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)

1. GEOMETRIA, ALGEBRA e ALGORITMI

Dipartimento di Matematica

Facoltà di Scienze Matematiche, Fisiche e Naturali

Capitolo 1

Geometria, Algebra e Algoritmi

In questo capitolo si introducono i temi fondamentali del corso. Saremo interessati alla geometria delle *varietà affini*, che sono curve, superfici e oggetti di dimensione più alta definiti da equazioni polinomiali. Per questo scopo dovremo studiare gli *ideali* nell'anello dei polinomi $k[x_1, \ldots, x_n]$. Studieremo, in particolare, i polinomi in una variabile per poter illustrare il ruolo svolto dagli algoritmi.

1.1 Polinomi e Spazi Affini

Per collegare l'Algebra con la Geometria studieremo i polinomi a coefficienti in un campo. Utilizzeremo diversi campi a seconda degli scopi prefissati. I più comuni saranno:

- I numeri complessi $\mathbf{C}$, quando vorremo essere sicuri che un problema abbia soluzione.
- I numeri reali $\mathbf{R}$, per disegnare le varietà in dimensione 2 e 3.
- I numeri razionali $\mathbf{Q}$, più utili ad illustrare i collegamenti con la teoria dei numeri.
- I campi finiti, più adatti per fare un'implementazione sul computer. Ci riferiremo in particolare al campo fondamentale $\mathbf{Z}_p$ (con p primo ≥ 2) dei campi a caratteristica p, o, più in generale, al campo di Galois di ordine $q = p^h$ ottenuto a partire da $\mathbf{Z}_p$ aggiungendo le radici di un

polinomio $g(x)$ irriducibile su $\mathbf{Z}_p$ e di grado h, ovvero:

$$GF(q) = \frac{\mathbf{Z}_p}{(g(x))}$$

[cfr[15]].

Definizione 1.1.1 *Un* **monomio** *in $x_1, \ldots, x_n$ è un'espressione del tipo:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n},$$

dove tutti gli α_i sono interi non negativi. Il **grado totale** *di tale monomio è la somma $|\alpha| = \alpha_1 + \ldots + \alpha_n$.*

La notazione per i monomi verrà semplificata scrivendo

$$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n},$$

ove $\alpha = (\alpha_1, \ldots, \alpha_n)$ è una n-pla di interi non negativi, e se $\alpha = (0, \ldots, 0)$ si ha $x^\alpha = 1$. Con questa notazione il *grado totale* del monomio x^α sarà denotato con $|\alpha| = \alpha_1 + \ldots + \alpha_n$.
A partire dalla definizione di monomio, si può definire un *polinomio* come somma di monomi.

Definizione 1.1.2 *Un* **polinomio** *in $x_1, \ldots, x_n$ a coefficienti in un campo k è una combinazione lineare finita di monomi, ossia è del tipo*

$$f(x_1, \ldots, x_n) = \sum_\alpha a_\alpha x^\alpha, \qquad a_\alpha \in k,$$

ove $\alpha = (\alpha_1, \ldots, \alpha_n)$ varia in un insieme finito di n-ple di interi non negativi. L'insieme di tutti i polinomi a coefficienti in k si indica con $k[x_1, \ldots, x_n]$.

Se $n = 1$, $k[x] = \{f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0 \mid a_i \in k, a_m \neq 0\}$. L'intero m si dice grado del polinomio, l'elemento a_m si dice coefficiente direttore, e il termine $a_m x^m$ si indicherà con $LT(f)$ (Leading Term o termine direttore di f).

Nel caso generale ($n \geq 1$):

- Chiameremo a_α il **coefficiente** del monomio x^α.
- Se $a_\alpha \neq 0$ chiameremo $a_\alpha x^\alpha$ un **termine** di f.

- **Grado totale** di $f(x_1, \ldots, x_n)$ è definito come:

$$\partial f = \max_{a_\alpha \neq 0}\{\mid \alpha \mid\}.$$

Useremo sempre le lettere f, g, h, p, q, r per indicare polinomi. Ad esempio il polinomio

$$3x^3y^2z + \frac{2}{3}x^4y^2 + 8xyz - 2y$$

è un polinomio in $\mathbf{Q}[x, y, z]$ che ha quattro termini e grado totale 6. Si noti che ci sono ben due termini di grado totale massimo 6, fatto che non può accadere per polinomi in una variabile. Per poter parlare anche nel caso di più variabili di termine direttore di F studieremo, nel Capitolo 2, come *ordinare* i termini di un polinomio.

Nell'anello $k[x_1, \ldots, x_n]$ si definiscono la somma e il prodotto fra polinomi con le regole usuali dell'algebra. Rispetto a tali operazioni $k[x_1, \ldots, x_n](+, \cdot)$ ha una struttura di anello commutativo dotato di unità e privo di divisori dello zero, o, come anche si dice, di *dominio*.

Così come dal dominio $\mathbf{Z}$ si costruisce il campo $\mathbf{Q}$ dei razionali:

$$\mathbf{Q} = \{\frac{p}{q} \mid p, q \in \mathbf{Z},\ q \neq 0 \ e\ \frac{p}{q} = \frac{r}{s} \Leftrightarrow ps = qr\},$$

da ogni dominio si può costruire il campo dei quozienti. Con tale costruzione a partire dal dominio $k[x_1, \ldots, x_n]$ si ottiene il **campo dei quozienti polinomiali**:

$$\begin{aligned} k(x_1, \ldots, x_n) \quad = \quad & \{\frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x_1, \ldots, x_n], g(x) \neq 0 \ e \\ & \frac{f(x)}{g(x)} = \frac{f^1(x)}{g^1(x)} \Leftrightarrow f(x)g^1(x) = f^1(x)g(x)\}. \end{aligned}$$

Per i nostri scopi sarà sufficiente dare per lo spazio affine la seguente definizione.

Definizione 1.1.3 *Dato un campo k ed un intero positivo n, si dice* **spazio affine** *n-dimensionale l'insieme :*

$$k^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}.$$

Ogni polinomio $f \in k[x_1, \ldots, x_n]$ individua una funzione polinomiale (che continueremo ad indicare con f):

$$f : k^n \longrightarrow k$$

che associa ad ogni elemento $a = (a_1, \ldots, a_n) \in k^n$ il valore $f(a) \in k$, che il polinomio $f(x)$ assume nel punto a.

Lo stesso discorso continua a valere se invece di f si considera il quoziente polinomiale $f(x)/g(x)$. Sia $W = \{a \in k^n \mid g(a) = 0\}$, si dice funzione *razionale* individuata da tale quoziente polinomiale l'applicazione

$$\frac{f}{g} : \ k^n - W \longrightarrow k$$

che associa ad ogni elemento $a = (a_1, \ldots, a_n) \in k^n - W$ l'elemento

$$f(a)/g(a) \in k.$$

Il campo delle funzioni razionali sarà indicato ancora con $k(x_1, \ldots, x_n)$.

Due polinomi $f, g \in k[x_1, \ldots, x_n]$ sono **uguali** se hanno i coefficienti tutti uguali, si dicono invece **identici** se individuano la stessa funzione polinomiale, ossia:

$$f(a) = g(a), \qquad \forall a \in k^n.$$

Ovviamente polinomi uguali individuano la stessa funzione polinomiale, difatti se $f = g$, allora f e g hanno gli stessi coefficienti e $f - g = \varphi = O_{k[x_1,\ldots,x_n]}$, da cui segue che $\varphi(a) = 0 \ \forall a \in k$, ossia $f(a) = g(a) \ \forall a \in k$. Il viceversa in generale non vale.

Se k è infinito vale il seguente **Principio d'identità dei polinomi**:

Proposizione 1.1.1 *Sia k un campo infinito ed $f \in k[x_1, \ldots, x_n]$. Allora f è lo zero dell'anello dei polinomi $f = O_{k[x_1,\ldots,x_n]}$ se e soltanto se la funzione polinomiale individuata da f è quella nulla:*

$$\begin{aligned} f : k^n &\longrightarrow k \\ a &\longrightarrow 0, \qquad \forall a \in k^n. \end{aligned}$$

Dimostrazione. ($\Rightarrow$) È ovvio che se $f = O_{k[x_1,\ldots,x_n]}$, allora $f(a) = 0 \ \forall a \in k^n$.

($\Leftarrow$) Si procede per induzione rispetto al numero n delle variabili.

Sia $n = 1$. Come dimostreremo nel paragrafo 1.6, un polinomio $f(x) = a_m x^m + \ldots + a_0$ di grado $m > 0$ ha al più m radici. Ora, se k è infinito e $f(a) = 0 \ \forall a \in k$, il polinomio f viene ad avere un numero infinito di radici, il che è assurdo se f ha grado positivo. L'unica possibilità è dunque che f sia lo zero dell'anello dei polinomi, ossia abbia coefficienti tutti nulli.

Sia $n \geq 2$. Per ipotesi induttiva assumiamo vera ($\Leftarrow$) per polinomi $g \in k[x_1, \ldots, x_{n-1}]$. Si osservi che, se abbiamo un polinomio in più variabili,

possiamo fissare la nostra attenzione su una di esse, ad esempio x_n, e considerare l'anello $k[x_1, \ldots, x_n] = A[x_n]$ come anello dei polinomi nell'unica variabile x_n, a coefficienti nell'anello $A = k[x_1, \ldots, x_{n-1}]$ dei polinomi nelle altre $n-1$ indeterminate. In altri termini si scrive:

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{\partial_{x_n} f} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

ove $\partial_{x_n} f$ è il grado, rispetto ad x_n, di f. Se $f : k^n \longrightarrow k$ è tale che $f(a) = 0,\ \forall a \in k^n$, dimostreremo che f ha coefficienti tutti uguali a zero, sfruttando l'ipotesi induttiva che sia vero per polinomi di grado $(n-1)$.

Infatti, fissato arbitrariamente $(a_1, \ldots, a_{n-1}) \in k^{n-1}$, il polinomio $\varphi(x_n) \in k[x_n]$, definito dalla:

$$\varphi(x_n) = f(a_1, \ldots, a_{n-1}, x_n) = \sum_{i=0}^{\partial_{x_n} f} g_i(a_1, \ldots, a_{n-1}) x_n^i$$

è tale che $\forall a \ \in k,\ \varphi(a) = f(a_1, \ldots, a_{n-1}, a) = 0$.

Poiché per $n = 1$ la proposizione è vera, sappiamo che $\varphi(x_n)$ ha coefficienti tutti nulli, quindi $\forall i = 1, \ldots, \partial_{x_n} f$, risulta $g_i(a_1, \ldots, a_{n-1}) = 0$. Essendo $(a_1, \ldots, a_{n-1})$ arbitrario in k^{n-1}, tutte le $g_i : k^{n-1} \longrightarrow k$ sono uguali alla funzione nulla.

L'ipotesi induttiva implica quindi che $g_i = O_{k[x_1,\ldots,x_{n-1}]}$, ossia per ogni i il polinomio g_i deve avere i coefficienti tutti nulli. Poiché tutti i coefficienti di g_i forniscono tutti i coefficienti di f si avrà che anche questi saranno a loro volta tutti nulli. ∎

L'ipotesi che k sia infinito è essenziale per la validità del teorema. Sia infatti $k = \mathbf{Z}_2 = \{0, 1\}$ e $f(x) = x^2 + x \ \in \mathbf{Z}_2[x]$. Si vede allora come, pur essendo $f(x) \neq O_{\mathbf{Z}_2[x]}$, si ha $f(0) = 0$ e $f(1) = 0$.

In generale si ha che se $k = GF(q)$ è un campo finito di ordine $q = p^h$ e $f : GF(q) \longrightarrow GF(q)$, allora f è la funzione polinomiale nulla se e solo se f è un multiplo del polinomio $g(x) = x^q - x = x(x^{q-1} - 1)$, come segue facilmente dal

Lemma 1.1.1 *Per ogni $a \in GF(q)$ vale l'identità $a^q = a$ e se $a \neq 0$ si ha $a^{q-1} = 1$.*

Dimostrazione. Il gruppo moltiplicativo $k - \{0\}$ è un gruppo di ordine $q - 1$. Sia $a \neq 0$ un arbitrario elemento di tale gruppo e sia $r = | < a > |$

il suo periodo (i.e. il minimo intero positivo tale che $a^r = 1$, che, come è noto dal corso di Algebra, coincide con l'ordine del sottogruppo ciclico $< a >$ generato da a). Dal teorema di Lagrange, [cfr[7]], segue subito che $q-1 = ir$ ove i è il numero delle classi laterali del sottogruppo $< a >$ quindi

$$a^{q-1} = a^{ir} = (a^r)^i = 1^i = 1.$$

Pertanto ogni elemento $a \in k - \{0\}$ soddisfa alla

$$a^{q-1} = 1.$$

Poiché banalmente lo zero soddisfa alla $a = 0$, si ha l'asserto. ∎

Se $a_0 = 0, a_1, \ldots, a_{q-1}$ sono i q elementi del campo finito si ha quindi che $g(x)$ ha su $GF(q)$ la fattorizzazione

$$g(x) = x(x - a_1) \cdot \ldots \cdot (x - a_{q-1}),$$

(infatti, come è noto e, comunque, richiameremo nel corso della dimostrazione del corollario 1.6.1, se α è radice di $g(x)$ necessariamente $(x - \alpha)$ divide $g(x)$). Ogni polinomio $f(x) \in GF(q)[x]$ che individui la funzione polinomiale nulla ammetterà le q radici distinte $a_0 = 0, a_1, \ldots, a_{q-1}$, e pertanto sarà divisibile per $g(x)$. Viceversa è ovvio che, se il polinomio f è multiplo di $g(x)$, risulta $f(a) = 0 \ \forall a \in GF(q)$.
Concludiamo questo paragrafo ricordando la proprietà che caratterizza il campo $\mathbf{C}$.

