CAPITOLO VIII. NULLSTELLENSATZ

Lucean le stelle

In realtà le stelle non c'entrano: semmai si potrebbe chiosare, alla Bergmann: "*Il posto degli zeri*" o più correttamente "proposizione sui luoghi degli zeri". Vedremo tre versioni di questo celebre teorema di Hilbert ed alcune sue ricadute in algebra e geometria.

Nel capitolo VI abbiamo aperto il problema di quali sono i polinomi che si annullano su una certa varietà e abbiamo mostrato che $I(V(\mathrm{I}))$ contiene I, ma in generale non coincide con I. È il caso di $\mathrm{I}=\langle x^2,y\rangle$ e più in generale di tutti gli ideali I che contengono una potenza intera f^m di un polinomio f senza contenere f : infatti, se $\mathbf{c}\in V(\mathrm{I})$ – e quindi, in particolare, se $0=f^m(\mathbf{c})=[f(\mathbf{c})]^m$ – allora anche $f(\mathbf{c})=0$, cioè f appartiene a $I(V(\mathrm{I}))$.
Questa osservazione porterà a dare una certa importanza all'insieme dei polinomi tali che una loro potenza intera stia in I che verrà detto *radicale* di I. Abbiamo appena provato che $I(V(\mathrm{I}))$ contiene non solo I, ma anche il suo radicale; una delle versioni del Nullstellensatz garantirà che, purché il campo in cui ci muoviamo sia algebricamente chiuso (e quindi valga il teorema di estensione) $I(V(\mathrm{I}))$ coincide con il radicale di I e quindi sposterà il problema, sul piano computazionale, alla descrizione dei generatori del radicale di I.
Per arrivare a questo punto però esaminiamo prima un altro problema, in apparenza diverso dal precedente, poiché non corrisponde a cercare $I(V(\mathrm{I}))$, bensì un I tale che $V(\mathrm{I})=\varnothing$:

"come può essere fatto un ideale i cui polinomi si annullano sulla varietà algebrica vuota?"

1. IL NULLSTELLENSATZ DEBOLE

Se il campo k non è algebricamente chiuso, non solo a differenti ideali I può corrispondere la stessa varietà $\mathrm{V}=V(\mathrm{I})$, ma addirittura può succedere che anche ideali diversi da $(1)=k[x_1,\ldots,x_n]$ abbiano come luogo di zeri la varietà vuota. Ad esempio, se $k=\mathbf{R}$ ideali come $\langle 1+x^2\rangle$, $\langle 1+x^2+x^4\rangle$… producono la sottovarietà vuota di $\mathbf{R}^1$, mentre ideali come $\langle 1+x^2+y^2\rangle$, $\langle 1+x^2\rangle$… producono la sottovarietà vuota di $\mathbf{R}^2$.
Puntiamo a mostrare che se il campo è algebricamente chiuso questo non succede.
Se stiamo lavorando nello spazio affine k^1 di dimensione 1, la cosa è insita nella definizione di campo algebricamente chiuso: infatti in $k[x]$ ogni ideale I è principale e il suo polinomio generatore f (essendo fattorizzabile in $\deg(f)$ polinomi di primo grado) ha un numero zeri (eventualmente contati con la loro molteplicità) pari al suo grado: se si vuole che $V(\mathrm{I})$ sia vuota, non ci devono essere zeri e quindi f deve avere grado zero, cioè essere un polinomio costante non nullo: ciò significa che f è invertibile e quindi nell'ideale I c'è anche 1. Ne segue che $\mathrm{I}=k[x]$.
L'estensione di ciò a spazi affini di dimensione superiore a 1 costituisce il:

NULLSTELLENSATZ DEBOLE *Se il campo k è algebricamente chiuso e* I *è un ideale di* $k[x_1,\ldots,x_n]$ *tale che* $V(\mathrm{I})$ *sia vuota, allora* I *contiene* 1 (*e quindi coincide con* $k[x_1,\ldots,x_n]$).

Avendo appena visto la dimostrazione per $n=1$, si può pensare di provare l'enunciato per induzione sul numero di indeterminate. Per dimostrare il passo induttivo sono necessari alcuni lemmi tecnici.

LEMMA 1.1 *Sia f un polinomio di $k[x_1,\dots,x_n]$ avente grado totale N. Operando il cambiamento di coordinate*

$$(*) \qquad \begin{cases} x_1 = y_1 \\ x_2 = y_2 + a_2 y_1 \\ \quad\vdots \\ x_n = y_n + a_n y_1 \end{cases} \qquad \text{con } a_2,\dots,a_n \in k$$

si ottiene un polinomio di $k[y_1,\dots,y_n]$ della forma

$$f = p(a_2,\dots,a_n)\cdot y_1^N + \text{termini in cui } y_1 \text{ ha grado } <N$$

ove $p(a_2,\dots,a_n)$ è un elemento del campo k e $p(x_2,\dots,x_n)$ è un polinomio non nullo di $k[x_2,\dots,x_n]$.

Dimostrazione Scriviamo f come somma di polinomi omogenei di grado N, $N-1,\dots,0$: alcuni di questi polinomi possono essere nulli (cioè possono mancare monomi di grado complessivo $=i$) ma, visto che il grado totale del polinomio è N, sicuramente non lo è il polinomio omogeneo di grado N

$$h_N = b_{(N,0,\dots,0)}x_1^N + b_{(N-1,1,\dots,0)}x_1^{N-1}x_2 + \dots + b_{(0,0,\dots,N)}x_n^N$$

e quindi almeno uno dei coefficienti b_α (anche se non necessariamente quello di x_1^N) deve essere non nullo. La sostituzione (*), essendo lineare, non altera il grado complessivo dei termini di f: quindi i termini in cui y_1 ha grado $=N$ si trovano operando la sostituzione (*) in h_N

$$h_N(y_1,\dots,y_n) = b_{(N,0,\dots,0)}y_1^N + b_{(N-1,1,\dots,0)}y_1^{N-1}(y_2+a_2y_1) + \dots + b_{(0,0,\dots,N)}(y_n+a_ny_1)^N,$$

per cui y_1^N ha coefficiente (in h_N, ma anche in f, visto che tutti gli altri termini hanno grado $<N$)

$$p(a_2,\dots,a_n) = b_{(N,0,\dots,0)} + b_{(N-1,1,\dots,0)}a_2 + \dots + b_{(0,0,\dots,N)}a_n^N = h_N(1,a_2,\dots,a_n).$$

Osserviamo che il polinomio $h_N(1,x_2,\dots,x_n)$ non è nullo, altrimenti tutti i coefficienti b_α (che coincidono con quelli che compaiono in $h_N(x_1,x_2,\dots,x_n)$) sarebbero nulli, contro le ipotesi. Quindi il polinomio $p(x_2,\dots,x_n)$ che valutato in $(a_2,\dots,a_n)$ dà il coefficiente di y_1^N è non nullo. C.V.D.

Sappiamo che se k è un campo infinito (come capita quando è algebricamente chiuso: vedi teorema 8.4 del Capitolo I) un polinomio in $n-1$ indeterminate si annulla su ogni $(n-1)$-upla $(a_2,\dots,a_n)\in k^n$ solo se è il polinomio nullo (teorema 7.4 del Capitolo I). Quindi dal lemma 1.1 si deduce che una opportuna trasformazione (*) permette di riscrivere il polinomio in modo che la prima variabile si presenti con grado pari al grado del polinomio:

COROLLARIO 1.2 *Se k è un campo infinito, è possibile trovare $a_2,\dots,a_n\in k$ in modo che, operata la sostituzione (*), il coefficiente $p(a_2,\dots,a_n)$ di y_1^N in $f(y_1, y_2+a_2y_1, \dots, y_n+a_ny_1)$ sia una costante non nulla.*

LEMMA 1.3 *Si consideri la corrispondenza T: $k[x_1,\dots, x_n] \to k[y_1,\dots, y_n]$ che a ogni polinomio f di $k[x_1,\dots, x_n]$ fa corrispondere il polinomio $f(y_1, y_2+a_2y_1,\dots, y_n+a_ny_1) =: g(y_1,\dots, y_n)$ di $k[y_1,\dots, y_n]$. Allora*

(i) *T è un isomorfismo di anelli*

(ii) *f è dotato di zeri in k^n se e solo se lo è $g = T(f)$*

(iii) *se I è un ideale di $k[x_1,\dots, x_n]$ anche il suo trasformato $T(\mathrm{I}) = \{g = T(f) |\ f\in \mathrm{I}\}$ lo è.*

Dimostrazione (i) La sostituzione (*) è invertibile [(1)]: $y_1 = x_1$, $y_2 = x_2 - a_2x_1,\dots, y_n = x_n - a_nx_1$ e ciò permette di trovare, per ogni $g(y_1,\dots, y_n)$ una e una sola preimmagine

$$f(x_1,\dots, x_n) := g(x_1, x_2-a_2x_1\dots, x_n-a_nx_1).$$

[(1)] Dal punto di vista geometrico la trasformazione (*) è una affinità (senza fattore di traslazione).

Dunque la corrispondenza T è 1-1. Essa è addirittura un isomorfismo di anelli, poiché $T(1) = 1$ e ogni termine di un polinomio somma $f + f^*$ (o di un polinomio prodotto $f \cdot f^*$) viene trasformato secondo le (*): $T(x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}) = y_1^{\alpha_1}(y_2+a_2y_1)^{\alpha_2}\ldots(y_n+a_ny_1)^{\alpha_n}$. Ad esempio, se

$$f = x_1x_2+x_3 \text{ e } f^* = x_2^2+x_1,$$

si ha

$$f\cdot f^* = (x_1x_2+x_1)(x_2^2+x_1) = x_1x_2^3+x_1^2x_2+x_1x_2^2+x_1^2$$

il cui trasformato è

$$y_1(y_2+a_2y_1)^3+y_1^2(y_2+a_2y_1)+x_1(y_2+a_2y_1)^2+y_1^2 = [y_1(y_2+a_2y_1)+y_1][(y_2+a_2y_1)^2+y_1] = T(f)\cdot T(f^*).$$

(ii) Se $(c_1,\ldots, c_n)\in k^n$ è tale che $f(c_1,\ldots, c_n)=0$ anche $g(c_1, c_2-a_2c_1\ldots, c_n-a_nc_1) = 0$ e viceversa se è tale che $g(c_1,\ldots, c_n) = 0$ anche $f(c_1, c_2+a_2c_1\ldots, c_n+a_nc_1) = 0$.

(iii) Il fatto che la corrispondenza T sia un isomorfismo implica che la preimmagine di un ideale sia un ideale: infatti se g e g^* stanno in $T(\mathrm{I})$, $T^{-1}(g) = f$ e $T^{-1}(g^*) = f^*$ stanno in I e quindi $f+f^*$ e $f\cdot f^*$ anche. Dunque $T(f+f^*) = T(f)+T(f^*) = g+g^*$ e $T(f\cdot f^*) = T(f)\cdot T(f^*) = g\cdot g^*$ stanno in $T(\mathrm{I})$. C.D.V.

Ora abbiamo tutti gli strumenti per provare il passo induttivo nella dimostrazione per induzione del Nullstellensatz debole, il che permetterà di ritenere provato il teorema, grazie al metodo induttivo.

Supponiamo dunque il teorema vero per l'anello di polinomi in $n-1$ indeterminate $k[x_2,\ldots, x_n]$ e sia $\mathrm{I} = \langle f_1,\ldots, f_s\rangle$ un ideale di $k[x_1,\ldots, x_n]$ con $V(\mathrm{I}) = \varnothing$.

A) Se un f_i è un polinomio costante $\neq 0$, I contiene 1 e quindi non c'è nulla da provare.

B) Se i generatori di I sono contenuti in $k[x_2,\ldots, x_n]$, essi generano anche I_1 in $k[x_2,\ldots, x_n]$ e quindi ogni zero di $f_1,\ldots, f_s$ in k^{n-1} si estende a (infiniti) zeri in k^n, cioè $\pi_1(V(\mathrm{I}))=V(\mathrm{I}_1)$. Ora visto che $V(\mathrm{I}) = \varnothing$ e $\pi_1(\varnothing) = \varnothing$, in k^{n-1} la varietà $V(\mathrm{I}_1)$ è vuota: questo, per l'ipotesi induttiva, prova che I_1 contiene l'unità 1 di $k[x_2,\ldots, x_n]$ e quindi anche I contiene 1 che è pure l'unità di $k[x_1,\ldots, x_n]$

C) Se i generatori di I non sono tutti contenuti in $k[x_2,\ldots, x_n]$, almeno uno di essi contiene un termine di grado ≥ 1 in x_1; in particolare, se almeno un f_i si può scrivere come

$$C\cdot x_1^N + \text{termini in cui } x_1 \text{ ha grado} < N, \quad \text{ove } C \text{ è una costante non nulla ed } N > 0$$

il teorema di estensione in forma geometrica (vedi Capitolo VII, teorema 6.3, rienunciato per un campo algebricamente chiuso qualunque) garantisce che se π_1: $k^n \to k^{n-1}$ è la proiezione sulle ultime $n-1$ componenti e $\mathrm{I}_1 = \mathrm{I}\cap k[x_2,\ldots, x_n]$ si ha $V(\mathrm{I}_1) = \pi_1(V(\mathrm{I}))$. Di nuovo, visto che $V(\mathrm{I}) = \varnothing$ e $\pi_1(\varnothing) = \varnothing$, in k^{n-1} la varietà $V(\mathrm{I}_1)$ è vuota, il che per l'ipotesi induttiva, prova che I_1, e di conseguenza I, contiene l'unità 1 di $k[x_2,\ldots, x_n]$ che è pure l'unità di $k[x_1,\ldots, x_n]$.

