Il Teorema degli zeri di Hilbert e la geometria algebrica

Lucia Caporaso

Note per un minicorso di quattro lezioni tenuto presso l'INdAM nel Gennaio 2007
Versione INCOMPLETA!

Indice

L'obiettivo di queste lezioni è quello di discutere il Teorema degli zeri di Hilbert (o "Hilbert Nullstellensatz") illustrandone il ruolo nella geometra algebrica.

1 Il teorema degli zeri di Hilbert.

1.1 Il teorema degli zeri di Hilbert su $\mathbb{C}$.

Fissiamo un intero positivo n e consideriamo l'insieme delle n-uple di numeri complessi, $\mathbb{C}^n$, e l'anello dei polinomi in n variabili a coefficenti in $\mathbb{C}$, denotato $\mathbb{C}[x_1, \ldots, x_n]$.

Theorem 1.1.1 (Hilbert Nullstellensatz)**.** *La corrispondenza che associa al punto $a_1, \ldots, a_n$ di $\mathbb{C}^n$ l'ideale $(x_1 - a_1, \ldots, x_n - a_n)$ di $\mathbb{C}[x_1, \ldots, x_n]$ è una corrispondenza biunivoca tra $\mathbb{C}^n$ e l'insieme degli ideali massimali di $\mathbb{C}[x_1, \ldots, x_n]$.*

Dunque i punti di $\mathbb{C}^n$, che vediamo come oggetti geometrici, sono in corrispondenza biunivoca con certi ben specificati oggetti algebrici: gli ideali massimali di $\mathbb{C}[x_1, \ldots, x_n]$.

Il Teorema vale più in generale sostituendo a $\mathbb{C}$ un qualsiasi campo algebricamente chiuso. Qua ne daremo una dimostrazione valida per $\mathbb{C}$ e particolarmente istruttiva (tratta da [1]). Per una dimostrazione su campi algebricamente chiusi qualsiasi si veda il primo capitolo di [3].

Ricordiamo che un ideale massimale di un anello R è un ideale proprio $M \subsetneq R$ che non è contenuto in nessun altro ideale proprio di R. Una caratterizzazione fondamentale è la seguente: un ideale M dell'anello R è massimale se e solo se il quoziente R/M è un campo.

Comiciamo col dimostrare il caso $n = 1$ del Teorema, che è particolarmente semplice.

Dimostrazione per $n = 1$. Comiciamo col dimostrare che, per qualsiasi $a \in \mathbb{C}$ l'ideale $(x - a)$ è un ideale massimale dell'anello $\mathbb{C}[x]$. Consideriamo l'omomorfismo *valutazione in* a, v_a, definito come segue

$$\begin{array}{ccc} \mathbb{C}[x] & \xrightarrow{v_a} & \mathbb{C} \\ p(x) & \mapsto & p(a) \end{array} \tag{1}$$

che è un omomorfismo di anelli per sua stessa definizione. Osserviamo che è suriettivo (infatti la restrizione di v_a a $\mathbb{C}$ non è che l'identità di $\mathbb{C}$). Dunque il suo nucleo, $\ker v_a$, è un ideale massimale di $\mathbb{C}[x]$. Dimostriamo adesso che

$$\ker v_a = (x - a),$$

osserviamo subito che $x - a \in \ker v_a$ e quindi $\ker v_a \supset (x - a)$. Per concludere, si usa il fatto che l'anello $\mathbb{C}[x]$ è un dominio a ideali principali (ricordiamo che questo vale in generale per l'anello $k[x]$ per ogni campo k). Dunque esiste un polinomio $f \in \mathbb{C}[x]$ tale che $(f) = \ker v_a$; inoltre è chiaro che possiamo scegliere tra tutti i possibili generatori un generatore f monico e di grado minimo. Ora, abbiamo che $(x - a) = f \cdot q$ con $q \in \mathbb{C}[x]$ (dato che $x - a$ appartiene a (f)); per la minimalità del grado di f, e per aver scelto f monico, possiamo concludere che $q = 1$ e $f = x - a$. Questo chiude la prima parte della dimostrazione per $n = 1$; osserviamo che la stessa dimostrazione funziona per campi qualsiasi, dunque per ogni campo k e ogni $a \in k$ l'ideale $(x - a)$ è massimale in $k[x]$.

