



UNIVERSITÀ DEGLI STUDI DI ROMA “LA SAPIENZA”

Dina Ghinelli

CORSO di ISTITUZIONI di ALGEBRA SUPERIORE

(Laurea Magistrale in Matematica per le Applicazioni)

(Anno Accademico 2013-2014)

3. TEORIA DELL'ELIMINAZIONE

Dipartimento di Matematica

Facoltà di Scienze Matematiche, Fisiche e Naturali

Capitolo 3

Teoria dell'Eliminazione

In questo capitolo studieremo metodi sistematici per eliminare variabili da sistemi di equazioni polinomiali. La strategia di base è data da due teoremi che dimostreremo con l'uso delle basi di Groebner e della teoria classica dei risultanti: il Teorema di Eliminazione e il Teorema di Estensione.

Accenneremo anche all'interpretazione geometrica dell'eliminazione, al Teorema di Chiusura, e, infine, alle applicazioni della teoria dell'eliminazione alla risoluzione del problema di implicitizzazione e allo studio degli involucri algebrici di famiglie di curve.

3.1 I Teoremi di Eliminazione e di Estensione

Cominciamo questo paragrafo con l'illustrare un esempio. Si chiede di risolvere il sistema:

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

Sia, dunque, I l'ideale:

$$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$$

dell'anello dei polinomi $k[x, y, z]$. Una base di Groebner per I rispetto all'ordine lessicografico (LEX) in cui si consideri $x > y > z$, è data dai polinomi:

$$\begin{cases} g_1 = x + y + z^2 - 1, \\ g_2 = y^2 - y - z^2 + z, \\ g_3 = 2yz^2 + z^4 - z^2, \\ g_4 = z^6 - 4z^4 + 4z^3 - z^2. \end{cases}$$

Risulta $I = \langle G \rangle = \langle g_1, g_2, g_3, g_4 \rangle$ e, come si può osservare, l'ultima equazione dipende unicamente dalla variabile z . Procedendo come per i sistemi lineari si ha che dalla

$$g_4 = z^2(z-1)^2(z^2 + 2z - 1) = 0$$

si ottengono per z i valori

$$z = 0, \quad z = 1, \quad z = -1 \pm \sqrt{2}.$$

Sostituendo tali valori in $g_2 = 0$ e $g_3 = 0$, si hanno le possibili y e, infine $g_1 = 0$ dà le corrispondenti x . In tal modo si hanno esattamente le seguenti cinque soluzioni

$$(1, 0, 0), \quad (0, 1, 0), \quad (0, 0, 1), \\ (-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}), \quad (-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}),$$

Nel procedimento utilizzato in questo esempio si sono effettuati due passi fondamentali:

- Passo di **Eliminazione**: dato in $k[x_1, \dots, x_n]$ il sistema di equazioni polinomiali $f_i = 0$, si considera l'ideale $I = \langle f_i \rangle$ e se ne determina una base di Groebner $G = \{g_1, \dots, g_t\}$, rispetto all'ordine lessicografico con $x_1 > \dots > x_n$. Si osserva poi che g_t dipende solo dalla variabile x_n (nell'esempio g_4 dipende unicamente da z). Dunque $g_t \in I \cap k[x_n]$.
- Passo di **Estensione**: data una soluzione x_n dell'equazione $g_t(x_n) = 0$, estenderla, se possibile, ad una soluzione di tutto il sistema.

Entrambi i passi si possono fare nella più grande generalità.

Definizione 3.1.1 Dato l'ideale $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$, si dice **primo ideale di eliminazione** di I l'intersezione:

$$I_1 = I \cap k[x_2, \dots, x_n].$$

I_1 consiste di tutte le conseguenze polinomiali del sistema $f_i = 0$ che eliminano la x_1 , ovvero dipendono solo da x_2, \dots, x_n .

Più in generale si può dare la seguente

Definizione 3.1.2 Dato l'ideale $I = \langle f_1, \dots, f_s \rangle \subseteq k[x_1, \dots, x_n]$, si dice **h-simo ideale di eliminazione** di I l'intersezione

$$I_h = I \cap k[x_{h+1}, \dots, x_n].$$

Analogamente a quanto osservato prima, si ha che I_h consiste di tutte le conseguenze polinomiali del sistema $f_i = 0$ che eliminano le x_1, \dots, x_h , ovvero dipendono solo da x_{h+1}, \dots, x_n .

Lo scopo di questo capitolo è la formalizzazione di questi due passi, fornendone i relativi teoremi.

Osservazioni:

1. I_h è un ideale dell'anello dei polinomi $k[x_{h+1}, \dots, x_n]$, infatti lo zero vi appartiene, la somma di due polinomi in $I_h = I \cap k[x_{h+1}, \dots, x_n]$ sarà ancora in I_h ed il prodotto di un polinomio di $k[x_{h+1}, \dots, x_n]$ per un elemento di I_h è ancora un elemento di I_h . Si noti però che I_h non è un ideale in $k[x_1, \dots, x_n]$, poiché un polinomio di $k[x_1, \dots, x_n]$ moltiplicato per un elemento di I_h non è più un elemento di I_h .
2. $I = I_0$, ovvero l'ideale I coincide con l'ideale di eliminazione di indice zero.
3. L'ideale di eliminazione $(h+1)$ -simo, I_{h+1} , si può pensare come il primo ideale di eliminazione dell'ideale I_h . Si ha infatti:

$$\begin{aligned} (I_h)_1 &= (I \cap k[x_{h+1}, \dots, x_n]) \cap k[x_{h+2}, \dots, x_n] \\ &= I \cap k[x_{h+2}, \dots, x_n] = I_{h+1} \end{aligned}$$

4. Ordinamenti diversi delle variabili x_1, \dots, x_n forniscono ideali di eliminazione diversi.

Eliminare le variabili x_1, \dots, x_h consiste, quindi, nel determinare i polinomi non nulli nell' h -simo ideale di eliminazione I_h . Utilizzando l'ordinamento opportuno, le basi di Groebner permettono tale eliminazione.

Teorema 3.1.1 (Teorema di eliminazione) *Sia I un ideale dell'anello dei polinomi $k[x_1, \dots, x_n]$, e sia $G = \{g_1, \dots, g_t\}$ una base di Groebner per I rispetto all'ordine lessicografico con $x_1 > \dots > x_n$. Per ogni $0 \leq h \leq n$, l'insieme:*

$$G_h = G \cap k[x_{h+1}, \dots, x_n]$$

è una base di Groebner per l' h -simo ideale di eliminazione I_h .

Dimostrazione. Riordinando, eventualmente, gli elementi di G , possiamo supporre, senza ledere alla generalità, che G_h sia costituito dai primi r polinomi di G , ossia $G_h = \{g_1, \dots, g_r\}$. Si vuole innanzi tutto provare che

G_h è un sistema di generatori per I_h e, successivamente, che è una base di Groebner per I_h .

Il fatto che ogni elemento f di I_h si può scrivere come combinazione lineare di elementi di G_h , ossia

$$f = a_1g_1 + \dots + a_rg_r, \quad \forall f \in I_h.$$

segue facilmente utilizzando l'algoritmo di divisione. Infatti:

- Essendo G una base di Groebner per I , il resto della divisione di ogni elemento di I per G è zero (cfr. Corollario 2.6.1). Quindi, anche per ogni $f \in I_h \subset I$ tale resto \bar{f}^G è zero.
- Poiché si sta usando l'ordine LEX con $x_1 > \dots > x_n$, e solo in g_1, \dots, g_r le variabili x_1, \dots, x_h non figurano, nei termini direttori di g_{r+1}, \dots, g_t deve figurare almeno una delle variabili x_1, \dots, x_h . Dunque i termini direttori dei polinomi g_{r+1}, \dots, g_t sono sempre più grandi di ciascun termine dei polinomi di I_h , nei quali figurano solo le variabili x_{h+1}, \dots, x_n . Ne segue, che i polinomi g_{r+1}, \dots, g_t non intervengono nella divisione di f per gli elementi di G .

Da queste due osservazioni segue che dividendo $f \in I_h$ per G si ha

$$f = a_1g_1 + \dots + a_rg_r + 0g_{r+1} + \dots + 0g_t.$$

Pertanto, ogni elemento $f \in I_h$ si può scrivere come combinazione lineare di elementi di $G_h = \{g_1, \dots, g_r\}$, e G_h è un sistema di generatori per I_h .

Per completare la dimostrazione, bisogna provare che G_h è una base di Groebner per I_h ossia, applicando il criterio di Buchberger, che per ogni $1 \leq i \leq j \leq r$ il resto della divisione degli s-polinomi $S(g_i, g_j)$ per gli elementi di G_h è uguale a zero.

Ma per ogni f appartenente ad I_h , fare la divisione per gli elementi di G_h o per quelli di G è equivalente in quanto, come visto sopra, solo gli r polinomi g_1, \dots, g_r intervengono come divisori. In particolare $\bar{f}^G = \bar{f}^{G_h} = 0$. Ricordando che per ogni $1 \leq i \leq j \leq r$ gli s-polinomi $S(g_i, g_j)$ sono particolari polinomi di I_h , si ottiene:

$$\overline{S(g_i, g_j)}^{G_h} = 0, \quad i \neq j, \quad i, j = 1, \dots, r.$$

Per il criterio di Buchberger si ha, dunque, che $G_h = \{g_1, \dots, g_r\}$ è una base di Groebner per I_h . ■

Un'applicazione di questo teorema si può vedere nell'esempio fatto all'inizio del capitolo. Avevamo visto che una base di Groebner dell'ideale

$$I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$$

è $G = \{g_1 = x + y + z^2 - 1, g_2 = y^2 - y - z^2 + z, g_3 = 2yz^2 + z^4 - z^2, g_4 = z^6 - 4z^4 + 4z^3 - z^2\}$. Poiché g_4 non dipende dalle variabili x e y ,

$$G_2 = G \cap k[z] = \{g_4\},$$

ed inoltre

$$I_2 = I \cap k[z] = \langle g_4 \rangle.$$

Quindi $g_4 = z^6 - 4z^4 + 4z^3 - z^2$ non è soltanto un possibile modo per eliminare le variabili x ed y , ma è anche il miglior modo possibile in quanto ogni altro polinomio che elimina le suddette variabili è un multiplo di g_4 .