D) Se nessuna delle ipotesi precedenti è valida, almeno un polinomio f_i ha coefficiente del termine di grado massimo rispetto a x_1 non nullo: operiamo il cambiamento di coordinate (*) in modo che il coefficiente $p(a_2,\ldots, a_n)$ di y_1^N in $T(f_i)$ sia una costante non nulla (ciò è possibile per il corollario 1.2): il lemma 1.3 (ii) garantisce che i polinomi di $T(\mathrm{I})$ non hanno zeri in comune, cioè

$$V(T(\mathrm{I})) = \varnothing$$

e quindi per quanto visto in (C) l'ideale $T(\mathrm{I})$ contiene l'unità 1_y di $k[y_1,\ldots,y_n]$ ed essendo T un isomorfismo di anelli, $\mathrm{I} = T^{-1}(T(\mathrm{I}))$ contiene $T^{-1}(1_y) = 1_x$, unità di $k[x_1,\ldots, x_n]$.[(2)] C.V.D.

[(2)] Osserviamo che, più in generale, se il campo è infinito, la sostituzione (*) permetterebbe di scaricare il problema dell'esistenza di una soluzione del sistema $f_1=0, \ldots, f_s=0$ da k^n a k^{n-1}, rendendo poi banale il passaggio di estensione finale. Se riprendiamo in esame l'esempio già illustrato nel Capitolo VI, in cui $\mathrm{I}=\langle x_1x_2-1, x_2-x_3\rangle$, la sostituzione con $a_2=1$ e $a_3=0$ porta all'ideale $T(\mathrm{I})=\langle y_1^2+y_1y_2-1, y_1+y_2-y_3\rangle$, che ha base di Gröbner rispetto a LEX: $\{y_1+y_2-y_3, y_2y_3-1\}$. Ora tutte le soluzioni $\{(1/t, t), t\neq 0\}$ di $y_2y_3-1=0$ si estendono alla dimensione superiore: basta prendere $(t-(1/t), 1/t, t)$; applicando poi la trasformazione inversa si possono eventualmente determinare le soluzioni del sistema di partenza. Ma ciò equivale solo a spostare i problemi da k^3 a k^2. Meglio quindi usare il test di risolubilità indicato alla fine di questo paragrafo.

Ricadute del Nullstellensatz sulla consistenza dei sistemi

La prima conseguenza del teorema ora dimostrato è che si può predire quando un sistema di equazioni polinomiali a coefficienti in un campo k algebricamente chiuso

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

è risolubile.

È già stato detto che se l'ideale $I = \langle f_1,\ldots,f_s \rangle$ contiene 1 il sistema è privo di soluzioni (anche se k non è algebricamente chiuso). Possiamo rendere questa affermazione più "computazionale" osservando che se I contiene 1, la sua base di Gröbner ridotta è {1}, quale che sia l'ordinamento monomiale scelto. Infatti LT(1) deve essere divisibile per il LT di ogni polinomio della base di Gröbner: quindi tali LT devono avere grado 0, il che significa innanzi tutto che nella base non ci sono polinomi non costanti e di conseguenza che nella base c'è un solo polinomio (gli altri sarebbero suoi multipli mediante elementi di k): questo polinomio, dovendo essere monico, è proprio 1. Dunque

Comunque sia fatto il campo k, il sistema polinomiale $f_1 = 0, \ldots, f_s = 0$ *non ha soluzioni se la base di Gröbner ridotta dell'ideale* $I = \langle f_1,\ldots,f_s \rangle$ *rispetto a un ordinamento monomiale è* {1} [(3)].

Il Nullstellensatz garantisce che

se il campo k è algebricamente chiuso, questo è il solo caso in cui succede

o anche

se il campo k è algebricamente chiuso e la base di Gröbner ridotta dell'ideale $I = \langle f_1,\ldots, f_s \rangle$ *rispetto a un ordinamento monomiale non è* {1}*, allora il sistema polinomiale* $f_1 = 0, \ldots, f_s = 0$ *ha almeno una soluzione.*

Da notare che, visto che non è specificato l'ordinamento, il test di risolubilità può essere fatto rispetto a un ordinamento diverso da LEX, che è quello normalmente usato per il calcolo degli ideali di eliminazione h-esima (cioè per trovare le soluzioni del sistema) ma è tutt'altro che maneggevole.

2. IL NULLSTELLENSATZ DI HILBERT

Si è già visto che anche se il campo è algebricamente chiuso ci sono diversi ideali che danno luogo a una stessa varietà: ad esempio, per ogni i intero, $V(\langle x^i \rangle) = \{0\}$ in k^1, per ogni coppia (i,j) di interi, $V(\langle x^i, y^j \rangle) = \{(0,0)\}$ in k^2 ecc.

Abbiamo anche osservato che se una potenza di un polinomio f sta in un ideale I allora f si annulla sulla varietà algebrica V(I): proveremo che se il campo è algebricamente chiuso è vero anche il viceversa, cioè che gli unici polinomi che si annullano su V(I) sono quelli una potenza dei quali sta in I.

Premettiamo due lemmi tecnici.

---

(3) Espressa per contronominale questa proposizione afferma che *se il sistema polinomiale* $f_1=0, \ldots, f_s=0$ *ha soluzioni la base di Gröbner dell'ideale* $I=\langle f_1,\ldots,f_s \rangle$ *rispetto a un ordinamento monomiale qualunque non contiene* 1: se si sa che il sistema ha soluzioni, questa proposizione può servire per verificare la verosimiglianza della base di Gröbner trovata, specie se la si è calcolata a mano!

LEMMA 2.1 *Sia k un campo arbitrario e siano* $f_1,\ldots,f_s,f$ *polinomi di* $k[x_1,\ldots,x_n]$. *Sono equivalenti:*

(i) *esiste un intero* $m\geq 1$ *tale che* f^m *stia nell'ideale* $<f_1,\ldots,f_s>$ *di* $k[x_1,\ldots,x_n]$

(ii) *l'ideale* $<f_1,\ldots,f_s,\ 1-yf>$ *di* $k[x_1,\ldots,x_n,y]$ *contiene l'unità* 1 *di tale anello.*

Dimostrazione (i) $\Rightarrow$ (ii) Se la potenza intera f^m di f sta nell'ideale $<f_1,\ldots,f_s>$ che è contenuto in $<f_1,\ldots,f_s,1-yf>$, in $k[x_1,\ldots,x_n,y]$ si ha che $1=(1-y^mf^m)+y^mf^m=(1-yf)(1+yf+\ldots+y^{m-1}f^{m-1})+y^mf^m$ appartiene all'ideale $<f_1,\ldots,f_s,\ 1-yf>$.

(ii) $\Rightarrow$ (i) Scriviamo per brevità $(x_1,\ldots,x_n,y)=:(\mathbf{x},y)$. Allora l'ipotesi significa che esistono $s+1$ polinomi $p_1(\mathbf{x},y),\ldots,p_s(\mathbf{x},y),q(\mathbf{x},y)$ in $k[\mathbf{x},y]$ tali che:

$$(\#)\qquad 1=p_1(\mathbf{x},y)f_1+\ldots+p_s(\mathbf{x},y)f_s+q(\mathbf{x},y)(1-yf).$$

Si può pensare $p_1(\mathbf{x},y)f_1+\ldots+p_s(\mathbf{x},y)f_s+q(\mathbf{x},y)(1-yf)$ come il polinomio 1 di $k(\mathbf{x})[y]$, che - come tutti i polinomi - definisce una funzione del campo $k(\boldsymbol{x})$ in sé. In particolare ponendo $y=1/f$, si trova la seguente uguaglianza in $k(\boldsymbol{x})$

$$1=p_1(\mathbf{x},1/f)f_1+\ldots+p_s(\mathbf{x},1/f)f_s.$$

Ogni $p_i(\mathbf{x},1/f)$ è - una volta operata la riduzione a denominatore comune - una frazione di polinomi con denominatore una potenza di f e quindi, detta m la massima potenza a cui compare y nei vari polinomi $p_i(\mathbf{x},y)$, si potrà scrivere

$$f^m=A_1(\mathbf{x})f_1+\ldots+A_s(\mathbf{x})f_s,$$

ove m è sicuramente ≥ 1 - avendo il polinomio in (#) grado 0 anche in y - e $A_i(\mathbf{x})=f^m\cdot p_i(\mathbf{x},1/f)$ è, per ogni i, un polinomio di $k[x_1,\ldots,x_n]$: dunque f^m appartiene all'ideale $<f_1,\ldots,f_s>$ di $k[x_1,\ldots,x_n]$. C.V.D.

LEMMA 2.2 *Sia k un campo arbitrario e siano* $f_1,\ldots,f_s,\ f$ *polinomi di* $k[x_1,\ldots,x_n]$. *Se f appartiene a* $I(V(f_1,\ldots,f_s))$, *la varietà* $V(f_1,\ldots,f_s,\ 1-yf)$ *di* k^{n+1} *è vuota.*

Dimostrazione Supponiamo che $(\mathbf{c},c_{n+1})$ sia un punto di $V(f_1,\ldots,f_s,1-yf)$. Visto che $f_1,\ldots,f_s,f$ non contengono l'indeterminata y, ciò significa

$$f_1(\mathbf{c})=0,\ \ldots\ ,\ f_s(\mathbf{c})=0,\ \ 1-c_{n+1}f(\mathbf{c})=0.$$

Dunque $\mathbf{c}$ appartiene a $V(f_1,\ldots,f_s))$ e di conseguenza f che appartiene a $I(V(f_1,\ldots,f_s))$ si annulla in $\mathbf{c}$. Quindi l'ultima uguaglianza non può essere mai verificata, cioè $V(f_1,\ldots,f_s,1-yf)$ è vuota. C.V.D.

NULLSTELLENSATZ DI HILBERT *Sia k algebricamente chiuso e siano* $f_1,\ldots,f_s,\ f$ *polinomi di* $k[x_1,\ldots,x_n]$. *Sono equivalenti*

(i) *esiste un intero* $m\geq 1$ *tale che* f^m *stia in* $<f_1,\ldots,f_s>$

(ii) *f appartiene a* $I(V(f_1,\ldots,f_s))$.

Dimostrazione Si è già visto che (i) $\Rightarrow$ (ii). Viceversa se vale (ii) siamo nelle ipotesi del lemma 2.2 e quindi $V(f_1,\ldots,f_s,1-yf)$ è vuota: dunque per il Nullstellensatz debole l'ideale $<f_1,\ldots,f_s,1-yf>$ contiene 1 e di conseguenza, per il lemma 2.1, esiste un intero $m\geq 1$ tale che f^m stia in $<f_1,\ldots,f_s>$. C.V.D.

3. RADICALE DI UN IDEALE E IDEALE RADICALE

Sia X un sottoinsieme di k^n (in particolare una varietà algebrica V): se esiste un intero $m\geq 1$ tale che f^m stia in $I(\mathrm{X})=\{g\in k[x_1,\ldots,x_n]\mid g(\mathbf{c})=0\ \forall\ \mathbf{c}\in\mathrm{X}\}$ anche f appartiene all'ideale $I(\mathrm{X})$, poiché se $\mathbf{c}\in\mathrm{X}$ da $0=f^m(\mathbf{c})=[f(\mathbf{c})]^m$ si ricava $f(\mathbf{c})=0$.

Conviene dare un nome a ideali con questa proprietà.

DEFINIZIONE 3.1 *Si dice che* $I \subseteq k[x_1,\ldots,x_n]$ *è un* ***ideale radicale*** *se gli unici polinomi f di* $k[x_1,\ldots,x_n]$ *per cui esiste un intero* $m\geq 1$ *tale che* f^m *appartenga a* I *sono i polinomi f di* I.

Dunque $I(X)$ è un ideale radicale; così pure lo sono tutti gli ideali primi ($f\cdot f^{m-1}\in I$ e $f\notin I \Rightarrow f^{m-1}\in I$, il che per ricorrenza dice che l'ipotesi $f\notin I$ è assurda). Esistono però sicuramente ideali non radicali: ad esempio $\langle x^2\rangle$. Comunque a partire da un qualunque ideale I si può costruire un ideale radicale.

LEMMA 3.2 *Siano k un campo arbitrario e* I *un ideale di* $k[x_1,\ldots,x_n]$. *L'insieme*

$$\sqrt{I} = \{f\in k[x_1,\ldots,x_n] \mid \exists m\geq 1 \text{ tale che } f^m\in I\}$$

(i) *contiene* I *ed è contenuto in* $I(V(I))$

(ii) *è un ideale di* $k[x_1,\ldots,x_n]$

(iii) *è un ideale radicale.*

Esso sarà detto ***radicale dell'ideale*** I. *Inoltre*

(iv) I *è un ideale radicale se e solo se coincide con* $\sqrt{I}$

(v) $\sqrt{\sqrt{I}} = \sqrt{I}$

(vi) *se* $I\subseteq J$ *risulta* $\sqrt{I}\subseteq\sqrt{J}$

(vii) $\sqrt{I}$ *è il più piccolo ideale radicale contenente* I.

Dimostrazione

(i) $\sqrt{I}$ contiene I poiché per ogni $f\in I$ si ha $f^1\in I$; per mostrare che è contenuto in $I(V(I))$, consideriamo un elemento **c** di $V(I)$. Se $f\in\sqrt{I}$, cioè se esiste un $m\geq 1$ tale che $f^m\in I$, risulta $f^m(\mathbf{c}) = 0$ e quindi $f(\mathbf{c}) = 0$, vale a dire $f\in I(V(I))$.