Teorema 1.1.1 (Teorema fondamentale dell'algebra) *Ogni polinomio $f(z)$ di $\mathbf{C}[z]$ di grado strettamente maggiore di zero ha almeno una radice in $\mathbf{C}$.*

Dimostrazione. Supponiamo per assurdo che $f(z)$ non ammetta radici in $\mathbf{C}$, ossia $f(z) \neq 0 \ \forall z \in \mathbf{C}$. In questa ipotesi $1/f(z)$ è una funzione olomorfa sull'intero piano della variabile complessa, o come anche si dice una funzione trascendente intera. Ovviamente il $\lim_{z\to\infty} 1/f(z) = 0$; ne segue facilmente che esiste una costante $M > 0$ tale che $|1/f(z)| < M$. Per il teorema di Liouville, ogni funzione trascendente intera limitata in modulo è costante, ma allora anche $f(z)$ dovrebbe essere costante, contro l'ipotesi che il grado di f è strettamente maggiore di zero. ∎

Ricordiamo che un campo k si dice *algebricamente chiuso* se vale in $k[x]$ il Teorema fondamentale dell'algebra ossia se ogni polinomio non costante ha almeno una radice in k.

1.2 Varietà Affini e Parametrizzazioni

Definizione 1.2.1 *Sia k un campo e siano $f_1, \ldots, f_s$ s polinomi in $k[x_1, \ldots, x_n]$. Si dice* **varietà affine** *definita da $f_1, \ldots, f_s$ l'insieme:*

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0, \ \forall\ 1 \leq i \leq s\}.$$

In altri termini, una varietà affine $\mathcal{V}(f_1, \ldots, f_s) \subset k^n$ è l'insieme di tutte le soluzioni del sistema:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0. \end{cases}$$

Esempio: Si consideri un sistema di m equazioni lineari in n incognite $x_1, \ldots, x_n$ a coefficienti in un campo k:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases}$$

L'insieme delle soluzioni di questo sistema è una varietà affine V in k^n, che chiameremo *varietà lineare*. Come è noto dal corso di Algebra lineare la sua **dimensione** è $n - r$, dove r è il rango della matrice dei coefficienti del sistema, ovvero il numero di equazioni linearmente indipendenti. Descriviamo ora alcune proprietà delle varietà affini.

Proposizione 1.2.1 *Se $V, W \subset k^n$ sono varietà affini, allora $V \cap W$ e $V \cup W$ sono anch'esse varietà affini.*

Dimostrazione. Se $V = \mathcal{V}(f_1, \ldots, f_s)$ e $W = \mathcal{V}(g_1, \ldots, g_t)$, si ha precisamente che

$$V \cap W = \mathcal{V}(f_1, \ldots, f_s, g_1, \ldots, g_t), \tag{1.1}$$
$$V \cup W = \mathcal{V}(f_i g_j \mid 1 \leq i \leq s, \ 1 \leq j \leq t). \tag{1.2}$$

La (1.1) segue banalmente dal fatto che in $V \cap W$ sia $f_1, \ldots, f_s$ che $g_1, \ldots, g_t$ si devono annullare, ovvero devono annullarsi simultaneamente tutte le $f_1, \ldots, f_s$, $g_1 \ldots, g_t$.

Dimostriamo ora la (1.2). Sia $a = (a_1, \ldots, a_n) \in V \cup W$. Se $a \in V$, tutte le f_i si annullano in a, per cui anche tutte le $f_i g_j$ si annulleranno in

tal punto e quindi $V \subset \mathcal{V}(f_i g_j)$. Similmente si vede che se $a \in W$, risulta necessariamente $W \subset \mathcal{V}(f_i g_j)$. Pertanto, $V \cup W \subset \mathcal{V}(f_i g_j)$.

Per dimostrare l'inclusione opposta consideriamo un punto b di $\mathcal{V}(f_i g_j)$ e supponiamo che sia $f_\alpha(b) \neq 0$ per qualche α (ossia $b \notin V$, altrimenti non c'è niente da dimostrare). Il fatto che $f_\alpha g_j$ si annulla in b per ogni j, ma $f_\alpha(b) \neq 0$ implica che tutti i g_j devono annullarsi in b, e quindi $b \in W \subset V \cup W$. ∎

Da questa proposizione segue che unioni ed intersezioni finite di varietà affini sono ancora varietà affini. Ovviamente $\mathcal{V}(0) = k^n$ e, ad esempio $\mathcal{V}(x, x-1) = \emptyset$ (in generale sarà vuota la varietà luogo degli zeri di un qualunque sistema incompatibile di equazioni polinomiali). Sarà uno dei nostri scopi quello di far vedere che le varietà affini sono i chiusi di una topologia di k^n, la cosidetta "Topologia di Zariski". A tale scopo resta solo da dimostrare che intersezioni qualsiansi di varietà affini sono varietà affini e questo seguirà dal Teorema della base di Hilbert.

Siano $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$, i problemi che si presentano nello studio delle varietà affini sono:

- il problema della **Compatibilità** del sistema, che consiste nello stabilire quando risulta $\mathcal{V}(f_i) \neq \emptyset$.
- il problema della **Finitezza**, ossia di determinare esplicitamente le soluzioni del sistema, cioè i punti di $V = \mathcal{V}(f_1, \ldots, f_s)$ e vedere se sono o meno in numero finito. Questo problema consiste sostanzialmente nel determinare le equazioni parametriche esplicite di V:

$$\begin{cases} x_1 = r_1(t_1, \ldots, t_m), \\ \vdots \\ x_n = r_n(t_1, \ldots, t_m). \end{cases}$$

- determinare la **Dimensione** di $\mathcal{V}(f_1, \ldots, f_s)$.

Osservazioni

1. La nozione intuitiva di dimensione (data dalla dimensione dello spazio ambiente meno il numero delle equazioni indipendenti) andrà modificata come mostra l'esempio della varietà di $\mathbf{R}^3$ data dall'unione fra l'asse z ($\mathcal{V}(x, y)$) e il piano (x, y) ($\mathcal{V}(z)$):

$$\mathcal{V}(z) \cup \mathcal{V}(x, y) = \mathcal{V}(zx, zy).$$

Dalla Proposizione precedente segue che tale unione è ancora una varietà affine, ottenuta tuttavia unendo una curva (asse z) ed una superficie (piano (x, y)), ossia un pezzo di dimensione intuitivamente 1 con un pezzo che intuitivamente ha dimensione 2.

2. La differenza di due varietà affini non sempre è una varietà affine.

   - Si consideri ad esempio in $\mathbf{R}^2$ la retta $y = x$ cui togliamo il punto $(1, 1)$:

     $$X = \{(x, x) \mid x \in \mathbf{R}, x \neq 1\} = \mathcal{V}(x - y) - \mathcal{V}(x - 1, y - 1).$$

     Se X fosse una varietà affine, dovrebbe essere del tipo:

     $$X = \mathcal{V}(f_1, \ldots, f_s) = \{a \in \mathbf{R}^2 \mid f_i(a) = 0, \forall\, i = 1, \ldots, s\}.$$

     Dovrebbero pertanto esistere s polinomi $\varphi_i(x) = f_i(x, x)$, nella variabile x e di gradi rispettivi n_i, che si annullano per ogni $x \neq 1$. Poiché il campo $k = \mathbf{R}$ è infinito e tali polinomi ammettono un numero di radici superiore al grado si ha che sono identicamente nulli, e pertanto anche $\varphi_i(1) = 0$. In altri termini: ogni polinomio che si annulla su tutti i punti di X deve necessariamente annullarsi anche in $(1, 1)$. Ne segue che non possono esistere s polinomi tali che $X = \mathcal{V}(f_1, \ldots, f_s)$. Questo è un particolare esempio di *retta bucata*, ma lo stesso discorso vale per qualsiasi altra retta privata di un suo punto.

3. Risulta, invece, una varietà affine il **prodotto cartesiano** di due varietà affini

   $$V = \mathcal{V}(f_1, \ldots, f_s), \quad f_i \in k[x_1, \ldots, x_n], \quad V \subseteq k^n,$$

   $$W = \mathcal{V}(g_1, \ldots, g_t), \quad g_j \in k[y_1, \ldots, y_m], \quad W \subseteq k^m.$$

   Precisamente:

   $$V \times W = \{(a, b) \mid a \in V,\ b \in W\} \subseteq k^{n+m}.$$

   In altre parole, se $x \in k^n$ e $y \in k^m$ la varietà prodotto $V \times W$ è definita come l'insieme dei punti $(x, y) \in k^{n+m}$ che, con le loro coordinate risolvono il sistema:

   $$\begin{cases} f_i(x) = 0, & i = 1, \ldots, s, \\ g_j(y) = 0, & j = 1, \ldots, t. \end{cases}$$

- Si consideri il punto $x = 3$ in $\mathbf{R}$ e la parabola $z = y^2$ nel piano yz. La varietà di $\mathbf{R^3}$ prodotto del punto per la parabola

$$V \times W : \begin{cases} x = 3, \\ z = y^2. \end{cases}$$

è chiaramente anche l'intersezione del piano di equazione $x = 3$, parallelo al piano yz, con il cilindro $z = y^2$ con generatrici parallele all'asse x che proietta parallelamente all'asse x i punti della parabola $z = y^2$ del piano yz.

Diamo ora la seguente definizione

Definizione 1.2.2 *Si dice che una varietà affine $V = \mathcal{V}(f_1, \ldots, f_s)$, con $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, ammette una* **parametrizzazione razionale** *se esistono n funzioni razionali $r_1, \ldots, r_n$ in $k(t_1, \ldots, t_m)$, campo dei quozienti del dominio $k[t_1, \ldots, t_m]$, tali che:*
i) i punti di coordinate:

$$\begin{cases} x_1 = r_1(t_1, \ldots, t_m), \\ \vdots \\ x_n = r_n(t_1, \ldots, t_m), \end{cases}$$

siano tutti su $V = \mathcal{V}(f_1, \ldots, f_s)$
ii) V sia la più piccola varietà affine di k^n contenenti tali punti.
Se le $r_1, \ldots, r_n$ sono dei polinomi, si parlerà semplicemente di **rappresentazione parametrica polinomiale** *di V.*

Le equazioni $f_1 = \ldots = f_s = 0$ di V forniscono invece una *rappresentazione implicita* di V.

Attraverso queste ultime è più facile verificare l'appartenenza o meno di un punto ad una varietà: basterà infatti verificare se le equazioni della varietà sono soddisfatte dalle coordinate del punto in questione o meno. Le equazioni parametriche risultano più utili quando, per mezzo di un computer, si vuole disegnare il grafico della varietà. Il fatto di voler ottenere entrambe le rappresentazioni di una varietà affine, porta ai seguenti problemi:

- **Parametrizzazione**: stabilire cioè quando una varietà affine ammette una rappresentazione parametrica razionale;

- **Implicitizzazione**: data una rappresentazione parametrica di una varietà affine, vedere se è possibile passare alle equazioni cartesiane o implicite.

La risposta al primo problema è in generale negativa; saranno solo le varietà *unirazionali* a godere di questa proprietà. Per quanto riguarda invece il secondo problema si ha che è sempre possibile passare da una rappresentazione parametrica razionale ad una rappresentazione implicita, come vedremo nel capitolo sulla teoria dell'eliminazione.

Concludiamo questo paragrafo accennando ai seguenti esempi di curve e superfici dello spazio reale tridimensionale (ampliato e complessificato con l'aggiunta degli elementi impropri), che hanno rappresentazioni parametriche razionali o polinomiali

Esempi.

1. Si consideri la retta in $\mathbf{R}^3$ definita dalle equazioni:

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

Si vede subito come le soluzioni siano infinite, essendo un sistema di 2 equazioni in 3 incognite. Ponendo, ad esempio, $z=t$, si ottiene il sistema

$$\begin{cases} x=-1-3t, \\ y=2+2t, \\ z=t, \end{cases}$$

che dà, al variare di t in $\mathbf{R}$, le equazioni parametriche della retta.

