Alma Mater Studiorum · Università di Bologna

**SCUOLA DI SCIENZE**
**Corso di Laurea in Matematica**

# TEORIA DELLA DIMENSIONE DI ANELLI AFFINI

**Tesi di Laurea in Geometria**

**Relatore:**
**Chiar.mo Prof.**
**Luca Migliorini**

**Presentata da:**
**Enrico Sintoni**

**III Sessione**
**Anno Accademico 2012/2013**

*So Long,*
*and Thanks for All the Fish*

# Introduzione

La tesi tratta la teoria della dimensione di anelli affini, che collega la teoria della dimensione sviluppata con metodi di algebra commutativa alla nozione intuitiva legata allo studio della geometria delle varietà algebriche. Alla fine del XIX secolo i matematici prestarono un certo interesse verso le superfici, intese come oggetti geometrici descritti come luoghi degli zeri di equazioni complesse in tre variabili. Il campo delle funzioni razionali definite su tali superfici, che giocava un ruolo centrale nella teoria, risulta avere grado di trascendenza su $\mathbb{C}$ pari a 2. Questo fatto fornì l'interpretazione che fossero sufficienti due funzioni algebriche per poter parametrizzare i punti di tali superfici, a meno di ambiguità finita, motivando la dimensione come 2.

Generalizzando tale studio a quello delle intersezioni di ipersuperfici nello spazio affine $X \subseteq k^n$, con $k$ campo algebricamente chiuso, è stato possibile definire l'anello delle coordinate su $X$ come il quoziente $k[X_1, \dots, X_n]/I$, dove $I$ è l'ideale delle funzioni polinomiali che si azzerano in $X$; per il teorema della base di Hilbert tale ideale è finitamente generato. Se l'anello delle coordinate è un dominio di integrità, ci si riferisce ad esso come anello affine e $X$ si definisce varietà algebrica affine. Assumendo l'assioma geometricamente inuitivo che uno spazio affine $k^n$ abbia dimensione $n$, nacque la definizione di dimensione geometrica per le varietà algebriche affini $X$ come il grado di trascendenza su $k$ del campo delle funzioni razionali definito su $X$, in altre parole il campo dei quozienti di $k[X_1, \dots, X_n]/I$.

Grazie al teorema degli zeri di Hilbert (Hilbert Nullstellensatz) e ai lavori di Noether è stato possibile stabilire una relazione tra la geometria e l'algebra, associando ad ogni varietà algebrica affine in $k^n$ un ideale radicale primo di $k[X_1, \dots, X_n]$, incoraggiando così un rapporto di reciproco sostegno tra l'algebra commutativa e la geometria algebrica. Nel merito della teoria della dimensione, ciò ha fornito numerose definizioni equivalenti di dimensione per le varietà algebriche affini.

In questa tesi verrà mostrata l'equivalenza tra la definizione di dimensione data dal grado di trascendenza su $k$ del campo delle funzioni razionali e una puramente algebrica, che coinvolge la funzione di Hilbert, strumento dell'algebra commutativa legato ai moduli graduati. In particolare, questa funzione coincide con un polinomio a coefficienti razionali per valori sufficientemente grandi, detto polinomio di Hilbert. Nel primo capitolo, di carattere puramente introduttivo, sono esposti i risultati e le nozioni fondamentali di algebra commutativa e di teoria dei campi necessarie per il secondo e il terzo capitolo. Nel secondo capitolo viene trattata la parte algebro commutativa. Vengono definiti i moduli graduati e la funzione di Hilbert, che viene mostrata essere polinomiale per valori sufficientemente grandi. In seguito viene definita la funzione di Hilbert-Samuel associata a un modulo finitamente generato su anello locale Noetheriano, anch'essa di tipo polinomiale, il cui grado differisce di una costante da quello del polinomio di Hilbert. Quest'ultima presenta notevoli vantaggi per la dimostrazione del teorema di dimensione, che afferma l'equivalenza tra la dimensione di un modulo finitamente generato su un anello locale Noetheriano (quindi di un anello locale Noetheriano) e il grado del polinomio di Hilbert-Samuel. Nel terzo capitolo viene presentato il lemma di normalizzazione di Noether, necessario per dimostrare che il grado di trascendenza di un anello affine sul campo $k$ è equivalente alla sua dimensione di Krull, che a sua volta è equivalente alla dimensione di Krull della sua localizzazione rispetto a un ideale massimale. Un'altra conseguenza è il Nullstellensatz, che implica il legame tra i punti di una varietà algebrica affine e gli ideali massimali del suo anello delle coordinate. Infine, viene dimostrato il legame tra la definizione geometrica di dimensione per una varietà algebrica affine, e il grado del polinomio di Hilbert associato all'anello affine localizzato in punto della varietà.

# Indice

# Capitolo 1

# Richiami e Nozioni Preliminari

Questo capitolo è destinato all'esposizione di alcuni concetti ed enunciati necessari per i risultati esposti nel secondo e terzo capitolo. Per le dimostrazioni si vedano [1], [2] e [3] per le prime cinque sezioni. Per la sesta si veda [5].

## 1.1 Anelli e Moduli Noetheriani e Artiniani

A partire da questa sezione, proseguendo per tutto il documento, si considerano solo anelli commutativi con unità.

**Definizione 1.1.1.** Un anello $R$ si dice **anello Noetheriano** se ogni catena ascendente di ideali $\{ I_n \}_{n\in\mathbb{N}}$ di $R$ è stazionaria.

**Proposizione 1.1.2.** *Un anello $R$ è Noetheriano se e solo se ogni ideale $I$ di $R$ è finitamente generato.*

**Teorema 1.1.3** (Teorema della Base di Hilbert)**.** *Sia $R$ un anello Noetheriano, allora $R[x]$ è un anello Noetheriano.*

**Definizione 1.1.4.** Un $R$-modulo $M$ si dice **modulo Noetheriano** se ogni catena ascendente di sottomoduli $\{ M_n \}_{n\in\mathbb{N}}$ di $M$ è stazionaria.

**Proposizione 1.1.5.** *Un $R$-modulo $M$ è modulo Noetheriano se e solo se ogni sottomodulo è finitamente generato.*

**Proposizione 1.1.6.** *Siano $R$ un anello Noetheriano e $M$ un $R$-modulo finitamente generato, allora $M$ è un modulo Noetheriano.*

**Definizione 1.1.7.** Un anello $R$ si dice **anello Artiniano** se ogni catena discendente di ideali $\{ I_n \}_{n\in\mathbb{N}}$ di $R$ è stazionaria. Si dice che $R$ soddisfa la **condizione della catena discendente sugli ideali**.

**Proposizione 1.1.8.** *Un anello $R$ è Artiniano se e solo se $R$ è Noetheriano e ogni ideale primo di $R$ è massimale.*

**Definizione 1.1.9.** Un $R$-modulo $M$ si dice **modulo Artiniano** se ogni catena discendente di sottomoduli $\{ M_n \}_{n \in \mathbb{N}}$ di $R$ è stazionaria.

**Proposizione 1.1.10.** *Siano $R$ un anello Artiniano e $M$ un $R$-modulo finitamente generato, allora $M$ è modulo Artiniano.*

## 1.2 Anelli e Moduli di Frazioni

**Definizione 1.2.1.** Sia $R$ un anello, un sottoinsieme $U \subseteq R$ si dice **moltiplicativamente chiuso** se $1 \in S$ e $a, b \in U \implies ab \in U$.

**Definizione 1.2.2.** Siano $R$ un anello e $U \subseteq R$ un sottoinsieme moltiplicativamente chiuso. Poniamo su $R \times U$ la relazione di equivalenza

$$(x, u) \sim (y, v) \quad \iff \quad \exists t \in U \ t(vx - uy) = 0.$$

Denotiamo le classi $[(x, u)]_\sim$ con $x/u$. L'anello quoziente $R[U^{-1}] := R \times U/ \sim$ con le operazioni di somma e prodotto definite come

$$\begin{aligned} (x/u) + (y/v) &:= (vx + uy)/uv, \\ (x/u)(y/v) &:= xy/uv, \end{aligned}$$

ha una struttura di anello e viene detto **anello delle frazioni** di $R$ rispetto a $U$ .

**Definizione 1.2.3.** Siano $M$ un $R$-modulo e $U \subseteq R$ un sottoinsieme moltiplicativamente chiuso. Poniamo su $M \times U$ la relazione di equivalenza

$$(x, u) \sim (y, v) \quad \iff \quad \exists t \in U \ t(vx - uy) = 0.$$

Denotiamo le classi $[(x, u)]_\sim$ con $x/u$. Il quoziente $M[U^{-1}] := M \times U/ \sim$ con l'operazione di somma

$$(x/u) + (y/v) := (vx + uy)/uv,$$

e col prodotto $R[U^{-1}] \times M[U^{-1}] \to M[U^{-1}]$ definito da

$$(x/u) \cdot (y/v) := x \cdot y/uv$$

ha una struttura di $R[U^{-1}]$-modulo e viene detto **modulo delle frazioni** di $M$ rispetto a $U$.

*Osservazione* 1.2.4. In entrambi i casi definiti è indotto il morfismo naturale $x \mapsto x/1$.

*Osservazione* 1.2.5. Siano $R$ un anello e $\mathfrak{p} \subseteq R$ un ideale primo, allora $R \backslash \mathfrak{p} \subseteq R$ è un sottinsieme moltiplicativamente chiuso, denotiamo $R_{\mathfrak{p}} := R[(R \backslash \mathfrak{p})^{-1}]$.

**Definizione 1.2.6.** Un anello $R$ si dice **anello locale** se possiede uno e un solo ideale massimale $\mathfrak{m}$. Verrà indicato con la coppia $(R, \mathfrak{m})$.

**Proposizione 1.2.7.** *Siano $R$ un anello e $\mathfrak{p} \subseteq R$ un ideale primo, allora $R_{\mathfrak{p}}$ è un anello locale.*

**Proposizione 1.2.8.** *Siano $I, \mathfrak{p}$ ideali di un anello $R$, con $\mathfrak{p}$ ideale primo. Allora $(R/I)_{\mathfrak{p}} \neq 0$ se e solo se $\mathfrak{p} \supseteq I$.*

## 1.3 Estensioni Intere di Anelli

**Definizione 1.3.1.** Siano $R \subseteq S$ un'estensione di anelli e $\alpha \in S$. Si dice che $\alpha$ **è intero su** $R$ se esiste $p \in R[X]$ monico per cui è soddisfatta la relazione

$$p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Si dice che $S$ **è intero su** $R$, o che $R \subseteq S$ è un'estensione intera di anelli, se ogni $\alpha \in S$ è intero su $R$.

**Definizione 1.3.2.** Sia $R \subseteq S$ un'estensione di anelli. Si dice **chiusura integrale di $R$ in $S$** l'insieme

$$R_C = \{\, \alpha \in S \mid \alpha \text{ è intero su } R \,\}.$$

Si dice che $R$ **è integralmente chiuso in** $S$ se $R = R_C$. Se $R$ è un dominio di integrità, diremo che $R$ **è integralmente chiuso** se lo è in $\operatorname{Frac} R$.

*Osservazione* 1.3.3. La chiusura integrale $R_C$ contiene $R$ ed è un sottoanello di $S$. In particolare è il più piccolo sottoanello di $S$ integralmente chiuso in $S$ contenente $R$.

**Teorema 1.3.4 (Transitività delle Estensioni Intere).** *Siano $A \subseteq B$ e $B \subseteq C$ estensioni intere di anelli. Allora $A \subseteq C$ è un'estensione intera di anelli.*

**Proposizione 1.3.5.** *Sia $R \subseteq S$ un'estensione intera di anelli, allora $S$ è una $R$-algebra finitamente generata se e solo se $S$ è un $R$-modulo finitamente generato.*

**Definizione 1.3.6.** Sia $f\colon R \to S$ un morfismo di anelli e $I \subseteq R$, $J \subseteq S$ ideali. Si dice che $J$ **giace su** $I$ se $I = f^{-1}(J)$.

**Notazione 1.3.7.** Se $R \subseteq S$ è una estensione di anelli, si considera il morfismo di inclusione. Ovvero, $J$ giace su $I$ se $I = i^{-1}(J) = R \cap J$.

**Proposizione 1.3.8.** *Sia $R$ un dominio a fattorizzazione unica, allora $R$ è integralmente chiuso.*

**Teorema 1.3.9** (**Going Up Theorem**)**.** *Sia $R \subseteq S$ un'estensione intera di anelli. Siano $\mathfrak{p}_1, \subseteq \cdots \subseteq \mathfrak{p}_n$ e $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ catene di ideali primi, rispettivamente, di $R$ e $S$, con $m < n$. Se $\mathfrak{q}_i$ giace su $\mathfrak{p}_i$ per ogni $i = 1, \ldots, m$, allora esistono $\mathfrak{q}_{m+1}, \ldots, \mathfrak{q}_n$ ideali primi di $S$ tali che $\mathfrak{q}_m \subseteq \mathfrak{q}_{m+1} \subseteq \cdots \subseteq \mathfrak{q}_n$ e $\mathfrak{q}_i$ giace su $\mathfrak{p}_i$ per ogni $i = m+1, \ldots, n$.*

**Teorema 1.3.10** (**Going Down Theorem**)**.** *Sia $R \subseteq S$ un'estensione intera di domini di integrità, con $R$ integralmente chiuso. Siano $\mathfrak{p}_1, \subseteq \cdots \subseteq \mathfrak{p}_n$ e $\mathfrak{q}_m \subseteq \cdots \subseteq \mathfrak{q}_n$ catene di ideali primi, rispettivamente, di $R$ e $S$, con $1 < m \leq n$. Se $\mathfrak{q}_i$ giace su $\mathfrak{p}_i$ per ogni $i = m, \ldots, n$, allora esistono $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m-1}$ ideali primi di $S$ tali che $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_{m-1} \subseteq \mathfrak{q}_m$ e $\mathfrak{q}_i$ giace su $\mathfrak{p}_i$ per ogni $i = m+1, \ldots, n$.*

## 1.4 Primi Associati e Supporto di un Modulo

**Definizione 1.4.1.** Siano $M$ un $R$-modulo e $S \subseteq M$ un sottoinsieme, si definisce l'**annichilatore di** $S$ come

$$\operatorname{Ann} S = \{\, r \in R \mid rs = 0 \quad \forall s \in S \,\}.$$

**Definizione 1.4.2.** Sia $M$ un $R$-modulo, si dice che un ideale primo $\mathfrak{p}$ di $R$ è un **primo associato** a $M$ se esiste $x \in M$ non nullo tale che $\mathfrak{p} = \operatorname{Ann} x$. Si denota l'insieme dei primi associati a $M$ come $\operatorname{Ass} M$.

**Proposizione 1.4.3.** *Sia $M$ un $R$-modulo. Allora $\mathfrak{p} \in \operatorname{Ass} M$ se e solo se esiste un morfismo iniettivo di $R$-moduli $R/\mathfrak{p} \hookrightarrow M$.*

**Proposizione 1.4.4.** *Siano $R$ un anello Noetheriano e $M$ un $R$-modulo. Allora $M = 0$ se e solo se $\operatorname{Ass} M = \emptyset$.*

**Teorema 1.4.5.** *Siano $R$ un anello Noetheriano e $M$ un $R$-modulo non nullo finitamente generato. Allora $\operatorname{Ass} M$ è finito.*

**Proposizione 1.4.6.** *Siano $R$ un anello Noetheriano, $\mathfrak{m}, I \subseteq R$ ideali di $R$ con $\mathfrak{m}$ ideale massimale. Allora esiste $n \in \mathbb{N}$ tale che $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ se e solo se $\operatorname{Ass} R/I = \{\, \mathfrak{m} \,\}$.*

**Definizione 1.4.7.** Sia $M$ un $R$-modulo, si definisce il **supporto di** $M$, denotato $\operatorname{Supp} M$, come l'insieme degli ideali primi $\mathfrak{p}$ di $R$ tali che $M_{\mathfrak{p}} \neq 0$.

