Alma Mater Studiorum • Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica

HILBERT NULLSTELLENSATZ E ALCUNE SUE CONSEGUENZE GEOMETRICHE

Tesi di laurea in Geometria 2

Relatore:
Chiar.ma Prof.
Fioresi Rita

Presentata da:
Rigolli Lorenzo

Sessione II
Anno accaddemico 2010/11

Indice

Introduzione

Il teorema degli zeri di Hilbert, noto anche col nome tedesco Nullstellensatz, è uno dei risultati fondamentali da cui ha avuto origine la geometria algebrica classica e riguarda la soluzione di equazioni in n indeterminate su campi algebricamente chiusi. Il teorema degli zeri è opera del famoso matematico tedesco David Hilbert (1862−1943) e può essere formulato in diverse versioni che differiscono per la generalità del contesto in cui si applicano. Le formulazioni più note sono quella forte e quella debole, ma successivamente ne sono state date ulteriori, ad esempio quella generale, dovuta a Bourbaki [4][p. 131-134, cap. 4.5], da cui seguono come corollario la formulazione forte e quella debole.

Nel capitolo 1 verranno esposti le definizioni e i risultati algebrici necessari per esprimere e dimostrare il teorema degli zeri di Hilbert nella formulazione forte e in quella debole. Saranno date le nozioni geometriche, relative a insiemi algebrici e topologia di Zariski, e quelle algebriche, relative ad estensioni di anelli, anello delle frazioni ed anelli Noetheriani. Nell'esposizione ci si avvarrà di esempi grafici per rendere più chiare le proposizioni e le definizioni.

Il capitolo 2 è invece incentrato sull'enunciato e la dimostrazione del Nullstellensatz in forma debole. In seguito, sfruttando risultati intermedi ottenuti per dimostrare la forma debole, si arriverà alla dimostrazione della forma forte. Inoltre, nel capitolo è brevemente spiegato il significato geometrico delle due formulazioni del teorema.

Capitolo 1

Premesse algebriche al Nullstellensatz

In questo capitolo si mostrano, nei casi più significativi con dimostrazione, i risultati algebrici fondamentali per la comprensione del teorema degli zeri di Hilbert.

1.1 Insiemi algebrici

Gli insiemi algebrici sono i luoghi di zeri di polinomi e costituiscono quindi il principale legame tra algebra e geometria di interesse per il presente testo. In questa sezione si vogliono definire in modo rigoroso gli insiemi algebrici ed i concetti basilari ad essi relativi. Inoltre si fanno le prime considerazioni utili per esplorare le relazioni tra gli ideali di polinomi e gli insiemi algebrici. D'ora innanzi si considereranno solo anelli commutativi e unitari. Inoltre, a meno che non si specifichi esplicitamente il contrario, si supporrà che K sia un campo algebricamente chiuso, anche se le premesse esposte nel primo capitolo sono valide per qualsiasi campo.

Definizione 1.1.1. Lo *spazio affine* di dimensione n su K, denotato con $\mathbf{A}^n$, è l'insieme delle n-uple ordinate di elementi in K, $\mathbf{A}^n = \{(x_1, \ldots, x_n) | x_i \in K\}$. L'anello dei polinomi in n indeterminate su un campo K sarà denotato con $K[x_1, \ldots, x_n]$ e i suoi elementi rappresentano le funzioni *regolari* su $\mathbf{A}^n$, cioè le funzioni polinomiali definite su $\mathbf{A}^n$.

Sia $S \subseteq K[x_1, \ldots, x_n]$ un insieme di polinomi. Si definisce:

$$V(S) = \{P \in K^n | f(P) = 0 \ \forall f \in S\}.$$

Definizione 1.1.2. Un sottoinsieme X di K^n si dice *insieme algebrico* se esiste un sottoinsieme $S \subseteq K[x_1, \ldots, x_n]$ tale per cui $X = V(S)$.

Osservazione 1.1.3. Sia S una famiglia di polinomi di $K[x_1, \ldots, x_n]$ e sia I l'ideale generato dai polinomi appartenenti ad S. Allora $V(I) = V(S)$.

Infatti si ha che $I \supseteq S$, cioè ogni elemento di S è anche elemento di I. Ciò implica che uno zero comune ad ogni elemento di I sia comune anche ad ogni elemento di S; in altre parole $V(I) \subseteq V(S)$. Altresì è vero che $V(I) \supseteq V(S)$, infatti ogni elemento di I è esprimibile come combinazione lineare di elementi di S a coefficienti in $K[x_1, \ldots, x_n]$. Perciò ogni zero di S è zero di I. Quindi $V(I) \supseteq V(S)$ e pertanto $V(I) = V(S)$.

Dall'osservazione si ha quindi che l'insieme algebrico associato ad una famiglia di polinomi coincide con l'insieme algebrico associato all'ideale generato da tale famiglia.

I grafici (1) e (2) aiutano a visualizzare geometricamente due esempi di insiemi algebrici.

Si vuole cercare di capire se la corrispondenza tra insiemi algebrici e ideali sia biunivoca e in quale senso il teorema degli zeri di Hilbert fornisca una risposta esaustiva a questa domanda. In dimensione 1, tuttavia, si ha una risposta immediata, come si vede dall'esempio che segue.

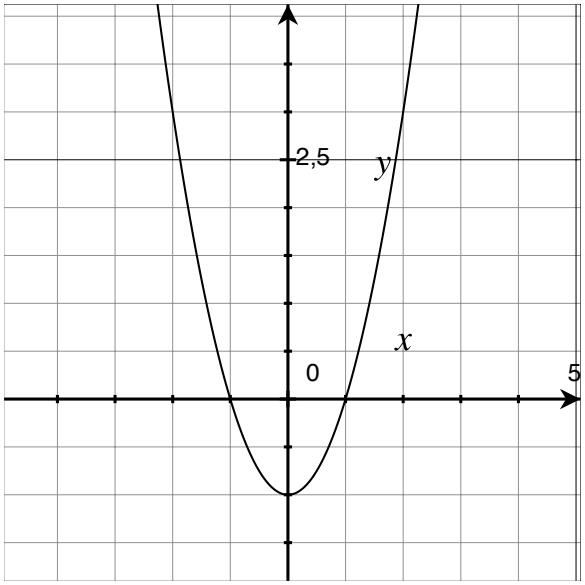
Esempio 1.1.4. In $\mathbf{A}^1$ gli unici insiemi algebrici propri sono insiemi finiti di punti. Infatti, $K[x]$ è dominio ad ideali principali (PID), quindi ogni insieme algebrico è individuato dagli zeri di un unico polinomio monico; inoltre, dato che K è algebricamente chiuso, ogni polinomio $f \in K[x]$ si può scrivere come $f = c(x - a_1) \ldots (x - a_n)$, $a_1, \ldots, a_n, c \in K$.