(ii) Per vedere che $\sqrt{I}$ è un ideale osserviamo che, se f è un suo elemento - cioè $f^m\in I$ per qualche $m\geq 1$ - e $h\in k[x_1,\ldots,x_n]$, si ha $(hf)^m = h^m f^m\in I$; se poi anche g è un suo elemento - cioè $g^l\in I$ per qualche $l\geq 1$ - si ha $(f+g)^{l+m-1}\in I$ poiché ogni addendo nello sviluppo contiene o una potenza di f di ordine almeno m o una potenza di g di ordine almeno l e quindi ogni addendo sta in I: dunque $f+g$ appartiene a $\sqrt{I}$ [(4)].

(iii) Supponiamo che f^m appartenga a $\sqrt{I}$: allora c'è una sua potenza $(f^m)^l$ con $l\geq 1$ appartenente a I, cioè $f^{ml}\in I$ e quindi f sta in $\sqrt{I}$: questa è la definizione di ideale radicale.

(iv) Se $I=\sqrt{I}$, I è un ideale radicale per (iii). Se poi I è un ideale radicale, tutti i polinomi $f\in\sqrt{I}$, cioè tali che $f^m\in I$, stanno in I. Dunque $\sqrt{I}$ è contenuto in I e poiché l'inclusione opposta è sempre soddisfatta si vede che i due ideali coincidono.

(v) Tenuto conto che $\sqrt{I}$ è un ideale radicale, la (iv) garantisce che $\sqrt{\sqrt{I}} = \sqrt{I}$.

(vi) $f\in\sqrt{I}$ implica $f^m\in I\subseteq J$, cioè $f\in\sqrt{J}$.

(vii) Se J è un ideale radicale contenente I si ha $I\subseteq\sqrt{I}\subseteq\sqrt{J} = J$ per la (vi).

Osserviamo che dal lemma 3.2 (iv) si deduce in particolare che $I(V)$ coincide con il suo radicale.

Facciamo qui una lista dei problemi pratici che potremmo voler risolvere dato un ideale I attraverso i suoi generatori.

1) Stabilire se un polinomio appartiene al radicale di un ideale (senza conoscere il radicale).
2) Trovare i generatori del radicale di I: non facile

[(4)] In modo analogo si potrebbe anche provare per ogni ideale I di $k[x_1,\ldots,x_n]$ esiste un intero positivo m tale che per ogni f appartenente al radicale di I si ha $f^m\in I$. Basta tener conto che il radicale di I ha sicuramente un numero finito s di generatori e che per ognuno di essi c'è un'opportuna potenza che sta in I: considerando come $m+s-1$ la somma di tutti questi esponenti si ha l'intero richiesto.

3) Stabilire se un ideale è radicale: non facile (in qualche misura si riconduce al precedente: se so come trovare i generatori di $\sqrt{I}$, posso stabilire se le basi di Gröbner ridotte di I e $\sqrt{I}$ rispetto allo stesso ordinamento monomiale coincidono).

Rileggendo in termini di radicali il lemma 2.1, siamo in grado di affrontare il primo problema:

CRITERIO di appartenenza al radicale *Sia k un campo arbitrario e sia* $I = \langle f_1,\dots,f_s\rangle$ *un ideale di* $k[x_1,\dots,x_n]$. *Sono equivalenti:*

(i) *il polinomio f appartiene al radicale* $\sqrt{I}$ *di* I

(ii) *l'ideale* $\langle f_1,\dots,f_s, 1-yf\rangle$ *di* $k[x_1,\dots,x_n,y]$ *contiene l'unità* 1 *di tale anello.*

Dal punto di vista del calcolo questo significa: il polinomio *f* appartiene al radicale di $\langle f_1,\dots,f_s\rangle$ se e solo se la base di Gröbner ridotta dell'ideale $\langle f_1,\dots,f_s,1-yf\rangle$ rispetto a un (arbitrario) ordinamento monomiale è {1}.

Se l'ideale I è principale [(5)], è possibile dare una risposta (almeno in linea teorica) facile anche al secondo quesito:

PROPOSIZIONE 3.4 *Sia k un campo arbitrario e sia* $I = \langle f\rangle$ *un ideale di* $k[x_1,\dots,x_n]$. *Se la fattorizzazione di f in polinomi irriducibili è data da* $f = f_1^{n_1}\cdot\ldots\cdot f_r^{n_r}$, *il radicale di* I *è l'ideale* $\langle f_1\cdot\ldots\cdot f_r\rangle$.

Dimostrazione Osserviamo che $f_1\cdot\ldots\cdot f_r = f_{\text{red}}$ appartiene a $\sqrt{I}$, poiché posto $N=\max(n_1,\dots,n_r)$, l'elemento $(f_1\cdot\ldots\cdot f_r)^N = (f_1^{N-n_1}\cdot\ldots\cdot f_r^{N-n_r})\cdot f$ appartiene a I.
Viceversa, dato $g\in\sqrt{I}$, esiste un intero positivo *m* tale che $g^m\in I$, cioè tale che *f* divida g^m: questo significa che tutti i fattori irriducibili di *f* (essendo primi) devono dividere g^m e quindi *g*; dunque *g* è un multiplo di $f_1\cdot\ldots\cdot f_r$, cioè *g* appartiene a $\langle f_1\cdot\ldots\cdot f_r\rangle$. C.V.D.

Quindi il radicale di un ideale principale è principale. Il problema, a livello computazionale, è che spesso non si conosce la fattorizzazione di *f* e trovarne una può non essere un'operazione banale. Si può aggirare il problema se il campo *k* contiene il sottocampo **Q** dei numeri razionali (o, come si suo dire, è di caratteristica 0). Enunciamo l'idea, che poggia sull'algoritmo visto al Capitolo V §12:

PROPOSIZIONE 3.5 *Sia k un campo contenente* **Q** *e sia* $I = \langle f\rangle$ *un ideale di* $k[x_1,\dots,x_n]$. *Il generatore* f_{red} *del radicale di* I *verifica l'uguaglianza*: $f_{\text{red}}\cdot\text{MCD}(f, (f)'_1,\dots,(f)'_n) = f$, *ove* $(f)'_i$ *denota la derivata (formale) parziale prima rispetto alla variabile* x_i.

Dimostrazione Se si scompone *f* come nella precedente proposizione, basta provare che

$$\text{MCD}(f, (f)'_1,\dots,(f)'_n) = f_1^{n_1-1}\cdot\ldots\cdot f_r^{n_r-1}.$$

Ora, è immediato verificare che, oltre a *f*, anche la derivata parziale di $f = f_1^{n_1}\cdot\ldots\cdot f_r^{n_r}$ (rispetto a qualunque variabile) è multipla di $f_1^{n_1-1}\cdot\ldots\cdot f_r^{n_r-1}$, per cui $f_1^{n_1-1}\cdot\ldots\cdot f_r^{n_r-1}$ è un fattore comune; bisogna garantire che nessun $f_i^{n_i}$ divida tutte le derivate parziali. Illustriamo la verifica per $i=1$: in

$$(f_1^{n_1}\cdot\ldots\cdot f_r^{n_r})'_h = f_1^{n_1-1}\cdot\ldots\cdot f_r^{n_r-1}\cdot[n_1(f_1)'_h\cdot f_2\cdot\ldots\cdot f_r + n_2(f_2)'_h\cdot f_1\cdot f_3\cdot\ldots\cdot f_r + \dots + n_r(f_r)'_h\cdot f_1\cdot f_2\cdot\ldots\cdot f_{r-1}]$$

il fattore f_1 divide gli addendi tra le parentesi quadre dal secondo in poi: dunque f_1, se divide $(f_1^{n_1}\cdot\ldots\cdot f_r^{n_r})'_h$, deve dividere $n_1(f_1)'_h\cdot f_2\cdot\ldots\cdot f_r$, cioè - essendo irriducibile e diverso dagli altri fattori irriducibili - deve dividere $n_1(f_1)'_h$ che però ha grado totale minore di quello di f_1 e quindi è il polinomio nullo: poiché il campo contiene **Q**, ciò significa che $(f_1)'_h = 0$ per ogni *h*, cioè f_1 è costante: assurdo. C.V.D.

---

(5) **Attenzione** Se l'ideale non è principale, non è vero in generale che il suo radicale si ottenga "eliminando le potenze eventualmente presenti nei generatori". Ad esempio $\sqrt{\langle f^2, g^3\rangle} \neq \langle f, g\rangle$ se $f=x^2-y$ e $g=y$ (in realtà il radicale è $\langle x, y\rangle$).

4. NULLSTELLENSATZ FORTE E TEOREMA DI CHIUSURA

Con la terminologia dei radicali, il Nullstellensatz di Hilbert si può enunciare come segue:

NULLSTELLENSATZ FORTE *Sia k un campo algebricamente chiuso* [(6)]. *Scelto comunque un ideale* I *in* $k[x_1,\ldots, x_n]$, *risulta:*

$$I(V(\mathrm{I})) = \sqrt{\mathrm{I}}\,.$$

Dimostrazione Per il lemma 3.2(i), qualunque sia il campo k, vale l'inclusione $I(V(\mathrm{I})) \supseteq \sqrt{\mathrm{I}}$. Viceversa, sia f un elemento di $I(V(\mathrm{I}))$: visto che il campo è algebricamente chiuso, vale il Nullstellensatz di Hilbert e quindi esiste un intero $m\geq 1$ tale che $f^m \in \mathrm{I}$, cioè f appartiene a $\sqrt{\mathrm{I}}$. C.V.D.

Il Nullstellensatz di Hilbert unito alla terminologia dei radicali permette anche di dare una dimostrazione del teorema di chiusura (annunciato nel Capitolo VII teorema 6.5).

Siano $\mathrm{I} = \langle f_1, \ldots, f_s\rangle$ un ideale di $k[x_1, \ldots, x_n]$, $\mathrm{I}_h = \mathrm{I}\cap k[x_{h+1}, \ldots, x_n]$ l'ideale di eliminazione h-esima di I e π_h: $k^n \to k^{n-h}$ la proiezione sulle ultime $n-h$ componenti. Osserviamo innanzi tutto che per il lemma 3.2 (i) il radicale $\sqrt{\mathrm{I}_h}$ di I_h in $k[x_{h+1}, \ldots, x_n]$ è contenuto nell'ideale $I((V(\mathrm{I}_h))$ di $k[x_{h+1}, \ldots, x_n]$ che a sua volta è contenuto in $I(\pi_h(V(\mathrm{I})))$, poiché $V(\mathrm{I}_h)$ contiene $\pi_h(V(\mathrm{I}))$. Se il campo k è algebricamente chiuso vale anche il viceversa, cioè con la terminologia appena usata:

LEMMA 4.1 *Se k è un campo algebricamente chiuso e* $\mathrm{I} = \langle f_1, \ldots, f_s\rangle$ *un ideale di* $k[x_1, \ldots, x_n]$, *il radicale* $\sqrt{\mathrm{I}_h}$ *di* I_h *in* $k[x_{h+1}, \ldots, x_n]$ *contiene l'ideale* $I(\pi_h(V(\mathrm{I})))$ *di* $k[x_{h+1}, \ldots, x_n]$.

Dimostrazione Sia f un polinomio di $I(\pi_h(V(\mathrm{I})))$: esso si annulla in ogni punto $(c_1, \ldots, c_h, c_{h+1}, \ldots, c_n)$ di $V(\mathrm{I})$ in quanto non contiene le prime h variabili e sulle altre si annulla per definizione; quindi f può essere pensato come polinomio di $I(V(\mathrm{I}))$. Allora, per il Nullstellensatz di Hilbert esiste un intero $m\geq 1$ tale che $f^m \in \mathrm{I}$ anzi a I_h, poiché $f \in k[x_{h+1}, \ldots, x_n]$. Dunque f sta in $\sqrt{\mathrm{I}_h}$. C.V.D.

LEMMA 4.2 *Sia k un campo arbitrario. Per ogni ideale* I *in* $k[x_1, \ldots, x_n]$ *risulta* $V(\mathrm{I}) = V(\sqrt{\mathrm{I}})$.

Dimostrazione Per il lemma 3.2(i) si ha $\mathrm{I} \subseteq \sqrt{\mathrm{I}} \subseteq I(V(\mathrm{I}))$: applicando la proprietà 1.3 b) e l'osservazione 2.4 c) del Capitolo VI, si trova allora $V(\mathrm{I}) \supseteq V(\sqrt{\mathrm{I}}) \supseteq V(I(V(\mathrm{I}))) = V(\mathrm{I})$. C.V.D.

TEOREMA DI CHIUSURA *Siano k un campo algebricamente chiuso e* $\mathrm{I} = \langle f_1, \ldots, f_s\rangle$ *un ideale di* $k[x_1, \ldots, x_n]$. *Con la simbologia utilizzata nel lemma 4.1,* $V(\mathrm{I}_h)$ *è la chiusura di Zariski di* $\pi_h(V(\mathrm{I}))$ *e quindi è la più piccola varietà affine di* k^{n-h} *contenente* $\pi_h(V(\mathrm{I}))$.

