Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Magistrale in Matematica

VARIETÀ ALGEBRICHE E PROBLEMA DI WARING

Tesi di Laurea in Geometria Algebrica

Relatore:
MONICA IDÀ
Correlatore:
DAVIDE VANZO

Presentata da:
CHIARA CASCIOLI

Sessione III
2017/2018

” Things we lose have a way
of coming back to us in the end,
if not always in the way we expect.”
Luna Lovegood

Introduzione

La Geometria Algebrica ha come principale studio le varietà algebriche, che sono oggetti geometrici definiti come soluzioni di equazioni polinomiali. Essa, nata nel 1600 con Cartesio e Fermat, si sviluppa in maniera intensa durante XIX e il XX secolo. In questo periodo infatti avviene una forte algebrizzazione della geometria attraverso l'algebra commutativa, che sfocia in due importanti risultati: il Nullstellensatz (o Teorema degli Zeri) ed il Teorema della Base, entrambi enunciati e dimostrati da Hilbert. Questi due sono le fondamenta della connessione tra geometria algebrica e algebra commutativa. Il Nullstellensatz, infatti, mette in relazione gli insiemi algebrici nello spazio affine $\mathcal{A}_k^n$ con gli ideali radicali nell'anello dei polinomi $k[t_1, \ldots, t_n]$, mentre il Teorema della Base ci garantisce che quest'ultimo anello sia noetheriano, e cioè ogni ideale in esso sia finitamente generato. Tutto ciò permette quindi di caratterizzare una varietà , che non è altro che un insieme algebrico irriducibile, come un luogo di zeri di un numero finito di polinomi.
Nello stesso periodo prende piede anche la geometria non euclidea; in particolare è stato Cayley a studiare lo spazio proiettivo e a introdurre l'idea di forme polinomiali omogenee. La differenza sostanziale che c'è tra $\mathcal{A}_k^n$ e $\mathbb{P}_k^n$ sta nel fatto che il secondo dei due spazi viene definito mediante una relazione di equivalenza, che identifica tutti i punti con coordinate equivalenti, a meno di una moltiplicazione per scalari. Di conseguenza, dato un polinomio qualsiasi ed un punto che lo annulla, non è detto che tutte le scritture equivalenti di tale punto annullino il polinomio dato. Questo problema viene risolto se si considerano ora degli ideali in $k[t_0, \ldots, t_n]$ detti omogenei. È grazie a questi che si riesce a mantenere la relazione tra insiemi algebrici e ideali. Si estendono quindi i risultati precedenti al caso proiettivo: i due Teoremi di Hilbert sono validi e una varietà proiettiva

viene caratterizzata mediante un numero finito di polinomi omogenei.
Lo scopo di questa tesi è appunto quello di introdurre le varietà proiettive sulla base delle conoscenze di quelle affini, di analizzare delle particolari funzioni e mappe (dette regolari) sia nel caso affine che nel caso proiettivo, e infine di introdurre il Problema di Waring nel quale è utile sfruttare un particolare morfismo proiettivo, chiamato mappa di Veronese.
Nel primo Capitolo vengono affrontati alcuni prerequisiti necessari alla comprensione dei Capitoli successivi: vengono ricordate le definizioni delle corrispondenze V ed $\mathfrak{I}$, che mettono in relazione i sottoinsiemi chiusi dello spazio affine $\mathcal{A}_k^n$ con gli ideali dell'anello dei polinomi $k[t_1, \ldots, t_n]$, ed alcuni importanti risultati ad esse collegati, come il Teorema della Base di Hilbert, il Nullstellensatz e la caratterizzazione delle varietà affini. Successivamente viene introdotto lo spazio proiettivo come spazio quoziente dello spazio $n+1$ dimensionale $k^{n+1} \setminus \{0\}/\sim$, dove $\sim$ è una relazione di equivalenza che identifica i punti con stesse coordinate a meno di una moltiplicazione per uno scalare, e vengono ricordate alcune definizioni e proprietà riguardanti i polinomi omogenei. Infine vengono definite le strutture di modulo e di algebra su un anello.
Nel secondo Capitolo ci si addentra nelle varietà proiettive: dopo aver definito e mostrato alcuni interessanti risultati su anelli graduati e ideali omogenei (tra cui, per esempio, che il radicale di un ideale omogeneo è ancora omogeneo), viene messa in luce la difficoltà di stabilire le corrispondenze V ed $\mathfrak{I}$ come nel caso affine. Come detto in precedenza, per far sì che tali applicazioni siano ben definite è necessario considerare solamente gli ideali omogenei; inoltre, per questi ultimi, è sempre possibile trovare un sistema di generatori omogenei. Viene data quindi la definizione di varietà proiettiva come luogo di zeri di un numero finito di polinomi omogenei, e si conclude il Capitolo con la dimostrazione del Nullstellensatz omogeneo che mette in luce la corrispondenza biunivoca (con alcuni accorgimenti) tra sottoinsiemi algebrici di $\mathbb{P}_k^n$ e ideali omogenei radicali di $k[t_0, \ldots, t_n]$.
Nel terzo Capitolo si introducono le funzioni (ossia applicazioni tra un insieme algebrico ed il suo campo base) e le mappe (cioè applicazioni tra due insiemi algebrici) nel caso affine e proiettivo, ponendo l'attenzione su quelle definite regolari. L'insieme di queste ultime, nel caso affine, viene chiamato anello delle coordinate della varietà e ci permette di dimostrare un importante risultato: due varietà sono isomorfe se e solo se sono iso-

morfi i rispettivi anelli delle coordinate. Anche in questo caso quindi, da un problema geometrico ci si può ricondurre ad un quesito algebrico. Viene infine fatto un accenno al campo delle funzioni razionali ed un esempio di un noto morfismo proiettivo: l'embedding di Segre. E' stata posta una maggiore attenzione invece sul morfismo proiettivo di Veronese perché viene utilizzata nel quarto ed ultimo Capitolo: in questo viene introdotto il calcolo tensoriale ed il Problema di Waring.
Il Problema di Waring nasce come un quesito di teoria dei numeri, di cui è stata fatta anche una formulazione geometrica:

Qual è il minimo $z \in \mathbb{Z}^+$ tale che una generica forma $f \in R_d$ si possa scrivere come combinazione di z potenze d-esime di forme lineari, ossia come $f = L_1^d + \ldots + L_z^d$?

La mappa di Veronese è il primo oggetto geometrico legato alla risoluzione di questo problema, infatti essa parametrizza le potenze d-esime dei tensori di rango 1. L'altro oggetto geometrico da prendere in considerazione sono le varietà secanti, in particolare le varietà secanti della Veronese: esse sono necessarie per studiare il rango di una generica forma, infatti studiare la dimensione della s-esima varietà secante corrisponde a risolvere il Problema di Waring. L'elaborato si conclude con l'enunciato del Teorema di Alexander-Hirschowitz che dà la dimensione delle varietà secanti delle Veronesi.

Indice

Capitolo 1

Prerequisiti

L'anello R indica un anello commutativo unitario e k un campo algebricamente chiuso. Tutti i risultati del capitolo sono stati dimostrati in [5] .

1.1 Anelli noetheriani

Ricordiamo la definizione di anello noetheriano ed enunciamo brevemente alcuni teoremi legati a questa struttura algebrica.

Proposizione-Definizione 1.1.1. Un anello R si dice *noetheriano* se soddisfa una delle seguenti caratteristiche equivalenti:

1. Ogni ideale $I \subset R$ è finitamente generato; cioè esistono $f_1, \ldots, f_k \in R$, tali che $I = \big(f_1, \ldots, f_k\big)$.

2. Ogni catena ascendente di ideali di R, $I_1 \subseteq I_2 \subseteq \ldots$, è stazionaria; cioè esiste N tale che $I_N = I_M$ per ogni $M \geq N$.

3. Ogni insieme non vuoto di ideali di R ha un elemento massimale.

Un importante risultato è il *Teorema della base di Hilbert*:

Teorema 1.1.2. Sia R un anello noetheriano; allora $R[t]$ è noetheriano.

da cui segue che

Corollario 1.1.3. Sia R un anello noetheriano, allora $R[t_1, \dots, t_n]$ è noetheriano.

Osservazione 1.1.4. Osserviamo che ogni campo k è un anello noetheriano; ciò è vero perché in un campo gli unici ideali sono quelli banali, ossia $\big(0\big)$ e $\big(1\big)$, che sono finitamente generati.
Segue dal teorema precedente che anche $k[t]$ e $k[t_1, \dots, t_n]$ sono anelli noetheriani.

1.2 Le corrispondenze V ed $\mathfrak{I}$, e il Nullstellensatz

Sia X un sottoinsieme dello spazio affine n-dimensionale sul campo k algebricamente chiuso, $X \subseteq \mathcal{A}_k^n$, e sia I un ideale dell'anello dei polinomi a n indeterminate $k[t_1, \dots, t_n]$. Definiamo la corrispondenza V come l'applicazione

$$\begin{array}{ccc} \{\text{ideali } J \subseteq k[t_1, \dots, t_n]\} & \longrightarrow & \{\text{sottoinsiemi } X \subseteq \mathcal{A}_k^n\} \\ J & \longmapsto & V(J) \end{array}$$

dove $V(J) = \{P \in \mathcal{A}_k^n \quad | \quad f(P) = 0 \quad \forall f \in J\}$, ossia l'insieme dei punti dello spazio affine che annullano ogni polinomio appartenente all'ideale J.

Definizione 1.2.1. Diciamo che un sottoinsieme X di $\mathcal{A}_k^n$ è *algebrico* se $X = V(I)$ per qualche ideale I di $k[t_1, \dots, t_n]$.