L'implicazione opposta è più interessante: sia $M \subset \mathbb{C}[x]$ un ideale massimale e dimostriamo che M è della forma $(x - a)$ per qualche $a \in \mathbb{C}$. Come abbiamo già ricordato, ogni ideale di $\mathbb{C}[x]$ è principale, dunque M ammette un generatore unico g; sicché $M = (g)$. Ora, poiché $\mathbb{C}$ è un campo algebricamente chiuso, il polinomio g ammette almeno una radice in $\mathbb{C}$. Altrimenti detto, esiste $a \in \mathbb{C}$ tale che $g(a) = 0$, equivalentemente, esiste $a \in \mathbb{C}$ tale che $g = (x - a)q$ dove $q \in \mathbb{C}[x]$. Ma allora l'ideale generato da g è contenuto nell'ideale (massimale come abbiamo visto prima) generato da $x - a$, ovvero $M \subset (x - a)$. Quindi, M essendo massimale, abbiamo $M = (x - a)$. ■

Osserviamo che l'unica proprietà di $\mathbb{C}$ che abbiamo utilizzato è il suo essere algebricamente chiuso. La stessa dimostrazione infatti dà che, per ogni campo algebricamente chiuso k, ogni ideale massimale $M \subset k[x]$ è della forma $(x-a)$ per $a \in k$. Il teorema è falso per campi non algebricamente chiusi, cioè esistono ideali massimali che non sono generati da polinomi di grado 1:

Esempio 1.1.2. Nell'anello $\mathbb{Q}[x]$ (polinomi a coefficienti razionali) l'ideale $M = (x^2 + 1)$ è massimale e non ammette un generatore di grado 1, poiché il polinomio $x^2 + 1$ non ha radici in $\mathbb{Q}$.

Dimostrazione per ogni n. Anche adesso procediamo dimostrando prima che un ideale della forma $(x_1 - a_1, \ldots, x_n - a_n)$ è massimale in $\mathbb{C}[x_1, \ldots, x_n]$; questa è la parte facile del teorema e vale per campi qualsiasi. Argomentiamo come per $n = 1$; dato $\underline{a} := (a_1, \ldots, a_n) \in \mathbb{C}^n$ definiamo l'omomorfismo di valutazione $v_{\underline{a}}$ come segue

$$\begin{array}{ccc} \mathbb{C}[x_1, \ldots, x_n] & \xrightarrow{v_{\underline{a}}} & \mathbb{C} \\ p(x_1, \ldots, x_n) & \mapsto & p(a_1, \ldots, a_n) \end{array} \tag{2}$$

Chiaramente $v_{\underline{a}}$ è un omomorfismo suriettivo il cui nucleo $\ker v_{\underline{a}}$ è quindi un ideale massimale di $\mathbb{C}[x_1, \ldots, x_n]$. Osserviamo che per ogni $i = 1, \ldots, n$ il polinomio $x_i - a_i$ sta in $\ker v_{\underline{a}}$, sicché

$$(x_1 - a_1, \ldots, x_n - a_n) \subset \ker v_{\underline{a}}.$$

Dobbiamo quindi dimostrare che $(x_1 - a_1, \ldots, x_n - a_n) = \ker v_{\underline{a}}$.

Trattiamo prima il caso speciale $\underline{a} = (0, \ldots, 0)$. Sia $f \in \ker v_{\underline{a}}$, cioè $f(0, \ldots, 0) = 0$; quindi a f manca il termine costante, ovvero abbiamo

$$f = \sum_{i=1}^{n} c_i x_i + \sum_{i \leq j} c_{i,j} x_i x_j + ... = \sum_{i=1}^{n} x_i g_i$$

dove le c_* sono elementi in $\mathbb{C}$ e i $g_i \in \mathbb{C}[x_1, \ldots, x_n]$ sono polinomi. Quindi $f \in (x_1, \ldots, x_n)$ che è quello che volevamo. Il caso $\underline{a}$ qualsiasi si riconduce al caso appena trattato effettuando il cambiamento di variabili $x_i' = x_i - a_i$ per $i = 1, \ldots, n$ (detto in altri termini, sviluppando f in serie di Taylor localmente nel punto $(a_1, \ldots, a_n)$).

Come per il caso $n = 1$ la parte veramente interessante è l'implicazione opposta: dimostrare che un ideale massimale $M \subset \mathbb{C}[x_1, \ldots, x_n]$ è generato da n polinomi lineari. Consideriamo il morfismo quoziente π

$$\mathbb{C}[x_1, \ldots, x_n] \xrightarrow{\pi} \frac{\mathbb{C}[x_1, \ldots, x_n]}{M} = K$$

dove K è un campo. Consideriamo la restrizione di π al sottoanello $\mathbb{C}[x_1] \subset \mathbb{C}[x_1, \ldots, x_n]$, e denotiamola π_1:

$$\mathbb{C}[x_1] \xrightarrow{\pi_1} K$$

π_1 è dunque un omomorfismo. Il punto della dimostrazione è il seguente
Passo cruciale: π_1 *non è iniettivo (ovvero* $\ker \pi_1 \neq (0)$*).*

Diamo per dimostrato il Passo cruciale e mostriamo come da esso il Teorema segue facilmente. Ricordiamo nuovamente che $\mathbb{C}[x_1]$ è un dominio a ideali principali, quindi esiste $f \in \mathbb{C}[x_1]$ tale che $\ker \pi_1 = (f)$, e possiamo scegliere f monico e di grado minimo. Poiché $\ker \pi_1$ non è l'ideale 0, certamente $f \neq 0$.