Ci si pone ora il problema dell'**estensione** di una soluzione parziale. Sia I un ideale di $k[x_1, \dots, x_n]$ e sia:

$$\mathcal{V}(I) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \quad \forall f \in I\}$$

la varietà affine definita da I . La varietà affine definita dall' h -simo ideale di eliminazione I_h è quindi

$$\mathcal{V}(I_h) = \{\mathbf{q} = (q_{h+1}, \dots, q_n) \in k^{n-h} \mid f(q_{h+1}, \dots, q_n) = 0 \quad \forall f \in I_h\}.$$

Si dice **soluzione parziale** del sistema di equazioni $f_i(x) = 0$, ogni punto \mathbf{q} appartenente a $\mathcal{V}(I_h)$.

Si dice, inoltre, che la soluzione parziale $\mathbf{q} \in \mathcal{V}(I_h)$ si **estende** ad una soluzione completa del sistema $f_i(x) = 0$ ($i = 1, \dots, s$), quando esiste un punto $\mathbf{p} = (p_1, \dots, p_h)$ appartenente a k^h tale che:

$$(\mathbf{p}, \mathbf{q}) = (p_1, \dots, p_h, q_{h+1}, \dots, q_n) \in \mathcal{V}(I),$$

ossia quando la coppia (\mathbf{p}, \mathbf{q}) annulla tutti i polinomi del sistema di equazioni originario. Si noti, tuttavia, che un sistema di equazioni può essere incompatibile, ossia, non ogni soluzione parziale si estende.

Sia dato ad esempio il seguente sistema:

$$\begin{cases} xy = 1, \\ xz = 1. \end{cases}$$

Passando al sistema equivalente:

$$\begin{cases} y - z = 0, \\ y = \frac{1}{x}, \end{cases}$$

si trovano facilmente le soluzioni comuni rappresentate dalla terna $(1/a, a, a)$, con $a \neq 0$. Si consideri, ora, l'ideale $I = \langle xy - 1, xz - 1 \rangle$ generato dalle equazioni del sistema, e la sua base di Groebner rispetto all'ordine lessicografico

$$G = \{xy - 1, xz - 1, y - z\}.$$

Per quanto visto in precedenza, si ha che il primo ideale di eliminazione $I_1 = I \cap k[y, z]$ è generato dagli elementi della $G_1 = G \cap k[y, z]$, ossia $I_1 = \langle y - z \rangle$. Sarà dunque soluzione parziale del sistema ogni elemento \mathbf{q} appartenente alla varietà affine definita da I_1 , ossia ogni coppia (a, a) soddisfacente l'equazione della bisettrice del primo e terzo quadrante del piano yz . Affinché tale soluzione parziale si estenda ad una completa, deve essere soddisfatta la condizione che a sia diverso da zero.

Si arriva così alla soluzione completa $(1/a, a, a) \in \mathcal{V}(I)$ a cui si estendono solo le soluzioni parziali $\mathbf{q} = (a, a) \in \mathcal{V}(I_1)$ soddisfacenti la condizione $a \neq 0$.

Il seguente *teorema di estensione* fornisce un criterio per stabilire a priori quando sia possibile estendere una soluzione parziale.

Restringiamoci al caso in cui si sia eliminata solo la prima variabile x_1 . Si vuole determinare quando una soluzione parziale $\mathbf{q} = (q_2, \dots, q_n)$, appartenente alla varietà affine $\mathcal{V}(I_1)$, si possa estendere ad una soluzione completa $(p, \mathbf{q}) = (p, q_2, \dots, q_n)$ in $\mathcal{V}(I)$.

Teorema 3.1.2 (Teorema di estensione) *Sia $I = \langle f_1, \dots, f_s \rangle$ un ideale nell'anello dei polinomi $k[x_1, \dots, x_n]$, con k campo algebricamente chiuso ($k = \bar{k}$), e sia I_1 il primo ideale di eliminazione di I . Per ogni, $1 \leq i \leq s$, si scriva f_i nella forma:*

$$f_i = c_i(x_2, \dots, x_n)x_1^{N_i} + \text{termini in cui } x_1 \text{ ha grado minore di } N_i$$

dove $N_i \geq 0$, $c_i = LC_{x_1}(f_i)$ è il coefficiente direttore, rispetto ad x_1 di f_i , e i coefficienti $c_i \in k[x_2, \dots, x_n]$ sono diversi da zero. Per ogni $\mathbf{q} = (q_2, \dots, q_n) \in \mathcal{V}(I_1)$, con $\mathbf{q} \notin V(c_1(x_2, \dots, x_n), \dots, c_s(x_2, \dots, x_n)) \subset k^{n-1}$, esiste $p \in k$ tale che

$$(p, \mathbf{q}) = (p, q_2, \dots, q_n) \in \mathcal{V}(I).$$

La dimostrazione di questo teorema, che verrà data in seguito, fa uso della teoria dei risultanti.

Osservazioni sul teorema di estensione.

- L'ipotesi che il campo k sia *algebricamente chiuso* è essenziale per la validità del teorema. Si consideri, infatti, il seguente sistema di equazioni nel caso in cui $k = \mathbf{R}$:

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

Eliminando la variabile x , si ottiene la soluzione parziale (a, a) per ogni $a \in \mathbf{R}$. I coefficienti direttori rispetto ad x dei polinomi $x^2 - y$ e $x^2 - z$ non si annullano mai, per cui il teorema di estensione garantisce l'esistenza di una soluzione completa nel campo algebricamente chiuso \mathbf{C} . In \mathbf{R} la situazione è differente in quanto l'equazione $x^2 = a$ ammette soluzioni solo nel caso in cui $a \geq 0$, pertanto, se a è minore di zero, la soluzione parziale (a, a) non si estende.

- Il teorema di estensione è enunciato solo nel caso in cui si voglia eliminare la prima variabile x_1 , ma può essere utilizzato anche nel caso in cui si voglia eliminare un numero arbitrario di variabili. Ad esempio si consideri in \mathbf{C}^3 il sistema:

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

Una base di Groebner dell'ideale $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$ rispetto all'ordine lessicografico con $x > y > z$ è :

$$\begin{cases} g_1 = y^4 z^2 + y^2 z^4 - y^2 z^2 + 1, \\ g_2 = x + y^3 z + y z^3 - y z. \end{cases}$$

Dal teorema di eliminazione si ha:

$$\begin{cases} I_1 = I \cap \mathbf{C}[y, z] = \langle g_1 \rangle, \\ I_2 = I \cap \mathbf{C}[z] = \{0\}. \end{cases}$$

Dal fatto che $I_2 = \{0\}$, segue $\mathcal{V}(I_2) = \mathbf{C}$ e, quindi, ogni $c \in \mathbf{C}$ è una soluzione parziale. Ci si chiede quale soluzione parziale $c \in \mathcal{V}(I_2) = \mathbf{C}$ si estende ad una soluzione (a, b, c) appartenente a $\mathcal{V}(I)$. L'idea è di estendere inizialmente c ad una soluzione (b, c) in $\mathcal{V}(I_1)$, e poi estendere quest'ultima ad una soluzione (a, b, c) di $\mathcal{V}(I)$. In generale I_{h+1} si può considerare come il primo ideale di eliminazione di I_h , per cui $I_2 = (I_1)_1$. Applichiamo, dunque, il teorema di estensione per passare

da una soluzione in $\mathcal{V}(I_2)$ ad una in $\mathcal{V}(I_1)$. Il coefficiente di g_1 rispetto ad y è z^2 , quindi $c \in \mathcal{V}(I_2)$ si estende alla soluzione (b, c) quando c è diverso da zero. Si noti, inoltre, che $g_1(y, c) = 0$ non ha soluzioni se $c = 0$. Il passo successivo consiste nell'estendere tale soluzione parziale (b, c) ad una completa (a, b, c) appartenente a $\mathcal{V}(I)$. Con la sostituzione $(y, z) = (b, c)$ nel sistema si ottengono due equazioni nella sola variabile x :

$$\begin{cases} f_1(x, b, c) = x^2 + b^2 + c^2 - 1 = 0, \\ f_2(x, b, c) = xbc - 1 = 0, \end{cases}$$

e non è ovvio che queste abbiano una soluzione comune $x = a$. In questo il teorema di estensione mostra la sua potenza. Infatti il coefficiente direttore rispetto ad x in f_1 e f_2 sono rispettivamente: $LC_x(x^2 + y^2 + z^2 - 1) = 1$ e il $LC_x(xyz - 1) = yz$. Poiché $LC_x(f_1) = 1$ non si annulla mai, il teorema di estensione ci assicura che tale elemento a esiste. Si è così provato che ogni soluzione parziale c diversa da zero si estende ad una soluzione completa (a, b, c) in $\mathcal{V}(I)$.

Abbiamo visto, nell'esempio precedente, come il teorema di estensione sia particolarmente facile da usare quando almeno uno dei coefficienti direttori è una costante non nulla, in quanto in tal caso $V(c_1, \dots, c_s)$ è sempre uguale all'insieme vuoto. Tale proprietà è espressa nel seguente corollario del teorema di estensione.

Corollario 3.1.1 *Sia k un campo algebricamente chiuso e sia $I = \langle f_1, \dots, f_s \rangle$ un ideale dell'anello dei polinomi $k[x_1, \dots, x_n]$. Se esiste un indice i tale che*

$$LC_{x_1}(f_i) = c$$

con $c \neq 0$ costante in k e $N_i > 0$, allora per ogni soluzione parziale $\mathbf{q} = (q_2, \dots, q_n) \in \mathcal{V}(I_1)$, esiste $p \in k$ tale che $(p, \mathbf{q}) \in \mathcal{V}(I)$, ovvero ogni soluzione parziale si estende.

Dimostrazione. Essendo $V(c_1, \dots, c_{i-1}, c, c_{i+1}, \dots, c_s)$ vuota per $c \neq 0$, il punto \mathbf{q} non appartiene mai alla varietà $V(c_1, \dots, c_s)$. Per il teorema di estensione, ogni soluzione parziale si estende ad una soluzione completa del sistema $f_i(x) = 0$, $i = 1, \dots, s$. ■

Concludiamo questo paragrafo con il seguente esempio

$$\begin{cases} xy = 4, \\ y^2 = x^3 - 1, \end{cases}$$

Usando l'ordine lessicografico, la base di Groebner ridotta è data da

$$\begin{cases} g_1 = 16x - y^2 - y^4, \\ g_2 = y^5 + y^3 - 64, \end{cases}$$

procedendo al solito modo si scopre che $y^5 + y^3 - 64 = 0$ non ha soluzioni razionali. Se ne possono tuttavia calcolare soluzioni approssimate con metodi numerici e poi proseguire al solito modo, ossia sostituire tali soluzioni in g_1 per determinare i corrispondenti valori per la x . In questo caso, si possono ottenere solo soluzioni approssimate.