Un insieme algebrico X è quindi definito come immagine di un ideale I mediante l'applicazione V; dunque X è l'insieme dei punti che annullano ogni polinomio dell'ideale I. Ma essendo I finitamente generato, X è l'insieme dei punti di $\mathcal{A}_k^n$ che annullano un qualunque insieme di generatori di I. Ciò significa che un insieme algebrico è il *luogo di zeri* di un numero finito di polinomi.
Ricordiamo inoltre che la collezione degli insiemi algebrici definisce la topologia di Zariski su $\mathcal{A}_k^n$ dove questi insiemi sono i chiusi di questa topologia.

Dato $X \subseteq \mathcal{A}_k^n$ un sottoinsieme algebrico, ossia tale che $X = V(I)$ con $I = (f_1, \dots, f_m)$ ideale in $k[t_1, \dots, t_n]$, chiameremo $f_1(t_1, \dots, t_n) = \ldots = f_m(t_1, \dots, t_n) = 0$ *equazioni di X*.

Esempio 1.2.2. $\mathcal{A}_k^n$ è un chiuso, infatti esso è il luogo di zeri del polinomio nullo.
Al contrario $\mathcal{A}_k^n \setminus \{0\}$ non lo è perché ogni polinomio $f(t_1, \ldots, t_n)$ che si annulla ovunque meno che nell'origine deve essere identicamente nullo.

Esempio 1.2.3. Determiniamo i chiusi di $\mathcal{A}_k^1$:
$X \subseteq \mathcal{A}_k^1$ chiuso è determinato da $f_1(t_1) = \ldots = f_s(t_1) = 0$ equazioni in una sola variabile.
Se i polinomi sono identicamente nulli, ovvero l'ideale è (0), allora $X = \mathcal{A}_k^1$.
Se i polinomi non hanno un fattore in comune, essi non hanno nemmeno una radice comune, quindi $X = \emptyset$.
Se i polinomi hanno uno o più fattori in comune, sia $(t_1 - a_1)^{\alpha_1} \cdots (t_1 - a_s)^{\alpha_s}$ il massimo comun divisore, allora $X = \{a_1, \ldots, a_s\}$.
Dunque i chiusi di $\mathcal{A}_k^1$ sono $\mathcal{A}_k^1$ stesso, l'insieme vuoto e gli insiemi finiti di punti.

Esempio 1.2.4. Siano $X \subseteq \mathcal{A}_k^n$ e $Y \subseteq \mathcal{A}_k^m$ due chiusi, determinati rispettivamente dalle equazioni $f_1(t_1, \ldots, t_n) = \ldots = f_s(t_1, \ldots, t_n) = 0$ e $g_1(z_1, \ldots, z_m) = \ldots = g_r(z_1, \ldots, z_m) = 0$. Allora $X \times Y \subseteq \mathcal{A}_k^{n+m}$ è ancora un chiuso definito dalle equazioni

$$\tilde{f}_1(t_1, \ldots, t_n, z_1, \ldots, z_m), \ldots, \tilde{f}_s(t_1, \ldots, t_n, z_1, \ldots, z_m)$$

$$\tilde{g}_1(t_1, \ldots, t_n, z_1, \ldots, z_m), \ldots, \tilde{g}_r(t_1, \ldots, t_n, z_1, \ldots, z_m)$$

dove per $i = 1, \ldots, s$ $\tilde{f}_i(t_1, \ldots, t_n, z_1, \ldots, z_m)$ non è altro che f_i visto però come polinomio in più variabili; analogamente per $\tilde{g}_j$.

Definizione 1.2.5. Sia $X \subseteq \mathcal{A}_k^n$ definito solamente da un polinomio $f(t_1, \ldots, t_n)$, allora X viene chiamato *ipersuperficie.*

Osservazione 1.2.6. Dati I e J due ideali in $k[t_1, \ldots, t_n]$ tali che $I \subseteq J$, allora si ha che $V(I) \supseteq V(J)$.

Come in precedenza, sia X un sottoinsieme di $\mathcal{A}_k^n$ e J un ideale di $k[t_1, \ldots, t_n]$; definiamo ora la corrispondenza $\mathfrak{I}$ come l'applicazione

$$\begin{array}{ccc} \{\text{sottoinsiemi } X \subseteq \mathcal{A}_k^n\} & \longrightarrow & \{\text{ideali } J \subseteq k[t_1, \ldots, t_n]\} \\ X & \longmapsto & \mathfrak{I}(X) \end{array}$$

dove $\mathfrak{I}(X) = \{f \in k[t_1, \ldots, t_n] \quad | \quad f(P) = 0, \quad \forall P \in X\}$, cioè l'ideale dei polinomi che si annullano su tutti i punti dell'insieme X.

Osservazione 1.2.7. Osserviamo anche in questo caso che, dati X e Y due sottoinsiemi di $\mathcal{A}_k^n$ tali che $X \subseteq Y$, allora vale $\mathfrak{I}(X) \supseteq \mathfrak{I}(Y)$.

In generale si ha che:

Proposizione 1.2.8. per ogni X sottoinsieme di $\mathcal{A}_k^n$ e per ogni J ideale di $k[t_1, \ldots, t_n]$ $X \subseteq V(\mathfrak{I}(X))$ e $J \subseteq \mathfrak{I}(V(J))$.

Infine, richiamiamo qualche nozione sugli ideali:

Definizione 1.2.9. Sia R un anello e I un suo ideale. I si dice *primo* se I è diverso da R e per ogni $f, g \in k[t_1, \ldots, t_n]$, tali che $fg \in I$, allora $f \in I$ o $g \in I$.

Proposizione-Definizione 1.2.10. Sia R un anello e siano I e J due ideali in R.

- $I + J := \{x + y \in R \quad | \quad x \in I, y \in J\}$
- $I \cdot J := \{\sum_{i=1}^{n} x_i y_i \in R \quad | \quad x_i \in I, y_i \in J, n \in \mathbb{N}\}$
- $I \cap J := \{x \in R \quad | \quad x \in I \quad e \quad x \in J\}$

Somma, prodotto e intersezione di due ideali, sono ancora degli ideali.
Inoltre, se I e J sono due ideali finitamente generati, $I = (f_1, \ldots, f_n)$ e $J = (g_1, \ldots, g_m)$, allora anche $I+J$ e $I \cdot J$ sono finitamente generati, in particolare $I+J = (f_1, \ldots, f_n, g_1, \ldots, g_m)$ e $I \cdot J = (f_i g_j)_{i=1,\ldots,n, j=1,\ldots,m}$.

Proposizione-Definizione 1.2.11. Sia I un ideale in $k[t_1, \ldots, t_n]$; l'insieme $\sqrt{I} = \{f \in k[t_1, \ldots, t_n] \mid \exists\, n > 0 \quad \text{tale che} \quad f^n \in I\}$ si dice *radicale di I* ed è un ideale.
Se I è un ideale in $k[t_1, \ldots, t_n]$ tale che $I = \sqrt{I}$, allora I si dice *ideale radicale*.

A questo punto possiamo enunciare l'importante *Teorema degli Zeri di Hilbert*, o *Nullstellensatz*:

Teorema 1.2.12. Sia k un campo algebricamente chiuso, sia $A = k[t_1, \ldots, t_n]$ l'anello dei polinomi in n variabili a coefficienti in k e siano V ed $\mathfrak{I}$ definite come in precedenza. Allora valgono:

(a) Ogni ideale massimale dell'anello A è della forma $m = \big(t_1 - a_1, \ldots, t_n - a_n\big)$, per un qualche punto $P = (a_1, \ldots, a_n) \in \mathcal{A}_k^n$.

(b) Sia $J \subseteq A$ un ideale, tale che $J \neq \big(1\big)$; allora $V(J) \neq \emptyset$.

(c) Per ogni $J \subseteq A$, si ha: $\mathfrak{I}(V(J)) = \sqrt{J}$.

Una delle conseguenze del teorema è che, sotto le opportune ipotesi che X sia un sottoinsieme algebrico di $\mathcal{A}_k^n$ e J sia un ideale radicale in $k[t_1, \ldots, t_n]$, le due corrispondenze V ed $\mathfrak{I}$ sono una l'inversa dell'altra, cioè esiste una corrispondenza biunivoca tra $\{X \subseteq \mathcal{A}_k^n,\ X \text{ sottoinsieme algebrico}\} \longleftrightarrow \{J \subseteq k[t_1, \ldots, t_n],\quad J \text{ ideale radicale}\}$

1.3 Varietà affini

Riprendiamo qualche nozione importante riguardo alle varietà affini:

Definizione 1.3.1. Sia $Y \subseteq \mathcal{A}_k^n$ un insieme algebrico non vuoto. Diciamo che Y è *irriducibile* se ogni volta che $Y = X_1 \cup X_2$, con X_1 e X_2 algebrici, implica che $X_1 = Y$ oppure $X_2 = Y$. In altre parole, un insieme algebrico si dice irriducibile se non si può scrivere come unione di insiemi algebrici entrambi strettamente contenuti in Y.

Possiamo dare ora la definizione di varietà nello spazio affine:

Definizione 1.3.2. X è detta *varietà* di $\mathcal{A}_k^n$ se è un sottoinsieme algebrico irriducibile di $\mathcal{A}_k^n$.

Ricordiamo infine il teorema di decomposizione nello spazio affine:

Teorema 1.3.3. Sia X un insieme algebrico nello spazio $\mathcal{A}_k^n$. Allora esistono $X_1, \ldots, X_n$ varietà tali che

$$X = X_1 \cup \ldots \cup X_n$$

Inoltre, se $X_i \nsubseteq X_j$ per ogni $i \neq j$, tale decomposizione è unica a meno dell'ordine.

1.4 Spazio proiettivo

In questa sezione riprenderemo qualche nozione fondamentale riguardo allo spazio proiettivo.

