CAPITOLO 1 VARIETÀ AFFINI

versione del (7-5-2002)

ALGEBRA COMMUTATIVA

1 Il Teorema degli zeri di Hilbert

L'algebra commutativa nasce dall'osservazione (Dedekind, Weber etc.) che vi sono delle idee simili nello sviluppo della teoria dei numeri algebrici e nella teoria delle curve algebriche.

Prima di tutto, il linguaggio geometrico delle equazioni algebriche:

Dato un sistema di equazioni polinomiali

$$\text{(S)} \qquad f_i(x_1, x_2, \ldots, x_n) = 0,\ i = 1, \ldots, m$$

si pensa (alla Cartesio) alle soluzioni come *varietà affine*.

Vorrei insistere subito sulle idee generali, un sistema di equazioni polinomiali è una famiglia di polinomi, in generale possiamo prendere come coefficienti elementi di un anello commutativo A (nei casi classici il campo reale o complesso), quindi la notazione è:

$$f_i(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n],\ i = 1, \ldots, m$$

risolvere le equazioni ha senso per ogni $A-$algebra R, questo perché, dati elementi $\underline{r} := r_1, r_2, \ldots, r_n \in R$ esiste il *morfismo di valutazione*

$$\phi_{\underline{r}} :\ A[x_1, x_2, \ldots, x_n] \to R,\ \phi_{\underline{r}}(x_i) = r_i, \quad \phi_{\underline{r}}(f(x_1, x_2, \ldots, x_n)) := f(r_1, r_2, \ldots, r_n).$$

Una soluzione del sistema di equazioni S nell'algebra R è dunque una $n-$upla $r_1, r_2, \ldots, r_n \in R$ per cui $\phi_{\underline{r}}(f_i) = f_i(r_1, r_2, \ldots, r_n) = 0,\ i = 1, \ldots, m.$

Notazioni e linguaggio:

L'insieme R^n delle $n-$uple $r_1, r_2, \ldots, r_n \in R$ si dice *spazio affine $n-$dimensionale su R.* Una $n-$upla è un *punto* dello spazio affine con *coordinate* $r_1, r_2, \ldots, r_n$.

L'insieme delle soluzioni del sistema S si chiama *varietà affine* definita dal sistema.

Dalle definizioni segue che, se $I := (f_1, f_2, \ldots, f_m)$ è l'ideale generato dai polinomi f_i un punto in R della varietà definita da tali polinomi si identifica ad un omomorfismo $\phi : A[x_1, x_2, \ldots, x_n]/I \to R$.

Se si prende una definizione cosí generale possiamo anche avere infinite variabili ed equazioni, vedremo in seguito come giocano le ipotesi di finitezza.

In questo punto di vista astratto R può variare e quindi è necessario pensare alla varietà definita da tali polinomi come al *funtore rappresentabile* $R \to \text{HOM}(A[x_1, x_2, \ldots, x_n]/I, R)$.

COEFFICIENTI IN UN CAMPO k ALGEBRICAMENTE CHIUSO.

Ovviamente il caso classico consiste nel prendere $A = R = \mathbb{C}$ i complessi o più in generale $A = R = k$ un campo algebricamente chiuso. In questo paragrafo quindi k denota un campo algebricamente chiuso e per polinomio intendiamo polinomio a coefficienti in k.

Dato un insieme S di polinomi denotiamo con

$$V(S) := \{p \in k^n \mid f(p) = 0,\ \forall f \in S\} \tag{1.1}$$

$V(S)$ è detta la *varietà affine* delle soluzioni (in k) del sistema $f(x) = 0,\ f \in S$.

Il teorema fondamentale è l'*Hilbert Nullstellensatz* che ci spiega quando una equazione è conseguenza di altre date. Scriviamo per semplicità $f(x)$ invece di $f(x_1, x_2, \ldots, x_n)$.

1.2 TEOREMA. *Un polinomio $g(x)$ svanisce su tutti gli zeri del sistema S se e solo se si ha una relazione:*

$$g(x)^N = \sum_{i=1}^{m} a_i(x) f_i(x),\ a_i(x) \in k[x_1, x_2, \ldots, x_n].$$

In una direzione l'enunciato è evidente. Questo Teorema fondamentale ha molte dimostrazioni. Iniziamo ad enunciarne un caso speciale:

1.3 DEFINIZIONE. *Un sistema di equazioni S è* **incompatibile** *se e solo se non ha alcuna soluzione, ovvero $V(S) = \emptyset$.*

Caso speciale del Nullstellensatz (per $g(x) = 1$):

1.4 TEOREMA. *Un sistema di equazioni $f_i(x) = 0$ è incompatibile se e solo se si ha una relazione:*

$$1 = \sum_{i=1}^{m} a_i(x) f_i(x),\ a_i(x) \in k[x_1, x_2, \ldots, x_n].$$

Osservazione : La relazione $1 = \sum_{i=1}^{m} a_i(x) f_i(x),\ a_i(x) \in k[x_1, x_2, \ldots, x_n]$ equivale a dire che l'ideale generato dai polinomi $f_i(x)$ è l'intero anello.

Vi è una riduzione del caso generale a quello speciale:

Il trucco di Rabinowitz Proviamo 1.2 a partire da 1.4, prendiamo $g(x)$, che svanisce sugli zeri dei polinomi $f_i(x)$, aggiungiamo una variabile y e consideriamo il polinomio $yg(x) - 1$. Dalle ipotesi fatte il sistema $yg(x) - 1 = 0,\ f_i(x) = 0,\ i = 1, \ldots, m$ è incompatibile e quindi esistono polinomi $a_i(y, x) \in k[y, x_1, x_2, \ldots, x_n],\ i = 0, \ldots, m$ con

$$1 = a_0(y, x)(yg(x) - 1) + \sum_{i=1}^{m} a_i(y, x) f_i(x). \tag{1.5}$$

Sostituiamo ad y la frazione $\frac{1}{g}$ ed otteniamo $1 = \sum_{i=1}^{m} a_i(1/g, x) f_i(x)$. Moltiplichiamo per una opportuna potenza di g per eliminare i denominatori ed otteniamo la eguaglianza richiesta.

Ora proviamo che il Teorema 1.4 è equivalente al seguente:

1.6 Teorema. *Se M è un ideale massimale di $k[x_1, x_2, \dots, x_n]$ si ha*

$$k[x_1, x_2, \dots, x_n]/M = k. \tag{1.7}$$

Dimostrazione della equivalenza. Assumiamo 1.4 e consideriamo M un ideale massimale di $k[x_1, x_2, \dots, x_n]$, quindi M definisce un sistema di equazioni compatibile ed esiste un omomorfismo (punto) $\phi : k[x_1, x_2, \dots, x_n]/M \to k$, poichè M è massimale $k[x_1, x_2, \dots, x_n]/M$ è un campo contenente k e quindi ϕ deve essere un isomorfismo. Assumiamo invece 1.6 e sia $f_i = 0$ un sistema incompatibile. Se per assurdo l'ideale generato dagli f_i non fosse tutto l'anello esisterebbe un ideale massimale M con $f_i \in M$ ma allora il punto associato ad M è una soluzione del sistema, una contraddizione.

Osservazione. Il Teorema 1.6 è equivalente a:

1.8 Teorema. *Se M è un ideale massimale di $k[x_1, x_2, \dots, x_n]$ esistono unici elementi $a_i \in k$ tali che*

$$M = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) \tag{1.9}$$

Dim. Se $k[x_1, x_2, \dots, x_n]/M = k$ si ha che, modulo M ogni variabile x_i è equivalente ad un elemento $a_i \in k$ ovvero $x_i - a_i \in M$. Ma ora è anche chiaro che dati elementi $a_i \in k$ si ha

$$k[x_1, x_2, \dots, x_n]/(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n) = k$$

quindi $(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ è massimale ed uguale ad M. Il viceversa è ovvio. □

Finora abbiamo fatto una serie di riduzioni, per completare la discussione bisogna provare il Teorema 1.6. Questo segue da un Teorema più generale.

1.10 Teorema. *Sia F un campo, M un ideale massimale di $F[x_1, x_2, \dots, x_n]$ e sia $G := F[x_1, x_2, \dots, x_n]/M$ (un campo). Si ha allora:*

$$[G : F] = \dim_F F[x_1, x_2, \dots, x_n]/M < \infty. \tag{1.11}$$

1.10 implica 1.6 in quanto se F è algebricamente chiuso non ammette estensioni di grado finito tranne se stesso ovvero $G = F$.

Dimostrazione di 1.10. Lo facciamo prima in un caso speciale che ha un suo interesse indipendente.

1.12 Teorema. *Sia G un campo estensione del campo dei complessi $\mathbb{C}$ se $[G : F]$ è finita o numerabile si ha $G = \mathbb{C}$.*[1]

Dim. Poiché $\mathbb{C}$ è algebricamente chiuso il caso di dimensione finita è evidente. Il caso numerabile è un po più sottile. Supponiamo $G \neq \mathbb{C}$ quindi esiste $a \in G,\ a \notin \mathbb{C}$. Necessariamente a è trascendente e quindi il campo generato da a in G è isomorfo al campo delle

[1] La stessa dimostrazione vale anche se G è un corpo non necessariamente commutativo

funzioni razionali $\mathbb{C}(x)$ in una variabile. In questo campo si vede facilmente che gli elementi $\frac{1}{x-a},\ a \in \mathbb{C}$ formano un insieme non numerabile di elementi linearmente indipendenti e quindi tale campo non può essere contenuto in una estensione a dimensione numerabile.

Il radicale di un ideale

Facciamo una piccola escursione formale sui concetti discussi nel paragrafo precedente. Dati polinomi f_i l'insieme dei polinomi $\sum_i g_i f_i$ altro non è che *l'ideale* $I := (f_1, \dots, f_m)$ *generato* da tali polinomi.

Le equazioni che svaniscono sugli zeri degli f_i sono dunque quei polinomi g tali che $g^N \in I$ per qualche N.

1.13 Proposizione. *Se I è un ideale di un anello commutativo A posto:*

$$\sqrt{I} := \{a \in N \mid \exists N \in \mathbb{N},\ a^N \in I\} \tag{1.14}$$

si ha che $\sqrt{I}$ è un ideale, detto **radicale** *di I.*

Si ha $\sqrt{\sqrt{I}} = \sqrt{I}$.

Dim. Se $a^p \in I,\ b^q \in I$ si vede subito dalla espansione binomiale che $(a+b)^{p+q} \in I$, inoltre se $r \in A$ si ha $(ra)^p = r^p a^p \in I$. Per l'ultima parte se $a^p \in \sqrt{I}$ esiste q con $(a^p)^q \in I$.[2] □

Usualmente un ideale I per cui $I = \sqrt{I}$ viene detto *ideale radicale*.

Dire che l'ideale $\{0\}$ di un anello A è radicale equivale a dire che A non possiede elementi nilpotenti[3] diversi da 0. Un tale anello viene anche detto *semiprimo*.

Caso generale

La dimostrazione di 1.10 in generale riposa su considerazioni più complesse, si collega al concetto di *integralità.*

Qualche premessa sull'integralità.

1.15 Definizione. *Dati due anelli $A \subset B$ e $b \in B$ si dice che:*

1) b è algebrico su A se b soddisfa un polinomio a coefficienti in A:

$$a_0 b^n + a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_n = 0,\ a_i \in A. \tag{1.16}$$

2) b è integrale su A se b soddisfa un polinomio monico a coefficienti in A:

$$b^n + a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_n = 0,\ a_i \in A. \tag{1.17}$$

Si dice che B è integrale (risp. algebrico) su A se ogni elemento di B è integrale (risp. algebrico) su A.

Il risultato più elementare che vedremo nel prossimo paragrafo è:

[2] La proprietà commutativa è essenziale come si vede con semplici esempi nelle matrici 2×2, la teoria non commutativa si può sviluppare ma richiede idee e risultati diversi da questi.

[3] un elemento a di un anello si dice *nilpotente* se $a^n = 0$ per qualche esponente n.

1.18 Teorema. *Se $b, c \in B$ sono integrali su A si ha che $b+c$ e bc sono integrali su A.*

Corollario. *Se $B = A[b_1, b_2, \ldots, b_m]$ è generato da elementi integrali allora B è integrale su A.*

Osservazione Se b soddisfa $a_0 b^n + a_1 b^{n-1} + a_2 b^{n-2} + \cdots + a_n = 0,\ a_i \in A$ si ha che $a_0 b$ è integrale su A (moltiplicare per a_0^{n-1}).

Assumendo questo teorema dimostriamo 1.10.