La relazione tra insiemi algebrici e ideali rovescia le inclusioni nel senso seguente:

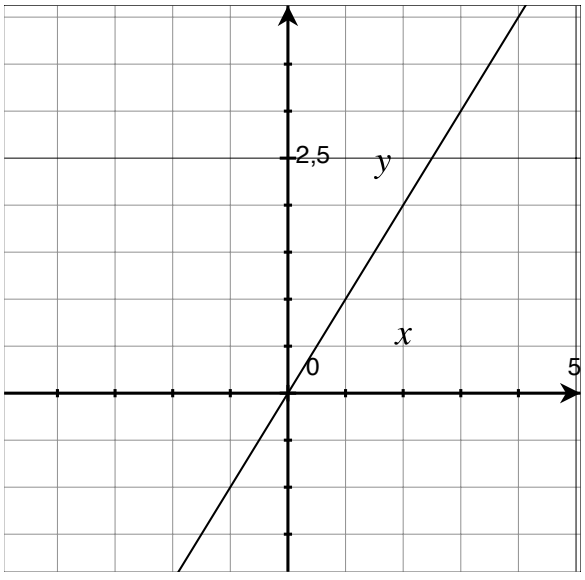
Osservazione 1.1.5. Siano I, J ideali di $K[x_1, \ldots, x_n]$ con $I \subseteq J$. Allora $V(I) \supseteq V(J)$.

Ciò si verifica facilmente in quanto ogni polinomio di J è contenuto in I e pertanto uno zero in comune ad ogni elemento di I è anche zero in comune ad ogni elemento di J.
Si danno infine due definizioni utili all'approfondimento degli argomenti, in questo caso le conseguenze geometriche del Nullstellensatz, di questa tesi.

Definizione 1.1.6. Sia I un ideale di $K[x_1, \ldots, x_n]$. Un insieme algebrico $V(I)$ si dice *irriducibile* se non può essere espresso come unione di due insiemi algebrici distinti da $V(I)$.



(1) $y - x^2 - 1 = 0$ *è un esempio di insieme algebrico in* $\mathbb{R}^2$.



(2) $y - x = 0$ *è un esempio di insieme algebrico in* $\mathbb{R}^2$.

Definizione 1.1.7. Una *varietà algebrica affine*, o *varietà affine*, è un insieme algebrico irriducibile.

Gli insiemi algebrici nei grafici (1) e (2) sono irriducibili, mentre quelli in (3) e (4) sono riducibili.

1.2 Topologia di Zariski

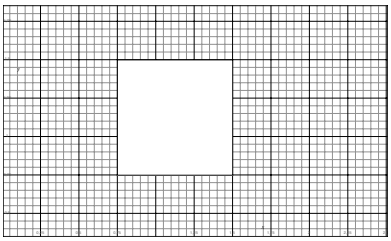
In questa sezione viene definita la topologia di Zariski, che è la topologia naturale da considerare per problemi di tipo algebrico.

Definizione 1.2.1. Si definisce *topologia di Zariski* su $\mathbf{A}^n$ la topologia nella quale gli aperti sono definiti come complementari di insiemi algebrici. Gli insiemi algebrici $V(I)$ di $\mathbf{A}^n$ sono dunque i chiusi in questa topologia.

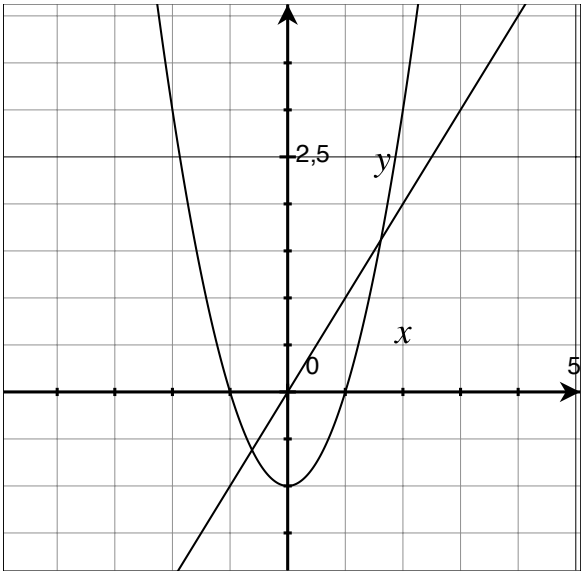
Osservazione 1.2.2. Si può verificare che la topologia di Zariski è una topologia e che gli aperti $\mathbf{A}^n \backslash V(f)$, ove $f \in K[x_1, \ldots, x_n]$, ne sono una base [6][p. 40]. Dunque, si ha che:

1. Lo spazio topologico X e l'insieme vuoto sono insiemi algebrici.
2. Intersezione di insiemi algebrici è un insieme algebrico.
3. Unione finita di insiemi algebrici è un insieme algebrico.

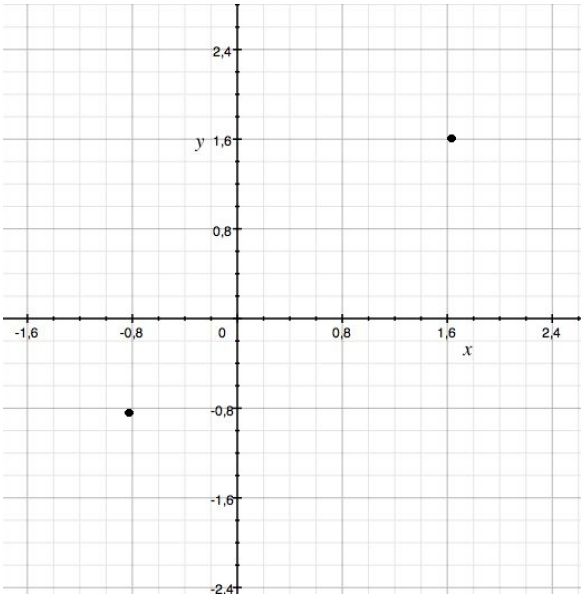
La topologia di Zariski in $\mathbb{R}^n$ è meno fine di quella euclidea, pertanto ogni aperto in tale topologia è aperto anche nella topologia euclidea e anche per i chiusi vale lo stesso. Tuttavia non è vero il contrario, come mostra chiaramente l'esempio seguente.