Dimostrazione Ricordiamo che nel lemma 6.2 del Capitolo VII si è provato che, qualunque sia il campo k, nello spazio affine k^{n-h} risulta $\pi_h(V(\mathrm{I})) \subseteq V(\mathrm{I}_h)$: quindi la chiusura di Zariski $V(I(\pi_h(V(\mathrm{I}))))$ di $\pi_h(V(\mathrm{I}))$ è contenuta in $V(\mathrm{I}_h)$. Viceversa, per il lemma 4.1, $\sqrt{\mathrm{I}_h} \supseteq I(\pi_h(V(\mathrm{I})))$ e quindi $V(I(\pi_h(V(\mathrm{I}))))$ contiene $V(\sqrt{\mathrm{I}_h})$ che coincide con $V(\mathrm{I}_h)$ per il lemma 4.2. C.V.D.

5. ANCORA SUI RADICALI

Vogliamo vedere che cosa succede componendo l'operatore "radicale" con altre operazioni tra ideali (intersezione, prodotto, somma…).

---

(6) L'ipotesi che il campo sia algebricamente chiuso è indispensabile. Ad esempio in $\mathbf{R}[x]$ si ha $I(V(\langle x^2+1\rangle)) = I(\varnothing) = \mathbf{R}[x]$, mentre $\sqrt{\langle x^2+1\rangle} = \langle x^2+1\rangle$, poiché $\mathbf{R}[x]$ è un PID (vedi Capitolo II) e se $[f(x)]^m = (x^2+1)g(x)$ il polinomio x^2+1, essendo irriducibile, deve dividere almeno uno dei fattori di $[f(x)]$ cioè di $f(x)$: ne segue che f sta in $\langle x^2+1\rangle$.

PROPOSIZIONE 5.1 *Siano* I *e* J *due ideali di* $k[x_1,\ldots, x_n]$. *Si ha* $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$. *Ne consegue che l'intersezione di due ideali radicali è un ideale radicale.*

Dimostrazione Se $f\in\sqrt{I\cap J}$ esiste un intero positivo m tale che f^m appartenga a I∩J e quindi tanto a I che a J: dunque f appartiene all'intersezione dei due radicali. Viceversa, se f appartiene all'intersezione dei due radicali, esistono due interi positivi m e M tali che f^m appartenga a I e f^M appartenga a J: basta allora prendere come esponente il maggiore tra m e M per trovare una potenza di f che appartiene a I∩J e quindi $f\in\sqrt{I\cap J}$. Infine I e J se sono ideali radicali coincidono con il loro radicale (lemma 3.2 (iv)) e quindi $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}=I\cap J$, cioè I∩J è un ideale radicale. C.V.D.

Per le successive considerazioni sulle varietà è anche utile esaminare il radicale del prodotto di due ideali.

Ricordiamo che (vedi Capitolo VI) si dice ***prodotto di due ideali*** I, J di $k[x_1,\ldots, x_n]$ l'ideale generato dall'insieme di tutti i prodotti di un elemento di I e di uno di J o, equivalentemente, se $I=\langle f_1,\ldots,f_s\rangle$ e $J=\langle g_1,\ldots, g_t\rangle$, l'ideale generato da tutti gli $s\cdot t$ prodotti $f_i\cdot g_j$ di generatori dei due ideali.

In particolare, se I = J, l'ideale prodotto si indica con I^2 e può non coincidere con I, se I è un ideale proprio [(7)]: ad esempio, se $I=\langle f\rangle$ e f non è nullo né costante, $I^2\neq I$.

Ciò mostra che *il prodotto di due ideali radicali può non essere radicale*: infatti, l'ideale I^2 contiene i quadrati dei generatori di I, onde $\sqrt{I^2}$ contiene I e coincide con I se I è un ideale radicale; dunque, se I è un ideale radicale diverso da I^2, si ha $\sqrt{I^2}\neq I^2$. Vale comunque la seguente

PROPOSIZIONE 5.2 *Siano* I *e* J *due ideali di* $k[x_1,\ldots, x_n]$. *Si ha*

(a) $\sqrt{I\cdot J}=\sqrt{I\cap J}$

(b) $\sqrt{I}\cdot\sqrt{J}\subseteq\sqrt{I\cdot J}$, *ma non sempre vale l'uguaglianza*

(c) $\sqrt{\sqrt{I}\cdot\sqrt{J}}=\sqrt{I\cdot J}$.

Dimostrazione (a) Poiché l'ideale I · J è contenuto in I∩J, risulta $\sqrt{I\cdot J}\subseteq\sqrt{I\cap J}$. Viceversa se $f\in\sqrt{I\cap J}$ esiste un intero $m>0$ tale che f^m appartiene tanto a I che a J e quindi f^{2m} appartiene a I·J.

(b) $\sqrt{I}\cdot\sqrt{J}\subseteq\sqrt{I}\cap\sqrt{J}=\sqrt{I\cap J}=\sqrt{I\cdot J}$, per le proposizione 5.1 e 5.2 parte (a). Che non valga l'uguaglianza è provato dal ragionamento che precede la proposizione.

(c) Poiché ogni ideale è contenuto nel suo radicale, $I\cdot J\subseteq\sqrt{I}\cdot\sqrt{J}$ e quindi $\sqrt{I\cdot J}\subseteq\sqrt{\sqrt{I}\cdot\sqrt{J}}$; d'altra parte, applicando il lemma 3.2(vi) all'inclusione (b), si vede che vale $\sqrt{I\cdot J}\supseteq\sqrt{\sqrt{I}\cdot\sqrt{J}}$. C.V.D.

PROPOSIZIONE 5.3 *Siano* I *e* J *due ideali di* $k[x_1,\ldots, x_n]$. *Si ha*

(a) $\sqrt{I}+\sqrt{J}\subseteq\sqrt{I+J}$, *ma non sempre vale l'uguaglianza*

(b) $\sqrt{\sqrt{I}+\sqrt{J}}=\sqrt{I+J}$.

Dimostrazione (a) Da $I\subseteq I+J$ segue $\sqrt{I}\subseteq\sqrt{I+J}$ e analogamente per J. L'uguaglianza non vale poiché ad esempio in $k[x, y]$ i due ideali $I=\langle x\rangle$ e $J=\langle x-y^2\rangle$ sono radicali, in quanto i polinomi generatori sono irriducibili, ma $I+J=\langle x, y^2\rangle$ ha radicale $\langle x, y\rangle$.

(b) Da $\sqrt{I}+\sqrt{J}\subseteq\sqrt{I+J}$ si ricava $\sqrt{\sqrt{I}+\sqrt{J}}\subseteq\sqrt{I+J}$; viceversa, poiché ogni ideale è contenuto nel suo radicale, $I+J\subseteq\sqrt{I}+\sqrt{J}$ e quindi $\sqrt{I+J}\subseteq\sqrt{\sqrt{I}+\sqrt{J}}$ C.V.D.

---

(7) Attenzione: in altri anelli la cosa può non risultare vera: ad esempio in $\mathbf{Z}_6$ l'ideale I generato dalla classe di resto [2] coincide con I^2, poiché quest'ultimo ideale contiene $[2]^2=[4]$, $[2]\cdot[4]=[2]$, $[2]\cdot[0]=[0]$.

6. SULLA CORRISPONDENZA TRA IDEALI E VARIETÀ

Si è già visto nel Capitolo VI (primi due paragrafi) che comunque sia fatto il campo k le due corrispondenze

$$I\text{: Varietà algebriche affini } \rightarrow \text{ Ideali di } k[x_1,\ldots, x_n]$$

definita da

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

e

$$V\text{: Ideali di } k[x_1,\ldots, x_n] \rightarrow \text{ Varietà algebriche affini}$$

definita da

$$V(\mathrm{I}) = \{\mathbf{c} \in k^n \mid f(\mathbf{c}) = 0 \ \forall\ f \in \mathrm{I}\}$$

sono mappe univoche che rovesciano le inclusioni e la V è l'inversa sinistra della I, nel senso che $V(I(\mathrm{V})) = \mathrm{V}$: ciò dice che I è una funzione iniettiva.
Si è inoltre dimostrato (lemma 4.3) che $V(\mathrm{I}) = V(\sqrt{\mathrm{I}})$.

Aggiungendo l'ipotesi che il campo sia algebricamente chiuso non si può comunque mostrare che V sia iniettiva ma vale la seguente

PROPOSIZIONE 6.1 *Se il campo k è algebricamente chiuso e si restringono le corrispondenze I e V agli ideali radicali, le mappe I e V sono due biiezioni, una inversa dell'altra.*

Dimostrazione $I(\mathrm{V})$ è un ideale radicale quindi si può effettivamente pensare di restringere il codominio di I e il dominio di V agli ideali radicali. Visto che si ha sempre $V(I(\mathrm{V})) = \mathrm{V}$, basta provare che $I(V(\mathrm{I})) = \mathrm{I}$, per ogni ideale radicale I: d'altra parte, per tali ideali si ha $\sqrt{\mathrm{I}} = \mathrm{I}$ e per il Nullstellensatz forte: $I(V(\mathrm{I})) = \sqrt{\mathrm{I}}$. Dunque le due mappe sono una l'inversa dell'altra. C.V.D.

Dunque i problemi sulle varietà possono essere riformulati in termini algebrici come problemi sugli ideali radicali e viceversa.
Per questo è stato importante stabilire nel precedente paragrafo che l'intersezione di due ideali radicali è un ideale radicale, mentre in generale non lo sono il prodotto e la somma.

Ricordiamo che si era provato nel Capitolo VI che

(*) $$V(\mathrm{I}+\mathrm{J}) = V(\mathrm{I}) \cap V(\mathrm{J}), \quad V(\mathrm{I} \cap \mathrm{J}) = V(\mathrm{I} \cdot \mathrm{J}) = V(\mathrm{I}) \cup V(\mathrm{J}), \quad I(\mathrm{V} \cup \mathrm{W}) = I(\mathrm{V}) \cap I(\mathrm{W}),$$

mentre in generale si può solo dire che $I(\mathrm{V} \cap \mathrm{W}) \supseteq I(\mathrm{V}) + I(\mathrm{W})$ o anche, visto che $I(\mathrm{V} \cap \mathrm{W})$ è un ideale radicale, $I(\mathrm{V} \cap \mathrm{W}) \supseteq \sqrt{I(\mathrm{V}) + I(\mathrm{W})}$. Se il campo non è algebricamente chiuso, però, anche questa inclusione può risultare propria, come mostra il seguente

ESEMPIO 6.2 In $\mathbf{R}^2$ l'intersezione di $\mathrm{V} = V(y)$, $\mathrm{W} = V(x^2 - y + 1)$ è vuota e quindi $I(\mathrm{V} \cap \mathrm{W}) = \mathbf{R}[x, y]$. Invece $I(\mathrm{V}) = \langle y \rangle$ e $I(\mathrm{W}) = \langle x^2 - y + 1 \rangle$ e quindi $I(\mathrm{V}) + I(\mathrm{W}) = \langle y, x^2 - y + 1 \rangle = \langle y, x^2 + 1 \rangle$. Se il radicale di questo ideale coincidesse con $\mathbf{R}[x, y]$, una potenza di 1… - cioè l'unità stessa - dovrebbe appartenere all'ideale $\langle y, x^2 + 1 \rangle$, cosa impossibile, poiché i generatori con cui è descritto l'ideale costituiscono una base di Gröbner ad esempio rispetto a LEX (con $x > y$) e tra essi non c'è l'unità.
Di passaggio si noti che $\langle y, x^2 + 1 \rangle$ è un ideale radicale!
Infatti sia f un qualunque polinomio di $\mathbf{R}[x, y]$: esso si può scrivere come $yq_1 + (x^2 + 1)q_2 + a_1x + a_0$, ove q_1 e q_2 sono i quozienti e $a_0 + a_1x$ il resto nella divisione di f per y e $x^2 + 1$. Se f appartiene al radicale di $\langle y, x^2 + 1 \rangle$, per il lemma 2.1 l'ideale $\mathrm{L} = \langle y, x^2 + 1, tf - 1 \rangle = \langle y, x^2 + 1, t(a_1x + a_0) - 1 \rangle$ di $\mathbf{R}[x, y, t]$ deve contenere 1. Ora,

- se $a_1 = 0$ la base di Gröbner rispetto a LEX (con $x > y > t$) di L è $\langle y, x^2 + 1, ta_0 - 1 \rangle$ e può contenere 1 solo se è anche $a_0 = 0$;

- in caso contrario si può supporre $a_1 = 1$ e i LT della base di Gröbner di L, che è
$$<y, x + (1+a_0^2)t - a_0, (1+a_0^2)t^2 - 2a_0t + 1>,$$
sono $\{y, x, (1+a_0^2)t^2\}$ e non possono quindi dividere 1.

Dunque i soli polinomi appartenenti al radicale di $<y, x^2+1>$ sono i polinomi di $<y, x^2+1>$.

PROPOSIZIONE 6.3 *Se il campo k è algebricamente chiuso per ogni coppia di varietà* V *e* W *di* k^n *risulta*
$$I(\mathrm{V} \cap \mathrm{W}) = \sqrt{I(\mathrm{V}) + I(\mathrm{W})}$$
Dimostrazione Ricordando che ogni varietà è la varietà di un ideale si può scrivere V = V(I) e W = V(J) e, applicando le (*), risulta
$$I(\mathrm{V} \cap \mathrm{W}) = I(V(\mathrm{I}) \cap V(\mathrm{J})) = I(V(\mathrm{I}+\mathrm{J}))$$
Visto che k è algebricamente chiuso si può applicare il Nullstellensatz forte:
$$I\left(V\left(\mathrm{I}+\mathrm{J}\right)\right) = \sqrt{\mathrm{I}+\mathrm{J}}$$
e, per la proposizione 5.3 (b):
$$\sqrt{\mathrm{I}+\mathrm{J}} = \sqrt{\sqrt{\mathrm{I}} + \sqrt{\mathrm{J}}}$$
da cui, riapplicando il Nullstellensatz forte:
$$\sqrt{\sqrt{\mathrm{I}} + \sqrt{\mathrm{J}}} = \sqrt{I\left(V\left(\mathrm{I}\right)\right) + I\left(V\left(\mathrm{J}\right)\right)} = \sqrt{I(\mathrm{V}) + I(\mathrm{W})}\,.$$
C.V.D.

