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)

4. DIZIONARIO DI ALGEBRA-GEOMETRIA

Dipartimento di Matematica

Facoltà di Scienze Matematiche, Fisiche e Naturali

Capitolo 4

Dizionario di algebra-geometria

In questo capitolo dimostreremo le diverse versioni del Nullstellensatz, teorema che permette di stabilire una precisa corrispondenza tra ideali e varietà. Questo permetterà la costruzione di un dizionario di algebra e geometria, attraverso il quale ogni affermazione di carattere geometrico, quindi riguardante varietà, potrà essere trasformata nella corrispettiva in ambito algebrico, o meglio in termini di ideali, e viceversa. Dopo aver affrontato questi argomenti, verranno definite le naturali operazioni algebriche tra ideali, quali ad esempio somma, prodotto, etc. per studiare l'analogo in ambito geometrico. Si svilupperà inoltre una serie di algoritmi attinenti a queste operazione tra ideali. Il capitolo si concluderà studiando alcuni concetti algebrici e geometrici connessi al teorema della base di Hilbert. Precisamente: la possibilità di decomporre una varietà in un'unione di varietà più semplici e la corrispondente nozione algebrica.

4.1 Nullstellensatz

Abbiamo visto nei capitoli precedenti una varietà $V \subset k^n$ può essere studiata passando all'ideale associato

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

costituito di tutti i polinomi che si annullano sulla varietà V. Precisamente, si definisce tra l'insieme delle Varietà affini di k^n e l'insieme degli ideali di $k[x_1, \ldots, x_n]$ la seguente applicazione

$$V \longrightarrow \mathcal{I}(V).$$

Viceversa, dato un ideale $I \subset k[x_1, \ldots, x_n]$ possiamo considerare l'insieme

$$\mathcal{V}(I) = \{x \in k^n \mid f(x) = 0 \ \forall \ f \in I\}.$$

Il Teorema della base di Hilbert ci garantisce che $\mathcal{V}(I)$ è sicuramente una varietà affine, ossia esiste un insieme finito di polinomi $f_1, \ldots, f_s \in I$ tale che $I =< f_1, \ldots, f_s >$ e $\mathcal{V}(I)$ è l'insieme delle radici comuni a questi polinomi. Possiamo in tal modo definire la seguente applicazione

$$I \longrightarrow \mathcal{V}(I).$$

tra ideali e varietà affini. Le due applicazioni sopra definite stabiliscono una corrispondenza tra ideali e varietà.

La prima cosa da osservare è che l' applicazione $\mathcal{V}$ *non è una corrispondenza iniettiva*, infatti ideali diversi possono dar luogo alla stessa varietà. Ad esempio $< x >$ e $< x^2 >$ sono ideali diversi di $k[x]$, ma definiscono la stessa varietà, $\mathcal{V}(x) = \mathcal{V}(x^2) = \{0\}$.

Se il campo su cui si sta lavorando non è algebricamente chiuso, possono sorgere altri problemi. Ad esempio, consideriamo i seguenti polinomi 1, $1 + x^2$, $1 + x^2 + x^4$, contenuti in $\mathbf{R}[x]$. Questi generano i tre ideali diversi:

$$I_1 =< 1 >= \mathbf{R}[x] \quad I_2 =< 1 + x^2 >, \quad I_3 =< 1 + x^2 + x^4 > .$$

Poichè ciascuno dei polinomi generatori non ammette radici reali, le corrispondenti varietà coincidono tutte con la varietà vuota:

$$\mathcal{V}(I_1) = \mathcal{V}(I_2) = \mathcal{V}(I_3) = \emptyset.$$

Possiamo fornire anche esempi di polinomi in due variabili, i quali non presentano radici reali come $1 + x^2 + y^2$, $1 + x^2 + y^4$ che dànno origine ad ideali diversi in $\mathbf{R}[x, y]$ ma che corrispondono alla varietà vuota.

Teorema 4.1.1 Nullstellensatz (versione debole). *Sia k un campo algebricamente chiuso e sia $I \leq k[x_1, \ldots, x_n]$ un ideale per il quale risulti $\mathcal{V}(I) = \emptyset$. Allora $I = k[x_1, \ldots, x_n]$.*

Dimostrazione. Per dimostrare che I è uguale a $k[x_1, \ldots, x_n]$ è sufficiente verificare che $1 \in I$, poiché in tal caso, per definizione di ideale, si ha $f = 1 \cdot f \in I$, per ogni $f \in k[x_1, \ldots, x_n]$.

La dimostrazione verrà fatta per induzione sul numero delle variabili. Se $n = 1$ ed $I \leq k[x]$, essendo l'anello $k[x]$ un anello principale (i.e. ogni

ideale è generato da un unico polinomio), dire che $\mathcal{V}(I) = \emptyset$ significa dire che il generatore g dell'ideale $I =< g >$ non ammette radici in k. Ma k è algebricamente chiuso e pertanto il teorema fondamentale dell'algebra implica che il grado di $g(x)$ deve necessariamente essere uguale a zero, e quindi g è una costante $c \in k$ diversa da zero, ossia:

$$g = \ cost = c \neq 0 \quad I =< c > .$$

Dalla $1 = c \cdot \ c^{-1}$ segue allora che $1 \in I =< c >$ e pertanto $I =< 1 >= k[x]$.

Supposto, vero il teorema per $n-1$ dimostriamolo per n. Sia $I = < f_1, \ldots, f_s > \leq k[x_1, \ldots, x_n]$ un ideale per il quale risulti $\mathcal{V}(I) = \emptyset$. Possiamo assumere, rinumerando eventualmente i polinomi f_i, che f_1 non sia costante (poiché altrimenti non ci sarebbe nulla da dimostrare) e quindi che il grado *totale* di f_1 sia $N \geq 1$.

Dimostriamo, in primo luogo, che possiamo supporre che f_1 abbia la forma

$$f_1(x_1, \ldots, x_n) = cx_1^N + \text{termini in cui x}_1 \text{ ha grado } < \text{N},$$

con $c \neq 0$ costante (questo perché avremo bisogno di applicare il corollario del teorema di estensione geometrico per mettere in relazione $\mathcal{V}(I)$ con la sua proiezione sul sottospazio delle ultime $n-1$ coordinate $x_2, \ldots, x_n$). A tale scopo, utilizziamo il seguente cambiamento di coordinate

$$\begin{aligned} x_1 &= \tilde{x_1} \\ x_2 &= \tilde{x_2} + a_2\tilde{x_1} \\ &\vdots \\ x_n &= \tilde{x_n} + a_n\tilde{x_1} \end{aligned}$$

ove le $a_i \in k$ sono delle costanti da determinare. Sostituendo, al posto di $x_1, \ldots, x_n$, nella f_1, si ottiene

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= f_1(\tilde{x_1}, \tilde{x_2} + a_2\tilde{x_1}, \ldots, \tilde{x_n} + a_n\tilde{x_1}) \\ &= c(a_2, \ldots, a_n)\tilde{x_1}^N + \text{termini in } \tilde{x_1} \text{ di grado minore di N.} \end{aligned}$$

Ora $c(a_2, \ldots, a_n)$ è un'espressione polinomiale non nulla in $a_2, \ldots a_n$ e, poiché un campo algebricamente chiuso è infinito, si può applicare il principio di identità dei polinomi. Questo implica che si possono scegliere $a_2, \ldots a_n$ in modo tale che $c(a_2, \ldots, a_n) \neq 0$.

Con questa scelta di $a_2, \ldots a_n$ e con il cambiamento di coordinate, ogni polinomio $f \in k[x_1, \ldots, x_n]$, si trasforma in un polinomio $\tilde{f} \in k[\tilde{x_1}, \ldots, \tilde{x_n}]$

e l'insieme $\tilde{I} = \{\tilde{f} \mid f \in I\}$ è un ideale di $k[\tilde{x_1}, \ldots, \tilde{x_n}]$. Risulta ancora che $\mathcal{V}(\tilde{I}) = \emptyset$, poiché se le equazioni trasformate avessero soluzioni anche le f_i di partenza ne avrebbero. Rimpiazzando le x_i con le $\tilde{x_i}$ e tutti i polinomi f con gli $\tilde{f}$, il polinomio f_1 verrà rimpiazzato da

$$\tilde{f_1}(\tilde{x_1}, \ldots, \tilde{x_n}) = c(a_2, \ldots, a_n)\tilde{x_1}^N + \text{termini in } \tilde{x_1} \text{ di grado minore di N.}$$

e poiché $c(a_2, \ldots, a_n) \neq 0$ siamo nella situazione voluta e possiamo applicare il Corollario del Teorema di estensione geometrico, valido in ogni campo algebricamente chiuso. Se

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

$$(x_1, \ldots, x_n) \longmapsto (x_2, \ldots, x_n)$$

è la proiezione sulle ultime $n-1$ coordinate e $\tilde{I_1} = \tilde{I} \cap k[\tilde{x_2}, \ldots, \tilde{x_n}]$ è il primo ideale di eliminazione, il suddetto corollario asserisce che ogni soluzione parziale in k^{n-1} può essere estesa cioè $\mathcal{V}(\tilde{I_1}) = \pi_1(\mathcal{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset$

Per l'ipotesi induttiva si ha che $\tilde{I_1} = k[\tilde{x_2}, \ldots, \tilde{x_n}]$. Ma questo implica che $1 \in \tilde{I_1} \subset \tilde{I}$, il che completa la dimostrazione. ∎

Si noti che, nel caso particolare in cui $k = \mathbf{C}$ la versione debole del Nullstellensatz è l'analogo del teorema fondamentale dell'algebra per polinomi in più variabili, ossia ogni insieme di polinomi, che generi un ideale più piccolo di $\mathbf{C}[x_1, \ldots, x_n]$ ha zeri comuni in $\mathbf{C}^n$.

Possiamo inoltre affermare che il Nullstellensatz ci suggerisce come risolvere il **problema di compatibilità**. Come già visto, tale problema consiste nel poter affermare se un sistema di equazioni polinomiali

$$\begin{cases} f_1 = 0 \\ f_2 = 0 \\ \vdots \\ f_s = 0 \end{cases}$$

ammetta soluzioni in $\mathbf{C}^n$. I polinomi non hanno soluzioni comuni se e soltanto se $\mathcal{V}(f_1, \ldots, f_s) = \emptyset$. Per il Nullstellensatz questo accade se e soltanto se $1 \in I =< f_1, \ldots, f_s >$. Non è difficile dimostrare che, *per ogni ordine monomiale* $\{1\}$ *è l'unica base di Groebner ridotta per l'ideale* $< 1 >$.

Infatti, sia $\{g_1, \ldots, g_s\}$ una base di Groebner per l'ideale $I =< 1 >$. Per definizione di base di Groebner abbiamo

$$1 \in < LT(g_1), \ldots, LT(g_t) >$$

Per il Lemma 2.4.1 si ha che 1 è divisibile per qualche $LT(g_i)$, sia ad esempio $LT(g_1)$. Ciò implica che $LT(g_1)$ è necessariamente una costante. Ma allora ogni altro $LT(g_i)$ è un multiplo di quella costante, e pertanto $g_2, \ldots, g_t$ possono essere eliminati dalla base di Groebner per il Lemma 2.7.1. Infine, poiché $LT(g_1)$ è una costante, anche g_1 è costante, poiché ogni monomio non costante è > 1 (cfr. Corollario 2.4.2) . Moltiplicando g_1, per una costante opportuna, possiamo fare in modo che $g_1 = 1$, la base di Groebner ridotta che si ottiene è pertanto $\{1\}$.

Riassumendo: abbiamo ricavato il seguente **algoritmo di compatibilità** Dati i polinomi $f_1, \ldots, f_s \in \mathbf{C}[x_1, \ldots, x_n]$ calcoliamo la base di Groebner ridotta, rispetto ad un qualsiasi ordinamento monomiale, dell'ideale $I =< f_1, \ldots, f_s >$. Se si ottiene $\{1\}$ i polinomi non hanno radici comuni in $\mathbf{C}^n$, se la base invece è diversa da $\{1\}$ il sistema è compatibile e viceversa. Si noti che che l'algoritmo funziona nei due versi solo su un campo algebricamente chiuso.

Osservazioni (1) Se stiamo lavorando in un campo che non sia algebricamente chiuso l'algoritmo di compatibilità funziona soltanto in una direzione. Precisamente, se $\{1\}$ è la base di Groebner ridotta di $< f_1, \ldots, f_s >$, allora il sistema

$$f_1 = 0, \ldots, f_s = 0$$

è incompatibile, mentre il viceversa non è vero, come dimostrano gli esempi che precedono la dimostrazione del teorema 4.1.1.

(2) Il Teorema 4.1.1 potrebbe far pensare che, se k è algebricamente chiuso, la corrispondenza $\mathcal{V}$ tra ideali e varietà affini sia iniettiva (lo è per la varietà $\emptyset$). Ciò non è vero, come mostra l'esempio $\mathcal{V}(x) = \mathcal{V}(x^2) = \{0\}$ che funziona su un campo qualunque. Analogamente, gli ideali $< x^i, y^j >$, per $i, j \in \mathbf{Z},\ i, j \geq 2$ sono diversi da $< x, y >$ ma definiscono tutti la stessa varietà affine ossia l'origine di k^2. Questi esempi illustrano uno dei motivi di base per cui l'applicazione $\mathcal{V}$ tra ideali di $k[x_1, \ldots, x_n]$ e varietà affini di k^n non è iniettiva: la potenza di un polinomio svanisce sullo stesso insieme su cui svanisce il polinomio. Il Nullstellensatz stabilisce che, sopra un campo algebricamente chiuso, questo è *l'unico* motivo per cui ideali diversi dànno luogo alla stessa varietà: se un polinomio f svanisce su tutti i punti della varietà $\mathcal{V}(I)$, allora qualche potenza di f deve appartenere ad I.

Teorema 4.1.2 Nullstellensatz di Hilbert. *Sia k un campo algebricamente chiuso, se $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ sono tali che $f \in \mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$ allora esiste un intero $m \geq 1$ tale che*

$$f^m \in < f_1, \ldots, f_s >,$$

(e viceversa).

Dimostrazione. Dato f un polinomio identicamente nullo su ogni soluzione comune ad $f_1, \ldots, f_s$, vogliamo dimostrare che esistono un intero $m \geq 1$ e dei polinomi $A_1, \ldots, A_s$ tali che

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

Infatti, se $f^m \in I$, deve potersi scrivere come combinazione lineare di polinomi appartenenti alla base dell'ideale I.