Sia k un campo e sia $\sim$ la relazione definita sui punti di $k^{n+1} \setminus \{0\}$ nel modo seguente:

$$(x_0, \dots, x_n) \sim (x'_0, \dots, x'_n) \iff \exists \lambda \in k \text{ tale che } (x_0, \dots, x_n) = \lambda(x'_0, \dots, x'_n)$$

Definiamo quindi *spazio proiettivo n-dimensionale sul campo k* l'insieme quoziente

$$\mathbb{P}^n_k := k^{n+1} \setminus \{0\}/ \sim$$

Un punto $P \in \mathbb{P}^n_k$ è definito da una $(n+1)$-upla $[t_0, \dots, t_n]$ di coordinate, chiamate *coordinate omogenee.*
Ad ogni elemento di $\mathbb{P}^n_k$ corrisponde quindi un insieme di vettori con le stesse coordinate a meno di una moltiplicazione per uno scalare $\lambda \neq 0$; dunque possiamo vedere i punti di $\mathbb{P}^n_k$ come le rette che passano per l'origine di k^{n+1}.
$\mathbb{P}^n_k$ è quindi l'insieme degli spazi vettoriali di dimensione 1 di k^{n+1}.

Definizione 1.4.1. Sia $f \in k[t_0, \dots, t_n]$ e sia $P = [\xi_0, \dots, \xi_n]$; si dice che f si annulla su P se $f(\xi_0, \dots, \xi_n) = 0$ per ogni scelta di rappresentanti di P. In questo caso scriveremo anche $f(P) = 0$.

Proposizione-Definizione 1.4.2. Sia $f \in k[t_0, \dots, t_n]$ e sia $P = (\xi_0, \dots, \xi_n)$; si definisce *decomposizione in elementi omogenei di* f la somma $f = f_0 + \dots + f_r$, dove f_j rappresenta la somma di tutti i termini di f di grado j; tale decomposizione è unica.
Si ha che $f(\lambda P) = f_0(P) + \lambda f_1(P) + \lambda^2 f_2(P) + \dots + \lambda^r f_r(P)$.

Dimostrazione. Per ogni j scriviamo

$$f_j(P) = f_j(\xi_0, \dots, \xi_n) = \sum_{i=1}^{l} c_i {\xi_0}^{t_0^i} \cdot \dots \cdot {\xi_n}^{t_n^i}$$

con $t_0^i + \dots + t_n^i = j$ per ogni $i = 1, \dots, l$.
Sostituiamo ora P con λP:

$$f_j(\lambda P) = f_j(\lambda\xi_0, \dots, \lambda\xi_n) = \sum_{i=1}^{l} c_i (\lambda\xi_0)^{t_0^i} \cdot \dots \cdot (\lambda\xi_n)^{t_n^i} = \sum_{i=1}^{l} c_i \lambda^{t_0^i} {\xi_0}^{t_0^i} \cdot \dots \cdot \lambda^{t_n^i} {\xi_n}^{t_n^i} =$$

$$= \sum_{i=1}^{l} c_i \lambda^{t_0^i + \ldots + t_n^i} {\xi_0}^{t_0^i} \cdot \ldots \cdot {\xi_n}^{t_n^i} = \lambda^j \sum_{i=1}^{l} c_i {\xi_0}^{t_0^i} \cdot \ldots \cdot {\xi_n}^{t_n^i} = \lambda^j f_j(\xi_0, \ldots, \xi_n)$$

□

Definizione 1.4.3. Sia $f \in k[t_0, \ldots, t_n]$; f si definisce *polinomio omogeneo di grado d* se la sua decomposizione è $f = f_d$.

Proposizione-Definizione 1.4.4. Sia $f \in k[t_1, \ldots, t_n]$ un polinomio non omogeneo, e sia $f = f_0 + \ldots + f_r$ la sua decomposizione in elementi omogenei. Allora definiamo $f^H(t_0, \ldots, t_n) := f_0(t_1, \ldots, t_n)t_0^r + f_1(t_1, \ldots, t_n)t_0^{r-1} + \ldots + f_r(t_1, \ldots, t_n) \in k[t_o, \ldots, t_n]$ l'*omogeneizzato* di f rispetto a t_0. Tale polinomio è omogeneo di grado r

Definizione 1.4.5. Sia $f \in k[t_0, \ldots, t_n]$ omogeneo; il polinomio $\tilde{f} \in k[t_1, \ldots, t_n]$ definito da $\tilde{f}(t_1, \ldots, t_n) := f(1, t_1, \ldots, t_n)$ si dice *deomogeneizzato* di f rispetto a t_0.

Osservazione 1.4.6. Sia $f \in k[t_0, \ldots, t_n]$ un polinomio omogeneo di grado d. Notiamo come, con le notazioni precedenti, $(\tilde{f})^H = f$ se f non è divisibile per t_0, altrimenti, detto l il massimo esponente tale che t_0^l divide f, si ha che $f = t_0^l(\tilde{f})^H$.

1.5 Moduli e algebre

Enunciamo qui di seguito qualche nozione fondamentale sui moduli e sulle algebre. In questa sezione R indicherà un anello commutativo unitario e k un campo.

Definizione 1.5.1. Si definisce R-modulo una coppia (M, μ) dove $(M, +)$ è un gruppo abeliano e μ è una mappa così definita:

$$\begin{array}{rcl} \mu : R \times M & \longrightarrow & M \\ (r, x) & \longmapsto & \mu(r, x) = rx \end{array}$$

tale che soddisfi i seguenti assiomi:
siano $r, s \in R$ e $x, y \in M$

- $r(x + y) = rx + ry$
- $(r + s)x = rx + sx$

- $(rs)x = r(sx)$
- $1_R x = x$

Definizione 1.5.2. Siano M e N due R-moduli. La mappa $f : M \longrightarrow N$ si definisce un *omomorfismo di R-moduli* se è un omomorfismo di gruppi e, per ogni $r \in R$ e per ogni $x \in M$ vale che $f(rx) = rf(x)$.

Proposizione 1.5.3. Siano M e N due R-moduli e siano f e g due omomorfismi tra M e N. Definiamo nel modo seguente l'addizione e il prodotto per scalare: $(f+g)(x) := f(x) + g(x)$ e $(af)(x) := a \cdot f(x)$ valide per ogni $x \in M$ e per ogni $a \in R$. Si ha che, con queste due operazioni, l'insieme di tutti gli omomorfismi di R-moduli tra M e N è esso stesso un R-modulo, e viene denotato con $Hom_R(M, N)$.

Dimostrazione. Per ogni $f, g \in Hom_R(M, N)$ e per ogni $r, t \in R$ si ha:

- $r(f+g)(x) = r(f(x) + g(x)) = rf(x) + rg(x) = (rf + rg)(x)$
- $(r+t)f(x) = rf(x) + tf(x) = (rf + tf)(x)$
- $(rt)f(x) = r(tf(x)) = r(tf)(x)$
- $1f(x) = f(x)$

□

Definizione 1.5.4. Sia M un R-modulo. Un sottoinsieme $N \subseteq M$ si definisce *sottomodulo di M* se $(N, +)$ è un sottogruppo di $(M, +)$ e se $\forall n \in N$, $\forall r \in R$ si ha che $rn \in N$.

Definizione 1.5.5. Sia M un R-modulo. M si definisce *modulo libero* se esiste un insieme E di elementi di M tali che:

- ogni elemento di M si può scrivere come combinazione finita a coefficienti in R di elementi di E, cioè per ogni $m \in M$ esistono $r_1, \dots, r_n \in R$ e $e_1, \dots, e_n \in E$ tali che $m = r_1e_1 + \ldots + r_ne_n$; si dice che E genera M.
- se ogni volta che $r_1e_1 + \ldots + r_se_s = 0$, con $r_i \in R$ e $e_i \in E$, questo implica che $r_i = 0$ per ogni i.

Definizione 1.5.6. Sia M un R-modulo. M si dice *finitamente generato* se esistono $m_1, \ldots, m_t \in M$, tali che ogni elemento in M si possa scrivere come loro combinazione a coefficienti in R, cioè $\forall m \in M \ \exists r_1, \ldots, r_t \in R$ tale che $m = r_1 m_1 + \ldots + r_t m_t$. In tal caso $m_1, \ldots, m_t$ si diranno *insieme di generatori*.

Teorema 1.5.7. Sia M un R-modulo. Le seguenti condizioni sono equivalenti:

1. Ogni catena ascendente di sottomoduli è stazionaria
2. Ogni insieme non vuoto di sottomoduli di M ha un elemento massimale
3. Ogni sottomodulo di M è finitamente generato

Dimostrazione. $1 \Rightarrow 2)$ Sia S un sottoinsieme non vuoto di sottomoduli di M. Per assurdo supponiamo che S non abbia un elemento massimale, allora preso $M_1 \in S$ esiste $M_2 \in S$ tale che $M_1 \subset M_2$. In maniera ricorsiva possiamo quindi costruire una catena di sottomoduli ascendente non stazionaria, andando contro l'ipotesi.
$2 \Rightarrow 3$ Sia N un sottomodulo di M e supponiamo per assurdo che N non sia finitamente generato. Allora per ogni sottomodulo N' di N finitamente generato si ha che $N' \neq N$, e quindi esiste $x \in N \setminus N'$. Sia ora N'' il sottomodulo di N generato dai generatori di N' e da x, questo sottomodulo è finitamente generato e $N' \subset N''$. Procedendo in questo modo si crea un insieme di sottomoduli di M che non ha un elemento massimale. Notando poi che questo insieme è diverso dal vuoto perché $\{0\}$ gli appartiene, si ottiene un assurdo.
$3 \Rightarrow 1$ Sia $M_1 \subseteq \ldots \subseteq M_t \ldots$ una catena ascendente di sottomoduli di M. Allora $N = \bigcup_{i \geq 1} M_i$ è un sottomodulo di M e quindi è finitamente generato. Siano $m_1, \ldots, m_n$ dei generatori di N. Per ogni $i = 1, \ldots, n$ esiste un indice j_i tale che $m_i \in M_{j_i}$. Consideriamo $j_{max} = max\{j_i \mid i = 1, \ldots, n\}$, allora $N \subseteq M_{j_{max}}$ e quindi per ogni indice i maggiore di j_{max} si ha $N \subseteq M_{j_{max}} \subseteq M_i \subseteq N$ da cui $M_{j_{max}} = M_i$. □

Definizione 1.5.8. Un R-modulo M è *noetheriano* se soddisfa una delle condizioni precedenti (e quindi tutte).