**Definizione 1.4.8.** Sia $I$ un ideale di un anello $R$, si denota con $V(I)$ l'insieme degli ideali primi $\mathfrak{p}$ di $R$ con $I \subseteq P$.

**Teorema 1.4.9.** *Sia $M$ un $R$-modulo finitamente generato, allora* $\operatorname{Supp} M = V(\operatorname{Ann} M)$.

**Teorema 1.4.10.** *Siano $R$ un anello Noetheriano e $M$ un $R$-modulo finitamente generato. Allora* $\operatorname{Ass} M \subseteq \operatorname{Supp} M$ *e gli elementi minimali in* $\operatorname{Ass} M$ *e in* $\operatorname{Supp} M$ *coincidono.*

**Proposizione 1.4.11.** *Siano $M$ e $N$ due $R$-moduli finitamente generati, allora* $\operatorname{Supp} M \otimes_R N = \operatorname{Supp} M \cap \operatorname{Supp} N$.

## 1.5 Dimensione di Krull di un Anello

**Definizione 1.5.1.** Siano $R$ un anello e $\mathfrak{p} \subseteq R$ un ideale primo. Si definisce la **altezza di** $\mathfrak{p}$, denotata $\operatorname{ht} \mathfrak{p}$, come il massimo della lunghezza $n$ delle catene di ideali primi $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ di $R$.

**Definizione 1.5.2.** Siano $R$ un anello e $\mathfrak{p} \subseteq R$ un ideale primo. Si definisce la **coaltezza di** $\mathfrak{p}$, denotata $\operatorname{coht} \mathfrak{p}$, come il massimo della lunghezza $n$ delle catene di ideali primi $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ di $R$.

**Definizione 1.5.3.** Sia $I \subseteq R$ un ideale. Si definiscono l'**altezza di** $I$ come l'estremo inferiore delle altezze degli ideali $\mathfrak{p} \supseteq I$, e la **coaltezza di** $I$ come l'estremo superiore delle coaltezze degli ideali $\mathfrak{p} \supseteq I$. Sono, rispettivamente, denotate con $\operatorname{ht} I$ e $\operatorname{coht} I$.

**Definizione 1.5.4.** Si definisce la **dimensione di Krull** (o **dimensione**) di un anello $R$, denotata $\dim R$, come l'estremo superiore della lunghezza $n$ delle catene di ideali primi $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ di $R$.

**Proposizione 1.5.5.** *Siano $R$ un anello e $\mathfrak{p} \subseteq R$ un ideale primo, allora* $\dim R_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}$ *e* $\dim R/\mathfrak{p} = \operatorname{coht} \mathfrak{p}$.

*Osservazione* 1.5.6. Sia $k$ un campo, allora $\dim k = 0$. Poiché ogni polinomio irriducibile di grado positivo genera un ideale massimale di $k[X]$, si ha $\dim k[X] = 1$. Più in generale si ha:

**Teorema 1.5.7.** *Sia $R$ un anello Noetheriano, allora* $\dim R[X] = 1 + \dim R$. *In particolare* $\dim R[X_1, \ldots, X_n] = n + \dim R$.

**Proposizione 1.5.8.** *Sia $R \subseteq S$ un'estensione intera di anelli, allora* $\dim R = \dim S$.

**Proposizione 1.5.9.** *Siano $R \subseteq S$ un'estensione intera di anelli e $J \subseteq S$ un ideale. Sia $I = J \cap R$ un ideale di $R$, allora* $\operatorname{coht} J = \operatorname{coht} I$.

## 1.6 Estensioni Trascendenti di Campi

**Definizione 1.6.1.** Siano $F$ e $E$ campi. Il campo $E$ si dice **estensione di $F$** se $F$ è sottocampo di $E$. L'inclusione $i\colon F \hookrightarrow E$ si dice **estensione di campi**, si denota con $F \subseteq E$.

**Definizione 1.6.2.** Sia $F \subseteq E$ un'estensione di campi, si definisce il **grado di $F$ su $E$** come $[E : F] := \deg_F E$, la dimensione di $E$ come $F$-spazio vettoriale. L'estensione di campi $F \subseteq E$ si dice **finita** se il grado di $F$ su $E$ è finito.

**Definizione 1.6.3.** Siano $F \subseteq E$ un'estensione di campi e $\alpha \in E$. Si definisce **morfismo di valutazione in $\alpha$** l'omomorfismo di anelli:

$$\begin{array}{rccc} \upsilon_\alpha\colon & F[x] & \longrightarrow & E \\ & p(x) & \longmapsto & p(\alpha) \end{array}$$

Se $\operatorname{Ker} \upsilon_\alpha \neq 0$, allora $\alpha$ si dice **algebrico su $F$**. Altrimenti, se $\operatorname{Ker} \upsilon_\alpha = 0$, si dice che $\alpha$ è **trascendente su $F$**.

**Definizione 1.6.4.** Un'estensione di campi $F \subseteq E$ si dice **estensione algebrica** se ogni $\alpha \in E$ è algebrico su $F$, altrimenti si dice **estensione trascendente**.

**Proposizione 1.6.5.** *Un'estensione di campi $F \subseteq E$ è finita se e solo se è algebrica e $E$ è una $F$-algebra finitamente generata.*

**Definizione 1.6.6.** Siano $F \subseteq \Omega$ un'estensione di campi e $\alpha_1, \dots, \alpha_n \in \Omega$. Si definisce **morfismo di valutazione in $\alpha = (\alpha_1, \dots, \alpha_n)$** il seguente omomorfismo di anelli:

$$\begin{array}{rccc} \upsilon_\alpha\colon & F[x_1, \dots, x_n] & \longrightarrow & \Omega \\ & p(x_1, \dots, x_n) & \longmapsto & p(\alpha_1, \dots, \alpha_n) \end{array}$$

Se $\operatorname{Ker} \upsilon_\alpha = 0$, allora $\alpha_1, \dots, \alpha_n$ si dicono **algebricamente indipendenti su $F$**. Altrimenti $\alpha_1, \dots, \alpha_n$ si dicono **algebricamente dipendenti su $F$**.

**Definizione 1.6.7.** Sia $F \subseteq \Omega$ un'estensione di campi. Un sottoinsieme $A \subseteq \Omega$ si dice **algebricamente indipendente su** $F$ se ogni sottoinsieme $U \subseteq A$ finito è algebricamente indipendente su $F$. Altrimenti $A$ si dice **algebricamente dipendente su** $F$.

**Definizione 1.6.8.** Siano $F \subseteq \Omega$ un'estensione di campi e $\alpha_1, \dots, \alpha_n \in \Omega$ algebricamente indipendenti su $F$. Il campo $F(\alpha_1, \dots, \alpha_n)$ si dice **estensione puramente trascendente** di $F$.

**Definizione 1.6.9.** Siano $F \subseteq \Omega$ un'estensione di campi, $\gamma \in \Omega$ e $A \subseteq \Omega$. Si dice che $\gamma$ è **algebricamente dipendente su** $A$ **sopra** $F$ se $\gamma$ è algebrico su $F(A)$.

**Definizione 1.6.10.** Siano $F \subseteq \Omega$ un'estensione di campi e $A, B \subseteq \Omega$. Si dice che $B$ è **algebricamente dipendente su** $A$ **(sopra** $F$**)** se ogni $\gamma \in B$ è algebrico su $F(A)$.

**Lemma 1.6.11** (**Proprietà di Scambio**)**.** *Siano $F \subseteq \Omega$ un'estensione di campi e $A = \{ \alpha_1, \dots, \alpha_m \} \subseteq \Omega$. Se $\beta \in \Omega$ è algebricamente dipendente su $A$ (sopra $F$) e non è algebricamente dipendente su $A' = A \setminus \{ \alpha_m \}$ (sopra $F$), allora $\alpha_m$ è algebricamente dipendente su $A' \cup \{ \beta \}$.*

**Lemma 1.6.12** (**Transitività della Dipendenza Algebrica**)**.** *Siano $F \subseteq \Omega$ un'estensione di campi e $A, B, C \subseteq \Omega$. Se $A$ è algebricamente dipendente su $B$ (sopra $F$) e $B$ è algebricamente dipendente su $C$ (sopra $F$), allora $A$ è algebricamente dipendente su $C$ (sopra $F$).*

**Teorema 1.6.13.** *Sia $F \subseteq \Omega$ un'estensione di campi. Siano*

$$A = \{ \alpha_1, \dots, \alpha_m \}, \qquad B = \{ \beta_1, \dots, \beta_n \}$$

*sottoinsiemi di $\Omega$. Se $A$ è algebricamente indipendente su $F$ e $A$ è algebricamente dipendente su $B$ (sopra $F$), allora $m \leq n$.*

**Definizione 1.6.14.** Sia $F \subseteq \Omega$ un'estensione di campi. Si dice **base di trascendenza per** $\Omega$ **su** $F$ un sottoinsieme $A \subseteq \Omega$ algebricamente indipendente su $F$ tale che $\Omega$ sia algebrico su $F(A)$.

**Lemma 1.6.15.** *Siano $F \subseteq \Omega$ un'estensione di campi e $A \subseteq \Omega$. Se $\Omega$ è algebrico su $F(A)$ e $A$ è elemento minimale nell'insieme dei sottoinsiemi di $\Omega$ algebrici su $F(A)$, allora $A$ è una base di trascendenza per $\Omega$ su $F$.*

**Teorema 1.6.16.** *Sia $F \subseteq \Omega$ un'estensione di campi. Se esiste $A \subseteq \Omega$ finito tale che $\Omega$ sia algebrico su $F(A)$, allora esiste $B \subseteq \Omega$ base di trascendenza per $\Omega$ su $F$. Inoltre, ogni base di trascendenza di $\Omega$ su $F$ è finita e hanno tutte la stessa cardinalità.*

**Definizione 1.6.17.** Siano $F \subseteq \Omega$ un'estensione di campi, $B \subseteq \Omega$ finito una base di trascendenza di $\Omega$ su $F$. Si definisce il **grado di trascendenza di $\Omega$ su $F$** come

$$\operatorname{tr}\deg_F \Omega := |B|.$$

**Proposizione 1.6.18.** *Sia $F \subseteq \Omega$ un'estensione di campi. Ogni elemento massimale $A \subseteq \Omega$ nell'insieme dei sottoinsiemi di $\Omega$ algebricamente indipendenti su $F$ è una base di trascendenza per $\Omega$ su $F$.*

# Capitolo 2

# Teoria della Dimensione

In questo capitolo verrà dimostrata l'equivalenza tra tre definizioni di dimensione per un modulo su un anello locale Noetheriano. In particolare, la definizione in termini di grado del polinomio di Hilbert presenta notevoli vantaggi da un punto di vista tecnico.

## 2.1 Anelli e Moduli Graduati

**Definizione 2.1.1.** Un anello $R$ si dice **anello graduato** se esiste una famiglia di sottogruppo additivi $\{ R_n \}_{n\in\mathbb{N}}$ tale che $R_iR_j \subseteq R_{i+j}$ per ogni $i, j \in \mathbb{N}$ e

$$R = \bigoplus_{n=0}^{\infty} R_n.$$

Gli elementi di $R_i$ si dicono **omogenei** di grado $i$.

**Definizione 2.1.2.** Sia $R$ un anello graduato, il sottoinsieme $R_+ = \bigoplus_{n=1}^{\infty} R_n$ è un ideale e si dice **ideale irrilevante** di $R$.

**Proposizione 2.1.3.** *Sia $R = \bigoplus_{n=0}^{\infty} R_n$ un anello graduato, allora:*

1. *$R_0$ è un sottoanello di $R$.*

2. *$R$ è un anello Noetheriano se, e solo se, $R_0$ è un anello Noetheriano e $R$ è una $R_0$-algebra finitamente generata.*

*Dimostrazione. (1.)* Per definizione $R_0R_0 \subseteq R_0$. Mostriamo che $1 \in R_0$. Si ha $1 = \sum_{n=0}^{\infty} x_n$, dove $x_n \in R_n$. Per ogni $a \in R_m$ si ha $a = \sum_{n=0}^{\infty} x_na$, uguagliando le componenti per grado otteniamo $a = x_0a$. Così per ogni $b \in R$ si ha $bx_0 = b$, ovvero $1 = x_0 \in R_0$.

*(2.)* Sia $R$ un anello Noetheriano. Poichè $R_0 \cong R/R_+$, si ottiene che $R_0$ è un anello Noetheriano. Per ipotesi $R_+$ è finitamente generato, diciamo da elementi omogenei $a_1, \ldots, a_r$, di grado $n_1, \ldots, n_r$ rispettivamente. Sia $R' = R_0[a_1, \ldots, a_r]$. Mostriamo che $R_n \subseteq R'$ per ogni $n \in \mathbb{N}$, così $R \subseteq R'$. Procediamo per induzione su $n$. Sia $n = 0$, per definizione $R_0 \subseteq R'$. Supponiamolo vero per $d \leq n-1$ e dimostriamolo per $n > 0$. Sia $b \in R_n \subseteq R_+$, dunque $b = x_1 a_1 + \cdots + x_r a_r$, dove, se $n_i \leq n$, ogni $x_i$ è omogeneo di grado $n - n_i < n$, altrimenti è $x_i$ è nullo. Per ipotesi induttiva $x_i \in R'$, quindi da $a_i \in R'$ si ha $b \in R'$.

Viceversa, siano $R_0$ un anello Noetheriano e $R$ una $R_0$-algebra finitamente generata. Dunque $R$ è isomorfo a un quoziente dell'anello di polinomi $R_0[X_1, \ldots, X_n]$, che è Noetheriano per il teorema della base di Hilbert. Quindi $R$ è Noetheriano. □

**Definizione 2.1.4.** Sia $R = \bigoplus_{n=0}^{\infty} R_n$ un anello graduato. Un $R$-modulo $M$ si dice **modulo graduato** se esiste una famiglia di sottogruppi additivi $\{ M_n \}_{n \in \mathbb{N}}$ tale che $R_i M_j \subseteq M_{i+j}$ per ogni $i, j \in \mathbb{N}$ e

$$M = \bigoplus_{n=0}^{\infty} M_n.$$

### 2.1.1 Anelli e Moduli Graduati Associati

**Definizione 2.1.5.** Sia $R$ un anello, una **filtrazione** $R = R_0 \supseteq R_1 \supseteq \cdots \supseteq R_n \supseteq \cdots$ di $R$ è una successione di sottogruppi additivi tali che $R_i R_j \subseteq R_{i+j}$ per ogni $i, j \geq 0$. Un anello dotato di una filtrazione si dice **anello filtrato**.