Poiché $\mathbb{C}$ è algebricamente chiuso, esiste $a_1 \in \mathbb{C}$ radice di f, ovvero $f = (x_1 - a_1)q$ dove $q \in \mathbb{C}[x_1]$ è un polinomio di grado minore del grado di f. Abbiamo quindi

$$0 = \pi_1(f) = \pi_1((x_1 - a_1))\pi_1(q),$$

poiché K è un campo, almeno uno dei due fattori del prodotto a destra si annulla. Ne concludiamo che almeno uno tra $x_1 - a_1$ e q sta nel nucleo di π_1. Ora, ricordando che f è un generatore monico e di grado minimo, l'unica possibilità è che $q = 1$ e $f = x_1 - a_1$.

La conclusione è che $x_1 - a_1 \in \ker \pi_1 \subset \ker \pi = M$. Applicando lo stesso ragionamento alle altre variabili, otteniamo che esistono $a_1, \ldots, a_n$ in $\mathbb{C}$ tali che l'ideale $(x_1 - a_1, \ldots, x_n - a_n)$ è contenuto in M. Sappiamo però che $(x_1 - a_1, \ldots, x_n - a_n)$ è un ideale massimale, quindi $(x_1 - a_1, \ldots, x_n - a_n) = M$. Si noti che abbiamo in particolare ottenuto che $K = \mathbb{C}$ e che $\pi = v_{\underline{a}}$.

Dimostrazione del passo cruciale. Supponiamo per assurdo che π_1 sia iniettivo, e quindi che il campo K contenga una copia dell'anello dei polinomi in una variabile a coefficienti in $\mathbb{C}$; denotiamo $\mathbb{C}[t] \subset K$ tale copia (sicché $t = \pi(x_1)$). Poiché K è un campo, K contiene anche il campo dei quozienti di $\mathbb{C}[t]$, che denotiamo, come d'uso, $\mathbb{C}(t)$ (il campo delle funzioni razionali in una variabile). Riassumendo, abbiamo un'inclusione

$$\mathbb{C}(t) \subset K = \frac{\mathbb{C}[x_1, \ldots, x_n]}{M}$$

che vogliamo ora studiare come inclusione di spazi vettorial su $\mathbb{C}$, e dimostrare in tal modo che tale inclusiome non può sussistere.

Lo spazio vettoriale $\mathbb{C}[x_1, \ldots, x_n]$ ha una base su $\mathbb{C}$ data dall'insieme di tutti i momomi: $\mathcal{B} = \{x_1^{d_1} \cdot \ldots \cdot x_n^{d_n} \ \ \forall d_i \geq 0\}$. $\mathcal{B}$ è ovviamente un insieme numerabile ovvero $\mathcal{B}$ ha la stessa cardinalità di $\mathbb{N}$; in simboli, scriveremo $\#\mathcal{B} = \#\mathbb{N}$. Ora, le immagini in K degli elementi di $\mathcal{B}$ generano necessariamente K come spazio vettoriale su $\mathbb{C}$; concludiamo quindi che la dimensione di K (come spazio vettoriale su $\mathbb{C}$) è al più numerabile (cioè o finita o uguale a $\#\mathbb{N}$).

Guardiamo ora a $\mathbb{C}(t)$ e costruiamo un suo sottoinsieme $\mathcal{G}$ di elementi linearmente indipendenti, tale che $\mathcal{G}$ ha cardinalità più che numerabile (ovvero $\#\mathcal{G} > \#\mathbb{N}$). Sia

$$\mathcal{G} := \{\frac{1}{t-a} \ \ \forall a \in \mathbb{C}\}.$$

É evidente che $\#\mathcal{G} = \#\mathbb{C}$ dato che $\mathcal{G}$ è in corrispondenza biunivoca con $\mathbb{C}$. É un fatto noto (si veda 1.2.3) che $\#\mathbb{C} > \#\mathbb{N}$; quindi $\mathcal{G}$ è un insieme più che numerabile. Ora, se $\mathcal{G}$ contiene un sottoinsieme di elementi linearmente indipendenti, abbiamo un'identità

$$\sum_{i=1}^{m} \frac{c_i}{t-a_i} = 0$$

dove le c_i sono numeri complessi non nulli e $a_i \neq a_j$. Nel punto a_1 (per fissare le idee) la funzione razionale $\frac{c_1}{t-a_1}$ non è definita, quindi il suo valore assoluto è una funzione non limitata localmente in a_1. D'altro canto per $i \geq 2$ le funzioni $\frac{c_i}{t-a_i}$ sono tutte di valore assoluto limitato in a_1. L'identità precedente darebbe quindi che una funzione non limitata è uguale ad una limitata il che è ovviamente impossibile.

