ci sono punti con differente ascissa a cui corrisponde una sola ordinata e che si sta estendendo dall'asse y al piano.
Se si fosse usato l'ordinamento LEX ($y > x$) si sarebbe trovata $\{y + x^2 - 1, 2x^4 + x^3 - 2x^2 - x\}$ come base di Gröbner ridotta e questa scrittura (che equivale ad estendere dall'asse x al piano) evidenzia che non ci possono essere più di 4 punti in $V(I)$.
I grafici sottostanti mostrano $V(I)$ rappresentata attraverso le varietà dei polinomi delle due diverse basi di Gröbner: in ogni figura, nello stesso colore sono indicate le componenti della stessa varietà.



Si potrebbe pensare che sia sempre possibile individuare l'indeterminata da cui far partire l'estensione in modo da conteggiare correttamente le soluzioni. Ma consideriamo il seguente

ESEMPIO 3.8 Se $I = <2x^2 + xy - 4x, xy - y^2 + y>$, la base di Gröbner ridotta di I rispetto a LEX ($x > y$) è $G = \{2x^2 - 4x + y^2 - y, xy - y^2 + y, y^3 - 3y^2 + 2y\}$ e $LM(G) = \{x^2, xy, y^3\}$. Pur essendo $r_1 \cdot r_2 = 6$, in realtà $V(I)$ è composta di soli 4 punti: (0,0), (0,1), (2,0), (2,1). D'altra parte, la base di Gröbner ridotta di I rispetto a LEX ($y > x$) è $G = \{y^2 - y + 2x^2 - 4x,\ yx + 2x^2 - 4x, x^3 - 3x^2 + 2x\}$, per cui $LM(G) = \{y^2, yx, x^3\}$ e ancora una volta $r_1 \cdot r_2 = 6$. Dei grafici sottostanti, il primo mostra $V(I)$ come intersezione di $V(2x^2 + xy - 4x)$ e $V(xy - y^2 + y)$, il secondo ed il terzo come intersezioni delle varietà dei polinomi delle due basi di Gröbner. L'analogia tra questi ultimi ed il primo grafico relativo all'esempio 3.7 illustra il motivo per cui il numero di punti di $V(I)$ è inferiore a $r_1 \cdot r_2$.



Ancora, guardando l'esempio 3.8 si potrebbe pensare che il numero di soluzioni sia legato al numero di monomi non appartenenti a <LT(I)>, confortati in ciò dal fatto che la stessa cosa vale nell'esempio 3.7, nel quale si vede che tale numero è 4, anche senza risolvere il sistema, osservando che la base di Gröbner di I rispetto a grLEX ($y > x$) è $\{x^2 + y - 1, -2y^2 + xy + 2y\}$. Ma

ESEMPIO 3.9 Se I = $<(2x + y - 4)\,x^2, (x - y + 1)\,y^2>$, la varietà V(I) è fatta da 4 punti, poiché coincide con quella dell'esempio 3.8; invece la base di Gröbner ridotta di I rispetto a LEX ($x > y$) è G = $\{2x^3 + x^2y - 4x^2, xy^2 - y^3 + y^2, y^5 - 4y^2 + 5y^3 - 2y^2\}$ ed, essendo LM(G) = $\{x^3, xy^2, y^5\}$, si trova che ci sono 9 monomi non appartenenti a <LT(I)>.

4. PASSAGGIO A FORMA IMPLICITA

Vedremo che, se il sistema di equazioni algebriche non ha un numero finito di soluzioni, si cercherà comunque di rappresentare l'insieme delle soluzioni come insieme dipendente da parametri, cioè (come si suol dire) di parametrizzare le soluzioni, operazione che viene già fatta quando un sistema lineare ha infinite soluzioni.
In algebra lineare (e soprattutto quando si rappresentano i sottospazi affini lineari: rette, piani, iperpiani ecc.) si è incontrato anche il procedimento inverso: nota la rappresentazione parametrica di un certo insieme lo si rappresenta in forma implicita stabilendo quali legami occorre imporre alle indeterminate perché la soluzione di quelle equazioni sia esattamente l'insieme considerato. Con alquanta cautela (e accontentandosi di un po' di meno) si può fare la stessa cosa anche con equazioni algebriche non lineari.
Dati gli n polinomi $f_1, \ldots, f_n$ di $k[t_1, \ldots, t_m]$ le equazioni parametriche:

$$x_1 - f_1(t_1,\ldots, t_m)=0, \ldots, x_n - f_n(t_1,\ldots, t_m)=0$$

rappresentano un sottoinsieme di una varietà affine di k^n. Ci domandiamo se lo stesso insieme può essere descritto implicitamente eliminando i parametri $t_1,\ldots, t_m$.
Consideriamo l'ideale I = $<x_1 - f_1,\ldots, x_n - f_n>$ dell'anello $k[t_1,\ldots, t_m, x_1,\ldots, x_n]$. Costruendo una base di Gröbner di I rispetto al l'ordinamento LEX e $t_1>\ldots>t_m>x_1>\ldots>x_n$, si arriva prima o poi ad avere polinomi che non contengono i parametri (vedi processo di eliminazione): questi polinomi sono candidati a descrivere una varietà che "differisce di poco" dall'insieme descritto dalle equazioni parametriche.
Premesso che, finché non si esaminano in dettaglio i teoremi di eliminazione ed estensione non ci sono garanzie che nella varietà affine così individuata non ci siano altre curve, superficie… oltre all'insieme descritto parametricamente, proviamo a fare un esempio.
Sia X l'insieme descritto dalle equazioni $x = t^4, y = t^3, z = t^2$.
Calcolo la base di Gröbner di I = $< x - t^4, y - t^3, z - t^2>$ rispetto a $t>x>y>z$:
$t^4 - x = (t^2 - z)t^2 + (t^2 - z)z + z^2 - x$ può essere sostituito da $x - z^2$
$t^3 - y = (t^2 - z)t + tz - y$ può essere sostituito da $tz - y$
Quindi partiamo dalla base $< t^2 - z, tz - y, x - z^2 >$.
S(f_1, f_2) = $ty - z^2 = ty - (z^2 - x) - x$: ha resto $ty - x = f_4$

$$< t^2 - z, tz - y, x - z^2, ty - x >$$

S(f_1, f_3) non è neppure da considerare poiché i LT dei due polinomi sono primi tra loro
S(f_2, f_3) non è neppure da considerare poiché i LT dei due polinomi sono primi tra loro
S(f_1, f_4) = $tx - yz = t(x - z^2) + tz^2 - yz = t(x - z^2) + (tz - y)z$ dà resto nullo
S(f_2, f_4) = $xz - y^2 = (x - z^2)z + z^3 - y^2$: l'opposto del resto è $y^2 - z^3 = f_5$

$$< t^2 - z, tz - y, x - z^2, ty - x, y^2 - z^3 >$$

S(f_3, f_4) non è neppure da considerare poiché i LT dei due polinomi sono primi tra loro
Analogamente per S(f_1, f_5), S(f_2, f_5), S(f_3, f_5).
S(f_4, f_5) = $tz^3 - xy = (tz - y)z^2 + y(z^2 - x)$ dà resto nullo.
Quindi si è trovata la base di Gröbner e i polinomi non contenenti parametri sono $x - z^2, y^2 - z^3$.
Quindi una varietà contenente (e in realtà coincidente con) X è $V(x - z^2, y^2 - z^3)$.