Nell'esempio in figura il quadrato pieno è un chiuso nella topologia euclidea in $\mathbb{R}^2$ ma non in quella di Zariski, infatti tale insieme di punti non può essere visto come luogo di zeri di polinomi. Come si vedrà, ogni insieme algebrico



(3) $V(y-x^2-1) \cup V(y-x)$ *è un insieme algebrico in* $\mathbb{R}^2$*, in quanto unione di insiemi algebrici. Inoltre è riducibile.*



(4) $V(I) = V(y-x^2-1, y-x) = V(y-x^2-1) \cap V(y-x)$ *è un insieme algebrico in* $\mathbb{R}^2$*, in quanto intersezione di insiemi algebrici. Inoltre è riducibile.*

può essere espresso come intersezione di insiemi algebrici. Per il momento osserviamo la seguente proprietà.

Osservazione 1.2.3. Sia $I = (f_1, \ldots, f_m)$ un ideale finitamente generato di $K[x_1, \ldots, x_n]$. Allora $V(I) = \bigcap_{i=1}^{m} V(f_i)$.

Verifichiamo che $V(I) \subseteq \bigcap_{i=1}^{m} V(f_i)$. Se $x \in V(I)$, allora ogni polinomio f_i, per $i = 1, \ldots, m$, si annulla in x, quindi $x \in \bigcap_{i=1}^{m} V(f_i)$. Vale anche l'inclusione inversa. Se $x \in \bigcap_{i=1}^{m} V(f_i)$ allora $f_i(x) = 0$ per $i = 1, \ldots, m$ e quindi, denotando con g_i un generico elemento di $K[x_1, \ldots, x_n]$, si ha $(\sum_{i=1}^{m} f_i g_i)(x) = 0$. In altre parole $x \in V(I)$.

Per non creare fraintendimenti va precisato che esiste un' altra topologia di Zariski, definita come segue, che però non sarà trattata ulteriormente in questa tesi.

Definizione 1.2.4. Sia A un anello, X l'insieme degli ideali primi di A ed E un sottoinsieme di A. Denotando con $V(E)$ l'insieme degli ideali primi contenenti E, si verifica [1][p. 12] che gli insiemi $V(E)$ soddisfano gli assiomi dei chiusi in uno spazio topologico. La topologia così ottenuta su X è detta *topologia spettrale di Zariski* e lo spazio topologico X viene denotato $Spec(A)$.

1.3 Anelli Noetheriani

Gli anelli Noetheriani sono anelli che godono della seguente proprietà, di importanza fondamentale:
"In un anello Noetheriano ogni ideale è finitamente generato".
Il prototipo di anello Noetheriano è l'anello dei polinomi in n indeterminate.

Definizione 1.3.1. Si dice che un insieme Σ parzialmente ordinato dalla relazione $\leqslant$ soddisfa la *condizione delle catene ascendenti (ACC)* se ogni successione $x_1 \leqslant x_2 \leqslant \ldots$ in Σ è stazionaria, cioè se esiste un numero naturale n tale per cui $x_n = x_{n+1} = x_{n+2} = \ldots$

Il seguente teorema si rivela fondamentale per la caratterizzazione degli anelli Noetheriani.

Teorema 1.3.2. *Dato un anello A e scegliendo come Σ l'insieme dei suoi ideali parzialmente ordinati tramite la relazione $\subseteq$ si ha che le condizioni seguenti sono equivalenti:*

(1) $(\Sigma, \subseteq)$ *soddisfa ACC.*

(2) Ogni sottoinsieme non vuoto di Σ *ha un elemento massimale.*

(3) Ogni ideale di A *è finitamente generato.*

Dimostrazione. Vedi [1][p. 74-75]. □

Definizione 1.3.3. Un *anello* che soddisfi una delle tre condizioni equivalenti del teorema 1.3.2 è detto *Noetheriano.*

Osservazione 1.3.4. Ogni campo è Noetheriano in quanto avendo solo i due ideali banali soddisfa (3).

Teorema 1.3.5 (Teorema della base di Hilbert)**.** *Se* A *è un anello Noetheriano allora l'anello dei polinomi* $A[x]$ *è Noetheriano.*

Dimostrazione. Vedi [1][p. 81]. □

Applicando il teorema della base di Hilbert più volte si ottiene che se A è Noetheriano allora $A[x_1, \ldots, x_n]$ è Noetheriano ed in particolare $K[x_1, \ldots, x_n]$ è un anello Noetheriano.

Essendo ogni ideale $I = (f_1, \ldots, f_m)$ di $K[x_1, \ldots, x_n]$ finitamente generato, da 1.2.3 e da 1.3.2 segue che $V(I)$ è esprimibile come intersezione di finiti insiemi algebrici $V(f_i)$.
La proprietà di $K[x_1, \ldots, x_n]$ di essere Noetheriano ha un'altra importante conseguenza, dovuta alla condizione delle catene ascendenti. Infatti, ogni catena ascendente di ideali in $K[x_1, \ldots, x_n]$ è superiormente limitata, perciò la corrispondente catena di insiemi algebrici è limitata inferiormente. Prima di passare alla dimostrazione del teorema degli zeri di Hilbert è necessario introdurre e richiamare alcune nozioni algebriche riguardanti le estensioni di campi, gli anelli interi e l'anello delle frazioni.

1.4 Estensione di anelli e campi

Com'è noto, esistono estensioni di campi algebriche ed estensioni trascendenti. Poiché nella dimostrazione del teorema degli zeri di Hilbert interviene questo secondo tipo di estensioni, si devono introdurre alcune definizioni e risultati relativi ad esse. In questa sezione F e K sono campi generici.

Definizione 1.4.1. Sia F/K un'estensione di campi e S un sottoinsieme di F. S è *algebricamente dipendente* su K se, per qualche intero positivo n, esiste un polinomio non identicamente nullo $f \in K[x_1, \ldots, x_n]$ tale per cui

$f(s_1, \ldots, s_n) = 0$, con $s_1, \ldots, s_n$ elementi distinti di S. Nel caso S non sia algebricamente dipendente su K si dice che S è *algebricamente indipendente* su K.

Dalla definizione si ha che:

- L'insieme $\{u\}$ è algebricamente dipendente su K se e solo se u è algebrico su K.
- Un elemento di un insieme algebricamente indipendente su K è trascendente su K.