2. Un altro esempio di varietà affine è dato da il *grafico di una funzione razionale* $y=\varphi(x)\in k(x)$ ossia $\varphi(x)=f(x)/g(x)$, con $f,g\in k[x]$, $g\neq 0$. Si ottiene in questo modo la varietà associata al polinomio $g(x)y-f(x)$

$$\mathcal{V}(g(x)y-f(x)).$$

Assumendo come parametro $x=t$, si hanno le equazioni parametriche

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

3. **Cubica sghemba** in $\mathbf{R}^3$. La curva di $\mathbf{R}^3$ di equazioni parametriche:

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

si dice *cubica sghemba*. Eliminando il parametro t dalle equazioni sopra scritte, si hanno le equazioni cartesiane:

$$\begin{cases} y = x^2, \\ z = x^3, \end{cases}$$

che ci mostrano come si tratti della varietà affine:

$$V = \mathcal{V}(y - x^2, z - x^3),$$

che risulta essere intersezione del cilindro quadrico $y - x^2 = 0$ e del cilindro cubico $z - x^3 = 0$ le cui generatrici sono, rispettivamente, parallele all'asse z e all'asse y.

Intersecando la curva con un piano

$$\pi : \quad ax + by + cz + d = 0,$$

si ottiene

$$at + bt^2 + ct^3 + d = 0,$$

che, per valori generici di $(a, b, c, d) \neq (0, 0, 0, 0)$, è un polinomio di terzo grado in t e, come tale, ha esattamente 3 soluzioni in $\mathbf{C}$ (il nome di "cubica trae la sua origine proprio dal fatto che un piano generico la incontra in 3 punti). Inoltre, non esiste nessun piano di $\mathbf{R}^3$ che contenga interamente la curva (o, come anche si dice, la curva è *sghemba*), in quanto se fosse

$$at + bt^2 + ct^3 + d = 0, \qquad \forall\ t \in \mathbf{R},$$

per il *principio d'identità dei polinomi*, si avrebbe $a = b = c = d = 0$, e $ax + by + cz + d = 0$ non potrebbe essere l'equazione di un piano.

In generale, l'ordine di una curva sghemba di $\mathbf{R}^3$ ha il significato geometrico di numero di punti complessi (da contarsi con la dovuta molteplicità) che la curva ha in comune con un generico piano di $\mathbf{R}^3$.

4. **Superficie tangenziale alla cubica sghemba** in $\mathbf{R}^3$.
Abbiamo visto nell'esempio precedente come la cubica sghemba abbia equazioni parametriche:

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

con $t \in \mathbf{R}$. Poiché il vettore tangente alla cubica ha per componenti le derivate prime

$$\begin{cases} \dot{x} = 1, \\ \dot{y} = 2t, \\ \dot{z} = 3t^2, \end{cases}$$

si ha che l'insieme delle tangenti alla curva in un generico punto è descritto dalle equazioni parametriche:

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

dove t ed u indicano rispettivamente la posizione sulla curva e sulla tangente. Eliminando i due parametri t ed u si ottiene l'equazione:

$$-4x^3z + 3x^2y^2 - 4y^2 + 6xyz - z^3 = 0.$$

della cosidetta Superficie tangenziale alla cubica sghemba.

1.3 Parametrizzazione della circonferenza

Si consideri nello spazio euclideo $\mathbf{R}^2$ la circonferenza di equazione implicita:

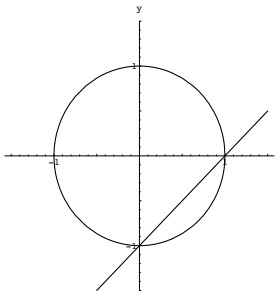
$$x^2 + y^2 = 1,$$

di cui una comune rappresentazione parametrica si ottiene sfruttando le funzioni trigonometriche :

$$\begin{cases} x = cos(t), \\ y = sin(t), \qquad 0 \leq t < 2\pi. \end{cases}$$

Per dare una parametrizzazione razionale fissiamo il punto $A = (0, -1)$ della circonferenza e consideriamo il fascio di rette passante per tale punto.

Ad ogni retta del fascio, diversa dalla tangente in A, corrisponde un unico punto della circonferenza diverso da A.



Precisamente, si ha una corrispondenza biunivoca α fra i punti della curva e le rette del fascio di centro A, che associa ad A la tangente in A alla curva, e ad ogni punto Q della circonferenza diverso da A la retta AQ del fascio. Si noti che tale corrispondenza è biunivoca in quanto la inversa α^{-1} è quella corrispondenza tra le rette del fascio e la curva C tale che alla tangente in A alla circonferenza associa il punto A stesso di C, e ad ogni retta r passante per A del fascio e diversa dalla tangente fa corrispondere il punto diverso da A di $r \cap C$.

Sia $r_t : \ y + 1 = tx$ la retta di coefficiente direttore t del fascio di centro A. L'intersezione tra la retta r_t e la curva C è data dal sistema

$$\begin{cases} y = tx - 1, \\ x^2 + y^2 = 1, \end{cases}$$

da cui si ottiene l'equazione:

$$x[(1 + t^2)x - 2t] = 0.$$

Scartando la soluzione $x = 0$ corrispondente al punto $(0, -1)$ si ottiene il punto $(2t/(1 + t^2), (t^2 - 1)/(t^2 + 1))$ che al variare di $t \in \mathbf{R}$ descrive tutta la circonferenza ad eccezione del punto $A' = (0, 1)$ (che non è rappresentato in quanto le equazioni ridotte non rappresentano la retta $x = 0$ del fascio). La circonferenza ha la rappresentazione parametrica razionale

$$\begin{cases} x = \dfrac{2t}{1 + t^2}, \\ \\ y = \dfrac{t^2 - 1}{1 + t^2}, \qquad \forall\, t \in \mathbf{R}, \end{cases}$$

ed è ovviamente la più piccola varietà affine che contiene tali punti. Questo sopra descritto è un procedimento standard per trovare le equazioni

parametriche razionali di curve algebriche piane, come vedremo nel prossimo paragrafo.

Osservazioni.

1. L'esempio sopra descritto della parametrizzazione della circonferenza mostra molto bene lo stretto legame che esiste tra la *Geometria Algebrica* e la *Teoria dei Numeri*. Infatti, dal sistema:

$$\begin{cases} x = \dfrac{2t}{1+t^2}, \\ \\ y = \dfrac{t^2-1}{1+t^2}, \qquad \forall\, t \in \mathbf{R}, \end{cases}$$

per ogni $t \in \mathbf{Z}$ otteniamo un punto $Q = (p/q, r/s)$ a coordinate razionali su C. Si noti che l'esistenza del punto a coordinate razionali Q sulla circonferenza, implica che:

$$(p/q)^2 + (r/s)^2 = 1,$$

o equivalentemente:

$$(ps)^2 + (rq)^2 = (qs)^2.$$

Ciò risolve un tipico problema della teoria dei numeri: quello della ricerca delle soluzioni intere non banali dell'equazione a coefficienti interi (o diofantea): $X^2 + Y^2 = Z^2$.

I punti razionali di una curva ci permettono, dunque, di trovare soluzioni intere non banali di equazioni diofantee; infatti, siano (X, Y, Z) le coordinate omogenee associate ad x e y

$$\begin{cases} x = \frac{X}{Z}, \\ \\ y = \frac{Y}{Z}. \end{cases}$$

Se (l, m) sono i parametri direttori della retta di coefficiente direttore t si ha anche $t = \frac{m}{l}$. Sostituendo a x, y, t le loro espressioni in funzione di X, Y, Z, l, m nelle equazioni parametriche della circonferenza, si ottiene

$$\begin{cases} \dfrac{X}{Z} = \dfrac{\frac{2m}{l}}{\frac{l^2+m^2}{l^2}} = \dfrac{2ml}{l^2+m^2}, \\ \\ \dfrac{Y}{Z} = \dfrac{\frac{m^2-l^2}{l^2}}{\frac{m^2+l^2}{l^2}} = \dfrac{m^2-l^2}{m^2+l^2}, \end{cases}$$

da cui:

$$\begin{cases} X = 2ml, \\ Y = m^2 - l^2, \\ Z = m^2 + l^2, \end{cases}$$

cha dà tutte le soluzioni intere non banali, con $Z > 0$ e X pari dell'equazione diofantea $X^2 + Y^2 = Z^2$.

2. Abbiamo trovato infinite soluzioni intere non banali dell'equazione

$$X^n + Y^n = Z^n,$$

nel caso particolare $n = 2$. È facile vedere che esistono infinite soluzioni intere non banali anche nel caso $n = 1$ dell'equazione diofantea $X + Y = Z$ (la retta $x + y = 1$ ha infatti infiniti punti razionali).

Per $n \geq 3$ si ha invece il teorema enunciato da Fermat nel 1637, e noto come l'*Ultimo Teorema di Fermat*, secondo cui l'equazione

$$X^n + Y^n = Z^n \qquad n \geq 3$$

non ammette soluzioni intere non banali.

Fermat scrisse l'enunciato di tale teorema nel margine di un libro di matematica con il commento "Ho scoperto una dimostrazione davvero notevole, che questo margine è troppo piccolo per contenere. Fermat poi non trovò mai posto per scrivere la dimostrazione generale, ma scrisse il caso $n = 4$.

Si noti come la condizione $n \geq 3$ possa essere sostituita dalla condizione $p \geq 3$, con p numero primo. Sia infatti $n = hp$ con p primo dispari. Allora l'equazione:

$$X^n + Y^n = Z^n,$$

si può riscrivere come:

$$X^{hp} + Y^{hp} = Z^{hp},$$

e se, per assurdo, tale equazione avesse una soluzione $(a, b, c) \neq (0, 0, 0)$ si avrebbe:

$$a^{hp} + b^{hp} = c^{hp},$$

e pertanto (a^h, b^h, c^h) risulterebbe soluzione intera non banale di $X^p + Y^p = Z^p$, in contraddizione con l'ipotesi che il teorema di Fermat valga per $n = p$ con $p \geq 3$ primo. Con un ragionamento simile si

può dimostrare che se l'equazione avesse soluzioni per $n = 2^h$ con $h \geq 2$ anche l'equazione ottenibile per $n = 4$ dovrebbe averne, il che è assurdo, per quanto già dimostrato da Fermat.

Cento anni dopo Fermat, il matematico svizzero *Leonardo Eulero* eliminò il caso $n = 3$. Nel 1820 e 1830 il teorema fu provato per $n = 5, 7$.

La teoria fece poi passi da gigante per opera del matematico *E.E. Kummer*, cui si deve la teoria di Kummer, che divide i numeri primi in primi regolari e irregolari, e stabilisce l'ultimo teorema di Fermat per i primi regolari (che sembrano più frequenti di quelli irregolari, costituendo il 60% di tutti i primi). Ma, ironicamente, mentre si può dimostrare facilmente che i primi irregolari sono infiniti, non mai stato dimostrato che i primi regolari lo sono (anche se questo è sicuramente vero).

Più tardi alcuni miglioramenti alla teoria di Kummer resero possibile studiare separatamente i primi irregolari, caso per caso, riducendo lo studio per vedere se il teorema di Fermat è vero ad un calcolo diretto ma lunghissimo, che sembra fatto a posta per i moderni calcolatori. Usando questi miglioramenti della teoria di Kummer vari ricercatori tra il 1970 e il 1993 hanno verificato che il teorema è vero per primi fino a 4.000.000. Estendere oltre il risultato è certamente possibile, ma farlo per questa strada richiederebbe nuove tecniche computazionali. Ciò non sarà necessario in quanto un ricercatore di teoria dei numeri Andrew Wiles nel settembre del 1994 ha completamente dimostrato il teorema, utilizzando comunque tecniche della teoria delle curve ellittiche che ai tempi di Fermat non esistevano ancora.

1.4 Richiami sulle curve algebriche piane

Scopo di questo paragrafo è mostrare come il procedimento utilizzato per dare la parametrizzazione razionale della circonferenza, si possa generalizzare a curve algebriche piane di ordine $n > 2$. Avremo bisogno, per questo scopo, di alcuni richiami.

Si consideri il piano affine reale $\mathbf{R}^2$, ampliato con gli elementi all'infinito e complessificato (si aggiungano cioè gli eventuali punti a coordinate complesse, considerando però sempre equazioni a coefficienti reali e sistemi di riferimento reali). Indicheremo con $f(x, y) \in \mathbf{R}[x, y]$ un polinomio di grado n, con $C^n = \mathcal{V}(f(x, y))$ una curva algebrica di ordine n (o, meglio, la sua

parte affine), con $P_0 = (x_0, y_0)$ un punto fissato di $\mathbf{R}^2$ e, infine, con r una retta del piano, di parametri direttori (l, m) passante per P_0 e non tutta contenuta in C^n. Si ha la seguente:

Definizione 1.4.1 *Si dice* **molteplicità di intersezione**, $\mu_{r\cap C}(P_0)$, *di una retta r con la curva C^n nel punto P_0 la molteplicità algebrica della soluzione $t = 0$, corrispondente al punto P_0, nell'equazione*

$$f(x_0 + lt, y_0 + mt) = 0,$$

risolvente il sistema

$$\begin{cases} x = x_0 + lt, \\ y = y_0 + mt, \\ f(x, y) = 0, \end{cases}$$

dato dalle equazioni della r e della C^n.