Dim. Per induzione su n, per $n = 1$ segue dalla teoria elementare dei polinomi in una variabile. Supponiamo dunque il Teorema per $n-1$.

Sia a_i la classe di x_i in G, se tutti gli a_i sono algebrici su F il teorema segue.

Sia $L := F(a_1)$ il sottocampo di G generato da a_1. Poiché $G = L[a_2, \ldots, a_n]$, per induzione gli elementi $a_2, \ldots, a_n$ sono algebrici su L, dobbiamo provare che a_1 è algebrico su F.

Scriviamo equazioni algebriche per gli elementi a_i a coefficienti in L, ovvero funzioni razionali in a_1. Prendendo un minimo comune multiplo $f(a_1)$ dei denomianatori che appaiono in tali equazioni abbiamo che $f(a_1)a_i$ è integrale su $F[a_1]$ per ogni i, ne segue che G è integrale su $F[a_1, 1/f(a_1)]$. Se per assurdo $F[a_1]$ è isomorfo all'anello dei polinomi in x, G contiene il campo $F(x)$ delle funzioni razionali e quindi ogni polinomio non nullo $g(x)$ è tale che $1/g(x)$ è integrale su $F[x, 1/f]$, un assurdo se $g(x)$ non divide una potenza di $f(x)$ perché ne seguirebbe una relazione:

$$(1/g)^m + c_1/f^N (1/g)^{m-1} + \ldots c_m/f^N = 0,\ c_i \in F[x],\ f^N = gP,\ P \in F[x]$$

Ora per ogni campo F esistono infiniti polinomi primi distinti (stesso ragionamento come per i numeri interi) una contraddizione.[4] □

2 Integralità, primi elementi

L'integralità è legata al concetto di generazione finita dei moduli.

2.1 Lemma. *Siano $A \subset B \subset C$ tre anelli. Supponiamo che C sia generato linearmente su B da elementi $m_1, \ldots, m_k$ e che B sia generato linearmente su A da elementi $n_1, \ldots, n_h$ allora C è generato linearmente su A dagli hk elementi $n_i m_j$.*

Dim. Ovvio. □

[4] questo ragionamento è in definitiva un caso speciale di un principio generale per le estensioni integrali, detto *blowing up*.

2.2 LEMMA. *i) M un $A-$modulo generato linearmente su A da elementi $m_1, \ldots, m_k$ supponiamo che $\sum_{j=1}^{k} a_{ij} m_j = 0,\ i = 1, \ldots, k,\ a_{ij} \in A$. Se $d := \det(a_{ij})$ si ha $dm_i = 0,\ \forall i$.*

ii) Se I è un ideale di A, M un $A-$modulo finitamente generato con $IM = M$ esiste un $r \in I$ con $(1 - r)M = 0$.

DIM. i) Sia A^{ij} la matrice dei cofattori con $\sum_j A^{ij} a_{jh} = \delta^i_h d$ si ha

$$0 = \sum_j A^{ij} \sum_{h=1}^{k} a_{jh} m_h = dm_i.$$

ii) Abbiamo $\sum_{j=1}^{k} u_{ij} m_j = m_i,\ i = 1, \ldots, k,\ u_{ij} \in I$ che riscriviamo $\sum_{j=1}^{k} u_{ij} m_j - m_i = 0$, poi applichiamo la parte precedente osservando che il determinante d ha la forma $1 - r,\ t \in I$. □

Come corollario otteniamo il teorema di Cayley-Hamilton. Nelle stesse ipotesi M un $A-$modulo generato linearmente su A da elementi $m_1, \ldots, m_k$ sia $X : M \to M$ un endomorfismo. Automaticamente M diventa un modulo sull'anello $A[X]$ e $Xm_i = \sum_j a_{ij} m_j$. Possiamo costruire un *polinomio caratteristico* come :

$$\chi_X(t) := \det((a_{ij}) - t1_k.$$

Riscriviamo $0 = \sum_{j \neq i} a_{ij} m_j + (a_{ii} - X)m_i$, una matrice di relazioni a coefficienti in $A[X]$. Il determinante di questa matrice (di relazioni), è il polinomio caratteristico valutato in X! Da 2.3 si ha:

2.3 TEOREMA. *(Cayley-Hamilton)*

$$\chi_X(X) = 0.$$

Possiamo ora ritornare alla dipendenza integrale. Primo criterio:

2.4 LEMMA. *Le seguenti condizioni sono equivalenti:*
1) Un elemento $b \in B$ è integrale su A.
2) L'anello $A[b]$ è un $A-$modulo di tipo finito.
3) L'anello $A[b]$ è contenuto in un $A[b]$ modulo M di tipo finito come $A-$modulo.

DIM. Se b soddisfa un polinomio monico di grado n è chiaro che $A[b]$ è generato linearmente su A dalle potenze $b^i,\ i < n$ quindi 1) $\implies$ 2). 2) $\implies$ 3) banalmente. Viceversa sia $A[b] \subset M$ ed M è generato linearmente su A da elementi $m_1, \ldots, m_k$. Abbiamo dunque $bm_i = \sum_j a_{ij} m_j,\ a_{ij} \in A$. Dal teorema di Cayley-Hamilton segue che b soddisfa il polinomio caratteristico della matrice (a_{ij}).

□

Dimostrazione del Teorema 1.15 (e fine della prova del Nullstellensatz):

DIM. Consideriamo gli anelli $A \subset A[b] \subset A[b, c]$. Poiché b, c sono integrali su A, 2.3 ci assicura che sono soddisfatte le ipotesi di 2.1 e quindi $A[b, c]$ è un modulo di tipo finito su A riapplicando 2.4 ogni elemento di $A[b, c]$ è integrale su A. □

Dalla discussione fatta segue anche:

2.5 Teorema. *1) Siano $A \subset B \subset C$ tre anelli. Supponiamo che C sia integrale su B e B sia integrale su A allora C è integrale su A.*

2) Siano $A \subset B$ due anelli. L'insieme C degli elementi di B integrali su A è un sottoanello. Se $b \in B$ è integrale su C allora $b \in C$.

3) Se $B = A[b_1, b_2, \ldots, b_m]$ è generato da elementi integrali allora B è un modulo di tipo finito su A.

Dim. Gli enunciati sono quasi evidenti, conviene soffermarsi su 2). Se c è integrale su C e prendiamo un polinomio monico da esso soddisfatto, tale polinomio ha un numero finito di coefficienti $b_1, \ldots, b_n$ che sono integrali su A, quindi c è integrale sull'anello $A[b_1, \ldots, b_n]$ che è un modulo di tipo finito su A. Se ne deduce che $A[b_1, \ldots, b_n, c]$ è un modulo di tipo finito su A. □

Dati $A \subset B$ due anelli. L'anello C degli elementi di B integrali su A si chiama *chiusura integrale di A in B*. Se $A = C$ si dice che A è integralmente chiuso. Ovviamente la chiusura integrale di A in B è integralmente chiusa in B.

2.6 Definizione. *Se A è un dominio e B il suo campo dei quozienti si chiama* **normalizzazione** *di A la chiusura integrale di A in B.*

Un dominio A si dice **normale** *se è integralmente chiuso nel suo campo dei quozienti.*

L'analisi precedente si può anche rivedere come segue:

Esercizio i) Sia A un dominio ed $a \in A$. Se $1/a$ è integrale su A allora $1/a \in A$ (sugg. scrivere una equazione monica ed eliminare il denominatore).

ii) Sia $A \subset B$ una estensione integrale con B un campo, allora A è un campo.

iii) Per ogni polinomio $f(x)$ l'algebra $F[x, 1/f]$ non è mai un campo.

Infatti in una trattazione assiomatica della teoria si possono studiare anelli per cui valgano analoghi di questi enunciati, gli *anelli di Jacobson*.

3 Varietà affini

In questo paragrafo k denota un campo algebricamente chiuso.

Introduciamo un linguaggio, dato un sistema $S \subset k[x_1, \ldots, x_n]$ di polinomi abbiamo denotato con $V(S) \subset k^n$ l'insieme delle soluzioni. Viceversa dato un insiame $A \subset k^n$ definiamo con $I(A)$ l'ideale dei polinomi che svaniscono su A.

Abbiamo le seguenti proprietà elementari;

3.1 Proposizione. *Data una famiglia di insiemi S_i di equazioni:*

$$V(\cup_i S_i) = \cap_i V(S_i) \tag{3.2}$$

Dati due insiemi S, T di equazioni:

$$V(ST) = V(S) \cup V(T) \tag{3.3}$$

$$V(\emptyset) = k^n, \quad V(\{1\}) = \emptyset \tag{3.4}$$

Se I_S è l'ideale generato da S si ha:

$$V(S) = V(I_S) = V(\sqrt{I}_S). \tag{3.5}$$

Infine:

$$S \subset T \subset k[x_1, \ldots, x_n] \implies V(T) \subset V(S), \qquad A \subset B \subset k^n \implies I(B) \subset I(A).$$

DIM. 3.2 e 3.4 sono ovvi. Per 3.3 osserviamo che è evidente che $V(ST) \supset V(S) \cup V(T)$. Viceversa sia $p \in V(ST)$, se $p \notin V(S)$ esiste un $f \in S$ con $f(p) \neq 0$. Per ogni $g \in T$ si ha per ipotesi $0 = (fg)(p) = f(p)g(p)$ da cui segue $g(p) = 0$, $\forall g \in T$ ossia $p \in V(T)$. 3.5 segue dal Nullstellensatz. □

Osservazione. Date due varietà W_1, W_2 detti I_1, I_2 i loro ideali (radicali) si ha che l'ideale associato a $W_1 \cup W_2$ è $I_1 \cap I_2$ che è un ideale radicale. Invece $W_1 \cap W_2$ è definita dall'ideale $I_1 + I_2$ che non è sempre radicale, come si vede prendendo ad esempio gli ideali di due curve tangenti in un punto!

Preso un insieme di punti $A \subset k^n$ poniamo:

$$\overline{A} := V(I(A)). \tag{3.6}$$

3.7 TEOREMA. *L'operatore $A \to \overline{A}$ è un operatore di chiusura per una topologia (topologia di Zariski) su k^n i cui chiusi sono le varietà affini $V(S)$.*

DIM. Il Teorema è una conseguenza immediata della Proposizione precedente. □

Dalle analisi fatte abbiamo:

3.8 TEOREMA. *Le due corrispondenze $S \to V(S)$, $A \to I(A)$ sono biunivoche, fra l'insieme degli ideali radicali di $k[x_1, \ldots, x_n]$ e l'insieme delle varietà affini di k^n.*

Un primo concetto geometrico sulle varietà è il concetto di irriducibilità.

3.9 DEFINIZIONE. *Una varietà affine V si dice* **riducibile** *se $V = W_1 \cup W_2$ con W_1, W_2 due varietà propriamente contenute in V, altrimenti si dice* **irriducibile**.

Sfruttando la corrispondenza fra varietà ed ideali si ha che una varietà riducibile corrisponde ad un ideale $I = I_1 \cap I_2$ intersezione propria di due ideali radicali.

Ricordiamo che, un ideale P di un anello commutativo A si dice *primo* se A/I è un dominio. Equivalentemente se soddisfa la condizione seguente: se $a, b \in A$, $ab \in I$ allora o $a \in I$ o $b \in I$.

3.10 Teorema. *Una varietà affine V è irriducibile se e solo se il suo ideale associato è primo.*

Dim. Dati due ideali $I_1,\ I_2$ si ha che $I_1 I_2 \subset I_1 \cap I_2$, quindi un ideale intersezione di due ideali che lo contengono propriamente non è primo. Pertanto se $V = W_1 \cup W_2$ è riducibile l'ideale I di V contiene il prodotto degli ideali I_1, I_2 di W_1, W_2 e non è primo. Viceversa se I non è primo si ha che esistono $a, b \in A,\ ab \in I,\ a \notin I,\ b \notin I$. Si ottiene che, posto $W_1 := V(a, I),\ W_2 := V(b, I)$ queste sono due sottovarietà propriamente contenute in V e $V = W_1 \cup W_2$.

□

Le varietà irriducibili sono i mattoni con cui si costruiscono tutte le varietà.

3.11 Teorema. *Una varietà affine V è unione di un numero finito di varietà irriducibili, la scrittura $V = W_1 \cup W_2 \cup \cdots \cup W_m$ con le W_i irreducibili e con $W_i \subsetneq W_j, \forall i, j$ è unica.*

Dim. La rimandiamo al paragrafo sulle proprietà legate al concetto di Noetheriano. □

ESEMPIO FONDAMENTALE. Una **ipersuperficie** di k^n è una sottovarietà di k^n definita da una unica equazione $f(x) = 0$.