Aggiungendo un elemento ad un insieme algebricamente dipendente si ottiene un insieme algebricamente dipendente e, per tale ragione, si ha che ogni sottoinsieme di un insieme algebricamente indipendente è a sua volta algebricamente indipendente. Si noti che il concetto di dipendenza algebrica può essere considerato un'estensione di quello di dipendenza lineare. Infatti, un insieme S è linearmente dipendente su K se esiste un polinomio $f \in K[x_1, \ldots, x_n]$, $deg(f) = 1$, che si annulla per $s_i \in S$ distinti. Di conseguenza se un insieme S è algebricamente indipendente allora è anche linearmente indipendente. Per concludere, si osservi che l'insieme vuoto è algebricamente indipendente. Si introduce ora un nuovo concetto associato alle estensioni di campi, quello di base di trascendenza.

Definizione 1.4.2. Sia F/K un'estensione di campi. Una *base di trascendenza* di F su K è un sottoinsieme S di F, algebricamente indipendente su K, con la proprietà di essere massimale (rispetto all'inclusione di insiemi) nell'insieme di tutti i sottoinsiemi di F algebricamente indipendenti.

Nelle condizioni precedenti l'esistenza di una base di trascendenza si può dedurre dal lemma di Zorn [3][p. 317].

Esempio 1.4.3. Data l'estensione di campi $K(x)/K, \{x\}$ è una base di trascendenza di $K(x)$ su K.

Definizione 1.4.4. Un campo F si dice *estensione puramente trascendente* di un campo K se, dato un insieme S algebricamente indipendente su K, si ha che $F = K(S)$.

Proseguendo con la teoria [3][p. 311-317, cap. VI] si può dimostrare che ogni estensione di campi può essere suddivisa in una parte puramente algebrica e una puramente trascendente, la cui base è, appunto, una base di trascendenza. Si può dimostrare che la cardinalità di basi di trascendenza relative alla stessa estensione di campi è identica; e pertanto è ben definito il grado di trascendenza di un'estensione di campi. Tale grado indica, appunto,

la cardinalità di una base di trascendenza. Nell'esempio dato sopra il grado di trascendenza è 1, in quanto la base $\{x\}$ ha un unico elemento.

Definizione 1.4.5. Un anello S si dice *estensione di un anello* R se R è sottoanello di S contenente l'unità di S.

Si dà ora un'altra definizione.

Definizione 1.4.6. Sia S un'estensione dell'anello R. Si dice che $s \in S$ è un elemento *intero* su R se esiste un polinomio monico $f(x) \in R[x]$ tale per cui $f(s) = 0$. L'estensione di R ad S si dice *intera* se ogni $s \in S$ è intero su R.

Nella definizione precedente bisogna prestare particolare attenzione al fatto che il polinomio $f(x)$ sia monico. Si illustrano ora alcuni esempi di estensioni intere.

Esempio 1.4.7. Qualsiasi anello R è intero su sé stesso, poiché ogni elemento $r \in R$ è zero del polinomio monico $f(x) = x - r \in R[x]$.

Esempio 1.4.8. Un'estensione algebrica di campi F/K è intera in quanto per ogni $y \in F$ esiste $f \in K[x]$ con coefficiente direttore a, tale per cui $f(y) = 0$. f in generale non è monico, ma dato che K è campo, f può essere moltiplicato per a^{-1} ottenendo $f' = a^{-1}f$. Fissato y, f' è monico e si annulla in y, quindi estensioni algebriche di campi sono intere.

Esempio 1.4.9. L'estensione di $\mathbb{Z}$ ad $\mathbb{R}$ è algebrica ma non intera, perché, ad esempio, $\dfrac{1}{\sqrt{2}}$ non è intero su $\mathbb{Z}$ (mentre invece lo è su $\mathbb{Q}$).

1.5 Anello delle frazioni

L'idea su cui si basa la costruzione dell'anello delle frazioni è simile a quella attraverso la quale si costruisce il campo dei numeri razionali a partire dall'anello degli interi. Questa costruzione trova diverse applicazioni nell'algebra, in particolare sarà utilizzata nella dimostrazione del Nullstellenstaz presentata nel prossimo capitolo.
Sia A un anello e $S \ni 1$ un sottoinsieme moltiplicativamente chiuso di A. Si definisce una relazione di equivalenza sull'insieme $A \times S$:

$$(a, s) \sim (a', s') \text{ se } \exists t \in S \text{ tale per cui } (as' - a's)t = 0$$

D'ora in poi (a, s) verrà spesso denotato con $\dfrac{a}{s}$. Si verifica che l'insieme quoziente $S^{-1}A := A \times S/\sim$ rispetto alla relazione di equivalenza di cui sopra è un anello, in cui, per definizione:

1. $\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$
2. $\frac{a}{s}\frac{b}{t} := \frac{ab}{st}$
3. l'elemento neutro additivo è $\frac{0}{1}$
4. l'elemento neutro moltiplicativo è $\frac{1}{1}$.

Definizione 1.5.1. $S^{-1}A$ è detto *anello delle frazioni* di A rispetto a S.

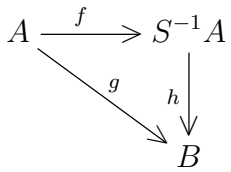
Dato un anello A si definisce un'applicazione $f : A \longrightarrow S^{-1}A$, $a \mapsto \frac{a}{1}$, che si verifica essere un morfismo di anelli, infatti:

$$f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$$
$$f(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = f(a)f(b)$$

Osservazione 1.5.2. Ogni elemento di $S^{-1}A$ nella forma $\frac{s}{1}$, con $s \in S$, è invertibile ed ha per inverso $\frac{1}{s}$.

Infatti $\frac{s}{1}\frac{1}{s} = \frac{s}{s} = \frac{1}{1}$, dato che $s1 - 1s = 0$.

Proposizione 1.5.3. *(Proprietà universale dell'anello delle frazioni.) Siano A, B anelli, S un sottoinsieme moltiplicativamente chiuso di A, f il morfismo di anelli definito sopra e $g : A \to B$ un morfismo per cui $g(s)$ sia invertibile $\forall s \in S$. Allora esiste ed è unico il morfismo di anelli $h\colon S^{-1}A \to B$, tale per cui $g = h \circ f$.*



Dimostrazione. Vedi [1][p. 37]. □

La costruzione dell'anello delle frazioni ha diverse importanti applicazioni, tra cui quelle mostrate nei seguenti esempi.