La dimostrazione di questo teorema si basa sulla seguente strategia particolare: si considera l'ideale

$$\tilde{I} =< f_1, \ldots, f_s, 1 - yf > \leq k[x_1, \ldots, x_n, y]$$

e si dimostra che $\mathcal{V}(\tilde{I}) = \emptyset$. A tale scopo, se $a = (a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$ è un punto arbitrariamente fissato, si possono verificare due casi:

- $(a_1, \ldots, a_n)$ è una radice comune di $f_1, \ldots, f_s$.
- $(a_1, \ldots, a_n)$ non è una radice comune di $f_1, \ldots, f_s$.

Nel primo caso $f(a_1, \ldots, a_n) = 0$, poiché f svanisce su ogni zero comune di $f_1, \ldots, f_s$. Quindi nel punto $a \in k^{n+1}$ risulta $(1 - yf)(a) = 1 - a_{n+1} \cdot 0 = 1 \neq 0$. Pertanto $a = (a_1, \ldots, a_n, a_{n+1}) \notin \mathcal{V}(\tilde{I})$.

Nel secondo caso, esiste almeno un $\bar{i}$ ($1 \leq \bar{i} \leq s$) tale che $f_{\bar{i}}(a_1, \ldots, a_n) \neq 0$. Pensando la $f_{\bar{i}}$ come funzione di $n+1$ variabili, ma che non dipende dall'ultima variabile si ha $f_{\bar{i}}(a_1, \ldots, a_n, a_{n+1}) \neq 0$. Pertanto anche in questo caso $a = (a_1, \ldots, a_n, a_{n+1}) \notin \mathcal{V}(\tilde{I})$.

Poichè il punto $a \in k^{n+1}$ è stato scelto in modo arbitrario, si ha $\mathcal{V}(\tilde{I}) = \emptyset$. Applicando il Nullstellensatz versione debole, si ottiene che $1 \in \tilde{I}$ e come elemento dell'ideale $\tilde{I}$ può scriversi come combinazione lineare con coefficienti con $p_i, q \in k[x_1, \ldots, x_n, y]$ dei generatori di $\tilde{I}$

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - fy).$$

Sostituendo, ora $y = 1/f$ nella sommatoria appena scritta si ottiene:

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, \frac{1}{f}) f_i,$$

identità che può essere scritta soltanto nel campo dei quozienti $k(x_1, \ldots, x_n)$. Moltiplicando ambo i membri dell'uguaglianza per f^m con m sufficientemente grande da cancellare tutti i denominatori, si giunge all'espressione:

$$f^m = \sum_{i=1}^{s} A_i f_i$$

ove A_i sono polinomi appartenenti a $k[x_1, \ldots, x_n]$. Questo dimostra appunto che esiste m tale che $f^m \in I$. (Il viceversa ovvio). ∎

4.2 Ideali radicali

Per illustrare la relazione esistente tra ideali e varietà è naturale riformulare il Nullstellensatz in termini di ideali e caratterizzare gli ideali che sono associati a varietà.

Lemma 4.2.1 *Sia V una varietà. Se $f^m \in \mathcal{I}(V)$, allora $f \in \mathcal{I}(V)$.*

Dimostrazione. Sia $x \in V$ un elemento arbitrariamente fissato. Se $f^m \in \mathcal{I}(V)$, allora $(f(x))^m = 0$; questo accade (se e) solo se $f(x) = 0$. Essendo x arbitrario si ha che $f \in \mathcal{I}(V)$. ∎

Un ideale che consista di *tutti* i polinomi che si annullano su una varietà V, gode della proprietà che se una potenza di un polinomio appartiene all'ideale anche il polinomio deve appartenere all'ideale.

Definizione 4.2.1 *Un ideale I si dice* **ideale radicale** *se $f^m \in I$ per qualche intero $m \geq 1$ implica $f \in I$.*

Rielaborando il Lemma 4.2.1 in termini di ideali abbiamo:

Corollario 4.2.1 *$\mathcal{I}(V)$ è un ideale radicale.*

Definizione 4.2.2 *Si dice* **radicale dell'ideale** *$I \leq k[x_1, \ldots, x_n]$, e si indica con $\sqrt{I}$, l'insieme*

$$\sqrt{I} = \{f \mid f^m \in I \text{ per qualche } m \geq 1\}.$$

Si noti che $I \subset \sqrt{I}$, infatti se $f \in I$ allora $f^1 \in I$ e $f \in \sqrt{I}$ per definizione. È un semplice esercizio verificare che I è radicale se e soltanto se $I = \sqrt{I}$.

Un fatto più sorprendente è, invece, che l'insieme $\sqrt{I}$ risulta sempre un ideale, come dimostreremo nel prossimo lemma. Per spiegare meglio tale affermazione consideriamo, ad esempio, l'ideale $J =< x^2, y^3 >\leq k[x, y]$. È

facile verificare che né x né y appartengono a J, ma risulta evidente che $x \in \sqrt{J}$ e $y \in \sqrt{J}$; inoltre $(x \cdot y)^2 = x^2y^2 \in J$ poiché $x^2 \in J$ e quindi anche $x \cdot y \in \sqrt{J}$. E' meno ovvio invece che $x + y \in \sqrt{J}$. Per vederlo, osserviamo che

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in J,$$

in quanto $x^4, 4x^3y, 6x^2y^2 \in J$ (essendo multipli di x^2) e $4xy^3$, $y^4 \in J$ (essendo multipli di y^3). Allora $x + y \in \sqrt{J}$. In definitiva, xy e $x + y$ sono nel $\sqrt{J}$ ma né xy né $x + y$ appartengono a J.

Lemma 4.2.2 *Se I è un ideale di $k[x_1, \ldots, x_n]$, allora $\sqrt{I}$ è un ideale di $k[x_1, \ldots, x_n]$ che contiene I, inoltre $\sqrt{I}$ è un ideale radicale.*

Dimostrazione. Abbiamo già visto che $I \subset \sqrt{I}$. Per dimostrare che $\sqrt{I}$ è un ideale si devono verificare le tre proprietà che caratterizzano gli ideali. Banalmente $0 \in \sqrt{I}$. Se $f, g \in \sqrt{I}$, per definizione di radicale, esistono m, ℓ interi positivi tali che $f^m,\ g^\ell \in I$. Nello sviluppo della potenza $(f+g)^{m+\ell-1}$ ogni termine ha un fattore $f^i g^j$ con $i + j = m + \ell - 1$. Si ha quindi $i \geq m$ oppure $j \geq \ell$ e pertanto f^i o g^j appartengono ad I: allora $f^i g^j \in I$ e ogni termine dello sviluppo appartiene ad I. Si ha $(f + g)^{m+\ell-1} \in I$ e quindi $f + g \in \sqrt{I}$. Infine, se $f \in \sqrt{I}$ e $h \in k[x_1, \ldots, x_n]$, per definizione di $\sqrt{I}$, $f^m \in I$ per qualche intero $m \geq 1$; essendo I un ideale si ha che $(f \cdot h)^m = f^m h^m \in I$, pertanto $fh \in \sqrt{I}$ e $\sqrt{I}$ è un ideale.

La dimostrazione del fatto che $\sqrt{I}$ è un ideale radicale è lasciata per esercizio al lettore. ∎

Teorema 4.2.1 Nullstellensatz versione forte. *Sia k un campo algebricamente chiuso. Se I è un ideale di $k[x_1, \ldots, x_n]$ allora:*

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

Dimostrazione. Per dimostrare l'uguaglianza verifichiamo le due inclusioni opposte. La prima inclusione $\sqrt{I} \subset \mathcal{I}(\mathcal{V}(I))$ si ottiene considerando che se $f \in \sqrt{I}$, allora $f^m \in I$ per qualche m. Quindi f^m svanisce su $\mathcal{V}(I)$ il che implica che anche f svanisce su $\mathcal{V}(I)$ e, pertanto, $f \in \mathcal{I}(\mathcal{V}(I))$.

Viceversa, sia $f \in \mathcal{I}(\mathcal{V}(I))$, per il Nullstellensatz di Hilbert, esiste un intero $m \geq 1$ tale che $f^m \in I$, e questo implica che $f \in \sqrt{I}$. Per l'arbitrarietà di f abbiamo che $\mathcal{I}(\mathcal{V}(I)) \subset \sqrt{I}$ da cui la tesi. ∎

Una conseguenza importante del Nullstellensatz è che ci permette di iniziare la costruzione del dizionario algebra-geometria. Il seguente Teorema getta le basi per tale costruzione.

Teorema 4.2.2 Corrispondenza tra ideali e varietà *Sia k un campo arbitrario.*
(i) Le applicazioni $\mathcal{I}$ e $\mathcal{V}$

$$\{varietà\ affini\} \stackrel{\mathcal{I}}{\to} \{ideali\}$$

e

$$\{ideali\} \stackrel{\mathcal{V}}{\to} \{varietà\ affini\}$$

invertono le inclusioni, nel senso che se $I_1 \subset I_2$ sono due ideali allora $\mathcal{V}(I_1) \supset \mathcal{V}(I_2)$ e analogamente se $V_1 \subset V_2$ sono due varietà, allora $\mathcal{I}(V_1) \supset \mathcal{I}(V_2)$. Inoltre, per ogni varietà V abbiamo

$$\mathcal{V}(\mathcal{I}(V)) = V,$$

quindi, $\mathcal{I}$ è sempre iniettiva e la sua inversa sinistra è proprio $\mathcal{V}$.
(ii) Se k è algebricamente chiuso e se ci restringiamo solo a considerare ideali radicali le applicazioni:

$$\{varietà\ affini\} \stackrel{\mathcal{I}}{\to} \{ideali\ radicali\}$$

e

$$\{ideali\ radicali\} \stackrel{\mathcal{V}}{\to} \{varietà\ affini\}$$

sono corrispondenze biunivoche che invertono le inclusioni e sono una inversa dell'altra.

Dimostrazione. (i) Che $\mathcal{I}$, e $\mathcal{V}$ invertono le inclusioni è un semplice esercizio lasciato al lettore.

Per verificare l'uguaglianza tra insiemi $\mathcal{V}(\mathcal{I}(V)) = V$ dimostriamo le due inclusioni apposte. Sappiamo che quando $V = \mathcal{V}(I)$ risulta $I \subset \mathcal{I}(V)$; sfruttando ora il fatto che V inverte le inclusioni si ha $\mathcal{V}(I) \supset \mathcal{V}(\mathcal{I}(V))$. L'inclusione inversa $\mathcal{V}(I) = V \subset \mathcal{V}(\mathcal{I}(V))$ segue direttamente dalle definizioni, poiché ogni $f \in \mathcal{I}(V)$ svanisce su V.

(ii) Poiché $\mathcal{I}(V)$ è radicale per il Corollario 4.2.1, possiamo pensare $\mathcal{I}$ come una funzione tra varietà e ideali radicali. Si sa, inoltre, che $\mathcal{V}(\mathcal{I}(V)) = V$ per ogni varietà V, rimane, quindi da dimostrare che $\mathcal{I}(\mathcal{V}(I)) = I$ se I è radicale. Se k è algebricamente chiuso dal Nullstellensatz si ha che $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, ma I è radicale e quindi $I = \sqrt{I}$ da cui l'uguaglianza desiderata. Per concludere abbiamo che $\mathcal{I}$ e $\mathbf{V}$ sono una inversa dell'altra, e quindi biunivoche, quando ci si restringe a considerare solo ideali radicali e k è algebricamente chiuso. ∎

Osservazioni.

(1) Come conseguenza di questo Teorema si ha che ogni affermazione riguardante le varietà può essere ricondotta ad un'affermazione di carattere algebrico, riguardante ideali radicali e vale, inoltre, il viceversa, naturalmente sempre sotto l'ipotesi che il campo sia algebricamente chiuso.

(2) Data l'importanza che il Nullstellensatz attribuisce agli ideali radicali è naturale chiedersi se sia possibile determinare i generatori del radicale $\sqrt{I}$ dai generatori dell'ideale $I =< f_1, \ldots, f_s >$. Precisamente, si presentano i seguenti tre problemi:

- **Generatori del radicale** Si può determinare un algoritmo che fornisca, fissato $I =< f_1, \ldots, f_s >$, un insieme $\{g_1, \ldots, g_m\}$ di polinomi tali che $\sqrt{I} =< g_1, \ldots, g_m >$?
- **Ideale radicale** Esiste un algoritmo che verifichi se I è radicale?
- **Appartenenza al radicale** Dato un polinomio $f \in k[x_1, \ldots, x_n]$ esiste un algoritmo che ci permetta di verificare se $f \in \sqrt{I}$?

L'esistenza di questi algoritmi segue da un lavoro di Hermann [14] del 1926, sfortunatamente gli algoritmi che si deducono per i primi due problemi non sono ottimali e inoltre sono di difficile implementazione. Tuttavia, lavori di Gianni, Trager e Zacharias [13] del 1988 e di Eisenbud, Huneke e Vasconcelos [10] del 1992 conducono ad algoritmi implementati in SCRATCHPAD e, rispettivamente, Macauley, per determinare il radicale di un ideale. Questi algoritmi sono, comunque piuttosto sofisticati e coinvolgono concetti al di fuori degli scopi di questo corso.

Ci proponiamo invece di risolvere il *problema di appartenenza al radicale*, ed esamineremo il *problema dei generatori del radicale di un ideale I, nel caso particolare in cui I sia principale.*

Per controllare che $f \in \sqrt{I}$ si potrebbe far riferimento all'algoritmo di appartenenza ad un ideale e verificare se $f^m \in I$ per tutti gli interi $m > 0$. Si deve però sottolineare che ciò non è conveniente perché potremmo dover arrivare a potenze troppo grandi di f e questo controllo non ci dirà mai se $f \notin \sqrt{I}$ (a meno di non stabilire a priori dei limiti per m). Possiamo invece adattare la dimostrazione del Nullstellensatz di Hilbert per determinare se $f \in \sqrt{< f_1, \ldots, f_s >}$.

Proposizione 4.2.1 (Appartenenza al radicale.) *Sia k un campo arbitrario e sia $I =< f_1, \ldots, f_s > \subseteq k[x_1, \ldots, x_n]$ un ideale. Allora $f \in \sqrt{I}$ se*

e soltanto se il polinomio costante 1 *verifica la*

$$1 \in \tilde{I} =< f_1, \ldots, f_s, 1 - yf > \leq k[x_1, \ldots, x_n, y].$$

Dimostrazione. Se $1 \in \tilde{I}$, 1 può essere espresso come combinazione lineare di elementi della base di $\tilde{I}$:

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + (1 - yf) q(x_1, \ldots, x_n, y).$$

Si considera, ora il campo dei quozienti $k(x_1, \ldots, x_n, y)$ nel quale si può porre $y = 1/f$. Sostituendo si ha:

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, \frac{1}{f}) f_i.$$

Moltiplicando ambo i membri per f^m con m sufficientemente grande da eliminare tutti i denominatori, si ottiene che esistono un intero $m \geq 1$ e dei polinomi $A_i \in k[x_1, \ldots, x_n]$ tali che

$$f^m = \sum_{i=1}^{s} A_i f_i,$$

e quindi che $f^m \in I$. Ma ciò implica che $f \in \sqrt{I}$.