Osserviamo che $f(x_0+lt, y_0+mt)$, per ogni fissato (l, m), è un polinomio in t di grado positivo (poiché $P_0 \in C^n$) e, in generale, $\leq n$. Precisamente: avrà grado esattamente n, se la retta r è "generica" nel senso che il suo punto all'infinito di coordinate $(Z, X, Y) = (0, 1, t)$ non soddisfa l'equazione omogenea $F(Z, X, Y) = Z^n f(X/Z, Y/Z) = 0$, ossia, non è un punto all'infinito della curva; avrà grado $n - h > 0$ se la curva passa per P_∞ con molteplicità h. Nel caso in cui r sia "generica", nel senso sopra precisato, l'equazione risolvente il sistema ha, per il teorema fondamentale dell'algebra, nel piano complessificato, esattamente n soluzioni da contare con la dovuta molteplicità. Questo sarà utile presto nella dimostrazione della Proposizione che ci darà il significato geometrico dell'ordine di $C^n = \mathcal{V}(f(x, y))$.

Un'ulteriore osservazione che, forse, andava fatta immediatamente è che tale definizione sembra dipendere sia dal sistema di riferimento scelto nel piano sia dalla parametrizzazione scelta per la retta. Si può dimostrare, tuttavia, che la molteplicità di intersezione (che è ovviamente 0 se $P_0 \notin r\cap C^n$) dipende solo dalla retta r, dalla curva C^n e dal punto P_0, e non dalla scelta del riferimento nel piano $\mathbf{R}^2$ o dalla scelta della parametrizzazione della retta r (ciò si può prevedere essendo ogni cambiamento del sistema di riferimento di primo grado).

La definizione di molteplicità di intersezione è quindi ben posta e da tale definizione, e dal teorema fondamentale dell'algebra segue subito la seguente:

Proposizione 1.4.1 *Sia $f(x, y) \in \mathbf{R}[x, y]$ un polinomio di grado n. L'ordine n di una curva algebrica C^n di equazione*

$$f(x, y) = 0,$$

ha il significato **geometrico**, *di numero di punti, eventualmente contati con la dovuta molteplicità, comuni alla curva C^n e ad una retta generica r del piano non tutta contenuta in C^n.*

Se la curva è solo affine, si deve intendere il termine retta "generica" nel senso sopra precisato.

Definizione 1.4.2 *Sia P_0 un punto appartenente ad una curva algebrica piana C^n di ordine n definita dall'equazione $f(x,y) = 0$. P_0 si dice* **semplice** *per C^n se sono verificate le seguenti condizioni:*

1. *Ogni retta passante per P_0 è tale che $\mu_{r\cap C}(P_0) \geq 1$.*
2. *Esiste almeno una retta $\bar{r}$ passante per P_0 per cui $\mu_{\bar{r}\cap C}(P_0) = 1$.*

Dimostreremo ora il seguente teorema che caratterizza la retta tangente in un punto semplice di una C^n.

Teorema 1.4.1 *Se P_0 è un punto semplice di $C^n = \mathcal{V}(f(x,y))$, nel fascio di rette di centro P_0 esiste un'unica retta, detta tangente in P_0 alla C^n, avente molteplicità di intersezione maggiore o uguale a 2 con la C^n in P_0. Tale retta ha equazione*

$$\frac{\partial f}{\partial x}(P_0)(x - x_0) + \frac{\partial f}{\partial y}(P_0)(y - y_0) = 0,$$

ottenuta annullando i termini di grado minimo nello sviluppo di Taylor del polinomio $f(x,y)$ di punto iniziale P_0. Tutte le altre rette r passanti per P_0 diverse dalla tangente hanno molteplicità d'intersezione con la C^n in P_0 esattamente 1.

Dimostrazione. La generica retta r del fascio passante per P_0 ha equazioni:

$$\begin{cases} x = x_0 + lt, \\ y = y_0 + mt, \end{cases} \tag{1.3}$$

e la sua intersezione con la curva C^n è data dalle soluzioni del sistema:

$$\begin{cases} f(x,y) = 0, \\ x = x_0 + lt, \\ y = y_0 + mt, \end{cases}$$

la cui equazione risolvente è :

$$f(x_0 + lt, y_0 + mt) = 0.$$

Sviluppando $f(x,y)$ in formula di Taylor con punto iniziale P_0, si ha:[1]

$$\begin{aligned} f(x,y) &= f(x_0,y_0) + [f_x^0(x-x_0) + f_y^0(y-y_0)] + \\ &+ \frac{1}{2!}[f_{xx}^0(x-x_0)^2 + 2f_{xy}^0(x-x_0)(y-y_0) + f_{yy}^0(y-y_0)^2] + \\ &+ \ldots + \frac{1}{n!}\{\frac{\partial f}{\partial x}(x-x_0) + \frac{\partial f}{\partial y}(y-y_0)\}_0^n. \end{aligned}$$

Per ipotesi P_0 appartiene a C^n, quindi $f(x_0,y_0) = 0$. Inoltre da (1.3) segue: $lt = x - x_0$, $mt = y - y_0$.
L'equazione risolvente il sistema diventa quindi:

$$\begin{aligned} f(x_0+lt, y_0+mt) &= [f_x^0 l + f_y^0 m]t + \frac{1}{2!}[f_{xx}^0 l^2 + +2f_{xy}^0 lm + \\ &+ f_{yy}^0 m^2]t^2 + \ldots + \frac{1}{n!}\{\frac{\partial f}{\partial x}l + \frac{\partial f}{\partial y}m\}_0^n t^n. \end{aligned}$$

La soluzione $t = 0$ ha molteplicità esattamente 1 se e soltanto se è possibile mettere in evidenza t ma non t^2, ossia il coefficiente di t non è identicamente nullo. Poiché P_0 è semplice l'esistenza di una retta $\bar{r}$ passante per P_0 per cui $\mu_{\bar{r}\cap C}(P_0) = 1$ ci dice

$$f_x^0 \bar{l} + f_y^0 \bar{m} \neq 0.$$

Ne segue che $(f_x^0, f_y^0) \neq (0,0)$, ossia in P_0 non si annullano simultaneamente le derivate prime (**condizione analitica** affinché un punto sia semplice). Ma allora, per valori generici di l e m

$$f_x^0 l + f_y^0 m \not\equiv 0,$$

e quindi il primo membro è un polinomio di primo grado in l e m e, come tale, ha un'unica radice. Esiste quindi un'unica retta i cui parametri direttori (l,m) soddisfano l'equazione

$$f_x^0 l + f_y^0 m = 0.$$

Per tale retta, nell'equazione risolvente il sistema si potrà mettere in evidenza almeno t^2; quindi tale retta avrà molteplicità di intersezione ≥ 2. Essendo

[1] Si noti che si è indicato con f_x^0 la derivata di f rispetto ad x calcolata nel punto P_0. L'esponente n che figura nell'ultimo termine sta ad indicare una potenza simbolica n-esima del binomio che, quando agisce sull'operatore di derivazione ha il significato di derivata parziale n-esima.

(l, m) proporzionale secondo il fattore $1/t$ a $(x - x_0, y - y_0)$, tale retta, che dicesi tangente in P_0 a C^n, avrà equazione

$$f_x^0(x - x_0) + f_y^0(y - y_0) = 0.$$

Resta così anche dimostrato che P_0 è un punto semplice per C^n se e soltanto se $f(x_0, y_0) = 0$ e $(f_x^0, f_y^0) \neq (0, 0)$, ossia se e soltanto se è un punto di C^n in cui esiste la retta tangente in P_0 alla C^n. ∎

Definizione 1.4.3 *Un punto P_0 si dice* **doppio** *per la curva algebrica $C^n = \mathcal{V}(f(x, y))$ se sono verificate le seguenti condizioni:*

1. *Ogni retta passante per P_0 di parametri direttori (l, m) è tale che: $\mu_{r_{(l,m)} \cap C}(P_0) \geq 2$.*
2. *Esiste almeno una retta $\bar{r}$ del fascio, passante per P_0 e di parametri direttori $(\bar{l}, \bar{m})$, per cui si ha: $\mu_{r_{(\bar{l},\bar{m})} \cap C}(P_0) = 2$.*

Come nel corso della dimostrazione del Teorema precedente si prova che P_0 è un punto doppio per C^n se e soltanto se:

- $f_x^0 l + f_y^0 m = 0$ per ogni coppia (l, m), ossia $(f_x^0, f_y^0) = (0, 0)$.
- Esiste almeno una coppia $(\bar{l}, \bar{m})$ per cui si ha:

$$f_{xx}^0 \bar{l}^2 + 2 f_{xy}^0 \bar{l}\bar{m} + f_{yy}^0 \bar{m}^2 \neq 0.$$

Ne segue che $f_{xx}^0 l^2 + 2 f_{xy}^0 lm + f_{yy}^0 m^2$ non è identicamente nullo, ed essendo quest'ultimo un polinomio di secondo grado in (l, m), ha esattamente due radici in $\mathbf{C}$ che corrispondono ai parametri direttori delle uniche due rette del fascio di centro P_0 aventi molteplicità di intersezione ≥ 3. Queste due rette ovviamente possono essere: reali distinte, reali coincidenti o complesse coniugate, in corrispondenza il punto doppio si dirà, rispettivamente *nodo, cuspide, punto doppio isolato.* Resta così dimostrato il seguente:

Teorema 1.4.2 *Se P_0 è un punto doppio per C^n allora tutte le rette del fascio, escluse le due rette di parametri direttori verificanti:*

$$f_{xx}^0 l^2 + 2 f_{xy}^0 lm + f_{yy}^0 m^2 = 0, \tag{1.4}$$

hanno molteplicità d'intersezione $\mu_{r \cap C}(P_0) = 2$.
Le due rette verificanti (1.4), per cui la $\mu_{r \cap C}(P_0) \geq 3$ si chiamano **tangenti principali** *alla curva nel punto doppio.*

La **condizione analitica** affinché un punto P_0 sia doppio è che siano tutte nulle le derivate prime di f in P_0, ma che non si annullino tutte le derivate seconde. Lo sviluppo di Taylor di punto iniziale P_0 ha quindi termini di grado minimo 2 e annullando tali termini si ottiene l'equazione complessiva delle due tangenti principali al punto doppio. Più in generale si ha:

Definizione 1.4.4 *Un punto P_0 si dice $s-plo$ (o di molteplicità s) per C^n se sono verificate le seguenti condizioni:*

1. *Ogni retta r passante per P_0 di parametri direttori (l,m) è tale che $\mu_{r_{(l,m)}\cap C}(P_0) \geq s$.*
2. *Esiste almeno una retta $\bar{r}$ del fascio passante per P_0 e di parametri direttori $(\bar{l},\bar{m})$ per cui si ha: $\mu_{r_{(\bar{l},\bar{m})}\cap C}(P_0) = s$.*

Come si è visto nel caso $s = 2$, si ha in generale che tutte le rette per P_0, escluse le s rette i cui parametri direttori soddisfano la

$$\{\frac{\partial f}{\partial x}l + \frac{\partial f}{\partial y}m\}_0^s = 0,$$

che si dicono **tangenti principali** nel punto $s-plo$, hanno molteplicità d'intersezione con la curva C^n in P_0 uguale ad s, ossia $\mu_{r\cap C}(P_0) = s$.

La **condizione analitica** affinché un punto P_0 sia $s-plo$ è che siano nulle tutte le derivate in P_0 fino all'ordine $(s-1)$, ma non tutte nulle quelle di ordine s. Inoltre se P_0 è un punto $s-plo$ l'equazione:

$$\{\frac{\partial f}{\partial x}(x-x_0) + \frac{\partial f}{\partial y}(y-y_0)\}_0^s = 0,$$

ottenuta annullando i termini di grado minimo nello sviluppo di Taylor è l'equazione complessiva delle s tangenti principali in P_0; rappresenta, infatti, una curva algebrica di ordine s che si spezza nelle s tangenti principali.

Osservazione Lo sviluppo di Taylor di un polinomio di centro $P_0 = (x_0, y_0)$ si ottiene effettuando le sostituzioni:

$$\begin{cases} x = x_0 + (x - x_0), \\ y = y_0 + (y - y_0), \end{cases}$$

e poi ordinando rispetto a $(x - x_0)$ e $(y - y_0)$. In particolare, nel caso in cui $P_0 \equiv O = (0,0)$, lo sviluppo di Taylor del polinomio è il polinomio stesso. Ne segue che se il polinomio $f = f(x,y)$ è privo di termine noto, la curva $C = \mathcal{V}(f)$ passa per l'origine O; se f ha termini di grado minimo

$s \geq 1$ l'origine è un punto s-plo e l'equazione complessiva delle s tangenti principali nel punto s-plo O si ottiene annullando il complesso dei termini di grado minimo.