Possiamo quindi concludere che K, contenendo $\mathbb{C}(t)$, contiene una collezione più che numerabile di elementi linearmente indipendenti. Questo è in contraddizione con il fatto che K ha dimensione al più numerabile (si veda 1.2.4). ■

1.2 Cenni sulla cardinalità di insiemi infiniti.

Proposizione 1.2.1. *Sia X un'unione numerabile di insiemi al più numerabili, ovvero $X = \cup_{i\in\mathbb{N}} X_i$ dove $\#X_i \leq \#\mathbb{N}$. Allora X è al più numerabile (ovvero $\#X \leq \#\mathbb{N}$).*

Dimostrazione. ■

Proposizione 1.2.2. *L'insieme dei numeri reali non è numerabile, ovvero $\#\mathbb{R} > \#\mathbb{N}$.*

Dimostrazione. ■

Corollario 1.2.3. $\#\mathbb{C} > \#\mathbb{N}$

Dimostrazione. Un sottoinsieme di un insieme numerabile è o finito o numerabile (esercizio). Dunque il Corollario segue dalla Proposizione 1.2.2. ■

Ci è utile il seguente

Lemma 1.2.4. *Sia V uno spazio vettoriale (su un campo qualsiasi) di dimensione numerabile. Allora ogni collezione di elementi linearmente indipendenti di V è o finita o numerabile.*

Dimostrazione. ■

2 Varietà algebriche

Nel definire le vaietà algebriche consideremo $\mathbb{C}^n$ come spazio ambiente. Premettiamo la seguente notazione: Sia $T \subset \mathbb{C}[x_1, \ldots, x_n]$ una qualsiasi collezione di polinomi.

$$Z(T) := \{\underline{a} \in \mathbb{C}^n : p(\underline{a}) = 0 \ \ \forall p \in T\}$$

Definizione 2.0.5. Un sottoinsieme $V \subset \mathbb{C}^n$ è una *varietà (algebrica)* se esiste $T \subset \mathbb{C}[x_1, \ldots, x_n]$ tale che $V = Z(T)$. Ovvero: una varietà algebrica in $\mathbb{C}^n$ è l'insieme di tutti gli zeri comuni ad una qualsiasi collezione di polinomi in

Esercizio 2.0.6. Se l'ideale generato da T è generato dai polinomi $f_1, \ldots, f_r$, allora

$$Z(T) = Z((T)) = Z(\{f_1, \ldots, f_n\}).$$

Esempio 2.0.7. $\mathbb{C}^n$ è una varietà algebrica: $\mathbb{C}^n = Z(0)$; un punto $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{C}^n$ è la varietà $\underline{a} = Z(x_1 - a_1, \ldots, x_n - a_n)$.

Dal Teorema degli zeri di Hilbert si deduce la seguente generalizzazione:

Proposizione 2.0.8. *Sia $I \subset \mathbb{C}[x_1, \ldots, x_n]$ un ideale e sia $V = Z(I)$. Allora i punti di V sono in corrispondenza biunivoca con gli ideali massimali di $\mathbb{C}[x_1, \ldots, x_n]/I$*

Dimostrazione. ■

Poniamoci adesso il problema di caratterizzare le collezioni di polinomi che determinano l'insieme vuoto, ovvero le collezioni di polinomi che non hanno zeri in comune. Sia $V = Z(I)$ e denotiamo $R := \mathbb{C}[\underline{x}]/I$ l'anello quoziente. Per il risultato precedente $V = \emptyset$ *se e solo se R non ha ideali massimali.* Dobbiamo quindi stabilire quali anelli sono privi di ideali massimali. Si tratta di una questione interessante per tutti gli anelli, dimostriamo quindi un risultato generale, piuttosto che uno limitato ai quozienti di anelli di polinomi.

Teorema 2.0.9. *Sia R un anello commutativo con unità . Allora R possiede un ideale massimale.*

Dimostrazione. Comiciamo con il considerare un ideale proprio, $I_1 \subsetneq R$, che sicuramente esiste, per esempio c'è l'ideale (0). Se I_1 è massimale abbiamo finito, altrimenti esiste un ideale I_2 tale che $I_1 \subsetneq I_2 \subsetneq R$. Di nuovo, se I_2 è massimale abbiamo finito, altrimenti iteriamo la costruzione. Questo ci porta a costruire una catena di ideali propri di R:

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_m \subsetneq \cdots \subsetneq R \tag{3}$$

Consideriamo l'unione di tutti gli ideali di questa catena,

$$\widehat{I} := \cup_{m \in \mathbb{N}} I_m$$

naturalmente $\widehat{I}$ è un ideale, inoltre $\widehat{I} \subsetneq R$ perché $\widehat{I}$ non contiene 1, dato che nessuno degli I_n contiene 1. Non possiamo però concludere che $\widehat{I}$ è un ideale massimale, difatti potrebbe benissimo non esserlo (si pensi al caso in cui R contiene catene più che numerabili di ideali).

Abbiamo due possibilità per procedere, che esaminiamo entrambe separatamente.