Per dimostrare l'implicazione inversa, si parte dall'ipotesi che $f \in \sqrt{I}$, ossia che $f^m \in I \subset \tilde{I}$ per qualche m. Ma abbiamo anche che $1 - yf \in \tilde{I}$ e pertanto:

$$1 = y^m f^m + (1 - y^m f^m) = y^m \cdot f^m + (1 - yf) \cdot (1 + yf + \ldots + y^{m-1} f^{m-1}) \in \tilde{I},$$

come volevasi dimostrare. ∎

La Proposizione 4.2.1, insieme alle osservazioni precedenti su come si stabilisca se 1 appartenga o meno ad un ideale (si veda la discussione sul problema di compatibilità) ci permettono di fornire il seguente

Algoritmo di appartenenza al radicale.

Volendo verificare se $f \in \sqrt{< f_1, \ldots, f_s >} \subset k[x_1, \ldots, x_n]$, si calcola la base di Groebner ridotta dell'ideale $< f_1, \ldots, f_s, 1 - yf >$ di $k[x_1, \ldots, x_n, y]$,

rispetto ad un ordinamento fissato. Se il risultato è $\{1\}$, allora $f \in \sqrt{I}$, altrimenti $f \notin \sqrt{I}$.

Esempio. Consideriamo l'ideale:

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

di $k[x, y]$. Si vuole verificare se il polinomio $f = y - x^2 + 1$ appartiene a $\sqrt{I}$.

Fissato l'ordinamento lessicografico in $k[x, y, z]$, scriviamo l'ideale $\tilde{I} =< xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) >$ di $k[x, y, z]$. Controllando che la base di Groebner ridotta di tale ideale è proprio $\{1\}$, si può concludere che $y - x^2 + 1 \in \sqrt{I}$.

Usando l'algoritmo di divisione possiamo determinare quale potenza di $f = y - x^2 + 1$ appartiene ad I. Una base di Groebner per I rispetto all'ordinamento lessicografico è $G = \{x^4 - 2x^2 + 1, y^2\}$; per ogni $p \in k[x_1, \ldots, x_n]$, indichiamo con $\overline{p}^G$ il resto della divisione di p per G. Risulta

$$\begin{aligned} \overline{y - x^2 + 1}^G &= y - x^2 + 1, \\ \overline{(y - x^2 + 1)^2}^G &= -2x^2y + 2y, \\ \overline{(y - x^2 + 1)^3}^G &= 0. \end{aligned}$$

Ne segue che $(y - x^2 + 1)^3 \in I$ ma potenze più basse non appartengono ad I, in particolare $y - x^2 + 1 \notin I$.

Interpretiamo, ora tale esempio dal punto di vista geometrico. L'insieme $\mathcal{V}(I) = \{(\pm 1, 0)\}$ delle soluzioni comuni ai polinomi di I, è costituito da soluzioni che hanno molteplicità almeno due. Questo si vede chiaramente dalla forma dei generatori dell'ideale I, infatti se li fattorizziamo si ha

$$xy^2 + 2y^2 = y^2(x + 2) \quad e \quad x^4 - 2x^2 + 1 = (x^2 - 1)^2.$$

Il polinomio $f = y - x^2 + 1$ si annulla in $(\pm 1, 0)$ ma la molteplicità di tali radici è uno; per avere un elemento di I si devono prendere delle potenze più alte della f.

Concludiamo questo paragrafo con il **calcolo del radicale di** un ideale I nel caso in cui $I =< f >$ sia **un ideale principale**.

Ricordiamo che un polinomio si dice irriducibile quando dalla $f = h \cdot g$ segue necessariamente che o h o g è una costante e che ogni polinomio f ammette una decomposizione, essenzialmente unica,

$$f = f_1^{a_1} f_2^{a_2} \cdots f_r^{a_r}$$

in fattori irriducibili f_i $(1 \leq i \leq r)$ tutti distinti tra loro.

Proposizione 4.2.2 *Sia $f \in k[x_1, \ldots, x_n]$ e sia $I =< f >$ l'ideale principale generato da f. Se $f = f_1^{a_1} f_2^{a_2} \ldots f_r^{a_r}$ è la decomposizione di f in fattori irriducibili allora:*

$$\sqrt{I} = \sqrt{< f >} =< f_1 \cdots f_r > .$$

Dimostrazione. Per prima cosa dimostriamo che il prodotto $f_1 \cdots f_r$ appartiene al $\sqrt{I}$. Sia N un intero più grande del massimo tra $a_1, \ldots, a_r$. Allora

$$(f_1 \cdots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \cdots f_r^{N-a_r} f$$

è un polinomio multiplo di f. Questo mostra che $(f_1 \cdots f_r)^N \in I$ e ciò implica che $f_1 \cdots f_r \in \sqrt{I}$. Quindi $< f_1 \cdots f_r > \subset \sqrt{I}$.

Viceversa, sia $g \in \sqrt{I}$ dobbiamo far vedere che $g \in < f_1 \cdots f_r >$. Poiché $g \in \sqrt{I}$, esiste un intero positivo M tale che $g^M \in I =< f >$. Quindi $g^M = h \cdot f$ per qualche polinomio h. Se $g = g_1^{b_1} \cdots g_s^{b_s}$ è la decomposizione di g in fattori irriducibili, allora $g^M = g_1^{b_1 M} \cdots g_s^{b_s M}$ è la decomposizione di $g^M = h \cdot f$ e risulta

$$g_1^{b_1 M} \cdots g_s^{b_s M} = h \cdot f_1^{a_1} f_2^{a_2} \cdots f_r^{a_r}.$$

Per l'unicità della fattorizzazione, i polinomi irriducibili in entrambi i membri devono essere uguali a meno di un fattore costante. Ne segue che ogni f_i $(1 \leq i \leq r)$ deve essere uguale ad un multiplo secondo una costante di qualche g_j. Questo implica che g è un polinomio multiplo secondo un fattore polinomiale di $f_1 \cdots f_r$ e pertanto g è contenuto nell'ideale $< f_1 \cdots f_r >$. ∎

Definizione 4.2.3 *Se $f \in k[x_1, \ldots, x_n]$ è un polinomio, si dice* **riduzione** *(o parte priva di quadrati) di f il polinomio*

$$f_{rid} = f_1 \cdots f_r$$

prodotto dei fattori irriducibili di f, presi ciascuno con molteplicità uno ossia $< f_{rid} >= \sqrt{< f >}$. Un polinomio si dice **ridotto** *se $f = f_{rid}$.*

Ad esempio: la riduzione del polinomio $f = (x + y^2)^3(x - y)$ è il polinomio $f_{rid} = (x + y^2)(x - y)$. Si noti che f_{rid} è unico a meno di un fattore costante in k.

Il problema principale della Proposizione 4.2.2 è che presuppone la fattorizzazione di f. Esiste, tuttavia, un algoritmo che permette di ricavare f_{rid} da f, senza fattorizzare f.

Definizione 4.2.4 *Siano $f, g \in k[x_1, \ldots, x_n]$. Un polinomio h si dice* **massimo comun divisore** *di f, g e si denota con $h = MCD(f, g)$ se:*
i) h divide f e g
ii) se p è un polinomio che divide sia f che g, allora p divide h

Si può verificare che il $MCD(f, g)$ esiste ed è unico, a meno di un fattore costante. Sfortunatamente, l'algoritmo euclideo per determinare il massimo comun divisore in una variabile non può essere utilizzato nel caso di più variabili. Per vederlo basta considerare $f = xy$ e $g = xz$ in $k[x, y, z]$. Ovviamente il $MCD(f, g) = x$, ma, in ogni ordine monomiale, la divisione di xy per xz dà quoziente 0 e resto xz e la divisione di xz per xy dà quoziente 0 e resto xy. Quindi non si può fare il passo successivo analogo a quello dell'algoritmo euclideo.

Ciononostante, esiste un algoritmo, che vedremo nel prossimo paragrafo, per il calcolo del massimo comun divisore di due polinomi in più variabili che, come nel caso di una variabile, si può estendere al calcolo del $MCD(f_1, \ldots, f_s)$ di $s > 2$ polinomi. Usando tale algoritmo, si può dare una formula per il calcolo del radicale di un ideale principale.

Proposizione 4.2.3 *Supponiamo di avere un campo k a caratteristica zero, sia $I =< f >$ un ideale principale di $k[x_1, \ldots, x_n]$. Allora $\sqrt{I} =< f_{rid} >$ ove*

$$f_{rid} = \frac{f}{MCD(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n})}.$$

Dimostrazione. Scrivendo f come nella Proposizione 4.2.2 sappiamo che $\sqrt{I} =< f_1 \cdots f_r >$. Quindi basta dimostrare che

$$MCD(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}) = f_1^{a_1 - 1} \cdots f_r^{a_r - 1}. \tag{4.1}$$

Applicando la regola di derivazione del prodotto si ottiene:

$$\frac{\partial f}{\partial x_j} = f_1^{a_1 - 1} f_2^{a_2 - 1} \cdots f_r^{a_r - 1} (a_1 \frac{\partial f_1}{\partial x_j} f_2 \cdots f_r + \cdots + a_r f_1 f_2 \cdots \frac{\partial f_r}{\partial x_j}).$$

Questo prova che $f_1^{a_1 - 1} \cdots f_r^{a_r - 1}$ divide il MCD. Resta da dimostrare che per ciascun i, esiste qualche $\frac{\partial f}{\partial x_j}$ che non è divisibile per $f_i^{a_i}$.

Scriviamo $f = f_i^{a_i} h_i$, con h_i non divisibile per f_i. Poiché f_i non è costante, qualche variabile x_j deve comparire in f_i. Dalla regola di derivazione del prodotto si ha

$$\frac{\partial f}{\partial x_j} = f_i^{a_i - 1} (a_i \frac{\partial f_i}{\partial x_j} h_i + f_i \frac{\partial h_i}{\partial x_j}).$$

Se questa espressione è divisibile per $f_i^{a_i}$ allora $\frac{\partial f_i}{\partial x_j} h_i$ deve essere divisibile per f_i; ma f_i è irriducibile e non divide h_i, ciò implica che f_i divide $\frac{\partial f_i}{\partial x_j} \neq 0$ in quanto la caratteristica del campo è 0 e x_j figura effettivamente in f_i.

Poiché $\frac{\partial f_i}{\partial x_j}$ ha grado minore di f_i si ha che f_i non può dividere $\frac{\partial f_i}{\partial x_j}$. Ne segue che $\frac{\partial f}{\partial x_j}$ non è divisibile per $f_i^{a_i}$, il che prova la (4.1). ∎

In tale Proposizione l'ipotesi che il campo su cui si sta lavorando sia a caratteristica zero è essenziale, in quanto per campi a caratteristica $p \neq 0$ la formula che dà f_{rid} può fallire (si pensi ad esempio al polinomio $f = x_1^2 + \ldots + x_n^2$ di $\mathbf{Z}_2[x_1, \ldots, x_n]$ per il quale $\frac{\partial f}{\partial x_j} = 0$ per ogni $j = 1, \ldots, n$, essendo il campo a caratteristica 2).

4.3 Operazioni tra ideali.

Gli ideali sono degli oggetti algebrici sui quali possiamo definire naturalmente una serie di operazioni. Ne consideriamo in questo paragrafo tre: **somma, intersezione e prodotto**, nel prossimo definiremo il quoziente.

Tali operazioni, come noto, sono operazioni binarie, cioè ad ogni coppia di ideali si può associare un nuovo ideale. Le domande che ci poniamo sono:

- dati i generatori di una coppia di ideali, come calcolare i generatori dell'ideale che si determina applicando tali operazioni?
- qual'è il significato geometrico di queste operazioni?

4.3.1 Somma di ideali

Definizione 4.3.1 *Siano I, J due ideali di $k[x_1, \ldots, x_n]$, si dice* **somma** *di I e J e si indica con $I + J$ l' insieme:*

$$I + J = \{f + g \mid f \in I \text{ e } g \in J\}. \tag{4.2}$$

Proposizione 4.3.1 *Se $I =< f_1, \ldots, f_r >$ e $J =< g_1, \ldots, g_s >$ sono due ideali di $k[x_1, \ldots, x_n]$, la loro somma $I+J$ è ancora un ideale di $k[x_1, \ldots, x_n]$, ed è il più piccolo ideale che contiene I e J; risulta*

$$I + J =< f_1, \ldots, f_r, g_1, \ldots, g_s > .$$

Dimostrazione. Per dimostrare che l'insieme (4.2) è ancora un ideale si devono verificare le tre proprietà degli ideali. Banalmente $0+0=0 \in I+J$.

Se $h_1, h_2 \in I+J$, per la definizione di $I+J$ esistono $f_1, f_2 \in I$ e $g_1, g_2 \in J$ tali che $h_1 = f_1+g_1$ e $h_2 = f_2+g_2$. Sommando (per le proprietà commutativa e associativa) si ha: $h_1+h_2 = (f_1+f_2)+(g_1+g_2)$; ora $f_1+f_2 \in I$ e $g_1+g_2 \in J$ perché I e J sono ideali. Quindi $h_1 + h_2 \in I + J$.

Per verificare la chiusura rispetto alla moltiplicazione, consideriamo $h \in I+J$ e $l \in k[x_1, \ldots, x_n]$, sempre per la definizione di somma di ideali esistono $f \in I$ e $g \in J$ tali che $h = f + g$; moltiplicando tale espressione per l si ottiene:

$$l \cdot h = l \cdot (f + g) = l \cdot f + l \cdot g.$$

Ora $l \cdot f \in I$ e $l \cdot g \in J$, conseguentemente $l \cdot h \in I + J$. Questo prova che $I + J$ è un ideale.

Ogni ideale H che contenga I e J dovrà contenere tutti gli elementi $f \in I$ e $g \in J$. Poiché H è un ideale, dovrà contenere tutti gli $f + g$ con $f \in I$ e $g \in J$, in particolare $H \supset I + J$. Poichè $I + J$ è esso stesso un ideale è necessariamente il più piccolo ideale che contiene I e J.

Infine, se $I =< f_1, \ldots, f_r >$ e $J =< g_1, \ldots, g_s >$ allora $< f_1, \ldots, f_r, g_1, \ldots, g_s >$ è un ideale che contiene I e J così $I + J \subset< f_1, \ldots, f_r, g_1, \ldots, g_s >$. L'inclusione inversa è ovvia. Quindi $I + J =< f_1, \ldots, f_r, g_1, \ldots, g_s >$. ∎

Dalla Proposizione 4.3.1 segue immediatamente.