Dal teorema di fattorizzazione unica dei polinomi abbiamo che $f(x) = \prod_i g_i(x)^{h_i}$ con $g_i(x)$ polinomi irriducibili distinti. Si ha dunque

$$V(f) = \cup_i V(g_i)$$

3.12 Proposizione. *L'ideale $(f(x))$ è primo se e solo se $f(x)$ è irriducibile,*

$$\sqrt{(f(x))} = (\prod_i g_i(x)).$$

Dim. Dati due polinomi $a(x), b(x)$ si ha che $a(x)b(x) \in (f(x)) \iff f(x) | a(x)b(x)$ ($f(x)$ divide il prodotto $a(x)b(x)$). Se $f(x)$ è irriducibile e $f(x)$ divide il prodotto $a(x)b(x)$ allora $f(x)$ divide $a(x)$ o $b(x)$ e quindi $(f(x))$ è primo. Se $f(x) = a(x)b(x)$ è prodotto di due polinomi di grado più basso è chiaro che $(f(x))$ non è primo.

Se $N \geq h_i,\ \forall i$ si ha $(\prod_i g_i(x))^N \in (\prod_i g_i(x)^{h_i})$ quindi $(\prod_i g_i(x)) \in \sqrt{(f(x))}$.

Viceversa, se $h(x)^N \in (\prod_i g_i(x))$ si ha che $\prod_i g_i(x)$ divide $h(x)^N$ e quindi essendo i g_i primi distinti si ha anche che $\prod_i g_i(x)$ divide $h(x)$ ovvero $h(x) \in (\prod_i g_i(x))$. □

Il punto generico

I geometri algebrici della scuola italiana amavano pensare che su *un punto generico* di una varietà $V(S)$ valgono solo le equazioni *deducibili* da S. Si può dare un senso preciso a questo enunciato (se la varietà è irriducibile) nel modo seguente. Iniziamo a ragionare nel caso dei coefficienti complessi.

Dato un punto p di coordinate $a_1, \ldots, a_n \in \mathbb{C}$ su p evidentemente valgono le equazioni $x_i - a_i = 0$ ma in qualche senso potrebbero non essere *deducibili* dalle equazioni date (per esempio con un algoritmo effettivo). Un modo di esprimere questa idea è il seguente.

I coefficienti che appaiono in un sistema finito di equazioni che generano un ideale primo sono un numero finito di numeri α_j e preso il sottocampo $F := \mathbb{Q}(\alpha_j)$ abbiamo che $\mathbb{C}$ ha grado di trascendenza infinito sia su F che sulla sua chiusura algebrica k. In particolare se pensiamo alla varietà $V(S)$ come defintita sul campo k e I è l'ideale primo che la definisce possiamo immergere il campo delle frazioni G dell'anello $k[x_1, \ldots, x_n]/I$ nei complessi. Ogni tale immersione corrisponde ad un punto in cui i soli polinomi a coefficienti in k che svaniscono sono quelli di I!

4 Il teorema della base e gli anelli Noetheriani

Un'altro teorema fondamentale di Hilbert è il teorema della base, che asserisce che da un qualunque sistema di equazioni se ne può estrarre uno finito da cui le altre si deducono per combinazione lineare.

Nel linguaggio più astratto questo teorema afferma:

4.1 Teorema. *Ogni ideale I di un anello $F[x_1, x_2, \ldots, x_n]$ di polinomi su un campo F è finitamente generato.*[5]

Emmy Nöether, allieva di Hilbert, ha formulato in modo astratto questa nozione, dalle sue ricerche nasce la teoria degli anelli Noetheriani che è la base dell'algebra commutativa moderna.

La osservazione iniziale fondamentale è la seguente:

4.2 Teorema. *Per un modulo M su un anello A le seguenti condizioni sono equivalenti:*

1) Ogni sottomodulo è finitamente generato.

2) Data una catena crescente di sottomoduli $I_1 \subset I_2 \subset \cdots \subset I_m \subset I_{m+1} \subset M \ldots$ esiste un n tale che $I_n = I_p,\ \forall p \geq n$.[6]

3) Ogni famiglia non vuota di sottomoduli ammette un elemento massimale.

Dim. 1) $\implies$ 2) Infatti, data tale catena consideriamo $I = \cup_{i=1}^{\infty} I_i$. Chiaramente I è un sottomodulo e per 1) è generato da un numero finito di elementi $a_1, a_2, \ldots, a_m$. Evidentemente deve esistere un n tale che $a_1, \ldots, a_m \in I_n$ da cui $I = I_n$ e la tesi.

2) $\implies$ 3) questo è un tipico ragionamento astratto di *induzione trasfinita* che viene usualmente formulato con il lemma di Zorn.[7] Prima di tutto si osserva che da 2) segue

[5] Un ideale I di un anello commutativo A è finitamente generato se esistono elementi $a_1, \ldots, a_m \in I$ con $I := \{\sum_{i=1}^{m} b_i a_i,\ b_i \in A\}$, si denota $I := (a_1, \ldots, a_m)$.

[6] In altre parole ogni catena crescente di ideali è stazionaria

[7] Il Lemma di Zorn è un enunciato equivalente all'assioma della scelta ed alla proprietà della esistenza dei numeeri ordinali trasfiniti, permette di fare una induzione anche su insiemi bene ordinati infiniti.

che ogni insieme totalmente ordinato di sottomoduli ammette un massimo da cui segue che un insieme qualunque di sottomoduli è una famiglia filtrante nel senso del Lemma di Zorn e quindi ha un elemento massimale. 3) $\implies$ 2) Data una catena crescente per 3) essa ammette un elemento I_n massimale.

2) $\implies$ 1) Se esistesse un sottomodulo I non finitamente generato, potremmo induttivamente scegliere elementi $a_1, a_2, \ldots, a_m \ldots$ per cui $a_{m+1} \in I,\ a_{m+1} \notin (a_1, a_2, \ldots, a_m)$.

La catena di sottomoduli $I_m := (a_1, a_2, \ldots, a_m)$ è dunque crescente e non stazionaria. □

La condizione 2) viene detta usualmente *condizione della catena ascendente*.

In onore di E.Nöether un modulo che soddisfi le precedenti proprietà equivalenti si dice **modulo Noetheriano**. In modo simile un anello A che soddisfi le precedenti proprietà come $A-$modulo (ovvero sugli ideali) si dice **anello Noetheriano.**

La classe più semplice di anelli Noetheriani, oltre a quella ovvia dei campi è la classe degli anelli ad ideali principali, ovvero in cui ogni ideale è generato da un unico elemento.[8]

Il prototipo di questa classe è l'anello $\mathbb{Z}$ dei numeri interi.

Prima di procedere osserviamo le seguenti proprietà elementari.

4.3 Proposizione. *1) Dato un modulo M ed un sottomodulo N, se M è finitamente generato anche M/N è finitamente generato.*[9]

2) Dato un modulo M ed un sottomodulo N, se N e M/N sono moduli finitamente generati anche M è finitamente generato.

3) Dato un modulo M ed un sottomodulo N, M è Noetheriano se e solo se N e M/N sono moduli Noetheriani.

4) Se $M_1,\ M_2$ sono due moduli Noetheriani, anche $M_1 \oplus M_2$ è Noetheriano.

5) Se A è un anello Noetheriano e M è un $A-$modulo finitamente generato allora M è Noetheriano.

Dim. 1) è ovvio, un sistema di generatori di M induce al quoziente generatori di M/N.

2) è quasi ovvio, presi $n_1, \ldots, n_k$ generatori di N e $m_1, \ldots, m_h$ elementi di M che, modulo N generano M/N, è evidente che gli elementi $n_1, \ldots, n_k, m_1, \ldots, m_h$ generano M linearmente.

3) Se M è Noetheriano è evidente che sia N che M/N lo sono. Il viceversa segue da 2), in quanto se $P \subset M$ è un sottomodulo si ha che $P \cap N$ è finitamente generato, in quanto sottomodulo di N e $P/P \cap N$ è finitamente generato, in quanto sottomodulo di M/N.

4) È un caso speciale di 3) in quanto $M_1 \subset M_1 \oplus M_2,\ M_2 = (M_1 \oplus M_2)/M_1$.

5) Se $M = \sum_{i=1}^n Am_i$ abbiamo un morfismo suriettivo $A^n \xrightarrow{p} M,\ p(a_1, a_2, \ldots, a_n) = \sum_{i=1}^n a_i m_i$.

Da 4) segue che A^n è Noetheriano, da 3) segue che anche M, suo quoziente, lo è. □

[8] Il caso più importante è quello dei domini, in inglese P.I.D. *principal ideal domains*.

[9] ma N non lo è in generale.

Nella formulazione precedente il teorema della base è il primo di una lunga serie di teoremi che ci assicurano che la proprietà di essere Noetheriano si conserva tramite molte costruzioni fondamentali.

4.4 Teorema. *Dato un anello Noetheriano A, l'anello dei polinomi $A[x]$ su A è anche esso Noetheriano.*

Dim. Sia $I \subset A[x]$ un ideale, consideriamo l'ideale J (verificarlo) di A formato dai coefficienti direttivi dei polinomi in I, ovvero $J := \{a \in A \,|\, \exists f(x) \in I,\ f(x) = ax^n + b_1x^{n-1} + \cdots + b_n\}$.

Per ipotesi $J = (a_1, \ldots, a_m)$ è finitamente generato. Siano $f_i(x) \in I, f_i = a_ix^{n_i} +$ termini più bassi.

Se $g(x) \in I$ ha grado maggiore o uguale del massimo N degli n_i possiamo sottrarre a $g(x)$ una combinazione lineare degli f_i ed abbassarne il grado. D'altra parte i polinomi in I di grado minore di N sono un $A-$sottomodulo del modulo (isomorfo ad A^N) di tutti i polinomi di grado minore di N e quindi sono un $A-$modulo finitamente generato. Pertanto i polinomi f_i insieme ai generatori di tale modulo generano I come ideale.

□

Corollario, Teorema della base di Hilbert. *Se F è un campo l'anello dei polinomi $F[x_1, \ldots, x_n]$ è Noetheriano.*

$\mathbb{Z}[x_1, \ldots, x_n]$ è Noetheriano.

Una semplice conseguenza di questo fatto è:

4.5 Teorema. *Ogni successione decrescente di varietà affini $k^n \supset V_1 \supset \ldots V_m \supset$ è stazionaria.*

Ogni varietà V è unione in modo unico di varietà irriducibili non mutualmente comparabili.

Dim. La prima parte segue dalla proprietà della catena ascendente per i rispettivi ideali. Per la seconda, sia per assurdo V una varietà minimale rispetto alla proprietà di non essere unione di varietà irriducibili. In particolare V non è irriducibile e $V = W_1 \cup W_2$ due varietà più piccole. Per la minimalità sia W_1 che W_2 sono unione di varietà irriducibili e quindi anche V lo è. Per la unicità si osservi che, se $V = W_1 \cup W_2 \cup \cdots \cup W_k$ è una unione di varietà irriducibili e $X \subset V$ è una varietà irriducibile, poiché $X = (X \cap W_1) \cup (X \cap W_2) \cup \ldots (X \cap W_k)$ si deve avere $X \subset W_i$ per qualche i. Se $V = U_1 \cup U_2 \cup \cdots \cup U_h$ è una altra unione di varietà irriducibili si ha dalla osservazione precedente $U_i \subset W_j$ per qualche j similmente $W_j \subset U_t$. Se assumiamo che le U_i non sono comparabili deve essere $t = i$ e dunque $W_j = U_i$, similmente ogni U_j è uguale ad una delle W_i. □

In effetti in modo simile si ottiene un enunciato sugli ideali. Notiamo prima di tutto che:

4.6 Lemma. *Se P è un ideale primo e $I_1 \ldots I_k$ sono ideali con $P \supset \cap_{t=1}^k I_t$ allora $P \supset I_i$ per qualche $i = 1, \ldots, k$.*

DIM. Per induzione basta farlo per due ideali. Se P è un ideale primo e I, J sono due ideali con $P \supset I \cap J$ allora $P \supset I$ oppure $P \supset J$ infatti $IJ \subset I \cap J \subset P$ e se esiste $a \in I,\ a \notin P$ allora da $aJ \subset P$ segue $J \subset P$. □

4.7 TEOREMA. *Dati un anello Noetheriano A ed un ideale radicale I gli ideali primi minimali su I sono in numero finito e la loro intersezione è I.*

DIM. Proviamo, prima di tutto, che un ideale radicale è intersezione di un numero finito di ideali primi. Sia, per assurdo I massimale rispetto alla negazione di tale proprietà. Evidentemente I non è un ideale primo e quindi esistono $a, b \notin I$ con $ab \in I$, se $J_1 := \sqrt{(a, I)},\ J_2 := \sqrt{(b, I)}$ affermo che $J_1 \cap J_2 = I$, questo porta per massimalità ad una contraddizione. Infatti se $u \in J_1 \cap J_2$ esiste un N per cui $u^N \in (a, I) \cap (b, I)$ da cui $u^{2N} \in (a, I)(b, I) \subset I$ e quindi $u \in I$.