Esempio 1.5.4. Sia A un anello e f un elemento di A. Si definisce $S := \{f^n \mid n \geq 0\}$. S è un sottoinsieme moltiplicativamente chiuso di A. Si ha $S^{-1}A = \{\frac{a}{f^n} | a \in A,\ n \in \mathbb{Z}^+\}$. $S^{-1}A$ viene anche denotato A_f oppure $A[f^{-1}]$ e si dice anello delle frazioni di A rispetto ad S.
Come esempio di tale costruzione si ha l'anello dei polinomi di Laurent, $K[x, x^{-1}] := \{\frac{a_0 + a_1 x + \ldots + a_n x^n}{x^m} | n \in \mathbb{Z}^+, m \in \mathbb{Z}^+,\ i = 0, \ldots, n,\ a_i \in K\}$.

Esempio 1.5.5. Sia A un dominio d'integrità e $\mathfrak{p} \subsetneq A$ un suo ideale primo. Ponendo $S = A \backslash \mathfrak{p}$ e sfruttando la definizione di ideale primo si verifica che S è un sottoinsieme moltiplicativamente chiuso contenente l'unità di A. Si definisce $A_\mathfrak{p} := (A \backslash \mathfrak{p})^{-1} A$. Non è difficile verificare che l'anello $A_\mathfrak{p}$ è locale, cioè ha un unico ideale massimale, ed ha come ideale massimale quello generato dall'immagine di $\mathfrak{p}$ tramite il morfismo f definito sopra. La procedura appena descritta, tramite la quale ad un anello A e ad un suo ideale primo $\mathfrak{p}$, viene associato un anello locale $A_\mathfrak{p}$, è detta *localizzazione* di A rispetto a $\mathfrak{p}$.

Si enuncia ora un'ultima proposizione utile alla dimostrazione del Nullstellensatz.

Proposizione 1.5.6. *Sia A un anello e B un anello intero su A. Se L è un campo algebricamente chiuso e $\varphi : A \to L$ è un morfismo allora φ si estende a un morfismo $\overline{\varphi} : B \to L$.*

Dimostrazione. Vedi [2][p. 347 cap. VII, prop. 3.1]. □

Capitolo 2

Il teorema degli zeri di Hilbert

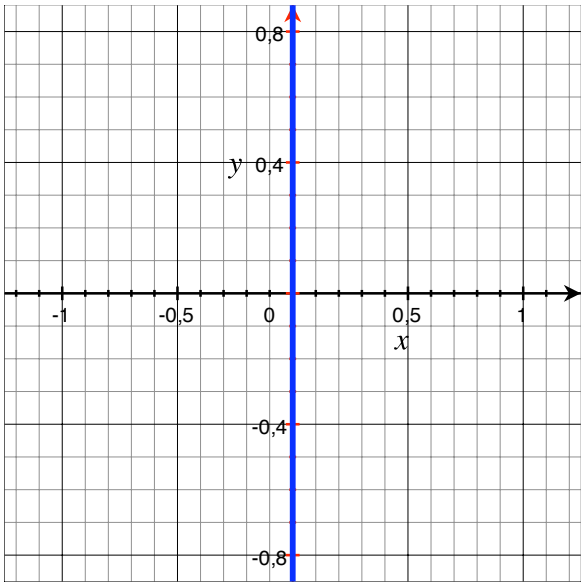
In questo capitolo si dimostra la formulazione debole del teorema degli zeri di Hilbert e, in seguito, si dà una dimostrazione della formulazione forte. Inoltre si cerca di esplorare brevemente le implicazioni geometriche delle due formulazioni del teorema.

2.1 Relazione tra ideali e insiemi algebrici

Dato un generico campo K ci si chiede che relazione intercorra tra un ideale I di $K[x_1, \ldots, x_n]$ e l' insieme algebrico $V(I)$, introdotto nel capitolo precedente. In generale non è vero che ad ideali distinti di $K[x_1, \ldots, x_n]$ corrispondono insiemi algebrici distinti in $\mathbf{A}^n$. In altre parole la corrispondenza che lega ideali di $K[x_1, \ldots, x_n]$ ad insiemi algebrici in $\mathbf{A}^n$ non è biunivoca; come si vede dall'esempio seguente.

Esempio 2.1.1. Siano $I = (x^2 + 1)$ e $J = \mathbb{R}[x]$ ideali di $\mathbb{R}[x]$. Allora $V(I) = V(J) = \varnothing$.

Dall'esempio precedente si evince che, tramite la relazione che associa $V(I)$ ad I, a ideali I e J differenti può corrispondere lo stesso insieme algebrico. La ragione per cui nell'esempio appena mostrato si verifica che ad ideali distinti corrisponde lo stesso insieme algebrico è che $\mathbb{R}$ non è un campo algebricamente chiuso. Nel caso K sia algebricamente chiuso ogni polinomio non costante di $K[x]$ ha almeno uno zero e pertanto non si può presentare la situazione sopra esposta, tuttavia la corrispondenza può ugualmente non essere biunivoca, come si evince dall'esempio seguente.



(5) $I = (x)$. $J = (x^2)$. *In* $K[x, y]$ *si ha* $V(I) = V(J)$, *nonostante* $I \neq J$.

Esempio 2.1.2. Sia $K[x]$ l'anello dei polinomi in una indeterminata su un campo algebricamente chiuso K. In questo caso $V(x) = 0 = V(x^2)$, però, evidentemente, $(x) \neq (x^2)$.

Dall'esempio, illustrato nel grafico (5), di cui sopra, si nota che, anche se K è algebricamente chiuso, non necessariamente ad ideali differenti corrispondono insiemi algebrici differenti. Il teorema degli zeri, come si vedrà, permette di trovare una corrispondenza biunivoca tra ideali e insiemi algebrici, a patto di limitarsi a considerare ideali, detti radicali, aventi una certa proprietà, e a considerare K algebricamente chiuso.

2.2 Nullstellensatz, forma debole

Il teorema che segue costituisce il più importante passo intermedio verso la dimostrazione del teorema degli zeri.

Teorema 2.2.1. *Sia* $K[\alpha_1, \ldots, \alpha_n]$ *un campo estensione finitamente generata di un generico campo* K *e sia* $\varphi : K \longrightarrow L$ *l'inclusione di* K *in un campo* L *algebricamente chiuso. Allora* φ *si può estendere ad un morfismo di campi* $\overline{\varphi} : K[\alpha_1, \ldots, \alpha_n] \longrightarrow L$.