7. VARIETÀ E IDEALI PARTICOLARI

DEFINIZIONE 7.1 *Una* ***varietà*** *algebrica affine* V *di* k^n *è detta* ***irriducibile*** *se non può essere scritta come unione di due varietà algebriche affini entrambe diverse da* V*, cioè se*
$$\mathrm{V} = \mathrm{V}_1 \cup \mathrm{V}_2 \quad (\text{con } \mathrm{V}_1, \mathrm{V}_2 \text{ varietà algebriche affini}) \quad \Rightarrow \quad \mathrm{V}_1 = \mathrm{V} \text{ o } \mathrm{V}_2 = \mathrm{V}$$
o anche
$$\mathrm{V} = \mathrm{V}_1 \cup \mathrm{V}_2 \quad (\text{con } \mathrm{V}_1, \mathrm{V}_2 \text{ varietà algebriche affini}) \quad \text{e } \mathrm{V}_1 \neq \mathrm{V} \quad \Rightarrow \quad \mathrm{V}_2 = \mathrm{V}.$$

È tutto sommato abbastanza facile mostrare che una varietà è riducibile (basta evidenziare due varietà diverse da V la cui unione dia V) mentre non lo è garantire l'irriducibilità per via geometrica. Ne cerchiamo perciò una traduzione algebrica.

PROPOSIZIONE 7.2 *Sia* V *una varietà algebrica affine di* k^n*. Essa è irriducibile se e solo se* I(V) *è un ideale primo di* $k[x_1,\ldots, x_n]$.

Dimostrazione Sia V una varietà irriducibile. Se $fg \in I(\mathrm{V})$ consideriamo le varietà $\mathrm{V}_1 = \mathrm{V} \cap V(f)$ e $\mathrm{V}_2 = \mathrm{V} \cap V(g)$: ogni punto **c** di V appartiene ad almeno una di esse. Infatti se $fg(\mathbf{c}) = 0$ e $f(\mathbf{c}) \neq 0$ allora $g(\mathbf{c}) = 0$. Ora se $f \notin I(\mathrm{V})$ c'è almeno un **c** appartenente a $\mathrm{V} \setminus \mathrm{V}_1$ e quindi, per l'irriducibilità di V si ha $\mathrm{V}_2 = \mathrm{V}$, cioè $V(g) \supseteq \mathrm{V}$: ne segue $I(V(g)) \subseteq I(\mathrm{V})$ ed in particolare g appartiene a I(V), che quindi risulta primo.

Viceversa, sia V riducibile, cioè $\mathrm{V} = \mathrm{V}_1 \cup \mathrm{V}_2$ ove $\mathrm{V}_1 \neq \mathrm{V} \neq \mathrm{V}_2$. Poiché la corrispondenza I inverte le inclusioni (e manda varietà diverse in ideali diversi), risulta $I(\mathrm{V}) \subset I(\mathrm{V}_1)$ e $I(\mathrm{V}) \subset I(\mathrm{V}_2)$: esistono quindi un polinomio $f \in I(\mathrm{V}_1) \setminus I(\mathrm{V})$ e un polinomio $g \in I(\mathrm{V}_2) \setminus I(\mathrm{V})$: il loro prodotto fg si annulla su tutto V (poiché il fattore f si annulla su V_1 e il fattore g si annulla su V_2) e quindi appartiene a I(V) che quindi non è primo. C.V.D.

COROLLARIO 7.3 *Se k è un campo algebricamente chiuso, la corrispondenza biunivoca tra varietà algebriche affini e ideali radicali* (*data dalle due mappe V e I*) *induce una corrispondenza biunivoca tra l'insieme delle varietà irriducibili di* k^n *e gli ideali primi di* $k[x_1, \ldots, x_n]$.

Diamo qui di seguito qualche esempio di varietà affine irriducibile

PROPOSIZIONE 7.4 *Sia k un campo infinito. Una varietà* V *di* k^n *definita parametricamente dalle equazioni polinomiali*

$$x_1 = f_1(t_1, \dots, t_m), \dots, x_n = f_n(t_1, \dots, t_m) \qquad con\ f_i \in k[t_1, \dots, t_m]$$

è irriducibile.

Dimostrazione Ricordiamo (vedi Capitolo VII, §7 e seguenti) che quando si parla di varietà V definita parametricamente si intende la minima varietà che contiene l'insieme di punti descritti dalla parametrizzazione [(8)]. Posto per brevità $(f_1(t_1,\dots, t_m),\dots, f_n(t_1,\dots, t_m)) = \mathrm{F}(t_1,\dots, t_m)$, la varietà V è la chiusura di Zariski di $\mathrm{F}(k^m)$ e $I(\mathrm{V}) = I(\mathrm{F}(k^m))$ (vedi capitolo 6, osservazione 2.6).

Allora, per ogni $\varphi \in I(\mathrm{V})$ la funzione composizione $\varphi\circ\mathrm{F}$ si annulla su tutto k^m e quindi, essendo il campo infinito, è il polinomio nullo di $k[t_1,\dots, t_m]$. Dunque, se $gh \in I(\mathrm{V})$ si ha

$$[(gh)\circ\mathrm{F}](t_1,\dots, t_m) = (g(\mathrm{F}(t_1,\dots, t_m)) \cdot (h(\mathrm{F}(t_1,\dots, t_m)) \equiv 0$$

e quindi almeno uno dei due fattori, supponiamo ad esempio $g(\mathrm{F}(t_1,\dots, t_m)$, è il polinomio nullo. Dunque la corrispondente funzione è nulla, cioè $g \in I(\mathrm{F}(k^m)) = I(\mathrm{V})$. Ne segue che $I(\mathrm{V})$ è primo e quindi V è irriducibile. C.V.D.

PROPOSIZIONE 7.5 *Sia k un campo infinito. È irriducibile ogni varietà* V *di* k^n *definita da una parametrizzazione razionale*

$$x_1 = f_1/g_1, \dots, x_n = f_n/g_n \qquad con\ f_i\ e\ g_i \in k[t_1,\dots, t_m].$$

Dimostrazione Poniamo $g = g_1\cdot\ldots\cdot g_n$ e $\mathrm{W} = V(g)$. Allora se $\mathrm{F}(t_1,\dots, t_m) = (f_1/g_1,\dots, f_n/g_n)$, la funzione F è definita su $k^m \setminus \mathrm{W}$ e V è la chiusura di Zariski [(9)] di $\mathrm{F}(k^m \setminus \mathrm{W})$ e

$$I(\mathrm{V}) = \{h \in k[x_1,\dots, x_n] \mid (h\circ\mathrm{F})(t_1,\dots, t_m) = 0\ \forall (t_1,\dots, t_m) \in k^m \setminus \mathrm{W}\ \}$$

Siano dunque p e q due polinomi di $k[x_1,\dots,x_n]$ tali che $pq \in I(\mathrm{V})$. Fare la composizione $[(pq)\circ\mathrm{F}]$ significa sostituire ogni x_i in pq con f_i/g_i e quindi alla fine trovarsi con una funzione razionale fratta in cui al denominatore comparirà g al più elevato al grado totale di pq. Ora, se M e N sono i gradi totali di p e q, il grado totale del loro prodotto è M+N e quindi

$$g^{\mathrm{M+N}}\cdot [(pq)\circ\mathrm{F}](t_1,\dots, t_m) = [g^{\mathrm{M}}\cdot(p(\mathrm{F}(t_1,\dots, t_m))]\cdot [g^{\mathrm{N}}\cdot(q(\mathrm{F}(t_1,\dots, t_m))]$$

è un polinomio di $k[t_1,\dots, t_m]$, anzi il suo polinomio nullo, poiché $pq \in I(\mathrm{V})$ e il campo è infinito. Quindi uno dei due fattori, ad esempio $g^{\mathrm{M}}\cdot(p(\mathrm{F}(t_1,\dots, t_m))$, deve essere il polinomio nullo e quindi anche la corrispondente funzione definita su $k^m \setminus \mathrm{W}$ deve essere nulla. D'altra parte su tale insieme g non si annulla mai e quindi su $k^m \setminus \mathrm{W}$ deve annullarsi la funzione $p(\mathrm{F}(t_1,\dots, t_m))$, cioè $p \in I(\mathrm{V})$. Ne segue che $I(\mathrm{V})$ è primo e quindi V è irriducibile. C.V.D.

Ci occupiamo per finire di varietà molto semplici: i punti **c** di k^n. Ovviamente ognuno di essi è una varietà irriducibile e quindi sicuramente i corrispondenti ideali $I(\mathbf{c})$ sono primi. In realtà sono addirittura massimali:

PROPOSIZIONE 7.6 *Sia k un campo arbitrario. Per ogni scelta di* $\mathbf{c} = (c_1,\dots, c_n)$ *in* k^n:

(a) *l'ideale* $\mathrm{I} = \langle x_1 - c_1, \dots, x_n - c_n \rangle$ *è massimale*

(b) *l'ideale della varietà* $\{\mathbf{c}\}$ *è* $\langle x_1 - c_1, \dots, x_n - c_n \rangle$.

---

(8) Ad esempio, al variare di t, le equazioni $x=1+t^2$ e $y=t(1+t^2)$ descrivono tutti i punti della cubica di equazione $x^2(x-1)=y^2$ tranne l'origine.

(9) $\mathrm{V}=V(\mathrm{J}_{m+1})$ ove J_{m+1} è l'ideale di eliminazione $(m+1)$-esima dell'ideale $\mathrm{J}=\langle g_1x_1-f_1, \dots, g_nx_n-f_n, 1-gy\rangle$ di $k[y, t_1,\dots, t_m, x_1,\dots,x_n]$.

Dimostrazione (a) Se J è un ideale che contiene I propriamente, esiste un polinomio $f \in$ J \ I: applicando l'algoritmo della divisione trovo un resto che appartiene a J ma è un elemento di k diverso da 0: dunque J è tutto $k[x_1,\ldots, x_n]$.
(b) ogni polinomio $x_i - c_i$ sta in $I(\{\mathbf{c}\})$ poiché si annulla sul punto. Quindi $I(\{\mathbf{c}\})$, che non coincide con $k[x_1,\ldots, x_n]$ visto che non contiene 1, contiene I che è massimale: ne segue che i due ideali sono uguali. C.V.D.

Non è però vero in generale che ogni ideale massimale sia l'ideale di un punto.

ESEMPIO 7.7 In $\mathbf{R}[x]$ l'ideale $I = \langle x^2+1\rangle$ ha come varietà associata $V(I)$ l'insieme vuoto e non può essere quindi $I = I(\{\mathbf{c}\})$ in quanto $V(I(\{\mathbf{c}\})) = \{\mathbf{c}\}$. D'altra parte l'ideale I è massimale: infatti se un ideale J lo contiene propriamente e $f \in$ J \ I si può pensare che f abbia grado ≤ 1 (altrimenti calcolo il resto nella divisione per x^2+1) e che tra i generatori di J ci siano tanto x^2+1 che f. D'altra parte $\mathbf{R}[x]$ è un PID e quindi J è generabile con un sol polinomio, che deve essere almeno il MCD di x^2+1 e f, i quali però sono primi tra loro: dunque J coincide con $\mathbf{R}[x]$.

TEOREMA 7.8 *Sia k un campo algebricamente chiuso. Ogni ideale massimale di* $k[x_1,\ldots, x_n]$ *ha la forma* $\langle x_1 - c_1, \ldots, x_n - c_n\rangle$, *per opportuni* c_i *in k.*
Dimostrazione Sia I un ideale massimale di $k[x_1,\ldots, x_n]$: poiché non coincide con $k[x_1,\ldots, x_n]$, esiste almeno un punto $\mathbf{c}$ in $V(I)$ (contronominale del Nullstellensatz debole: $V(I) = \varnothing \Rightarrow I = k[x_1,\ldots,x_n]$).
Da $\{\mathbf{c}\} \subseteq V(I)$ si deduce $\langle x_1 - c_1, \ldots, x_n - c_n\rangle = I(\{\mathbf{c}\}) \supseteq I(V(I))$ e poiché $I(V(I)) \supseteq I$ che è massimale si ottiene che $I = \langle x_1 - c_1, \ldots, x_n - c_n\rangle$. C.V.D.

Dunque, se k è algebricamente chiuso c'è corrispondenza biunivoca tra i punti di k^n e gli ideali massimali di $k[x_1,\ldots, x_n]$.

OSSERVAZIONE 7.9 *Se k non è algebricamente chiuso esiste sicuramente un ideale massimale* I *in* $k[x_1,\ldots, x_n]$ *tale che* $V(I) = \varnothing$.
Infatti consideriamo $I = \langle f(x_1), x_2,\ldots, x_n\rangle$ ove f è un polinomio irriducibile di $k[x_1]$ che non ha radici in k.
Osserviamo che

- $I \neq k[x_1,\ldots, x_n]$ poiché abbiamo espresso I come generato da una base di Gröbner ridotta rispetto a LEX (ogni generatore contiene una sola indeterminata!) e tale base non contiene 1
- I è massimale poiché se g è un polinomio che non sta in I, al più operando la divisione di g per la base di I, possiamo pensare g come polinomio nella sola x_1 di grado $\leq \deg(f(x_1))$ e quindi primo con il polinomio irriducibile $f(x_1)$. Allora l'ideale $\langle f\rangle + \langle g\rangle$ di $k[x_1]$ contiene l'unità 1 e a maggior ragione la contiene $I + \langle g\rangle$ che quindi esaurisce $k[x_1,\ldots, x_n]$.