**Definizione 2.1.6.** Siano $R$ un anello filtrato, si definisce l'**anello graduato associato** a $R$ come

$$\operatorname{gr} R := \bigoplus_{n=0}^{\infty} R_n / R_{n+1},$$

dove il prodotto su $\operatorname{gr}_I R$ è definito per ogni $a \in R_m$ e $b \in R_n$ come

$$(a + R_{m+1}) \cdot (b + R_{n+1}) := ab + R_{m+n+1} \in R_{m+n}/R_{m+n+1}.$$

**Definizione 2.1.7.** Siano $R$ un anello filtrato e $M$ un $R$-modulo, una **filtrazione** $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots$ di $M$ è una successione di sottomoduli tali che $R_i M_j \subseteq M_{i+j}$ per ogni $i, j \geq 0$. Un modulo dotato di una filtrazione si dice **modulo filtrato**.

**Definizione 2.1.8.** Siano $M$ un $R$-modulo filtrato, si definisce il **modulo graduato associato** a $M$ come

$$\operatorname{gr} M := \bigoplus_{n=0}^{\infty} M_n/M_{n+1}.$$

Ammette una struttura di gr $R$-modulo, dove il prodotto per scalare è definito per ogni $a \in R_m$ e $x \in M_n$ come

$$(a + R_{m+1}) \cdot (x + M_{n+1}) := a \cdot x + M_{m+n+1} \in M_{m+n}/M_{m+n+1}.$$

### 2.1.2 $I$-filtrazioni e Lemma di Artin-Rees

**Definizione 2.1.9.** Siano $M$ un $R$-modulo filtrato e $I \subseteq R$ un ideale. Una filtrazione $\{ M_n \}_{n\in\mathbb{N}}$ di $M$ si dice **$I$-filtrazione** se $IM_n \subseteq M_{n+1}$ per ogni $n \geq 0$. Una $I$-filtrazione si dice **$I$-stabile** se esiste $N \in \mathbb{N}$ tale che $IM_n = M_{n+1}$ per ogni $n \geq N$.

*Osservazione* 2.1.10. Siano $I$ un ideale di un anello $R$ e $M$ un $R$-modulo, le successioni $\{ I^n \}_{n\in\mathbb{N}}$ e $\{ I^n M \}_{n\in\mathbb{N}}$ (si pone $I^0 = R$) sono filtrazioni $I$-stabili, rispettivamente, di $R$ e $M$

**Proposizione 2.1.11.** *Siano $R$ un anello Noetheriano, $M$ un $R$-modulo finitamente generato e $I \subseteq R$ un ideale. Sia $\{ M_n \}_{n\in\mathbb{N}}$ una $I$-filtrazione. Definiamo l'anello graduato $\tilde{R}$ e il $\tilde{R}$-modulo graduato $\tilde{M}$ come segue*

$$\tilde{R} = \bigoplus_{n=0}^{\infty} I^n, \qquad \tilde{M} = \bigoplus_{n=0}^{\infty} M_n.$$

*Allora sono equivalenti:*

1. *$\{ M_n \}_{n\in\mathbb{N}}$ è $I$-stabile.*

2. *$\tilde{M}$ è un $\tilde{R}$-modulo graduato finitamente generato.*

*Dimostrazione.* Sia $N_n = \bigoplus_{i=0}^{n} M_i$, quindi poniamo

$$\tilde{M}_n = N_n \oplus (\bigoplus_{i=1}^{\infty} I^i M_n) = M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots .$$

Poiché $M$ è Noetheriano, ogni suo sottomodulo è finitamente generato. Così $N_n$ è un $R$-modulo finitamente generato e $\tilde{M}_n$ è un $\tilde{R}$-modulo finitamente generato. Per definizione

$$\tilde{M} = \bigcup_{n=0}^{\infty} \tilde{M}_n, \qquad \tilde{M}_0 \subseteq \tilde{M}_1 \subseteq \cdots \subseteq \tilde{M}_n \subseteq \cdots ,$$

quindi $\tilde{M}$ è un $\tilde{R}$-modulo finitamente generato se e solo se esiste $m \in \mathbb{N}$ tale che $\tilde{M}_n = \tilde{M}_m$ per ogni $n \geq m$, cioè equivale ad affermare che $I^n M_m = M_{m+n}$ per ogni $n \geq 0$, ovvero $\{ M_n \}_{n\in\mathbb{N}}$ è $I$-stabile. □

**Lemma 2.1.12 (Lemma di Artin-Rees).** *Siano $R$ un anello Noetheriano, $M$ un $R$-modulo filtrato finitamente generato e $N \subseteq M$ un sottomodulo. Siano $I \subseteq R$ un ideale e $\{ M_n \}_{n\in\mathbb{N}}$ una filtrazione $I$-stabile di $M$, allora la filtrazione $\{ N \cap M_n \}_{n\in\mathbb{N}}$ indotta su $N$ è $I$-stabile.*

*Dimostrazione.* Sia $N_n = N \cap M_n$. Poiché $IN_n \subseteq N, M_{n+1}$, deve essere $IN_n \subseteq N \cap M_{n+1} = N_{n+1}$, pertanto è una $I$-filtrazione. Ora poniamo

$$\tilde{R} = \bigoplus_{n=0}^{\infty} I^n, \qquad \tilde{M} = \bigoplus_{n=0}^{\infty} M_n, \qquad \tilde{N} = \bigoplus_{n=0}^{\infty} N_n.$$

Per ipotesi $R$ è Noetheriano, quindi $I$ è finitamente generato e così $\tilde{R}$ è una $R$-algebra finitamente generata. Per (2.1.3) $\tilde{R}$ è un anello Noetheriano e per (2.1.11) $\tilde{M}$ è un $\tilde{R}$-modulo finitamente generato, quindi è un modulo Noetheriano. Allora il suo sottomodulo $\tilde{N}$ è finitamente generato e, di nuovo per (2.1.11) la filtrazione indotta è $I$-stabile. □

## 2.2 Serie di Poincaré e Funzione di Hilbert

**Definizione 2.2.1.** Siano $R$ un anello e $\mathbf{C}$ una sottoclasse della classe degli $R$-moduli. Una funzione $\lambda \colon \mathbf{C} \to \mathbb{Z}$ si dice **additiva** se, per ogni successione esatta corta di $R$-moduli

$$0 \to M \to N \to P \to 0, \qquad M, N, P \in \mathbf{C},$$

si ha

$$\lambda(M) - \lambda(N) + \lambda(P) = 0$$

*Osservazione* 2.2.2. Siano $R$ un anello, $\mathbf{C}$ una classe di $R$-moduli con $0 \in \mathbf{C}$ e $\lambda \colon \mathbf{C} \to \mathbb{Z}$ additiva, allora $\lambda(0) = 0$. Posti $M = N = P = 0$ si ha una successione esatta corta, quindi

$$\lambda(0) = \lambda(0) - \lambda(0) + \lambda(0) = 0$$

**Proposizione 2.2.3.** *Siano $R$ un anello, $\mathbf{C}$ una classe di $R$-moduli e la seguente una successione esatta*

$$0 = M_{-1} \to M_0 \to M_1 \to \cdots \to M_n \to M_{n+1} = 0.$$

*Sia $N_i$ l'immagine dell'omomorfismo $M_{i-1} \to M_i$, per $i = 0, \dots, n+1$. Se $M_i, N_i \in \mathbf{C}$, allora per ogni $\lambda \colon \mathbf{C} \to \mathbb{Z}$ funzione additiva si ha*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

*Dimostrazione.* Osserviamo che $N_0 = N_{n+1} = 0$. Per ogni $i = 0, \dots, n$ si ha la successione esatta corta

$$0 \to N_i \to M_i \to N_{i+1} \to 0,$$

e per ipotesi di additività

$$\lambda(N_i) - \lambda(M_i) + \lambda(N_{i+1}) = 0 \quad \iff \quad \lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1}).$$

Sostituendo nella somma a segni alterni, per l'osservazione precedente si ottiene

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = \sum_{i=0}^{n} (-1)^i (\lambda(N_i) + \lambda(N_{i+1})) = \lambda(N_0) + (-1)^n \lambda(N_{n+1}) = 0$$

□

**Definizione 2.2.4.** Siano $R$ un anello graduato Noetheriano, $M$ un $R$-modulo graduato finitamente generato, $\mathbf{C}$ la classe degli $R_0$-moduli finitamente generati e $\lambda \colon \mathbf{C} \to \mathbb{Z}$ additiva. Si definisce la **serie di Poincaré di $M$ rispetto a $\lambda$** come la serie di potenze

$$P_M(X) := \sum_{n=0}^{\infty} \lambda(M_n) X^n \qquad \in \mathbb{Z}[[X]].$$

**Teorema 2.2.5 (Teorema di Hilbert-Serre).** *Nelle ipotesi di (2.2.4), esistono $f(X) \in \mathbb{Z}[X]$ e $k_1, \dots, k_s \in \mathbb{N}$ tali che*

$$P_M(X) = \frac{f(X)}{\prod_{i=1}^{s} (1 - X^{k_i})}.$$

*Dimostrazione.* Poiché $R$ è Noetheriano esistono $x_1, \dots, x_s \in R$ omogenei, rispettivamente di grado $k_1, \dots, k_s > 0$, tali che $R = R_0[x_1, \dots, x_s]$. Per dimostrare l'asserto, procediamo per induzione su $s$.

Sia $s = 0$, dunque $R = R_0$ e $M$ è un $R_0$-modulo graduato finitamente generato, pertanto esistono $m_1, \dots, m_t \in M$ omogenei, rispettivamente di grado

$r_1, \dots, r_t$, che generano $M$. Segue $M_n = 0$ per ogni $n > r = \max_{i=1,\dots,t}\{r_i\}$. Dunque

$$P_M(X) = \sum_{n=0}^{\infty} \lambda(M_n)X^n = \sum_{n=0}^{r} \lambda(M_n)X^n \qquad \in \mathbb{Z}[X].$$

Supponiamo vero l'asserto per $s-1$, quindi dimostriamolo per $s > 0$. Definiamo su $M$ l'endomorfismo $\chi$ dato da $m \mapsto x_s m$. Così per ogni $n \in \mathbb{N}$ otteniamo l'omomorfismo di $R_0$-moduli

$$\begin{array}{rccc} \chi_n\colon & M_n & \longrightarrow & M_{n+k_s} \\ & m & \longmapsto & x_s m \end{array}$$

È indotta la seguente successione esatta di $R_0$-moduli per ogni $n \in \mathbb{N}$

$$0 \to \operatorname{Ker}\chi_n \hookrightarrow M_n \xrightarrow{\chi_n} M_{n+k_s} \twoheadrightarrow M_{n+k_s}/x_s M_n \to 0.$$

Per additività di $\lambda$, ne consegue

$$\lambda(M_{n+k_s}) - \lambda(M_n) = \lambda(M_{n+k_s}/x_s M_n) - \lambda(\operatorname{Ker}\chi_n).$$

Ora osserviamo che

$$R_0[x_1, \dots, x_{s-1}] \cong R/x_s R = \bigoplus_{n=0}^{\infty} (R_n + x_s R)/x_s R$$

è un anello graduato finitamente generato come $R_0$-algebra, con $R_0$ Noetheriano, quindi è Noetheriano. Inoltre

$$K = \bigoplus_{n=0}^{\infty} \operatorname{Ker}\chi_n \cong \operatorname{Ker}\chi, \qquad L = \bigoplus_{n=0}^{\infty} M_n/(M_n \cap x_s M)$$

sono $R_0[x_1, \dots, x_{s-1}]$-moduli graduati finitamente generati in quanto, rispettivamente, sottomodulo e modulo quoziente di $M$. Ora osserviamo che

$$\begin{aligned}
(1 - X^{k_s})P_M(X) &= \sum_{n=0}^{\infty} \lambda(M_n)X^n - \sum_{n=0}^{\infty} \lambda(M_n)X^{n+k_s} \\
&= \sum_{n=0}^{k_s-1} \lambda(M_n)X^n + \sum_{n=0}^{\infty} (\lambda(M_{n+k_s}) - \lambda(M_n))X^{n+k_s} \\
&= p(X) + \sum_{n=0}^{\infty} (\lambda(M_{n+k_s}/x_s M_n) - \lambda(\operatorname{Ker}\chi_n))X^{n+k_s} \\
&= p(X) + \sum_{n=0}^{\infty} \lambda(M_{n+k_s}/x_s M_n)X^{n+k_s} - X^{k_s} \sum_{n=0}^{\infty} \lambda(\operatorname{Ker}\chi_n)X^n.
\end{aligned}$$

Le due serie sono, rispettivamente, $P_L(X) - \sum_{n=0}^{k_s-1} \lambda(M_n/(M_n \cap x_s M))X^n$ e $P_K(X)$. Quindi per ipotesi induttiva esistono $f_L, f_K \in \mathbb{Z}[X]$ tali che

$$(1 - X^{k_s})P_M(X) = \frac{\left(\prod_{i=1}^{s-1}(1 - X^{k_i})\right) g(X) + f_L(X) - X^{k_s} f_K(X)}{\prod_{i=1}^{s-1}(1 - X^{k_i})}$$

Infine, denotando il polinomio a numeratore come $f(X)$, si ottiene

$$P_M(X) = \frac{f(X)}{\prod_{i=1}^{s}(1 - X^{k_i})}.$$

□

**Notazione 2.2.6.** Per convenzione, poniamo $\binom{n}{-1} = 0$ per $n \geq 0$ e $\binom{-1}{-1} = 1$.

**Corollario 2.2.7.** *Nelle ipotesi di (2.2.4). Se esistono $x_1, \ldots, x_s \in R_1$ tali che $R = R_0[x_1, \ldots, x_s]$, allora esistono $h_M(X) \in \mathbb{Q}[X]$ e $N \in \mathbb{N}$ tali che*

$$\lambda(M_n) = h_M(n) \qquad \forall n \geq N.$$

*Si definisce $h_M(n)$ come il* ***polinomio di Hilbert di*** *$M$* ***rispetto a*** *$\lambda$. Inoltre, $\deg(h_M(n)) = d - 1$, dove $d$ è l'ordine di $1$ come polo di $P_M(X)$.*

*Dimostrazione.* Per il teorema precedente, e nelle sue notazioni, $k_i = 1$ per ogni $i = 1, \ldots, s$ ed esiste $f(X) \in \mathbb{Z}[X]$ tale che

$$P_M(X) = \sum_{n=0}^{\infty} \lambda(M_n)X^n = \frac{f(X)}{(1 - X)^s} = \frac{g(X)}{(1 - X)^d}, \qquad g(1) \neq 0.$$

In particolare si avrà

$$g(X) = a_0 + a_1 X + \cdots + a_N X^N \qquad \in \mathbb{Z}[X],$$

inoltre osserviamo che

$$\frac{1}{(1 - X)^d} = \sum_{n=0}^{\infty} \binom{d + n - 1}{d - 1} X^n.$$

Sostituendo i due valori nella prima equazione si ottiene

$$\lambda(M_n) = \sum_{k=0}^{N} a_k \binom{d + n - k - 1}{d - 1} \qquad \forall n \geq N,$$

il cui grado è $d-1$. Infatti, osservando

$$\begin{aligned}\binom{d+n-k-1}{d-1} &= \frac{(d+n-k-1)\cdot(d+n-k-2)\cdots(n-k+1)}{(d-1)!} \\ &= \frac{n^{d-1}}{(d-1)!}+p(n), \qquad \deg p(n) = d-2\end{aligned}$$

si ottiene che il termine di grado massimo in $\lambda(M_n)$ sia

$$\sum_{k=0}^{N} \frac{a_k}{(d-1)!} n^{d-1} = \frac{g(1)}{(d-1)!} n^{d-1}.$$

□

## 2.3 Polinomio di Hilbert e di Hilbert-Samuel

**Definizione 2.3.1.** Sia $M$ un $R$-modulo. Una catena finita di sottomoduli

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

si dice **serie di composizione** se è una catena massimale o, equivalentemente, se $M_{i-1}/M_i$ è un modulo **semplice** per ogni $i = 1, \ldots, n$. *(Un $R$-modulo $M$ si dice semplice se gli unici suoi sottomoduli sono* $0$ *e $M$)*

**Definizione 2.3.2.** Sia $M$ un $R$-modulo. Si definisce la **lunghezza** di $M$, denotata $\operatorname{len}_R M$, come il minimo della lunghezza delle sue serie di composizione. Se $M$ non ha serie di composizione, si definisce $\operatorname{len}_R M = \infty$.