Esempio 1.5.9.

- Un modulo noetheriano è sempre finitamente generato, e ciò è conseguenza del punto 3 del Teorema 1.5.7.

- Un anello R è noetheriano se R è noetheriano come R-modulo, infatti valgono i 3 punti del Teorema 1.5.7 per gli ideali (che sono sottomoduli) di R.

- Ogni gruppo abeliano finito G è uno $\mathbb{Z}$-modulo finitamente generato. Infatti per avere la struttura di $\mathbb{Z}$-modulo basta definire, per $a \in G$ e $n \in \mathbb{Z}$:

$$na = a + \ldots + a, \quad n > 0$$

$$na = (-a) + \ldots + (-a), \quad n < 0$$

$$0a = 0$$

Inoltre se G è finito, allora come $\mathbb{Z}$-modulo è finitamente generato.

Definizione 1.5.10. Si definisce *R-algebra* un anello A che sia dotato di una struttura di R-modulo tale che per ogni $a, b \in A$, per ogni $r \in R$ valga $r(ab) = (ra)b = a(rb)$.

Definizione 1.5.11. Sia R un anello, A e B due R-algebre. e Diciamo che $f : A \longrightarrow B$ è un *omomorfismo di R-algebre* se f è un omomorfismo di anelli e di $R-$moduli

Definizione 1.5.12. Sia A una R-algebra. A si dice *finitamente generata* se esiste un omomorfismo suriettivo di R-algebre da un anello dei polinomi con un numero finito di indeterminate $R[t_1, \ldots, t_n]$ ad A.

Capitolo 2

Varietà proiettive

2.1 Anelli graduati e ideali omogenei

Con k denotiamo sempre un campo algebricamente chiuso.

Definizione 2.1.1. Un anello R si definisce *anello graduato* se esiste una famiglia di sottogruppi abeliani di R tale che R si possa scrivere come somma diretta di tali gruppi,

$$R = \bigoplus_{d \geq 0} R_d$$

e se per ogni $d, e \geq 0$ si ha $R_d \cdot R_e \subseteq R_{d+e}$, cioè per ogni $a_d \in R_d, a_e \in R_e$ implica che $a_d a_e \in R_{d+e}$. Un elemento appartenente a R_d è detto omogeneo di grado d.
Se a è un elemento di R, esso si può scrivere in modo unico come somma di elementi omogenei, ossia $a = \sum_{d \geq 0} a_d$ dove solo un numero finito di a_d è diverso da 0. a_d è detta componente omogenea di grado d di a.

Definizione 2.1.2. Un ideale I di R è chiamato *ideale omogeneo* se per ogni $f \in I$, le componenti omogenee f_d di f appartengono a I.

Consideriamo ora l'anello dei polinomi in $(n+1)$ variabili a coefficienti in un campo k, cioè $R = k[t_0, \ldots, t_n]$, che ha chiaramente la struttura di anello graduato data dal grado.

Proposizione 2.1.3. Sia I un ideale in $k[t_0, \dots, t_n]$. I è omogeneo se e solo se I può essere generato da elementi omogenei, cioè esistono $f_1, \dots, f_r$ polinomi omogenei tali che $I = (f_1, \dots, f_r)$.

Dimostrazione. $\Rightarrow$) I omogeneo, cioè $\forall f \in I$ tutte le componenti omogenee f_d di f di grado d appartengono ad I. Sappiamo che $k[t_0, \dots, t_n]$ è noetheriano, quindi I è finitamente generato; siano $g_1, \dots, g_r$ i suoi generatori. Ognuno di questi generatori si può scrivere come decomposizione in componenti omogenee,

$$g_j = \sum_{d=0}^{l_j} g_d^j \; \forall j = 1, \dots, r$$

e si ha per ipotesi che ogni $g_d^j \in I$. Sia ora I' l'ideale generato da tutti gli elementi g_d^j; mostriamo che $I = I'$ utilizzando la doppia inclusione:
$\subseteq :$ $I \subseteq I'$ perché preso $f \in I$, esso si scrive come combinazione lineare dei generatori di I, ossia $f = a_1 g_1 + \ldots + a_r g_r$ con $a_i \in k[t_0, \dots, t_n]$, sostituendo ogni g_i con la sua decomposizione in elementi omogenei si ottiene $f = a_1 \sum_{d=0}^{l_1} g_d^1 + \ldots + a_r \sum_{d=0}^{l_r} g_d^r$, cioè f è combinazione lineare dei generatori di I', e quindi $f \in I'$.
$\supseteq :$ $I \supseteq I'$, infatti $\forall j = 1, \dots, r$ si ha che $g_{d_j} \in I$ perché I omogeneo e quindi contiene tutte le componenti omogenee dei suoi elementi.

$\Leftarrow$) I può essere generato da elementi omogenei, cioè $I = (f_1, \dots, f_r)$ con $f_1, \dots, f_r$ polinomi omogenei. Dobbiamo dimostrare che $\forall g \in I$ polinomio qualsiasi, le sue componenti omogenee g_d di grado d appartengono ad I. Sia dunque $g \in I$; esso si scrive come combinazione dei generatori di I, $g = a_1 f_1 + \ldots + a_r f_r$ dove $a_i \in k[t_0, \dots, t_n]$. Ogni componente omogenea di grado d di g si scrive come $g_d = \tilde{a}_1 f_1 + \ldots + \tilde{a}_r f_r$, dove $\tilde{a}_i$ è nulla oppure è parte omogenea di grado d_i di a_i tale che $d_i + deg\ f_i = d$; allora $g_d \in I$ per ogni d, cioè ogni componente omogenea di g sta in I. Di conseguenza I è omogeneo. □

Proposizione 2.1.4. Siano I e J due ideali omogenei. La somma, il prodotto e l'intersezione di due ideali omogenei sono a loro volta ideali omogenei.

Dimostrazione.

- $I + J$: I e J sono omogenei, pertanto possono essere generati da polinomi omogenei, $I = (x_1, \dots, x_r)$, $J = (y_1, \dots, y_t)$. Per quanto ricordato nella proposizione 1.2.10, $I + J = (x_1, \dots, x_r, y_1, \dots, y_t)$, cioè $I + J$ è generato da polinomi omogenei e quindi è un ideale omogeneo.

- $I \cdot J$: Come sopra, I e J sono ideali omogenei e quindi possono essere generati da polinomi omogenei; siano essi $I = (x_1, \dots, x_r)$, $J = (y_1, \dots, y_t)$. Sempre per quanto visto nella proposizione 1.2.10, l'ideale prodotto $I \cdot J = (x_i y_j,\ i = 1, \dots, r, j = 1, \dots, t)$; anche i suoi generatori sono omogenei, perché il prodotto di polinomi omogenei è ancora omogeneo. Quindi $I \cdot J$ è omogeneo.

- $I \cap J$: Sia $f \in I \cap J$, cioè $f \in I$ e $f \in J$. I e J sono omogenei, quindi contengono le componenti omogenee di ogni elemento che gli appartiene; in particolare se $f = \sum f_d$ è la decomposizione omogenea di $f \in I \cap J$, allora ogni $f_d \in I$ e ogni $f_d \in J$, cioè per ogni d, $f_d \in I \cap J$. Quindi $I \cap J$ contiene ogni componente omogenea dei suoi elementi, ed è dunque un ideale omogeneo.

□

Proposizione 2.1.5. Sia I un ideale omogeneo. Il radicale di I, $\sqrt{I}$, è ancora un ideale omogeneo.

Dimostrazione. Sia I omogeneo; preso $f \in \sqrt{I}$, significa che esiste un $n > 0$ naturale tale che $f^n \in I$. Sia $f = f_0 + \ldots + f_r$ la decomposizione di f in elementi omogenei. Quindi $f^n = (f_0 + \ldots + f_r)^n = f_0^n + n f_0^{n-1} f_1 + \ldots + f_r^n$. Considero f_0^n, che è omogeneo e di grado minimo; esso appartiene ad I, ma quindi $f_0 \in \sqrt{I}$. Allora $f - f_0 \in \sqrt{I}$ e questo significa che esiste un $m > 0$ tale che $(f_1 + \ldots + f_r)^m \in I$. Iterando il ragionamento si dimostra che ogni componente omogenea di f sta in $\sqrt{I}$. Ciò significa che $\sqrt{I}$ è omogeneo. □

Proposizione 2.1.6. Sia I un ideale omogeneo diverso da tutto l'anello. I è primo se e solo se per ogni f, g polinomi omogenei tali che $fg \in I$, si ha che $f \in I$ o $g \in I$.