Ne consegue che se k non è algebricamente chiuso si possono dare due casi per le varietà degli ideali massimali I di $k[x_1,\ldots, x_n]$:
1) $V(I) \neq \varnothing$ e allora $I = \langle x_1 - c_1, \ldots, x_n - c_n\rangle$;
2) $V(I) = \varnothing$ e allora l'ideale può essere fatto in molti modi.

Val la pena di notare per finire che il teorema sulla forma degli ideali massimali equivale al Nullstellensatz debole. Infatti, supponendo di sapere che gli ideali massimali in $k[x_1,\ldots, x_n]$ abbiano tutti la forma $\langle x_1 - c_1, \ldots, x_n - c_n\rangle$ possiamo far vedere che se I è un ideale diverso da $k[x_1,\ldots, x_n]$ allora $V(I) \neq \varnothing$. Basta osservare che esiste un ideale massimale $\langle x_1 - c_1, \ldots, x_n - c_n\rangle$ che contiene I e quindi $V(I)$ contiene almeno la varietà $\{\mathbf{c}\}$ associata a $\langle x_1 - c_1, \ldots, x_n - c_n\rangle$: dunque non è vuota.

8. SCOMPOSIZIONE DI UNA VARIETÀ IN COMPONENTI IRRIDUCIBILI

La validità della condizione catenaria ascendente sugli ideali di $k[x_1,\ldots, x_n]$ implica quella della condizione catenaria discendente sulle varietà algebriche affini:

PROPOSIZIONE 8.1 *Ogni catena strettamente discendente di varietà algebriche affini*

$$V_1 \supset V_2 \supset \ldots \supset V_n \supset \ldots \qquad \text{con } V_i \neq V_j \text{ per ogni } i \neq j$$

di k^n *deve essere finita, cioè da un certo indice n in poi risulta* $V_n = V_{n+1} = V_{n+2} = \ldots$

Dimostrazione È noto che la mappa I che ad ogni varietà associa l'ideale della varietà rovescia le inclusioni ed è iniettiva, per cui a varietà distinte corrispondono ideali distinti. Di conseguenza alla catena strettamente discendente di varietà corrisponde una catena strettamente ascendente di ideali

$$I(V_1) \subset I(V_2) \subset \ldots \subset I(V_n) \subset \ldots \qquad \text{con } I(V_i) \neq I(V_j) \text{ per ogni } i \neq j$$

che è necessariamente finita, per la c.c.a. sugli ideali. D'altra parte per ogni indice i risulta $V(I(V_i))=V_i$ e quindi dal fatto che da un certo indice n in poi risulta $I(V_n) = I(V_{n+1}) = I(V_{n+2}) = \ldots$ si ricava che da un certo indice n in poi anche $V_n = V_{n+1} = V_{n+2} = \ldots$ C.V.D.

Ne segue che

COROLLARIO 8.2 *Ogni varietà algebrica affine* V *di* k^n *può essere scritta come unione finita di varietà irriducibili.*

Dimostrazione In caso contrario V non solo non potrebbe essere irriducibile, ma potrebbe essere scritta V come unione di due varietà distinte da V

$$V = V_1 \cup V_1'$$

almeno una della quali, ad es. V_1, unione non finita di varietà irriducibili.
Lo stesso discorso si può ripetere allora per $V_1 = V_2 \cup V_2'$ e, iterando, si potrebbe scrivere una catena infinita strettamente discendente di varietà $V_1 \supset V_2 \supset \ldots \supset V_n \supset \ldots$ con $V_i \neq V_j$ per ogni $i \neq j$: assurdo. C.V.D.

ESEMPIO 8.3 La varietà $V = V(xz - y^2, x^3 - yz)$ di $\mathbf{R}^3$ si scompone nell'asse z e in un'altra varietà che si può rappresentare parametricamente come $x = t^3$, $y = t^4$, $z = t^5$ (basta risolvere il sistema usando una base di Gröbner rispetto a LEX) e quindi è una varietà irriducibile (vedi proposizione 7.4).

DEFINIZIONE 8.4 *Sia* V *una varietà algebrica affine di* k^n*. Una sua scomposizione*

$$V = V_1 \cup V_2 \cup \ldots \cup V_m$$

come unione finita di varietà si dice ***scomposizione minimale di*** V *se*

i) *ogni varietà* V_i *è irriducibile*

ii) *varietà distinte non sono contenute una nell'altra, cioè se* $V_i \subseteq V_j$ *allora* $i = j$ *e* $V_i = V_j$.

TEOREMA 8.5 *Ogni varietà algebrica affine* V *di* k^n *ammette una scomposizione minimale ed essa è unica, a meno dell'ordine delle componenti* [(10)] .

Dimostrazione Si è visto nel corollario 8.2 che è possibile scrivere V come unione finita di varietà irriducibili

$$V = V_1 \cup V_2 \cup \ldots \cup V_m$$

e rimuovendo da questa rappresentazione le eventuali varietà contenute in altre (e quindi inessenziali) si ha una scomposizione minimale.

[(10)] Si può garantire che la rappresentazione è unica solo perché l'unione è finita. Infatti, se k è infinito, l'intero piano k^2 si può scrivere come unione dei suoi infiniti punti ma anche come unione delle infinite rette passanti per un suo punto fissato.

Se $V = V_1' \cup V_2' \cup \ldots \cup V_l'$ è un'altra scomposizione minimale, per ogni $i \in \{1,\ldots, l\}$ si ha

$$V_i' = V \cap V_i' = (V_1 \cap V_i') \cup (V_2 \cap V_i') \cup \ldots \cup (V_m \cap V_i')$$

e, poiché V_i' è irriducibile, esiste un $j \in \{1,\ldots,m\}$ tale che $V_i' = V_j \cap V_i'$, cioè $V_i' \subseteq V_j$.
Similmente, a partire da V_j, si ricava che esiste un $k \in \{1,\ldots, l\}$ tale che $V_j \subseteq V_k'$; quindi

$$V_i' \subseteq V_j \subseteq V_k'$$

e, visto che le varietà in esame sono irriducibili e la scomposizione è minimale, deve risultare $i=k$ e di conseguenza $V_i' = V_j$.
Dunque ogni varietà della seconda rappresentazione fa parte anche della prima.
Rovesciando il ragionamento si vede che nella prima non ci sono varietà che non appartengano alla seconda, e quindi l'unicità della rappresentazione resta provata. C.V.D.

Passiamo ora ad una rilettura algebrica di quanto visto.

LEMMA 8.6 *Sia* I *un ideale di* $k[x_1,\ldots, x_n]$. *Il radicale di* I *è l'intersezione degli ideali primi che contengono* I.

Dimostrazione Se P è un ideale primo che contiene I risulta $\sqrt{I} \subseteq \sqrt{P} = P$: quindi il radicale di I è contenuto nell'intersezione dei primi che contengono I.
Viceversa mostriamo che se $f \in k[x_1,\ldots, x_n]$ non appartiene al radicale di I (cioè nessuna sua potenza appartiene a I) c'è almeno un ideale primo che contiene I e non contiene f.
Allo scopo consideriamo la famiglia di ideali di $k[x_1,\ldots, x_n]$

$$\Im = \{J |\ J \supseteq I \text{ e per ogni } m>0, f^m \notin J\}$$

che non è vuota in quanto contiene almeno l'ideale I e quindi per il lemma di Zorn [(11)] ha almeno un elemento massimale: denotiamo con P questo ideale e mostriamo che è primo, facendo vedere che un prodotto di polinomi gh non può appartenere a P se nessuno dei due polinomi sta in P.
Siano dunque $g, h \in k[x_1,\ldots, x_n] \setminus P$: i due ideali $P+\langle g\rangle$ e $P+\langle h\rangle$ contengono P propriamente e quindi non stanno in $\Im$, poiché P è massimale in $\Im$. Dunque – visto che entrambi gli ideali contengono I e quindi il non appartenere alla famiglia deve essere letto sulla seconda condizione – esistono due interi m e M tali che $f^m \in P+\langle g\rangle$ e $f^M \in P+\langle h\rangle$. Ne segue che $f^{m+M} \in (P+\langle g\rangle)(P+\langle h\rangle) \subseteq P+\langle gh\rangle$, cioè $P+\langle gh\rangle \notin \Im$: quindi gh non può appartenere a P.
Ciò prova che P è primo; inoltre P, in quanto elemento di $\Im$, contiene I e non può contenere f. C.V.D.

Vale l'analogo del Corollario 8.2:

COROLLARIO 8.7 *Ogni ideale radicale* I *di* $k[x_1,\ldots, x_n]$ *può essere scritto come intersezione finita di ideali primi.*

Dimostrazione Infatti ogni ideale radicale coincide con il suo radicale e quindi per il lemma è l'intersezione degli ideali primi che lo contengono. Inoltre supponiamo che l'ideale I non possa essere rappresentato come intersezione finita di primi: allora anche dopo aver scartato gli ideali primi inutili nella rappresentazione (perché contengono l'intersezione degli altri), si rimane con un insieme infinito $\Im$ di ideali primi contenenti I: facendone una partizione in due famiglie, almeno una di queste, $\Im_1$, dovrebbe essere infinita e l'intersezione I_1 dei suoi elementi dovrebbe contenere propriamente l'intersezione I degli elementi di $\Im$. Proseguendo in questo modo si verrebbe a creare una catena infinita strettamente ascendente di ideali $I \subset I_1 \subset I_2 \subset \ldots \subset \ldots$, il che è impossibile per la validità della c.c.a. sugli ideali di $k[x_1,\ldots, x_n]$. C.V.D.

[(11)] Lemma di Zorn: se S è un insieme parzialmente ordinato (in questo caso per inclusione) in cui ogni catena di elementi è dotato di estremo superiore (qui: l'unione di tutti gli ideali della catena) allora S ha almeno un elemento massimale rispetto all'ordinamento scelto.

D'altra parte un'intersezione finita di ideali primi è sicuramente radicale in quanto intersezione di ideali radicali (vedi esempio dopo definizione. 3.1 e proposizione 5.1): quindi un ideale è radicale se e solo se si può scrivere come intersezione finita di ideali primi.

DEFINIZIONE 8.8 *Sia* I *un ideale radicale di* $k[x_1,\ldots, x_n]$. *Una sua rappresentazione*

$$I = P_1 \cap P_2 \cap \ldots \cap P_m$$

come intersezione finita di ideali primi si dice ***scomposizione minimale*** (*o intersezione irridondante*) *di* I *se non esistono in essa due primi distinti contenuti uno nell'altro.*

Anche in questo caso vale un teorema di esistenza e unicità. Premettiamo alla sua dimostrazione qualche breve considerazione sugli ideali primi, che risulterà utile anche nel seguito.

LEMMA 8.9

a) *Un ideale* P *è primo se e solo se allorché contiene il prodotto* IJ *di una coppia di ideali* I, J *ne contiene almeno uno dei due.*
b) *Se un ideale primo* P *contiene l'intersezione di un numero finito di ideali contiene almeno uno di essi.*

Dimostrazione a) Sia P primo. Se il prodotto di due ideali I e J è contenuto in P ma I non è contenuto in P, esiste un $f \in I \setminus P$; allora per ogni $g \in J$ risulta $fg \in IJ \subseteq P$ ma $f \notin P$ e quindi $g \in P$, cioè $J \subseteq P$. Viceversa, se $fg \in P$ ma $f \notin P$, il prodotto $\langle f \rangle\langle g \rangle$ è contenuto in P mentre $\langle f \rangle$ non lo è e quindi, se vale la condizione, si ha $\langle g \rangle \subseteq P$, cioè $g \in P$.
b) Supponiamo che P contenga $I_1 \cap I_2 \cap \ldots \cap I_m$: allora contiene il prodotto $I_1 (I_2 \cap \ldots \cap I_m)$ e quindi per la parte (a) contiene I_1 oppure $(I_2 \cap \ldots \cap I_m)$. Iterando il ragionamento si trova che almeno uno degli I_j è contenuto in P. C.V.D.

TEOREMA 8.10 *Ogni ideale radicale* I *di* $k[x_1,\ldots, x_n]$ *ammette una ed una sola scomposizione minimale come intersezione finita di ideali primi.*

Dimostrazione Si è già visto nel corollario 8.7 che ne ammette una.
L'unicità si prova "come per le varietà". Se

$$I = P_1 \cap P_2 \cap \ldots \cap P_m = P_1' \cap P_2' \cap \ldots \cap P_l',$$

per ogni $i \in \{1,\ldots, l\}$ si ha $P_i' \supseteq P_1 \cap P_2 \cap \ldots \cap P_m$ e quindi per il lemma 8.9 (b) esiste $j \in \{1,\ldots,m\}$ tale che $P_i' \supseteq P_j$.
Similmente, a partire da P_j, si ricava che esiste un $k \in \{1,\ldots, l\}$ tale che $P_j \supseteq P_k'$; quindi

$$P_i' \supseteq P_j \supseteq P_k'$$

e, visto che la scomposizione è minimale, deve risultare $i=k$ e di conseguenza $P_i' = P_j$.
Dunque ogni ideale primo della seconda rappresentazione fa parte anche della prima.
Rovesciando il ragionamento si vede che nella prima non ci sono ideali primi che non appartengano alla seconda, e quindi l'unicità della rappresentazione resta provata. C.V.D.