Ora se $I = P_1 \cap P_2 \cap \cdots \cap P_k$ con P_i ideali primi e $P \supset I$ è primo si ha che $P \supset P_j$ per un indice j dalle osservazioni precedenti il teorema, ne segue che i primi minimali appaiono necessariamente in questa espressione, evidentemente quelli non minimali possono essere tolti.

□

Notiamo infine un fatto utile.

4.8 PROPOSIZIONE. *Dato un anello Noetheriano A ed un suo ideale I esiste un intero k per cui $(\sqrt{I})^k \subset I$.*

DIM. Se $\sqrt{I} = (a_1, \ldots, a_h)$ esiste un N tale che $a_i^N \in I,\ \forall i$ allora dalla formula multinomiale segue subito che $(\sqrt{I})^{hN} \subset I$.

□

In particolare possiamo applicare la precedente Proposizione all'insieme degli elementi nilpotenti, che è dunque un ideale J *nilpotente*, ovvero $J^k = 0$, detto *radicale nilpotente* dell'anello A.

L'insieme degli elementi nilpotenti di un anello commutativo è sempre un ideale ma non necessariamente nilpotente, vediamo qualche proprietà generale nel prossimo paragrafo.

5 Radicali

Facciamo una breve digressione di carattere generale, in cui la ipotesi Noetheriana non è necessaria.

Introduciamo prima di tutto una nozione che ha un ruolo molto importante nella teoria.

5.1 DEFINIZIONE. *Un insieme $S \subset A$ di un anello commutativo si dice* **insieme moltiplicativo** *se $s, t \in S$ implica $st \in S$.*

Dato un insieme moltiplicativo S l'insieme degli ideali I per cui $I \cap S = \emptyset$, ordinato per inclusione, è chiaramente filtrante e quindi, dal lemma di Zorn, ha un elemento massimale, ne deduciamo:

5.2 Teorema. *Sia A un anello commutativo.*
1) Se S è un iniseme moltiplicativo e I è un ideale massimale rispetto alla condizione $I \cap S = \emptyset$, allora I è un ideale primo.
2) Dato un ideale I di A si ha che $\sqrt{I}$ è la intersezione di tutti gli ideali primi $P \supset I$.

Dim. 1) Se per assurdo I_1, I_2 sono due ideali contenenti propriamente I con $I_1 I_2 \subset I$ si avrebbe $s_1 \in I_1 \cap S \neq \emptyset, s_2 \in I_2 \cap S \neq \emptyset$ e quindi $s_1 s_2 \in I \cap S$ una contraddizione.

2) Se $a^n \in I$ e $P \supset I$ è un ideale primo si deve avere $a \in P$ quindi $\sqrt{I}$ è contenuto in ogni ideale primo contenente I. Viceversa se $a^n \notin I, \forall n$ consideriamo l'insieme moltiplicativo $S := \{a^n\},\ n \in \mathbb{N}$. Se $P \supset I$ è massimale rispetto a $P \cap S = \emptyset$, da 1) si ha che P è primo ed $a \notin P$. □

5.3 Definizione. *L'insieme degli elementi nilpotenti di un anello commutativo si dice radicale nil dell'anello.*[10]

Dal teorema precedente il radicale nil di un anello commutativo A è l'intersezione di tutti gli ideali primi di A. Vi è un secondo radicale interessante.

5.4 Definizione. *Il radicale di Jacobson $J(A)$ di un anello commutativo A è l'intersezione di tutti gli ideali massimali di A.*

Gli elementi del radicale di Jacobson sono cosí caratterizzati:

5.5 Proposizione.

$$J(A) := \{r \in A | 1 - ar \quad \text{è invertibile} \quad \forall a \in A\}. \tag{5.6}$$

Dim. Sia $1 - ar$ invertibile $\forall a \in A$ e $\underline{m}$ un ideale massimale. Se $r \notin \underline{m}$ esiste un suo inverso modulo $\underline{m}$, ovvero un a_0 con $1 - a_0 r \in \underline{m}$ non invertibile. Viceversa se $r \in J(A)$ si ha $Ar \subset J(A)$ quindi se $1 - ar$ non fosse invertibile per qualche $a \in A$ esisterebbe un ideale massimale $\underline{m}$ con $1 - ar \in \underline{m}$ e quindi $1 \in \underline{m}$ una contraddizione. □

6 Decomposizione primaria

Lasker e Noether hanno scoperto che una forma non unica di decomposizione vale per tutti gli ideali, questa decomposizione viene detta *decomposizione primaria.*

Si parte da:

[10] In algebra non commutativa si deve invece prendere il massimo ideale formato da elementi nilpotenti.

6.1 Definizione. *Un ideale I si dice riducibile se $I = J_1 \cap J_2$ è intersezione di due ideali strettamente più grandi, altrimenti si dice irriducibile.*

Similmente un sottomodulo N di un modulo M si dice riducibile (in M) se $N = P_1 \cap P_2$ è intersezione di due sottomoduli strettamente più grandi, altrimenti si dice irriducibile.[11]

L'induzione noetheriana immediatamente implica:

6.2 Proposizione. *Ogni ideale I di un anello Noetheriano è intersezione di un numero finito di ideali irriducibili.*

Dim. Altrimenti esiste un ideale massimale I che viola questa proprietà. I non è in particolare irriducibile e $I = J_1 \cap J_2$ è intersezione di due ideali strettamente più grandi che pertanto sono intersezione di un numero finito di ideali irriducibili, ma allora anche I lo è una contraddizione. □

Risultato analogo per i sottomoduli di un modulo noetheriano. Ora gli ideali irriducibili sono oggetti misteriosi, ma cadono in una classe interessante.

6.3 Definizione. *Un ideale I si dice* **primario** *se dati $a, b \in A$ con $ab \in I$ e $a \notin I$ allora $b^k \in I$ per qualche k.*

6.4 Proposizione. *Se I è un ideale primario $\sqrt{I}$ è un ideale primo.*
I è primario in A se e solo se $\{0\}$ è primario in A/I.

Dim. Sia $ab \in \sqrt{I}$ ovvero $(ab)^N \in I$, se $a \notin \sqrt{I}$ si ha $a^N \notin I$ quindi per ipotesi $(b^N)^M \in I$ e $b \in \sqrt{I}$. La seconda parte è evidente. □

È importante rivedere la definizione in altro modo.

Osservazione. I è primario in A se e solo se ogni divisore di 0 in A/I è nilpotente.
Se $\sqrt{I} = P$ è un ideale primo, I è primario se e solo se $ab \in I$ e $b \notin P$ implica $a \in I$.

Questa è solo una riformulazione, però osserviamo subito che da questa ossservazione segue che, se I è primario, l'insieme dei divisori di 0 di A/I è un ideale primo e coincide con il radicale nilpotente di A/I. Diremo anche che A/I è un anello *coprimario*.

6.5 Proposizione. *Se I è un ideale irriducibile in un anello Noetheriano, allora I è primario.*

Dim. Siano $a, b \in A$ con $ab \in I$ e $b \notin \sqrt{I}$ dobbiamo provare che $a \in I$. Sia $J_k := \{x \in A | xb^k \in I\}$, evidentemente questa è una catena crescente e quindi esiste un n con $J_m = J_n, \forall m \geq n$.

Proviamo che $I = (I + Ab^n) \cap (I + Aa)$, infatti se $u + rb^n = v + sa,\ u, v \in I$ si ha $bu + rb^{n+1} = bv + sab \in I$ e $r \in J_{n+1}$ da cui $rb^n \in I$ e quindi $u + rb^n \in I$. Per ipotesi I è irriducibile e $b^n \notin I,\ I \subsetneq I + Ab^n$ quindi $a \in I$. □

Da queste proposizioni abbiamo dedotto che ogni ideale è intersezione di un numero finito di ideali primari.

Si può fare la stessa discussione per i moduli.

[11] questa è una notazione molto infelice, in quanto usualmente un modulo si dice irriducibile se non ha sottomoduli propri non banali.

6.6 Definizione. *Un modulo N si dice* **coprimario** *se dati $a \in A, n \in N$ con $an = 0$, $n \neq 0$ allora a è localmente nilpotente, ovvero per ogni $m \in N$ esiste un k con $a^k m = 0$. In particolare se N è finitamente generato esiste k con $a^k N = 0$.*

Provare gli analoghi di 6.4 e 6.5.

Esercizio L'annullatore di un modulo coprimario finitamente generato è un ideale primario.

Se $\{0\}$ è un sottomodulo irriducibile in un modulo noetheriano M allora M è coprimario. □

Questo è solo l'aspetto più elementare della decomposizione primaria di Lasker Noether. Sia $I = \cap_i Q_i$ una decomposizione primaria. È immediato verificare che $\sqrt{I} = \cap_i \sqrt{Q_i}$, questa decomposizione dell'ideale radicale deve contenere tutti i primi minimali su I dal Lemma 4.6, quindi nella decomposizione primaria vi sono alcuni ideali il cui radicale è uno dei primi minimali e poi a priori altri ideali con radicale non minimale, i primi che si ottengono da una decomposizione non ridondante (cioè da cui non si possono togliere termini) sono in realtà indipendenti dalla decomposizione e vengono detti *primi associati*, questo non è a priori evidente. I primi minimali definiscono nel caso geometrico le componenti irriducibili della varietà definita da I mentre gli altri definiscono delle componenti più piccole dette *componenti immerse*.

Esempio Nell'anello dei polinomi $k[x, y]$ in due variabili l'ideale (x^2, xy) ha la decomposizione primaria $(x^2, xy) = (x) \cap (x^2, y)$, i primi associati definiscono la retta $x = 0$ ed il suo punto $(0, 0)$, una componente immersa.

In effetti la teoria si svolge molto più convenientemente, e semplicemente, generalizzandola ad i moduli e passa attraverso una analisi dei divisori di 0.

Se M è un modulo ed $m \in M,\ m \neq 0,\ a \in A,\ a \neq 0,\ am = 0$ allora diremo che a è un *divisore di 0* su M. Questa nozione generalizza evidentemente la nozione di divisore di 0 in un anello.

Se $X \subset M$ si pone

$$Ann(X) = (0 : X) := \{a \in A | am = 0, \forall m \in X\}.$$

$(0 : m)$ è evidentemente un ideale, detto l'*annullatore* di X.

In particolare abbiamo l'annullatore di tutto M ovvero $Ann(M) = \cap_{m \in M} Ann(m)$ e gli annullatori degli elementi di M, per definizione l'insieme dei divisori di 0 su M è $\cup_{m \neq 0} Ann(m)$.

6.7 Definizione. *Dato un $A-$modulo M ed un ideale primo P di A si dice che P è* **associato** *ad M se P è l'annullatore di un elemento $m \in M$ ossia $P = \{a \in A | am = 0\}$.*

Osservazione Se I è l'annullatore di un elemento $m \in M$ si ha che I è il nucleo dell'omomorfismo $A \to M$ dato da $a \to am$ con immagine il sottomodulo Am. Dal teorema di omomorfismo $Am \cong A/I$. Se I è primo A/I è un dominio e I è l'annullatore di ciascun elemento non nullo di Am.