(1)*Supponiamo R Noetheriano* (come nel caso in cui R è della forma $\mathbb{C}[\underline{x}]/I$). Ricordiamo che un anello noetheriano è caratterizzato dalla condizione della catena ascendente di ideali, ovvero R è Noetheriano se e solo se ogni catena ascendente di ideali

$$J_1 \subset J_2 \subset \ldots \subset J_m \subset \ldots$$

diventa stazionaria dopo un numero finito di passi (ovvero esiste m_0 tale che $J_m = J_{m_0}$ per $m \geq m_0$). Allora la catena costruita in (3) è stazionaria dopo finiti passi, e quindi l'ideale $\widehat{I}$ è sicuramente massimale.
(2)*caso generale.* Utilizziamo il
Lemma di Zorn: *Sia $\mathcal{S}$ un insieme parzialmente ordinato tale che ogni catena (catena = insieme totalmente ordinato) $\mathcal{T}$ di elementi di $\mathcal{S}$ possiede un elemento maggiorante in $\mathcal{S}$ (ovvero per ogni catena $\mathcal{T}$ esiste $M(\mathcal{T}) \in \mathcal{S}$ tale che $M(\mathcal{T}) \geq T$ per ogni $T \in \mathcal{T}$). Allora $\mathcal{S}$ contiene un elemento massimale.*

Applichiamo il Lemma di Zorn prendendo come $\mathcal{S}$ l'insieme di tutti gli ideali propri di R parzialmente ordinato rispetto all'inclusione. Ragionando come prima abbiamo che ogni catena possiede un elemento maggiorante (l'unione di tutti gli ideali appartenenti alla catena). Quindi $\mathcal{S}$ ha un elemento massimalo, che è un ideale massimale di R. ■

Corollario 2.0.10. *Siano $f_1, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$. Allora*

$$Z(f_1, \ldots, f_r) = \emptyset \iff \exists\, h_1, \ldots, h_r \in \mathbb{C}[x_1, \ldots, x_n] : \sum_{i=1}^{r} h_i f_i = 1$$

Dimostrazione. Per 2.0.8 $Z(f_1, \ldots, f_r) = \emptyset$ se e solo se $\mathbb{C}[\underline{x}]/(f_1, \ldots, f_n)$ non possiede ideali massimali. Per il Teorema 2.0.9 questo è possibile solo se $\mathbb{C}[\underline{x}]/(f_1, \ldots, f_n)$ è l'anello $\{0\}$, ovvero se e solo se $(f_1, \ldots, f_n) = (1) = \mathbb{C}[x_1, \ldots, x_n]$. Quest'ultima condizione è equivalente a dire che esistono polinomi $h_1, \ldots, h_r$ tali che $\sum_{i=1}^{r} h_i f_i = 1$. ■

Osserviamo adesso che mentre un ideale I determina una varietà $V = Z(I)$, l'ideale I non è univocamente determinato da Z. Per esempio, è chiaro che in $\mathbb{C}$, il punto 0 soddisfa $0 = Z(x^d)$ per qualsiasi $d \in \mathbb{N}$. Ne segue che non possiamo neanche associare a V un unico anello R i cui ideali massimali corrispondano ai punti di V. Per ovviare a questo problema restringiamo l'attenzione ad ideali "radicali di $\mathbb{C}[x_1, \ldots, x_n]$.

Definizione 2.0.11. Sia I un ideale di $\mathbb{C}[x_1, \ldots, x_n]$. Il *radicale di I* è l'ideale $\sqrt{I}$

$$\sqrt{I} := \{f \in \mathbb{C}[x_1, \ldots, x_n] : \exists d \in \mathbb{N} : f^d \in I\}$$

Un ideale I si dice *radicale* se $I = \sqrt{I}$.

Esercizio 2.0.12. I dimostri che $\sqrt{I}$ è un ideale. È ovvio che $I \subset \sqrt{I}$. Si dimostri che $Z(I) = Z(\sqrt{I})$.

Limitiamoci quindi a considerare i soli ideali radicali di $\mathbb{C}[x_1, \ldots, x_n]$. Abbiamo una corrispondenza che associa ad ogni ideale radicale I la varietà $Z(I)$. Vogliamo mostrare che questa è una corrispondenza biunivoca tra gli ideali radicali di $\mathbb{C}[x_1, \ldots, x_n]$ e le varietà di $\mathbb{C}^n$. Per far ciò costruiamone l'inversa.

Sia $V \subset \mathbb{C}^n$ una varietà algebrica e definiamo

$$\mathcal{I}(V) := \{f \in \mathbb{C}[x_1, \ldots, x_n] : \ f(\underline{a}) = 0 \ \forall \underline{a} \in V\} \tag{4}$$

Allora, come conseguenza del Teorema degli zeri di Hilbert si dimostra il seguente Teorema, che è in realtà la forma originale Teorema degli zeri di Hilbert.

Theorem 2.0.13. *Sia $I \subset \mathbb{C}[x_1, \ldots, x_n]$ un ideale. Allora*

$$\mathcal{I}(Z(I)) = \sqrt{I}$$

Osservazione 2.0.14. In particolare se I è un ideale radicale, $\mathcal{I}(Z(I)) = I$. Abbiamo quindi una corrispondenza biunivoca tra varietà di $\mathbb{C}^n$ e ideali radicali di $\mathbb{C}[x_1, \ldots, x_n]$.