3.2 La geometria dell'eliminazione

Lo scopo di questo paragrafo è fornire un'interpretazione geometrica della teoria dell'eliminazione e, in particolare, del teorema di estensione. L'eliminazione corrisponde alla proiezione di una varietà su un sottospazio di dimensione minore. Supporremo d'ora innanzi che il campo k sia algebricamente chiuso.

Definiamo cosa si intende per *proiezione* di una varietà affine. Data una varietà $V = \mathcal{V}(f_1, \dots, f_s) \subseteq k^n$, per eliminare le prime h variabili consideriamo la proiezione

$$\pi_h : k^n \longrightarrow k^{n-h}$$

che manda (a_1, \dots, a_n) in (a_{h+1}, \dots, a_n) . Applicando π_h a $V \subseteq k^n$ si ottiene $\pi_h(V) \subseteq k^{n-h}$, ed il suo legame con l' h -simo ideale di eliminazione è stabilito dal seguente lemma:

Lemma 3.2.1 *Sia $I_h = \langle f_1, \dots, f_s \rangle \cap k[x_{h+1}, \dots, x_n]$ l' h -simo ideale di eliminazione. In k^{n-h} si ha*

$$\pi_h(V) \subseteq \mathcal{V}(I_h).$$

Dimostrazione. Sia a un elemento di $\mathcal{V}(I)$, con

$$a = (\mathbf{p}, \mathbf{q}) = (p_1, \dots, p_h, q_{h+1}, \dots, q_n).$$

Dalla definizione di π_h segue che $\pi_h(a) = \mathbf{q} = (q_{h+1}, \dots, q_n)$ ed è un elemento di $\pi_h(\mathcal{V}(I))$. Per provare l'asserto, occorre dimostrare che per ogni f appartenente all' h -simo ideale di eliminazione I_h , si ha $f(\pi_h(a)) = 0$. Questo segue banalmente dal fatto che a appartiene alla varietà definita dall'ideale I , per cui ogni $f \in I$ si annulla in tal punto. Di conseguenza per ogni $f \in I_h$ si ha $f(\pi_h(a)) = f(q_{h+1}, \dots, q_n) = 0$. ■

I punti di $\mathcal{V}(I_h)$ sono le *soluzioni parziali*, mentre $\pi_h(V)$ è esattamente l'insieme delle soluzioni parziali che si estendono ad una soluzione completa.

Indichiamo, per semplicità, con $a = (a_1, \dots, a_h)$ un punto di k^h , con $b = (b_{h+1}, \dots, b_n)$ un punto di k^{n-h} e con (a, b) un punto di $k^n = k^h \times k^{n-h}$. Per il lemma precedente possiamo scrivere $\pi_h(V)$ come:

$$\pi_h(V) = \{b \in \mathcal{V}(I_h) \mid \exists a \in k^h \text{ con } (a, b) \in V\}.$$

Consideriamo il caso $h = 1$ e la proiezione

$$\pi_1 : k^n \longrightarrow k^{n-1}$$

con k campo algebricamente chiuso. Il teorema di estensione ha, allora, la seguente interpretazione geometrica.

Teorema 3.2.1 (Teorema di estensione geometrico) *Data la varietà $V = \mathcal{V}(f_1, \dots, f_s) \subset k^n$, con k campo algebricamente chiuso, siano c_i , $i = 1, \dots, s$ i coefficienti direttori delle f_i rispetto ad x_1 . Se I_1 è il primo ideale di eliminazione di $\langle f_1, \dots, f_s \rangle$, in k^{n-1} risulta*

$$\mathcal{V}(I_1) = \pi_1(V) \cup [\mathcal{V}(c_1, \dots, c_s) \cap \mathcal{V}(I_1)],$$

dove $\pi_1 : k^n \longrightarrow k^{n-1}$ è la proiezione sullo spazio delle ultime $n - 1$ coordinate.

Dimostrazione. Segue dal lemma precedente e dal teorema di estensione. I dettagli sono lasciati, per esercizio, al lettore. ■

Come per il teorema di estensione visto nel precedente paragrafo, si ha il seguente corollario del teorema di estensione geometrico.

Corollario 3.2.1 *Sia k un campo algebricamente chiuso e sia $I = \langle f_1, \dots, f_s \rangle$ un ideale dell'anello $k[x_1, \dots, x_n]$. Se per qualche i , il polinomio f_i è della forma*

$$f_i = cx_1^{N_i} + \text{termini di ordine minore di } N_i \text{ rispetto ad } x_1,$$

con c costante non nulla del campo k e $N_i > 0$, allora si ha la seguente uguaglianza:

$$\mathcal{V}(I_1) = \pi_1(\mathcal{V}(I)).$$

ove $I_1 = I \cap k[x_2, \dots, x_n]$ è il primo ideale di eliminazione.

Si noti che $W = \mathcal{V}(I_1) \cap \mathcal{V}(c_1, \dots, c_s)$ è una varietà affine in quanto intersezione di varietà affini, mentre $\pi_1(V)$ in generale non lo è, come mostra il seguente esempio.

Sia data la varietà di equazioni

$$\begin{cases} xy = 1, \\ xz = 1. \end{cases}$$

In questo caso, $\mathcal{V}(I_1)$ è la retta di equazione $y = z$ nel piano yz , mentre $\pi_1(V) = \{(a, a) \in \mathbf{C}^2 \mid a \neq 0\}$ non è una varietà affine in quanto è una retta privata del suo punto $(0, 0)$.

Il teorema di estensione geometrico ci dice sostanzialmente che la proiezione $\pi_1(V)$ riempie la varietà affine $\mathcal{V}(I_1)$, ad eccezione, eventualmente, di una parte che comunque si trova nella varietà $\mathcal{V}(c_1, \dots, c_s)$. Sfortunatamente non è chiaro quanto grande possa essere questa parte $W = \mathcal{V}(I_1) \cap \mathcal{V}(c_1, \dots, c_s)$ e, talora, è grande in modo quasi innaturale. Un esempio in cui $W = \mathcal{V}(I_1) \cap \mathcal{V}(c_1, \dots, c_s) = \mathcal{V}(I_1)$ è dato dal seguente sistema

$$\begin{cases} f_1 = (y-z)x^2 + xy - 1 = 0, \\ f_2 = (y-z)x^2 + xz - 1 = 0. \end{cases}$$

Il primo ideale di eliminazione I_1 di $I = \langle f_1, f_2 \rangle$ è $I_1 = \langle y-z \rangle$; la varietà $\mathcal{V}(I_1)$ è il piano $y-z=0$; poiché $c_1 = c_2 = y-z$, risulta che anche $\mathcal{V}(c_1, c_2) = \mathcal{V}(y-z)$ e quindi $W = \mathcal{V}(I_1)$, e il teorema di estensione geometrico non ci dice niente sulla grandezza di $\pi_1(V)$. Anche in casi estremi come questo si possono comunque sempre fare le seguenti affermazioni sulla relazione tra $\pi_h(V)$ e la varietà $\mathcal{V}(I_h)$ definita dall' h -simo ideale di eliminazione.

Teorema 3.2.2 (Teorema di Chiusura) *Sia k un campo algebricamente chiuso, $V = \mathcal{V}(f_1, \dots, f_s) \subset k^n$ una varietà affine e sia I_h l' h -simo ideale di eliminazione di $I = \langle f_1, \dots, f_s \rangle$. Allora:*

i) $\mathcal{V}(I_h)$ è la più piccola varietà affine contenente $\pi_h(V)$, ossia

$$\mathcal{V}(I_h) = \overline{\pi_h(V)},$$

è la chiusura di Zariski di $\pi_h(V)$.

ii) Se $V \neq \emptyset$, esiste una varietà affine $W \subset \mathcal{V}(I_h)$ ma diversa da $\mathcal{V}(I_h)$ tale che $\mathcal{V}(I_h) - W \subset \pi_h(V)$.

Dimostrazione. (i) Dire che $\mathcal{V}(I_h)$ è la più piccola varietà affine contenente $\pi_h(V)$, significa che:

- $\pi_h(V) \subset \mathcal{V}(I_h)$,
- se Z è un'altra varietà affine in k^{n-h} contenente $\pi_h(V)$, allora $\mathcal{V}(I_h) \subset Z$.

La dimostrazione di questo primo punto richiederà il teorema degli zeri di Hilbert (*Nullstellensatz*), che verrà dimostrato nel capitolo 4.

(ii) Si vuole provare che sebbene $\pi_h(V)$ non sia uguale a $\mathcal{V}(I_h)$, ciò che manca affinché sussista l'uguaglianza è una varietà affine strettamente inclusa in $\mathcal{V}(I_h)$. Proveremo questo secondo punto nel caso $h=1$, in quanto la dimostrazione, nel caso $h > 1$, richiede tecniche che vanno al di là di questa trattazione.

A questo scopo si ricorre al teorema di estensione geometrico e, in particolare, alla decomposizione

$$\mathcal{V}(I_1) = \pi_1(V) \cup [\mathcal{V}(c_1, \dots, c_s) \cap \mathcal{V}(I_1)].$$

Sia $W = \mathcal{V}(c_1, \dots, c_s) \cap \mathcal{V}(I_1)$. Per quanto osservato in precedenza W è una varietà affine, per cui se $W \neq \mathcal{V}(I_1)$ il teorema è dimostrato.

Resta da esaminare il caso in cui $W = \mathcal{V}(I_1)$ che, come visto nell'esempio, può accadere. Sia dunque

$$W = \mathcal{V}(c_1, \dots, c_s) \cap \mathcal{V}(I_1) = \mathcal{V}(I_1).$$

Considerato l'ideale $\bar{I} = \langle f_1, \dots, f_s, c_1, \dots, c_s \rangle$, si dimostra che:

$$V = \mathcal{V}(I) = \mathcal{V}(\bar{I}).$$

Infatti, è ovvio che $I \subset \bar{I}$, da cui $\mathcal{V}(\bar{I}) \subset \mathcal{V}(I)$. Per dimostrare l'inclusione opposta, sia $(a_1, \dots, a_n) \in V$. Ogni f_i si annulla in tal punto, e siccome $(a_2, \dots, a_n) \in \pi_1(V) \subset \mathcal{V}(I_1) = W$, segue che le c_i si annullano in (a_2, \dots, a_n) , ossia $(a_1, \dots, a_n) \in \mathcal{V}(f_1, \dots, f_s, c_1, \dots, c_s)$.