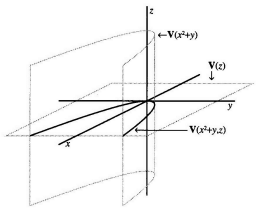
Corollario 4.3.1 *Se $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, allora*

$$< f_1, \ldots, f_r >=< f_1 > + \ldots + < f_r > .$$

Osservazione. Per comprendere cosa accade geometricamente consideriamo i seguenti ideali di $\mathbf{R}[x, y, z]$

$$I =< x^2 + y >, \quad J =< z > .$$

Sappiamo che $\mathcal{V}(I) = \mathcal{V}(x^2+y)$ è il cilindro con generatrici parallele all'asse z che si appoggia alla parabola $y = -x^2$ del piano xy mentre $\mathcal{V}(J) = \mathcal{V}(z)$ è il piano xy. L'ideale $I + J =< x^2 + y, z >$ contiene $x^2 + y$ e z; quindi la varietà $\mathcal{V}(I+J)$ deve essere costituita da tutti i punti che annullano sia x^2+y che z ossia $\mathcal{V}(I + J)$ deve essere l'intersezione di $\mathcal{V}(I)$ e $\mathcal{V}(J)$. Graficamente si può rappresentare con la figura seguente.



Teorema 4.3.1 *Se I e J sono due ideali di $k[x_1, \ldots, x_n]$, allora*

$$\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J).$$

Dimostrazione. Se $x \in \mathcal{V}(I + J)$, allora $x \in \mathcal{V}(I)$ perché $I \subset I + J$; analogamente risulta anche $x \in \mathcal{V}(J)$, essendo $J \subset I + J$. Quindi $x \in \mathcal{V}(I) \cap \mathcal{V}(J)$ e si ha $\mathcal{V}(I + J) \subset \mathcal{V}(I) \cap \mathcal{V}(J)$.

Per dimostrare l'inclusione inversa, supponiamo che $x \in \mathcal{V}(I) \cap \mathcal{V}(J)$. Sia h un polinomio in $I + J$, allora esistono $f \in I$ e $g \in J$ tali che $h = f + g$. Ma $f(x) = 0$ poiché $x \in \mathcal{V}(I)$ e $g(x) = 0$ perché $x \in \mathcal{V}(J)$. Quindi $h(x) = f(x) + g(x) = 0 + 0 = 0$. Per l'arbitrarietà di h possiamo concludere che $x \in \mathcal{V}(I + J)$. Pertanto $\mathcal{V}(I + J) \supset \mathcal{V}(I) \cap \mathcal{V}(J)$. ∎

4.3.2 Prodotto di ideali.

Come si è visto nel Capitolo 1, l'ideale generato dal prodotto dei generatori di due ideali corrisponde all'unione di due varietà:

$$\mathcal{V}(f_1, \ldots, f_r) \cup \mathcal{V}(g_1, \ldots, g_s) = \mathcal{V}(f_i g_j, 1 \leq i \leq r, 1 \leq j \leq s).$$

Ad esempio, la varietà $\mathcal{V}(xz, yz)$, che corrisponde ad un ideale generato dal prodotto di generatori degli ideali $< x, y >$ e $< z >$, è unione della varietà $\mathcal{V}(x, y)$, che rappresenta l'asse z e della varietà $\mathcal{V}(z)$, che rappresenta il piano xy. Questo ci suggerisce la seguente definizione.

Definizione 4.3.2 *Si dice prodotto di due ideali I e J di $k[x_1, \ldots, x_n]$, e si indica con $I \cdot J$, l'ideale generato da tutti i prodotti $f \cdot g$ di polinomi con $f \in I$ e $g \in J$.*

Il prodotto $I \cdot J$ è l'insieme

$$I \cdot J = \{f_1 g_1 + \ldots + f_r g_r \mid f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, r \in \mathbf{Z}_{\geq 0}\}.$$

delle somme finite di polinomi della forma fg con $f \in I$ e $g \in J$, ed è un semplice esercizio verificare che tale insieme è un ideale. Si noti che l'insieme dei prodotti non sarebbe un ideale perchè non sarebbe chiuso rispetto alla somma.

Proposizione 4.3.2 *Se* $I =< f_1, \ldots, f_r >$ *e* $J =< g_1, \ldots, g_s >$ *sono ideali di* $k[x_1, \ldots, x_n]$ *l'ideale prodotto* $I \cdot J$ *è generato dall'insieme di tutti i prodotti dei generatori di* I *e* J*:*

$$I \cdot J =< f_i g_j : 1 \leq i \leq r,\ 1 \leq j \leq s > .$$

Dimostrazione. È chiaro che l'ideale generato dai prodotti $f_i g_j$ è contenuto nell'ideale $I \cdot J$. Per verificare l'inclusione opposta, osserviamo che ogni polinomio in $I \cdot J$ è somma di polinomi della forma fg con $f \in I$ e $g \in J$. Ricordando che possiamo scrivere f e g in termini di generatori $f_1, \ldots, f_r$ e $g_1, \ldots, g_s$, rispettivamente come:

$$f = a_1 f_1 + \ldots + a_r f_r, \qquad g = b_1 g_1 + \ldots + b_s g_s,$$

con appropriati polinomi $a_i, \ldots a_r$ e $b_1, \ldots, b_s$, si ottiene che $f \cdot g$ e ogni somma di polinomi di questa forma possono essere scritti come $\sum c_{ij} f_i g_j$ con $c_{ij} \in k[x_1, \ldots, x_n]$. ∎

La seguente Proposizione garantisce che il prodotto di ideali corrisponde geometricamente all'operazione di prendere l'unione delle due varietà definite da tali ideali.

Teorema 4.3.2 *Se* I *e* J *sono ideali di* $k[x_1, \ldots, x_n]$*, risulta*

$$\mathcal{V}(I \cdot J) = \mathcal{V}(I) \cup \mathcal{V}(J).$$

Dimostrazione. Sia $x \in \mathcal{V}(I \cdot J)$. Allora $g(x)h(x) = 0$ per ogni $g \in I$ e per ogni $h \in J$. Se $g(x) = 0$ per ogni $g \in I$ allora $x \in \mathcal{V}(I)$. Se, invece, $g(x) \neq 0$ per qualche $g \in I$, si deve avere che $h(x) = 0$ per ogni $h \in J$ e quindi $x \in \mathcal{V}(J)$. In definitiva $x \in \mathcal{V}(I) \cup \mathcal{V}(J)$.

Viceversa, se $x \in \mathcal{V}(I) \cup \mathcal{V}(J)$ risulta o $g(x) = 0$ per ogni $g \in I$ oppure $h(x) = 0$ per ogni $h \in J$. Pertanto $g(x)h(x) = 0$ per ogni $g \in I$ e $h \in J$, il che implica che $f(x) = 0$ per ogni $f \in I \cdot J$ da cui segue che $x \in \mathcal{V}(I \cdot J)$. ∎

4.3.3 Intersezione di ideali.

Definizione 4.3.3 *L'intersezione di due ideali I, J in $k[x_1, \ldots, x_n]$ è l'insieme dei polinomi che appartengono sia a I che a J, ossia l'intersezione insiemistica $I \cap J$.*

Proposizione 4.3.3 *Se I e J sono ideali di $k[x_1, \ldots, x_n]$, allora $I \cap J$ è ancora un ideale.*

Dimostrazione. Si ha $0 \in I \cap J$ perchè $0 \in I$ e $0 \in J$. Se $f, g \in I \cap J$, allora $f + g \in I$ perché $f, g \in I$ e I è un ideale. Analogamente $f + g \in J$ perché $f, g \in J$ e J è un ideale quindi $f + g \in I \cap J$.

Per verificare la chiusura rispetto alla moltiplicazione, consideriamo $f \in I \cap J$ e $h \in k[x_1, \ldots, x_n]$, poiché $f \in I$ ed I è un ideale, si ha che $h \cdot f \in I$ e analogamente per J; quindi $h \cdot f \in I \cap J$. ∎

Si noti che la terza proprietà che caratterizza gli ideali implica che $I \cdot J \subset I \cap J$ ma l'inclusione può essere stretta come mostra il seguente esempio.

Esempio. Consideriamo i seguenti ideali di $k[x, y]$

$$I = J =< x, y > .$$

Il prodotto $I \cdot J$ è uguale a $< x^2, xy, y^2 >$. Si può facilmente constatare che $I \cdot J$ è strettamente contenuto in $I \cap J = I = J =< x, y >$. Infatti $x \in I \cap J$ ma $x \notin I \cdot J$.

Dati due ideali e i corrispettivi insiemi di generatori vogliamo poter calcolare l'insieme dei generatori dell'ideale intersezione. Tale problema è molto più delicato dell'analogo problema per la somma e il prodotto di ideali; per comprendere meglio le difficoltà del problema, consideriamo il seguente esempio.

Esempio. Consideriamo i seguenti ideali di $k[x, y]$

$$I =< f >=< (x + y)^4(x^2 + y)^2(x - 5y) >,$$

$$J =< g >=< (x + y)(x^2 + y)^3(x + 3y) > .$$

È un facile esercizio dimostrare che

$$I \cap J =< (x + y)^4(x^2 + y)^3(x - 5y)(x + 3y) > .$$

La semplicità di questo calcolo deriva dal fatto che f e g sono dati come prodotto di fattori irriducibili. In generale, tale fattorizzazione non è disponibile e qualsiasi algoritmo per determinare i generatori dell'intersezione deve essere sufficientemente potente da aggirare questa difficoltà.

Tuttavia esiste un modo per ridurre il calcolo dell'intersezione al calcolo di un ideale di eliminazione, problema che sappiamo risolvere.

Notazione. *Siano I un ideale di $k[x_1, \ldots, x_n]$ e $f(t) \in k[t]$ un polinomio nell'unica variabile t. Indichiamo con $f(t)I$ l'ideale di $k[x_1, \ldots, x_n, t]$ generato dall'insieme di polinomi $\{f \cdot h \mid h \in I\}$.*

Lemma 4.3.1 *Se $I =< p_1(x), \ldots, p_r(x) >$ è un ideale di $k[x_1, \ldots, x_n]$:*

(i) *$f(t)I$ è un ideale di $k[x_1, \ldots, x_n, t]$, generato da $f(t)p_1(x), \ldots, f(t)p_r(x)$.*

(ii) *Se $g(x,t) \in f(t)I$ e a è un qualsiasi elemento del campo k, allora $g(x,a) \in I$.*

Dimostrazione. Per dimostrare la prima affermazione, notiamo che qualsiasi polinomio $g(x,t) \in f(t)I$ può essere espresso come somma di termini della forma $h(x,t) \cdot f(t) \cdot p(x)$ con $h \in k[x_1, \ldots, x_n, t]$ e $p \in I$. Poiché I è generato da $p_1, \ldots, p_r$, il polinomio $p(x)$ può essere espresso come somma di termini della forma $q_i(x)p_i(x)$, con $1 \leq i \leq r$:

$$\sum_{i=1}^{r} q_i(x)p_i(x).$$

Quindi

$$h(x,t) \cdot f(t) \cdot p(x) = \sum_{i=1}^{r} h(x,t)q_i(x)f(t)p_i(x).$$

Per $1 \leq i \leq r$, $h(x,t) \cdot q_i(x) \in k[x_1, \ldots, x_n, t]$. Pertanto $h(x,t) \cdot f(t) \cdot p(x)$ appartiene all'ideale di $k[x_1, \ldots, x_n, t]$, generato da $f(t)p_1(x), \ldots, f(t)p_r(x)$. Dato che $g(x,t)$ è somma di tali termini

$$g(x,t) \in < f(t)p_1(x), \ldots, f(t)p_r(x) >,$$

il che prova la (i).

La (ii) segue immediatamente sostituendo $a \in k$ a t. ∎

Siamo ora in grado di dimostrare il seguente teorema

Teorema 4.3.3 *Se I e J sono ideali di $k[x_1, \ldots, x_n]$, risulta*

$$I \cap J = [tI + (1-t)J] \cap k[x_1, \ldots, x_n].$$

Dimostrazione. Osserviamo per prima cosa che $[tI + (1-t)J]$ è un ideale di $k[x_1, \ldots, x_n, t]$. Per verificare l'uguaglianza desiderata dimostriamo le due inclusioni opposte.

Se $f \in I \cap J$, allora $f \in I$ e $tf \in tI$. Analogamente, se $f \in J$, allora $(1-t) \cdot f \in (1-t)J$. Poiché f si può scrivere come $f = t \cdot f + (1-t) \cdot f$ si ha che:

$$f = t \cdot f + (1-t) \cdot f \in tI + (1-t)J$$

Poiché I e J sono ideali di $k[x_1, \ldots, x_n]$ allora $f \in [tI+(1-t)J] \cap k[x_1, \ldots, x_n]$, pertanto $I \cap J \subset [tI + (1-t)J] \cap k[x_1, \ldots, x_n]$.

Viceversa, se $f \in [tI + (1-t)J] \cap k[x_1, \ldots, x_n]$, scriviamo f come somma di due polinomi:

$$f(x) = g(x,t) + h(x,t),$$

con $g(x,t) \in tI$ e $h(x,t) \in (1-t)J$. Ponendo $t = 0$, poiché ogni elemento di tI è multiplo di t, si ha $g(x,t) = 0$ e quindi $f(x) = h(x,0)$ e $f(x) \in J$.

Ponendo $t = 1$ si ha che la relazione $f(x) = g(x,t) + h(x,t)$ diventa $f(x) = g(x,1)$ in quanto $h(x,1) = 0$. Ma allora $f(x) \in I$. Ne segue che f appartiene sia ad I che a J, quindi $f \in I \cap J$. Questo dimostra che $I \cap J \supset [tI + (1-t)J] \cap k[x_1, \ldots, x_n]$ da cui la tesi. ∎

Il Teorema 4.3.3 e il Teorema di eliminazione ci permettono di formulare il seguente algoritmo.

Algoritmo per il calcolo dell'intersezione di ideali.

Dati gli ideali $I =< f_1, \ldots, f_r >$ e $J =< g_1, \ldots, g_s >$ in $k[x_1, \ldots, x_n]$, per determinare i generatori dell'ideale intersezione, consideriamo l'ideale:

$$< tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s > \ \leq k[x_1, \ldots, x_n, t]$$

e calcoliamone la base di Groebner rispetto all'ordinamento lessicografico, con t maggiore di ogni x_i.

Gli elementi di questa base che non contengono la variabile t formano una base per $I \cap J$.