Il problema è che non abbiamo indicazioni concrete su come sono fatti gli ideali primi che entrano nella rappresentazione, poiché tutti i precedenti enunciati sono basati sulla validità della c.c.a. e quindi del teorema della base di Hilbert, che non è costruttivo. A partire dal 1926 sono stati forniti algoritmi (più o meno efficienti) per decidere se un certo ideale è primo e per trovare la scomposizione minimale in primi di un ideale radicale (o corrispondenti problemi per le varietà).
Nel paragrafo successivo introduciamo uno strumento che permette di gettare uno sguardo ulteriore su queste scomposizioni.

9. QUOZIENTE DI DUE IDEALI E IDEALI RADICALI

Ci proponiamo ora di rispondere alla domanda: "come si possono individuare gli ideali primi che compaiono nella scomposizione minimale di un ideale radicale?" Allo scopo introduciamo la

DEFINIZIONE 9.1 *Siano* I *e* J *due ideali di* $k[x_1,\ldots, x_n]$. *Si dice* ***quoziente di*** **I** ***mediante*** **J** *l'insieme dei polinomi che moltiplicati per qualunque polinomio di* J *danno polinomi di* I

$$I : J = \{f\in k[x_1,\ldots, x_n] \mid \text{per ogni } g\in J \text{ si ha } fg\in I\} = \{f\in k[x_1,\ldots, x_n] \mid f\, J \subseteq I\}.$$

Se l'ideale J è generato da un sol elemento g invece di $I : < g >$ si scrive più semplicemente $I : g$. Notiamo che in questo caso la definizione di quoziente diventa semplicemente

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

poiché, se $fg\in I$, per ogni altro elemento $hg\in J$ si ha $f(hg) = h(fg) \in I$.

OSSERVAZIONE 9.2 *Siano* I, J *e* L *ideali di* $k[x_1,\ldots, x_n]$. *Valgono le seguenti affermazioni:*

(i) $I : J$ *è un ideale di* $k[x_1,\ldots, x_n]$ *contenente* I

(ii) *se* $J \subseteq L$ *allora* $I : J \supseteq I : L$

(iii) $I : k[x_1,\ldots, x_n] = I$

(iv) $J \subseteq I$ *se e solo se* $I : J = k[x_1,\ldots, x_n]$

(v) $JL \subseteq I$ *se e solo se* $L \subseteq I : J$

(vi) $(I : J) : L = I : JL$

La verifica di queste affermazioni è abbastanza banale: solo in (vi) si presti attenzione al fatto che JL è l'ideale generato dai prodotti di elementi di J e di L.

PROPOSIZIONE 9.3 *Siano* $I, I_1, \ldots, I_r, J, J_1, \ldots, J_r$ *ideali di* $k[x_1,\ldots, x_n]$. *Valgono le seguenti affermazioni:*

a) $(I_1 \cap \ldots \cap I_r) : J = (I_1 : J) \cap \ldots \cap (I_r : J)$

b) $I : (J_1 + \ldots + J_r) = (I : J_1) \cap \ldots \cap (I : J_r)$

Dimostrazione (a) per ogni $i\in \{1, \ldots, r\}$ si ha $f\, J \subseteq I_i$ se e solo se $f\, J \subseteq (I_1 \cap \ldots \cap I_r)$.

(b) $I : (J_1 + \ldots + J_r) \subseteq (I : J_1) \cap \ldots \cap (I : J_r)$ poiché $(J_1 + \ldots + J_r) \supseteq J_i$ per ogni $i\in \{1, \ldots, r\}$ e vale l'osservazione 9.2(ii); viceversa, se per ogni $i\in \{1, \ldots, r\}$ si ha $f\, J_i \subseteq I$, anche $f(J_1 + \ldots + J_r) \subseteq I$ e quindi vale l'inclusione opposta. C.V.D.

Possiamo ora affrontare il problema di trovare i generatori dell'ideale quoziente di I mediante J. Innanzi tutto, se $J = < g_1, \ldots, g_r >$, la proposizione 9.3 (b) dice che $I : J = (I : g_1) \cap \ldots \cap (I : g_r)$ e quindi, pur di sapere come calcolare i generatori di $(I : g)$, si può trovare la base di $I : J$ utilizzando $r - 1$ volte l'algoritmo per il calcolo della base dell'intersezione (vedi Capitolo V).
Osserviamo ora che se f appartiene $(I : g)$ esiste in I un elemento che si scrive come fg e quindi appartiene a $I \cap <g>$; se ne deduce che per trovare una base di $(I : g)$ è opportuno fare riferimento ad una base di $I \cap <g>$, come mostra il seguente

TEOREMA 9.4 *Se* $\{h_1, \ldots, h_r\}$ *è una base di* $I \cap <g>$, *allora* $\{h_1 g^{-1}, \ldots, h_r g^{-1}\}$ *è una base di* $I : g$.

Dimostrazione Notiamo che ogni elemento di $I \cap <g>$, e in particolare i generatori, possono essere pensati come prodotti: $h_i = l_i g$. Dunque se f appartiene a $<h_1 g^{-1}, \ldots, h_r g^{-1}> = < l_1, \ldots, l_r >$ allora fg appartiene a $I \cap <g> \subseteq I$ e quindi $f\in (I : g)$. Viceversa se $f\in (I : g)$ si ha $fg \in I \cap <g> = <h_1, \ldots, h_r>$, cioè $fg = a_1h_1 + \ldots + a_rh_r = a_1l_1g + \ldots + a_rl_rg$, da cui $f = a_1l_1 + \ldots + a_rl_r$. C.V.D.

Dunque per trovare una base di $(I : g)$, se $I = < f_1, \dots , f_s >$ basta calcolare la base di Gröbner dell'ideale di eliminazione prima rispetto a LEX $(t > x_1 > \dots > x_n)$ di $< tf_1, \dots , tf_s, (1-t)g >$, ottenendo con ciò una base di $I \cap <g>$ e dividere ogni elemento di tale base per g.

Se l'ideale di cui si fa il quoziente è primo la situazione è ancora più semplice. Infatti

OSSERVAZIONE 9.5 *Sia* P *un ideale primo. Se* $f \in P$ *si ha* $(P : f) = <1>$, *mentre se* $f \notin P$ *si ha* $(P : f) = P$.

Dal teorema 8.10 e dalla proposizione 9.3 (a) segue allora che se I è un ideale radicale ed $f \notin I$

$$I : f = (P_1 \cap \dots \cap P_r) : f = (P_1 : f) \cap \dots \cap (P_r : f)$$

è ancora un ideale radicale, intersezione di almeno una parte degli ideali P_i la cui intersezione dà I. Quest'osservazione suggerisce che gli ideali primi che compaiono nella scomposizione minimale sono correlati con gli ideali quozienti $I : f$ al variare di f in $k[x_1, \dots, x_n]$:

TEOREMA 9.6 *Gli ideali primi* P_i *che compaiono nella scomposizione minimale di un ideale radicale proprio* I *sono esattamente gli ideali primi propri che appartengono alla famiglia*

$$\Im = \{ (I : f), \quad f \in k[x_1, \dots, x_n] \}$$

Dimostrazione Innanzitutto, visto che I è un ideale proprio, i primi che compaiono nella scomposizione minimale devono essere ideali propri.
Ora, se $(I : f) = (P_1 : f) \cap \dots \cap (P_r : f)$ è un ideale primo proprio, esiste un $i \in \{1, \dots, m\}$ per il quale $(I : f) \supseteq (P_i : f)$ (vedi lemma 8.9 (b)) e visto che $(I : f) \subseteq (P_i : f)$ i due ideali devono coincidere; ne consegue che $(P_i : f)$ è un ideale proprio e quindi deve coincidere con P_i. Dunque se $(I : f)$ è un ideale primo proprio esso è uno degli ideali della scomposizione minimale in primi di I.
Viceversa, per vedere che ogni ideale P_i della scomposizione minimale in primi di I ha questa forma, consideriamo un polinomio $f \in (P_1 \cap \dots \cap P_{i-1} \cap P_{i+1} \cap \dots \cap P_r) \setminus P_i$: tale differenza non è vuota poiché la scomposizione è minimale. Risulta $(P_i : f) = P_i$ e $(P_j : f) = <1>$ per ogni $j \neq i$; dunque

$$I : f = (P_1 : f) \cap \dots \cap (P_r : f) = (P_i : f) = P_i$$

C.V.D.

Vedremo parlando di scomposizioni di ideali generici in ideali primari che questo è solo un caso particolare del teorema di Lasker – Nöther.

10. SCOMPOSIZIONE DI IDEALI NON RADICALI IN IDEALI PRIMARI

Non tutti gli ideali di $k[x_1, \dots, x_n]$ sono intersezione di ideali primi (sarebbero ideali radicali) e neanche intersezioni di loro potenze (vedi $<x^2, y>$), come suggerirebbe l'esempio degli ideali di **Z** [(12)]: serve quindi una rappresentazione più evoluta di quella introdotta nel paragrafo 8.

DEFINIZIONE 10.1 *Un ideale proprio* Q *di* $k[x_1, \dots, x_n]$ *è detto* ***ideale primario*** *se ogni volta che* $fg \in Q$ *e* $f \notin Q$ *esiste un intero* $m>0$ *tale che* $g^m \in Q$.

[(12)] Questi ultimi sono tutti principali ed, essendo ogni numero intero scomponibile in maniera unica come prodotto di potenze di fattori irriducibili distinti, sono rappresentabili come intersezione degli ideali generati da ciascuna potenza, cioè come intersezione delle corrispondenti potenze degli ideali generati da ciascun fattore irriducibile.

OSSERVAZIONI 10.2

a) Ogni ideale primo è primario, ma non è vero il viceversa: si veda l'esercizio 8.

b) Un ideale Q è primario se e solo se l'anello quoziente $k[x_1,\ldots, x_n]/Q$ è non nullo e tutti i suoi divisori dello zero (se ce ne sono!) sono nilpotenti, cioè hanno una potenza che è = 0.

LEMMA 10.3 *Se* Q *è un ideale primario, il suo radicale è un ideale primo ed è il più piccolo ideale primo contenente* Q.

Infatti, se $fg\in\sqrt{Q}$ esiste un intero $m>0$ tale che $(fg)^m = f^m g^m \in Q$ e quindi o $f^m\in Q$, cioè $f\in\sqrt{Q}$, oppure esiste un intero $M>0$ tale che $(g^m)^M\in Q$, cioè $g\in\sqrt{Q}$. Inoltre, se $Q\subseteq P$ e P è primo, si ha $\sqrt{Q}\subseteq\sqrt{P} = P$.

DEFINIZIONE 10.4 *Se* Q *è un ideale primario di* $k[x_1,\ldots, x_n]$ *avente radicale* P *si dice che* Q *è* **P-*primario***.

Il radicale di un ideale P^r *potenza di un ideale primo* P *è esattamente* P (poiché ovviamente P è contenuto nel radicale di P^r e se $f^m\in P^r\subseteq P$ allora anche f deve appartenere all'ideale primo P) : ma in generale non è detto che P^r sia primario.

Ad esempio, nell'anello $A = k[x, y, z]/(xy - z^2)$ l'ideale P generato dalle classi laterali $[x]$ e $[z]$ è primo, poiché l'anello quoziente $A/\langle[x], [z]\rangle$ è isomorfo a $k[x, y, z]/\langle x, z\rangle$ che a sua volta è isomorfo al dominio di integrità $k[y]$; ma

- P^2 contiene $[z]^2 = [x][y]$
- $[x]\notin P^2$
- per nessun m risulta $[y]^m\in P^2\subseteq P$ poiché P è primo e $[y]\notin P$.

Invece l'ideale M^r potenza di un ideale massimale M è M-primario. Ciò dipende dalla seguente

PROPOSIZIONE 10.5 *Se il radicale di* I *è un ideale massimale* M*, allora* I *è primario.*

Dimostrazione La scomposizione minimale in primi dell'ideale radicale $\sqrt{I}$ è data proprio da M e quindi M/I è l'unico ideale primo (e massimale) dell'anello $k[x_1,\ldots, x_n]/I$. Ogni elemento non invertibile (e non nullo) dell'anello quoziente genera un ideale proprio che è sicuramente contenuto in un ideale massimale, cioè in M/I. Ne segue che, degli elementi che stanno in $k[x_1,\ldots, x_n]/I$, quelli che non stanno in M/I sono invertibili e quindi non divisori dello zero, mentre gli altri sono nilpotenti, poiché se $f+I\in M/I$ si ha $f\in M$, cioè $f^m\in I$ per qualche intero $m>0$.
Per l'osservazione 10.2 (b) l'ideale I è primario. C.V.D.

DEFINIZIONE 10.6 *Un* ***ideale*** I *di* $k[x_1,\ldots, x_n]$ *è detto* ***irriducibile*** *se* $I = I_1\cap I_2$ *implica* $I = I_1$ *oppure* $I = I_2$.

Ogni ideale primo P è irriducibile poiché se $P = I_1\cap I_2\supseteq I_1 I_2$ e $P\neq I_1$, risulta $P\supseteq I_2$ (per il lemma 8.9 (a)): valendo l'inclusione opposta per motivi insiemistici si vede che $P = I_2$.