6.8 Lemma. *Se un ideale I è massimale fra gli annullatori degli elementi di M allora I è un ideale primo.*

Dim. Sia I l'annullatore di m e sia $ab \in I$. Se $a \notin I$ si ha $am \neq 0$, $b(am) = 0$. Poiché l'annullatore di am contiene I ed I è massimale si ha $b \in I$ e I è primo. □

Per gli anelli noetheriani si ha pertanto che:

6.9 Proposizione. *L'insieme dei primi associati ad un modulo $M \neq 0$ è non vuoto e l'insieme dei divisori di 0 su M è l'unione dei primi associati ad M.*

Corollario. *Dato un modulo finitamente generato M su un anello Noetheriano, esiste una serie di composizione finita $0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ tale che per ogni $i = 1, \ldots, n$ si ha che M_i/M_{i-1} è isomorfo come modulo ad A/P_i con P_i un ideale primo.*

Dim. Per induzione noetheriana sia N un sottomodulo di M massimale con la proprietà di possedere una catena siffatta. Se per assurdo $N \neq M$ si ha $M/N \neq 0$ ed esiste un elemento $m \in M/N$ con $Am = A/P$ per P primo. Il sottomodulo N' controimmagine di Am in M contraddice la massimalità di N. □

L'insieme dei primi associati viene indicato con $Ass(M)$.[12]

Esercizio Se N è un modulo coprimario su un anello noetheriano, N ha un unico primo associato $Q := \sqrt{Ann(N)}$. (sugg. se P è l'annullatore di un elemento non nullo si ha dalle ipotesi $P \subset \sqrt{Ann(N)}$. Viceversa $Q^k \subset Ann(N)$ per qualche k quindi $Q^k \subset P$ e dunque $Q \subset P$.) Viceversa se N ha un unico primo associato P, si ha che N è coprimario. Infatti P è l'insieme dei divisori di 0 di N, se $a \in P$ ed $m \in N$ la catena $Ann(a^k n)$ si stabilizza, e se $Ann(a^k n) = Ann(a^{k+1} n)$ si ha che a non è un divisore di 0 nel sottomodulo $Aa^k n$, questa è una contraddizione se $Aa^k n \neq 0$ in quanto P deve essere primo associato a tale sottomodulo, pertanto $a^k n = 0$.

6.10 Lemma. *i) Dati due moduli M_1, M_2 si ha $Ass(M_1 \oplus M_2) = Ass(M_1) \cup Ass(M_2)$.*
ii) Dato un modulo M ed un sottomodulo N si ha $Ass(N) \subset Ass(M)$, $Ass(M) \subset Ass(N) \cup Ass(M/N)$.[13]

Dim. i) È evidente che $Ass(M_1 \oplus M_2) \supset Ass(M_1) \cup Ass(M_2)$.
Viceversa sia $P \in Ass(M_1 \oplus M_2)$ l'annullatore di (m_1, m_2). Si ha che $P = P_1 \cap P_2$ dove P_i è l'annullatore di m_i. Essendo P primo deve essere $P = P_1$ o $P = P_2$.
ii) $Ass(N) \subset Ass(M)$ è immediato, sia $P = Ann(m)$, $m \in M$ un primo associato. Osserviamo prima di tutto che $Am = A/P$ come modulo, e quindi essendo P primo P è l'annullatore di ogni elemento non nullo di Am. Pertanto se $Am \cap N \neq 0$ si ha che $P \in Ass(N)$ altrimenti si ha che Am è isomorfo alla sua immagine in M/N e quindi P è anche l'annullatore della classe di m in M/N. □

Nel caso di un anello noetheriano A ed un ideale I, passando ad A/I possiamo ridurci a studiare una decomposizione primaria dell'ideale 0.

[12] per un gioco di parole *Ass* si pensa come l'*assassinatore* di M.
[13] esempi banali mostrano che in generale $Ass(M/N) \quad Ass(M)$.

6.11 DEFINIZIONE. *Una decomposizione primaria* $\{0\} = \cap_{j=1}^{k} Q_j$ *si dice non ridondante se non si può omettere nessun termine* Q_j *ovvero, per ogni* $i = 1, \ldots, k$ *si ha* $\{0\} \neq \cap_{j \neq i} Q_j$.

6.12 TEOREMA. *Data una qualunque decomposizione primaria* $\{0\} = \cap_{j=1}^{k} Q_j$ *non ridondante.*

a) Per ogni $i = 1, \ldots, k$ *si ha che* $P_i := \sqrt{Q_i}$ *è l'unico primo associato a* $\cap_{j \neq i} Q_j$.

b) I primi associati ad una decomposizione primaria di 0, sono esattamente i primi associati ad A come modulo.

c) L'insieme dei divisori di 0 di A è l'unione dei primi associati ad A.

DIM. a) Per semplicità sia $i = 1$. Consideriamo il modulo $N_1 := \cap_{j \neq 1} Q_j$ poiché $N_1 \cap Q_1 = 0$ si ha che $N_1 \subset A/Q_1$ in modo naturale, ma $Ass(A/Q_1) = \{P_1\}$ e l'enunciato segue.

b) Da a) sappiamo che tutti i primi $P_i = \sqrt{Q_i}$ sono associati.

$$\{P_1, \ldots, P_k\} \subset Ass(A).$$

Per il viceversa analizziamo prima il caso in cui $\{0\}$ è primario. Se P è l'annullatore di un elemento non 0, si ha che per $p \in P$ $pa = 0$ implica $p^k = 0$ ovvero $P \subset \sqrt{\{0\}}$. Ma $\sqrt{\{0\}}^k = \{0\} \subset P$ e quindi essendo P primo $P \supset \sqrt{\{0\}}$.

Ora il caso generale, si ha $A \subset \oplus_{i=1}^{k} A/Q_i$ quindi

$$Ass(A) \subset \cup_{i=1}^{k} Ass(A/Q_i) = \{P_1, \ldots, P_k\}.$$

c) segue da b) e dalla proposizione 6.9.

□

7 La categoria delle varietà affini

È importante considerare una varietà in modo indipendente da una sua immersione, in particolare va stabilito il concetto di *isomorfismo* fra varietà. Per questo è molto più conveniente introdurre il concetto più generale di *morfismo regolare* fra varietà.

7.1 DEFINIZIONE. *Data una varietà* $V \subset k^n$, *le funzioni regolari su* V *sono la restrizione a* V *delle funzioni polinomiali su* k^n.

Date due varietà $V \subset k^n$, $W \subset k^m$ *un morfismo regolare* $f : V \to W$ *è una funzione per cui le coordinate in* W *sono funzioni regolari su* V.

Poichè la restrizione di una funzione a V è un omomorfismo, con nucleo l'ideale $I(V)$ dei polinomi che svaniscono su V, le funzioni regolari su V sono per costruzione isomorfe all'algebra $k[x_1, \ldots, x_n]/I(V)$.

Per definizione si pone:

(7.2) $\qquad k[V] := k[x_1, \ldots, x_n]/I(V), \qquad$ l'anello delle funzioni regolari su V.

La seconda parte dell'enunciato dice che, dette $y_1, \dots, y_m$ coordinate in k^m, esistono dei polinomi $f_i(x_1, \dots, x_n)$ per cui, dato $p = (x_1, \dots, x_n) \in V$, si ha che $y_i = f_i(x_1, \dots, x_n)$ sono le coordinate di $f(p)$.

La composizione di morfismi regolari è regolare e le varietà con i morfismi regolari formano una categoria.

Osservazione Il campo k si può pensare come lo spazio affine A^1 di dimensione 1 e $k[A^1] = k[x]$. Una funzione regolare $f : V \to k$ si può pensare dunque come un morfismo regolare da V a k, il comorfismo f^* è $f^*(x) = f$.

Il campo k si può però anche pensare come l'anello delle coordinate della varietà $\{0\} \in k^0$, lo spazio affine di dimensione 0 ridotto ad un punto. In questo caso la funzione *costante* $p : V \to \{0\}$ ha come comorfismo l'inclusione di k in $k[V]$ come costanti. Un punto $p \in V$ si può pensare come morfismo $\{0\} \xrightarrow{i_p} V$, $i_p(0) := p$. Il comorfismo associato è la valutazione nel punto p. Ovvero il passaggio al quoziente per l'ideale massimale $\underline{m}_p$ delle funzioni che svaniscono in p.

7.3 Teorema. *1) Una funzione $f : V \to W$ fra due varietà $V \subset k^n$, $W \subset k^m$ è un morfismo regolare se e solo se, per ogni $g \in k[W]$ si ha $g \circ f \in k[V]$.*

2) Dato un morfismo regolare $f : V \to W$ l'applicazione $g \to g \circ f$ si denota con $f^* : k[W] \to k[V]$, è un omomorfismo di $k-$algebre detto **comorfismo** *associato ad f.*

3) Dato un omomorfismo $F : k[W] \to k[V]$ di $k-$algebre esiste un unico morfismo regolare $f : V \to W$ per cui $F = f^*$.

Dim. 1) Per definizione $f : V \to W$ è un morfismo regolare se e solo se per ogni coordinata $y_i \in k[W]$ si ha $y_i \circ f = f_i(x_1, \dots, x_n) \in k[V]$. In questo caso, se $g = g(y_1, \dots, y_m)$ è una funzione polinomiale su W si ha $g \circ f = g(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$.

2) è evidente. Per quanto riguarda 3), indichiamo con $\overline{y}_i$, $i = 1, \dots, m$ le funzioni coordiante su W e $\overline{x}_j$ $j = 1, \dots, n$ le funzioni coordiante su V. Per ipotesi esistono polinomi (non unici) $f_i(x_1, \dots, x_n)$ per cui $F(\overline{y}_i) = f_i(\overline{x}_1, \dots, \overline{x}_n)$, $i = 1, \dots, m$. Consideriamo l'applicazione polinomiale $f : k^n \to k^m$ data in coordinate da $y_i := f_i(x_1, \dots, x_n)$. f manda V in W ovvero $f(V) \subset W$. Infatti F è un omomorfismo e se $h(y_1, \dots, y_m)$ è 0 su W si ha che

$$0 = F(h(\overline{y}_1, \dots, \overline{y}_m)) = h(F(\overline{y}_1), \dots, F(\overline{y}_m)) = h(f_1(\overline{x}_1, \dots, \overline{x}_n), \dots, f_m(\overline{x}_1, \dots, \overline{x}_n)).$$

Per definizione $f^*(\overline{y}_i) = F(\overline{y}_i)$. Poiché $k[W]$ è generato dalle coordinate $\overline{y}_i$, F è determinato dal valore che prende sulle coordinate e ne segue che $F = f^*$.

□

Per costruzione date 3 varietà U, V, W e due morfismi $U \xrightarrow{f} V \xrightarrow{g} W$ si ha $(g \circ f)^* = f^* \circ g^*$ in quanto se $h : W \to k$ è una funzione regolare si ha

$$(g \circ f)^*(h) = h \circ (g \circ f) = (h \circ g) \circ f = f^*(h \circ g) = f^*(g^*(h)) = (f^* \circ g^*)(h).$$

È anche evidente che il comorfismo associato alla applicazione identica di una varietà è l'identità dell'anello delle coordinate, in definitiva abbiamo costruito un *funtore controvariante* $V \to k[V]$ dalla categoria delle varietà affini alla categoria delle algebre finitamente generate su k e prive di elementi nilpotenti. Il Teorema 7.3 si può reinterpretare come.

7.4 Teorema. *Il funtore controvariante $V \to k[V]$ stabilisce una equivanza fra la categoria delle varietà affini e l'opposta della categoria delle algebre finitamente generate su k e prive di elementi nilpotenti.*

Vi è un punto che va chiarito immediatamente ed è che la nozione di isomorfismo $f : V \to W$ fra varietà è, per la definizione categorica, un morfismo per cui esiste un inverso $g : W \to V$ $(f \circ g = 1_W,\ g \circ f = 1_V)$.

Certamente un isomorfismo $f : V \to W$ induce una corrispondenza biunivoca fra i punti delle varietà, ma anche un isomorfismo fra gli anelli delle coordinate.

NON è vero che un morfismo $f : V \to W$ fra varietà, il quale induce una corrispondenza biunivoca fra i punti, è un isomorfismo.[14] L'esempio più semplice si ha nella parametrizzazione della cubica cuspidata, ovvero la curva piana C di equazione $y^2 = x^3$. L'applicazione $f : A^1 \to C$ data in coordinate $t \to (t^2, t^3)$ è biunivoca ma non è un isomorfismo, infatti il comorfismo manda l'anello $k[x, y]/(y^2 - x^3)$ delle coordinate di C nell'anello $k[t]$ delle coordinate di A^1 mandando le classi di x, y in t^2, t^3. Si vede facilmente che $t \notin k[t^2, t^3] \subsetneq k[t]$.

Un'altro esempio importante è il *morfismo di Frobenius* in caratteristica $p > 0$.

L'applicazione $F : A^1 \to A^1$, data dalla formula $t \to t^p$, è biunivoca ma ha *grado p*. Si tratta dell'esempio più semplice di *morfismo inseparabile*.