Dimostrazione.
$\Rightarrow$) Questa implicazione segue dalla definizione di ideale primo.
$\Leftarrow$) Se uno dei due elementi è l'elemento nullo non c'è nulla da dimostrare. Dimostriamo questa implicazione utilizzando il principio di induzione sul grado del polinomio fg.
Sia $deg(fg) = 0$; allora si ha che $deg\ f = 0$ e $deg\ g = 0$. Quindi sono omogenei e per

ipotesi $fg \in I$ implica che $f \in I$ o $g \in I$.
Supponiamo che l'ipotesi sia vera per $deg(fg) = n-1$ e dimostriamo che vale anche per $deg(fg) = n$.
Siano quindi $f = f_0 + \ldots + f_t$ e $g = g_0 + \ldots + g_s$ le rispettive decomposizioni in elementi omogenei di f e g; poiché il grado di fg è n, la componente omogenea di grado massimo è data dal prodotto delle due componenti omogenee di grado massimo $f_t g_s$. I è omogeneo, dunque $f_t g_s \in I$ e per ipotesi $f_t \in I$ o $g_s \in I$. Supponiamo senza perdere di generalità che $f_t \in I$, allora $fg - (f_t g_0 + \ldots + f_t g_s) \in I$ perché I è chiuso rispetto alla somma, ma $fg - (f_t g_0 + \ldots + f_t g_s) = (f_0 + \ldots + f_{t-1})(g_0 + \ldots + g_s) \in I$, e per ipotesi induttiva si ha che uno dei due fattori appartiene ad I, cioè $(f_0 + \ldots + f_{t-1}) \in I$ o $(g_0 + \ldots + g_s) \in I$. Nel primo caso si ottiene che $f = (f_0 + \ldots + f_{t-1}) + f_t \in I$, mentre nell'altro che $g \in I$. $\square$

2.2 Corrispondenze V, $\mathfrak{I}$ e Nullstellensatz omogeneo

Come nel caso affine, il nostro scopo è ora quello di definire le corrispondenze V ed $\mathfrak{I}$ nel caso proiettivo.

Osservazione 2.2.1. Poniamoci ad esempio in $\mathbb{P}^3_{\mathbb{C}}$ e consideriamo il polinomio $f \in k[t_0, t_1, t_2, t_3]$ con $f = t_0^2 - 2t_3$.
Ponendo $V(f) = \{P \in \mathbb{P}^3_{\mathbb{C}} \mid f(P) = 0\}$ bisogna fare attenzione che $f(P) = 0$ si intenda come nella Definizione 1.4.1. Nel nostro caso il punto $Q = [1, 1, 1, \frac{1}{2}]$ sembrerebbe appartenere all'insieme $V(f)$ visto che annulla f ma Q in $\mathbb{P}^3_{\mathbb{C}}$ può essere scritto anche come $[2, 2, 2, 1]$ e sostituendo queste coordinate in f risulterebbe $4 - 2 = 2 \neq 0$, cioè $Q \notin V(f)$.

Per poter definire la corrispondenza V nel caso proiettivo in maniera corretta occorre quindi lavorare solo con alcuni ideali.

Osservazione 2.2.2. Osserviamo che, se f un polinomio omogeneo in $k[t_0, \ldots, t_n]$ e $P \in \mathbb{P}^n_k$ un punto di coordinate $P = [\xi_0, \ldots, \xi_n]$ e $f(\xi_0, \ldots, \xi_n) = 0$, allora per la Proposizione 1.4.2 si ha $f(\lambda\xi_0, \ldots, \lambda\xi_n) = 0 \quad \forall \lambda \in k$.

Definiamo quindi la corrispondenza V come l'applicazione

$$\begin{array}{ccc} \{\text{ideali omogenei } J \subseteq k[t_0, \dots, t_n]\} & \longrightarrow & \{\text{sottoinsiemi } X \subseteq \mathbb{P}^n_k\} \\ J & \longmapsto & V(J) \end{array}$$

dove $V(J) = \{P \in \mathbb{P}^n_k \quad | \quad f(P) = 0 \quad \forall f \in J\}$, ossia l'insieme dei punti dello spazio proiettivo che annullano ogni polinomio appartenente all'ideale J.
Sappiamo inoltre che un ideale è omogeneo se e solo se esso può essere generato da polinomi omogenei (vedi Prop. 2.1.3). Questo fatto, insieme all'Osservazione 2.2.1, ci permette di dire che la definizione di V è ben posta.

Definizione 2.2.3. Diciamo che un sottoinsieme Y di $\mathbb{P}^n_k$ è *algebrico* se $Y = V(I)$ per qualche I ideale omogeneo di $k[t_0, \dots, t_n]$.

Osservazione 2.2.4. Ricordiamo che l'anello $k[t_0, \dots, t_n]$ è noetheriano quindi per ogni ideale in esso si può trovare un numero finito di generatori, ossia $J = (f_1, \dots, f_t)$, e poiché un ideale è omogeneo se e solo se esso può essere generato da polinomi omogenei (vedi Prop. 2.1.3), possiamo sempre assumere di trovare un insieme di generatori finito per J, $g_1, \dots, g_l$, formato da polinomi omogenei (i g_i potrebbero per esempio essere le componenti omogenee di tutti gli f_j).
In conclusione un insieme algebrico $Y \subseteq \mathbb{P}^n_k$ è il *luogo di zeri* di un numero finito di polinomi omogenei.

Definizione 2.2.5. Sia $Y \subseteq \mathbb{P}^n_k$ un insieme algebrico non vuoto. Diciamo che Y è *irriducibile* se $Y = Y_1 \cup Y_2$, con Y_1 e Y_2 algebrici, implica che $Y_1 = Y$ oppure $Y_2 = Y$. Come nel caso affine, un insieme algebrico si definisce irriducibile se non si può scrivere come unione di insiemi algebrici strettamente contenuti in Y.

Definizione 2.2.6. Una *varietà proiettiva* X di $\mathbb{P}^n_k$ è un sottoinsieme algebrico irriducibile di $\mathbb{P}^n_k$.

Definiamo ora analogamente al caso affine la corrispondenza $\mathfrak{I}$ come l'applicazione

$$\begin{array}{ccc} \{\text{sottoinsiemi algebrici } Y \subseteq \mathbb{P}^n_k\} & \longrightarrow & \{\text{ideali omogenei } J \subseteq k[t_0, \dots, t_n]\} \\ Y & \longmapsto & \mathfrak{I}(Y) \end{array}$$

dove $\mathfrak{I}(Y) = \{f \in k[t_0, \dots, t_n] \quad | \quad f(P) = 0, \quad \forall P \in Y\}$; per quanto detto nelle pagine precedenti, essendo il campo k infinito, $\mathfrak{I}(Y)$ è un ideale omogeneo perché se $f \in \mathfrak{I}(Y)$ allora tutte le componenti omogenee di f devono stare in $\mathfrak{I}(Y)$.

Concludiamo il capitolo con il *Teorema degli zeri di Hilbert*, o Nullstellensatz, nel caso proiettivo:

Lemma 2.2.7. Sia $I \in k[t_0, \dots, t_n]$ ideale omogeneo, e sia $I_s = (t_0, \dots, t_n)^s$. Si ha che $V(I) = \emptyset$ se e solo se $I_s \subseteq I$ per qualche $s > 0$.

Dimostrazione.
$\Longrightarrow$) Sia $I = (f_1, \dots, f_r)$ omogeneo, tale che $V(I) = \emptyset$. Questo significa che i polinomi deomogeneizzati rispetto alla prima variabile $f_i(1, z_1, \dots, z_n)$ non hanno radici in comune, dove $z_i = t_i/t_0$. Quindi $V(f_1(1, z_1, \dots, z_n), \dots, f_r(1, z_1, \dots, z_n)) = \emptyset$ e dal Nullstellensatz segue che $(f_1(1, z_1, \dots, z_n), \dots, f_r(1, z_1, \dots, z_n)) = (1)$, e cioè che 1 si può scrivere come combinazione degli $f_i(1, z_1, \dots, z_n)$; quindi

$$\sum_{i=1}^{r} f_i(1, z_1, \dots, z_n) g_i(z_1, \dots, z_n) = 1$$

è uguale a

$$\sum_{i=1}^{r} f_i(1, t_1/t_0, \dots, t_n/t_0) g_i(t_1/t_0, \dots, t_n/t_0) = 1$$

che è a sua volta equivalente ad una scrittura del tipo

$$\sum_{i=1}^{r} \frac{f_i(t_0, t_1, \dots, t_n)\tilde{g}_i(t_1, \dots, t_n)}{t_0^l} = 1$$

con l opportuno (moltiplicando se necessario per $(t_0/t_0)^{b_i}$ come da osservazione 1.4.6). Ottenendo quindi

$$\sum_{i=1}^{r} f_i(t_0, t_1, \dots, t_n)\tilde{g}_i(t_1, \dots, t_n) = t_0^l$$

A seconda della variabile t_i per cui si decide di deomogeneizzare il polinomio, otterremo che tale t_i elevato ad un esponente l_i è uguale ad una combinazione dei generatori di I, e quindi scegliendo l_{max} esponente massimo tra questi sicuramente $t_j^{l_{max}} \in I$ per ogni j; allora per un opportuno s, si ha che $I_s \subseteq I$.

$\Longleftarrow$) Sia $I_s \subseteq I$ per qualche $s > 0$; allora per le proprietà della V si ha che $V(I_s) \supseteq V(I)$. Ma $V(I_s) = \{[t_0, \ldots, t_n] \in \mathbb{P}_k^n \mid f([t_0, \ldots, t_n]) = 0 \ \forall f \in I_s\} = \emptyset$, dunque $V(I) = \emptyset$. □

Teorema 2.2.8 (Nullstellensatz)**.** Sia Y un sottoinsieme algebrico non vuoto di $\mathbb{P}_k^n$ tale che $Y = V(I)$, con I ideale omogeneo di $k[t_0, \ldots, t_n]$. Allora $\mathfrak{I}(V(I)) = \sqrt{I}$.