Esempi

- Consideriamo la cubica:

$$y^3 - 3x^2 = 0.$$

  Si chiede di studiare la natura dell'origine $O = (0, 0)$ e di determinare equazioni parametriche razionali.

I termini di grado minimo del polinomio in questione sono quelli di secondo grado, quindi $O = (0, 0)$ è un punto doppio e le tangenti principali hanno equazione complessiva $3x^2 = 0$. Per parametrizzare tale curva, osserviamo che ogni retta per O ha con la curva due intersezioni assorbite in O, trattandosi di una cubica, una tale retta ha dunque un un'unico punto di intersezione distinto da O con la cubica. Similmente a quanto fatto per determinare le equazioni parametriche della circonferenza, intersechiamo la cubica con il fascio di rette di centro O, ovvero consideriamo il sistema:

$$\begin{cases} y^3 - 3x^2 = 0, \\ y = tx, \end{cases}$$

la cui equazione risolvente è :

$$t^3x^3 - 3x^2 = x^2(t^3x - 3) = 0.$$

Scartando la soluzione (di molteplicità 2) $x = 0$ corrispondente all'origine, si ottiene l'ascissa dell'unico ulteriore punto di intersezione distinto da O. Sostituendo tale ascissa nella $y = tx$ si hanno per la cubica le equazioni parametriche razionali:

$$\begin{cases} x = \dfrac{3}{t^3}, \\ \\ y = \dfrac{3}{t^2}. \end{cases}$$

- Studiamo ora la quartica:

$$x^4 - x^3 + xy^2 = 0,$$

  nell'origine $O = (0, 0)$.

Per quanto osservato sopra, lo sviluppo di Taylor del polinomio nell'origine è il polinomio stesso. I termini di grado minimo sono quelli di terzo grado, quindi $O = (0, 0)$ è un punto triplo e l'equazione complessiva delle tangenti principali è

$$xy^2 - x^3 = x(y - x)(y + x) = 0.$$

Pertanto, le tre tangenti principali sono le rette

$$x = 0, \qquad y = x, \qquad y = -x.$$

Una generica retta per O avrà con la curva oltre alle tre intersezioni assorbite in O, solo un'ulteriore intersezione (trattandosi di una quartica). Per parametrizzare tale curva possiamo quindi ragionare analogamente a quanto fatto sia per la circonferenza che per la cubica dell'esempio precedente. Precisamente, intersecando con la generica retta per O si ha il sistema:

$$\begin{cases} x^4 - x^3 + xy^2 = 0, \\ y = tx, \end{cases}$$

la cui equazione risolvente è :

$$x^3(x - 1 + t^2) = 0$$

Scartando la soluzione tripla $x = 0$ corrispondente all'origine, si ottiene l'ascissa $x = 1 - t^2$ dell'ulteriore punto di intersezione della retta $y = tx$ con la quartica. Sostituendo tale espressione nella $y = tx$ si hanno le equazioni parametriche razionali della curva:

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

I due esempi generalizzano ad una cubica con un punto doppio e ad una quartica con un punto triplo il procedimento con cui abbiamo ottenuto la parametrizzazione razionale della circonferenza (che ha ordine 2 e in cui ogni punto è semplice). Tenendo presente il significato geometrico dell'ordine e la definizione di punto $(n - 1)$-plo, possiamo generalizzare il procedimento alle C^n con $n \geq 2$.

Teorema 1.4.3 *Una curva algebrica C^n con un punto $(n-1)-plo$ è razionale.*

Dimostrazione. Sia $P_0 = (x_0, y_0)$ il punto $(n-1)$-plo di C^n. Sviluppando in formula di Taylor di punto iniziale P_0, la equazione della curva si scrive nella forma

$$f(x,y) = \phi_n(x - x_0, y - y_0) + \phi_{n-1}(x - x_0, y - y_0) = 0,$$

dove $\phi_n(x-x_0, y-y_0)$ è la parte omogenea di grado n mentre $\phi_{n-1}(x-x_0, y-y_0)$ è la parte omogenea di grado $(n-1)$. Per quanto visto precedentemente $\phi_{n-1}(x - x_0, y - y_0) = 0$ è l'equazione complessiva delle $(n-1)$ tangenti principali in $P_0 = (x_0, y_0)$.

Per trovare una parametrizzazione razionale, studiamo l'intersezione tra la curva C^n e la generica retta del fascio passante per P_0:

$$\begin{cases} \phi_n(x - x_0, y - y_0) + \phi_{n-1}(x - x_0, y - y_0) = 0, \\ y - y_0 = t(x - x_0). \end{cases}$$

L'equazione risolvente tale sistema è:

$$\phi_n(x - x_0, t(x - x_0)) + \phi_{n-1}(x - x_0, t(x - x_0)) = 0.$$

Ricordiamo che una funzione $g(x,y)$ omogenea di grado α soddisfa per ogni t la

$$g(tx, ty) = t^\alpha g(x,y).$$

Essendo ϕ_n e ϕ_{n-1} due funzioni omogenee rispettivamente di grado n e $n-1$, si avrà

$$(x - x_0)^n \phi_n(1,t) + (x - x_0)^{n-1} \phi_{n-1}(1,t) = 0.$$

Mettendo in evidenza il termine $(x - x_0)^{n-1}$ si ottiene pertanto

$$(x - x_0)^{n-1}[(x - x_0)\phi_n(1,t) + \phi_{n-1}(1,t)] = 0.$$

Scartando la soluzione $(x-x_0)^{n-1}$ corrispondente al punto $(n-1)$-plo P_0, si ha l'ascissa dell'ulteriore punto Q_t di intersezione tra la retta r_t e la curva. Sostituendo nella $y - y_0 = t(x - x_0)$ si ha per la curva la parametrizzazione razionale:

$$\begin{cases} x = x_0 - \dfrac{\phi_{n-1}(1,t)}{\phi_n(1,t)}, \\ \\ y = y_0 - \dfrac{t\phi_{n-1}(1,t)}{\phi_n(1,t)}. \end{cases}$$

Come nel caso della circonferenza, non è detto che la parametrizzazione riempia tutta la varietà; non è infatti rappresentato il punto di intersezione con la retta $x = x_0$. ∎

1.5 Ideali

L'interesse degli ideali è che ci daranno un linguaggio per eseguire dei calcoli con varietà affini. In questo paragrafo, richiameremo la nozione di ideale direttamente nell'anello $A = k[x_1, \ldots, x_n]$, che è quello che a noi interessa, e inizieremo a vedere la relazione tra ideali di $k[x_1, \ldots, x_n]$ e varietà affini.

Definizione 1.5.1 *Un sottoinsieme I dell'anello $A = k[x_1, \ldots, x_n]$ è un* **ideale** *se soddisfa le seguenti condizioni:*
(i) $0 \in I$.
(ii) Se f *e* $g \in I$, *anche* $f + g \in I$.
(iii) Se $f \in I$ *e* $h \in k[x_1, \ldots, x_n]$, *anche* $hf \in I$.

Ovviamente, l'intersezione insiemistica di due ideali è ancora un ideale di A, mentre l'unione insiemistica non è, in generale, un ideale. Si dà allora la seguente

Definizione 1.5.2 *Sia S un sottoinsieme di un anello A. Si dice* **ideale generato da S** *e si indica con $< S >$, il minimo ideale di A contenente S.*

Si noti che che $< S >$ esiste come intersezione della famiglia, non vuota (in quanto contiene almeno A), di ideali di A contenenti S:

$$< S > \stackrel{\text{def}}{=} \bigcap_{A \geq I_h \supset S} I_h$$

Dati s polinomi $f_1, \ldots, f_s$ appartenenti all'anello $k[x_1, \ldots, x_n]$ ovviamente $< f_1, \ldots, f_s >$ contiene la totalità T delle combinazioni lineari, a coefficienti $h_i \in k[x_1, \ldots, x_n]$, degli elementi $f_1, \ldots, f_s$; basterà quindi verificare che T è un ideale perchè sia proprio l'ideale generato da $f_1, \ldots, f_s$.

Proposizione 1.5.1 *Sia $A = k[x_1, \ldots, x_n]$. Dati s polinomi $f_1, \ldots, f_s$ in A, l'insieme*

$$T = \{\sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in k[x_1, \ldots, x_n]\}$$

è un ideale dell'anello A, e coincide con l'ideale $< f_1, \ldots, f_s >$ generato da $f_1, \ldots, f_s$.

Dimostrazione. (i) Banalmente $0 \in T$, in quanto 0 si ottiene come combinazione lineare a coefficienti tutti nulli degli f_i.

Siano $f = \sum_{i=1}^{s} h_i f_i$ e $g = \sum_{i=1}^{s} q_i f_i$ e sia h un qualunque elemento di $k[x_1, \ldots, x_n]$.

(ii) Si ha che

$$f + g = \sum_{i=1}^{s} (h_i + q_i) f_i$$

è ancora una combinazione lineare dei polinomi $f_1, \ldots, f_s$, e quindi appartiene a T.

(iii) Sfruttando la proprietà distributiva dell'anello $k[x_1, \ldots, x_n]$, si ha poi

$$h(\sum_{i=1}^{s} h_i f_i) = \sum_{i=1}^{s} (h h_i) f_i$$

che di nuovo risulta essere una combinazione lineare a coefficienti $h h_i \in k[x_1, \ldots, x_n]$ di elementi di T. ∎

Nel caso in cui S sia costituito da un numero qualsiasi di polinomi basta osservare che ogni ideale contenente S dovrà contenere l'insieme T delle combinazioni lineari *finite* a coefficienti in $k[x_1, \ldots, x_n]$ di elementi di S e, poiché è semplice dimostrare, analogamente, che T è un ideale, si avrà ancora che $< S >$ coincide con l'insieme T.
Diamo ora un'interpretazione, in termini di equazioni polinomiali, dell' ideale $< f_1, \ldots, f_s >$. A tal fine, consideriamo il sistema:

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_s = 0 \end{cases}$$

ove $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Moltiplicando tali equazioni, rispettivamente, per $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$ e poi sommandole, otteniamo l'equazione:

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

e, per come abbiamo definito l'ideale $I =< f_1, \ldots, f_s >$, si ha anche che $h_1 f_1 + \ldots + h_s f_s \in I$, ossia $< f_1, \ldots, f_s >$ consiste di tutte le "conseguenze polinomiali" delle equazioni $f_1 = \ldots = f_s = 0$.

Esempio. Si consideri il sistema:

$$\begin{cases} x = 1 + t \\ y = 1 + t^2 \end{cases} \tag{1.5}$$

Eliminando il parametro t nel modo usuale, si ha l' equazione:

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

Possiamo però riscrivere la (1.5) nel modo seguente:

$$\begin{cases} f_1 = x - 1 - t = 0 \\ f_2 = y - 1 - t^2 = 0 \end{cases}$$

con $f_1, f_2 \in k[t, x, y]$. Moltiplicando f_1 per $g_1 = [(x-1)+t]$ e sottraendo a tale termine f_2, si ottiene ancora l'equazione:

$$g_1 f_1 - f_2 = (x-1)^2 - y + 1 = 0$$

Si ha quindi che

$$1 - y + (x-1)^2 = g_1 f_1 - f_2 \in < x - 1 - t, y - 1 - t^2 >,$$

e non dipende da t. Allo stesso modo ogni altra conseguenza polinomiale di f_1 e f_2 è un elemento dell'ideale $< f_1, f_2 >$.

Definizione 1.5.3 *Un ideale I di $k[x_1, \ldots, x_n]$ si dice* **finitamente generato** *se esistono s polinomi $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ tali che $I =< f_1, \ldots, f_s >$. I polinomi $(f_1, \ldots, f_s)$ si dicono* **base** *di I.*

Nel capitolo successivo, vedremo che ogni ideale di A è finitamente generato (questo è noto come "teorema della base di Hilbert), ed è per questo che la proposizione 1.5.1 è stata dimostrata solo in questo caso. Vedremo anche come scegliere delle basi particolarmente utili: le *basi di Groebner*.

Analogie con l'algebra lineare

1. Si osservi che uno stesso ideale può avere basi diverse e con un numero di elementi diversi. Mostriamo ad esempio che:

   $$< x, y >=< x + xy, y > .$$

   Dobbiamo far vedere che $x, y \in < x+xy, y >$ e che $x+xy, y \in < x, y >$. Posto $f_1 = x + xy$, $f_2 = y$ e $g_1 = x$, si ha

   $$\begin{cases} x = f_1 - g_1 f_2, & \text{con } g_1 \in k[x, y], \\ y = f_2, \end{cases}$$

   ossia x, y sono una combinazione lineare a coefficienti polinomiali degli elementi dell' ideale $< x + xy, y >$. Viceversa, si vede facilmente come $x + xy, y \in < x, y >$.