Si noti che sebbene gli ideali \bar{I} ed I siano diversi, le varietà da essi definite coincidono. Anche per quanto riguarda i corrispondenti ideali di eliminazione vale lo stesso discorso, ovvero sebbene $\bar{I}_1 \neq I_1$, si ha $\mathcal{V}(\bar{I}_1) = \mathcal{V}(I_1)$.

Posto

$$\bar{f}_i = f_i - c_i x_1^{N_i}, \quad \forall i = 1, \dots, s,$$

si noti che ogni \bar{f}_i o è uguale a zero, oppure ha grado, rispetto ad x_1 , minore del grado di f_i . Inoltre

$$\bar{I} = \langle f_1, \dots, f_s, c_1, \dots, c_s \rangle = \langle \bar{f}_1, \dots, \bar{f}_s, c_1, \dots, c_s \rangle,$$

come si può verificare per esercizio. Se si applica il teorema di estensione geometrico a $\mathcal{V}(\bar{f}_1, \dots, \bar{f}_s, c_1, \dots, c_s)$, essendo diversi i coefficienti direttori dei generatori, si ottiene una decomposizione diversa

$$\mathcal{V}(I_1) = \mathcal{V}(\bar{I}_1) = \pi_1(V) \cap \bar{W},$$

dove \bar{W} è l'insieme delle soluzioni parziali in cui si annullano i coefficienti direttori di $\bar{f}_1, \dots, \bar{f}_s, c_1, \dots, c_s$.

In generale, non ci sono garanzie che \bar{W} sia più piccola di $\mathcal{V}(I_1)$; può accadere che $\bar{W} = \mathcal{V}(I_1)$, ed in tal caso si riapplica il procedimento visto

sopra. Se si ottiene una varietà più piccola di $\mathcal{V}(I_1)$ la dimostrazione è completata.

Rimane da studiare il caso in cui si ottiene sempre $\mathcal{V}(I_1)$. A questo proposito si osservi che ogni volta che si ripete il processo descritto sopra, il grado rispetto ad x_1 dei generatori diminuisce, fino eventualmente ad annullarsi. Questo significa che V può essere definita dall'annullarsi di polinomi in $k[x_2, \dots, x_n]$. Quindi, se (a_2, \dots, a_n) è una soluzione parziale, per ogni a_1 appartenente a k , risulta che $(a_1, \dots, a_n) \in V$, che per ipotesi è non vuota (questo in quanto x_1 non compare nelle equazioni che definiscono V). Pertanto *ogni* soluzione parziale si estende, il che prova che $\pi_1(V) = \mathcal{V}(I_1)$. In tal caso la parte (ii) del teorema è soddisfatta per $W = \emptyset$ ed il teorema è dimostrato. ■

Dal Teorema di Chiusura sappiamo che $\pi_h(V)$ riempie $\mathcal{V}(I_h)$ a meno di punti che appartengono ad una varietà W strettamente inclusa in $\mathcal{V}(I_h)$. Può però accadere che tali punti non riempiano W . Precisamente, la struttura di $\pi_h(V)$ può essere descritta nel seguente modo: esistono varietà affini $Z_i \subset W_i \subset \mathbf{C}^{n-h}$, per $1 \leq i \leq l$, tali che

$$\pi_h(V) = \bigcup_{i=1}^l (W_i - Z_i).$$

In generale un insieme che ha tale forma è detto *insieme costruibile*.

3.3 Implicitizzazione

Nel corso del Capitolo 1, si è visto come una varietà affine possa essere descritta utilizzando le equazioni parametriche. Il problema principale che si presenta, volendo “eliminare” i parametri e passare ad “equazioni cartesiane” della varietà è nel fatto che una parametrizzazione può non riempire tutta la varietà (come visto nel caso specifico della circonferenza). Formalmente il problema dell’implicitizzazione si divide in tre passi:

- determinare la più piccola varietà affine W contenente l’immagine della parametrizzazione;
- stabilire se la parametrizzazione riempie o meno tale varietà W ;
- nel caso in cui la parametrizzazione non riempia tutta W , determinare i punti mancanti.

In questo paragrafo, si farà uso della teoria dell’eliminazione per dare una risposta completa a tale problema. Faremo vedere che anche il secondo passo si può risolvere utilizzando basi di Groebner e il teorema di estensione.

Illustreremo quanto sopra indicato nel caso della superficie tangenziale alla cubica sghemba in \mathbf{R}^3 già definita nel Capitolo 1. Tale superficie ammette la parametrizzazione polinomiale

$$\begin{cases} x = t + u, \\ y = t^2 + 2tu, \\ z = t^3 + 3t^2u. \end{cases}$$

Calcolando la base di Groebner G per l’ideale $I = \langle x - t - u, y - t^2 - 2tu, z - t^3 - 3t^2u \rangle$, rispetto all’ordine lessicografico con $t > u > x > y > z$, si trovano come vedremo tra breve 7 elementi g_1, \dots, g_7 . Di questi solo

$$g_7 = x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2$$

non contiene t ed u . La varietà V definita da g_7 è una superficie contenente la superficie tangenziale alla cubica sghemba. Non sappiamo comunque né se V sia la più piccola varietà contenente tale superficie né, in caso affermativo, se la superficie tangenziale riempia completamente la $\mathcal{V}(g_7)$.

Cominceremo a risolvere il problema di implicitizzazione nel caso di *parametrizzazioni polinomiali*.

3.3.1 Implicitizzazione per parametrizzazioni polinomiali

Sia data la parametrizzazione polinomiale

$$\begin{aligned} x_1 &= f_1(t_1, \dots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \dots, t_m), \end{aligned} \tag{3.1}$$

con f_1, \dots, f_n polinomi di $k[t_1, \dots, t_m]$. Geometricamente possiamo pensare tale parametrizzazione come una funzione

$$F : k^m \longrightarrow k^n$$

definita da: $F(t_1, \dots, t_m) = (f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m))$. Sotto queste ipotesi $F(k^m) \subseteq k^n$ è l'immagine della parametrizzazione (3.1). Il problema dell'implicitizzazione si riconduce dunque a trovare la più piccola varietà contenente $F(k^m)$, ovvero la chiusura $\overline{F(k^m)}$, rispetto alla topologia di Zariski.

Possiamo riscrivere la (3.1) come un sistema di equazioni polinomiali

$$\begin{cases} x_1 - f_1(t_1, \dots, t_m) = 0, \\ \vdots \\ x_n - f_n(t_1, \dots, t_m) = 0, \end{cases}$$

definite in $k[t_1, \dots, t_m, x_1, \dots, x_n]$. L'ideale associato

$$I = \langle x_1 - f_1(t_1, \dots, t_m), \dots, x_n - f_n(t_1, \dots, t_m) \rangle$$

individua la varietà

$$V = \mathcal{V}(x_1 - f_1, \dots, x_n - f_n) \subset k^{n+m},$$

i cui punti possono essere scritti nella forma

$$(t_1, \dots, t_m, f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)),$$

il che mostra che V si può considerare il *grafico* della funzione F . Restano individuate inoltre due funzioni:

$$i : k^m \longrightarrow k^{n+m}, \quad \pi_m : k^{n+m} \longrightarrow k^m$$

definite nel modo seguente:

$$i(t_1, \dots, t_m) = (t_1, \dots, t_m, f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m)),$$

$$\pi_m(t_1, \dots, t_m, x_1, \dots, x_n) = (x_1, \dots, x_n).$$

Il seguente diagramma:

$$\begin{array}{ccc} & k^{n+m} & \\ i \nearrow & & \searrow \pi_m \\ k^m & \xrightarrow{F} & k^n \end{array}$$

è commutativo. Dunque l'applicazione F è data dalla composizione $F = \pi_m \circ i$. Inoltre $i(k^m) = V$, per cui si ha l'uguaglianza

$$F(k^m) = \pi_m(i(k^m)) = \pi_m(V),$$

ossia l'immagine della parametrizzazione è la proiezione del suo grafico. Si vuole ora determinare quale sia la più piccola varietà contenente $F(k^m)$.

Teorema 3.3.1 (Teorema di implicitizzazione polinomiale) *Sia k un campo infinito. Si consideri la funzione $F : k^m \rightarrow k^n$ determinata dalla parametrizzazione polinomiale (3.1), e siano I l'ideale*

$$I = \langle x_1 - f_1, \dots, x_n - f_n \rangle \leq k[t_1, \dots, t_m, x_1, \dots, x_n],$$

e $I_m = I \cap k[x_1, \dots, x_n]$ l' m -simo ideale di eliminazione di I . In tali ipotesi, $\mathcal{V}(I_m)$ è la più piccola varietà affine in k^n contenente $F(k^m)$, ossia

$$\mathcal{V}(I_m) = \overline{F(k^m)}.$$

Dimostrazione. Sia $V = \mathcal{V}(I) \subset k^{n+m}$. Da quanto osservato in precedenza V è il grafico della funzione $F : k^m \rightarrow k^n$.

Se k è un campo algebricamente chiuso, dal Teorema di Chiusura sappiamo che $\mathcal{V}(I_m)$ è la più piccola varietà contenente $\pi_m(V)$, ossia

$$\mathcal{V}(I_m) = \overline{\pi_m(V)}.$$

Dal diagramma commutativo si ha inoltre

$$F(k^m) = \pi_m(V),$$

da cui segue l'asserto.

Supponiamo ora che k sia un sottocampo del campo complesso \mathbf{C} . Il campo k contiene il campo fondamentale \mathbf{Q} dei razionali e, pertanto è infinito. Poiché k può essere strettamente più piccolo di \mathbf{C} non si può usare

direttamente il teorema di chiusura. La strategia sarà quella di passare da k a \mathbf{C} scrivendo in indice il campo sul quale si stanno facendo le varie considerazioni. Quindi, $\mathcal{V}_k(I_m)$ sarà la varietà di k^n definita da I_m , mentre $\mathcal{V}_{\mathbf{C}}(I_m)$ sarà la varietà di \mathbf{C}^n definita da I_m . Si deve dimostrare che $\mathcal{V}_k(I_m)$ è la più piccola varietà di k^n contenente $F(k^m)$.