Finalmente un punto che chiariremo in seguito, in generale non è vero che l'immagine $f(V)$ di un morfismo $f : V \to W$ sia una sottovarietà di W, un semplice esempio è il morfismo $p : k^2 \to k^2,\ p(x, y) := (xy, y)$. In ogni caso ogni morfismo ha una fattorizzazione canonica $f : V \to \overline{f(V)} \to W$ dove $\overline{f(V)}$ è la sottovarietà di W definita dall'ideale nucleo del comorfismo $f^* : k[W] \to k[V]$, e quindi $k[\overline{f(V)}] = f^*k[W]$.

7.5 Definizione. *Un morfismo $f : V \to W$ di varietà si dice una* **immersione chiusa** *se f è un isomorfismo di V con una sottovarietà di W.*

Un morfismo $f : V \to W$ di varietà irriducibili si dice **dominante** *se $\overline{f(V)} = W$.*

In questo linguaggio possiamo dire che:

7.6 Proposizione. *Un morfismo $f : V \to W$ di varietà irriducibili si fattorizza in modo canonico come $f : V \xrightarrow{p} U \xrightarrow{i} W$ con $V \xrightarrow{p} U$ dominante e $U \xrightarrow{i} W$ una immersione chiusa.*

8 Lo spettro

Aspetti geometrici elementari

Possiamo ora vedere alcuni aspetti geometrici elementari di questa costruzione.

La prima osservazione che vogliamo fare è la seguente.

[14] lo è se e solo se induce isomorfismo sugli anelli di coordinate.

8.1 Proposizione. *Dato un morfismo $f : V \to W$ di varietà, se $U = V(I)$, $I \subset W$ è una sottovarietà si ha*

$$f^{-1}(U) = V(f^*(I)).$$

In particolare f è continua per la topologia di Zariski.

Inoltre, date due varietà $V \subset k^n$, $W \subset k^m$ ed un morfismo regolare $f : k^n \to k^m$, esso induce un morfismo regolare $f : V \to W$ fra le due varietà se e solo se $f^*(I(W)) \subset I(V)$.

Dim. $f(x) \in U$ se e solo se per ogni $g \in I$ si ha $g(f(x)) = 0$ ma $g(f(x)) = f^*(g)(x)$ e quindi $f(x) \in U$ se e solo se $x \in V(f^*(I))$. Per la seconda parte, $f(V) \subset W$ se e solo se $V \subset f^{-1}(W)$ se e solo se $I(V) \supset f^*(I(W))$. □

Il secondo punto è il modo *intrinseco* di ricostruire V a partire dal suo anello $A = k[V]$.

8.2 Proposizione. *Dato un anello finitamente generato su k e senza nilpotenti i punti della varietà ad esso associata sono in corrispondenza biunivoca con gli ideali massimali di A.*

Dim. Segue immediatamente dai teoremi 1.6 ed 1.8. □

Per un anello commutativo A qualunque l'insieme degli ideali massimali

$$Spec_m(A) := \{\underline{m} \subset A| \quad \underline{m} \quad \text{ideale massimale in} \quad A\},$$

è detto *spettro massimale di A.*

Assumiamo ora che A è finitamente generato su un campo algebricamente chiuso k e vediamo come A induce un anello di funzioni e la topologia di Zariski su $Spec_m(A)$.

Dato $S \subset A$ poniamo

$$V(S) := \{\underline{m} \in Spec_m(A)| \ S \subset \underline{m}\}.$$

Inoltre da 1.6 si ha che, se $\underline{m} \in Spec_m(A)$ abbiamo $A/\underline{m} = k$ pertanto ogni elemento $a \in A$ modulo $\underline{m}$ è uguale ad un elemento:

$$\overline{a}(\underline{m}) := a + \underline{m} \in A/\underline{m} = k, \qquad \textit{valore di } a \textit{ in } \underline{m}.$$

Abbiamo definito, per ogni $a \in A$, una funzione $\overline{a}$ su $Spec_m(A)$ a valori in k.

L'applicazione $a \to \overline{a}$ è chiaramente un omomorfismo da A all'algebra delle funzioni su $Spec_m(A)$ a valori in k. L'ipotesi che A sia un anello finitamente generato su k implica che $\overline{a} = 0$ se e solo se a è nilpotenete, ovvero $A/\sqrt{\{0\}}$ si identifica ad un anello di funzioni su $Spec_m(A)$.

Dato un morfismo $F : A \to B$ fra anelli finitamente generati su k ed un ideale massimale $\underline{m} \subset B$ di B abbiamo:

8.3 LEMMA. *$F^{-1}(\underline{m}) \subset A$ è un ideale massimale di A. Inoltre se $a \in A$ si ha*

$$\overline{a}(F^{-1}(\underline{m})) = \overline{F(a)}(\underline{m}).$$

DIM. Abbiamo $k \subset A/F^{-1}(\underline{m}) \subset B/\underline{m} = k$ pertanto $k = A/F^{-1}(\underline{m})$, la formula segue dalle identificazioni fatte. □

In definitiva abbiamo percorso alla rovescia la costruzione *varietà → algebre*.
Vi è comunque un modo più simmetrico di pensare che lasciamo al lettore come esercizio.

8.4 TEOREMA. *Siano X un insieme A un anello, k un campo algebricamente chiuso e $v : X \times A \to k$ una funzione detta valutazione, allora X è una varietà affine, A il suo anello di coordinate e $v(p, a)$ la valutazione della funzione $\overline{a}$ nel punto p se e solo se valgono le seguenti proprietà.*

(1) *A è un'algebra finitamente generata su k.*
(2) *Per ogni $p \in X$ l'applicazione $a \to v(p, a)$ è un omomorfismo $A \to k$ di k algebre.*
(3) *$v(p, a) = 0$ per ogni p se e solo se $a = 0$.*
(4) *Se $p \neq q \in X$ esiste $a \in A$ con $v(p, a) \neq v(q, a)$, separazione dei punti.*
(5) *Se $F : A \to k$ è un omomorfismo di k algebre esiste un punto $p \in X$ per cui $F(a) = v(p, a)$, completezza.*

Esercizio Mostrare con esempi che tutte le 5 condizioni precedenti sono necessarie ed indipendenti.

9 Aperti affini

Iniziamo ora una analisi che porta molto lontano, abbiamo visto che, quando V è una varietà affine, per definizione ogni sottoinsieme chiuso è una varietà. Cosa possiamo dire per gli insiemi aperti?
Iniziamo con un semplice esempio:

9.1 DEFINIZIONE. *Data una varietà affine V ed una funzione non nulla $f \in k[V]$ l'aperto:*

$$V_f := \{p \in V |\ f(p) \neq 0\}$$

è detto aperto affine elementare.

Vediamo in che senso V_f è affine. Prima di tutto una osservazione insiemistica (che ricorda il trucco di Rabinowitz). Supponiamo che $k[V] = k[x_1, \ldots, x_n]/I$, aggiungiamo una variabile y e consideriamo in $k[x_1, \ldots, x_n, y]$ l'ideale generato da $I, yf(x) - 1$, chiamiamo W_f la varietà affine che esso definisce.
L'esempio più semplice è $V = A^1$ l'asse x ed $f = x$, allora W_f è l'iperbole $xy = 1$.
Per costruzione, la proiezione $\pi : k^{n+1} \to k^n$, $(x_1, \ldots, x_n, y) \to (x_1, \ldots, x_n)$, manda W_f biunivocamente sull'aperto V_f di V. Osserviamo inoltre che, su V_f si possono definire le

funzioni $g(x)f(x)^{-k},\ g(x) \in k[V],\ k \in \mathbb{N}$. Abbiamo dunque un anello finitamente generato di funzioni su V_f che si denota con $k[V][1/f]$. Su W_f la funzione $f(x)$ è invertibile in $k[W_f]$ ed ha come inversa la classe della coordinata y. Nel comorfismo π^* l'anello delle funzioni $k[V][1/f]$ viene mandato (iniettivamente in quanto π è biunivoca) in $k[W_f]$, questo morfismo è anche suriettivo dato che $k[W_f]$ è generato dalle coordinate x_i che provengono da $k[V]$, e dalla coordinata y che corrisponde ad f^{-1}. Pertanto V_f con il suo anello di funzioni $k[V]_f$ è una varietà affine nel senso del Teorema 8.4, ed è isomorfa alla sottovarietà W_f di k^{n+1}.

È interessante vedere un'altra cosa:

9.2 Proposizione. *1) Una funzione $g(x) \in k[V]$ svanisce su V_f se e solo se $gf = 0$.*
2) L'ideale $J := (I, yf(x) - 1)$, è l'ideale di tutte le funzioni che svaniscono su W_f.

Dim. Se $g(p)f(p) = 0$ e $f(p) \neq 0$ si deve avere $g(p) = 0$ quindi g svanisce su V_f. Viceversa se g svanisce su V_f si ha $g(p)f(p) = 0$ in ogni punto di V e quindi $gf = 0$.

2) Poiché y è invertibile modulo $J := (I, yf(x) - 1)$ si ha che, modulo questo ideale, ogni elemento si scrive nella forma $g(x)y^h$. Supponiamo che un tale elemento svanisce su W_f, allora dalla analisi precedente deve essere $g(x)f(x) \in I$. Ma modulo J si ha $1 = yf(x)$ e $g(x)y^h = g(x)y^h yf(x) = g(x)f(x)y^{h+1} \in J$. □

9.3 Teorema. *Per gli aperti affini elementari di una varietà V valgono le seguenti proprietà.*

$$V_1 = V, \quad V_0 = \emptyset, \quad V_f \cap V_g = V_{fg}, \quad V - V(S) = \cup_{s \in S} V_s.$$

Gli aperti affini elementari sono una base per la topologia di Zariski della varietà V.

L'anello $k[V]_f$ viene detto *localizzazione* di $k[V]$ rispetto al sistema moltiplicativo $\{f^k\}$ delle potenze di f. La localizzazione è un metodo potente che studieremo in dettaglio.

Per ora introduciamolo in un caso speciale. Se A è un dominio, abbiamo il suo campo delle frazioni F. Se S è un insieme moltiplicativo di A poniamo:

$$A[S^{-1}] := \{\frac{a}{s} \mid a \in A,\ s \in S\}. \tag{9.4}$$

$A[S^{-1}]$ è un anello, in quanto:

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}, \quad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \tag{9.5}$$

$A[S^{-1}]$ è detto *localizzazione di A ad S*. Di fatto una costruzione più generale vale anche se A non è un dominio e verrà studiata nel Cap. 2.

10 Connessione ed idempotenti

Per una varietà V, come per ogni spazio topologico, si può studiare la proprietà di connessione (per la topologia di Zariski). Per definizione V è sconnessa, se $V = W_1 \cup W_2$ con W_1, W_2 due sottovarietà non vuote e $W_1 \cap W_2 = \emptyset$. Chiaramente la sconnessione è una proprietà più forte della riducibilità. Ad esempio due rette distinte nel piano formano sempre una varietà riducibile, che è sconnessa se e solo se le due rette sono parallele.

Sia $V = W_1 \cup W_2$ sconnessa, indichiamo per semplicità con A il suo anello di coordinate e siano I_1, I_2 gli ideali che definiscono W_1, W_2. Poiché $W_1 \cap W_2 = \emptyset$ si deve avere $I_1 + I_2 = A$, d'altra parte $V = W_1 \cup W_2$ e quindi $I_1 \cap I_2 = 0$.

Questo vuol dire che $A = I_1 \oplus I_2 = A/I_1 \oplus A/I_2$ è una somma diretta dei due anelli $A_1 := A/I_1,\ A_2 := A/I_2$, delle funzioni regolari su W_1 e W_2. In particolare 1 si scrive come somma $1 = e + f,\ e \in A_1,\ f \in A_2$ con $e^2 = e,\ f^2 = f$. Geometricamente e è la funzione caratteristica di W_1 ed f quella di W_2.

Viceversa si vede facilmente che, se un anello A contiene un idempotenete $e,\ e^2 = e$ allora $A = Ae \oplus A(1 - e)$.

Pertanto una varietà V è connessa se e solo se il suo anello di coordinate $k[V]$ non possiede idempotenti non banali (ovvero $\neq 0, 1$).

Per induzione Noetheriana si prova che una varietà affine V si scrive in modo unico come unione disgiunta di componenti connesse ed il suo anello A di coordinate si decompone $A = A_1 \oplus A_2 \oplus \cdots \oplus A_k$ come somma diretta di anelli privi di idempotenti non banali.

11 Prodotti

Vogliamo discutere il concetto di *prodotto di varietà*, iniziamo in modo elementare, prendiamo due varietà $V \subset k^n,\ W \subset k^m$, usiamo in k^n coordinate $(x_1, \ldots, x_n)$ ed in k^m coordinate $(y_1, \ldots, y_m)$.