**Proposizione 2.3.3.** *Un $R$-modulo $M$ possiede una serie di composizione se e solo se $M$ è un modulo Noetheriano e Artiniano. Inoltre, tutte le serie di composizione hanno la stessa lunghezza.*

*Osservazione* 2.3.4. Siano $R$ un anello Artiniano e $M$ un $R$-modulo finitamente generato. Per (1.1.8) $R$ è Noetheriano. Quindi per (1.1.6) e (1.1.10) $M$ è un modulo Noetheriano e Artiniano. In particolare, vale la proposizione precedente.

**Proposizione 2.3.5.** *Sia $\mathscr{M}$ la classe degli $R$-moduli di lunghezza finita, allora la funzione* $\operatorname{len}_R : \mathscr{M} \to \mathbb{Z}$ *è additiva.*

*Dimostrazione.* Mostriamo che per ogni successione esatta corta di $R$-moduli

$$0 \to M \overset{\alpha}{\hookrightarrow} N \overset{\beta}{\twoheadrightarrow} P \to 0$$

sia verificato
$$\operatorname{len}_R M - \operatorname{len}_R N + \operatorname{len}_R P = 0.$$
Siano $(M_i)_{0\leq i\leq m}$ e $(P_j)_{0\leq j\leq n}$ serie di composizione di, rispettivamente, $M$ e $P$. Mappando la prima per $\alpha$ si ottiene
$$\operatorname{Im}\alpha = \alpha(M_0) \supset \alpha(M_1) \supset \cdots \supset \alpha(M_m) = 0,$$
mentre, considerando la controimmagine della seconda per $\beta$, si ha
$$N = \beta^{-1}(P_0) \supset \beta^{-1}(P_1) \supset \cdots \supset \beta^{-1}(P_n) = \operatorname{Ker}\beta.$$
Per ipotesi di successione esatta $\operatorname{Im}\alpha = \operatorname{Ker}\beta$, dunque la seguente è una serie di composizione di lunghezza $m+n$
$$N = \beta^{-1}(P_0) \supset \cdots \supset \beta^{-1}(P_n) = \alpha(M_0) \supset \cdots \supset \alpha(M_m) = 0.$$
Pertanto $\operatorname{len}_R N = n + m$ e di conseguenza
$$\operatorname{len}_R M - \operatorname{len}_R N + \operatorname{len}_R P = m - (n+m) + n = 0.$$
$\square$

Sotto opportune ipotesi, è possibile definire la funzione di Hilbert rispetto alla lunghezza per i moduli graduati. Ponendo ulteriori restrizioni tale funzione è polinomiale per $n \gg 0$.

**Proposizione 2.3.6.** *Sia $R = \bigoplus_{n=0}^{\infty} R_n$ un anello graduato. Siano $R_0$ un anello Artiniano e $R$ una $R_0$-algebra finitamente generata. Sia $M = \bigoplus_{n=0}^{\infty} M_n$ un $R$-modulo graduato finitamente generato. Allora $M_n$ è un $R_0$-modulo finitamente generato per ogni $n \geq 0$.*

*Dimostrazione.* Per (1.1.8) $R_0$ è Noetheriano e per (2.1.3) lo è anche $R$, pertanto $M$ è un modulo Noetheriano. Sia $N_n = \bigoplus_{m\geq n} M_m$. Poiché $M$ è Noetheriano, allora $N_n$ è finitamente generato su $R$, diciamo da $x_1, \ldots, x_t \in N_n$. Poiché $N_n = M_n \oplus (\bigoplus_{m>n} M_m)$ possiamo scrivere $x_i = y_i + z_i$, dove $y_i \in M_n$ e $z_i \in \bigoplus_{m>n} M_m$.

Mostriamo che $y_1, \ldots, y_t$ generano $M_n$ su $R_0$. Sia $y \in M_n \subseteq N_n$, allora
$$y = a_i x_i + \cdots + a_t x_t,$$
con $a_i \in R$. Possiamo scrivere $a_i = b_i + c_i$, con $b_i \in R_0$ e $c_i \in \bigoplus_{m>0} R_m$. Pertanto
$$y = (b_1 + c_1)(y_1 + z_1) + \cdots (b_t + c_t)(y_t + z_t) = \sum_{i=1}^{t} b_i y_i + \alpha,$$
con $\alpha \in \bigoplus_{m>n} M_m$, e uguagliando i gradi si ha $\alpha = 0$. Così $y = \sum_{i=1}^{t} b_i y_i$.
$\square$

**Proposizione 2.3.7.** *Sia $R = \bigoplus_{n=0}^{\infty} R_n$ un anello graduato. Siano $R_0$ un anello Artiniano e $R$ una $R_0$-algebra finitamente generata. Sia $M = \bigoplus_{n=0}^{\infty} M_n$ un $R$-modulo graduato finitamente generato. Allora $\operatorname{len}_{R_0} M_n$ è finito per ogni $n \geq 0$.*

*Dimostrazione.* Per la proposizione precedente $M_n$ è un $R_0$-modulo finitamente generato. Per (2.3.4) $\operatorname{len}_{R_0} M_n$ è finito poiché $R_0$ è Artiniano. □

**Definizione 2.3.8.** Sia $R = \bigoplus_{n=0}^{\infty} R_n$ un anello graduato. Siano $R_0$ un anello Artiniano e $R$ una $R_0$-algebra finitamente generata. Sia $M = \bigoplus_{n=0}^{\infty} M_n$ è un $R$-modulo graduato finitamente generato. Si definisce la **funzione di Hilbert** come

$$H_M(n) := \operatorname{len}_{R_0}(M_n).$$

**Teorema 2.3.9.** *Sia $R = \bigoplus_{n=0}^{\infty} R_n$ un anello graduato. Siano $R_0$ un anello Artiniano e $R = R_0[x_1, \ldots, x_t]$ con $x_i \in R_1$. Sia $M = \bigoplus_{n=0}^{\infty} M_n$ un $R$-modulo graduato finitamente generato. Allora esistono $h_M(X) \in \mathbb{Q}[X]$ e $N \in \mathbb{N}$ tali che*

$$H_M(n) = h_M(n) \qquad \forall n \geq N$$

*Inoltre,* $\deg h_M(n) \leq t-1$. *Si definisce $h_M(n)$ come il* ***polinomio di Hilbert di*** *$M$.*

*Dimostrazione.* Per (1.1.8) $R_0$ è Noetheriano e per (2.1.3) $R$ è Noetheriano. Per le proposizioni (2.3.6) e (2.3.7) ogni $M_n$ è $R_0$-modulo finitamente generato e $\operatorname{len}_{R_0} M_n$ è finito per ogni $n \geq 0$. Per (2.3.5) $\operatorname{len}_{R_0}$ è additiva sugli $R_0$-moduli di lunghezza finita. Per ipotesi $R = R_0[x_1, \ldots, x_t]$ con $x_i \in R_1$, quindi possiamo applicare il corollario (2.2.7) e, osservando che nella sua notazione $\deg h_M(n) = d - 1 \leq t - 1$, si ha l'asserto. □

### 2.3.1 Polinomio di Hilbert-Samuel

**Definizione 2.3.10.** Una funzione $f\colon \mathbb{N} \to \mathbb{Q}$ si dice **polynomial-like** se esistono $N \in \mathbb{N}$ e $g \in \mathbb{Q}[X]$ tali che $f(n) = g(n)$ per ogni $n \geq N$. Si definisce il **grado** di $f$ come $\deg f := \deg g$.

*Osservazione* 2.3.11. Per il Teorema 2.3.9, la funzione di Hilbert $H_M(n)$ è polynomial-like.

**Definizione 2.3.12.** Sia $(R, \mathfrak{m})$ un anello locale Noetheriano. Un ideale $I \subseteq R$ si dice **ideale di parametri** se esiste $n \in \mathbb{N}$ tale che $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.

*Osservazione* 2.3.13. Un ideale $I$ è di parametri se e solo se $R/I$ è Artiniano.

Ora mostreremo che, per ogni modulo finitamente generato su un anello locale Noetheriano, è possibile definire la funzione di Hilbert sul modulo graduato associato rispetto alla filtrazione $I$-adica, con $I$ ideale di parametri, in modo tale che sia polynomial-like.

*Osservazione* 2.3.14. Siano $(R, \mathfrak{m})$ un anello locale Noetheriano e $I \subseteq R$ un ideale di parametri. Se $M$ è un $R$-modulo finitamente generato, allora $M/IM$ è un $R/I$-modulo finitamente generato, con $R/I$ Artiniano.

Consideriamo l'anello e il modulo graduati associati a $R$ e $M$ rispetto alla filtrazione $I$-adica

$$\operatorname{gr}_I R = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}, \qquad \operatorname{gr}_I M = \bigoplus_{n=0}^{\infty} I^n M/I^{n+1}M.$$

Per ipotesi $I$ è finitamente generato su $R$, allora $I/I^2$ è finitamente generata su $R/I$. Poiché $(I/I^2)^n = I^n/I^{n+1}$ per ogni $n \geq 0$, si ha che $\operatorname{gr}_I R$ è una $R/I$-algebra finitamente generata da $a_1, \ldots, a_t \in I/I^2$. Inoltre $(I^n/I^{n+1})M/IM = I^nM/I^{n+1}M$, quindi $\operatorname{gr}_I M$ è un $\operatorname{gr}_I R$-modulo finitamente generato. Per quanto detto è ben definita la funzione di Hilbert

$$H_{\operatorname{gr}_I M}(n) = \operatorname{len}_{R/I}(I^nM/I^{n+1}M).$$

e per (2.3.9) è polynomial-like di grado $\leq t-1$. Osserviamo che se $M$ è un $R$-modulo e l'ideale $I$ annulla $M$, allora $M$ è un $R/I$-modulo, quindi

$$\operatorname{len}_{R/I}(I^nM/I^{n+1}M) = \operatorname{len}_R(I^nM/I^{n+1}M).$$

Introduciamo ora la funzione di Hilbert-Samuel. Risulterà evidente dalla dimostrazione del teorema della dimensione che questa presenta vantaggi rispetto alla funzione di Hilbert.

**Definizione 2.3.15.** Siano $(R, \mathfrak{m})$ un anello locale Noetheriano, $I \subseteq R$ un ideale di parametri e $M$ un $R$-modulo finitamente generato, si definisce la **funzione di Hilbert-Samuel** come

$$s_{I,M}(n) := \operatorname{len}_R M/I^nM.$$

Dobbiamo ora mostrare che sia ben definita, per farlo utilizzeremo il seguente lemma.

**Lemma 2.3.16.** *Una funzione $f\colon \mathbb{N} \to \mathbb{Q}$ è polynomial-like di grado $r$ se e solo se $F(n) := f(n+1) - f(n)$ è polynomial-like di grado $r-1$.*

**Proposizione 2.3.17.** *Nelle ipotesi e notazioni di (2.3.15):*

1. *$s_{I,M}(n) = \sum_{i=0}^{n-1} \operatorname{len}_R I^nM/I^{n+1}M$ per ogni $n \geq 1$, in particolare è finito.*

2. *$s_{I,M}(n)$ è polynomial-like e $\deg s_{I,M}(n) = \deg H_{\mathrm{gr}_I M}(n) + 1$. Inoltre, nella notazione di (2.3.14) $\deg s_{I,M}(n) \leq t$. Con un piccolo abuso di linguaggio, ci riferiremo a $s_{I,M}$ come al* ***polinomio di Hilbert-Samuel****.*

*Dimostrazione.* Se $n = 0$, allora $s_{I,M}(0) = 0$. Procediamo per induzione su $n$. Se $n = 1$ si ha $s_{I,M}(1) = \operatorname{len}_R M/IM$ per definizione. Supponiamo vero per $n$ e dimostriamo per $n + 1$. Posta la successione esatta corta

$$0 \to I^nM/I^{n+1}M \to M/I^{n+1}M \to M/I^nM \to 0,$$

per addività di $\operatorname{len}_R$ e per ipotesi induttiva si ottiene

$$\begin{aligned}\operatorname{len}_R M/I^{n+1}M &= \operatorname{len}_R I^nM/I^{n+1}M + \operatorname{len}_R M/I^nM \\ &= \operatorname{len}_R I^nM/I^{n+1}M + \sum_{i=0}^{n-1} \operatorname{len}_R I^nM/I^{n+1}M.\end{aligned}$$

Per l'osservazione (2.3.14) sono tutti valori finiti, così è dimostrato *(1.)*. Inoltre

$$s_{I,M}(n+1) - s_{I,M}(n) = H_{\mathrm{gr}_I M}(n).$$

Per il lemma precedente, da $H_{\mathrm{gr}_I M}(n)$ polynomial-like si ottiene $s_{I,M}(n)$ polynomial-like di grado $\deg s_{I,M}(n) = \deg H_{\mathrm{gr}_I M}(n) + 1$. Così è dimostrato anche *(2.)* □

**Proposizione 2.3.18.** *Siano $(R, \mathfrak{m})$ un anello locale Noetheriano e $M$ un $R$-modulo finitamente generato. Siano $I, J \subseteq R$ ideali di parametri, allora*

$$\deg s_{I,M} = \deg s_{J,M}.$$

*Poiché il grado del polinomio di Hilbert-Samuel è indipendente dalla scelta dell'ideale di parametri, verrà denotato con $d(M)$.*

*Dimostrazione.* Sia $I \subseteq R$ un ideale di parametri e sia $r \in \mathbb{N}$ tale che $\mathfrak{m}^r \subseteq I \subseteq \mathfrak{m}$. Per ogni $n \geq 1$ si ha $\mathfrak{m}^{rn} \subseteq I^n \subseteq \mathfrak{m}^n$. Quindi

$$s_{\mathfrak{m},M}(rn) \geq s_{I,M}(n) \geq s_{\mathfrak{m},M}(n).$$

Siano i rispettivi gradi dei polinomi $d_1$, $d_2$ e $d_3$, allora

$$O(n^{d_1}) \geq O(n^{d_2}) \geq O(n^{d_3}).$$

Poiché $d_1 = d_3$, ne consegue $d_1 = d_2 = d_3$. □

**Teorema 2.3.19.** *Siano* $(R, \mathfrak{m})$ *un anello locale Noetheriano e* $I \subseteq R$ *un ideale di parametri. Sia* $0 \to M' \hookrightarrow M \twoheadrightarrow M'' \to 0$ *una successione esatta di* $R$*-moduli finitamente generati. Allora*

$$s_{I,M'}(n) + s_{I,M''}(n) = s_{I,M}(n) + r(n),$$

*dove* $r(n)$ *è una funzione polynomial-like di grado minore di* $d(M)$ *con coefficiente direttore non negativo.*

*Dimostrazione.* Poniamo $M'_n = M' \cap I^n M$, quindi la seguente successione è esatta

$$0 \to M'/M'_n \to M/I^n M \to M''/I'nM'' \to 0.$$

Per addività di $\operatorname{len}_R$ si ottiene

$$s_{I,M}(n) - s_{I,M''}(n) = \operatorname{len}_R M'/M'_n.$$

dunque $\operatorname{len}_R M'/M'_n$ è polynomial-like. Per il lemma di Artin-Rees (2.1.12) la filtrazione $\{ M'_n \}$ è $I$-stabile. Quindi esiste $N \in \mathbb{N}$ tale che $IM'_n = M'_{n+1}$ per $n \geq N$. Dunque per ogni $n \in \mathbb{N}$ si ha $M'_{n+N} = M' \cap I^{n+N} M \supseteq I^{n+N} M'$. Segue

$$I^{n+N} M' \subseteq M'_{n+N} = I^n M'_N \subseteq I^n M'.$$

Ciò comporta

$$s_{I,M'}(n+N) = \operatorname{len}_R M'/I^{n+N} M' \geq \operatorname{len}_R M'/M'_{n+N} \geq \operatorname{len}_R M'/I^n M' = s_{I,M'}(n).$$

Procedendo come nella proposizione precedente, si dimostra che $\operatorname{len}_R M'/M'_n$ e $s_{I,M'}(n)$ abbiano lo stesso grado e lo stesso coefficiente direttore. Di conseguenza $r(n) = s_{I,M'}(n) - \operatorname{len}_R M'/M'_n$ è polynomial-like di grado strettamente minore di $\deg \operatorname{len}_R M'/M'_n \leq s_{I,M}(n)$ e positiva per $n$ abbastanza grande. Ora

$$s_{I,M}(n) - s_{I,M''}(n) = \operatorname{len}_R M'/M'_n = s_{I,M'}(n) - r(n),$$

da cui segue $s_{I,M'}(n) + s_{I,M''}(n) = s_{I,M}(n) + r(n)$. □

**Corollario 2.3.20.** *Siano* $(R, \mathfrak{m})$ *un anello locale Noetheriano,* $M$ *un* $R$*-modulo finitamente generato e* $M' \subseteq M$ *un suo sottomodulo. Allora* $d(M') \leq d(M)$.