Per il Lemma 3.2.1. sappiamo che $F(k^m) = \pi_m(V_k(I)) \subset \mathcal{V}_k(I_m)$. Per dimostrare che $\mathcal{V}_k(I_m)$ è la più piccola, proviamo che se esiste un'altra varietà Z_k contenente $F(k^m)$, deve necessariamente essere $Z_k \supseteq \mathcal{V}_k(I_m)$.

Sia $Z_k = \mathcal{V}(g_1, \dots, g_s) \subset k^n$ una varietà di k^n tale che $F(k^m) \subset Z_k$; cominciamo con il notare che i g_i ($i = 1, \dots, s$), essendo nulli su Z_k sono a maggior ragione nulli sull'insieme più piccolo $F(k^m)$, ossia per ogni $i = 1, \dots, s$

$$g_i \circ F : k^m \longrightarrow k$$

è un polinomio a coefficienti in k che svanisce su tutti i punti di k^m . Essendo $k \subset \mathbf{C}$ un campo infinito ne segue, per il principio di identità dei polinomi, che per ogni $i = 1, \dots, s$ anche $g_i \circ F$ è identicamente nullo su \mathbf{C}^m e pertanto i g_i svaniscono su $F(\mathbf{C}^m)$. Quindi $Z_{\mathbf{C}} = \mathcal{V}_{\mathbf{C}}(g_1, \dots, g_s)$ è una varietà di \mathbf{C}^n contenente $F(\mathbf{C}^m)$.

Poiché il teorema è vero per $k = \mathbf{C}$, risulta $\mathcal{V}_{\mathbf{C}}(I_m) \subseteq Z_{\mathbf{C}}$ in \mathbf{C}^n . Guardando alle soluzioni che giacciono in k^n , segue immediatamente che $\mathcal{V}_k(I_m) \subseteq Z_k$. Questo dimostra che $\mathcal{V}_k(I_m)$ è la più piccola varietà di k^n contenente $F(k^m)$.

Nel caso in cui k sia un campo infinito non necessariamente contenuto in \mathbf{C} , se ne considera la chiusura algebrica \bar{k} , e, poiché il teorema di chiusura vale in ogni campo algebricamente chiuso, la dimostrazione è simile a quella sopra esposta, a patto di sostituire alla coppia (k, \mathbf{C}) la coppia (k, \bar{k}) . ■

Il *teorema di implicitizzazione polinomiale* fornisce un algoritmo per trovare le equazioni implicite di una parametrizzazione: data infatti la parametrizzazione

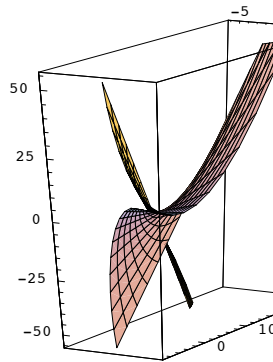
$$\begin{aligned} x_1 &= f_1(t_1, \dots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \dots, t_m), \end{aligned}$$

con $f_1, \dots, f_n \in k[t_1, \dots, t_m]$, si considera l'ideale $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle$ e si calcola la base di Groebner rispetto all'ordine lessicografico con $t_1 > \dots > t_m > x_1 > \dots > x_n$. Dal teorema di eliminazione sappiamo che gli elementi della base di Groebner che non dipendono da $t_1 > \dots > t_m$ formano una base per I_m , e per il teorema precedente si ha che essi definiscono la più piccola varietà di k^n contenente la parametrizzazione.

Illustriamo quanto detto con l'esempio della superficie tangenziale alla cubica sghemba in \mathbf{R}^3 definita dalla parametrizzazione polinomiale

$$\begin{cases} x = t + u, \\ y = t^2 + 2tu, \\ z = t^3 + 3t^2u. \end{cases}$$

il cui grafico è:



Dobbiamo considerare l'ideale $I = \langle x - t - u, y - t^2 - 2tu, z - t^3 - 3t^2u \rangle$; una base di Groebner per I , rispetto all'ordine lessicografico con $t > u > x > y > z$, è data da:

$$\begin{aligned} g_1 &= t + u - x, \\ g_2 &= u^2 - x^2 + y, \\ g_3 &= ux^2 - uy - x^3 + (3/2)xy - (1/2)z, \\ g_4 &= uxy - uz - x^2y - xz - 2y^2, \\ g_5 &= uxz - uy^2 + x^2z - (1/2)xy^2 - (1/2)yz, \\ g_6 &= uy^3 - uz^2 - 2x^2yz + (1/2)xy^3 - xz^2 + (5/2)y^2z, \\ g_7 &= x^3z - (3/4)x^2y^2 - (3/2)xyz + y^3 + (1/4)z^2. \end{aligned}$$

Il teorema di eliminazione ci dice che $I_2 = I \cap \mathbf{R}[x, y, z] = \langle g_7 \rangle$, mentre dal teorema precedente si ha che $\mathcal{V}(g_7)$ è la più piccola varietà affine contenente la superficie tangenziale.

Ciò che ancora non sappiamo è se tale superficie tangenziale riempie o meno $\mathcal{V}(g_7)$. Per rispondere a tale problema dobbiamo vedere se tutte le soluzioni parziali $(x, y, z) \in \mathcal{V}(I_2)$ si estendono ad una soluzione completa $(t, u, x, y, z) \in \mathcal{V}(I)$.

Se il campo è algebricamente chiuso si utilizza il teorema di estensione, che in questo caso ci assicura che ogni soluzione $(x, y, z) \in \mathcal{V}(I_2)$ si estende ad

una $(u, x, y, z) \in \mathcal{V}(I_1)$, in quanto I_1 ha un generatore, g_2 , il cui coefficiente direttore rispetto ad u è costante. Si riapplica poi il teorema di estensione alle soluzioni parziali $(u, x, y, z) \in \mathcal{V}(I_1)$, che di nuovo è possibile estendere in quanto I ha un generatore, g_1 , il cui coefficiente direttore rispetto a t è costante.

Se il campo non è algebricamente chiuso, non è possibile decidere a priori se una soluzione è estendibile o meno; nell'esempio precedente in cui $k = \mathbf{R}$, partendo da una soluzione $(x, y, z) \in \mathbf{R}^3$ di $g_7 = 0$, sappiamo che questa si estende ad una soluzione $(t, u, x, y, z) \in \mathcal{V}(I) \subset \mathbf{C}^5$, ma non sappiamo se t ed u siano reali. Guardando però alla base di Groebner si vede facilmente come t ed u siano reali quando $(x, y, z) \in \mathbf{R}^3$. Infatti, ricavando u da $g_3 = 0$ segue che, per $y \neq x^2$ la $u \in \mathbf{R}$ se $x, y, z \in \mathbf{R}$; ma per $y = x^2$ la $g_2 = 0$ implica che $u = 0$ e quindi è ancora reale. Poiché $u, x, y, z \in \mathbf{R}$ dalla $g_1 = 0$ si deduce che anche $t = x - u$ è reale. Ne segue che la superficie tangenziale alla cubica sghemba in \mathbf{R}^3 coincide con la varietà definita da $g_7 = 0$.

3.3.2 Implicitizzazione per parametrizzazioni razionali

In generale una parametrizzazione razionale è del tipo

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \dots, t_m)}{g_1(t_1, \dots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \dots, t_m)}{g_n(t_1, \dots, t_m)}, \end{aligned} \tag{3.2}$$

dove $f_1, g_1, \dots, f_n, g_n$ sono polinomi di $k[t_1, \dots, t_m]$. L'applicazione $F : k^m \rightarrow k^n$ non è più definita in tutto k^m (a causa dei denominatori), ma in $k^m - \mathcal{V}(g_1 \cdots g_n)$. Sarà quindi del tipo

$$\begin{aligned} F : k^m - \mathcal{V}(g_1 \cdots g_n) &\longrightarrow k^n \\ (t_1, \dots, t_m) &\longmapsto \left(\frac{f_1}{g_1}, \dots, \frac{f_n}{g_n} \right) \end{aligned}$$

Per risolvere il problema di implicitizzazione dobbiamo trovare la più piccola varietà di k^n contenente $F(k^m - \mathcal{V}(g_1 \cdots g_n))$. Riscriviamo il sistema (3.2) nella forma

$$\begin{cases} \varphi_1 = g_1(t_1, \dots, t_m)x_1 - f_1(t_1, \dots, t_m) = 0, \\ \vdots \\ \varphi_n = g_n(t_1, \dots, t_m)x_n - f_n(t_1, \dots, t_m) = 0, \end{cases}$$

dove le $\varphi_i \in k[t_1, \dots, t_m, x_1, \dots, x_n]$, per $i = 1, \dots, n$, sono ottenute eliminando i denominatori dalla (3.2). Consideriamo quindi l'ideale $I = \langle \varphi_1, \dots, \varphi_n \rangle$ e la varietà $\mathcal{V}(I) \subseteq k^{n+m}$. Posto $W = \mathcal{V}(g_1 \cdots g_n)$ si definiscono le due applicazioni:

$$\begin{aligned} i : k^m - W &\longrightarrow k^{n+m} \\ (t_1, \dots, t_m) &\longmapsto (t_1, \dots, t_m, \frac{f_1}{g_1}, \dots, \frac{f_n}{g_n}); \\ \\ \pi_m : k^{n+m} &\longrightarrow k^n \\ (t_1, \dots, t_m, x_1, \dots, x_n) &\longmapsto (x_1, \dots, x_n). \end{aligned}$$

È facile verificare che $i(k^m - W) \subset \mathcal{V}(I)$, ma in questo caso non è detto che $\mathcal{V}(I)$ sia la più piccola varietà contenente $i(k^m - W)$.