Dimostrazione. Indichiamo con V la corrispondenza nel caso proiettivo e con $\tilde{V}$ quella nel caso affine:

$$V(I) = \{[x_o, \ldots, x_n] \in \mathbb{P}_k^n \mid f([x_o, \ldots, x_n]) = 0 \ \forall f \in I\}$$

$$\tilde{V}(I) = \{(x_o, \ldots, x_n) \in \mathcal{A}_k^{n+1} \mid f(x_o, \ldots, x_n) = 0 \ \forall f \in I\}$$

Poiché I è omogeneo, esso può essere generato da polinomi omogenei; $I = (f_1, \ldots, f_r)$.
Prendiamo $P \in \tilde{V}(I)$ diverso dallo 0, allora $[P]$ appartiene a $V(I)$, infatti $f_j(P) = 0 \ \forall j = 1, \ldots, r$, ma poiché gli f_j sono omogenei, si ha che $\forall \lambda \neq 0,\ f_j(\lambda P) = 0$. Questo significa che se un punto Q sta in $\tilde{V}(I)$, allora tutti i punti della retta che passa per $(0, \ldots, 0)$ e Q stanno in $\tilde{V}(I)$, ovvero $[P] \in V(I)$.
Come in precedenza, chiamiamo $\mathfrak{I}$ la corrispondenza nel caso proiettivo, e $\tilde{\mathfrak{I}}$ quella nel caso affine:

$$\mathfrak{I}(V(I)) = \{f \in k[t_0, \ldots, t_n] \mid f([t_0, \ldots, t_n]) = 0 \ \forall [t_0, \ldots, t_n] \in V(I)\}$$

$$\tilde{\mathfrak{I}}(\tilde{V}(I)) = \{f \in k[t_0, \ldots, t_n] \mid f(t_0, \ldots, t_n) = 0 \ \forall t_0, \ldots, t_n \in \tilde{V}(I)\}$$

Essendo il radicale di un ideale omogeneo anch'esso omogeneo e sapendo che $\mathfrak{I}(V(I))$ deve essere omogeneo, in entrambi i casi possiamo cercare un insieme di generatori per questi due ideali che sia formato da elementi omogenei. Ma, per quanto notato prima, i polinomi omogenei che si annullano nei punti di $V(I)$ si annullano anche nei punti di $\tilde{V}(I)$ e viceversa.
Dunque per il Nullstellensatz affine si ha: $\sqrt{I} = \tilde{\mathfrak{I}}(\tilde{V}(I)) = \mathfrak{I}(V(I))$. □

Unito al lemma 2.2.7 questo risultato può essere riformulato come segue:

Teorema 2.2.9. Si ha una corrispondenza biunivoca tra lo spazio degli insiemi algebrici proiettivi di $\mathbb{P}^n_k$ e lo spazio degli ideali omogenei radicali di $k[t_0 \ldots, t_n]$ a patto che da quest'ultimo si elimini l'ideale $(t_0, \ldots, t_n)$.

Capitolo 3

Funzioni e mappe

Ricordiamo che stiamo lavorando su un campo algebricamente chiuso.

3.1 Caso affine

Definizione 3.1.1. Sia X un chiuso in $\mathcal{A}_k^n$ e sia $F: \ X \longrightarrow k$ una funzione. F si dice *regolare* se esiste un polinomio $f \in k[t_1, \ldots, t_n]$ tale che $F(x) = f(x)$ per ogni $x \in X$.

L'insieme delle funzioni regolari su un dato insieme chiuso X forma una k-algebra con le comuni definizioni di somma, prodotto e moltiplicazione per scalare tra funzioni. Tale anello viene denotato con $k[X]$ e viene chiamato *anello delle coordinate di X.*
Consideriamo ora l'omomorfismo π tra $k[t_1, \ldots, t_n]$ e $k[X]$ che ad un certo polinomio f associa la funzione regolare $F = f|_X$; esso è chiaramente suriettivo.
Il nucleo di tale omomorfismo è $ker\pi = \{f \in k[t_1, \ldots, t_n] \mid f(x) = 0 \ \forall x \in X\}$, che non è altro che $\mathfrak{I}(X)$.
Applicando il Teorema Fondamentale di Omomorfismo di Anelli si ottiene

$$k[X] \cong k[t_1, \ldots, t_n]/\mathfrak{I}(X)$$

cioè l'ideale $\mathfrak{I}(X)$ ci permette di determinare l'anello delle coordinate $k[X]$.

Esempio 3.1.2. Supponiamo che l'insieme X sia dato solamente dal punto $P = (a_1, \ldots, a_n)$, allora $\mathfrak{I}(X) = (t_1 - a_1, \ldots, t_n - a_n)$. Passiamo al quoziente:

$k[t_1, \ldots, t_n]/(t_1 - a_1, \ldots, t_n - a_n)$ e vediamo che $[t_1 - a_1] = [0]$ cioè $[t_1] = [a_1]$, ossia nel quoziente possiamo identificare ogni variabile ad una particolare costante. Quindi $k[t_1, \ldots, t_n]/\mathfrak{I}(X) \cong k$, concludendo che $k[X] \cong k$.
Si può arrivare alla stessa conclusione passando per la definizione di funzione regolare, e cioè $F(x) = f(x)$ per ogni $x \in X$ con f polinomio. Nel nostro caso X è dato solo da un punto, quindi F non è nient'altro che la restrizione di f al punto P, $F = f|_P$, che corrisponde a valutare f in $(a_1, \ldots, a_n)$. Le differenti funzioni regolari sono quindi tutti i possibili valori in k.

Esempio 3.1.3. Se $X = \mathcal{A}^n_k$, si ha che $\mathfrak{I}(X) = (0)$. Quindi

$$k[t_1, \ldots, t_n]/(0) = k[t_1, \ldots, t_n] \cong k[X]$$

.

Esempio 3.1.4. Sia $X \in \mathcal{A}^2_k$ dato dall'equazione $t_1t_2 = 1$. Allora $\mathfrak{I}(X) = (t_1t_2 - 1)$ e nel quoziente $k[t_1, t_2]/(t_1t_2 - 1)$ si ha $[t_1][t_2] = [1]$, cioè $[t_1] = [t_2]^{-1}$. Quindi $k[t_1, t_2]/\mathfrak{I}(X) \cong k[t_1, t_1^{-1}]$.

Abbiamo visto in precedenza che esiste un omomorfismo suriettivo tra $k[t_1, \ldots, t_n]$ e $k[X]$ e per questo $k[X]$ è isomorfo al quoziente $k[t_1, \ldots, t_n]/\mathfrak{I}(X)$. Poiché $k[t_1, \ldots, t_n]$ è noetheriano, allora lo è anche $k[X]$ e quindi possiamo dire che anche per $k[X]$ vale il Teorema della Base di Hilbert e concludere che ogni ideale in $k[X]$ è finitamente generato. Inoltre l'insieme algebrico X soddisfa anche un analogo caso di Nullstellensatz:

Teorema 3.1.5. Sia F una funzione in $k[X]$ e $X \subseteq \mathcal{A}^n_k$ insieme algebrico. Se $F(a) = 0$ in ogni punto $a \in X$ sul quale si annullano le funzioni $G_1 = \ldots = G_m$, con $G_i \in k[X]$ allora $F^r \in (G_1, \ldots, G_m)$ per un qualche $r > 0$.

Dimostrazione. Ricordiamo che $\pi : \ k[t_1, \ldots, t_n] \longrightarrow k[t_1, \ldots, t_n]/\mathfrak{I}(X) \cong k[X]$ è la proiezione canonica sul quoziente ed è suriettiva. Prese $G_1, \ldots, G_m \in k[X]$ esistono $g_1, \ldots, g_m \in k[t_1, \ldots, t_n]$ tali che $\pi(g_i) = G_i$. Sia X dato da $f_1, \ldots, f_l$, cioè $X = V(f_1, \ldots, f_l)$ e sia $Y = V(g_1, \ldots, g_m, f_1, \ldots, f_l)$; esso è contenuto in X. Data $F \in k[X]$ tale che $F(P) = 0$ per ogni $P \in Y$, dobbiamo mostrare che esiste $r > 0$ per cui

$F^r \in (G_1, \ldots, G_m)$. Per ipotesi esiste $f \in k[t_1, \ldots, t_n]$ tale che $\pi(f) = F$. Se $a \in Y$ allora $F(a) = 0$, dunque sicuramente a annulla anche f. Per il Nullstellensatz si ha che $f \in \mathfrak{I}(V(g_1, \ldots, g_m, f_1, \ldots, f_l))$ e quindi esiste $t > 0$ tale che $f^t \in (f_1, \ldots, f_l, g_1, \ldots, g_m)$. Applicando la π si ottiene $F^t \in (\pi(f_1), \ldots, \pi(f_l), \pi(g_1), \ldots, \pi(g_m)) = (0, \ldots, 0, G_1, \ldots, G_m) = (G_1, \ldots, G_m)$.

□

Osservazione 3.1.6. Sia $Y \subseteq X$ e sia $f \in \mathfrak{I}(Y)$; sia F la funzione nell'anello delle coordinate $k[X]$ definita da f mediante l'omomorfismo π precedentemente definito. Allora l'insieme delle $F \in k[X]$ definite da $f \in \mathfrak{I}(Y)$ forma un insieme, $\mathfrak{A}_Y$ che coincide con $\{F \in k[X] \mid F(P) = 0 \; \forall P \in Y\}$, che è chiaramente un ideale.
Si ha che $Y = \emptyset$ se e solo se $\mathfrak{I}(Y) = k[t_1, \ldots, t_n]$ che è equivalente a dire che $\mathfrak{A}_Y = k[X]$. Inoltre se $Y = \{P\}$ con $P = (a_1, \ldots, a_n)$, si ha che $\pi(\mathfrak{I}(P))$ corrisponde all'ideale $\mathfrak{A}_P = \{F \in k[X] \mid F(P) = 0\} = \pi(x_1 - a_1, \ldots, x_n - a_n)$. Sia $\psi : \; k[X] \longrightarrow k$ il morfismo di valutazione che associa ad F il suo valore calcolato in P, questa funzione è chiaramente suriettiva. Il nucleo di questo morfismo è $ker\psi = \{F \in k[X] \mid F(P) = 0\} = \mathfrak{A}_P$. Ma allora il quoziente $k[X]/\mathfrak{A}_P$ è isomorfo a k, e poiché k è un campo, $\mathfrak{A}_P$ è un ideale massimale.