Esempio. Siano $I =< x^2y >$ e $J =< xy^2 >$ ideali di $k[x,y]$. Per determinare i generatori di $I \cap J$, consideriamo l'ideale

$$tI + (1-t)J =< tx^2y, (1-t)xy^2 >=< tx^2y, txy^2 - xy^2 >=< f_1, f_2 >$$

di $k[t,x,y]$. Calcolando l'S-polinomio dei generatori si ottiene:

$$S(f_1, f_2) = tx^2y - (tx^2y - x^2y^2) = x^2y^2,$$

da cui è semplice verificare che $\{tx^2y, txy^2 - xy^2, x^2y^2\}$ è una base di Groebner per $tI + (1-t)J$ rispetto all'ordinamento $t > x > y$. Applicando il Teorema di eliminazione si ottiene che $\{x^2y^2\}$ è una base di Groebner per $[tI + (1-t)J] \cap k[x_1, \ldots, x_n]$. Pertanto

$$I \cap J =< x^2y^2 > .$$

Definizione 4.3.4 *Un polinomio $h \in k[x_1, \ldots, x_n]$ si dice* **minimo comune multiplo** *di $f, g \in k[x_1, \ldots, x_n]$, e si indica con $mcm(f,g)$ se è un multiplo comune a f e g che divide ogni loro multiplo comune, ossia:*

(i) f e g dividono h,

(ii) h divide ogni polinomio che f, g dividono.

Osservazione. Se $f, g \in k[x_1, \ldots, x_n]$ e $f = f_1^{a_1}, \ldots, f_r^{a_r}$ e $g = g_1^{a_1}, \ldots, g_s^{a_s}$ sono le rispettive decomposizioni in fattori irriducibili. Può accadere che qualche fattore irriducibile di f sia un multiplo secondo una costante (non nulla) di qualche fattore di g. In tal caso supponiamo di averli riordinati nelle espressioni di f e g in modo che per qualche ℓ $(1 \leq \ell \leq min(r,s))$ f_i sia un multiplo secondo una costante (non nulla) di g_i $(1 \leq i \leq \ell)$, mentre per tutti gli $i, j > \ell$ il polinomio f_i non è mai un multiplo secondo una costante di g_j. Dall'unicità della fattorizzazione segue che

$$mcm(f,g) = f_1^{max(a_1,b_1)} \ldots f_\ell^{max(a_\ell,b_{l\ell})} \cdot g_{\ell+1}^{b_{\ell+1}} \ldots g_s^{b_s} \cdot f_{\ell+1}^{a_{\ell+1}} \ldots f_r^{a_r}. \quad (4.3)$$

Se f e g non hanno fattori comuni, $mcm(f,g) = f \cdot g$. Questo implica la seguente proposizione.

Proposizione 4.3.4 *In $k[x_1, \ldots, x_n]$ si ha*

(i) *L'intersezione di due ideali principali I e J è un ideale principale.*

(ii) *Se $I =< f >$, $J =< g >$ e $h = mcm(f,g)$*

$$I \cap J =< h >=< mcm(f,g) > .$$

Dimostrazione È lasciata come esercizio al lettore. ∎

La Proposizione 4.3.4, insieme all'algoritmo per calcolare l'intersezione di due ideali ci fornisce, immediatamente **l'algoritmo per il calcolo del minimo comune multiplo** di due polinomi. Precisamente, dati i due polinomi $f, g \in k[x_1, \ldots, x_n]$ volendo calcolare il $mcm(f, g)$ applichiamo l'algoritmo sopra illustrato per determinare il generatore dell'ideale intersezione $< f > \cap < g >$, (che è principale per la Proposizione 4.3.4). Tale generatore, per la Proposizione 4.3.4, è proprio il minimo comune multiplo di f e g cercato.

Questo algoritmo ci permette di chiarire un punto, lasciato in sospeso nel Paragrafo 4.2; precisamente, il calcolo del massimo comun divisore di due polinomi. L'osservazione cruciale è la seguente:

Proposizione 4.3.5 *Se $f, g \in k[x_1, \ldots, x_n]$, risulta*

$$mcm(f, g)MCD(f, g) = fg.$$

Dimostrazione. E' un semplice esercizio. Basta considerare le decomposizioni in fattori irriducibili di f e g, e tener conto dell'osservazione che precede la Proposizione 4.3.4 e, in particolare della (4.3). ∎

Dalla Proposizione 4.3.5 segue immediatamente la formula

$$MCD(f, g) = \frac{f \cdot g}{mcm(f, g)}. \tag{4.4}$$

che permette di dare un **Algoritmo per il calcolo del massimo comun divisore** di due polinomi semplicemente utilizzando prima l'algoritmo per il minimo comune multiplo e poi l'algoritmo di divisione. Va messo, comunque, in evidenza che tale algoritmo non è ottimale e che si usano di solito algoritmi più efficienti

Illustriamo ora l'interpretazione geometrica dell'ideale intersezione.

Teorema 4.3.4 *Se I, J sono due ideali di $k[x_1, \ldots, x_n]$, risulta*

$$\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J).$$

Dimostrazione. Se $x \in \mathcal{V}(I) \cup \mathcal{V}(J)$, allora $x \in \mathcal{V}(I)$ o $x \in \mathcal{V}(J)$, quindi o $f(x) = 0$ per ogni $f \in I$ o $f(x) = 0$ per ogni $f \in J$, certamente si ha che $f(x) = 0$ per ogni $f \in I \cap J$, quindi $x \in \mathcal{V}(I \cap J)$ da cui si ottiene che $\mathcal{V}(I) \cup \mathcal{V}(J) \subset \mathcal{V}(I \cap J)$.

Poiché $IJ \subset I \cap J$ e $\mathcal{V}$ inverte le inclusioni risulta $\mathcal{V}(I \cap J) \subset \mathcal{V}(IJ)$. Ma $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$, per il Teorema 4.3.2, quindi si ha anche l'inclusione inversa $\mathcal{V}(I) \cup \mathcal{V}(J) \supset \mathcal{V}(I \cap J)$. ∎

Il Teorema 4.3.4 ci dice che l'intersezione di due ideali corrisponde alla stessa varietà del prodotto di tali ideali. Essendo l'intersezione più difficile da calcolare del prodotto non avrebbe senso occuparsene se non fosse che si comporta meglio del prodotto rispetto all'operazione (unaria) di prendere il radicale. Infatti, mentre il prodotto di due ideali radicali non è necessariamente un ideale radicale (come mostra l'esempio di IJ con $I = J$), l'intersezione di ideali radicali è sempre un ideale radicale, come segue applicando la proposizione seguente ad ideali radicali.

Proposizione 4.3.6 *Se I, J sono due ideali qualsiasi di $k[x_1, \ldots, x_n]$, si ha*

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Dimostrazione. Se $f \in \sqrt{I \cap J}$ allora $f^m \in I \cap J$, per qualche intero $m > 0$. Poiché $f^m \in I$, risulta $f \in \sqrt{I}$. Analogamente dalla $f^m \in J$ si ottiene $f \in \sqrt{J}$. In definitiva: $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$.

Per dimostrare l'inclusione inversa, prendiamo $f \in \sqrt{I} \cap \sqrt{J}$, esistono, per definizione $m, p > 0$, interi positivi, tali che $f^m \in I$ e $f^p \in J$. Allora $f^m f^p = f^{m+p} \in I \cap J$ e quindi $f \in \sqrt{I \cap J}$. ∎

4.4 Chiusura di Zariski

Nei Capitoli precedenti abbiamo considerato diversi insiemi che non sono varietà affini, quali la differenza di due varietà o la proiezione di una varietà su uno spazio di dimensione minore. Se S è un qualunque insieme di k^n, l'insieme:

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

è, comunque, un ideale di $k[x_1, \ldots, x_n]$ (anche quando S non è una varietà) anzi è radicale e, per la corrispondenza tra ideali e varietà si ha che $\mathcal{V}(\mathcal{I}(S))$, è una varietà affine che, ovviamente, contiene S, come si può verificare per esercizio.

La Proposizione seguente dimostra che $\mathcal{V}(\mathcal{I}(S))$ è la più piccola varietà affine che contiene l'insieme S e, pertanto, sarà la **chiusura** rispetto alla topologia **di Zariski** dell'insieme S.

Proposizione 4.4.1 *Se $S \subset k^n$, la varietà affine $\mathcal{V}(\mathcal{I}(S))$ è la più piccola varietà affine che contiene S, nel senso che se $W \subset k^n$ è una varietà che contiene S, allora $\mathcal{V}(\mathcal{I}(S)) \subset W$. Pertanto la chiusura di Zariski, che si indica con $\overline{S}$, di S sarà*

$$\overline{S} = \mathcal{V}(\mathcal{I}(S)).$$

Dimostrazione. Sia W una varietà affine contenente S. Da $W \supset S$ segue che $\mathcal{I}(W) \subset \mathcal{I}(S)$ (poiché $\mathcal{I}$ inverte le inclusioni) e $\mathcal{V}(\mathcal{I}(W)) \supset \mathcal{V}(\mathcal{I}(S))$ (poiché $\mathcal{V}$ inverte le inclusioni). Ma $\mathcal{I}$ è iniettiva e W è una varietà affine, quindi $\mathcal{V}(\mathcal{I}(W)) = W \supset \mathcal{V}(\mathcal{I}(S))$, da cui la tesi. ∎

Un naturale esempio di chiusura di Zariski è fornito dagli ideali di eliminazione. Siamo ora in grado di provare la prima affermazione del *Teorema di Chiusura*, enunciato nel Capitolo 3.

Teorema 4.4.1 (Teorema di chiusura) *Siano k un campo algebricamente chiuso, $V = \mathcal{V}(I)$ la varietà di k^n definita dall'ideale $I =< (f_1, \ldots, f_s) >$ di $k[x_1, \ldots, x_n]$ e $\pi_h : k^n \longrightarrow k^{n-h}$ la proiezione sullo spazio delle ultime $n - h$ coordinate. Se $I_h = I \cap k[x_{h+1}, \ldots, x_n]$ è l'h-esimo ideale di eliminazione, risulta*

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

ossia $\mathcal{V}(I_h)$ è la chiusura di Zariski di $\pi_h(V)$.

Dimostrazione. Stante la Proposizione 4.4.1 dobbiamo dimostrare che $\mathcal{V}(I_h) = \mathcal{V}(\mathcal{I}(\pi_h(V)))$. Sappiamo dal Lemma 3.2.1 che $\pi_h(V) \subseteq \mathcal{V}(I_h)$ e quindi è ovvio che $\mathcal{V}(I_h)$ contenga la chiusura di Zariski di $\pi_h(V)$ che è $\mathcal{V}(\mathcal{I}(\pi_h(V)))$.

Viceversa si deve far vedere che ogni punto di $\mathcal{V}(I_h)$ sta in tale chiusura di Zariski. Se supponiamo di aver già dimostrato che

$$\mathcal{I}(\pi_h(V)) \subset \sqrt{I_h},$$

si avrà

$$\mathcal{V}(\mathcal{I}(\pi_h(V)) \supset \mathcal{V}(\sqrt{I_h}) = \mathcal{V}(I_h)$$

da cui la tesi. Resta quindi da dimostrare che $\mathcal{I}(\pi_h(V)) \subset \sqrt{I_h}$. A tale scopo consideriamo $f \in \mathcal{I}(\pi_h(V))$ cioè $f(a_{h+1}, \ldots, a_n) = 0$ per ogni $(a_{h+1}, \ldots, a_n) \in \pi_h(V)$. Considerando f come elemento di $k[x_1, \ldots, x_n]$, abbiamo sicuramente che $f(a_1, \ldots, a_n) = 0$ per ogni $(a_1, \ldots, a_n) \in V$, ossia

$f \in \mathcal{I}(\mathcal{V}(I))$. Per il *Nullstellensatz di Hilbert*, allora $f \in \sqrt{I}$ e pertanto $f^N \in I$ per qualche intero N. Ma f non dipende da $x_1, \ldots, x_h$, quindi anche f^N non dipende da $x_1, \ldots, x_h$, ossia $f^N \in I \cap k[x_{h+1}, \ldots, x_n] = I_h$. Questo implica che $f \in \sqrt{I_h}$ e quindi $\mathcal{I}(\pi_h(V)) \subset \sqrt{I}_h$, come volevasi dimostrare. ∎

Un altro contesto in cui abbiamo incontrato insiemi che non sono varietà affini è quando abbiamo considerato la differenza di due varietà. Ad esempio in $\mathbf{R}^3$ sia $W = \mathcal{V}(z) \cup \mathcal{V}(x, y) = \mathcal{V}(zx, zy)$ la varietà unione del piano xy (ossia $V = \mathcal{V}(z)$) e dell'asse z (ossia $\mathcal{V}(x, y)$. La differenza $W - V$ è l'asse z privato dell'origine, e, come retta bucata in uno spazio sopra un campo infinito (in cui vale il principio di identità dei polinomi), non è una varietà affine. In questo caso l'asse z è la più piccola varietà che contiene $W - V$.

Ci si potrebbe chiedere, se esista un modo per calcolare l'ideale corrispondente alla chiusura di Zariski $\overline{W - V}$ della differenza di due varietà W e V. La risposta è affermativa, ma necessita di altre costruzioni algebriche sugli ideali. Per illustrare ciò cominciamo dimostrando la seguente Proposizione.

Proposizione 4.4.2 *Se V e W sono due varietà tali che $V \subset W$, allora*

$$W = V \cup (\overline{W - V}).$$

Dimostrazione. Poiché W contiene $W - V$ e W è una varietà si ha che W deve contenere la più piccola varietà che contiene $W - V$. Quindi $\overline{W - V} \subset W$, ma per ipotesi $V \subset W$, sarà pertanto $V \cup (\overline{W - V}) \subset W$.

Per dimostrare l'inclusione inversa, consideriamo $x \in W$. Possiamo distinguere due casi: o $x \in V$ o $x \in W - V$. Se $x \in V$, certamente $x \in V \cup (\overline{W - V})$. Se $x \in W - V$, allora $x \in \overline{W - V}$, che è un insieme più grande, perciò $x \in V \cup (\overline{W - V})$. Per l'arbitrarietà con cui è stato scelto x in W si può concludere che $W \subset V \cup (\overline{W - V})$. ∎

Definizione 4.4.1 *Se I, J sono ideali di $k[x_1, \ldots, x_n]$ si dice* **ideale quoziente** *di I e J, e si indica $I : J$ l'insieme*

$$I : J = \{f \in k[x_1, \ldots, x_n] \mid fg \in I \ \ \forall\ g \in J\}.$$

Esempio. In $k[x, y, z]$ si ha

$$\begin{aligned} < xz, yz > : < z > &= \{f \in k[x, y, z] \mid z \cdot f \in < xz, yz >\} \\ &= \{f \in k[x, y, z] \mid z \cdot f = Axz + Byz\} \\ &= \{f \in k[x, y, z] \mid f = Ax + By\} \\ &= < x, y > . \end{aligned}$$

Proposizione 4.4.3 *Se I, J sono ideali di $k[x_1, \ldots, x_n]$, allora $I : J$ è un ideale di $k[x_1, \ldots, x_n]$ e $I : J$ contiene I.*

Dimostrazione. Per dimostrare che $I : J$ contiene I è sufficiente osservare che se $f \in I$, per definizione di ideale, $fg \in I$ per ogni $g \in k[x_1, \ldots, x_n]$, quindi $fg \in I$ anche per ogni $g \in J \subset k[x_1, \ldots, x_n]$.