2. La definizione di *ideale* è molto simile a quella di *sottospazio vettoriale*. Entrambi devono essere chiusi rispetto all'addizione e alla moltiplicazione per coefficienti polinomiali nel primo caso e per gli scalari nel secondo. Si ha, inoltre, che l'*ideale generato* dai polinomi $f_1, \ldots, f_s$ è simile al *sottospazio generato* dal numero finito di vettori $v_1, \ldots, v_s$. In ogni caso, infatti, bisogna studiarne le combinazioni lineari: a coefficienti polinomiali nel caso di ideali, a coefficienti in un campo, quando si opera con i sottospazi vettoriali.
   Il concetto di base è comunque diverso in quanto una base di un ideale è semplicemente un *sistema di generatori*.

Vediamo ora la seguente proposizione che mostra come una varietà affine dipenda unicamente dall'ideale generato dai polinomi che la definiscono.

Proposizione 1.5.2 *Se $f_1, \ldots, f_s$ e $g_1, \ldots, g_t$ sono due basi dello stesso ideale di $k[x_1, \ldots, x_n]$ ossia $< f_1, \ldots, f_s >=< g_1, \ldots, g_t >$, si ha necessariamente che $\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t)$.*

Dimostrazione. Poiché per ipotesi $< g_1, \ldots, g_t > \subseteq < f_1, \ldots, f_s >$, ogni g_j è combinazione lineare degli f_i, ossia $g_j = \sum_{i=1}^{s} h_i f_i$.

Se a è un elemento di $\mathcal{V}(f_i)$, risulta $f_i(a) = 0$ per ogni $i = 1, \ldots, s$; pertanto, $g_j(a) = \sum_{i=1}^{s} h_i(a) f_i(a) = 0$ per ogni $j = 1, \ldots, t$, il che dimostra, per l'arbitrarietà di a in $\mathcal{V}(f_i)$, che

$$\mathcal{V}(f_1, \ldots, f_s) \subseteq \mathcal{V}(g_1, \ldots, g_t).$$

L'inclusione inversa si dimostra allo stesso modo, partendo dall'ipotesi che $< f_1, \ldots, f_s > \subseteq < g_1, \ldots, g_t >$. ∎

Il risultato di questa proposizione è di grande utilità nelle applicazioni pratiche. In alcuni casi, infatti, cambiando base in un ideale si trovano più facilmente i punti della varietà, come mostra il seguente

Esempio:

- Si consideri l'ideale:

  $$I =< 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 >=< x^2 - 4, y^2 - 1 >,$$

  come si verifica facilmente. Dalla proposizione precedente segue che :

  $$\mathcal{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathcal{V}(x^2 - 4, y^2 - 1) = \{\pm 2, \pm 1\}$$

  Utilizzando la seconda base scritta per l'ideale è, dunque, più semplice determinare la varietà.

Dalla proposizione precedente e dal sopracitato Teorema della base di Hilbert segue che ad un ideale I di $k[x_1, \ldots, x_n]$ (che, per il teorema di Hilbert è necessariamente del tipo $I =< f_1, \ldots, f_s >$) resta associata la varietà affine $V = \mathcal{V}(I)$. Viceversa:

Proposizione 1.5.3 *Se $V = \mathcal{V}(I)$ è una varietà affine di k^n, l'insieme*

$$\mathcal{I}(\mathcal{V}(I)) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \ \forall\, a \in V\}$$

dei polinomi che si annullano su V, è un ideale di $k[x_1, \ldots, x_n]$, che dicesi ideale associato a V

Dimostrazione. Lo 0 di $k[x_1, \ldots, x_n]$ appartiene a $\mathcal{I}(V)$ dato che si annulla in ogni punto di k^n e dunque in tutti i punti di V.

Se f e g sono due polinomi di $\mathcal{I}(V)$, per definizione di $\mathcal{I}(V)$ si ha $f(a) = g(a) = 0$ per ogni $a \in V$, da cui $f(a) + g(a) = 0 \ \forall\, a \in V$. Pertanto, anche $f + g$ appartiene a $\mathcal{I}(V)$.

Siano infine $h \in k[x_1, \ldots, x_n]$ ed $f \in \mathcal{I}(V)$. Di nuovo $f(a) = 0 \ \forall\, a \in V$, per cui anche $h(a)f(a) = 0 \ \forall\, a \in V$. Abbiamo così dimostrato che anche hf è un elemento di $\mathcal{I}(V)$. ∎

Si noti che se $V = \mathcal{V}(f_1, \ldots, f_s)$, sicuramente $f_1, \ldots, f_s \in \mathcal{I}(V)$.

Esempi:

1. Si consideri la varietà costituita dall'origine $\{(0,0)\}$ di k^2, definita ovviamente dal sistema:
$$\begin{cases} x = 0, \\ y = 0. \end{cases}$$
L'ideale associato a tale varietà , $\mathcal{I}(\mathcal{V}(x,y))$, è formato da tutti i polinomi appartenenti a $k[x,y]$ che si annullano in $\{(0,0)\}$.
Vogliamo provare che risulta:
$$\mathcal{I}(\mathcal{V}(x,y)) =< x, y > .$$
Banalmente, ogni polinomio appartenente all'ideale $< x, y >$ è della forma $A(x,y)x + B(x,y)y$, e quindi si annulla nell'origine. Risulta allora $< x, y > \subset \mathcal{I}$.
Per quanto riguarda l'inclusione inversa, si consideri un generico polinomio $f(x,y) = \sum_{i,j} a_{ij} x^i y^j$ appartenente a $k[x,y]$ e che si annulli

nell'origine. Si ha $a_{00} = f(0,0) = 0$, per cui:

$$\begin{aligned} f &= a_{00} + \sum_{(i,j)\neq(0,0)} a_{ij}x^i y^j \\ &= 0 + (\sum_{i>0,j} a_{ij}x^{i-1}y^j)x + (\sum_{j>0} a_{0j}y^{j-1})y \ \in < x, y > . \end{aligned}$$

Si noti che $I =< f_1, \ldots, f_s > \subseteq \mathcal{I}(\mathcal{V}(I))$, ma in generale risulta

$$< f_1, \ldots, f_s > \neq \mathcal{I}(\mathcal{V}(I)).$$

Infatti, avremmo potuto determinare l'origine anche come soluzione del sistema:

$$\begin{cases} x^2 = 0, \\ y^2 = 0. \end{cases}$$

Per quanto visto sopra l'ideale

$$\mathcal{I}(\mathcal{V}(x^2, y^2)) =< x, y >,$$

e risulta $< x^2, y^2 > \subset < x, y >$ ma $< x^2, y^2 > \neq < x, y >$, dato che $x \notin < x^2, y^2 >$ e $y \notin < x^2, y^2 >$.

2. Ci proponiamo ora di studiare l'ideale associato alla cubica sghemba in $\mathbf{R^3}$, di equazioni parametriche:

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

e di equazioni cartesiane:

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

In questo caso si vuole provare che:

$$\mathcal{I}(\mathcal{V}(I)) = I =< y - x^2, z - x^3 > .$$

Per arrivare a questo risultato dovremo fare vedere che per ogni $f \in k[x, y, z]$ tale che $f(t, t^2, t^3) = 0$ per ogni $t \in k$, risulta $f(x, y, z) = h_1(y - x^2) + h_2(z - x^3)$.

Proposizione 1.5.4 *Dato un polinomio $f \in k[x, y, z]$, è sempre possibile scrivere f nella forma:*

$$f(x, y, z) = h_1(y - x^2) + h_2(z - x^3) + r(x),$$

dove h_1 e h_2 sono polinomi nell'anello $k[x, y, z]$, mentre r è un polinomio nella sola x.

Dimostrazione. Sarà sufficiente dimostrare la proposizione nel caso in cui f sia un monomio, dato che ogni polinomio si può scrivere nella forma

$$f(x, y, z) = \sum_{\alpha,\beta,\gamma} c_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma$$

con $c_{\alpha\beta\gamma} \in k$.

Per un arbitrario monomio $x^\alpha y^\beta z^\gamma$, si può scrivere

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (x^2 + y - x^2)^\beta (x^3 + z - x^3)^\gamma \\ &= x^\alpha [x^2 + (y - x^2)]^\beta [x^3 + (z - x^3)]^\gamma \\ &= x^\alpha [x^{2\beta} + g_1(x, y, z)(y - x^2)][x^{3\gamma} + g_2(x, y, z)(z - x^3)] \\ &= x^{\alpha+2\beta+3\gamma} + h_1(x, y, z)(y - x^2) + h_2(x, y, z)(z - x^3) \end{aligned}$$

ove g_1, g_2, h_1, h_2 sono opportuni polinomi di $k[x, y, z]$. L'asserto è dunque vero per i monomi, il che completa la dimostrazione. ∎

Tornando ora all'esempio precedente della cubica sghemba $\mathcal{C}^3$, si ha che un polinomio f appartiene all'ideale $\mathcal{I}(\mathcal{C}^3)$ associato alla cubica se, e solo se, risulta $f(t, t^2, t^3) = r(t) = 0$ per ogni $t \in k$.

Abbiamo così trovato un polinomio della sola x, $r(x)$ che ammette infinite radici, ma, se k è infinito, per il principio d'identità dei polinomi, questo è possibile soltanto se $r(x) \equiv 0$.

Dunque ogni polinomio f appartenente all'ideale associato alla cubica sghemba si può scrivere:

$$f(x, y, z) = h_1(y - x^2) + h_2(z - x^3)$$

e, pertanto, appartiene all'ideale $I =< y - x^2, z - x^3 >$, da cui l'uguaglianza:

$$\mathcal{I}(\mathcal{C}^3) =< y - x^2, z - x^3 > .$$

Si è visto tuttavia che, in generale, $< f_1, \ldots, f_s > \subset \mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$ ma $< f_1, \ldots, f_s > \neq \mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$, come mostra l'esempio dato dall'ideale $< x^2, y^2 >$. Per quanto possa essere diverso da $< f_1, \ldots, f_s >$, l'ideale $\mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$ contiene abbastanza informazione da determinare univocamente la varietà.

Proposizione 1.5.5 *Siano V e W due varietà affini in k^n. Allora:*
(i) $V \subset W$ se e soltanto se $\mathcal{I}(V) \supset \mathcal{I}(W)$,
(ii) $V = W$ se e soltanto se $\mathcal{I}(V) = \mathcal{I}(W)$.

Dimostrazione. (i) Se $V \subset W$, ogni polinomio che si annulla su W si annulla, in particolare, anche su V, per cui si ha $\mathcal{I}(V) \supset \mathcal{I}(W)$.

Viceversa, sia W la varietà affine definita dal sistema:

$$\begin{cases} g_1 = 0 \\ \vdots \\ g_t = 0 \end{cases}$$

e, per ipotesi, si abbia che tutte le funzioni nulle su W sono nulle anche su V, ossia $\mathcal{I}(V) \supset \mathcal{I}(W)$. Poiché $g_1, \ldots, g_t$ sono in $\mathcal{I}(W) \subset \mathcal{I}(V)$, si deve avere:

$$\begin{cases} g_1(a) = 0 \\ \vdots \\ g_t(a) = 0, \quad \forall\, a \in V \end{cases}$$

Pertanto, ogni $a \in V$ è soluzione del sistema:

$$\begin{cases} g_1 = 0 \\ \vdots \\ g_t = 0 \end{cases}$$

da cui segue necessariamente che $V \subset W$.
(ii) Se vale l'uguaglianza $V = W$ si ha che $V \subseteq W$ e $W \subseteq V$ e quindi, per quanto dimostrato sopra, si hanno le due inclusioni $\mathcal{I}(V) \supseteq \mathcal{I}(W)$, e $\mathcal{I}(W) \supseteq \mathcal{I}(V)$ da cui $\mathcal{I}(V) = \mathcal{I}(W)$. Viceversa, partendo da quest'ultima uguaglianza, sempre per la (i) già dimostrata si deduce analogamente che $V = W$. ∎

Per quanto riguarda gli ideali si presentano i seguenti problemi, che affronteremo, per l'anello dei polinomi in una variabile, nei paragrafi che seguono.

- **Descrizione dell'ideale**, che consiste nel determinare se un ideale I si possa scrivere come $< f_1, \ldots, f_s >$ per opportuni polinomi $f_1, \ldots, f_s$ di $k[x_1, \ldots, x_n]$.
- **Appartenenza**, che consiste nella ricerca di un algoritmo che ci permetta di stabilire se un polinomio f appartiene o meno all'ideale $< f_1, \ldots, f_s >$.
- **Nullstellensatz** che consiste nello stabilire l'esatta relazione tra l'ideale $< f_1, \ldots, f_s >$ e l'ideale $\mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$.

1.6 Polinomi in una variabile

Nel corso di questo paragrafo studieremo i polinomi in una variabile, analizzando sia l'*algoritmo di divisione* che l*'algoritmo euclideo delle divisioni successive per la ricerca del Massimo Comun Divisore di due polinomi*. Questo ci aiuterà a studiare la struttura degli ideali nell'anello $k[x]$ dei polinomi in una indeterminata.