Dimostrazione. L'inclusione $\sqrt{I} \subset \mathcal{I}(Z(I))$ è facile: sia $f \in \sqrt{I}$, ovvero $f^d \in I$ per qualche intero d. Quindi per ogni $\underline{a} \in Z(I)$ abbiamo che $f^d(\underline{a}) = 0$. Abbiamo $0 = f^d(\underline{a}) = f(\underline{a})^d$, il che implica che $f(\underline{a}) = 0$ e quindi $f \in \mathcal{I}(Z(I))$.

Scegliamo ora per I un sistema finito di generatori: $I = (f_1 \ldots, f_r)$. Mostrare l'inclusione opposta significa mostrare che se $g \in \mathbb{C}[x_1, \ldots, x_n]$ si annulla in ogni zero comune di $f_1, \ldots, f_r$, allora esiste un intero d tale che $g^d \in I$. Nell'anello di polinomi in $r+1$ variabili $\mathbb{C}[x_1, \ldots, x_n, y]$ consideriamo il polinomio $g(\underline{x})y - 1$; questi ovviamente non si annulla laddove g si annulla. Da ciò segue che i polinomi $f_1, \ldots, f_r, g(\underline{x})y - 1$ non ammettono zeri comuni (in $\mathbb{C}^{r+1}$). Per 2.0.10 questo equivale a dire che esistono polinomi $h_1(\underline{x}, y), \ldots, h_{r+1}(\underline{x}, y)$ in $C[x_1, \ldots, x_n, y]$ tali che vale l'identità

$$1 = \sum_{i=1}^{r} h_1(\underline{x}, y) f(\underline{x}) + h_{r+1}(\underline{x}, y)(g(\underline{x})y - 1)$$

Sostituendo in essa la funzione razionale $g(\underline{x})^{-1}$ al posto di y otteniamo

$$1 = \sum_{i=1}^{r} h_1(\underline{x}, \frac{1}{g(\underline{x})}) f(\underline{x}).$$

Questa è un'identità di funzioni razionali nelle $x_1, \ldots, x_n$, con un (possibile) denominatore comune di tipo g^d. Moltiplicando entrambi i lati per tale g^d si ottiene $g^d = \sum_1^r p_i f_i$ con $p_i \in \mathbb{C}[x_1, \ldots, x_n]$ e quindi la tesi. ■

2.1 La topologia di Zariski su $\mathbb{C}^n$.

La topologia di Zariski su $\mathbb{C}^n$ è definita dall'avere come classe di insiemi chiusi la classe $\mathcal{C}$ di tutte le varietà in $\mathbb{C}^n$, ovvero

$$\mathcal{C} := \{Z(T), \ \forall T \subset \mathbb{C}[x_1, \ldots, x_n]\}$$

Ricordiamo che per definire una topologia la classe $\mathcal{C}$ deve
(1) contenere $\emptyset$ e $\mathbb{C}^n$,
(2) contenere l'unione di due suoi elementi qualsiasi;
(3) contenere l'intersezione di una qualsiasi collezione di suoi elementi.
Dimostriamo che valgono queste tre proprietà : Poiché $Z(0) = \mathbb{C}^n$ e $Z(1) = \emptyset$ la (1) vale.

La (2) segue dal fatto che $Z(T_1) \cup Z(T_2) = Z(T_1 \cdot T_2)$ per ogni coppia di sottoinsiemi T_1, T_2 di $\mathbb{C}[x_1, \ldots, x_n]$ (dove $T_1 \cdot T_2 := \{t_1 t_2,\ \forall t_i \in T_i\}$).

Infatti, sia $\underline{a} \in Z(T_1)$, allora $f(\underline{a}) = 0$ per ogni $f \in T_1$, quindi per ogni $g \in T_2$ abbiamo $fg(\underline{a}) = f(\underline{a})g(\underline{a}) = 0$ e quindi $\underline{a} \in Z(T_1 \cdot T_2)$. Dunque $Z(T_1) \subset Z(T_1 \cdot T_2)$; analogamente si mostra che $Z(T_2) \subset Z(T_1 \cdot T_2)$ e quindi $Z(T_1) \cup Z(T_2) \subset Z(T_1 \cdot T_2)$.

Per l'inclusione opposta, sia $\underline{a} \in Z(T_1 \cdot T_2)$; se $\underline{a} \in Z(T_1)$ abbiamo finito. Altrimenti esiste $f \in T_1$ tale che $f(\underline{a}) \neq 0$. Allora per ogni $g \in T_2$, poiché $0 = (fg)(\underline{a}) = f(\underline{a})g(\underline{a})$, otteniamo $g(\underline{a}) = 0$ e quindi $\underline{a} \in Z(T_2)$.

La (3) segue osservando che, se J è una qualsiasi collezione di indici, allora per ogni $T_j \subset \mathbb{C}[x_1, \ldots, x_n]$ abbiamo $\cap_{j \in J} Z(T_j) = Z(\cup_{j \in J} T_j)$. Quest'ultima verifica è banale.