*Dimostrazione.* Sia $I \subseteq R$ un ideale di parametri. Posta la successione esatta corta $0 \to M' \hookrightarrow M \twoheadrightarrow M/M' \to 0$, per il teorema precedente

$$s_{I,M'}(n) + s_{I,M/M'}(n) = s_{I,M}(n) + r(n).$$

Poiché $\deg r(n) < d(M)$, deve essere $d(M') \leq d(M)$. □

## 2.4 Teorema di Dimensione

In questa sezione dimostreremo l'uguaglianza tra il grado del polinomio di Hilbert-Samuel e la dimensione di un modulo secondo la definizione di Krull e di Chevalley.

**Definizione 2.4.1.** Sia $M \neq 0$ un $R$-modulo. Si definisce la **dimensione di** $M$ come segue:

$$\dim M := \dim R/\operatorname{Ann} M.$$

Se $M = 0$, si definisce $\dim M := -1$.

*Osservazione* 2.4.2. Se $M = R$, allora $\operatorname{Ann} R = 0$. Pertanto $\dim M$ coincide con la dimensione di Krull di $R$.

*Osservazione* 2.4.3. Siano $R$ un anello Noetheriano e $M$ un $R$-modulo non nullo finitamente generato. Per (1.4.4) esiste $\mathfrak{p} \in \operatorname{Ass} M$. Per (1.4.9) $\mathfrak{p} \supseteq \operatorname{Ann} M$ se e solo se $\mathfrak{p} \in \operatorname{Supp} M$ e per (1.4.10) gli elementi minimali in $\operatorname{Ass} M$ e $\operatorname{Supp} M$ sono gli stessi. Pertanto

$$\dim M = \sup \{ \operatorname{coht} \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp} M \} = \sup \{ \operatorname{coht} \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass} M \}.$$

**Proposizione 2.4.4.** *Siano $R$ un anello Noetheriano e $M$ un $R$-modulo finitamente generato. Sono equivalenti*

1. $\dim M = 0$.
2. $\operatorname{len}_R M$ *è finito.*
3. *Ogni* $\mathfrak{p} \in \operatorname{Ass} M$ *è massimale.*
4. *Ogni* $\mathfrak{p} \in \operatorname{Supp} M$ *è massimale.*

*Osservazione* 2.4.5. Sia $(R, \mathfrak{m})$ un anello locale Noetheriano. Per (1.4.9)

$$\operatorname{Supp} M/\mathfrak{m}M = V(\operatorname{Ann} M/\mathfrak{m}M) = \{ \mathfrak{m} \},$$

quindi per la proposizione precedente $\operatorname{len}_R M/\mathfrak{m}M$ è finito. Per ipotesi $\mathfrak{m}$ è finitamente generato su $R$, quindi esistono $n \in \mathbb{N}$ e $a_1, \dots, a_n \in \mathfrak{m}$ tali che $\operatorname{len}_R M/\mathfrak{m}M$ sia finito.

**Definizione 2.4.6.** Siano $(R, \mathfrak{m})$ un anello locale Noetheriano e $M$ un $R$-modulo. Si definisce la **dimensione di Chevalley** di $M$ come

$$\delta(M) := \min \{ n \in \mathbb{N} \mid \exists a_1, \dots, a_n \in \mathfrak{m} \quad \operatorname{len}_R M/(a_1, \dots, a_n) < \infty \}.$$

Se $M = 0$, si definisce $\delta(M) := -1$.

Prima di enunciare il prossimo lemma ricordiamo che il radicale di Jacobson $J(R)$ di un anello, è, per definizione, l'intersezione di tutti gli ideali massimali di $R$.

**Lemma 2.4.7.** *Siano $M$ un $R$-modulo finitamente generato e $I \subseteq R$ un ideale contenuto nel radicale di Jacobson $J(R)$. Se $IM = M$, allora $M = 0$.*

**Lemma 2.4.8.** *Siano $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$, per $s \geq 2$, ideali di un anello $R$, con $\mathfrak{p}_i$ primo per $i > 2$. Sia $I$ un ideale di $R$ tale che $I \subseteq \bigcup_{i=1}^{s} \mathfrak{p}_i$, allora esiste $1 \leq i \leq s$ tale che $I \subseteq \mathfrak{p}_i$.*

**Teorema 2.4.9 (Teorema della Dimensione).** *Siano $(R, \mathfrak{m})$ un anello locale Noetheriano e $M$ un $R$-modulo finitamente generato, allora*

$$\dim M = d(M) = \delta(M).$$

*Dimostrazione.* La dimostrazione consta di tre parti. Osserviamo prima di tutto che, poiché $d(M)$ è invariante per la scelta dell'ideale di parametri, è possibile considerare $\mathfrak{m}$ come ideale di parametri senza perdere in generalità.

*(1.)* Dimostriamo che $\dim M \leq d(M)$. Osserviamo che ciò implica $\dim M$ finito, poiché lo è $d(M)$. Se $d(M) = -1$, allora esiste $N \in \mathbb{N}$ tale che $s_{\mathfrak{m},M}(n) = \operatorname{len}_R M/\mathfrak{m}^n M = 0$ per ogni $n \geq N$. Per (2.4.7) $M = 0$, così $\dim M = -1$.

Supponiamo ora $d(M) \geq 0$. Per (1.4.5) $\operatorname{Ass} M$ è finito. Per (2.4.3) e (1.5.5) esiste $\mathfrak{p} \in \operatorname{Ass} M$ tale che

$$\dim M = \operatorname{coht} \mathfrak{p} = \dim R/\mathfrak{p}.$$

Per (1.4.3) esiste un morfismo iniettivo $R/\mathfrak{p} \hookrightarrow M$, così per (2.3.20) vale $d(R/\mathfrak{p}) \leq d(M)$. Dimostriamo che $\dim R/\mathfrak{p} \leq d(R/\mathfrak{p})$, che comporta

$$\dim M = \dim R/\mathfrak{p} \leq d(R/\mathfrak{p}) \leq d(M).$$

È sufficiente osservare che per ogni catena di ideali primi $\mathfrak{p} = \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r$ in $R$ la lunghezza è $r \leq d(R/\mathfrak{p})$. Dimostriamolo per induzione su $r$.

Se $r = 0$, allora da $R/\mathfrak{p} \neq 0$ segue $d(R/\mathfrak{p}) \neq -1$ e si ha l'asserto. Supponiamo ora sia vero per $r - 1$ e dimostriamolo per $r > 0$. Sia $a \in \mathfrak{p}_1 \setminus \mathfrak{p}$ e consideriamo gli ideali primi $\mathfrak{q}$ tali che $Ra + \mathfrak{p} \subseteq \mathfrak{q} \subseteq \mathfrak{p}_1$. Per (1.2.8) sappiamo che $Ra + \mathfrak{p} \subseteq \mathfrak{q}$ se e solo se $(R/(Ra + \mathfrak{p}))_{\mathfrak{q}} \neq 0$, quindi scegliamo $\mathfrak{q} \in \operatorname{Supp} R/(Ra + \mathfrak{p})$ minimale, e per (1.4.10) $\mathfrak{q} \in \operatorname{Ass} R/(Ra + \mathfrak{p})$. Per (1.4.3) esiste un morfismo inettivo $R/\mathfrak{q} \hookrightarrow R/(Ra + \mathfrak{p})$, quindi per (2.3.20)

$d(R/\mathfrak{q}) \leq d(R/(Ra + \mathfrak{p})$. A questo punto la catena $\mathfrak{q} \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_r$ ha lunghezza $r-1$ e per ipotesi induttiva

$$r - 1 \leq d(R/\mathfrak{q}) \leq d(R/(Ra + \mathfrak{p})).$$

Posto su $R/\mathfrak{p}$ l'endomorfismo di $R$-moduli $a\colon x \to ax$, la seguente è una successione esatta

$$0 \to R/\mathfrak{p} \xrightarrow{a} R/\mathfrak{p} \to R/(Ra + \mathfrak{p}) \to 0.$$

e per (2.3.19) esiste $r(n)$ polynomial-like di grado minore di $d(R/\mathfrak{p})$ tale che

$$s_{\mathfrak{m},R/\mathfrak{p}}(n) + s_{\mathfrak{m},R/(Ra+\mathfrak{p})}(n) = s_{\mathfrak{m},R/\mathfrak{p}}(n) + r(n).$$

Pertanto $d(R/(Ra + \mathfrak{p})) < d(R/\mathfrak{p})$, da cui segue $r - 1 < d(R/\mathfrak{p})$ e di conseguenza $r \leq d(R/\mathfrak{p})$, ottenendo la disuguaglianza cercata.

*(2.)* Dimostriamo che $d(M) \leq \delta(M)$. Se $\delta(M) = -1$, allora $M = 0$ e $d(M) = -1$. Sia ora $M \neq 0$ e poniamo $r = \delta(M) \leq 0$, quindi abbiamo $a_1, \ldots, a_r \in \mathfrak{m}$ tali che $\operatorname{len}_R M/(a_1, \ldots, a_r)M$ sia finito. Poniamo $I = (a_1, \ldots, a_r)$ e $Q = I + \operatorname{Ann} M$. Osserviamo che per (2.4.7) se $M/IM = 0$, allora $M = 0$, giungendo a una contraddizione.

Ora mostriamo che $\operatorname{Supp} R/Q = \{\, \mathfrak{m} \,\}$. Poiché $M/IM \cong M \otimes_R R/I$, per (1.4.11)

$$\operatorname{Supp} M/IM = \operatorname{Supp} M \otimes_R R/I = \operatorname{Supp} M \cap \operatorname{Supp} R/I.$$

Per (1.4.9) abbiamo $\operatorname{Supp} M = V(\operatorname{Ann} M)$ e $\operatorname{Supp} R/I = V(I)$ e per definizione di $Q$ vale $V(\operatorname{Ann} M) \cap V(I) = V(Q)$, così

$$\operatorname{Supp} M/IM = V(Q) = \operatorname{Supp} R/Q.$$

Per (2.4.4) da $\operatorname{len}_R M/IM$ segue $\operatorname{Supp} M/IM = \{\, \mathfrak{m} \,\}$ ed è dimostrata l'uguaglianza. Di nuovo per (2.4.4) $\operatorname{Ass} R/Q = \{\, \mathfrak{m} \,\}$ e per (1.4.6) $Q$ è ideale di parametri per $R$.

Siano $\bar{R} = R/\operatorname{Ann} M$ e $\bar{Q} = Q/\operatorname{Ann} M$ e consideriamo $M$ come $\bar{R}$-modulo. In particolare $\bar{R}$ è locale e Noetheriano, mentre $\bar{Q}$ è un ideale di parametri per $\bar{R}$ generato dalle classi $\bar{a}_1, \ldots, \bar{a}_r$, dove $\bar{a}_i = a_i + \operatorname{Ann} M$.

Per (2.3.17) $\deg s_{\bar{Q},M}(n) \leq r$ e per il teorema di corrispondenza degli ideali con l'anello quoziente $\operatorname{len}_{\bar{R}} M/\bar{Q}^n M = \operatorname{len}_R M/Q^n M$, pertanto $s_{\bar{Q},M}(n) = s_{Q,M}(n)$. Infine si ha

$$d(M) = \deg s_{Q,M}(n) = \deg s_{\bar{Q},M}(n) \leq r = \delta(M).$$

*(3.)* Dimostriamo che $\delta(M) \leq \dim M$. Se $\dim M = -1$, allora $M = 0$ e $\delta(M) = -1$. Dunque, sia $M \neq 0$ e procediamo per induzione su $r = \dim M$.

Se $\dim M = 0$, per (2.4.4) $\operatorname{len}_R M$ è finito, quindi il numero minimo di $a_i \in \mathfrak{m}$ tali che $\operatorname{len}_R M/(a_1, \ldots, a_r)M < \infty$ è $\delta(M) = 0$.

Sia ora $\dim M > 0$, che per *(1.)* è finito. Supponiamo la disuguaglianza sia vera per dimensioni $< \dim M$. Siano $\mathfrak{p}_1, \ldots, \mathfrak{p}_t \in \operatorname{Ass} M$ tutti e soli i primi associati tali che $\operatorname{coht} \mathfrak{p}_i = \dim M$. Poiché $\dim M > 0$ devono essere $\mathfrak{p}_i \subset \mathfrak{m}$ per ogni $i = 1, \ldots, t$, così per (2.4.8) $\mathfrak{m} \nsubseteq \cup_{i=1}^t \mathfrak{p}_i$. Possiamo ora scegliere $a \in \mathfrak{m}$ che non appartenga a $\cup_{i=1}^t \mathfrak{p}_i$, quindi poniamo $N = M/aM$ e mostriamo che

$$\operatorname{Supp} N \subseteq \operatorname{Supp} M \setminus \{\, \mathfrak{p}_1, \ldots, \mathfrak{p}_t \,\}\,.$$

Se $N_\mathfrak{p} \neq 0$ deve essere $M_\mathfrak{p} \neq 0$, quindi $\operatorname{Supp} N \subseteq \operatorname{Supp} M$. Poiché $a \notin \mathfrak{p}_i$ e $aM = 0$ in $N$, la localizzazione è $N_{\mathfrak{p}_i} = 0$, così $\mathfrak{p}_i \notin \operatorname{Supp} N$. Per ipotesi $\mathfrak{p}_i$ sono gli ideali di massima coaltezza in $\operatorname{Supp} M$, pertanto $\dim N < \dim M$. Sia $r = \delta(N)$, poniamo $a_1, \ldots, a_r \in \mathfrak{m}$ tali che $\operatorname{len}_R N/(a_1, \ldots, a_r)N$ sia finito. Per il primo teorema di isormofismo

$$M/(a, a_1, \ldots, a_r)M \cong N/(a_1, \ldots, a_r)N,$$

dunque anche $\operatorname{len}_R M/(a, a_1, \ldots, a_r)M$ è finito e di conseguenza $\delta(M) \leq r+1$. Per ipotesi induttiva $\delta(N) \leq \dim N$, così

$$\delta(M) \leq r + 1 = \delta(N) + 1 \leq \dim N + 1 \leq \dim M.$$

□

# Capitolo 3

# Dimensione di Anelli Affini

In questo capitolo tratteremo due definizioni di dimensione equivalenti per gli anelli affini, introducendo il concetto di varietà algebrica affine e mostrando che ad ogni anello affine ne è associata una. Quindi mostrermo l'equivalenza tra la dimensione geometricamente intuitiva definita su una varietà algebrica affine e il grado del polinomio di Hilbert-Samuel dell'anello affine associato localizzato in punto.