Passiamo ora al caso delle mappe, ossia di funzioni tra due insiemi algebrici:

Definizione 3.1.7. Siano $X \subseteq \mathcal{A}_k^n$ e $Y \subseteq \mathcal{A}_k^m$ due insiemi algebrici. Una funzione $F : \; X \longrightarrow Y$ si definisce *mappa regolare* se esistono $F_1, \ldots, F_m \in k[X]$ funzioni regolari tali che $F(x) = (F_1(x), \ldots, F_m(x)) \in Y$ per ogni $x \in X$.

Esempio 3.1.8. Sia X dato dall'equazione $x^3 - y^2 = 0$, cioè $X = V(x^3 - y^2) = \{(x, y) \in \mathcal{A}_k^2 \mid x^3 = y^2\}$ e sia F la seguente mappa:

$$\begin{array}{rccc} F : & \mathcal{A}_k^1 & \longrightarrow & X \\ & t & \longmapsto & (t^2, t^3) \end{array}$$

Essa è una mappa regolare della retta $\mathcal{A}_k^1$ alla curva $x^3 = y^2$, infatti per ogni $t \in \mathcal{A}_k^1$ si ha che $F(t) = (t^2, t^3)$, quindi $(t^2)^3 - (t^3)^2 = 0$ e cioè appartiene ad X.

Definizione 3.1.9. Sia $F : \; X \longrightarrow Y$ una mappa regolare; F è un *isomorfismo* se esiste $G : \; Y \longrightarrow X$ mappa regolare tale che $F \circ G = id_Y$ e $G \circ F = id_X$. In questo caso diremo che X ed Y sono isomorfi e scriveremo $X \cong Y$

Proposizione-Definizione 3.1.10. Sia $F: X \longrightarrow Y$ una mappa regolare. Data u funzione regolare su Y si può definire $v(x) = u(F(x))$. v così definita risulta essere una funzione regolare su X.. Poniamo $v = F^*(u)$ e chiamiamo F^* il *pullback* di u. F^* è una mappa tra le funzioni regolari di Y e le funzioni regolari di X, cioè $F^*: k[Y] \longrightarrow k[X]$. Questa mappa è un omomorfismo di anelli.

Dimostrazione. Sia $F: X \longrightarrow Y$ regolare, $F = (F_1, \ldots, F_m)$ con $F_i \in k[X]$ tali che $F_i = \pi(f_i)$ dove $f_i \in k[t_1, \ldots, t_n]$. Sia inoltre $u \in k[Y]$ regolare, allora esiste $g(z_1, \ldots, z_m) \in k[z_1, \ldots, z_m]$ tale che $\pi(g) = u$. Ora la $v = F^*(u)$ si ottiene semplicemente sostituendo $f_1, \ldots, f_m$ a $z_1, \ldots, z_m$ in g, cioè $g(f_1(t_1, \ldots, t_n), \ldots, f_m(t_1, \ldots, t_n))$. Abbiamo quindi ottenuto un polinomio in $k[t_1, \ldots, t_n]$ che, mediante la π, è uguale a v. $\square$

Dimostriamo qui di seguito un importante risultato:

Teorema 3.1.11. Siano $X \subseteq \mathcal{A}_k^n$ e $Y \subseteq \mathcal{A}_k^m$ due varietà , e siano $k[X]$ e $k[Y]$ i rispettivi anelli delle coordinate. Si ha che $X \cong Y$ se e solo se $k[X] \cong k[Y]$.

Dimostrazione. $\Rightarrow$) Sia $F: X \longrightarrow Y$ un isomorfismo, allora per definizione esiste $G: Y \longrightarrow X$ isomorfismo tale che $F \circ G = id_Y$ e $G \circ F = id_X$. Quindi F^* e G^* sono due applicazioni così definite:

$$F^*: \begin{array}{ccc} k[Y] & \longrightarrow & k[X] \\ v & \longmapsto & v \circ F \end{array} \qquad G^*: \begin{array}{ccc} k[X] & \longrightarrow & k[Y] \\ u & \longmapsto & u \circ G \end{array}$$

Allora la loro composizione è :

$$F^* \circ G^*: \begin{array}{ccc} k[X] & \longrightarrow & k[X] \\ u & \longmapsto & v \circ G \circ F = u \end{array} \qquad G^* \circ F^*: \begin{array}{ccc} k[Y] & \longrightarrow & k[Y] \\ v & \longmapsto & v \circ F \circ G = v \end{array}$$

Cioè $F^* \circ G^* = id_{k[X]}$ e $G^* \circ F^* = id_{k[Y]}$, e dunque sono due isomorfismi.
$\Leftarrow$) Sia $\phi: k[Y] \longrightarrow k[X]$ un isomorfismo di algebre, con $k[Y]$ generata da $t_1, \ldots, t_m$; poniamo inoltre $s_i = \phi(t_i)$. Sia ora $F: X \longrightarrow \mathcal{A}_k^m$ la mappa che ad $x \in X$ associa $F(x) = (s_1(x), \ldots, s_m(x))$; essa è regolare. Mostriamo che $F(X) \subseteq Y$: prendiamo $h \in \mathfrak{I}(Y)$ allora per ogni $x \in X$ si ha che $h(F(x)) = h(s_1(x), \ldots, s_m(x)) = h((\phi(t_1)(x), \ldots, \phi(t_m)(x)),$ d'altra parte quest'ultima espressione è uguale a $\phi(h)(x)$, ma $\phi(h) = 0$ e quindi $F(x) \in Y$. Dunque abbiamo mostrato che F è una mappa regolare da X a Y e quindi ϕ è del tipo

F^*.
Il fatto che questa mappa regolare sia un isomorfismo deriva dal fatto che la stessa ϕ è un isomorfismo, e quindi dotato di un inversa che indurrà l'inversa di F. □

Questo teorema appena dimostrato, definisce una equivalenza tra i sottoinsiemi chiusi dello spazio affine e tra una certa categoria di algebre della forma $k[X]$. Vediamo qui di seguito quali sono tali algebre:

Teorema 3.1.12. Sia A un'algebra su un campo k. Si ha che $A \cong k[X]$, con $X \subseteq \mathcal{A}_k^n$ insieme algebrico, se e solo se A non ha nilpotenti non nulli ed è finitamente generata.

Dimostrazione.
$\Rightarrow$) Sappiamo che $A = k[X] = k[t_1, \ldots, t_n]/\mathfrak{I}(X)$. $k[t_1, \ldots, t_n]$ è un'algebra finitamente generata e quindi lo è anche il quoziente $k[t_1, \ldots, t_n]/\mathfrak{I}(X)$. Inoltre $\mathfrak{I}(X)$ è un ideale radicale, dunque contiene le potenze dei suoi elementi, perciò il quoziente $k[t_1, \ldots, t_n]/\mathfrak{I}(X)$ non contiene elementi nilpotenti diversi dallo 0.
$\Leftarrow$) Supponiamo A finitamente generata; questo significa che esiste un omomorfismo suriettivo da $k[t_1, \ldots, t_n]$ ad A e quindi $A \cong k[t_1, \ldots, t_n]/I$ con I ideale in $k[t_1, \ldots, t_n]$. I essendo un ideale in un anello noetheriano è finitamente generato, supponiamo $I = (f_1, \ldots, f_m)$ e consideriamo l'insieme X definito dalle equazioni $f_1 = \ldots = f_m = 0$. Otteniamo quindi $\sqrt{I} = \mathfrak{I}(X)$. Sicuramente, $I \subseteq \mathfrak{I}(X)$. Vediamo che vale anche il contrario: se $f \in \mathfrak{I}(X)$ allora si ha che esiste un $r > 0$ tale che $f^r \in I$, ma poiché A non contiene elementi nilpotenti non nulli, f deve appartenere ad I. Quindi $I \supseteq \mathfrak{I}(X)$ e allora vale l'uguaglianza $I = \mathfrak{I}(X)$. Questo significa che $A \cong k[t_1, \ldots, t_n]/\mathfrak{I}(X) = k[X]$. □

Nel Capitolo 1, sezione Varietà affini, abbiamo ricordato che un sottoinsieme algebrico X è irriducibile se esso non può essere scritto come unione di due sottoinsiemi algebrici entrambi strettamente contenuti. Ora vogliamo vedere come questa caratteristica è collegata all'anello delle coordinate $k[X]$.