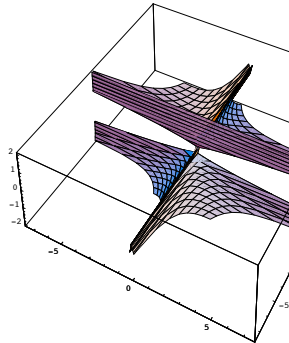
Possiamo scrivere il diagramma nel modo

$$\begin{array}{ccc} & k^{n+m} & \\ i \nearrow & & \searrow \pi_m \\ k^m - W & \xrightarrow{F} & k^n \end{array}$$

Vediamo un esempio che chiarisce quanto detto, ovvero che nel caso di parametrizzazioni razionali $\mathcal{V}(I_m)$ non è in generale la varietà minima contenente $F(k^m - W)$. Si consideri la parametrizzazione:

$$\begin{cases} x = u^2/v, \\ y = v^2/u, \\ z = u, \end{cases}$$

il cui grafico è :



ossia l'applicazione

$$F : k^2 - \mathcal{V}(u \cdot v) \longrightarrow k^3.$$

Con semplici sostituzioni si ottiene l'equazione implicita $z(x^2y - z^3) = 0$, ossia la varietà $V = \mathcal{V}(z) \cup \mathcal{V}(x^2y - z^3)$, ma $\mathcal{V}(z)$ non può far parte della parametrizzazione in quanto $z = u$ e $u \neq 0$, quindi la varietà minima contenente $F(k^2 - \mathcal{V}(u \cdot v))$ è $\mathcal{V}(x^2y - z^3)$, e non $\mathcal{V}(z) \cup \mathcal{V}(x^2y - z^3)$.

Lo stesso risultato si ottiene con il metodo dell'eliminazione, infatti eliminando i denominatori dalla parametrizzazione iniziale si ha

$$\begin{cases} vx = u^2, \\ uy = v^2, \\ z = u. \end{cases}$$

Calcolando la base di Groebner per l'ideale $I = \langle vx - u^2, uy - v^2, z - u \rangle$, e calcolando il secondo ideale di eliminazione $I_2 = I \cap k[x, y, z]$, si ottiene

$$I_2 = \langle z(x^2y - z^3) \rangle.$$

Anche in questo caso si è arrivati alla varietà $\mathcal{V}(I_2) = \mathcal{V}(z) \cup \mathcal{V}(x^2y - z^3)$ che, per quanto osservato in precedenza, non è la varietà minima contenente l'immagine della parametrizzazione.

Si rende quindi necessario trovare un'altra tecnica nel caso di parametrizzazioni razionali. Introduciamo a questo scopo una variabile aggiuntiva y per il controllo dei denominatori.

Si consideri l'anello dei polinomi $k[y, t_1, \dots, t_m, x_1, \dots, x_n]$ e lo spazio affine k^{n+m+1} . Sia inoltre g il prodotto $g = g_1 \cdot g_2 \cdot \dots \cdot g_n$, e quindi $W = \mathcal{V}(g)$. Consideriamo poi l'ideale

$$J = \langle g_1x_1 - f_1, \dots, g_nx_n - f_n, 1 - gy \rangle \subseteq k[y, t_1, \dots, t_m, x_1, \dots, x_n].$$

L'equazione $1 - gy = 0$ implica che i denominatori g_1, \dots, g_n non si annullano mai in $\mathcal{V}(J)$. Si definiscono inoltre le applicazioni

$$j : k^m - W \longrightarrow k^{n+m+1}$$

$$(t_1, \dots, t_m) \longmapsto \left(\frac{1}{g}, t_1, \dots, t_m, \frac{f_1}{g_1}, \dots, \frac{f_n}{g_n} \right);$$

$$\pi_{m+1} : k^{n+m+1} \longrightarrow k^n$$

$$(y, t_1, \dots, t_m, x_1, \dots, x_n) \longmapsto (x_1, \dots, x_n).$$

Si ottiene così il diagramma

$$\begin{array}{ccc}
 & k^{n+m+1} & \\
 j \nearrow & & \searrow \pi_{m+1} \\
 k^m - W & \xrightarrow{F} & k^n
 \end{array}$$

Dalla commutatività del diagramma si ha $F = \pi_{m+1} \circ j$. Si dimostra inoltre che $j(k^m - W) = \mathcal{V}(J)$ in k^{n+m+1} ; infatti dalla definizione di j e J segue facilmente $j(k^m - W) \subset \mathcal{V}(J)$. Per quanto riguarda l'inclusione inversa, se $(y, t_1, \dots, t_m, x_1, \dots, x_n) \in \mathcal{V}(J)$, allora la condizione $g(t_1, \dots, t_m)y = 1$ implica che nessun g_i si annulla in (t_1, \dots, t_m) , per cui l'uguaglianza $g_i(t_1, \dots, t_m)x_i = f_i(t_1, \dots, t_m)$ è risolta per $x_i = f_i(t_1, \dots, t_m)/g_i(t_1, \dots, t_m)$. Siccome $y = 1/g$ ove $g = \prod g_i$, si ha che $(y, t_1, \dots, t_m, x_1, \dots, x_n) \in j(k^m - W)$. Questo prova che $\mathcal{V}(J) \subset j(k^m - W)$.

Da $F = \pi_{m+1} \circ j$ e $j(k^m - W) = \mathcal{V}(J)$, otteniamo

$$F(k^m - W) = \pi_{m+1}(j(k^m - W)) = \pi_{m+1}(\mathcal{V}(J)).$$

Ciò significa che l'immagine della parametrizzazione è la proiezione della varietà $\mathcal{V}(J)$. Utilizziamo ora la teoria dell'eliminazione per risolvere il problema di implicitizzazione.

Teorema 3.3.2 (Teorema di implicitizzazione razionale) *Sia k un campo infinito e sia $F : k^m - W \rightarrow k^n$ la funzione determinata dalla parametrizzazione razionale (3.2). Posto $g = g_1 \cdot g_2 \cdot \dots \cdot g_n$, consideriamo l'ideale*

$$J = \langle g_1x_1 - f_1, \dots, g_nx_n - f_n, 1 - gy \rangle$$

di $k[y, t_1, \dots, t_m, x_1, \dots, x_n]$ e sia $J_{m+1} = J \cap k[x_1, \dots, x_n]$ l' $(m+1)$ -simo ideale di eliminazione di J . La varietà $\mathcal{V}(J_{m+1})$ è la più piccola varietà di k^n contenente $F(k^m - W)$.

Dimostrazione. La dimostrazione è analoga a quella del teorema di implicitizzazione per parametrizzazioni polinomiali, per cui si preferisce ometterla. ■

Abbiamo così un **algoritmo di implicitizzazione per parametrizzazioni razionali**: data la parametrizzazione $x_i = f_i/g_i$, con $i = 1, \dots, n$ e $f_i, g_i \in k[t_1, \dots, t_m]$, $g_i \neq 0$, introduciamo una nuova variabile y e, considerato l'ideale $J = \langle g_1x_1 - f_1, \dots, g_nx_n - f_n, 1 - gy \rangle$, dove $g = g_1 \cdot g_2 \cdot \dots \cdot g_n$, se ne calcola la base di Groebner rispetto all'ordine lessicografico con $y >$

$t_1 > \dots > t_m > x_1 > \dots > x_n$. Gli elementi della base che non dipendono da y, t_1, \dots, t_m definiscono la più piccola varietà di k^n contenente la parametrizzazione. La parametrizzazione riempie tale varietà minima se ogni soluzione parziale si estende ad una completa.

Al fine di illustrare quanto detto, riprendiamo l'esempio della parametrizzazione razionale:

$$\begin{cases} x = u^2/v, \\ y = v^2/u, \\ z = u. \end{cases}$$

Introduciamo la nuova variabile w , ed alle equazioni polinomiali

$$\begin{cases} vx = u^2, \\ uy = v^2, \\ z = u, \end{cases}$$

aggiungiamo l'equazione $1 - wuv = 0$. Rispetto all'ordine lessicografico in cui $w > u > v > x > y > z$ consideriamo l'ideale

$$J = \langle u^2 - vx, uy - v^2, u - z, wuv - 1 \rangle.$$

Una base di Groebner per J è $G = \{g_1, \dots, g_8\}$, dove:

$$\begin{aligned} g_1 &= u - z, \\ g_2 &= v^2 - yz, \\ g_3 &= vx - z^2, \\ g_4 &= -wz^3 + x, \\ g_5 &= -wyz^2 + v, \\ g_6 &= vz - xy, \\ g_7 &= wxy - 1, \\ g_8 &= x^2y - z^3, \end{aligned}$$

da cui $J_3 = J \cap k[x, y, z] = \langle g_8 \rangle = \langle x^2y - z^3 \rangle$. Come già osservato, $\mathcal{V}(x^2y - z^3)$ è la più piccola varietà affine contenente la parametrizzazione.

3.4 Punti singolari e Inviluppi

In questo paragrafo si studieranno gli *inviluppi algebrici* di famiglie di curve. Il nostro scopo sarà mostrare come le equazioni fornite dalla geometria possano essere risolte con le tecniche fin qui studiate.

3.4.1 Punti singolari

Riprendendo la definizione data nel Capitolo 1 di *punti singolari*, ed introducendo la nozione di *gradiente* di f , definito come

$$\nabla f = \left(\frac{\partial}{\partial x} f, \frac{\partial}{\partial y} f \right),$$

ci si pone il problema della ricerca di punti singolari di una curva. Si osservi che affinché un punto sia singolare devono essere soddisfatte sia la condizione di appartenenza del punto alla curva, sia quella di annullamento del vettore gradiente ∇f . In termini di equazioni

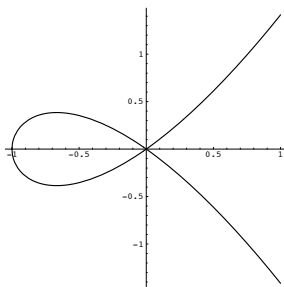
$$f = \frac{\partial}{\partial x} f = \frac{\partial}{\partial y} f = 0.$$

Per risolvere tali sistemi si adoperano i metodi descritti nei paragrafi 1 e 2.

Esempio: Si consideri in \mathbf{R}^2 la curva di equazione $y^2 = x^2(1+x)$. Per trovare i punti singolari di tale curva bisogna risolvere il sistema:

$$\begin{cases} f = y^2 - x^2 - x^3 = 0, \\ \frac{\partial}{\partial x} f = -2x - 3x^2 = 0, \\ \frac{\partial}{\partial y} f = 2y = 0. \end{cases}$$

Da queste equazioni si vede facilmente come il punto $(0, 0)$ sia l'unico punto singolare di $\mathcal{V}(f)$. Tale risultato è in accordo con il grafico della curva.