D'ora in poi con $k$ verrà indicato un campo algebricamente chiuso.

## 3.1 Lemma di Normalizzazione di Noether

**Definizione 3.1.1.** Un dominio di integrità $A$ si dice **$k$-algebra affine** se è un'algebra finitamente generata su un campo $k$. In simboli

$$\exists x_1, \dots, x_n \in A \qquad A = k[x_1, \dots, x_n].$$

Se non è richiesto specificare il campo $k$, ci riferiremo ad $A$ come **anello affine**.

*Osservazione* 3.1.2. Sia $A = k[x_1, \dots, x_n]$ un anello affine, allora esiste $\mathfrak{p} \subset k[Y_1, \dots, Y_n]$ ideale primo nell'anello dei polinomi in $n$ indeterminate tale che $A \cong k[Y_1, \dots, Y_n]/\mathfrak{p}$. Definito il morfismo di valutazione

$$\begin{array}{rccc} \varphi\colon & k[Y_1, \dots, Y_n] & \longrightarrow & k[x_1, \dots, x_n] \\ & p(Y_1, \dots, Y_n) & \longmapsto & p(x_1, \dots, x_n) \end{array}$$

si ha $A \cong k[Y_1, \dots, Y_n]/\ker\varphi$, in particolare $\ker\varphi$ è un ideale primo poiché $A$ è un dominio di integrità.

**Notazione 3.1.3.** Siano $Y_1, \dots, Y_n$ indeterminate e $\alpha = (a_1, \dots, a_n)$, con $a_i$ intero. Definiamo $Y^\alpha := Y_1^{a_1} \cdots Y_n^{a_n}$.

**Lemma 3.1.4.** *Sia $\mathscr{Y} = \{ Y^{\alpha_i} \}_{i \in I}$ una famiglia finita di monomi in $Y_1, \dots, Y_n$ indeterminate. Esistono interi positivi $r_1, \dots, r_{n-1}, r_n = 1$ tali che la funzione*

$$\begin{array}{rccc} \rho\colon & \mathscr{Y} & \longrightarrow & \mathbb{N} \\ & Y^\alpha & \longmapsto & \sum_{k=1}^n r_k a_k \end{array}$$

*sia iniettiva. Ovvero, sia tale che*

$$\alpha_i \neq \alpha_j \quad \Longrightarrow \quad \sum_{k=1}^n r_k a_{ik} \neq \sum_{k=1}^n r_k a_{jk}.$$

*Dimostrazione.* Dimostriamo l'asserto per induzione su $n$. Per $n = 1$ ogni monomio in $\mathscr{Y}$ è della forma $Y^\alpha = Y_1^{a_1}$, quindi per $r_1 = 1$ è verificato.

Supponiamo vero l'enunciato per $n-1$ e dimostriamolo per $n > 0$. È possibile scrivere ogni monomio come $Y^\alpha = Y_1^{a_1} Y^{\alpha'}$, dove $\alpha' = (0, a_2, \dots, a_n)$. Otteniamo così una famiglia finita $\mathscr{Y}' = \{ Y^{\alpha'_j} \}_{j \in J}$ di monomi nelle $n-1$ indeterminate $Y_2, \dots, Y_n$. Per ipotesi induttiva esistono $r_2, \dots, r_{n-1}, r_n = 1$ tali che $\rho'\colon \mathscr{Y}' \to \mathbb{N}$ sia iniettiva. Scegliamo un intero

$$r_1 > \max_{Y^{\alpha'} \in \mathscr{Y}'} \rho'(Y^{\alpha'}).$$

Siano $\alpha_i \neq \alpha_j$ in $\mathscr{Y}$, per fissare le idee sia $a_{i1} \geq a_{j1}$. Si ha

$$\sum_{k=1}^n r_k a_{ik} = \sum_{k=1}^n r_k a_{jk} \quad \Longleftrightarrow \quad r_1(a_{i1} - a_{j1}) + \rho'(Y^{\alpha'_i}) - \rho'(Y^{\alpha'_j}) = 0.$$

Se $a_{i1} = a_{j1}$, allora $\rho(Y^{\alpha_i}) - \rho(Y^{\alpha_j}) = \rho'(Y^{\alpha'_i}) - \rho'(Y^{\alpha'_j}) \neq 0$. Altrimenti, se $a_{i1} \neq a_{j1}$, si ha $a_{i1} - a_{j1} \geq 1$. Per definizione di $r_1$

$$r_1(a_{i1} - a_{j1}) > \rho'(Y^{\alpha'_j})(a_{i1} - a_{j1}) \geq \rho'(Y^{\alpha'_j}).$$

Applicando la disuguaglianza nella prima equazione si ottiene

$$\begin{aligned} r_1(a_{i1} - a_{j1}) + \rho'(Y^{\alpha'_i}) - \rho'(Y^{\alpha'_j}) &> \rho'(Y^{\alpha'_j}) + \rho'(Y^{\alpha'_i}) - \rho'(Y^{\alpha'_j}) \\ &= \rho'(Y^{\alpha'_i}) \geq 0. \end{aligned}$$

□

**Teorema 3.1.5 (Lemma di Normalizzazione di Noether).** *Siano $A$ un anello affine e $I_1 \subset \cdots \subset I_r$ una catena di ideali propri di $A$ non nulli. Esistono $n \in \mathbb{N}$ ed elementi $x_1, \dots, x_n \in A$ algebricamente indipendenti su $k$ tali che siano soddisfatte le seguenti condizioni:*

1. *$A$ è intero su $B = k[x_1, \dots, x_n]$.*

2. *Per ogni $i = 1, \dots, r$ esiste $h_i$ intero positivo tale che $I_i \cap B$ sia generato da $x_1, \dots, x_{h_i}$ come ideale di $B$.*

*Dimostrazione.* La dimostrazione procede in quattro punti.

*(i)* È sufficiente studiare il caso in cui $A = k[Y_1, \dots, Y_m]$ sia un anello di polinomi. Sia $A' = k[x_1, \dots, x_m]$ un anello affine, per l'osservazione (3.1.2) $A \cong A'/I'_0$, dove $A' = k[Y_1, \dots, Y_m]$ e $I'_0$ è un ideale primo. Nella stessa notazione, posto $I'_i = \varphi^{-1}(I_i)$, otteniamo in $A'$ la catena di ideali propri

$$I'_0 \subset I'_1 \subset \cdots \subset I'_r.$$

Supponiamo che valga il teorema per $A'$, allora esistono $x'_0, \dots, x'_m \in A'$ algebricamente indipendenti su $k$ tali che $A'$ sia intero su $B' = k[x'_0, \dots, x'_m]$ e per ogni $i = 0, \dots, r$ esiste $h_i$ intero positivo tale, che come ideale di $B'$,

$$I'_i \cap B' = (x'_1, \dots, x'_{h_i}).$$

Poiché gli ideali formano una catena per l'inclusione, per $0 \leq i \leq j$ si ha $h_0 \leq h_i \leq h_j$. Posto $B = \varphi(B') = k[\varphi(x'_1), \dots, \varphi(x'_m)]$, poiché $\varphi(I'_0) = 0$ deve essere $\varphi(x'_1) = \cdots = \varphi(x'_{h_0}) = 0$, quindi

$$B = k[x_{h_0+1}, \dots, x_m], \qquad x_i = \varphi(x'_i).$$

Poiché $A'$ è intero su $B'$, dalla suriettività di $\varphi$ si ha $A$ intero su $B$. Inoltre

$$I_i \cap B = \varphi(I'_i \cap B') = \varphi((x'_1, \dots, x'_{h_i})) = (x_{h_0+1}, \dots, x_{h_i}).$$

Ora dimostriamo il teorema per $A$ anello di polinomi. Procediamo per induzione su $r$.

*(ii)* Sia $r = 1$. Consideriamo ora il caso in cui $I_1 = (x_1) = x_1 A$ sia un ideale principale, con $x_1 \notin k$ poiché ideale proprio. Per assunzione di $A = k[Y_1, \dots, Y_m]$ come anello di polinomi, $x_1 = g(Y_1, \dots, Y_m)$ è polinomio non costante a coefficienti in $k$. Dimostriamo che esistono interi positivi $r_i$, per $i = 2, \dots, m$, tali che $A$ sia intero su $B = k[x_1, \dots, x_m]$, dove

$$x_i = Y_i - Y_1^{r_i}, \qquad i = 2, \dots, m.$$

Poiché gli $x_i$ sono interi su $B$, se mostriamo che $Y_1$ è intero su $B$, allora ogni $Y_i$ è intero su $B$, così $A$ è intero su $B$.

Si osservi che da $x_1 = g(Y_1, \dots, Y_m)$ si ottiene la relazione

$$g(Y_1, x_2 + Y_1^{r_2}, \dots, x_m + Y_1^{r_m}) - x_1 = 0.$$

Scrivendo il polinomio $g$ (nella notazione di (3.1.4)) come somma finita di monomi $\sum c_\alpha Y^\alpha$, con $\alpha = (a_1, \dots, a_n)$, $c_\alpha \in k$, $c_\alpha \neq 0$, la relazione diventa

$$\sum_{j \in J} c_{\alpha_j} Y_1^{a_{j1}} (x_2 + Y_1)^{a_{j2}} \cdots (x_m + Y_1^{r_m})^{a_{jm}} - x_1 = 0, \qquad |J| < \infty.$$

Definiamo $f(\alpha) = a_1 + a_2 r_2 + \cdots + a_m r_m$ e scegliamo gli $r_i$ tali che gli $f(\alpha_j)$ siano a due a due distinti. Tali $r_i$ esistono per il lemma (3.1.4). Esiste ed è unico $\beta \in \{ \alpha_j \}_{j \in J}$ che massimizzi $f$ rispetto agli $\alpha_j$. Scrivendo la relazione come polinomio in $Y_1$, diventa

$$c_\beta Y_1^{f(\beta)} + \sum_{j < f(\beta)} p_j(x_1, \dots, x_m) Y_1^j = 0,$$

quindi, dividendo per $c_\beta$, segue che $Y_1$ sia intero su $B$. Come abbiamo osservato sopra, $A = k[Y_1, \dots, Y_m]$ è intero su $B = k[x_1, \dots, x_m]$. Così è dimostrato il punto (1) dell'enunciato per $I_1$ ideale principale.

Poiché $B \subseteq A$ è una estensione intera di domini di integrità, si ha $\operatorname{Frac} B \subseteq \operatorname{Frac} A$ estensione algebrica di campi. Poiché $x_1, \dots, x_m \notin k$ e $k$ è algebricamente chiuso, sono trascendenti su $k$. Per $\operatorname{tr\,deg}_k \operatorname{Frac} A = m$ e (1.6.16) ne consegue che $x_1, \dots, x_m$ sono algebricamente indipendenti su $k$. Inoltre $B$ è isomorfo a un anello di polinomi in $n$ indeterminate.

Mostriamo che $I_1 \cap B = (x_1) = x_1 B$. Da $I_1 = x_1 A$ segue $x_1 B \subseteq x_1 A = I_1$, quindi $x_1 B \subseteq I_1 \cap B$. Sia ora $t \in I_1 \cap B$, allora $t = x_1 u$ con $u \in A$, pertanto dividendo per $x_1$ si ottiene $u \in A \cap \operatorname{Frac} B$. Poiché $B$ è isomorfo a un anello di polinomi, allora è un dominio a fattorizzazione unica e per (1.3.8) è integralmente chiuso. Poiché $A$ è intero su $B$, si ha dunque $u \in B$. Così $x_1 A \cap B = x_1 B$ ed è dimostrato il punto (2) per $I_1$ ideale principale.

*(iii)* Sia $r = 1$, mostriamo il caso per $I_1$ ideale proprio qualsiasi. Procediamo per induzione su $m$. Se $m = 0$ non c'è niente da dimostrare. Per $m = 1$ si ha che $A = k[x]$ è un dominio a ideali principali e ci si riconduce al punto *(ii)*. Sia vero l'enunciato per $m - 1$ e dimostriamolo per $m > 0$.

Sia $x_1 \in I_1$ non nullo, allora $x_1 \notin k$ in quanto $I_1$ ideale proprio. Per il punto *(ii)* esistono $t_2, \dots, t_m \in A$ tali che $x_1, t_2, \dots, t_m$ siano algebricamente indipendenti su $k$, $A$ sia intero su $C = k[x_1, t_2, \dots, t_m]$ e $x_1 A \cap C = x_1 C$.

Consideriamo l'anello affine $k[t_2, \dots, t_m]$ e il suo ideale proprio $I_1 \cap k[t_2, \dots, t_m]$, per ipotesi induttiva esistono $x_2, \dots, x_m \in k[t_2, \dots, t_m]$ algebricamente indipendenti su $k$ tali che $k[t_2, \dots, t_m]$ sia intero su $k[x_2, \dots, x_m]$ ed esiste un intero $2 \leq h \leq m$ tale che

$$(I_1 \cap k[t_2, \ldots, t_m]) \cap k[x_2, \ldots, x_m] = I_1 \cap k[x_2, \ldots, x_m] = (x_2, \ldots, x_h).$$

Poniamo $B = k[x_1, x_2, \ldots, x_m]$. Poiché $k[t_2, \ldots, t_m]$ è intero su $k[x_2, \ldots, x_m]$, allora $C$ è intero su $B$. Da $A$ intero su $C$ ne consegue che $A$ sia intero su $B$. Così è dimostrato (1). Per l'indipendenza algebrica di $x_1, \ldots, x_m$ su $k$ si procede come in *(ii)*. Ora, poiché $I_1 \supseteq x_1 A \supseteq x_1 B$,

$$I_1 \cap B = x_1 B + I_1 \cap k[x_2, \ldots, x_m] = x_1 B + (x_2, \ldots, x_h) = (x_1, \ldots, x_h).$$

In questo modo è dimostrato anche (2).