Sia V data da equazioni $f_i(x) = 0,\ i = 1, \ldots, a$ e W data da equazioni $g_j(y) = 0,\ i = 1, \ldots, b$. In modo evidente il sistema di equazioni composto $f_i(x) = 0,\ i = 1, \ldots, a;\ g_j(y) = 0,\ i = 1, \ldots, b$ definisce in k^{n+m} e coordinate $(x_1, \ldots, x_n, y_1, \ldots, y_m)$ la varietà che come insieme è $V \times W \subset k^m \times k^m = k^{n+m}$. Per giustificare a pieno che questa è la costruzione di prodotto di varietà vanno svolte varie considerazioni. Prima di tutto riformuliamo in termini dei due ideali, che siano:

$$I := (f_1(x), \ldots, f_a(x)) \subset k[x_1, \ldots, x_n],\ J := (g_1(y), \ldots, g_b(y)) \subset k[y_1, \ldots, y_m],$$

In $k[x_1, \ldots, x_n, y_1, \ldots, y_m] = k[x_1, \ldots, x_n] \otimes k[y_1, \ldots, y_m]$ l'ideale K generato dai polinomi $f_i(x),\ i = 1, \ldots, a;\ g_j(y),\ i = 1, \ldots, b$ è $K = I \otimes k[y_1, \ldots, y_m] + k[x_1, \ldots, x_n] \otimes J$ e quindi:

$$k[x_1, \ldots, x_n, y_1, \ldots, y_m]/K = k[x_1, \ldots, x_n]/I \otimes k[y_1, \ldots, y_m]/J$$

Il teorema principale è:

11.1 Teorema. *1) Se I, J sono ideali radicali anche K lo è ovvero:*
$k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J$ è privo di nilpotenti.
2) Se I, J sono ideali primi anche K lo è ovvero $k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J$ è un dominio.

Dim. Sia $u_1, u_2, \dots, u_t, \dots$ una base di $k[x_1, \dots, x_n]/I$ su k che quindi è una base di $k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J$ su $k[y_1, \dots, y_m]/J$. Prendiamo un elemento non nullo $a := \sum_{j=1}^{N} u_j \otimes h_j(y) \in k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J$. Vogliamo provare che non è nilpotente. Poiché almeno uno dei polinomi $h_j(y)$ è non nullo, dal Nullstellensatz segue che esiste un morfismo $p : k[y_1, \dots, y_m]/J \to k$ con $p(h_j) \neq 0$. Questo da luogo ad un morfismo $1 \otimes p : k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J \to k[x_1, \dots, x_n]/I \otimes k = k[x_1, \dots, x_n]/I$ con $(1 \otimes p)(a) = \sum_{j=1}^{N} u_j p(h_j(y)) \in k[x_1, \dots, x_n]/I$. Per ipotesi u_j è una base e quindi $(1 \otimes p)(a) \neq 0$. Poiché per ipotesi $k[x_1, \dots, x_n]/I$ è privo di nilpotenti si ha che a non può essere nilpotente.

2) Supponiamo ora che $k[x_1, \dots, x_n]/I$ e $k[y_1, \dots, y_m]/J$ sono domini. Prendiamo due elementi non nulli $a := \sum_{j=1}^{N} u_j \otimes h_j(y)$, $b := \sum_{j=1}^{N} u_j \otimes r_j(y) \in k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J$. Vogliamo provare che il loro prodotto non è 0. Sia ad esempio $h_s(y) \neq 0$, $r_t(y) \neq 0$ poichè $k[y_1, \dots, y_m]/J$ è un dominio $h_s(y) r_t(y) \neq 0$ ed esiste un morfismo $p : k[y_1, \dots, y_m]/J \to k$ con $p(h_s(y) r_t(y)) \neq 0$. Questo da luogo ad un morfismo $1 \otimes p : k[x_1, \dots, x_n]/I \otimes k[y_1, \dots, y_m]/J \to k[x_1, \dots, x_n]/I \otimes k = k[x_1, \dots, x_n]/I$ con $(1 \otimes p)(ab) = \sum_{j=1}^{N} u_j p(h_j(y)) \sum_{j=1}^{N} u_j p(r_j(y)) \in k[x_1, \dots, x_n]/I$. Per ipotesi u_j è una base e quindi $(1 \otimes p)(a) \neq 0$, $(1 \otimes p)(b) \neq 0$. Poiché per ipotesi $k[x_1, \dots, x_n]/I$ è un dominio si ha che $(1 \otimes p)(ab) \neq 0$ e quindi $ab \neq 0$.

□

Osservazione È essenziale per questo teorema che k sia algebricamente chiuso, altrimenti si possono avere vari fenomeni.
i) ESEMPIO $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}$, il prodotto tensoriale di due domini non è un dominio.

ii) ESEMPIO Sia k un campo di caratteristica $p > 0$ e sia $K := k(x)$, $F := k(x^p)$. È facile vedere che $0 \neq x \otimes 1 - 1 \otimes x \in K \otimes_F K$ mentre $(x \otimes 1 - 1 \otimes x)^p = x^p \otimes 1 - 1 \otimes x^p = 0$. Questo è un fenomeno che dipende dalla *inseparabilità*.

ESERCIZIO Siano A, B due algebre sopra un campo F di caratteristica 0 e senza elementi nilpotenti, dimostrare che $A \otimes_F B$ non ha elementi nilpotenti.

Il teorema 11.1 ci assicura che la costruzione intuitiva fatta è in effetti ben posta perchè prova che, se V, W sono varietà con anelli di coordinate $k[V]$, $k[W]$ allora $k[V] \otimes_k k[W]$ è un'algebra finitamente generata priva di nilpotenti per cui:

$$Spec_m(k[V] \otimes_k k[W]) = Spec_m(k[V]) \times Spec_m(k[W]). \tag{11.2}$$

Finalmente se usiamo il linguaggio delle categorie vediamo che $V \times W$ prima definita è un *prodotto categorico* nella categoria delle varietà, nel senso che vi è una corrispondenza

biunivoca funtoriale, per ogni varietà X fra l'insieme dei morfismi regolari $X \to V \times W$ e le coppie di morfismi $X \to V,\ X \to W$. Infatti le proprietà analoghe dei prodotti tensoriali implicano che:

$$hom(k[V] \otimes_k k[W], k[X]) = hom(k[V], k[X]) \times hom(k[W], k[X]). \tag{11.3}$$

Prendiamo ora due algebre B, C su un anello commutativo A, possiamo considerare l'anello $B \otimes_A C$. Esso gode della proprietà universale, vi sono due morfismi ed un diagramma commutativo universale:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & {\scriptstyle i}\downarrow \\ C & \xrightarrow{j} & B \otimes_A C \end{array} \quad , \qquad i(b) := b \otimes 1,\ j(c) := 1 \otimes c$$

ovvero per ogni altro diagramma commutativo:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & {\scriptstyle \overline{i}}\downarrow \\ C & \xrightarrow{\overline{j}} & D \end{array} \quad , \qquad \exists!\ p : B \otimes_A C \to D,\ p(b \otimes c) := \overline{i}(b)\overline{j}(c)$$

Possiamo esprimere tutto questo in un liguaggio geometrico più evocativo. Ricordiamo che, dato un diagramma di insiemi:

$$\begin{array}{ccc} & & C \\ & & {\scriptstyle j}\downarrow \\ B & \xrightarrow{i} & A \end{array} \quad , \qquad B \times_A C := \{(b, c) \in B \times C | i(b) = j(c)\}$$

$B \times_A C$ è detto *prodotto fibrato* di B, C su A.

Negli anelli, abbiamo detto che un anello A si può pensare come l'anello delle coordinate di una specie di varietà, schema affine, che denotiamo $\underline{A}$ e gli omomorfismi $\underline{A}(D) := hom(A, D)$ come i *punti* di $\underline{A}$ di coordinate in D.

In questo senso lo schema affine $\underline{B \otimes_A C}$ associato a $B \otimes_A C$ è prodotto fibrato in quanto i suoi punti con coordinate in D sono proprio $\underline{B}(D) \times_{\underline{A}(D)} \underline{C}(D)$, per ogni D.

In particolare se A, B, C sono anelli di coordinate di varietà V, W, Z su un campo algebricamente chiuso k, $B \otimes_A C$ è un algebra finitamente generata su k ed i punti a valori in k di $B \otimes_A C$ sono il prodotto fibrato $W \times_V Z$. Quello che però non è in generale vero è che $B \otimes_A C$ sia priva di nilpotenti. Infatti è interessante capire cosa significa questo fenomeno.

Facciamo un esempio significativo, la *fibra* in un punto. Prendiamo dunque come W un punto, il morfismo $W \to V$ consiste nel scegliere un punto p di V, mentre $f : Z \to V$ è

un morfismo dato. Identificando $\{p\} \times Z \cong Z$, insiemisticamente $\{p\} \times_V Z := f^{-1}(p)$ è la fibra di p nel morfismo f. A livello di anelli abbiamo

$$A = k[V],\ B = k = A/\underline{m},\ C = k[Z], \quad A/\underline{m} \otimes_A C = C/\underline{m}C.$$

dove C è un A modulo tramite f^*.

Facciamo un esempio:

Z sia il cerchio di equazioni $x^2 + y^2 - 1 = 0$ con coordinate $C = \mathbb{C}[x, y]/(x^2 + y^2 - 1)$. Sia A l'asse x con coordinate $\mathbb{C}[x]$, il morfismo è la proiezione $(x, y) \to x$ a cui corrisponde l'omomorfismo $\mathbb{C}[x] \to \mathbb{C}[x, y]/(x^2 + y^2 - 1)$. Preso un punto $x = a$ l'anello $C/\underline{m}C$ è $\mathbb{C}[x, y]/(x^2 + y^2 - 1, x - a) = \mathbb{C}[y]/(y^2 + a^2 - 1)$. Se $1 - a^2 \neq 0$ vi sono due radici quadrate $\pm\alpha = \sqrt{1 - a^2}$ e $\mathbb{C}[y]/(y^2 + a^2 - 1) = \mathbb{C}[y]/(y - \alpha) \oplus \mathbb{C}[y]/(y + \alpha) = \mathbb{C} \oplus \mathbb{C}$ per $a^2 = 1$ abbiamo invece $\mathbb{C}[y]/(y^2 + a^2 - 1) = \mathbb{C}[y]/(y^2)$ ha un elemento nilpotente.

Geometricamente questo corrisponde al fatto che per $a \neq \pm 1$ la retta $x = a$ interseca il cerchio in due punti distinti, mentre per $a = \pm 1$ è *tangente*. In termini più analitici i punti di tangenza del cerchio sono esattamente i due punti in cui il differenziale del morfismo di proiezione si annulla, ovvero punti di singolarità del morfismo. In qualche senso quindi il fenomeno degli elementi nilpotenti è legato a questioni infinitesimali, o da pensare come tangenze o come singolarità!

12 Dipendenza integrale, 2

Abbiamo già visto giuocare un ruolo importante nel Nullstellensatz del concetto di dipendenza integrale. Vogliamo espandere su queste idee.

12.1 Teorema. *Sia F un campo, $A \subset F$ un sottoanello con F integrale su A. Allora A è un campo.*

Dim. Sia $a \neq 0,\ a \in A$, prendiamo una equazione intera per $1/a$ del tipo $(1/a)^n + b_1(1/a)^{n-1} + \cdots + b_n = 0,\ b_i \in A$. Moltiplicando per a^n abbiamo $1 + b_1 a + \cdots + b_n a^n = 0,\ 1 = a(-b_1 - \cdots - b_n a^{n-1})$ quindi $1/a = -b_1 - \cdots - b_n a^{n-1} \in A$. □

Il lettore attento si accorgerà che un ragionamento quasi identico è stato usato per dimostrare il Nullstellensatz.

Come corollario di questo Teorema otteniamo il cosidetto *Teorema di going up di Cohen Seidenberg.*

Corollario. *Siano $A \subset B$ anelli con B integrale su A e P un ideale primo di A, allora esiste un ideale primo Q di B con $Q \cap A = P$.*

Se P è massimale si può prendere Q massimale.

Dim. Sia $S := A - P$ e formiamo le localizzazioni $A[S^{-1}] \subset B[S^{-1}]$. Chiaramente $B[S^{-1}]$ è integrale su $A[S^{-1}] = A_P$, un anello locale. Sia ora M un ideale massimale di

$B[S^{-1}]$. Il campo $B[S^{-1}]/M$ è integrale su $A_P/M \cap A_P$. Dal teorema precedente questo implica che $A_P/M \cap A_P$ è un campo e quindi $M \cap A_P$ è l'unico ideale massimale di A_P. Dal diagramma commutativo:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & {\scriptstyle p}\downarrow \\ A_P/M \cap A_P & \longrightarrow & B[S^{-1}]/M \end{array}$$

deduciamo che $Q := ker\, p$ è un ideale primo con $Q \cap A = P$.