Si intende per *algoritmo* un insieme di istruzioni che permettono di elaborare dati simbolici o numerici. La struttura di un algoritmo è caratterizzata da un *input*, costituito dai dati numerici che noi inseriamo, e da un *output*, che è, invece, il risultato dell'algoritmo stesso.

Presenteremo gli algoritmi in *pseudocodice*, ossia in un linguaggio molto simile al Pascal. Ciò permetterà una facile comprensione della loro struttura.

Per studiare l'algoritmo di divisione fra polinomi dell'anello $k[x]$ richiamiamo la nozione di *termine direttore* (Leading Term) di un polinomio in una variabile.

Definizione 1.6.1 *Dato un polinomio non nullo $f \in k[x]$, ovvero:*

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0$$

dove $a_i \in k$ e $a_m \neq 0$ (per cui il grado di f è uguale ad m), il termine $a_m x^m$ si dice **termine direttore** *(leading term) di f, e si indica con $LT(f) = a_m x^m$.*

Si osservi che, dati due polinomi $f, g \in k[x]$ non nulli, si ha:

$$deg(f) \leq deg(g) \Longleftrightarrow LT(f) \text{ divide } LT(g).$$

Passiamo ora a descrivere l'algoritmo di divisione fra polinomi.

Proposizione 1.6.1 *Sia k un campo e sia g un polinomio non nullo in $k[x]$. Ogni polinomio $f \in k[x]$ può essere scritto nella forma:*

$$f = gq + r,$$

dove q ed r appartengono a $k[x]$, e risulta o $r = 0$ oppure $deg(r) < deg(g)$. Inoltre, q ed r sono unici ed esiste un algoritmo per calcolarli.

Dimostrazione. Siano f e g due polinomi in $k[x]$ di gradi rispettivi n ed m:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \qquad \text{con } LT(f) = a_n x^n,\ a_n \neq 0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0, \qquad \text{con } LT(g) = b_m x^m,\ b_m \neq 0.$$

Si ponga inizialmente il resto della divisione di f per g uguale ad $r_0 = f$. Se il grado di f è minore del grado di g basterà porre $f = 0g + f$. Se il grado di f è maggiore o uguale al grado di g, allora si può procedere nella divisione ottenendo al passo successivo r_1.

$$\begin{array}{l|l} r_0 = f(x) = a_n x^n + \ldots + a_0 & b_m x^m + \ldots + b_0 \\ \hline r_1 = r_0 - [LT(r_0)/LT(g)]g(x) & LT(r_0)/LT(g)) \end{array}$$

Ad ogni passo si possono presentare 3 casi:

- r è uguale a zero;
- il grado di r è minore del grado di g;
- il grado di r è maggiore o uguale al grado di g.

Nei primi due casi la divisione si arresta, mentre nel terzo caso si va avanti fino a quando non si presenti uno dei primi due casi.

Diamo ora, in pseudocodice, un algoritmo per il calcolo di q ed r. Nell'algoritmo si è posto inizialmente $q = 0$ e $r = f$, come conseguenza del fatto che ogni polinomio f si può esprimere come $f = 0g + f$.

Input: g, f
$q := 0$
$r := f$
WHILE $r \neq 0$ AND $LT(g)$ divides $LT(r)$ DO

$q := q + LT(r)/LT(g)$
$r := r - [LT(r)/LT(g)]\ g$
Output : q, r

Una volta assegnato l'algoritmo per il calcolo effettivo della divisione resta da dimostrare:

1. che l'algoritmo si arresta,

2. che l'output è costituito da due polinomi q ed r tali che $f = qg + r$,

3. l'unicità del quoziente e del resto.

1. Si osservi che l'insieme dei gradi dei resti è un insieme di numeri non negativi che ad ogni passo decresce. All'inizio il grado del resto è uguale ad n ma, dopo un numero finito di passi (al massimo $n-m+1$), sarà sicuramente inferiore al grado di g e, per quanto visto prima, in tal caso l'algoritmo si arresta.

2. La dimostrazione procede per induzione sul grado n di $f(x)$. Se $n = 0$, allora f è uguale ad una costante c, per cui $f = c = 0g + c$. Supponiamo allora che per ogni polinomio di grado $\leq n - 1$ esistano due polinomi q ed r soddisfacenti alle condizioni di cui nell'enunciato, e dimostriamo che questo vale anche per polinomi di grado n.
Si può sempre riscrivere $f(x)$ come:

$$f(x) = [f(x) - \frac{LT(f)}{LT(g)}g(x)] + \frac{LT(f)}{LT(g)}g(x)$$

e l'espressione entro parentesi è di grado minore di n, in quanto si cancella il termine direttore di f. Quindi per l'ipotesi induttiva:

$$f - \frac{LT(f)}{LT(g)}g = q_1 g + r$$

per cui

$$f(x) = (\frac{LT(f)}{LT(g)} + q_1)g(x) + r.$$

Posto $q = LT(f)/LT(g) + q_1$ si ha la tesi.

3. Supponiamo per assurdo che il quoziente ed il resto non siano unici, ossia:

$$f = qg + r = q_1 g + r_1 \tag{1.6}$$

ove sia r che r_1 hanno grado minore del grado di g (oppure uno dei due o entrambi sono nulli). Ne segue che, se $r \neq r_1$, necessariamente, il grado di $r - r_1$ è minore del grado di g. Ma dall'uguaglianza (1.6) segue:

$$(q_1 - q)g = (r - r_1)$$

se $r - r_1 \neq 0$ non può essere $q - q_1 = 0$ e pertanto se $r \neq r_1$ si ha $\partial(r - r_1) = \partial(q - q_1) + \partial g \geq \partial g$, il che contraddice il fatto $\partial(r - r_1) < \partial g$. L'assurdo prova dunque che è necessariamente $r - r_1 = 0$ e $q_1 - q = 0$, da cui la tesi.∎

Molti sistemi di algebra computazionale implementano l'algoritmo descritto per la divisione fra polinomi (cfr. DAVENPORT, SIRET e TOURNIER, (1988), [cfr[9]]).

Da questo teorema segue un utile corollario riguardo al numero di radici di un polinomio in una variabile.

Corollario 1.6.1 *Se k è un campo e $f(x) \in k[x]$ è un polinomio non nullo di grado $N = \partial f(x)$, si ha che $f(x)$ ha al più N radici in k.*

Dimostrazione. Si procede per induzione su N. Se $N = 0$, allora f è costante e l'equazione $f(x) = 0$ non ammette nessuna soluzione se non nel caso particolare $f = c = 0$.

Se $N = 1$, allora f si può scrivere come $f(x) = ax + b$ e l'equazione $f(x) = 0$ ammette l'unica soluzione $x = -(a)^{-1}b$.

Supposto vero l'enunciato per polinomi di grado $\leq N-1$, dimostriamolo vero per polinomi di grado N. A tale scopo faremo uso dell'algoritmo di divisione fra polinomi. Fissato comunque a in k, ogni polinomio f si può scrivere nella forma:

$$f(x) = (x - a)q(x) + r$$

dove o $r = 0$, oppure $\partial r < \partial(x - a) = 1$. Quindi se $r \neq 0$ si ha che r è una costante. In entrambi i casi valutando l'espressione in a si ottiene $f(a) = r$.

Se $f(a) = 0$, allora $(x-a)$ divide $f(x)$. In generale, se $f(x)$ non ha radici la tesi è banalmente verificata. Se invece $f(x)$ ha almeno una radice $a \in k$, allora:

$$f(x) = (x - a)q(x),$$

da cui, passando ai gradi si ottiene

$$\partial f = N = 1 + \partial(q(x)).$$

Pertanto $\partial(q(x)) = N - 1$ e, per ipotesi induttiva, $q(x)$ ha al più $N - 1$ radici. Dalla

$$f(x) = (x - a)q(x)$$

segue, valutando ambo i membri per una radice $b \neq a$ di $f(x)$, che ogni radice diversa da a di $f(x)$ è anche radice di $q(x)$. Infatti, essendo $b - a \neq 0$

$$0 = f(b) = (b - a)q(b) \ \Rightarrow q(b) = 0.$$

Resta così dimostrata la tesi. ∎

Dall'algoritmo di divisione dei polinomi segue anche il seguente corollario che fornisce una descrizione della struttura degli ideali in $k[x]$.

Corollario 1.6.2 *Sia k un campo. Ogni ideale $I \leq k[x]$ è* **principale***, ossia generato da un polinomio $g(x)$:*

$$I =< g >= \{hg \mid h \in k[x]\}$$

ed è perciò costituito dai multipli secondo polinomi di $g(x)$. Inoltre, $g(x)$ è unico a meno di una costante moltiplicativa non nulla in k, ed è un polinomio di grado minimo tra quelli appartenenti all'ideale I.

Dimostrazione. Se $I = \{0\}$, allora il risultato è banale in quanto $I =< 0 >$. Se $I \neq \{0\}$. esiste almeno un $g(x) \neq 0$ tale che $g(x) \in I$. Quindi l'insieme S dei gradi dei polinomi $g(x) \neq 0$ appartenenti ad I è un sottoinsieme non vuoto dell'insieme $\mathbf{N}$ degli interi non negativi, e, per la proprietà di buon ordinamento di $\mathbf{N}$, S ammette un minimo. Sia ora $g(x) \neq 0$ un polinomio di grado minimo tra i polinomi che appartengono ad I.

Per ogni polinomio $f(x) \in k[x]$, possiamo eseguire la divisione di $f(x)$ per $g(x)$:

$$f(x) = q(x)g(x) + r(x)$$

e $r = 0$ oppure $\partial r < \partial g$. Se $r = 0$, necessariamente f appartiene all' ideale. Se fosse $\partial r < \partial g$, essendo $g(x)$ un polinomio di grado minimo fra quelli appartenenti ad I, si avrebbe che r non può appartenere ad I. Ma

$$r(x) = f(x) - q(x)g(x)$$

e se $f(x) \in I$, il resto $r(x)$ deve appartenere ad I in quanto combinazione lineare di elementi di I. Risulta, pertanto, che $r(x) = 0$ e per ogni $f \in I$ si ha $f(x) = q(x)g(x)$.

Vogliamo ora dimostrare che $g(x)$ è unico a meno di una costante moltiplicativa non nulla. Sia per assurdo $< g >=< g_1 >$. Deve quindi essere verificato sia che $g \in< g_1 >$, sia che $g_1 \in< g >$; in termini equivalenti, si avrà che esistono h e t in $k[x]$ tali che $g = hg_1$ e $g_1 = tg$. Prendendo i gradi si ottiene $\partial g = \partial h + \partial g_1$ (il che implica $\partial g \geq \partial g_1$) e $\partial g_1 = \partial t + \partial g$ (il che implica che $\partial g_1 \geq \partial g$). In definitiva, risulta $\partial g = \partial g_1$ e quindi $\partial h = \partial t = 0$. Da ciò segue necessariamente che t ed h sono due costanti moltiplicative e ovviamente risultano l'una inversa dell'altra, da cui la tesi. ∎

Da questo corollario segue un criterio per stabilire l'**appartenenza** di un polinomio ad un ideale I. Siano infatti $I =< g(x) >$ e $f(x) \in k[x]$.
Il resto della divisione di $f(x)$ per $g(x)$ è uguale a zero, se e solo se, $f(x) \in I$.

La dimostrazione del corollario precedente non è costruttiva in quanto non fornisce un metodo per il calcolo del polinomio $g(x)$, ovvero del generatore dell'ideale I assegnato. Allo scopo di risolvere questo problema introduciamo la nozione di **massimo comun divisore** (MCD) fra polinomi.

Definizione 1.6.2 Un *massimo comun divisore dei polinomi f e g appartenenti all'anello $k[x]$ è un polinomio $h \in k[x]$ tale che:*

(i) h divide f e g,

(ii) se p è un altro polinomio che divide f e g, allora p divide h.

Se h è un polinomio che gode di tali proprietà, allora scriveremo:

$$h = MCD(f, g).$$

Studiamo ora alcune proprietà del massimo comun divisore.

Teorema 1.6.1 *Per ogni f e g appartenenti all'anello $k[x]$ si ha:*

(i) Esiste $h(x) = MCD(f, g)$ ed è unico a meno di una costante moltiplicativa non nulla.

(ii) $< h >=< f, g >$.

(iii) Esiste un algoritmo per calcolare $h(x)$ (l'algoritmo euclideo delle divisioni successive).

Dimostrazione. La (i) e la (ii) seguono dal fatto che l'ideale generato da due polinomi è principale, per il corollario 1.6.2. Se

$$< f, g >=< h >,$$

facciamo vedere che h è un massimo comun divisore tra f e g.

Dall'uguaglianza $< f, g >=< h >$, segue che $f \in< h >$ e $g \in< h >$, da cui $f = f_1 h$ e $g = g_1 h$, ossia h divide f e g.