*(iv)* Ora supponiamo l'enunciato sia vero per $r - 1$ e dimostriamolo per $r > 0$. Ricordiamo che $A = k[Y_1, \ldots, Y_m]$ e la catena è $I_1 \subset \cdots \subset I_r$. Consideriamo la sottocatena $I_1 \subset \cdots \subset I_{r-1}$, per ipotesi induttiva esistono $t_1, \ldots, t_m \in A$ algebricamente indipendenti su $k$ tali che $A$ sia intero su $k[t_1, \ldots, t_m]$ e per ogni $i = 1, \ldots, r-1$ esiste un intero positivo $h_i$ tale che, come ideale di $k[t_1, \ldots, t_m]$,

$$I_i \cap k[t_1, \ldots, t_m] = (t_1, \ldots, t_{h_i}).$$

Sia $s = h_{r-1}$. Consideriamo l'anello affine $k[t_{s+1}, \ldots, t_m]$ e il suo ideale proprio $I_r \cap k[t_{s+1}, \ldots, t_m]$. Per *(iii)* esistono $x_{s+1}, \ldots, x_m \in k[t_{s+1}, \ldots, t_m]$ algebricamente indipendenti su $k$ tali che $k[t_{s+1}, \ldots, t_m]$ sia intero su $k[x_{s+1}, \ldots, x_m]$ ed esiste un intero positivo $s + 1 \leq h_r \leq m$ tale che, come ideale di $k[x_{s+1}, \ldots, x_m]$,

$$I_r \cap k[x_{s+1}, \ldots, x_m] = (x_{s+1}, \ldots, x_{h_r}).$$

Si ottiene che $k[t_1, \ldots, t_m]$ sia intero su $B = k[t_1, \ldots, t_s, x_{s+1}, \ldots, x_m]$, quindi $A$ è intero su $B$. Così è dimostrato (1). Poniamo $x_i = t_i$ per $i = 1, \ldots, s$. Procedendo come in *(ii)* si dimostra che $x_1, \ldots, x_m$ siano algebricamente indipendenti su $k$.

Ora mostriamo che vale (2). Sia $1 \leq i \leq r - 1$, allora

$$I_i \cap C = (t_1, \ldots, t_{h_i})C = (x_1, \ldots, x_{h_i})C \quad \Longrightarrow \quad x_1, \ldots, x_{h_i} \in I_i,$$

pertanto $I_i \cap B \supseteq (x_1, \ldots, x_{h_i})B$. Sia ora $x \in (I_i \cap B)$, è possibile scriverlo in modo unico come

$$x = \sum c_{a_1 \ldots a_{h_i}} \, p_{a_1 \ldots a_{h_i}}(x_{h_i+1}, \ldots, x_m) \, x_1^{a_1} \cdots x_{h_i}^{a_{h_i}}.$$

Sia $p = p_{0\dots 0}$, poiché $I_i \cap B \supseteq (x_1, \dots, x_{h_i})B$ ed è un gruppo abeliano, deve essere $p \in I_i$. Così $p \in I_i \cap k[x_{h_i+1}, \dots, x_m] = 0$, infatti

$$\begin{aligned} I_i \cap k[x_{h_i+1}, \dots, x_m] &\subseteq I_i \cap k[t_{h_i+1}, \dots, t_m] \\ &= I_i \cap C \cap k[t_{h_i+1}, \dots, t_m] \\ &= (t_1, \dots, t_{h_i})C \cap k[t_{h_i+1}, \dots, t_m] = 0. \end{aligned}$$

Deve quindi essere $I_i \cap B = (x_1, \dots, x_{h_i})B$. Sia ora $i = r$. Per ipotesi $x_1, \dots, x_{h_{r-1}} \in I_{r-1} \subseteq I_r$ e $x_{h_{r-1}+1}, \dots, x_{h_r} \in I_r$, quindi $I_r \cap B \supseteq (x_1, \dots, x_r)B$. Per ipotesi $I_r \cap k[x_{h_r+1}, \dots, x_m] = 0$, quindi procedendo come per $i < r$ si ottiene $I_r \cap B = (x_1, \dots, x_r)B$ e si ha l'asserto. □

**Corollario 3.1.6.** *Sia $A$ un anello affine. Se $A$ è un campo, allora $k \subseteq A$ è un'estensione di campi finita.*

*Dimostrazione.* Per ipotesi $A = k[x_1, \dots, x_n]$ e per il lemma di normalizzazione di Noether esistono $t_1, \dots, t_r \in A$ algebricamente indipendenti su $k$ tali che $A$ sia intero su $B = k[t_1, \dots, t_r]$. Sia $b \in B$, allora $b^{-1} \in A$ e per ipotesi esistono $\alpha_0, \dots, \alpha_{n-1} \in B$ tali che

$$(b^{-1})^n + (b^{-1})^{n-1}\alpha_{n-1} + \cdots + b^{-1}\alpha_1 + \alpha_0 = 0,$$

moltiplicando per $b^{n-1}$ otteniamo

$$b^{-1} = -(\alpha_{n-1} + b\alpha_{n-2} + \cdots + b^{n-2}\alpha_1 + b^{n-1}\alpha_0) \in B.$$

Quindi $B$ è un campo e $t_i^{-1} = p(t_1, \dots, t_r)$ per ogni $i = 1, \dots, r$, così

$$t_i p(t_1, \dots, t_r) - 1 = t_i t_i^{-1} - 1 = 0,$$

contraddicendo l'indipendenza algebrica di $t_1, \dots, t_r$ su $k$. Pertanto $r = 0$. Così $k \subseteq A$ è estensione algebrica e, per l'ipotesi di $A$ anello affine, è finita. □

**Teorema 3.1.7.** *Siano $A$ un anello affine e $\mathfrak{p} \subseteq A$ un ideale primo, allora*

$$\dim A = \operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p}.$$

*Dimostrazione.* Per il teorema di normalizzazione di Noether (3.1.5) esistono $x_1, \dots, x_n \in A$ algebricamente indipendenti su $k$ tali che $A$ sia intero su $B = k[x_1, \dots, x_n]$ ed esiste $1 \leq h \leq n$ tale che $\mathfrak{p} \cap B = (y_1, \dots, y_h)$ come ideale di $B$. Osserviamo che $B/(\mathfrak{p} \cap B) \cong k[x_{h+1}, \dots, x_n]$ e per (1.5.7) si ottiene $\operatorname{coht} \mathfrak{p} \cap B = \dim B/(\mathfrak{p} \cap B) = n - h$. Per (1.5.9) $\operatorname{coht} \mathfrak{p} = \operatorname{coht} \mathfrak{p} \cap B$, quindi $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} = h + (n - h) = n = \dim A$. □

**Teorema 3.1.8.** *Sia $A$ un anello affine, allora*

$$\dim A = \operatorname{tr\,deg}_k \operatorname{Frac} A.$$

*Dimostrazione.* Per il lemma di normalizzazione di Noether (3.1.5) esistono $x_1, \ldots, x_n \in A$ algebricamente indipendenti su $k$ tali che $A$ sia intero su $k[x_1, \ldots, x_n]$. Per (1.5.8) $\dim A = \dim k[x_1, \ldots, x_n]$ e per (1.5.7)

$$\dim k[x_1, \ldots, x_n] = n + \dim k = n,$$

quindi $\dim A = n$. Sia $F = \operatorname{Frac} k[x_1, \ldots, x_n]$, da $k[x_1, \ldots, x_n] \subseteq A$ estensione intera di anelli, segue $F \subseteq \operatorname{Frac} A$ estensione algebrica di campi. Per (1.6.16) $\operatorname{tr\,deg}_k \operatorname{Frac} A = \operatorname{tr\,deg}_k F = n$. Se ne deduce che $\dim A = n = \operatorname{tr\,deg}_k \operatorname{Frac} A$. □

## 3.2 Varietà Algebriche Affini

In questa sezione presenteremo la definizione di *varietà algebrica affine* su un campo $k$ algebricamente chiuso. Quindi mostreremo che ad ogni anello affine è associata una varietà algebrica affine.

**Definizione 3.2.1.** Sia $S \subseteq k[X_1, \ldots, X_n]$ un sottoinsieme dell'anello dei polinomi in $n$ indeterminate su $k$. Si definisce **insieme algebrico affine** di $k^n$ un sottoinsieme della forma

$$Z(S) = \{ (a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \quad \forall f \in S \}.$$

*Osservazione* 3.2.2. Sia $I$ l'ideale generato da $S$, allora $Z(I) = Z(S)$. Quindi gli insiemi algebrici affini di $k^n$ sono tutti della forma $Z(I)$, con $I$ ideale di $k[X_1, \ldots, X_n]$.

*Osservazione* 3.2.3. Per il teorema della base di Hilbert, ogni ideale $I \subseteq k[X_1, \ldots, X_n]$ è finitamente generato.

**Proposizione 3.2.4.** *Siano $I, J \subseteq k[X_1, \ldots, X_n]$ ideali e $\{ I_a \}_{a \in \Lambda}$ una famiglia di ideali di $k[X_1, \ldots, X_n]$.*

1. *Se $I \subseteq J$, allora $Z(I) \supseteq Z(J)$.*
2. *$Z(0) = k^n$ e $Z(k[x_1, \ldots, x_n]) = \emptyset$.*
3. *$Z(IJ) = Z(I \cap J) = Z(I) \cup Z(J)$.*
4. *$Z(\sum_{a \in \Lambda} I_a) = \bigcap_{a \in \Lambda} Z(I_a)$.*

*Dimostrazione.* *(1.)* Ogni $p \in Z(J)$ annulla ogni $f \in J \supseteq I$. Dunque $p \in Z(I)$.

*(2.)* Per ogni $p \in k^n$ si ha $0(p) = 0$ e $1(p) = 1 \neq 0$. Quindi esiste $f \in k[x_1, \dots, x_n]$ tale che $f(p) \neq 0$ per ogni $p \in k^n$.

*(3.)* Per *(1)*, da $IJ \subseteq I \cap J \subseteq I, J$ segue $Z(IJ) \supseteq Z(I \cap J) \supseteq Z(I) \cup Z(J)$. Sia $p \notin Z(I) \cup Z(J)$, dunque esistono $f \in I$ e $g \in J$ tali che $f(p), g(p) \neq 0$. Così $(fg)(p) \neq 0$ e $fg \in IJ$. Quindi $p \notin Z(IJ)$.

*(4.)* $I_a \subseteq \sum_{a \in \Lambda} I_a$ per ogni $a \in \Lambda$, quindi $Z(\sum_{a \in \Lambda} I_a) \subseteq \bigcap_{a \in \Lambda} Z(I_a)$ per *(1)*. Sia $p \in \bigcap_{a \in \Lambda} Z(I_a)$, per definizione ogni $f \in \sum_{a \in \Lambda} I_a$ è somma finita di elementi in $I_a$, quindi $f(p) = 0$ e si ha l'altra inclusione.

□

*Osservazione* 3.2.5. Dai punti *(2.)*, *(3.)* e *(4.)* segue che gli insiemi algebrici affini di $k^n$ verificano gli assiomi per la famiglia dei chiusi di una topologia su $k^n$.

**Definizione 3.2.6.** Definiamo la **topologia di Zariski** su $k^n$ come la topologia i cui chiusi sono gli insiemi algebrici affini di $k^n$.

La topologia di Zariski è indotta da $k^n$ su ogni suo insieme algebrico affine $X \subseteq k^n$.

**Definizione 3.2.7.** Sia $X \subseteq k^n$ un insieme algebrico affine, definiamo in $k[X_1, \dots, X_n]$ l'ideale

$$I(X) = \{ f \in k[X_1, \dots, X_n] \mid f(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in X \}.$$

Si definisce **anello delle coordinate di** $X$ l'anello quoziente

$$A(X) = k[X_1, \dots, X_n]/I(X).$$

Se $I(X)$ è un ideale primo, $X$ si dice **varietà algebrica affine**.

*Osservazione* 3.2.8. L'anello delle coordinate di una varietà algebrica affine è un anello affine.

**Definizione 3.2.9.** Siano $R$ un anello e $I \subseteq R$ un ideale, si dice **radicale di** $I$ l'ideale

$$\sqrt{I} := \{ x \in R \mid \exists n \in \mathbb{N} \quad x^n \in I \}.$$

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

*Osservazione* 3.2.10. Per ogni insieme algebrico affine $X \subseteq k^n$ l'ideale $I(X)$ è radicale. Sia $f^n \in I(X)$ per qualche $n \in \mathbb{N}$. Per ogni $p \in X$ si ha $(f^n)(p) = f(p)^n = 0$, così $f(p) = 0$ e $f \in I(X)$.

**Proposizione 3.2.11.** *Siano $R$ un anello e $I \subseteq R$ un ideale, allora $\sqrt{I}$ è l'intersezione di tutti gli ideali primi di $R$ contenenti $I$.*

**Teorema 3.2.12 (Nullstellensatz).** *Sia $I \subseteq A = k[X_1, \ldots, X_n]$ un ideale, allora $I(Z(I)) = \sqrt{I}$. In particolare esiste una corrispondenza biunivoca*

$$\begin{array}{ccc} \{\, I \subseteq A \text{ ideale radicale} \,\} & \longleftrightarrow & \{\, X \subseteq k^n \text{ insieme algebrico affine} \,\} \\ I & \longmapsto & Z(I) \\ I(X) & \longleftarrow\!\shortmid & X \end{array}$$

*Dimostrazione.* Sia $f \in \sqrt{I}$, allora $f^n \in I$ per qualche $n \in \mathbb{N}$. Per ogni $p \in Z(I)$ si ha $(f^n)(p) = f^n(p) = 0$, pertanto $f(p) = 0$. Segue $f \in I(Z(I))$ e l'inclusione $\sqrt{I} \subseteq I(Z(I))$.

Ora sia $f \notin \sqrt{I}$, allora esiste $\mathfrak{p} \subseteq A$ ideale primo contenente $I$ tale che $f \notin \mathfrak{p}$. Dunque $A/\mathfrak{p} = k[\bar{X}_1, \cdots, \bar{X}_n]$, dove $\bar{X}_i = X_i + \mathfrak{p}$. Posto $\bar{f} = f + \mathfrak{p} \in A/\mathfrak{p}$, consideriamo la localizzazione di $A/\mathfrak{p}$ in $\{\, 1/\bar{f}^n \,\}_{n \in \mathbb{N}}$

$$B = (A/\mathfrak{p})[1/\bar{f}] = k[(\bar{X}_1/1), \ldots, (\bar{X}_n/1), (1/\bar{f})].$$

Sia $\mathfrak{m}$ un ideale massimale di $B$, allora $k \subseteq B/\mathfrak{m}$ è un'estensione di campi e $B/\mathfrak{m}$ è un anello affine. Per (3.1.6) questa estensione è algebrica, e dalla chiusura algebrica di $k$ segue $k \cong B/\mathfrak{m}$. La composizione dei morfismi $A \twoheadrightarrow A/\mathfrak{p} \hookrightarrow B \twoheadrightarrow B/\mathfrak{m} \cong k$ mappa ogni $X_i \mapsto a_i \in k$, quindi ogni $p \in A \mapsto p(a_1, \ldots, a_n)$. Allora $I \mapsto 0$ e $f \mapsto \alpha \neq 0$, ottenendo infine $(a_1, \ldots, a_n) \in Z(I)$ e $f \notin I(Z(I))$. Così $\sqrt{I} = I(Z(I))$.