Dimostrazione. Si suppone che esista $k \in \mathbb{N}$ tale per cui α_k sia trascendente su K. Se ciò non si verifica, il morfismo inclusione $i : K[\alpha_1, \ldots, \alpha_n] \hookrightarrow \overline{K} \subseteq$

L, dove con $\overline{K}$ si intende la chiusura algebrica di K, sarebbe il morfismo $\overline{\varphi}$ cercato e la dimostrazione del teorema sarebbe conclusa. Quindi si suppone che l'estensione di campi presa in considerazione sia trascendente di grado $r \geq 1$ e la base di trascendenza sia $(t_1, t_2, \ldots, t_r)$. A questo punto, per ogni j compreso tra 1 e n, α_j dev'essere algebrico su $K(t_1, \ldots . t_r)$ e pertanto deve esistere il polinomio minimo in $K(t_1, \ldots, t_r)[Y]$ (anello dei polinomi nell'indeterminata Y a coefficienti in $K(t_1, \ldots, t_r)$) di α_j su $K(t_1, \ldots, t_r)$. Moltiplicando ciascun polinomio minimo per un opportuno elemento non nullo di $K[t_1, \ldots, t_r]$ si ottengono polinomi a coefficienti in $K[t_1, \ldots, t_r]$. Siano $a_1(t), \ldots, a_n(t)$ i coefficienti direttori di tali polinomi, ove $t = (t_1, \ldots, t_r)$, e sia $a(t) = a_1(t)a_2(t) \ldots a_n(t)$. Dato che $a(t) \neq 0$ esistono $s_1, \ldots, s_r \in \overline{K}$ per i quali $a(s) \neq 0$ e quindi si ha che $a_i(s) \neq 0$ per $i = 1, \ldots, n$. Si noti che ogni α_j è intero sull'anello $K[t_1, \ldots, t_r, \frac{1}{a_1(t)}, \ldots, \frac{1}{a_n(t)}]$ e che il morfismo $\varphi' : K[t_1, \ldots, t_r] \longrightarrow \overline{K}$ tale per cui $\varphi' \mid_K = \varphi = id_K$ e $\varphi'(t_j) = s_j \ \forall j = 1, \ldots, r$ è completamente definito, in quanto definito sui generatori di $K[t_1, \ldots, t_r]$. Sia $\mathfrak{p} = Ker\varphi'$, allora $a(t) \notin \mathfrak{p}$. $Im\varphi' = K(s_1, \ldots, s_r)$ è un campo e dal diagramma in figura si ha che, dato che $K[t_1, \ldots, t_r]/\mathfrak{p}$ è un campo, allora $\mathfrak{p}$ dev'essere massimale e in particolare primo.

$$\begin{array}{ccc} K[t_1, \ldots, t_r] & \xrightarrow{\varphi'} & \overline{K} \\ \pi \big\downarrow & & \big\uparrow i \\ K[t_1, \ldots, t_r]/\mathfrak{p} & \xrightarrow{\cong} & Im\varphi' \end{array}$$

Sia $S := K[t_1, \ldots, t_r] \backslash \mathfrak{p}$. Si verifica che, per ogni elemento $v \in S$, $\varphi'(v)$ è invertibile e, applicando la proprietà universale dell'anello delle frazioni, si trova che φ' estende in modo unico ad un morfismo $\varphi'' : (K[t_1, \ldots, t_r])_{\mathfrak{p}} \longrightarrow \overline{K}$. $(K[t_1, \ldots, t_r])_{\mathfrak{p}}\ [\alpha_1, \ldots, \alpha_n] \supset K[\alpha_1, \ldots, \alpha_n]$ è un' estensione intera di $(K[t_1, \ldots, t_r])_{\mathfrak{p}}$, quindi, per la proposizione 1.5.6, il morfismo φ'' si estende a $K[\alpha_1, \ldots, \alpha_n]$ ottenendo il morfismo $\overline{\varphi}$ voluto. □

Corollario 2.2.2. *Dato un generico campo K, se $K[\alpha_1, \ldots, \alpha_n]$ è un campo, allora $K[\alpha_1, \ldots, \alpha_n]$ è estensione algebrica di K.*

Dimostrazione. Sia $\varphi : K \hookrightarrow \overline{K}$ l'inclusione di K nella sua chiusura algebrica. Se $K[\alpha_1, \ldots, \alpha_n]$ è un campo, il teorema 2.2.1 garantisce che φ si estenda ad un morfismo di campi $\overline{\varphi} : K[\alpha_1, \ldots, \alpha_n] \to \overline{K}$. Poiché ogni morfismo di campi è iniettivo, si ha in $\overline{K}$ un'immagine isomorfa a $K[\alpha_1, \ldots, \alpha_n]$ e da qui il risultato. □

Come conseguenza del corollario si ha che, dato un ideale massimale $\mathfrak{M}$ dell'anello dei polinomi in n indeterminate $K[x_1, \ldots, x_n]$, l'estensione

$K[x_1, \ldots, x_n]/\mathfrak{M}$ è algebrica su K. Come ulteriore immediata conseguenza del precedente corollario si ha il risultato seguente, di importanza capitale nella dimostrazione del Nullstellensatz.

Corollario 2.2.3. *Se K è un campo algebricamente chiuso e $\mathfrak{M}$ è un ideale massimale di $K[x_1, \ldots, x_n]$, allora $K[x_1, \ldots, x_n]/\mathfrak{M} \cong K$.*

Dimostrazione. Si ha che $K[x_1, \ldots, x_n]/\mathfrak{M} \supseteq K'$, ove K' é un campo isomorfo a K. D'altronde, l'estensione $K[x_1, \ldots, x_n]/\mathfrak{M}$ è algebrica su K', ma visto che K, e quindi K', è algebricamente chiuso, si ha anche $K[x_1, \ldots, x_n]/\mathfrak{M} \subseteq K'$. Perciò $K[x_1, \ldots, x_n]/\mathfrak{M} = K' \cong K$. □

Esempio 2.2.4. È noto che:

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C} \tag{2.1}$$
$$\mathbb{C}[x]/(x - a) \cong \mathbb{C}. \tag{2.2}$$

In (2.1) non si ottiene un isomorfismo tra $\mathbb{R}[x]/(x^2 + 1)$ e $\mathbb{R}$, in quanto $\mathbb{R}$ non è algebricamente chiuso, mentre in (2.2) si ottiene un isomorfismo tra $\mathbb{C}[x]/(x - a)$ e $\mathbb{C}$, in quanto $\mathbb{C}$ è algebricamente chiuso.

D'ora innanzi, se non specificato altrimenti, con K si intenderà un campo algebricamente chiuso. Dopo queste premesse si è pronti per dimostrare la forma debole del teorema degli zeri di Hilbert.