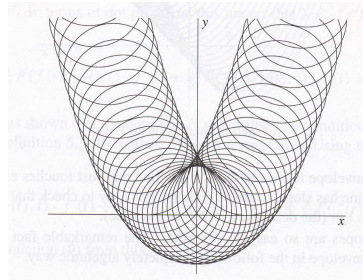


3.4.2 Involuppi

Allo scopo di spiegare quello che intendiamo per *inviluppo*, mostriamo un esempio. Sia k il campo dei reali \mathbf{R} e $t \in \mathbf{R}$. Studiamo l'equazione di una circonferenza in \mathbf{R}^2 definita dall'equazione

$$(x - t)^2 + (y - t^2)^2 = 4. \quad (3.3)$$

Siccome (t, t^2) parametrizza una parabola, possiamo pensare alla (3.3) come alla famiglia di circonferenze di raggio 2 in \mathbf{R}^2 il cui centro si muove sulla parabola di equazione $y = x^2$.



Si noti che la curva di frontiera è tangente contemporaneamente a tutte le circonferenze della famiglia. Questo è un caso particolare di involuppo di una famiglia di curve. L'idea di base è che l'inviluppo di una famiglia di curve è quella singola curva che è tangente a tutte le curve della famiglia. Ci proponiamo di studiare gli involuppi ed in particolare di trovare un procedimento per determinarne le equazioni.

Prima di dare una definizione formale di involuppo di una famiglia di curve, definiamo cosa intendiamo per **famiglia di curve** in \mathbf{R}^2 .

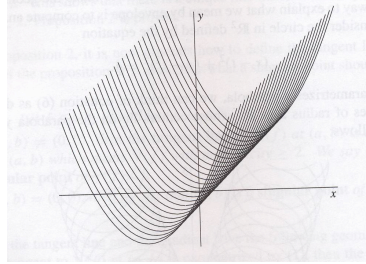
Definizione 3.4.1 Dato un polinomio $F \in \mathbf{R}[x, y, t]$ e fissato $t \in \mathbf{R}$, la varietà in \mathbf{R}^2 definita dall'equazione $F(x, y, t) = 0$ è $\mathcal{V}(F_t)$, e la **famiglia di curve** determinata da F si ottiene da $\mathcal{V}(F_t)$, al variare di t in \mathbf{R} .

Nella precedente definizione t è il parametro che ci indica quale curva della famiglia stiamo considerando.

Come altro esempio di famiglia di curve e relativo involuppo, consideriamo le curve definite dall'equazione

$$F(x, y, t) = (x - t)^2 - y + t = 0. \quad (3.4)$$

Riscrivendola come $y - t + (x - t)^2$, vediamo come la (3.4) descriva la famiglia $\mathcal{V}(F_t)$ di parabole ottenute trasladando la parabola di equazione $y = x^2$ lungo la bisettrice del primo e terzo quadrante $y = x$:



In questo caso, l'inviluppo è dato dalla retta che *tocca* ogni parabola della famiglia, ossia da $y = x - 1/4$.

Diamo ora una caratterizzazione algebrica di inviluppo.

Definizione 3.4.2 *Data una famiglia $\mathcal{V}(F_t)$ di curve in \mathbf{R}^2 , il suo inviluppo consiste di tutti i punti $(x, y) \in \mathbf{R}^2$ che soddisfino alle condizioni*

$$\begin{aligned} F(x, y, t) &= 0, \\ \frac{\partial}{\partial t} F(x, y, t) &= 0, \end{aligned}$$

al variare di t in \mathbf{R} .

Si fornisce nel seguito una spiegazione, non rigorosa, di come si è arrivati alla condizione $\frac{\partial}{\partial t} F = 0$. Per maggiori dettagli si veda BRUCE e GIBLIN (1984), [cfr[3]].

Data una famiglia $\mathcal{V}(F_t)$, pensiamo all'inviluppo come ad una curva C che in ogni suo punto sia tangente ad una delle curve $\mathcal{V}(F_t)$ della famiglia. Supponiamo che C sia parametrizzata da

$$\begin{aligned} x &= f(t), \\ y &= g(t). \end{aligned}$$

Assumeremo che al tempo t , il punto $(f(t), g(t))$ appartenga alla curva $\mathcal{V}(F_t)$, ossia che C incontri tutti gli elementi della famiglia. Da un punto di vista algebrico, questo significa

$$F(f(t), g(t), t) = 0, \text{ per ogni } t \in \mathbf{R}. \quad (3.5)$$

Affinché C sia l'involuppo della famiglia, dobbiamo determinare quando C è tangente a $\mathcal{V}(F_t)$ in $(f(t), g(t))$. Sappiamo che il vettore tangente a C è $(f'(t), g'(t))$.

Così come visto per $\mathcal{V}(F_t)$, abbiamo il gradiente $\nabla F = (\frac{\partial}{\partial x} F, \frac{\partial}{\partial y} F)$, e sappiamo che ∇F è perpendicolare alla retta tangente a $\mathcal{V}(F_t)$. Affinché C sia tangente a $\mathcal{V}(F_t)$, il vettore tangente $(f'(t), g'(t))$ deve quindi essere perpendicolare al gradiente ∇F . In termini di *prodotto scalare* questo significa che $\nabla F \cdot (f'(t), g'(t)) = 0$ o, equivalentemente,

$$\frac{\partial}{\partial x} F(f(t), g(t), t) \cdot f'(t) + \frac{\partial}{\partial y} F(f(t), g(t), t) \cdot g'(t) = 0. \quad (3.6)$$

Abbiamo così mostrato che l'involuppo è determinato dalle condizioni (3.5) e (3.6). Differenziando la (3.5) rispetto a t ci si riconduce alla definizione di *involuppo*. Infatti:

$$\frac{\partial}{\partial x} F(f(t), g(t), t) f'(t) + \frac{\partial}{\partial y} F(f(t), g(t), t) g'(t) + \frac{\partial}{\partial t} F(f(t), g(t), t) = 0.$$

Sottraendo da quest'ultima equazione la (3.6), otteniamo

$$\frac{\partial}{\partial t} F(f(t), g(t), t) = 0. \quad (3.7)$$

Come conseguenza della definizione (3.4.2) si ha che l'involuppo di $\mathcal{V}(F_t)$ è determinato dalle equazioni

$$\begin{aligned} F(x, y, t) &= 0, \\ \frac{\partial}{\partial t} F(x, y, t) &= 0. \end{aligned}$$

Si noti che nelle precedenti equazioni, x e y stanno ad indicare dove siamo sull'involuppo, mentre la t indica a quale curva della famiglia siamo tangenti. Siccome in queste equazioni compaiono la x , la y e la t , dobbiamo eliminare la t per trovare l'equazione dell'involuppo. Per fare ciò, si applica la teoria dell'eliminazione studiata nei precedenti paragrafi.

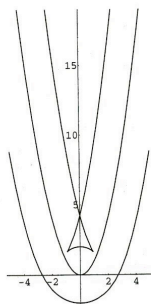
A titolo di **esempio** consideriamo di nuovo la famiglia di circonferenze il cui centro appartiene alla parabola di equazione $y = x^2$. In questo caso $F = (x - t)^2 + (y - t^2)^2 - 4$, per cui l'involuppo è descritto dalle equazioni

$$\begin{aligned} F &= (x - t)^2 + (y - t^2)^2 - 4 = 0, \\ \frac{\partial}{\partial t} F &= -2(x - t) - 4t(y - t^2) = 0. \end{aligned} \quad (3.8)$$

Utilizzando l'ordine lessicografico con $t > x > y$, una base di Groebner è data da:

$$\begin{aligned}
 g_1 &= -1156 + 688x^2 - 191x^4 + 16x^6 + 544y + 30x^2y - 40x^4y \\
 &\quad + 225y^2 - 96x^2y^2 + 16x^4y^2 - 136y^3 - 32x^2y^3 + 16y^4, \\
 g_2 &= (7327 - 1928y - 768y^2 - 896y^3 + 256y^4)t + 6929x - 2946x^3 \\
 &\quad + 224x^5 + 2922xy - 1480x^3y + 128x^5y - 792xy^2 - 224x^3y^2 \\
 &\quad - 544xy^3 + 128x^3y^3 - 384xy^4, \\
 g_3 &= (431x - 12xy - 48xy^2 - 64xy^3)t + 952 - 159x^2 - 16x^4 + 320y \\
 &\quad - 214x^2y + 32x^4y - 366y^2 - 32x^2y^2 - 80y^3 + 32x^2y^3 + 32y^4, \\
 g_4 &= (697 - 288x^2 + 108y - 336y^2 + 64y^3)t + 23x - 174x^3 \\
 &\quad + 32x^5 + 322xy - 112x^3y + 32xy^2 + 32x^3y^2 - 96xy^3, \\
 g_5 &= 135t^2 + (26x + 40xy + 32xy^2)t - 128 + 111x^2 \\
 &\quad - 16x^4 + 64y + 8x^2y + 32y^2 - 16x^2y^2 - 16y^3.
 \end{aligned}$$

Abbiamo scritto gli elementi della base di Groebner come polinomi in t a coefficienti in $\mathbf{R}[x, y]$. Dal Teorema di Eliminazione sappiamo che g_1 genera il primo ideale di eliminazione. L'inviluppo giace quindi sulla curva di equazione $g_1 = 0$. Il grafico di g_1 insieme a quello della parabola di equazione $y = x^2$ è :



La particolarità di tale grafico è il *triangolo*, che appartiene all'inviluppo come si può facilmente verificare disegnando alcune circonferenze della famiglia.

Abbiamo dimostrato che l'inviluppo giace sulla varietà $\mathcal{V}(g_1)$, ma non sappiamo ancora se è uguale a $\mathcal{V}(g_1)$. In merito ci poniamo due quesiti interessanti:

- Se ogni punto di $\mathcal{V}(g_1)$ appartiene all'inviluppo, il che equivale a chiederci se ogni soluzione parziale (x, y) di (3.8) si estende ad una soluzione completa (x, y, t) .

- Dato un punto appartenente all'inviluppo, quante curve della famiglia sono tangenti all'inviluppo in tale punto. Questo equivale a stabilire per quante t , (x, y) si estende a (x, y, t) .

Il coefficiente direttore di t in g_5 è 135, ossia una costante. Il Teorema di Estensione garantisce quindi che ogni soluzione parziale si estende, a condizione di lavorare sui numeri complessi. Quindi, t esiste ma potrebbe essere un numero complesso. Questo esempio illustra le capacità ed i limiti del Teorema di Estensione, il quale garantisce l'esistenza di una soluzione, ma probabilmente nel campo sbagliato.