D'altra parte, $h \in< f, g >$, quindi esistono A e B appartenenti a $k[x]$ tali che $h = Af + Bg$. Ne segue che ogni $p \in k[x]$ che divida f e g, necessariamente divide $Af + Bg = h$.

(iii) Siano N e M i gradi rispettivi di f e g. Scambiando, eventualmente, il ruolo di f e g, si può supporre, senza restrizioni, che $N \geq M$. Operiamo le seguenti divisioni:

$$\begin{aligned}
f &= q_1 g + r_1, \qquad \partial r_1 < \partial g, \\
g &= q_2 r_1 + r_2, \qquad \partial r_2 < \partial r_1, \\
r_1 &= q_3 r_2 + r_3, \qquad \partial r_3 < \partial r_2, \\
&\vdots \\
r_{n-1} &= q_{n+1} r_n + r_{n+1} \qquad \partial r_{n+1} < \partial r_n, \\
r_n &= q_{n+2} r_{n+1} + 0.
\end{aligned}$$

Non è difficile vedere che r_{n+1}, l'ultimo resto non nullo della divisione è un massimo comun divisore tra f e g. Infatti, partendo dall'ultima equazione e risalendo, via via fino alla prima, si vede che r_{n+1} divide r_n, ma allora divide anche $r_{n-1}, \ldots, r_3, r_2, r_1$ e quindi anche g ed f. Viceversa, partendo dalla prima equazione si vede che, se p è un divisore comune ad f e g, deve necessariamente dividere r_1, ma allora essendo un divisore comune a r_1 e a g si vede dalle successive che divide anche $r_2, r_3, \ldots, r_{n+1}$. Si ha quindi che r_{n+1} è un massimo comun divisore di f e g.

Dalle equazioni sopra scritte seguono le uguaglianze:

$$\begin{aligned}
< f, g > &= < g, r_1 >, \\
< g, r_1 > &= < r_1, r_2 >, \\
&\vdots \\
< r_{n-1}, r_n > &= < r_n, r_{n+1} > .
\end{aligned}$$

Mostriamo ora in pseudocodice l'algoritmo euclideo delle divisioni successive.

Abbiamo due variabili h e s che rappresentano il dividendo e, rispettivamente, il divisore delle divisioni. Indicheremo poi con rem il resto della divisione tra h e s:

Input: g, f
$h := f$

$s := g$
WHILE $s \neq 0$ DO
$rem := rem(h, s)$
$h := s$
$s := rem$
Output: h

Si noti che l'algoritmo si arresta in quanto l'insieme dei gradi dei resti è un insieme di interi non negativi che ad ogni passo decresce. ∎

Si ricorda che esiste anche una versione dell'Algoritmo Euclideo per trovare il massimo comun divisore di due interi, o, più in generale, di due elementi di una anello euclideo. La maggior parte dei sistemi di algebra computazionale hanno un comando per il calcolo del MCD di due polinomi (o interi), che utilizza una versione modificata dell'Algoritmo Euclideo. Per maggiori dettagli si consiglia DAVENPORT, SIRET e TOURNIER (1988), [cfr[9]].

1.7 Nullstellensatz nel caso di una variabile

Abbiamo visto come nel caso dell'anello $k[x]$, l'ideale generato dai polinomi f e g coincida con $< h(x) >$, dove $h(x) = MCD(f, g)$. Nel caso in cui, invece di due polinomi, consideriamo una s-pla $f_1, \ldots, f_s$, si ha la seguente

Definizione 1.7.1 *Siano $f_1, \ldots, f_s \in k[x]$, si dice* **massimo comun divisore** *dei polinomi $f_1, \ldots, f_s$ un polinomio h tale che*
(i) h divide $f_1, \ldots, f_s$,
(ii) Se p è un altro polinomio che divide $f_1, \ldots, f_s$, allora p divide h.
Quando h gode di queste proprietà, scriviamo $h = MCD(f_1, \ldots, f_s)$.

Non è difficile dimostrare la seguente Proposizione che estende al caso $s > 2$ quella già vista per $s = 2$ polinomi.

Proposizione 1.7.1 *Siano $f_1, \ldots, f_s \in k[x]$, con $s \geq 2$. Risulta:*
(i) esiste un $MCD(f_1, \ldots, f_s)$ ed è unico a meno di una costante moltiplicativa non nulla di k.
(ii) Un $MCD(f_1, \ldots, f_s)$ è un generatore dell'ideale $< f_1, \ldots, f_s >$.
(iii) Se $s \geq 3$, si ha

$$MCD(f_1, \ldots, f_s) = MCD(f_1, MCD(f_2, \ldots, f_s)).$$

(iv) Esiste un algoritmo per trovare un MCD tra s polinomi.

Si è visto inoltre come un generico polinomio $f \in k[x]$ appartiene all'ideale $I =< h(x) >$ se e soltanto se il resto della divisione fra f ed h è uguale a zero.

Vogliamo ora stabilire l'esatta relazione tra l'ideale I che definisce la varietà $V = \mathcal{V}(f_1, \ldots, f_s)$ e l'ideale ad essa associato $\mathcal{I}(V)$.

Si è già osservato in precedenza che $I \subset \mathcal{I}$. Sia ora k un *campo algebricamente chiuso* e V la varietà definita dal seguente sistema:

$$\begin{cases} f_1 = 0, \\ \vdots \\ f_s = 0. \end{cases}$$

La varietà V è altrettanto ben definita da ogni altra base dell'ideale

$$I =< f_1, \ldots, f_s > .$$

Poiché in $k[x]$ ogni ideale è principale, dalla (ii) della proposizione precedente segue che V è anche definita da $h(x) = MCD(f_1, \ldots, f_s)$.

Sia n il grado di $h(x)$, ossia:

$$h(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0,$$

con $a_n = LC(h) \neq 0$. Se $n \geq 1$, dal teorema fondamentale dell'algebra segue che $h(x)$ ha almeno una radice α_1, e sia r_1 la sua molteplicità . Esiste allora $H(x) \in k[x] - \{0\}$ tale che

$$h(x) = (x - \alpha_1)^{r_1} H(x), \qquad \text{con } H(\alpha_1) \neq 0.$$

Ogni α_i radice di $h(x)$, con $\alpha_i \neq \alpha_1$, è radice di $H(x)$. Per induzione sul grado n di $h(x)$, segue che $h(x)$ si può decomporre nel modo:

$$h(x) = (x - \alpha_1)^{r_1} \cdot \ldots \cdot (x - \alpha_t)^{r_t} a_n.$$

L'ideale I che definisce la varietà V si può quindi riscrivere come:

$$I =< (x - \alpha_1)^{r_1} \cdot \ldots \cdot (x - \alpha_t)^{r_t} > .$$

Definizione 1.7.2 *Dato il polinomio* $h(x) = (x - \alpha_1)^{r_1} \ldots (x - \alpha_t)^{r_t}$, *si definisce* **riduzione** *di* $h(x)$ *il polinomio:*

$$h_{rid}(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_t),$$

ossia il polinomio monico che ha esattamente le stesse radici distinte di h, *ma con molteplicità uguale ad uno.*

Studiamo ora il teorema degli zeri di Hilbert nel caso di una variabile.

Teorema 1.7.1 (Nullstellensatz) *Sia k un campo algebricamente chiuso. Assegnati s polinomi $f_1, \ldots, f_s$ in $k[x]$, si denoti con h un loro massimo comun divisore. Allora, dette $\alpha_1, \ldots, \alpha_t$ le radici distinte di h, risulta:*

$$\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(h) = \{\alpha_1, \ldots, \alpha_t\}$$

$$\mathcal{I}(\mathcal{V}(f_1, \ldots, f_s)) = \mathcal{I}(\mathcal{V}(h)) =< h_{rid} >=< (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_t) > .$$

Dimostrazione. Se il campo è algebricamente chiuso il polinomio h ha almeno una radice α_i; ma allora è divisibile per il binomio $x-\alpha_i$. Tale osservazione porta per induzione alla fattorizzazione sopra citata per h e alla definizione di h_{rid}. L'ideale $\mathcal{I}(\mathcal{V}(h))$ è costituito, per definizione, dai polinomi che si annullano su $\alpha_1, \ldots, \alpha_t$ e come tali sono divisibili per $x-\alpha_1, \ldots, x-\alpha_t$ e, quindi, sono divisibili anche per il loro prodotto h_{rid}. Si ha pertanto $\mathcal{I}(\mathcal{V}(h)) \subseteq < h_{rid} >$. Viceversa, poiché $\mathcal{V}(h) = \{\alpha_1, \ldots, \alpha_t\}$, ogni multiplo di h_{rid} è nullo su $\mathcal{V}(h)$ e, come tale, appartiene a $\mathcal{I}(\mathcal{V}(h))$ si ha pertanto che $\mathcal{I}(\mathcal{V}(h)) \supseteq < h_{rid} >$. Ovviamente, se k non è algebricamente chiuso non si ha la base per applicare l'induzione e arrivare alla fattorizzazione, in quanto esistono polinomi di grado positivo privi di radici. ∎

Nel caso di una variabile e se il campo è algebricamente chiuso, abbiamo così trovato la relazione tra I e l'ideale $\mathcal{I}(\mathcal{V}(I))$. Ma la risposta data non è soddisfacente in quanto è necessario saper fattorizzare completamente in fattori lineari il polinomio h per determinare h_{rid}. Vogliamo ora far vedere che si può determinare h_{rid} anche senza decomporre h nel prodotto dei suoi fattori lineari.

Dato un polinomio $h(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$, si definisce il *derivato formale* mediante le formule usuali dell'analisi:

$$h' = \frac{dh(x)}{dx} = \sum_{i=1}^{n} i a_i x^{i-1}$$

e non è difficile provare che valgono le regole di derivazione:

$$(ah)' = ah', \qquad (h+g)' = h' + g', \qquad (hg)' = h'g + hg',$$

dove $a \in k$ mentre $h, g \in k[x]$.

Proposizione 1.7.2 *Se α è una radice di molteplicità r per $h(x)$, allora α è una radice di molteplicità $(r-1)$ per il suo derivato h'.*

Dimostrazione. Se α è una radice di molteplicità r per $h(x)$ si ha:

$$h(x) = (x-\alpha)^r H(x), \qquad \text{con } H(\alpha) \neq 0,$$

da cui, calcolando il derivato di ambo i membri si ottiene:

$$\begin{aligned} h' &= r(x-\alpha)^{r-1}H(x) + (x-\alpha)^r H'(x) \\ &= (x-\alpha)^{r-1}[rH(x) + (x-\alpha)H'(x)]. \end{aligned}$$

Si vede quindi che α ha almeno molteplicità $(r-1)$ per h'. Dobbiamo mostrare che tale molteplicità è esattamente $(r-1)$. Posto $p(x) = rH(x) + (x-\alpha)H'(x)$, risulta:

$$p(\alpha) = rH(\alpha) + 0 = rH(\alpha) \neq 0,$$

ossia p non ammette $x = \alpha$ come radice. Ne segue che α è uno zero di molteplicità esattamente $r-1$ per $h'(x) = (x-\alpha)^{r-1}p(x)$. ∎

In base a questa proposizione possiamo scrivere h_{rid} in funzione di h e del suo derivato h':

$$h_{rid} = \frac{h}{MCD(h, h')}.$$

L'ideale associato alla varietà definita da $f_1, \ldots, f_s$, è quindi

$$\mathcal{I}(\mathcal{V}(I)) = < \frac{h}{MCD(h, h')} >,$$

ove $h = MCD(f_1, \ldots, f_s)$.

Esempio: Si vuole trovare una base per l'ideale associato alla varietà affine definita dai due polinomi:

$$\begin{aligned} f_1(x) &= x^5 - 2x^4 + 2x^2 - x \\ f_2(x) &= x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \end{aligned}$$

Si ha:

$$\begin{aligned} f_1(x) &= x[(x^4-1) - 2x(x^2-1)] = x(x-1)^3(x+1) \\ f_2(x) &= (x-1)[x^4 - 2x^2 + 1] = (x-1)^3(x+1)^2 \end{aligned}$$

Un massimo comun divisore tra $f_1(x)$ e $f_2(x)$ è quindi:

$$h(x) = MCD(f_1, f_2) = (x-1)^3(x+1)$$

Per quanto osservato in precedenza $I =< (x-1)^3(x+1) >$. Risulta quindi $\mathcal{V}(I) = \{-1, 1\}$. Inoltre:

$$h' = (x-1)^2[4x+2],$$

da cui:

$$MCD(h, h') = (x-1)^2.$$

Applicando quanto visto sulla *riduzione* di h si ha:

$$h_{rid} = \frac{h(x)}{MCD(h, h')} = \frac{(x-1)^3(x+1)}{(x-1)^2} = (x-1)(x+1).$$

In base a quanto affermato in precedenza, possiamo concludere che l'ideale associato alla varietà affine definita dai due polinomi f_1 ed f_2, si può scrivere come:

$$\mathcal{I}(\mathcal{V}(I)) =< (x-1)(x+1) > .$$