Per verificare che $I : J$ è un ideale si devono verificare le proprietà che caratterizzano gli ideali. Ovviamente $0 \in I : J$ in quanto $0 \in I$. Se $f_1, f_2 \in I : J$, allora $f_1 g$ e $f_2 g$ sono in I per ogni $g \in J$. Essendo I un ideale $(f_1 + f_2)g = f_1 g + f_2 g \in I$ per ogni $g \in J$, e pertanto $f_1 + f_2 \in I : J$. Se $f \in I : J$ e $h \in k[x_1, \ldots, x_n]$, per ogni $g \in J$ si ha $fg \in I$ e quindi, essendo I un ideale, $hfg \in I$ e ciò significa che $hf \in I : J$. ∎

Il seguente teorema evidenzia che l'ideale quoziente è l'analogo algebrico della chiusura di Zariski della differenza di due varietà.

Teorema 4.4.2 *(i) Se I e J sono ideali di $k[x_1, \ldots, x_n]$, si ha*

$$\mathcal{V}(I : J) \supset \overline{\mathcal{V}(I) - \mathcal{V}(J)}$$

(ii) Se, inoltre, k è un campo algebricamente chiuso ed I è un ideale radicale, allora

$$\mathcal{V}(I : J) = \overline{\mathcal{V}(I) - \mathcal{V}(J)}.$$

Dimostrazione. (i) Per definizione $\overline{\mathcal{V}(I) - \mathcal{V}(J)} = \mathcal{V}[\mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J))]$; poiché $\mathcal{V}$ inverte le inclusioni, basterà dimostrare che

$$I : J \subset \mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J)).$$

Se $f \in I : J$ si ha che $fg \in I$ per ogni $g \in J$ quindi se $x \in \mathcal{V}(I) - \mathcal{V}(J)$ risulta $fg(x) = f(x)g(x) = 0$ per ogni $x \in \mathcal{V}(I)$ e ogni $g \in J$. Ma $x \notin \mathcal{V}(J)$ implica che esiste una $\overline{g} \in J$ tale che $\overline{g}(x) \neq 0$. Per tale $\overline{g}$ si ha $(f\overline{g})(x) = f(x)\overline{g}(x) = 0$ e $\overline{g}(x) \neq 0$. Ne segue che $f(x) = 0$ per ogni $x \in \mathcal{V}(I) - \mathcal{V}(J)$ e quindi $f \in \mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J))$

(ii) Se k è un campo algebricamente chiuso e $I = \sqrt{I}$ dimostriamo che vale anche l'inclusione inversa

$$\mathcal{V}(I : J) \subset \overline{\mathcal{V}(I) - \mathcal{V}(J)} = \mathcal{V}[\mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J))].$$

Poiché $\mathcal{V}$ inverte le inclusioni, basterà far vedere che

$$I : J \supset \mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J)),$$

ossia che se $h \in \mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J))$ (ossia $h(x) = 0$ per ogni $x \in \mathcal{V}(I) - \mathcal{V}(J)$) allora $h \in I : J$ ossia che, per ogni $g \in J$, $hg \in I$. Ma, per ipotesi $I = \sqrt{I}$ e per il Nullstellensatz, che vale essendo k algebricamente chiuso, $I = \sqrt{I} = \mathcal{I}(\mathcal{V}(I))$. In definitiva basterà far vedere che hg si annulla su ogni punto x di $\mathcal{V}(I)$. Ma questo immediato in quanto $(hg)(x) = h(x)g(x)$ e $h \in \mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J))$ si annulla su $\mathcal{V}(I) - \mathcal{V}(J)$ mentre $g \in \mathcal{I}(\mathcal{V}(J)$ si annulla su $\mathcal{V}(J)$. ∎

Corollario 4.4.1 *Sia k un campo qualsiasi. Se V e W sono due varietà affini di k^n risulta*

$$\mathcal{I}(V) : \mathcal{I}(W) = \mathcal{I}(V - W).$$

Dimostrazione. Nella parte (i) della dimostrazione del Teorema 4.4.2, abbiamo visto che $I : J \subset \mathcal{I}(\mathcal{V}(I) - \mathcal{V}(J))$ (qualunque sia il campo k). Applicando tale relazione a $I = \mathcal{I}(V)$ e $J = \mathcal{I}(W)$ si ottiene $\mathcal{I}(V) : \mathcal{I}(W) \subset \mathcal{I}(V - W)$.

L'inclusione inversa $\mathcal{I}(V) : \mathcal{I}(W) \supset \mathcal{I}(V - W)$ segue immediatamente dalla definizione di ideale quoziente. ∎

La proposizione seguente illustra alcune proprietà dell'ideale quoziente e mette in relazione l'operazione di quoziente con le altre operazioni definite per gli ideali; naturalmente, tutte le affermazioni fatte in termini di ideali possono essere trasformate in termini di varietà, il che è lasciato per esercizio al lettore.

Proposizione 4.4.4 *Siano I, J e K ideali di $k[x_1, \ldots, x_n]$. Allora*

$$\begin{aligned} &(i) \quad I : k[x_1, \ldots, x_n] = I, \\ &(ii) \quad IJ \subset K \Longleftrightarrow I \subset K : J, \\ &(iii) \quad J \subset I \Longleftrightarrow I : J = k[x_1, \ldots, x_n]. \end{aligned}$$

Se I, I_i, J, J_i e K sono ideali di $k[x_1, \ldots, x_n]$ con $1 \leq i \leq r$, risulta:

$$\begin{aligned} &(iv) \quad (\bigcap_{i=1}^{r} I_i) : J = \bigcap_{i=1}^{r} (I_i : J), \\ &(v) \quad I : (\sum_{i=1}^{r} J_i) = \bigcap_{i=1}^{r} (I : J_i), \\ &(vi) \quad (I : J) : K = I : JK. \end{aligned}$$

Dimostrazione. È lasciata per esercizio al lettore. ∎

Se f è un polinomio ed I è un ideale scriveremo brevemente $I : f$ per $I :< f >$. Un caso particolare della proprietà (v) nella Proposizione 4.4.4 è

$$I :< f_1, \ldots, f_r >= \bigcap_{i=1}^{r} (I : f_i) \tag{4.5}$$

Esaminiamo ora il problema di determinare i generatori dell'ideale quoziente $I : J$ assegnati i generatori di due ideali I e J.

Teorema 4.4.3 *Considerati in $k[x_1, \ldots, x_n]$ un ideale I e un polinomio g, se $\{h_1, \ldots, h_p\}$ è una base per l'ideale $I \cap < g >$, allora una base per l'ideale quoziente $I :< g >$ è data da $\{h_1/g, \ldots, h_p/g\}$.*

Dimostrazione. Mostriamo dapprima che $< h_1/g, \ldots, h_p/g > \subseteq I :< g >$. Se $a \in< g >$, allora $a = bg$ per qualche polinomio b. Ora, se $f \in< h_1/g, \ldots, h_p/g >$ si ha

$$af = bgf \in< h_1, \ldots, h_p >= I \cap < g > \subset I,$$

quindi $f \in I :< g >$.

Per l'inclusione inversa, supponiamo che $f \in I : < g >$, cosicché $fg \in I$, e dato che $fg \in< g >$ si ha $fg \in I \cap < g >$. Ma $I \cap < g >=< h_1, \ldots, h_p >$, quindi $fg = \sum r_i h_i$ per opportuni polinomi r_i. Poiché ogni $h_i \in< g >$ ciascun h_i/g è un polinomio e possiamo scrivere $f = \sum r_i (h_i/g)$, il che prova appunto che $f \in< h_1/g, \ldots, h_p/g >$. ∎

Questo Teorema insieme al procedimento che ci permette il calcolo dell'intersezione di ideali e all'equazione (4.5) ci fornisce immediatamente un **algoritmo per determinare una base di un ideale quoziente**. Precisamente, assegnati i due ideali

$$I =< f_1, \ldots, f_r >,$$

e

$$J =< g_1, \ldots, g_s >=< g_1 > + < g_2 > + \ldots, + < g_s >,$$

per calcolare una base di $I : J$ si calcola, in primo luogo, una base per $I :< g_i >$ per ogni i, al modo seguente. Si determina, una base di Groebner di $< tf_1, \ldots, tf_r, (1-t)g_i >$, rispetto all'ordinamento lessicografico secondo cui t precede tutte le variabili x_i e si escludono da tale base tutti gli elementi

che dipendono da t. Usando, poi, l'*algoritmo di divisione*, si divide ogni elemento di tale base per g_i e si ottiene una base per $I :< g_i >$.

Una base di $I : J$ si calcola poi applicando *l'algoritmo di intersezione*, $s-1$ volte, ossia determinando prima una base per

$$I :< g_1, g_2 >= (I :< g_1 >) \cap (I :< g_2 >),$$

poi un base per

$$I :< g_1, g_2, g_3 >= (I :< g_1, g_2 >) \cap (I :< g_3 >),$$

e così via, fino ad ottenere

$$I :< g_1, \ldots, g_s >= (I :< g_1, \ldots, g_{s-1} >) \cap (I :< g_s >).$$

4.5 Varietà irriducibili e ideali primi

Abbiamo visto che l'unione di due varietà è ancora una varietà. In esempi già mostrati, avevamo osservato che $\mathcal{V}(xz, yz)$ era unione di due varietà e precisamente dell'asse z con il piano xy. Intuitivamente, è naturale pensare che il piano e la retta sono "entità più fondamentali" di $\mathcal{V}(xz, yz)$. Basandoci su una pura intuizione possiamo affermare che il piano e la retta sono **irriducibili** nel senso di indecomponibili, ma in generale il tutto non è così ovvio. Per formalizzare meglio tali nozioni cominciamo con le seguenti definizioni.

Definizione 4.5.1 *Una varietà affine $V \subset k^n$ è* **irriducibile** *se dall'essere $V = V_1 \cup V_2$, dove V_1, V_2 sono varietà affini, segue che o $V = V_1$ oppure $V = V_2$.*

Come abbiamo visto $\mathcal{V}(xz, yz)$ non è una varietà irriducibile, ma come stabilire quando una varietà è irriducibile? Se a questa definizione si fa corrispondere l'interpretazione geometrica intuitiva, è chiaro che i punti, le rette e i piani devono essere irriducibili. Ma come dimostrarlo?

La chiave giusta è interpretare tale definizione algebricamente, o meglio caratterizzare gli ideali che definiscono queste particolari varietà: in tal caso, forse, avremo un modo per stabilire quando queste varietà sono irriducibili.

Definizione 4.5.2 *Un ideale I di $k[x_1, \ldots, x_n]$ è un* **ideale primo** *se dall'essere $f, g \in k[x_1, \ldots, x_n]$ e $fg \in I$ segue che o $f \in I$ o $g \in I$.*

La Proposizione seguente evidenzia il legame esistente tra varietà irriducibili ed ideali primi.

Proposizione 4.5.1 *Una varietà affine $V \subset k^n$ è irriducibile se e soltanto se $\mathcal{I}(V)$ è un ideale primo.*

Dimostrazione. Partiamo dall'ipotesi che V sia irriducibile e consideriamo $fg \in \mathcal{I}(V)$. Gli insiemi $V_1 = V \cap \mathcal{V}(f)$ e $V_2 = V \cap \mathcal{V}(g)$ sono due varietà affini in quanto intersezione di due varietà affini. L'essere $fg \in \mathcal{I}(V)$ implica che $\mathcal{V}(fg) \supset V$. Ne segue che $V = V_1 \cup V_2$, infatti

$$V_1 \cup V_2 = (V \cap \mathcal{V}(f)) \cup (V \cap \mathcal{V}(g)) = V \cap [\mathcal{V}(f) \cup \mathcal{V}(g)] = V \cap \mathcal{V}(fg) = V,$$

poiché $\mathcal{V}(fg) \supset V$. Ma V è irriducibile e pertanto o $V = V_1$ o $V = V_2$. Se risulta $V = V_1$ si ha che f svanisce su V, quindi $f \in \mathcal{I}(V)$; analogamente, se $V = V_2$ risulta $g \in \mathcal{I}(V)$. Ne segue che $\mathcal{I}(V)$ è primo.

Assumiamo ora che $\mathcal{I}(V)$ sia primo e $V = V_1 \cup V_2$ con $V \neq V_1$; ciò che vogliamo dimostrare è che $\mathcal{I}(V) = \mathcal{I}(V_2)$, da cui, applicando $\mathcal{V}$, essendo $\mathcal{I}$ sempre iniettiva, seguirà la tesi $V = V_2$. Per provare che $\mathcal{I}(V) = \mathcal{I}(V_2)$, osserviamo che $\mathcal{I}(V) \subset \mathcal{I}(V_2)$ poiché $V_2 \subset V$. Per l'inclusione inversa si ha che, essendo $V \neq V_1$, $\mathcal{I}(V)$ è contenuto propriamente in $\mathcal{I}(V_1)$. Allora possiamo prendere $f \in \mathcal{I}(V_1) - \mathcal{I}(V)$ e un qualsiasi $g \in \mathcal{I}(V_2)$; poiché $V = V_1 \cup V_2$ il prodotto fg svanisce sulla varietà V, ossia $fg \in \mathcal{I}(V)$. Ma per ipotesi $\mathcal{I}(V)$ è un ideale primo e poichè $f \notin \mathcal{I}(V)$ necessariamente $g \in \mathcal{I}(V)$, da cui per l'arbitrarietà di g si ha l'inclusione voluta e $\mathcal{I}(V) = \mathcal{I}(V_2)$. Da questa inclusione, come già osservato, applicando $\mathcal{V}$ e per l'iniettività di $\mathcal{I}$ segue $V = V_2$ e quindi che V è una varietà irriducibile. ∎

Corollario 4.5.1 *Se k è un campo algebricamente chiuso le funzioni $\mathcal{I}$ e $\mathcal{V}$ inducono una corrispondenza biunivoca tra varietà irriducibili di k^n ed ideali primi di $k[x_1, \ldots, x_n]$.*

Dimostrazione. Non è difficile dimostrare che *ogni ideale primo I è radicale*: basta far vedere che, se I è primo allora

$$I \supseteq \{f \in k[x_1, \ldots, x_n \mid f^m \in I, m \geq 1\} = \sqrt{I}.$$

A tale scopo, fissiamo arbitrariamente una $f \in \sqrt{I}$. Esiste un $m \geq 1$ tale che $f^m \in I$, quindi l'insieme di interi non negativi $S = \{m \mid f^m \in I\}$ è non vuoto. Sia m_0 il minimo di $S = \{m \mid f^m \in I\} \neq \emptyset$. Ovviamente $f^{m_0} = f \cdot f^{m_0 - 1} \in I$ ideale primo implica che o f o f^{m_0-1} sono in I; ma f^{m_0-1} non può appartenere ad I, essendo m_0 il minimo di S e quindi $f \in I$. Possiamo ora, per la seconda parte del teorema di corrispondenza, affermare che la corrispondenza tra ideali primi e varietà irriducibili è biunivoca. ∎

Esempio. Per vedere come utilizzare la Proposizione 4.5.1 appena dimostrata consideriamo l'ideale $\mathcal{I}(V)$ associato alla cubica sghemba. Il nostro obiettivo è quello di verificare che $\mathcal{I}(V)$ è primo. Se $fg \in \mathcal{I}(V)$; poiché la curva è parametrizzata da (t, t^2, t^3), risulta per ogni t

$$f(t, t^2, t^3)g(t, t^2, t^3) = 0;$$

ciò implica che $f(t, t^2, t^3)$ o $g(t, t^2, t^3)$ deve essere il polinomio nullo, e così o f o g svaniscono su V, ossia o f o g appartengono all'ideale $\mathcal{I}(V)$ il che prova che $\mathcal{I}(V)$ è primo. Per la Proposizione 4.5.1 la cubica sghemba è pertanto una varietà irriducibile in $\mathbf{R}^3$. Questo esempio ci fornisce il modo con cui verificare che la retta è una varietà irriducibile, infatti si considera prima la parametrizzazione e poi con gli stessi argomenti si giunge all'irriducibilità.