Esercizio 2.1.1. Si dimostri che la topologia di Zariski su $\mathbb{C}$ non è di Hausdorff, dimostrando che ogni aperto non vuoto di $\mathbb{C}$ è denso in $\mathbb{C}$.

La topologia di Zariski induce una topologia sulle varietà algebriche di $\mathbb{C}^n$ per restrizione. Ovvero, data $V \subset \mathbb{C}^n$, i chiusi di V sono tutti e soli quelli ottenuti intersecando V con i chiusi (cioè le varietà) di $\mathbb{C}^n$.

Da ora in poi quindi le nostre varietà saranno dotate di una struttura topologica. Possiamo quindi considerare il concetto di funzioni e applicazioni *continue*. Il termine *funzione* è di norma usato per denotare un'applicazione a valori nel campo di numeri di "base (il campo $\mathbb{C}$ nel nostro caso).

Sulle nostre varietà possiamo considerare le funzioni determinate da polinomi.

Consideriamo il caso di $\mathbb{C}^n$; sia $p \in \mathbb{C}[x_1, \ldots, x_n]$, allora p definisce la funzione seguente

$$\begin{array}{ccc} \mathbb{C}^n & \longrightarrow & \mathbb{C} \\ \underline{a} & \mapsto & p(\underline{a}) \end{array} \tag{5}$$

è ovvio che due polinomi diversi definiscono funzioni diverse. Dunque $\mathbb{C}[x_1, \ldots, x_n]$ può esser visto come un insieme di particolari funzioni su $\mathbb{C}^n$, dette funzioni regolari.

Sia ora $V \subset \mathbb{C}^n$ una varietà; un polinomio p definisce anche una funzione su V. Due polinomi p e p' definiscono su V la stessa funzione se e solo se per ogni $\underline{a} \in V$ risulta $p(\underline{a}) = p'(\underline{a})$, ovvero se e solo se $p - p' \in \mathcal{I}(V)$. Sia $I = \mathcal{I}(V)$; da quanto detto segue che l'anello quoziente $\mathbb{C}[x_1, \ldots, x_n]/I$ definisce un insieme di funzioni su V, dette funzioni regolari. Dunque l'anello quoziente $\mathbb{C}[x_1, \ldots, x_n]/I$ ha una sua interpretazione geometrica; introduciamo la notazione

$$\mathbb{C}[V] := \frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathcal{I}(V)}.$$

Per caratterizzare gli anelli di tipo $\mathbb{C}[V]$ premettiamo

Osservazione 2.1.2. Sia $I \subset \mathbb{C}[x_1, \ldots, x_n]$ un ideale. Allora I è un ideale radicale se e solo se $\mathbb{C}[x_1, \ldots, x_n]/I$ è un anello *ridotto*, ovvero, un anello privo di elementi nilpotenti. La dimostrazione è lasciata per esercizio (ricordiamo che un elemento nilpotente è un elemento non nullo f tale che esiste $d \in \mathbb{N}$ per cui $f^d = 0$.

Dunque la corrispondenza biunivoca descritta in 2.0.14 tra varietà in $\mathbb{C}^n$ e ideali radicali in $\mathbb{C}[x_1, \ldots, x_n]$ induce una corrispondenza biunivoca tra l'insieme di tutte le varietà in $\mathbb{C}^n$ e l'insieme di tutti i quozienti di $\mathbb{C}[x_1, \ldots, x_n]$ che siano privi di nilpotenti. Più precisamente, tale corrispondenza è infatti un'equivalenza di categorie che inverte i morfismi. Questo significa che ad ogni omomorfismo $\lambda : \mathbb{C}[V] \longrightarrow \mathbb{C}[V']$ corrisponde un unico morfismo di varietà $\Phi : V' \longrightarrow V$ tale che λ coincide con il pull-back di funzione tramite Φ.

3 Geometria algebrica su anelli commutativi arbitrari.

Sia adesso R un anello commutativo qualsiasi, tale che $1 \in R$. Vogliamo associare ad R un oggetto geometrico, estendendo quanto fatto nel caso in cui R è un anello di polinomi a coefficienti in $\mathbb{C}$ o, più in generale, una $\mathbb{C}$-algebra finitamente generata. Chiameremo *schema* tale oggetto geometrico

Il primo passo è quello di associare a R uno spazio, che costituisca l'insieme di punti soggiacente allo "schema che vogliamo definire. Sul modello di quanto studiato, ispirati dal teorema degli zeri di Hilbert, un candidato naturale per tale spazio è l'insieme di tutti gli ideali massimali di R. Denotiamo $Max(R)$ l'insieme di tutti gli ideali massimali di R.

L'obiettivo finale è quello di ottenere una equivalenza di categorie tra la categoria degli anelli commutativi unitari, con gli omomorfismi di anelli, e la categoria di questi schemi (da definire) con i loro morfismi (anch'essi da definire).

Tale equivalenza, come nel caso delle varietà , deve invertire le frecce, ovvero ad un omomorfismo $\lambda : R \longrightarrow R'$ deve corrispondere un morfismo di schemi che vada dallo schema associato ad R' a quello associato ad R.