Ciò nonostante l'equazione $g_5 = 0$ fornisce delle informazioni utili: è quadratica in t , per cui un dato punto (x, y) si estende al più in due modi ad una soluzione completa, ne segue che *un punto dell'inviluppo è tangente al più a due circonferenze della famiglia*.

Per ulteriori informazioni consideriamo ora gli altri polinomi della base di Groebner. Si noti che g_2, g_3 e g_4 sono polinomi in cui la t compare solo al primo grado, per cui si possono scrivere nella forma

$$g_i = A_i(x, y)t + B_i(x, y), \quad i = 2, 3, 4.$$

Se A_i non si annulla in (x, y) per qualche $i = 2, 3, 4$, allora possiamo risolvere $A_i t + B_i = 0$ ottenendo

$$t = \frac{B_i(x, y)}{A_i(x, y)}.$$

Da questa uguaglianza si vede come t sia reale quando $(x, y) \in \mathbf{R}$. Inoltre t è univocamente determinato quando $A_i(x, y) \neq 0$. Da ciò si deduce che *un punto dell'inviluppo non appartenente a $\mathcal{V}(A_2, A_3, A_4)$ è tangente ad esattamente una circonferenza della famiglia*.

Rimane da stabilire quando A_2, A_3 ed A_4 si annullano contemporaneamente. Utilizzando le tecniche studiate nel paragrafo 1 si dimostra che le soluzioni reali di $A_2 = A_3 = A_4 = 0$ sono

$$(x, y) = (0, 17/4) \text{ e } (\pm 0.936845, 1.63988).$$

Guardando al grafico di $\mathcal{V}(g_1)$ si può notare come questi coincidano con i punti singolari di $\mathcal{V}(g_1)$.

Abbiamo visto come i punti singolari di $\mathcal{V}(g_1)$ siano determinati dalle equazioni $g_1 = \frac{\partial}{\partial x} g_1 = \frac{\partial}{\partial y} g_1 = 0$, il che implica:

$$\mathcal{V}(A_2, A_3, A_4) = \mathcal{V}(g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1).$$

Per provare ciò bisogna dimostrare che

$$\begin{aligned} g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1 &\in \langle A_2, A_3, A_4 \rangle, \\ A_2, A_3, A_4 &\in \langle g_1, \frac{\partial}{\partial x} g_1, \frac{\partial}{\partial y} g_1 \rangle. \end{aligned} \quad (3.9)$$

La dimostrazione si effettua applicando l'algoritmo di appartenenza ad un ideale.

Si è così arrivati a dimostrare che *un punto non singolare di $\mathcal{V}(g_1)$ appartiene all'inviluppo e, in tale punto, l'inviluppo è tangente ad esattamente una circonferenza della famiglia.*

Si osservi che nell'esempio (3.8), le equazioni dell'inviluppo erano facili da determinare ma, per comprenderne le implicazioni, abbiamo dovuto utilizzare le basi di Groebner ed i Teoremi di Eliminazione ed Estensione.

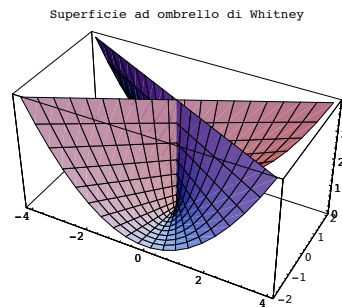
3.5 Applicazioni

3.5.1 Ombrello di Whitney

Si consideri la *superficie ad ombrello di Whitney* descritta parametricamente dalle equazioni:

$$\begin{cases} x = uv, \\ y = v, \\ z = u^2. \end{cases}$$

Il grafico di tale superficie è il seguente:



Dal teorema di Implicitizzazione per parametrizzazioni polinomiali, sappiamo che la più piccola varietà contenente tale superficie è $\mathcal{V}(I_2)$, mentre dal Teorema di Eliminazione si ha che gli elementi della base di Groebner che non dipendono da u e v , formano una base di Groebner per I_2 , ed inoltre tali elementi definiscono la più piccola varietà contenente l'immagine della parametrizzazione. Sia quindi $I = \langle x - uv, y - v, z - u^2 \rangle$. Il primo passo è quindi calcolare la base di Groebner per tale ideale.

Per fare ciò utilizziamo il sistema di Computer Algebra **CoCoA**, che è un sistema per fare *Computazioni in Algebra Commutativa*, scritto in linguaggio C e disponibile in diverse piattaforme. La parte più importante di tale sistema consiste in un'implementazione dell'algoritmo di Buchberger per calcolare la base di Groebner di ideali su un anello di polinomi a coefficienti in un campo.

Attraverso le istruzioni

```
Use R ::= Q[u, v, x, y, z], Lex;
```

```
GBasis(Ideal(uv - x, v - y, u^2 - z));
```

si ottiene l'output

$$[v - y, u^2 - z, uy - x, ux - yz, x^2 - y^2z],$$

dunque la base di Groebner per I è data da:

$$\begin{cases} g_1 = v - y, \\ g_2 = u^2 - z, \\ g_3 = uy - x, \\ g_4 = ux - yz, \\ g_5 = x^2 - y^2z. \end{cases}$$

Dal teorema di eliminazione, sappiamo che la base di Groebner G_2 per il secondo ideale di eliminazione $I_2 = I \cap \mathbf{C}[x, y, z]$ è data da $G \cap \mathbf{C}[x, y, z]$, ovvero da $g_5 = x^2 - y^2z$. Abbiamo così determinato $\mathcal{V}(I_2) = \mathcal{V}(g_5) = \mathcal{V}(x^2 - y^2z)$, ossia la varietà minima contenente l'immagine della parametrizzazione.

Ci proponiamo ora di stabilire se tale immagine riempie o meno la suddetta varietà, il che equivale a vedere se tutte le soluzioni parziali $(x, y, z) \in \mathcal{V}(I_2)$ si estendono ad una soluzione completa $(u, v, x, y, z) \in \mathcal{V}(I)$.

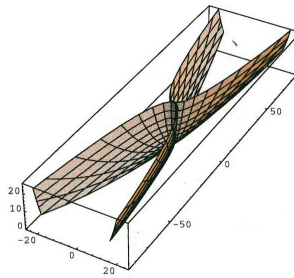
Se $k = \mathbf{C}$, il Teorema di Estensione fornisce a priori una risposta a tale problema. Sappiamo infatti che $(x, y, z) \in \mathcal{V}(I_2)$ si estende ad una soluzione $(v, x, y, z) \in \mathcal{V}(I_1)$, in quanto $I_1 = \langle v - y, x^2 - y^2z \rangle$ ha un generatore, g_1 , il cui coefficiente direttore rispetto a v è costante. Si ripete il ragionamento per I_1 , e si vede come I abbia un generatore, g_2 , il cui coefficiente direttore rispetto ad u è costante. Questo ci assicura che in \mathbf{C} ogni soluzione parziale si estende ad una soluzione completa, ossia che l'immagine della parametrizzazione riempie la varietà minima che la contiene.

3.5.2 Un altro esempio

Sia S la superficie definita dalle equazioni parametriche

$$\begin{cases} x = uv, \\ y = uv^2, \\ z = u^2. \end{cases}$$

Il grafico di tale superficie è il seguente:



Vogliamo determinare la più piccola varietà V contenente la superficie S . Di nuovo calcoliamo, con l'ausilio di **CoCoA**, la base di Groebner per l'ideale $I = \langle uv - x, v - y, u^2 - z \rangle$, rispetto all'ordine lessicografico con $u > v > x > y > z$. Attraverso le istruzioni:

```
Use R ::= Q[u, v, x, y, z], Lex;
```

```
GBasis(Ideal uv - x, uv^2 - y, u^2 - z));
```

si ottiene l'output

$$[u^2 - z, uv - x, -vx + y, uy - x^2, ux - vz, vyz - x^3, v^2z - x^2, x^4 - y^2z]$$

gli elementi della base di Groebner per I sono dunque:

$$\begin{cases} g_1 = u^2 - z, \\ g_2 = uv - x, \\ g_3 = -vx + y, \\ g_4 = uy - x^2, \\ g_5 = ux - vz, \\ g_6 = vyz - x^3, \\ g_7 = v^2z - x^2, \\ g_8 = x^4 - y^2z \end{cases}$$

Dal teorema di eliminazione, sappiamo che la base di Groebner G_2 , relativa al secondo ideale di eliminazione I_2 , è data dagli elementi di $G \cap \mathbf{C}[x, y, z]$, ovvero da $g_8 = x^4 - y^2z$. La più piccola varietà contenente l'immagine della parametrizzazione è definita proprio da $g_8 = 0$. Vogliamo vedere se, in \mathbf{C} , la superficie S riempie o meno tale varietà.

Per fare ciò, bisogna vedere se le soluzioni parziali si estendono ad una soluzione completa. Si noti che il campo è algebricamente chiuso, per cui è possibile applicare il Teorema di Estensione. Andiamo quindi a vedere chi sono i generatori del primo ideale di eliminazione I_1 , al fine di verificare se la soluzione parziale $(x, y, z) \in \mathcal{V}(I_2)$ si estende ad una soluzione in $\mathcal{V}(I_1)$. I generatori di I_1 sono gli elementi di $G_1 = G \cap \mathbf{C}[v, x, y, z] = \{-vx - y, vyz - x^3, v^2z - x^2, x^4 - y^2z\}$. Dal Teorema di Estensione, sappiamo che ogni soluzione parziale non appartenente alla varietà definita dai coefficienti direttori, rispetto a v , dei generatori di I_1 , si estende. Tale varietà è $\mathcal{V}(x, z, yz)$, per cui ogni soluzione parziale non appartenente all'asse y si estende ad una soluzione in $\mathcal{V}(I_1)$.

Riapplichiamo ora il Teorema di Estensione alle soluzioni parziali $(v, x, y, z) \in \mathcal{V}(I_1)$. Tali soluzioni si estendono ad una soluzione completa appartenente a $\mathcal{V}(I)$, in quanto esiste un generatore di I , g_1 , il cui coefficiente direttore rispetto ad u è costante.

Possiamo pertanto concludere che, in \mathbf{C} , la superficie S non riempie la varietà minima $\mathcal{V}(I_2)$ che la contiene, in quanto le soluzioni parziali appartenenti all'asse y non si estendono.