Proposizione 4.5.2 *Se k è un campo infinito e $V \subset k^n$ una varietà che ammette la parametrizzazione polinomiale*

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

con $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$, allora V è irriducibile.

Dimostrazione. Consideriamo l'applicazione $F : k^m \longrightarrow k^n$ definita dalla

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

La varietà V è la chiusura di Zariski di $F(k^m)$. In particolare, $\mathcal{I}(V) = \mathcal{I}(F(k^m)$. Per ogni polinomio $g \in k[x_1, \ldots, x_n]$ la funzione $g \circ F$ è un polinomio in $k[t_1, \ldots, t_m]$, infatti $g \circ F$ è il polinomio ottenuto componendo g con le $f_1, \ldots, f_m$

$$g \circ F = g(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Essendo k un campo infinito, $\mathcal{I}(V) = \mathcal{I}(F(k^m))$ è l'insieme di tutti i polinomi di $k[x_1, \ldots, x_n]$ i quali composti con F sono il polinomio nullo in $k[t_1, \ldots, t_m]$:

$$\mathcal{I}(V) = \{g \in k[x_1, \ldots, x_n] \mid g \circ F = 0\}.$$

Ora supponiamo che $gh \in \mathcal{I}(V)$, risulta $(gh) \circ F = (g \circ F)(h \circ F) = 0$. Se il prodotto di due polinomi in $k[t_1, \ldots, t_m]$ è il polinomio nullo allora uno dei due fattori deve essere nullo. Si ha così che o $(g \circ F) = 0$ o $(h \circ F) = 0$. Questo significa che o $g \in \mathcal{I}(V)$ o $h \in \mathcal{I}(V)$, ciò prova che $\mathcal{I}(V)$ è un ideale primo e quindi per la Proposizione 4.5.1 che $V = \overline{F(k^m)}$ è una varietà irriducibile. ∎

Con un minimo di attenzione possiamo estendere il risultato appena dimostrato anche al caso di varietà definite tramite una parametrizzazione razionale.

Proposizione 4.5.3 *Se k è un campo infinito e $V \subset k^n$ è una varietà definita dalla parametrizzazione razionale*

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

ove $f_1, \ldots, f_m, g_1, \ldots, g_m \in k[t_1, \ldots t_m]$, $\prod_{i=1}^n g_i \neq 0$, allora V è irriducibile.

Dimostrazione. Sia $W = \mathcal{V}(\prod_{i=1}^{n} g_i)$. Consideriamo l'applicazione

$$F : (k^m - W) \longrightarrow k^n$$

definita dalla:

$$F(t_1, \ldots, t_m) = (\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}).$$

V è la chiusura di Zariski di $F(k^m - W)$, ciò implica che $\mathcal{I}(V)$ è l'insieme degli $h \in k[x_1, \ldots, x_n]$ per i quali la funzione $h \circ F$ è nulla su tutti i punti $(t_1, \ldots, t_m) \in k^m - W$. La difficoltà principale risiede nel fatto che la funzione $h \circ F$ non è necessariamente un polinomio e per questo non possiamo applicare gli stessi ragionamenti utilizzati prima. Possiamo però aggirare tale difficoltà nel modo seguente.

Sia $h \in k[x_1, \ldots, x_n]$ poiché

$$g_1(t_1, \ldots, t_m) g_2(t_1, \ldots, t_m) \ldots g_n(t_1, \ldots, t_m) \neq 0$$

per ogni $(t_1, \ldots, t_m) \in k^m - W$, la funzione $(g_1 g_2 \ldots g_n)^N (h \circ F)$, è uguale a zero negli stessi punti in cui $h \circ F$ è nulla. Inoltre, se N è il grado totale di $h \in k[x_1, \ldots, x_n]$ allora $(g_1 g_2 \ldots g_n)^N (h \circ F)$ è un polinomio di $k[t_1, \ldots t_m]$, come si può dimostrare per esercizio. Ne deduciamo che $h \in \mathcal{I}(V)$ se e soltanto se $(g_1 g_2 \ldots g_n)^N (h \circ F)$ è zero per ogni $t \in k^m - W$, ma ciò si verifica se e soltanto se $(g_1 g_2 \ldots g_n)^N (h \circ F)$ è il polinomio nullo in $k[t_1, \ldots t_m]$. Per riassumere abbiamo dimostrato che

$$h \in \mathcal{I}(V) \ \textit{ se e soltanto se } \ (g_1 g_2 \ldots g_n)^N (h \circ F) = 0 \in k[t_1, \ldots t_m].$$

Ora possiamo continuare a dimostrare che $\mathcal{I}(V)$ è primo.

Supponiamo che $p, q \in k[x_1, \ldots, x_n]$, siano polinomi tali che $p \cdot q \in \mathcal{I}(V)$. Se i gradi totali di p e q sono rispettivamente M e N, allora il grado totale di $p \cdot q$ è $M + N$. Quindi $(g_1 g_2 \ldots g_n)^{M+N} (p \circ F) \cdot (q \circ F) = 0$, ma questo è precisamente il prodotto dei seguenti polinomi $(g_1 g_2 \ldots g_n)^M (p \circ F)$ e $(g_1 g_2 \ldots g_n)^N (q \circ F)$ in $k[t_1, \ldots t_m]$. Necessariamente uno dei due deve essere il polinomio nullo, in particolare o $p \in \mathcal{I}(V)$ o $q \in \mathcal{I}(V)$. Ciò mostra che $\mathcal{I}(V)$ è un ideale primo e, pertanto, la varietà V è irriducibile. ∎

Un'altra categoria di ideali che vogliamo mettere in evidenza ora, è quella degli ideali **massimali**.

Definizione 4.5.3 *Un ideale $I \subset k[x_1, \ldots, x_n]$ si dice* **massimale** *se $I \neq k[x_1, \ldots, x_n]$ e ogni altro ideale J che contiene I è tale che o $I = J$ o $J = k[x_1, \ldots, x_n]$.*

Definizione 4.5.4 *Un ideale $I \subset k[x_1, \ldots, x_n]$ si dice* **proprio** *se I non è uguale a $k[x_1, \ldots, x_n]$.*

Un ideale massimale è quindi un ideale proprio che non è contenuto in nessun altro ideale proprio.

Proposizione 4.5.4 *Se k è un campo, un ideale I di $k[x_1, \ldots, x_n]$ della forma*

$$I =< x_1 - a_1, \ldots, x_n - a_n >,$$

con $a_1, \ldots, a_n \in k$, è un ideale massimale.

Dimostrazione. Supponiamo che J sia un ideale che contenga strettamente l'ideale I, esiste quindi un polinomio $f \in J$ ma $f \notin I$. Usando l'algoritmo di divisione possiamo scrivere f come combinazione lineare di elementi della base di I, ossia

$$f = A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) + b$$

dove $b \in k$. Poiché $A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) \in I$ e $f \notin I$, deve essere $b \neq 0$. Tuttavia $f \in J$ e dato che $A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) \in I \subset J$, si ha anche

$$b = f - [A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n)] \in J.$$

Ma $b \neq 0$, per cui $1 = 1/b \cdot b \in J$ così $J = k[x_1, \ldots, x_n]$. ∎

Essendo

$$\mathcal{V}(x_1 - a_1, \ldots, x_n - a_n) = \{a = (a_1, \ldots a_n) \in k^n\},$$

ad ogni punto $a \in k^n$ corrisponde un ideale massimale di $k[x_1, \ldots, x_n]$.

Il viceversa non è vero se il campo non è algebricamente chiuso.

Proposizione 4.5.5 *Sia k un campo, un ideale massimale di $k[x_1, \ldots, x_n]$ è un ideale primo.*

Dimostrazione. Per assurdo, supponiamo che I sia un ideale proprio, ma non primo e sia $fg \in I$ con $f \notin I$ e $g \notin I$. Consideriamo, l'ideale $< f > +I$. Tale ideale contiene strettamente I perché $f \notin I$. Se fosse $< f > +I = k[x_1, \ldots, x_n]$, allora $1 = cf + h$ per qualche polinomio c e qualche $h \in I$. Moltiplicando amboi i membri per g si ottiene $g = gcf + gh \in I$ il che contraddice la nostra scelta di g. Quindi $I+ < f >$ è un ideale proprio che contiene strettamente I e I non è massimale il che è assurdo. ∎

Le proposizioni 4.5.4 e la 4.5.5 implicano che $< x_1 - a_1, \ldots, x_n - a_n >$ è un ideale primo in $k[x_1, \ldots, x_n]$ anche se k non è infinito. In un campo algebricamente chiuso si ha che ogni ideale massimale corrisponde ad un punto di k^n.

Teorema 4.5.1 *Se k è un campo algebricamente chiuso, allora ogni ideale massimale di $k[x_1, \ldots, x_n]$ ha la forma*

$$< x_1 - a_1, \ldots, x_n - a_n >$$

per qualche $a_1, \ldots, a_n \in k$.

Dimostrazione. Sia $I \subset k[x_1, \ldots, x_n]$ un ideale massimale. I è un ideale proprio di $k[x_1, \ldots, x_n]$ per questo possiamo affermare che la varietà $\mathcal{V}(I) \neq \emptyset$. Per il *Nullstellensatz versione debole*, esiste almeno un punto $(a_1, \ldots, a_n) \in \mathcal{V}(I)$. Passando agli ideali abbiamo

$$\mathcal{I}(\mathcal{V}(I)) \subset \mathcal{I}(\{(a_1, \ldots, a_n)).$$

Ma $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, per il *Nullstellensatz forte*. Ora I è massimale per ipotesi, quindi primo per la Proposizione 4.5.5, ma abbiamo provato nella dimostrazione del Corollario 4.5.1 che ogni ideale primo è radicale, dunque $I = \sqrt{I} = \mathcal{I}(\mathcal{V}(I))$. Possiamo, pertanto, scrivere

$$I \subset \mathcal{I}(\{(a_1, \ldots, a_n)\}).$$

Abbiamo già osservato che $\mathcal{I}(\{(a_1, \ldots, a_n)\}) =< x_1 - a_1, \ldots, x_n - a_n >$, per questo l'inclusione sopra diventa

$$I \subset < x_1 - a_1, \ldots, x_n - a_n > \subset k[x_1, \ldots, x_n]$$

Ma I è massimale e $< x_1 - a_1, \ldots, x_n - a_n > \neq k[x_1, \ldots, x_n]$; pertanto, si ha che $I =< x_1 - a_1, \ldots, x_n - a_n >$. ∎

Corollario 4.5.2 *Se k è un campo algebricamente chiuso, allora esiste una corrispondenza biunivoca tra i punti di k^n e gli ideali massimali di $k[x_1, \ldots, x_n]$.*

Abbiamo così esteso il nostro dizionario algebra-geometria, infatti abbiamo dimostrato che in un campo algebricamente chiuso ogni varietà non vuota e irriducibile corrisponde ad un ideale primo e viceversa, e che ogni punto corrisponde ad un ideale massimale e viceversa.

4.6 Decomposizione di una varietà

Nel paragrafo precedente abbiamo visto diversi esempi di varietà irriducibili. E' spontaneo chiedersi se assegnata una varietà non irriducibile sia possibile decomporla in sottovarietà irriducibili. In questo paragrafo studieremo questo problema e varie questioni connesse. Iniziamo traducendo la Condizione della Catena Ascendente (CCA) per gli ideali nel linguaggio delle varietà.

Proposizione 4.6.1 (Condizione della Catena Discendente) *Ogni catena discendente di varietà*

$$V_1 \supset V_2 \supset V_3 \cdots\cdots$$

in k^n si stabilizza. Ossia esiste un intero N tale che $V_N = V_{N+i}$, per ogni $i \geq 1$.

Dimostrazione. Poiché $\mathcal{I}$ inverte le inclusioni, da una catena discendente di varietà, passando agli ideali associati, si ottiene la catena ascendente

$$\mathcal{I}(V_1) \subset \mathcal{I}(V_2) \subset \mathcal{I}(V_3) \cdots\cdots$$

che, essendo $k[x_1, \ldots, x_n]$ noetheriano, si stabilizza (cfr. il paragrafo 5 del Capitolo 2). Esiste quindi un N tale che $\mathcal{I}(V_N) = \mathcal{I}(V_{N+i})$, per ogni $i \geq 1$. Poiché $\mathcal{V}(\mathcal{I}(V)) = V$ per ogni varietà V, essendo $\mathcal{I}$ sempre iniettiva, si ha $V_N = V_{N+i}$, per ogni $i \geq 1$. ∎

La Proposizione 4.6.1 si può usare per dimostrare il seguente risultato sulla struttura delle varietà affini.

Teorema 4.6.1 *Ogni una varietà affine V di k^n può essere scritta come unione finita*

$$V = V_1 \cup V_2 \cup \ldots \cup V_n.$$

di varietà irriducibili.

Dimostrazione. Sia V sia una varietà affine che non può essere scritta come unione finita di varietà irriducibili. Allora V non è irriducibile, e quindi $V = V_1 \cup V_1'$ con $V \neq V_1$ e $V \neq V_1'$. Osserviamo che una almeno tra V_1 e V_1', non può essere unione finita di varietà irriducibili, altrimenti V sarebbe, contrariamente a quanto supposto, una tale unione di irriducibili.