Se i nostri schemi fossero supportati sull'insieme degli ideali massimali, dovremmo avere un morfismo $\phi : Max(R') \longrightarrow Max(R)$ associato a λ in modo funtoriale. In particolare dovremmo avere che $\phi(M') = \lambda^{-1}(M')$. C'è però un problema: se $M \subset R'$ è un ideale massimale in R', l'ideale $\lambda^{-1}(M')$ non è necessariamente un ideale massimale di R.

Per esempio, nell'inclusione $\lambda : \mathbb{Z} \hookrightarrow \mathbb{Q}[x]$ la preimmagine dell'ideale massimale (x) è l'ideale 0 in $\mathbb{Z}$ che certo non è massimale.

Questo ci dice che $Max(R)$ non è lo spazio giusto. Osserviamo ora che per ogni omomorfismo $\lambda : R \longrightarrow R'$, la preimmagine di un ideale *primo* di R' è un ideale primo di R. Il modo giusto di procedere è infatti proprio quello di considerare non solo gli ideali massimali (che ovviamente sono anche primi) ma tutti gli ideali primi di R. Definiamo

$$\operatorname{Spec} R := \{P \subsetneq R : \ P \text{ è un ideale primo } \}.$$

(Ricordiamo che un ideale primo di un anello R è un ideale proprio $P \subset R$ tale che l'anello quoziente R/P è privo di divisori dello 0).

Consideriamo questa definizione nel caso $R = \mathbb{C}[x]$, e confrontiamola con $\mathbb{C}$, la *varietà* associata ad R precedentemente. Notiamo che, come insiemi di punti, $\operatorname{Spec}\mathbb{C}[x]$ contiene esattamente un punto in più rispetto a $\mathbb{C}$. Sia infatti $P \subset \mathbb{C}[x]$ un ideale primo, allora ci sono due possibilità , o P è l'ideale (0) oppure P è un ideale massimale. Sappiamo che gli ideali massimali di $\mathbb{C}[x]$ sono in corrispondenza biunivoca con i punti di $\mathbb{C}$; concludiamo quindi che, come insieme, $\operatorname{Spec}\mathbb{C}[x]$ è come $\mathbb{C}$ con l'aggiunta del punto (0). Vedremo tra poco che questo comporta un'importante differenza geometrica (anzi, topologica).

3.1 $\operatorname{Spec} R$ come spazio topologico

Procedendo in modo analogo a quanto fatto per le varietà , definiremo ora su $\operatorname{Spec} R$ una struttura di spazio topologico, basata sulla definizione seguente: sia $T \subset R$,

$$V(T) := \{P \in \operatorname{Spec} R : \ T \subset P\} \subset \operatorname{Spec} R$$

Ovvero: $V(T)$ è il luogo di tutti gli ideali primi contenenti T. Definiamo ora su $\operatorname{Spec} R$ la *topologia di Zariski*, che ha come classe di insiemi chiusi la classe $\mathcal{C}$ definita qua sotto in

due modi equivalenti

$$\mathcal{C} = \{V(T), \quad \forall T \subset R\} = \{V(I), \quad \forall I \text{ ideale di } R\}. \tag{6}$$

Va verificato che la classe $\mathcal{C}$ definisce una topologia, e che le due definizioni sono equivalenti. Questa seconda verifica è banale e lasciata per esercizio. Dimostriamo invece che (1) $\mathcal{C}$ contiene l'insieme vuoto e tutto $\operatorname{Spec} R$, e che $\mathcal{C}$ è chiusa (2) rispetto all'unione finita e (3) rispetto all'intersezione qualsiasi.

Per (1), osserviamo che $\emptyset = V(1)$ e $\operatorname{Spec} R = V(0)$.

Per (2) abbiamo che $V(I_1) \cup V(I_2) = V(I_1 \cdot I_2)$.

Infatti, l'inclusione $V(I_1) \cup V(I_2) \subset V(I_1 \cdot I_2)$ è ovvia, poichè $I_j \supset I_1 \cdot I_2$.

Viceversa, se $P \in V(I_1 \cdot I_2)$ e, diciamo, P non contiene I_1, allora esiste $f \in I_1$ non contenuto in P. Poiché $P \supset I_1 \cdot I_2$, per ogni $g \in I_2$ abbiamo che $fg \in P$ e quindi, poiché P è primo e non contiene f, ogni elemento g di I_2 sta in P. Quindi $P \in V(I_2) \subset V(I_1) \cup V(I_2)$.

Per (3) si mostra facilmente che $\cap_i V(T_i) = V(\cup_i T_i)$ per i in qualsiasi insieme di indici.

Riferimenti bibliografici

[1] Michael Artin *Algebra.* Prentice Hall, Inc., Englewood Cliffs, NJ, 1991

[2] M.F.Atiyah, I.G. Macdonald *Introduzione all'algebra commutativa* Feltrinelli

[3] D. Mumford *The red book of Varieties and Schemes* Springer LNM 1358