Per l'ultima parte sia $M \supset Q$ massimale, si ha $M \cap A \supset P$. Poiché P è massimale $M \cap A = P$. □

Nel caso gemetrico in cui A, B sono anelli di coordinate di varietà V, W l'inclusione corrisponde ad un morfismo $f : W \to V$ ed il teorema precedente, implica che f è *suriettivo*.

In generale si può utilizzare la dipendenza integrale per ottenere delle riduzioni, tramite il fondamentale *lemma di normalizzazione*.

Lo vediamo prima nella forma di Hilbert poi in quella di Noether.

Sia $A = F[x_1, \dots, x_n]/I$ un algebra finitamente generata su un campo F, assumiamo prima di tutto che F sia infinito.

Indichiamo con $\overline{x}_i$ la classe di x_i modulo I.

12.2 Teorema. *A) Esiste un cambiamento di coordinate invertibile* $x_i := \sum_{j=1}^{n} a_{ij} z_j$, $a_{ij} \in F$ *ed un* $k \leq n$ *per cui, indicando con* $\overline{z}_i$ *la classe di* z_i *modulo* I.

i) Gli elementi $\overline{z}_i$, $i \leq k$ *sono algebricamente indipendenti su* F.

ii) A *è integrale su* $F[\overline{z}_1, \dots, \overline{z}_k]$.

B) Se non assumiamo F *infinito esistono comunque elementi* z_i, $i \leq k$ *algebricamente indipendenti su* F *con* A *integrale su* $F[z_1, \dots, z_k]$.

Dim. Se $I \neq 0$ prendiamo una equazione $f(x_1, \dots, x_n) \in I$, sia f di grado k e sia $f_k(x_1, \dots, x_n)$ la parte omogenea di grado massimo. Sostituiamo $x_i = z_i + a_i z_n$, $i < n$, $x_n = a_n z_n$ in f e $f(z_1 + a_1 z_n, z_2 + a_2 z_n, \dots, a_n z_n) \in I$. Il termine di grado massimo in z_n è $f_k(a_1 z_n, a_2 z_n, \dots, a_n z_n) = f_k(a_1, a_2, \dots, a_n) z_n^k$. Poiché F è infinito possiamo trovare elementi $a_i \in F$ per cui $= f_k(a_1, a_2, \dots, a_n) \neq 0$, ne deduciamo una equazione integrale di $\overline{z}_n$ su $F[\overline{z}_1, \dots, \overline{z}_{n-1}]$. Possiamo ora continuare nello stesso modo fino a quando non troviamo classi algebricamente indipendenti su F.

Nel caso generale bisogna fare un cambiamento di variabili non lineare, prendere $x_n = y_n$, $x_i = y_i + y_n^{r_i}$. Se $I \neq 0$ prendiamo una equazione $f(x_1, \dots, x_n) \in I$, di grado k e sia $f_k(x_1, \dots, x_n) = \sum a_{h_1, \dots, h_n} x_1^{h_1} \dots x_n^{h_n}$ la parte omogenea di grado massimo. Sostituiamo le y e scegliamo gli r_i in modo tale che i numeri $r_1 h_1 + r_2 h_2 + \dots + h_n$ siano distinti, il termine di grado massimo in y_n viene quindi da uno di questi monomi ed ha coefficiente costante non nullo, di nuovo y_n è integrale sul sottoanello generato dai rimanenti y_i, $i < n$. Come prima si conclude per induzione. □

Interpretiamo i precedenti risultati nel linguaggio geometrico.

12.3 Definizione. *Un morfismo $f : V \to W$ di varietà affini si dice* **finito** *se $k[V]$ è integrale su $f^*k[W]$.*

12.4 Teorema. *Un morfismo finito $f : V \to W$ di varietà affini è suriettivo se e solo se il comorfismo $f^* : k[W] \to k[V]$ è iniettivo.*

Se $V \subset k^n$ è una varietà affine esiste $m \leq n$ e **proiezioni lineari generiche,** *$\pi : k^n \to k^m$ per cui $\pi : V \to k^m$ è finita e suriettiva.*

Dim. La prima parte viene dal teorema di Cohen Seidenberg, e la seconda dal teorema 12.2 A. □

Possiamo finalmente utilizzare i risultati ottenuti per elucidare la natura dell'immagine di un morfismo. Possiamo prima enunciare un teorema algebrico.

12.5 Teorema. *Siano $A \supset B$ anelli, supponiamo che $A = B[r_1, \ldots, r_t]$ è finitamente generato su B e che B è un dominio. Esiste una $f \in B$, $f \neq 0$ e k elementi $a_1, \ldots, a_k$ in A tali che:*

i) $a_1, \ldots, a_k$ sono algebricamente indipendenti su $B[1/f]$.

ii) $A[1/f]$ è integrale su $B[1/f][a_1, \ldots, a_k]$.

Dim. Sia F il campo delle frazioni di B e costruiamo $A := A \otimes_B F$ (localizziamo ai non divisori di 0 di B). Applichiamo il Teorema di normalizzazione ad A su F e troviamo elementi $a_1, \ldots, a_k$ che a meno di moltiplicare per un denominatore possiamo assumere in A tali che $a_1, \ldots, a_k$ sono algebricamente indipendenti su F ed A è integrale su $F[a_1, \ldots, a_k]$. Scriviamo per ciascuno dei k generatori r_i una equazione integrale a coefficienti in $F[a_1, \ldots, a_k]$.

Esiste un $g \in B - 0$ per cui tali equazioni integrali hanno coefficienti in $B[1/g]$. Il fatto che tali equazioni siano 0 in A implica che esiste un $h \in B - 0$ per cui tali equazioni sono verificate in $A[1/g][1/h]$, prendendo $f := gh$ si ha l'asserto. □

Geometricamente il Teorema precedente ha il seguente significato. Supponiamo dunque $p : V \to W$ un morfismo di varietà con W irriducibile e $p(V)$ densa in W. Quindi $k[W] \subset k[V]$ soddisfa le ipotesi del precedente Teorema. Esiste una $f \neq 0$ tale che il morfismo ritretto agli aperti $p_f : V_f \to W_f$ si può scomporre come:

$$p_f : V_f \xrightarrow{q} W_f \times k^s \xrightarrow{\pi_1} W_f, \quad q \quad \text{finito e,} \quad \pi_1 \quad \text{la prima proiezione}$$

Notiamo in particolare che p_f è suriettivo e quindi l'immagine di p in W contiene l'aperto W_f.

Completiamo l'analisi mostrando che alcuni domini sono integralmente chiusi (nel campo delle frazioni).

12.6 Teorema. *i) Un anello a fattorizzazione unica è integralmente chiuso (in particolare un anello di polinomi $k[x_1, \ldots, x_n]$).*

ii) Se A è integralmente chiuso e S un sistema moltiplicativo $A[S^{-1}]$ è integralmente chiuso.

iii) Se A è integralmente chiuso l'anello dei polinomi $A[x]$ è integralmente chiuso.

DIM. i) Il ragionamento è simile al classico ragionamento sulle radici razionali di un polinomio. Prendiamo una frazione $f/g,\ f,g \in A$ e primi fra loro, se tale frazione soddisfacesse un polinomio di $t^m + a_1 t^{m-1} + \cdots + a_m$ di grado m in una variabile t moltiplicando per g^m si avrebbe $f^m + a_1 g f^{m-1} + \cdots + g^m a_m = 0$ e g divide f^m una contraddizione, a meno che g sia costante.

ii) Supponiamo che una frazione $u = f/g,\ f,g \in A$ soddisfa un polinomio di grado m in una variabile t a coefficienti $A[S^{-1}]$, sia s un denominatore comune dei coefficienti e moltiplichiamo per s^m otteniamo che us soddisfa un polinomio monico a coefficienti in A e quindi per ipotesi $us \in A$ ed $u \in A[S^{-1}]$.

iii) Per ora non dimostriamo questo teorema in generale ma solo sotto la ipotesi che A contenga un campo infinito F. Sia K il campo delle frazioni di A poiché $K[x]$ è integralmente chiuso basta mostrare che, se $u(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in K[x]$ è integrale su $A[x]$ allora $u(x) \in A[x]$. Sia $u(x)^m + a_1(x)u(x)^{m-1} + \cdots + a_m(x) = 0$ un polinomio a coefficienti in $A[x]$ soddisfatto da $u(x)$, ponendo $x = \alpha \in F$ abbiamo che $u(\alpha)$ è integrale su A e quindi $u(\alpha) = a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n \in A$. Ora prendendo n elementi distinti $\alpha_i \in F$ il sistema di equazioni $u(\alpha_i) = a_0\alpha_i^n + a_1\alpha_i^{n-1} + \cdots + a_n$ (in cui le a_i sono considerate incognite) si può risolvere con la regola di Cramer e le $a_i \in A$. □

13 L'immagine di un morfismo

Possiamo ora capire la natura dell'immagine di un morfismo.

13.1 DEFINIZIONE. *In uno spazio topologico X un insieme A si dice* **localmente chiuso** *se A è aperto nella sua chiusura $\overline{A}$.*

Un insieme A si dice **costruibile** *se A è unione finita di insiemi localmente chiusi.*

13.2 LEMMA. *In uno spazio topologico X l'unione finita, l'intersezione finita ed il complementare di insiemi costruibili è costruibile.*

DIM. Evidente. □

13.3 TEOREMA. *Dato un morfismo $p : V \to W$ di varietà affini l'immagine $p(V)$ è un insieme costruibile di W nella topologia di Zariski.*

DIM. Riduciamoci prima di tutto al caso di varietà irriducibili. Osserviamo che, se V è irriducibile, l'immagine di V è tutta contenuta in una componente irriducibile di W, poiché da $W = W_1 \cup W_2$ segue $V = p^{-1}W_1 \cup p^{-1}W_2$ e quindi $V = p^{-1}W_1$ ovvero $V = p^{-1}W_2$. Inoltre se $V = \cup_i V_i,\ p(V) = \cup p(V_i)$.

Supponiamo dunque V, W varietà irriducibili, possiamo anche assumere che $p(V)$ è densa in W e quindi $k[W] \subset k[V]$. Dal teorema 12.5 e sue conseguenze sappiamo che $p(V)$ contiene un aperto W_f.

Procediamo per induzione Noetheriana. Supponiamo per assurdo che esistano sottovarietà $X \subset V$ per cui l'immagine di $p_{|p^{-1}X} : p^{-1}X \to X$ non sia costruibile, prendiamone una minimale e chiamiamola ancora X, denotiamo per semplicità $p : p^{-1}X \to X$. Dalle osservazioni precedenti X è irriducibile e l'immagine di $p(p^{-1}X)$ contiene un aperto non vuoto X_f, detta dunque $Y := X - X_f$ abbiamo per induzione che $p(p^{-1}Y)$ è costruibile e $p(p^{-1}X) = p(p^{-1}Y) \cup X_f$ un insieme costruibile, otteniamo una contraddizione. □

Possiamo ulteriormente raffinare i teorema precedente, osserviamo prima di tutto che, poiché un insieme localmente chiuso è un aperto di una sottovarietà ha senso parlare di insiemi localmente chiusi affini.

13.4 Lemma. *Un insieme costruibile X di una varietà affine V è unione finita di insiemi localmente chiusi affini e disgiunti.*[15]

Dim. Per induzione noetheriana se esistono insiemi costruibili che non soddisfano la consizione data ne esiste uno X per cui $\overline{X}$ è minimale, ora è facile verificare che esiste un aperto affine U di $\overline{X}$ con $U \subset X$, per cui $X - U$ è costruibile e la sua chiusura è contenuto in $\overline{X} - U$. Pertanto per induzione $X - U$ è unione disgiunta di insiemi localmente chiusi affini e disgiunti e pertanto $X = (X - U) \cup U$ lo è. □

13.5 Teorema. *Dato un morfismo $p : V \to W$ di varietà affini l'immagine $p(X)$ di un insieme costruibile $X \subset V$ è un insieme costruibile di W nella topologia di Zariski.*

Dim. Dal lemma precedente X è unione di affini e possiamo applicare il Teorema 13.3 a ciascuno di tali affini ed infine il lemma 13.2. □

[15] volendo anche irriducibili