Sia, ad esempio, V_1 la varietà che non è unione di varietà irriducibili. Ripetendo per V_1 il ragionamento sopra fatto per V, possiamo scrivere $V_1 = V_2 \cup V_2'$, dove $V_1 \neq V_2$ e $V_1 \neq V_2'$ e V_2 non è unione di varietà irriducibili.

Continuando in questo modo si ottiene una successione infinita di varietà affini

$$V \supset V_1 \supset V_2 \supset \cdots$$

con

$$V \neq V_1 \neq V_2 \cdots$$

il che è assurdo, in quanto vale la Condizione della Catena Discendente (CCD) per le varietà affini (cfr. la Proposizione 4.6.1). ∎

Esempio. Consideriamo la varietà $V = \mathcal{V}(xz - y^2, x^3 - yz)$ e cerchiamo di scriverla come unione di varietà irriducibili.

Sicuramente V contiene $\mathcal{V}(x, y)$ ossia l'asse z in quanto entrambi i polinomi $xz - y^2$ e $x^3 - yz$ svaniscono sull'asse z. L'asse z è dunque una varietà irriducibile contenuta nella nostra V. La parte mancante sarà la chiusura di Zariski di $V - \mathcal{V}(x, y)$. Cerchiamo di comprendere meglio come è fatta tale chiusura. Il teorema 4.4.2 suggerisce di considerare l'ideale quoziente

$$< xz - y^2, x^3 - yz >:< x, y >:= I :< x, y > .$$

Per calcolarlo possiamo usare l'algoritmo per determinare una base di un ideale quoziente. Per le proprietà dell'ideale quoziente si ha

$$I :< x, y >= I : (< x > + < y >) = (I : x) \cap (I : y)$$

Per determinare una base $I :< x >$ usiamo il Teorema 4.4.3 e l'algoritmo per il calcolo di una base di $I \cap < x >$. Ossia calcoliamo prima una base di Groebner G rispetto all'ordine LEX con $t > z > x > y$ dell'ideale

$$< t(xz - y^2), t(x^3 - yz), (1 - t)x >$$

poi dividiamo per x gli elementi di $G' = G \cap k[x, y, z]$. Si ottiene:

$$I \cap < x >=< G' >=< x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3 > .$$

Possiamo escludere $x^5 - xy^3$ percé combinazione lineare con coefficienti rispettivi y e x del primo e secondo elemento della base. Quindi $I :< x >$

$$I :< x >=< \frac{x^2z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3y - xz^2}{x} >$$

$$=< xz - y^2, x^3 - yz, x^2y - z^2 >$$

Ossia:

$$I :< x >= I + < x^2y - z^2 >=< xz - y^2, x^3 - yz, x^2y - z^2 > .$$

In modo del tutto analogo si calcola $I :< y >$ e si ottiene $I :< y >= I :< x >$, pertanto

$$I :< x, y >= I :< x >= I :< y >=< xz - y^2, x^3 - yz, x^2y - z^2 > .$$

(Lo studente è pregato di controllare i conti usando CoCoA o un altro sistema di Algebra Computazionale).

La varietà $W = \mathcal{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ è una curva irriducibile. Per vederlo si può considerarne la parametrizzazione (t^3, t^4, t^5). Infatti è chiaro che $(t^3, t^4, t^5) \in W$ per ogni t, ed è un semplice esercizio, lasciato al lettore, vedere che ogni punto di W ha questa forma. Per la Proposizione 4.5.2 dunque $W = \mathcal{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ è una curva irriducibile.

In conclusione la nostra varietà $V = \mathcal{V}(xz - y^2, x^3 - yz)$ viene decomposta nell'unione di due curve irriducibili

$$\mathcal{V}(xz - y^2, x^3 - yz) = \mathcal{V}(x, y) \cup W.$$

Un Esempio più semplice è dato dall'unione dell'asse z e del piano xy

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

In entrambi gli esempi appare chiaramente che la decomposizione in irriducibili è unica. E' spontaneo chiedersi se ciò vale in generale. Per evitare casi banali escludiamo decomposizioni in cui la stessa componente irriducibile appaia più di una volta o in cui una componente irriducibile contenga un'altra. A tale scopo diamo la seguente definizione.

Definizione 4.6.1 *Sia $V \subset k^n$ una varietà affine. Una decomposizione*

$$V = V_1 \cup V_2 \cup \ldots \cup V_n.$$

dove ogni V_i è irriducibile, è chiamata **decomposizione minimale** *o* **unione irridondante** *se $V_i \not\subset V_j$ per $i \neq j$.*

Con questa definizione possiamo dimostrare il seguente risultato di unicità.

Teorema 4.6.2 *Ogni varietà affine $V \subset k^n$ ha una decomposizione minimale*

$$V = V_1 \cup V_2 \cup \ldots \cup V_n,$$

e tale decomposizione è unica a meno dell'ordine con cui sono state scritte le componenti irriducibili $V_1, \ldots, V_n$.

Dimostrazione. Per il Teorema 4.6.1 possiamo decomporre V in un'unione finita di componenti irriducibili V_i, $(i = 1, \ldots, n)$, ossia scrivere

$$V = V_1 \cup V_2 \cup \ldots \cup V_n.$$

Se una V_i è contenuta in qualche V_j per $i \neq j$ la eliminiamo e V risulterà unione delle rimanenti V_j per $j \neq i$. Ripetendo questo procedimento si ottiene una decomposizione minimale.

Per dimostrare l'unicità, supponiamo di avere un'altra decomposizione minimale

$$V = V_1' \cup \ldots \cup V_m'.$$

Allora per ogni V_i della prima decomposizione, abbiamo

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \ldots \cup V_m') = (V_i \cap V_1') \cup \ldots \cup (V_i \cap V_m').$$

Ma V_i è irriducibile, e quindi $V_i = V_i \cap V_j'$ per qualche j; ne segue che $V_i \subset V_j'$. Ragionando analogamente su V_j' si vede che esiste un indice h tale che $V_j' = V_j' \cap V_h$ dunque $V_j' \subset V_h$ per qualche h. Si ha allora

$$V_i \subset V_j' \subset V_h$$

Dalla minimalità delle decomposizioni segue allora che $i = h$ e $V_i = V_j'$. Pertanto ogni V_i, per $i = 1, \ldots, n$, della prima decomposizione minimale appare nella seconda decomposizione $V = V_1' \cup \ldots \cup V_m'$. Ciò implica che $n \leq m$. Analogamente si prova che $m \leq n$ e pertanto $n = m$, e le V_i' sono solo una permutazione delle V_i e l'unicità è dimostrata. ∎

Si noti che l'unicità della decomposizione non sussiste se non si decompone in un numero *finito* di varietà. Ad esempio un piano è unione infinita dei suoi punti; ma può anche considerarsi unione di qualcuna delle sue rette e dei punti residui e, in questo caso, la decomposizione non è unica.

Traducendo **algebricamente** i due teoremi che danno la decomposizione in componenti irriducibili si ha il seguente teorema.

Teorema 4.6.3 *Se k è un campo algebricamente chiuso, ogni ideale radicale I di $k[x_1, \ldots, x_n]$ può essere scritto in modo unico come unione finita di ideali primi*

$$I = P_1 \cap \ldots \cap P_r,$$

con $P_i \not\subset P_j$ per $i \neq j$. (Come nel caso di varietà una tale presentazione di $I = \sqrt{I}$ si definisce **decomposizione minimale** *o anche* **intersezione irridondante***).*

Dimostrazione. La dimostrazione di questo Teorema è conseguenza immediata della corrispondenza ideali-varietà e dei Teoremi 4.6.1 e 4.6.2. ∎

Possiamo utilizzare gli ideali quozienti, per descrivere gli ideali primi che compaiono nella decomposizione minimale di un ideale radicale.

Teorema 4.6.4 *Se k è un campo algebricamente chiuso, I è un ideale radicale proprio di $k[x_1, \ldots, x_n]$ e*

$$I = \bigcap_{i=1}^{r} P_i \qquad P_i \not\subset P_j,\ i \neq j,$$

è la sua decomposizione minimale come intersezione di ideali primi, allora i P_i sono esattamente gli ideali primi propri dell'insieme

$$\{I : f \ \mid f \in k[x_1, \ldots, x_n]\}.$$

ove indichiamo per brevità con $I : f$ il quoziente $I :< f >$.

Dimostrazione. Per prima cosa possiamo osservare che, poiché I è un ideale proprio, ciascun P_i è anche un ideale proprio (ciò segue dalla minimalità in quanto se per un fissato i fosse $P_i = k[x_1, \ldots, x_n]$, per ogni $j \neq i$ si avrebbe $P_j \subset P_i$).

Per ogni $f \in k[x_1, \ldots, x_n]$ le proprietà di cui gode l'ideale quoziente implicano che

$$I : f = (\bigcap_{i=1}^{r} P_i) : f = \bigcap_{i=1}^{r} (P_i : f).$$

Inoltre, dalle definizioni di ideale, ideale quoziente e ideale primo, segue immediatamente, per ogni ideale primo P, che se $f \in P$ si ha $P : f =< 1 >$, mentre se $f \notin P$, si ha $P : f = P$.

Ora supponiamo che $I : f$ sia un ideale primo proprio. Osserviamo in primo luogo che se un ideale primo $P \supseteq \bigcap_{i=1}^{r} I_i$, allora $P \supseteq I_i$ per qualche i. Inoltre, se $P = \bigcap_{i=1}^{r} I_i$ allora $P = I_i$ per qualche i. (Infatti se I e J sono Ideali e un primo $P \supseteq I \cdot J$ risulta o $P = I$ oppure $P = J$. Ma $I \cdot J \subseteq I \cap J \subseteq P$ e pertanto l'asserto vale se $r = 2$ da cui, per induzione, segue il caso $r \geq 2$).

Da questa osservazione segue che se $I : f = P$ è un primo proprio, allora esiste un i tale che $I : f = P_i : f$ ma $I : f = P \neq k[x_1, \ldots, x_n]$, quindi anche $P_i : f \neq k[x_1, \ldots, x_n]$ e come tale $P_i : f = P_i$. In definitiva resta dimostrato che un primo proprio dell'insieme $\{I : f \ \mid f \in k[x_1, \ldots, x_n]\}$ è

necessariamente uno dei P_i che figurano nella decomposizione minimale di I come intersezione di ideali primi.

Viceversa, si deve far vedere che ogni P_i è del tipo $I : f$. Fissato i esiste un $f \in (\bigcap_{i \neq j}^{r} P_j) - P_i$ perché $\bigcap_{i=1}^{r} P_i$ è minimale. Si ha che $P_i : f = P_i$ mentre $P_j : f =< 1 >$ per ogni $j \neq i$. Se ora combiniamo questo risultato con la formula con cui si può esprimere $I : f$ si ha che che $I : f = P_i$ ∎

Osserviamo che I teoremi 4.6.3 e 4.6.4 sussistono per ogni campo, ma nel caso generale le dimostrazioni sono diverse.

Quanto finora visto in questo e nel paragrafo precedente suggerisce i seguenti problemi

- **Primalità** Esiste un algoritmo per decidere se un ideale è primo?
- **Irriducibilità** Esiste un algoritmo per decidere se una varietà affine è irriducibile?
- **Decomposizione** Esiste un algoritmo per trovare la decomposizione minimale di una data varietà o di un dato ideale?

La risposta ai tre problemi è affermativa (cfr. [14], [19], [22],[23] [13], [10]), ma esula da questa trattazione.

Concludiamo questo capitolo con un esempio che faccia capire cosa dicono i teoremi 4.6.3 e 4.6.4.

Esempio. Consideriamo l'ideale $I =< xz - y^2, x^3 - yz >$ che definisce la varietà $V = \mathcal{V}(I)$ già discussa in questo paragrafo. Supponiamo che $I = \sqrt{I}$ (vedremo in seguito che ciò è vero in quanto proveremo che I è intersezione di ideali primi e ogni intersezione di ideali primi è radicale). La decomposizione geometrica

$$V = \mathcal{V}(x, y) \cup W,$$

ove $W = \mathcal{V}(I+ < x^2y - z^2 >)$ suggerisce che

$$I =< x, y > \cap < I+ < x^2y-z^2 >=< x, y > \cap < xz-y^2, x^3-yz, x^2y-z^2 >,$$

e ciò si dimostra facilmente con le tecniche imparate finora. Sappiamo, inoltre, che $I :< x >=< xz - y^2, x^3 - yz, x^2y - z^2 >$, Dunque

$$I =< x, y > \cap (I : x).$$

Per rappresentare $< x, y >$ come un ideale quoziente di I, pensiamo geometricamente. L'idea è di rimuovere la varietà W da V. Delle 3 equazioni

che definiscono W, le prime due danno V. Ha quindi senso usare la terza, $x^2y-z^2=0$ e si può verificare per esercizio che che $I :< x^2y-z^2 >=< x, y >$. Quindi

$$I = (I :< x^2y - z^2 >) \cap (I :< x >).$$

Resta da dimostrare che $I :< x^2y - z^2 >$ e $I :< x >$ sono ideali primi. Il primo è semplice in quanto $I :< x^2y - z^2 >=< x, y >$ è ovviamente primo. Quanto al secondo, abbiamo già visto che

$$W = \mathcal{V}(I+ < x^2y - z^2 >) = \mathcal{V}(I :< x >)$$

è irriducibile inoltre si può verificare per esercizio che

$$J = \mathcal{I}(W) = I+ < x^2y - z^2 >= I :< x >$$

(Suggerimento: calcolare una base di Groebner di J rispetto a LEX con $z > y > x$ e far vedere che ogni $f \in k[x, y, z]$ si può crivere nella forma

$$f = g + a + bz + A(x) + yB(x) + y^2C(x)$$

con $g \in J$, $a, b, \in k$ e $A, B, C \in k[x]$). Poiché W è irriducibile, per la Proposizione 4.5.1 si ha che $\mathcal{I}(W) = I :< x >$ è primo e quindi

$$I = (I :< x^2y - z^2 >) \cap (I :< x >)$$

è la decomposizione minimale di I in ideali primi. Ne segue che $I = \sqrt{I}$, in quanto ogni intersezione di ideali primi è radicale. I ragionamenti qui usati sono strettamente relativi all'esempio considerato. Sarebbe auspicabile avere tecniche generali applicabili ad ogni ideale.

Si noti infine che i teoremi di questo paragrafo sulle decomposizioni di varietà e di ideali radicali ci dicono che le decomposizioni esistono ma non ci indicano come trovarle. Questo in quanto si poggiano sul teorema della base di Hilbert che, essenzialmente, è un teorema non costruttivo.