Mostriamo che le mappe $I \mapsto Z(I)$ e $X \mapsto I(X)$ sono una l'inversa dell'altra. Per quanto appena visto $I(Z(I)) = \sqrt{I} = I$. Sia ora $X = Z(J)$, con $J$ ideale di $A$, dunque $J \subseteq I(X)$. Allora $X \subseteq Z(I(X)) \subseteq Z(J) = X$. □

*Osservazione* 3.2.13. Il Nullstellensatz stabilisce una relazione biunivoca tra gli ideali primi di $k[X_1, \ldots, X_n]$ e le varietà algebriche affini. Quindi se $A$ è un anello affine, per (3.1.2) è della forma $A \cong k[X_1, \ldots, X_n]/\mathfrak{p}$, con $\mathfrak{p}$ ideale primo di $k[X_1, \ldots, X_n]$. Per il Nullstellensatz $\mathfrak{p}$ corrisponde a una varietà algebrica affine $Z(\mathfrak{p})$ in $k^n$. Quindi è possibile associare ad ogni anello affine una varietà algebrica affine. Segue dalla teoria della decomposizione primaria che ogni ideale radicale $I$ è intersezione dei suoi primi minimali associati. Le varietà algebriche affini corrispondenti a questi primi minimali sono contenuti in $Z(I)$ e si dicono le sue componenti irriducibili. Quindi ogni insieme algebrico affine è l'unione delle sue componenti irriducibili.

Ora ci accingiamo a definire le mappe che ci interessa considerare come morfismi tra varietà algebriche affini, con un approccio locale e non meramente globale.

**Definizione 3.2.14.** Sia $X \subseteq k^n$ una varietà algebrica affine e $U \subseteq X$ un aperto. Una funzione $f\colon U \to k$ si dice **regolare** se per ogni $p \in U$ esistono $V \subseteq U$ intorno di $p$ e $g, h \in A(X)$, con $h \neq 0$ su tutto $V$, tali che

$$f|_V = \left.\frac{g}{h}\right|_V .$$

Denotiamo con $\mathcal{O}_X(U)$ l'insieme delle funzioni regolari su $U$.

**Definizione 3.2.15.** Siano $X \subseteq k^n$ e $Y \subseteq k^m$ varietà algebriche affini. Una funzione $f\colon X \to Y$ si dice **morfismo di varietà algebriche affini** se è continua per la topologia di Zariski e per ogni $U \subseteq Y$ aperto $\varphi \in \mathcal{O}_Y(U) \implies \varphi \circ f \in \mathcal{O}_X(f^{-1}(U))$.

*Osservazione* 3.2.16. Siano $X \subseteq k^n$ e $Y \subseteq k^m$ varietà algebriche affini e $f_1, \dots, f_m \in k[X_1, \dots, X_n]$ tali che la mappa $\phi\colon p \mapsto (f_1(p), \dots, f_m(p))$ verifichi $\phi(X) \subseteq Y$. Allora $\phi\colon X \to Y$ è un morfismo di varietà algebriche affini. Poniamo il morfismo di anelli

$$\begin{array}{rccc} \phi_{\#}\colon & k[Y_1, \dots, Y_m] & \longrightarrow & k[X_1, \dots, X_n] \\ & p(Y_1, \dots, Y_m) & \longmapsto & p(f_1, \dots, f_m) \end{array}$$

Ogni chiuso in $Y$ per la topologia di Zariski è un insieme algebrico affine $Z \subseteq Y$. Per il Nullstellensatz (3.2.12), $q \in Z$ se e solo se per ogni $g \in I(Z)$ si ha $g(q) = 0$ e per il teorema della base di Hilbert $I(Z) = (g_1, \dots, g_r)$, quindi

$$\begin{aligned} \varphi^{-1}(Z) &= \{\, p \in X \mid g_i(\phi(p)) = 0 \quad \forall i = 1, \dots, r \,\} \\ &= \{\, p \in X \mid \phi_{\#}(g_i)(p) = 0 \quad \forall i = 1, \dots, r \,\} \\ &= Z((\phi_{\#}(g_1), \dots, \phi_{\#}(g_r))). \end{aligned}$$

Pertanto $\phi^{-1}(Z)$ è un chiuso di $X$ e $\phi$ è continua. Siano $U \subseteq Y$ un aperto e $\varphi \in \mathcal{O}_Y(U)$. Sia $p \in \phi^{-1}(U)$, per ipotesi esistono $V \subseteq U$ intorno aperto di $\phi(p)$ e $g, h \in A(Y)$, con $h \neq 0$ su tutto $V$, tali che

$$\varphi|_V = \left.\frac{g}{h}\right|_V .$$

Quindi su $\phi^{-1}(V)$, intorno aperto di $p$, si ha

$$\varphi \circ \phi|_{\phi^{-1}(V)} = \left.\frac{g \circ \phi}{h \circ \phi}\right|_{\phi^{-1}(V)} = \left.\frac{\phi_{\#}(g)}{\phi_{\#}(h)}\right|_{\phi^{-1}(V)},$$

dove $\phi_{\#}(g), \phi_{\#}(h) \in A(X)$ e $\phi_{\#}(h) \neq 0$ su tutto $\phi^{-1}(V)$ per costruzione, pertanto $\varphi \circ \phi \in \mathcal{O}_X(\phi^{-1}(U))$.

## 3.3 Dimensione di una Varietà Algebrica Affine

Ora definiremo la dimensione di una varietà algebrica affine da un punto di vista geometricamente intuitivo, che verrà giustificato con una conseguenza del lemma di normalizzazione di Noether. A seguire verrà dimostrata, grazie al Nullstellensatz, l'equivalenza tra la dimensione globale e locale per una varietà algebrica affine. Infine verrà applicato il teorema della dimensione per ottenere una definizione di dimensione equivalente a quelle illustrate, ma puramente algebrica e legata al polinomio di Hilbert.

**Definizione 3.3.1.** Sia $X \subseteq k^n$ una varietà algebrica affine, si definisce la **dimensione di** $X$ come

$$\dim X := \operatorname{tr}\deg_k \operatorname{Frac} A(X).$$

Il Nullstellensatz stabilisce una corrispondenza naturale tra i punti di una varietà algebrica affine e gli ideali massimali del suo anello delle coordinate.

**Proposizione 3.3.2.** *Dati un insieme algebrico affine $X \subseteq k^n$ e un punto $p = (a_1, \dots, a_n) \in X$, poniamo*

$$\mathfrak{m}_p := (X_1 - a_1, \dots, X_n - a_n).$$

*Per ogni ideale massimale $\mathfrak{m} \subseteq k[X_1, \dots, X_n]$ esiste $p \in X$ tale che $\mathfrak{m} = \mathfrak{m}_p$. In particolare, esiste una corrispondenza biunivoca (con un lieve abuso di linguaggio, indichiamo con $Z(\mathfrak{m}) = Z(\mathfrak{m}_p)$ il singolo punto $p$)*

$$\begin{array}{ccc} X & \longleftrightarrow & \{\mathfrak{m}/I(X) \subseteq A(X) \text{ ideale massimale}\} \\ p & \longmapsto & \mathfrak{m}_p/I(X) \\ Z(\mathfrak{m}) & \longleftarrow\!\shortmid & \mathfrak{m}/I(X) \end{array}$$

*Dimostrazione.* Per la corrispondenza tra gli ideali massimali di $k[X_1, \dots, X_n]$ contenenti $I(X)$ e gli ideali massimali di $A(X) = k[X_1, \dots, X_n]/I(X)$, è sufficiente studiare il caso per $I(X) = 0$, quindi $X = k^n$.

Ogni ideale massimale $\mathfrak{m}$ è radicale, quindi per il Nullstellensatz (3.2.12) $I(Z(\mathfrak{m})) = \mathfrak{m}$. Se $p \in Z(\mathfrak{m})$, allora $\mathfrak{m} \subseteq \mathfrak{m}_p$ e per massimalità $\mathfrak{m} = \mathfrak{m}_p$. Così è dimostrata anche la suriettività.

Poiché $k[X_1, \dots, X_n]/\mathfrak{m}_p \cong k$, deve essere $\mathfrak{m}_p$ ideale massimale. Siano $p, p' \in k^n$ distinti, allora $a_i \neq a'_i$ per qualche $1 \leq i \leq n$. Pertanto $X_i - a_i \notin \mathfrak{m}_{p'}$ e $X_i - a'_i \notin \mathfrak{m}_p$, così $\mathfrak{m}_p \neq \mathfrak{m}_{p'}$. Per quanto detto la mappa è iniettiva. □

Mostriamo che, per il lemma di normalizzazione di Noether (3.1.5), la definizione di dimensione data per le varietà algebriche affini non presenta patologie.

**Definizione 3.3.3.** Siano $X \subseteq k^n$ e $Y \subseteq k^m$ varietà algebriche affini, un morfismo $f\colon X \to Y$ si dice **a fibre finite** se per ogni $p \in Y$ la fibra $f^{-1}(p)$ è finita.

**Proposizione 3.3.4.** *Sia $X \subseteq k^n$ una varietà algebrica affine di dimensione $\dim X = r$, allora esiste un morfismo suriettivo a fibre finite $f\colon X \to k^r$.*

*Dimostrazione.* Consideriamo l'anello delle coordinate di $X$

$$A(X) = k[X_1, \dots, X_n]/I(X)$$

e poniamo $x_i = X_i + I(X)$, quindi $A(X) = k[x_1, \dots, x_n]$. Per il lemma di Normalizzazione di Noether (3.1.5) esistono $y_1, \dots, y_r \in A(X)$ algebricamente indipendenti su $k$ tali che $A(X)$ sia intero su $B = k[y_1, \dots, y_s]$. Poiché $\operatorname{tr}\deg_k \operatorname{Frac} A(X) = r$ e l'estensione di campi $\operatorname{Frac} B \subseteq \operatorname{Frac} A(X)$ è algebrica, per (1.6.16) $\operatorname{tr}\deg_k \operatorname{Frac} B = r$; pertanto $s = r$. In particolare $y_i = y_i(x_1, \dots, x_n)$, quindi possiamo definire la mappa $\varphi\colon p \to (y_1(p), \dots, y_r(p))$. Consideriamone la restrizione a $X$, sia

$$\begin{array}{rccc} f\colon & X & \longrightarrow & k^r \\ & p & \longmapsto & (y_1(p), \dots, y_r(p)) \end{array}$$

Per l'osservazione (3.2.16) è un morfismo. Mostriamo la suriettività. Sia $q = (b_1, \dots, b_r) \in k^r$, per (3.3.2) è associato a un ideale massimale $\mathfrak{m}_q \subset B$. Poiché $B \subseteq A(X)$ è un'estensione intera, per il going-up theorem (1.3.9) esiste un ideale primo $\mathfrak{p} \subset A(X)$ che giace su $\mathfrak{m}_q$, ovvero $\mathfrak{m}_q = \mathfrak{p} \cap B$. Per massimalità di $\mathfrak{m}_q$ deve essere $\mathfrak{p}$ massimale, quindi di nuovo per (3.3.2) esiste $p = (a_1, \dots, a_n) \in X$ tale che $\mathfrak{p} = \mathfrak{m}_p$. Osserviamo che per ogni $j = 1, \dots, r$

$$y_j - b_j = h_1^j(x_1, \dots, x_n)(x_1 - a_1) + \dots + h_n^j(x_1, \dots, x_n)(x_n - a_n).$$

Valutando in $p$ si ha

$$y_j(p) - b_j = h_1^j(p)(x_1(p) - a_1) + \dots + h_n(p)^j(x_n(p) - a_n) = 0,$$

pertanto $y_j(p) = b_j$ e di conseguenza $f(p) = q$. Ora mostriamo che per ogni $q \in k^r$ la fibra $f^{-1}(q)$ sia finita. Poiché $A(X)$ è intero su $B$, per ogni $x_i$ vale la relazione

$$x_i^t + g_{t-1}^i(y_1, \dots, y_r)x_i^{t-1} + \dots + g_1^i(y_1, \dots, y_r)x_i + g_0^i(y_1, \dots, y_r) = 0,$$

ovvero

$$X_i^t + g_{t-1}^i(y_1, \dots, y_r)X_i^{t-1} + \dots + g_1^i(y_1, \dots, y_r)X_i + g_0^i(y_1, \dots, y_r) = G_i(X_1, \dots, X_n),$$

con $G_i(X_1, \ldots, X_n) \in I(X)$. Siano $q \in k^r$ e $p \in f^{-1}(q)$, allora $y_j(p) = b_j$ e $X_i(p) = a_i$, quindi per ogni $i = 1, \ldots n$

$$G_i(p) = a_i^t + g_{t-1}^i(q)a_i^{t-1} + \cdots + g_1^i(q)a_i + g_0^i(q) = 0.$$

Posto

$$g_i(T) = T^t + g_{t-1}^i(q)T^{t-1} + \cdots + g_1^i(q)T + g_0^i(q) \in k[T],$$

per il teorema fondamentale dell'algebra ha un numero finito di radici, sia $Z_i$ l'insieme costituito da esse. Quindi $p \in Z_1 \times \cdots \times Z_n$, che è un insieme finito. Ne consegue $f^{-1}(q)$ finito. □

Ora è possibile dimostrare il legame tra la definizione di dimensione data in (3.3.1) e il grado del polinomio di Hilbert-Samuel, quindi del polinomio di Hilbert, rispetto alla localizzazione dell'anello delle coordinate in un qualsiasi punto della varietà algebrica affine.

**Proposizione 3.3.5.** *Sia $X \subseteq k^n$ una varietà algebrica affine, per ogni $p \in X$*

$$\dim A(X) = \dim A(X)_{\mathfrak{m}_p/I(X)} = d(A(X)_{\mathfrak{m}_p/I(X)}).$$

*Dove $d(A(X)_{\mathfrak{m}_p/I(X)})$ è il grado del polinomio di Hilbert-Samuel.*

*Dimostrazione.* Poniamo $\mathfrak{m} = \mathfrak{m}_p/I(X)$. Per ipotesi $A(X)$ è un anello affine, quindi per (3.1.7) si ha $\dim A(X) = \operatorname{ht}\mathfrak{m} + \operatorname{coht}\mathfrak{m}$. Per massimalità $\operatorname{coht}\mathfrak{m} = 0$ e per (1.5.5) vale $\dim A_{\mathfrak{m}} = \operatorname{ht}\mathfrak{m}$. Infine $\dim A(X) = \dim A(X)_{\mathfrak{m}}$. Per (1.2.7) $A(X)_{\mathfrak{m}}$ è un anello locale, così per il teorema della Dimensione (2.4.9) e (2.4.2) si ha $\dim A(X)_{\mathfrak{m}} = d(A(X)_{\mathfrak{m}})$, da cui segue l'asserto. □

# Bibliografia


[1] D. Eisenbud, *Commutative Algebra: with a View Toward Algebraic Geometry*, Springer-Verlag, 1995

[2] M. F. Atiyah, I.g. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, Inc., 1969

[3] Robert B. Ash, *A Course in Commutative Algebra*, Robert B. Ash, 2003

[4] J. Schettler, *Hilbert Functions*

[5] J. S. Milne, *Field and Galois Theory*, J. S. Milne, 2013

# Ringraziamenti

Vorrei ringraziare il mio relatore Luca Migliorini, per essere stato sempre disponibile ed avermi aiutato in modo costruttivo, nonché per aver condiviso con me la passione per la musica.
Un grazie va alla mia famiglia, a mio padre Marcello e a mia madre Emanuela che mi hanno costantemente incoraggiato a non demordere nei momenti critici, e a mio fratello Filippo per avermi distratto quando ne ho avuto bisogno. Ringrazio i miei amici per avermi supportato, in particolare Laura e Francesca per avermi anche coraggiosamente sopportato e spronato.
Un ringraziamento va a Mariagiulia, Marina e Ilaria per il loro aiuto durante i tre anni trascorsi insieme.
Non sono una persona molto espansiva, ma ci tenevo a esprimere il mio pensiero.