Teorema 2.2.5 (Nullstellensatz, forma debole.)**.** *Sia I un ideale di $K[x_1, \ldots, x_n]$, ove K è algebricamente chiuso, e sia X un insieme algebrico tale per cui $X = V(I)$. Allora si ha una corrispondenza biunivoca:*

$$\{ \textit{ punti di } X \} \longleftrightarrow \{ \textit{ ideali massimali in } K[x_1, \ldots, x_n]/I \}$$
$$(a_1, a_2, \ldots, a_n) \longleftrightarrow (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n).$$

Dimostrazione. Innanzitutto si prova, nel caso $I = (0)$, che c' è una corrispondenza biunivoca tra punti in K^n e ideali massimali di $K[x_1, \ldots, x_n]$. Sia $P = (a_1, \ldots, a_n)$ un punto di K^n, allora $\mathfrak{M} = (x_1 - a_1, \ldots, x_n - a_n)$ è un ideale massimale di $K[x_1, \ldots, x_n]$ e $V(\mathfrak{M}) = P$. Bisogna ora mostrare che ogni ideale massimale $\mathfrak{M}$ di $K[x_1, \ldots, x_n]$ può essere espresso come $\mathfrak{M} = (x_1 - a_1, \ldots, x_n - a_n)$, dove $(a_1, \ldots, a_n) \in K^n$. Applicando il corollario 2.2.3 si ha che $K[x_1, \ldots, x_n]/\mathfrak{M} \cong K$, quindi:

$$\begin{aligned} K[x_1, \ldots, x_n]/\mathfrak{M} &\xrightarrow{\cong} K \\ x_i &\longmapsto a_i. \end{aligned}$$

Dimostriamo ora il teorema nel caso in cui intervenga un ideale non banale I di $K[x_1, \ldots, x_n]$. Sia $P = (a_1, \ldots, a_n) \in V(I)$. Se $1 \notin I$, allora $I \neq K[x_1, \ldots, x_n]$, quindi $K[x_1, \ldots, x_n]/I \neq (0)$. Se è così, $K[x_1, \ldots, x_n]/I \supseteq K'$, ove K' é campo isomorfo a K; perciò, quozientando con $(x_1 - a_1, \ldots, x_n - a_n)$, si ottiene un insieme contenente e contenuto in K', quindi $(K[x_1, \ldots, x_n]/I)/(x_1 - a_1, \ldots, x_n - a_n) \cong K$. Pertanto $(x_1 - a_1, \ldots, x_n - a_n)$ è un ideale massimale di $K[x_1, \ldots, x_n]/I$. Adesso si vuole mostrare che a ideali massimali di $K[x_1, \ldots, x_n]/I$ corrispondono punti appartenenti ad X. In principio si ricordi che, dati un anello A ed un suo ideale I, vi è una corrispondenza biunivoca tra ideali J di A/I e ideali $J' \supseteq I$ di A. in particolare ad ideali massimali J corrispondono ideali massimali J'. Dunque, se $\mathfrak{M}'$ è un ideale massimale di $K[x_1, \ldots, x_n]/I$, $\mathfrak{M}'$ corrisponde ad un ideale massimale $\mathfrak{M}$ di $K[x_1, \ldots, x_n]$, contenente I; perciò per quanto detto inizialmente, $\mathfrak{M}'$ corrisponde ad un punto $(a_1, \ldots, a_n) \in K^n$. Per concludere basta verificare che $(a_1, \ldots, a_n) \in X$, ma ciò è vero in quanto $f(a_1, \ldots, a_n) = 0 \ \forall f \in \mathfrak{M}$, quindi $f(a_1, \ldots, a_n) = 0 \ \forall f \in I \subseteq \mathfrak{M}$. Perciò $(a_1, \ldots, a_n) \in X$ e il teorema è dimostrato.

□

Si noti che la formulazione debole del Nullstellensatz è una generalizzazione del teorema fondamentale dell'algebra, infatti, se $n = 1$, l'ideale I in $K[x]$ è generato da un polinomio e $V(I)$ è l'insieme dei punti di K in cui tale polinomio si annulla.

2.3 Significato geometrico della forma debole

In questo paragrafo si cerca di illustrare il significato geometrico della formulazione debole del teorema degli zeri. Per farlo bisogna introdurre il concetto di polinomi definiti su insiemi algebrici. Sia $K[x_1, \ldots, x_n]$ l'anello dei polinomi in n indeterminate e sia I un suo ideale i cui elementi si annullano sull'insieme algebrico X.

Definizione 2.3.1. $K[x_1, \ldots, x_n]/I := P(X)$= *polinomi definiti su* X.

Tale definizione è ragionevole, infatti, se per polinomi $f, g \in K[x_1, \ldots, x_n]$ si ha che $f|_X = g|_X$, cioè $(f - g)|_X = 0 \ \forall x \in X$, allora $f - g \in I$; cioè le classi di equivalenza di f e g sono la stessa. In altre parole, due polinomi di $K[x_1, \ldots, x_n]$ che si comportano allo stesso modo sull'insieme algebrico X, corrispondono alla stessa classe in $K[x_1, \ldots, x_n]/I$. Un'ulteriore osservazione è la seguente. Visto che la relazione che associa ideali a insiemi algebrici rovescia le inclusioni, è intuitivo che ad ideali massimali di un anello

$K[x_1, \ldots, x_n]/I$ siano associati punti di X, cioè gli elementi più piccoli dell' insieme algebrico X. Questo, infatti, é precisamente l'enunciato del teorema degli zeri.

2.4 Nullstellensatz, forma forte

Ora, con l'ausilio di un ultimo teorema preliminare, è possibile dare una dimostrazione della forma forte del teorema degli zeri di Hilbert. Nei due teoremi seguenti con K si intenderà un campo qualsiasi.