Invece *non ogni ideale primario è irriducibile*.
Ad esempio, $\langle x^2, xy, y^2\rangle = \langle x, y\rangle^2$ è primario in $k[x, y]$ in quanto potenza dell'ideale massimale $\langle x, y\rangle$, ma non è irriducibile poiché risulta $\langle x^2, xy, y^2\rangle = \langle x^2, y\rangle\cap\langle x, y^2\rangle$ (si verifica velocemente la coincidenza osservando che la base di Gröbner rispetto a LEX ($t>x>y$) di $< tx^2, ty, tx-x, ty^2-y^2 >$ è $\{tx-x, ty, x^2, xy, y^2\}$ e quindi l'intersezione è generata proprio da x^2, xy, y^2).

Al contrario

PROPOSIZIONE 10.7 *Ogni ideale irriducibile* I *di* $k[x_1,\ldots, x_n]$ *è primario.*

Dimostrazione Supponiamo che I sia un ideale irriducibile e che risulti $fg \in I$ ma $f \notin I$. Per provare che esiste un intero $m>0$ tale che $g^m \in I$, considero gli ideali della forma $(I : g^r)$, con $r>0$: per l'osservazione 9.2 (ii) risulta $(I : g^r) \subseteq (I : g^{r+1})$ comunque si scelga r ma, visto che vale la c.c.a. sugli ideali, la catena deve essere finita, cioè esiste un intero $m>0$ tale che

$$(I : g^m) = (I : g^{m+1}) = (I : g^{m+2}) = \ldots$$

Osserviamo che $(I + <f>) \cap (I + <g^m>) = I$. Infatti ogni elemento dell'intersezione può essere scritto in due modi:

$$i + pf = i' + qg^m, \quad \text{ove } i, i' \in I \quad \text{e} \quad p, q \in k[x_1,\ldots, x_n]$$

da cui, moltiplicando per g, si vede che $qg^{m+1} = ig + pfg - i'g$ appartiene a I, cioè $q \in (I : g^{m+1}) = (I : g^m)$. Dunque $i' + qg^m$ sta in I.

Ciò implica che l'ideale irriducibile I, non potendo coincidere con $(I + <f>)$ visto che $f \notin I$, deve coincidere con $I + <g^m>$: dunque $g^m \in I$. C.V.D.

PROPOSIZIONE 10.8 *Ogni ideale* I *di* $k[x_1,\ldots, x_n]$ *può essere rappresentato come intersezione finita di ideali irriducibili.*

Dimostrazione (Analoga a quella vista per le varietà) Se I non è intersezione di ideali irriducibili, a maggior ragione non è irriducibile e quindi esistono due ideali I_1 e I_1' tali che $I = I_1 \cap I_1'$ ma $I \neq I_1$ e $I \neq I_1'$. A sua volta almeno uno di questi ideali, ad es. I_1, non può essere rappresentato come intersezione finita di irriducibili e quindi il ragionamento si ripete e si viene così a formare una catena infinita strettamente ascendente di ideali: $I \subset I_1 \subset I_2 \subset \ldots$: ciò è impossibile per la validità della c.c.a. sugli ideali e quindi è assurda l'ipotesi iniziale. C.V.D.

Allora, tenuto conto della proposizione 10.7, si vede che ogni ideale I di $k[x_1,\ldots, x_n]$ può essere rappresentato come intersezione finita di ideali primari: si parlerà in questo caso di scomposizione primaria di I.

DEFINIZIONE 10.9 *Una* ***scomposizione primaria*** *di un ideale* I *di* $k[x_1,\ldots, x_n]$

$$I = (Q_1 \cap \ldots \cap Q_r)$$

è detta ***irridondante*** *se*

i) *per ogni scelta degli indici* i *e* j *in* $\{1, \ldots, m\}$, $\sqrt{Q_i} = \sqrt{Q_j}$ *implica* $i = j$

ii) *per ogni* $i \in \{1, \ldots, m\}$, *l'ideale primario* Q_i *non contiene* $(Q_1 \cap \ldots \cap Q_{i-1}) \cap (Q_{i+1} \cap \ldots \cap Q_r)$.

Vogliamo provare che ogni ideale ammette una scomposizione primaria irridondante. Non ci sono problemi a rimuovere da una scomposizione primaria un ideale che contenga l'intersezione degli altri, senza alterare l'ideale I rappresentato, ma che fare degli ideali aventi lo stesso radicale?

LEMMA 10.10 *Se* Q_1 *e* Q_2 *sono primari e* $\sqrt{Q_1} = \sqrt{Q_2}$ *allora* $Q_1 \cap Q_2$ *è primario.*

Infatti supponiamo che $fg \in Q_1 \cap Q_2$ e $f \notin Q_1 \cap Q_2$: ad esempio sia $f \notin Q_1$. Allora esiste un intero $m>0$ tale che $g^m \in Q_1$, cioè $g \in \sqrt{Q_1} = \sqrt{Q_2}$ e quindi esiste un intero $M>0$ tale che $g^M \in Q_2$. Ne segue che $g^{\max(m, M)} \in Q_1 \cap Q_2$, cioè $Q_1 \cap Q_2$ è primario.

Primo TEOREMA di Lasker – Nöther *Ogni ideale* I *di* $k[x_1, \ldots, x_n]$ *ha una scomposizione primaria irridondante.*

Dimostrazione Le proposizioni 10.7 e 10.8 garantiscono l'esistenza di una scomposizione primaria; il lemma 10.10 garantisce che a coppie di ideali che compaiano in essa e abbiano lo stesso radicale P si può sostituire l'ideale intersezione dei due che è ancora primario ed ha come radicale l'intersezione dei due radicali (proposizione 5.1) cioè ancora P: dunque con un numero finito di operazioni di questo tipo ci si riconduce ad una scomposizione in cui tutti i radicali sono diversi; infine rimuovendo gli eventuali ideali primari che contengono l'intersezione dei rimanenti si ha la scomposizione irridondante. C.V.D.

Uno stesso ideale può avere diverse scomposizioni primarie irridondanti. Ad esempio

$$<x^2, xy> = <x> \cap <x^2, xy, y^2> = <x> \cap <x^2, y>.$$

Per cercare qualche forma di unicità bisogna far riferimento agli ideali primi che sono i radicali degli ideali primari che compaiono nelle scomposizioni primarie irridondanti. Vale il

LEMMA 10.11 *Siano* Q *un ideale primario e* P *il suo radicale. Per ogni* $f \in k[x_1, \ldots, x_n]$

i) *se* $f \in$ Q *risulta* $(Q : f) = <1>$

ii) *se* $f \notin$ Q *l'ideale* $(Q : f)$ *è* P*-primario*

iii) *se* $f \notin$ P *risulta* $(Q : f) = Q$

Dimostrazione (i) Vedi osservazione 9.2 (iv).

(ii) Se $gh \in (Q : f)$ e $g \notin (Q : f)$ risulta $fgh \in Q$ e $fg \notin Q$, da cui essendo Q primario si deduce che esiste un intero $m>0$ tale che $h^m \in Q$ e quindi $(Q : f)$ è primario. Il radicale di $(Q : f)$ contiene quello di Q che è P; viceversa, se g appartiene al radicale di $(Q : f)$, esiste un intero $m>0$ tale che $g^m \in (Q : f)$ cioè $fg^m \in Q$ e quindi – avendo ipotizzato $f \notin Q$ e Q primario – esiste un intero $M>0$ tale che $(g^m)^M \in Q$, cioè $g \in \sqrt{Q} = P$. Dunque $(Q : f)$ è P-primario.

(iii) Se $g \in (Q : f)$, cioè $fg \in Q \subseteq P$, ma $f \notin P$ allora non esiste alcun intero $m>0$ tale che $f^m \in Q$ e quindi deve risultare $g \in Q$. C.V.D.

Secondo TEOREMA di Lasker – Nöther *Siano* I *un ideale proprio di* $k[x_1, \ldots, x_n]$ *e*

$$I = (Q_1 \cap \ldots \cap Q_r)$$

una sua scomposizione primaria irridondante. I radicali $P_1, \ldots, P_r$ *degli ideali* $Q_1, \ldots, Q_r$ *sono tutti e soli gli ideali primi propri che appartengono alla famiglia*

$$\Im = \{ \sqrt{(I : f)}, \quad f \in k[x_1, \ldots, x_n] \}$$

e quindi, in particolare, gli ideali $P_1, \ldots, P_r$ *sono indipendenti dalla scomposizione primaria irridondante scelta: per questo essi verranno detti* ***ideali primi appartenenti a*** **I**.

Dimostrazione Osserviamo innanzi tutto che ogni ideale proprio ha radicale proprio (e viceversa): infatti se il radicale di I coincide con $k[x_1, \ldots, x_n]$ contiene 1 e quindi una potenza di 1, cioè 1 stesso, deve stare in I. Inoltre gli ideali primi appartenenti ad un ideale I proprio sono propri. Infatti se I è proprio gli ideali primari della scomposizione irridondante non possono coincidere con l'anello e d'altra parte, come appena ricordato, se un radicale P_i contenesse 1 anche il corrispondente ideale primario Q_i conterrebbe 1. Ricordiamo che per la proposizione 9.3 si ha

$$I : f = (Q_1 \cap \ldots \cap Q_m) : f = (Q_1 : f) \cap \ldots \cap (Q_m : f)$$

e per la proposizione 5.1 il radicale di un'intersezione è l'intersezione dei radicali e quindi $\sqrt{(I : f)}$ è l'intersezione degli ideali $\sqrt{(Q_i : f)}$ su cui ora concentriamo la nostra attenzione. Per il lemma 10.11, se $f \in Q_i$ tale radicale è tutto l'anello, mentre se $f \notin Q_i$ esso coincide con P_i. Allora esiste un indice j tale che $f \notin Q_j \Leftrightarrow f \notin I \Leftrightarrow (I : f)$ è un ideale proprio $\Leftrightarrow \sqrt{(I : f)}$ è un ideale proprio e in questo caso $\sqrt{(I : f)}$ è intersezione di (tutti o una parte degli ideali) P_i.

Ora supponiamo che $\sqrt{(\mathrm{I} : f)}$ sia un ideale primo proprio: per quanto appena detto esso è un'intersezione finita non vuota di ideali P_i e quindi per il lemma 8.9 ne contiene uno anzi, essendo anche contenuto in esso, coincide con esso.
Viceversa, se vogliamo rappresentare un ideale P_j come $\sqrt{(\mathrm{I} : f)}$ basta scegliere f in modo che appartenga all'intersezione di tutti gli ideali primari Q_i diversi da Q_j e non appartenga a Q_j : ciò è sempre possibile, visto che la rappresentazione è irridondante e porta ad avere $(\mathrm{Q}_i : f) = <1>$ per tutti gli indici $i \neq j$ e quindi $\sqrt{(\mathrm{I} : f)} = \sqrt{(\mathrm{Q}_j : f)} = \mathrm{P}_j$. C.V.D.

Vediamo come si traduce il secondo teorema di Lasker – Nöther se I è un ideale radicale. In tal caso anche $(\mathrm{I} : f)$ lo è (poiché da $g^m \in (\mathrm{I} : f)$ si ricava $fg^m \in \mathrm{I}$ e quindi $(fg)^m \in \mathrm{I}$, cioè $fg \in \mathrm{I}$). Inoltre, visto che I coincide con il suo radicale, si ha

$$\mathrm{I} = \sqrt{\mathrm{I}} = \sqrt{\mathrm{Q}_1 \cap \ldots \cap \mathrm{Q}_m} = \sqrt{\mathrm{Q}_1} \cap \ldots \cap \sqrt{\mathrm{Q}_m} = \mathrm{P}_1 \cap \ldots \cap \mathrm{P}_m$$

ove i P_i sono primi distinti: quindi questa è una scomposizione primaria di I.

Mostriamo che essa risulta irridondante cioè che nessun P_i contiene l'intersezione degli altri (che è quanto dire che non ne contiene uno, per il lemma 8.9).
In caso contrario per ottenere una rappresentazione irridondante basterebbe scartare gli eventuali primi che ne contengano un altro: ma questo porterebbe a rimuovere degli ideali primi appartenenti all'ideale I, il che è impossibile visto che proprio secondo teorema di Lasker – Nöther dice che gli ideali primi appartenenti all'ideale sono univocamente individuati: dunque nessun P_i contiene l'intersezione degli altri. Allora

Secondo TEOREMA di Lasker – Nöther per gli ideali radicali *Siano* I *un ideale radicale proprio di* $k[x_1, \ldots, x_n]$ *e*

(*) $$\mathrm{I} = \mathrm{Q}_1 \cap \ldots \cap \mathrm{Q}_r$$

una sua scomposizione primaria irridondante. Allora gli ideali $\mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *sono primi e quindi esiste una sola scomposizione* (*)*, che coincide con la (unica!) scomposizione minimale in primi dell'ideale radicale proprio* I. *Ciascuno degli ideali* $\mathrm{Q}_1, \ldots, \mathrm{Q}_r$ *è un ideale primo appartenente a* I *e non contiene l'intersezione degli altri*. *Essi sono tutti e soli gli ideali primi propri che appartengono alla famiglia*

$$\Im = \{(\mathrm{I} : f), \quad f \in k[x_1, \ldots, x_n] \}.$$

Si vede dunque che il secondo teorema di Lasker – Nöther precisa il contenuto del teorema 9.6.

Per finire osserviamo che questo enunciato non vale per ideali non radicali. Abbiamo già visto che

$$<x^2, xy> = <x> \cap <x^2, xy, y^2> = <x> \cap <x^2, y>$$

ha almeno due scomposizioni primarie irridondanti; ovviamente gli ideali della scomposizione non sono entrambi primi e dei due ideali primi appartenenti all'ideale, $<x>$ e $<x, y>$, uno contiene l'altro.