Teorema 2.4.1. *Sia $\mathfrak{a}$ un ideale di $K[x_1, \ldots, x_n]$. Allora $\mathfrak{a} = K[x_1, \ldots, x_n]$, oppure esiste $P \in \overline{K}^n$ tale per cui $f(P) = 0$ per ogni $f \in \mathfrak{a}$.*

Dimostrazione. Supponendo $\mathfrak{a} \neq K[x_1, \ldots, x_n]$, dunque $\mathfrak{a}$ è contenuto in almeno un ideale massimale $\mathfrak{M}$, si deve provare che in $\overline{K}^n$ esiste uno zero comune a tutti gli elementi di $\mathfrak{a}$. $K[x_1, \ldots, x_n]/\mathfrak{M}$ è un campo contenente un sottocampo isomorfo a K, in quanto ciò non sarebbe vero solo nel caso si fosse quozientato per un ideale contenente un elemento di K, ma in tal caso si sarebbe verificato $\mathfrak{a} = K[x_1, \ldots, x_n]$.
Dal corollario 2.2.2 segue che $K[x_1, \ldots, x_n]/\mathfrak{M}$ è un'estensione algebrica di K e può quindi essere incluso in $\overline{K}$ tramite un morfismo i.

$$\begin{array}{ccccc} K[x_1, \ldots, x_n] & \xrightarrow{\pi} & K[x_1, \ldots, x_n]/\mathfrak{M} & \xhookrightarrow{i} & \overline{K} \\ g & \longrightarrow & \overline{g} & \longrightarrow & g' \end{array}$$

Tramite il morfismo $i \circ \pi$ si trova uno zero di $\mathfrak{M}$ e quindi anche uno zero di $\mathfrak{a}$, dato che $\mathfrak{M} \supset \mathfrak{a}$ implica $V(\mathfrak{M}) \subset V(\mathfrak{a})$. □

Teorema 2.4.2 (Nullstellensatz, forma forte)**.** *Sia $\mathfrak{a}$ un ideale di $K[x_1, \ldots, x_n]$. Sia $f \in K[x_1, \ldots, x_n]$ un polinomio per cui $f(c_1, \ldots, c_n) = 0$ $\forall (c_1, \ldots, c_n) \in V(\mathfrak{a}) \subseteq \overline{K}^n$. Allora esiste un numero naturale positivo m per cui $f^m \in \mathfrak{a}$.*

Dimostrazione. Si osservi innanzitutto che se $f = 0$ il teorema è valido, infatti, per $m = 1$, si ha $0^1 = 0 \in \mathfrak{a}$. Quindi non è restrittivo provare il teorema supponendo $f \neq 0$. Nella dimostrazione si fa uso del cosiddetto *Rabinowitsch trick*, che consiste nell'introdurre una nuova variabile Y e considerare l'ideale $\mathfrak{a}'$ generato da $1 - Yf$ e $\mathfrak{a}$ in $K[x_1, \ldots, x_n, Y]$. Siano $g, h \in K[x_1, \ldots, x_n, Y]$, $a \in \mathfrak{a}$. Si ha che $\mathfrak{a}'$ non si annulla in alcun punto di $\overline{K}^n$, dato che

$$ga + (1 - Yf)h = 0 \Longleftrightarrow ga + h - Yfh = 0 \Longleftrightarrow \frac{ga + h}{hf} = Y.$$

Infatti, se esistesse z, zero di $\mathfrak{a}'$, allora z sarebbe anche zero di $\mathfrak{a}$, però ciò non si può verificare, in quanto $f(z) = 0$. Pertanto, applicando il teorema precedente (2.4.1), si ha che $\mathfrak{a}'= K[x_1, \ldots, x_n, Y]$.
Quindi esistono polinomi $h_i \in \mathfrak{a}$ e $g_i \in K[x_1, \ldots, x_n, Y]$ per i quali

$$1 = g_0(1 - Yf) + g_1h_1 + \ldots + g_rh_r.$$

Sostituendo $f^{-1} = Y$ risulta

$$1 = g_0 0 + \frac{g_1'}{f^{n_1}}h_1 + \ldots + \frac{g_r'}{f^{n_r}}h_r.$$

Se si moltiplica per f^m, ove $m = \max n_i$, si ha

$$f^m = h_1g_1' + h_2g_2' + \ldots + h_rg_r' \Longrightarrow f^m \in \mathfrak{a}$$

ottenendo così il risultato voluto. □

Se si prendono in esame solo campi algebricamente chiusi i due teoremi precedenti si possono formulare non tenendo conto della differenza tra K e $\overline{K}$. Come conseguenza della forma forte del Nullstellensatz si ha che i seguenti concetti avranno un ruolo importante nella teoria.

Definizione 2.4.3. Sia $\mathfrak{a}$ un ideale di un anello A. Si definisce $r(\mathfrak{a})=\{x \in A \mid x^n \in \mathfrak{a}$ per qualche $n >0\}$. $r(\mathfrak{a})$ si dice *radicale dell'ideale* $\mathfrak{a}$. $\mathfrak{a}$ si dice ideale *radicale* se $r(\mathfrak{a}) = \mathfrak{a}$.

Esempio 2.4.4. Se $\mathfrak{a} = (x^3)$ si ha che $r(\mathfrak{a}) = (x) \neq \mathfrak{a}$. Perciò in questo esempio $\mathfrak{a}$ non è un ideale radicale.

Proposizione 2.4.5. *Nel caso K sia un campo algebricamente chiuso vi è una corrispondenza biunivoca :*

$\{$*ideali radicali di* $K[x_1, \ldots, x_n]\} \longleftrightarrow \{$*insiemi algebrici in* $K^n\}$

$$I \longleftrightarrow V(I).$$

Osservazione 2.4.6. Se un ideale $\mathfrak{p}$ è primo, allora è radicale.

Infatti, se $xy \in \mathfrak{p}$ primo allora x o $y \in \mathfrak{p}$ e, in particolare, se $x^n \in \mathfrak{p}$ allora x o $x^{n-1} \in \mathfrak{p}$. Nel caso $x \notin \mathfrak{p}$, ripetendo un numero finito di volte lo stesso procedimento con x^{n-1}, si ottiene che $x \in \mathfrak{p}$. Pertanto un ideale primo è anche radicale e, a maggior ragione, se un ideale è massimale allora è radicale.

Bibliografia

[1] Atiyah, M.F. & Macdonald, I.G. *Introduction to commutative algebra*, Addison-Wesley, 1969.

[2] Lang, S. *Algebra*, Springer, 2002.

[3] Hungerford, T.H. *Algebra*, Springer, 1996.

[4] Eisenbud, D. *Commutative algebra with a view toward algebraic geometry*, Springer, 1995.

[5] Hartshorne, R. *Algebraic Geometry*, Springer, 1997.

[6] Manetti, M. *Topologia*, Springer, 2008.

Ringraziamenti

Nonostante la timidezza che mi coglie nello scrivere pubblicamente dell'argomento, non posso non scrivere brevemente alcuni doverosi ringraziamenti a chi mi ha aiutato in questi tre anni di università. Meritano infatti di essere ringraziati: la prof. Fioresi per la pazienza e il tempo dedicato alla lettura e correzione delle bozze (spesso poco comprensibili) di questa tesi, i miei genitori per il sostegno economico datomi finora e, infine, le diverse persone incontrate in facoltà, senza le quali frequentare sarebbe certo stato molto molto più stancante.