Proposizione 3.1.13. Sia X un sottoinsieme algebrico di $\mathcal{A}_k^n$. Le tre seguenti affermazioni sono equivalenti:

1. X è irriducibile

2. $k[X]$ non ha zero divisori diversi da zero

3. $\mathfrak{I}(X)$ è un ideale primo

Dimostrazione. 1. $\Rightarrow$ 2. Supponiamo che $k[X]$ abbia due zero divisori non nulli, siano essi F_1, F_2 tali che $F_1F_2 = 0$. Chiamo X_1, X_2 i sottoinsiemi di X che corrispondono rispettivamente agli ideali $(F_1), (F_2)$ in $k[X]$, cioè ogni X_i è l'insieme degli $x \in X$ tali che $F_i(x) = 0$. Poiché $F_i \neq 0$ in X allora $X_i \not\subseteq X$, e poiché $F_1F_2 = 0$ in X allora $X = X_1 \cup X_2$, cioè ogni punto $x \in X$ è tale che $F_1(x) = 0$ oppure $F_2(x) = 0$. Si ha quindi un assurdo sull'irriducibilità di X.
2. $\Rightarrow$ 1. Supponiamo per assurdo che X sia riducibile, cioè $X = X_1 \cup X_2$ con $X_1, X_2 \subset X$. Allora esistono due elementi $F_1, F_2 \in k[X]$, più precisamente $f_1 \in \mathfrak{I}(X_1)$ e $f_2 \in \mathfrak{I}(X_2)$ tali che f_1 si annulli su X_1 ma non sia completamente nullo su X_2 e viceversa per f_2. Il loro prodotto f_1f_2 è chiaramente nullo su tutto X, ma ciò sarebbe un assurdo in quanto avremmo due zero divisori non nulli.
2. $\iff$ 3. Sappiamo che un anello senza zero divisori non nulli è un dominio, ma un quoziente è un dominio se e solo se l'ideale è primo. □

Osservazione 3.1.14. Una ipersuperficie $X \subseteq \mathcal{A}^n_k$ di equazione $f = 0$ è irriducibile se e solo se il polinomio f è irriducibile.
Infatti se f è diversa da zero, f è irriducibile se e solo se (f) è primo.

3.2 Funzioni razionali

Sappiamo che, dato un dominio, possiamo costruire il suo campo dei quozienti. Nel nostro caso abbiamo visto che $k[X]$ è un dominio, vediamo quindi qual è il suo campo dei quozienti:

Definizione 3.2.1. Sia X un sottoinsieme irriducibile di $\mathcal{A}^n_k$ e sia $k[X]$ il suo anello delle coordinate. Allora

$$k(X) = \{F/G;\ F, G \in k[X],\ G \neq 0\}$$

Ogni elemento dell'insieme è detto *funzione razionale su* X e $k(X)$ viene chiamato *campo delle funzioni razionali di* X. Mentre se $X = \mathcal{A}^n_k$ allora $k(X)$ è detto campo delle funzioni razionali e coincide con il campo dei quozienti di $k[t_1, \ldots, t_n]$, ovvero $k(t_1, \ldots, t_n)$.

Proposizione-Definizione 3.2.2. Sia X un sottoinsieme irriducibile di $\mathcal{A}_k^n$; denotiamo con $\mathfrak{O}(X) = \{f = P/Q \text{ con } P, Q \in k[t_1, \ldots, t_n] \text{ e } Q \notin \mathfrak{I}(X)\}$ e con
$\mathfrak{M}(X) = \{P/Q \text{ con } P, Q \in k[t_1, \ldots, t_n],\ P \in \mathfrak{I}(X) \text{ e } Q \notin \mathfrak{I}(X)\}$ i due sottoinsiemi del campo delle funzioni razionali.
$\mathfrak{M}(X)$ è un ideale, mentre $\mathfrak{O}(X)$ è un sottoanello, ed il primo è contenuto nel secondo.

Dimostrazione. Chiaramente $\mathfrak{O}(X)$ è un sottoanello del campo delle funzioni razionali, $\mathfrak{M}(X)$ è banalmente un suo sottoinsieme, mostriamo che è un ideale osservando che per ogni $f \in \mathfrak{M}(X)$ e per ogni $h \in \mathfrak{O}(X)$ si ha: $hf = P/Q \cdot P_1/Q_1 = PP_1/QQ_1$ con $PP_1 \in \mathfrak{I}(X)$ perché è un ideale, e quindi $hf \in \mathfrak{M}(X)$. □

Osservazione 3.2.3. Essendo $\mathfrak{M}(X)$ un ideale, possiamo quozientare $\mathfrak{O}(X)$ con $\mathfrak{M}(X)$: $\mathfrak{O}(X)/\mathfrak{M}(X)$ in questo insieme quoziente ci stanno le funzioni razionali che sono in relazione tra loro se e solo se $f - g \in \mathfrak{M}(X)$ che equivale a dire $P_1/Q_1 - P_2/Q_2 \in \mathfrak{M}(X) \iff \frac{P_1Q_2 - P_2Q_1}{Q_1Q_2} \iff P_1Q_2 - P_2Q_1 \in \mathfrak{I}(X)$. Ma questo non è altro che il campo dei quozienti $k(X)$, quindi concludiamo che $k(X) \cong \mathfrak{O}(X)/\mathfrak{M}(X)$.

Definizione 3.2.4. Una funzione razionale $\phi \in k(X)$ si dice *regolare* in $x \in X$ se essa può essere scritta nella forma $\phi = F/G$ con $F, G \in k[X]$ e $G(x) \neq 0$. Diciamo inoltre che $\phi(x) = F(x)/G(x)$ è il valore di ϕ in x.

Proposizione 3.2.5. Sia $\phi \in k(X)$; se ϕ è regolare in ogni punto di X allora ϕ è una funzione regolare di X, cioè appartiene a $k[X]$.

Dimostrazione. Supponiamo che $\phi \in k(X)$ sia regolare in ogni punto di X, cioè $\forall x \in X$ esistono $F_x, G_x \in k[X]$ tali che $\phi = F_x/G_x$. Considero I l'ideale generato da tutte le G_x; esso è finitamente generato perché $k[X]$ è noetheriano, quindi $I = (G_{x_1}, \ldots, G_{x_r})$. I generatori non hanno uno zero in comune, altrimenti si avrebbe che $G_x(x) = 0$ per qualche x. Quindi $V(I) = \emptyset$ e per il Nullstellensatz si ha che $I = (1)$. Dunque esistono $u_1, \ldots, u_r \in k[X]$ tali che $1 = \sum G_{x_i} u_i$. Moltiplico entrambi i membri per ϕ: $\phi = \sum \phi G_{x_i} u_i = \sum \frac{F_{x_i}}{G_{x_i}} G_{x_i} u_i = \sum F_{x_i} u_i$, cioè $\phi \in k[X]$. □

Proposizione-Definizione 3.2.6. Sia $\phi \in k(X)$, l'insieme dei punti in cui ϕ è regolare è un insieme aperto e diverso dal vuoto. Chiamiamo tale insieme *dominio di definizione di* ϕ.

Dimostrazione. Si vede facilmente che è diverso dal vuoto; infatti ϕ può essere scritta come F/G con $F, G \in k[X]$ e $G \neq 0$, quindi $G(x) \neq 0$ per qualche $x \in X$ e dunque ϕ è regolare in quel punto.
Per provare che tale insieme è aperto, consideriamo tutte le possibili rappresentazioni di $\phi = F_i/G_i$. Per ogni G_i, si ha che l'insieme $X_i \subseteq X$ dei punti in cui $G_i(x) = 0$ è chiuso, e quindi $X \setminus X_i$ è aperto. L'unione di questi aperti è ancora un insieme aperto. $\square$

Definizione 3.2.7. Una *mappa razionale* $\phi : X \longrightarrow Y \subseteq \mathcal{A}_k^m$ è una m-upla di funzioni razionali $\phi_1, \ldots, \phi_m \in k(X)$ tali che $\phi(x) = (\phi_1(x), \ldots, \phi_m(x)) \in Y$ per ogni $x \in X$ in cui $\phi_1, \ldots, \phi_m$ sono regolari. Nei punti in cui $\phi_1, \ldots, \phi_m$ sono regolari la mappa si dice regolare.
Inoltre, detta $\phi(X)$ la sua immagine, se $\phi(X)$ è densa in Y la mappa ϕ si definisce *dominante*.

Proposizione 3.2.8. Siano $\phi_1, \ldots, \phi_m \in k(X)$. Si ha che $\phi_1, \ldots, \phi_m$ definiscono una mappa razionale $\phi : X \longrightarrow Y$ se e solo se $\phi_1, \ldots, \phi_m$ soddisfano tutte le equazioni di Y.

Dimostrazione. $\Rightarrow$) Supponiamo ϕ mappa razionale fatta così :

$$\begin{array}{rccc} \phi : & X & \longrightarrow & Y \\ & x & \longmapsto & (\phi_1(x), \ldots, \phi_m(x)) \end{array}$$

Chiaramente poiché $\phi(x) \in Y$, essa annulla qualunque elemento $u \in \mathfrak{I}(Y)$, ovvero le ϕ_i soddisfano le equazioni di Y.
$\Leftarrow$) Viceversa supponiamo che $\phi_1, \ldots, \phi_m$ soddisfino le equazioni di Y, cioè per ogni $u \in \mathfrak{I}(Y)$ vale $u(\phi_1, \ldots, \phi_m) = 0$. Quindi per ogni $x \in X$ su cui tutte le ϕ_i sono regolari si ha $u(\phi_1(x), \ldots, \phi_m(x)) = 0$ per ogni $u \in \mathfrak{I}(Y)$, cioè $(\phi_1(x), \ldots, \phi_m(x)) \in Y$.

$\square$

3.3 Caso proiettivo

Vediamo ora come poter estendere questi concetti al caso proiettivo.

Sia $X \subseteq \mathbb{P}^n_k$ una varietà proiettiva; vogliamo definire una funzione regolare su X. Ricordiamo la definizione data nel caso affine e supponiamo che valga anche nel caso proiettivo, e cioè una funzione $F: X \longrightarrow k$ è regolare se esiste un polinomio $f \in k[t_0, \ldots, t_n]$ tale che $f(x) = F(x)$ per ogni $x \in X$.
Mostriamo con un controesempio che non è adatta: prendiamo $X \subseteq \mathbb{P}^2_k$ e supponiamo che $F: X \longrightarrow k$ sia una funzione regolare su di esso. Sia $f \in k[t_0, t_1, t_2]$ il polinomio che per ogni punto di X soddisfi l'uguaglianza $f(x) = F(x)$, con $f = t_0^2 + t_1^2 - 2t_2^2$. Se $P \in X$ è un punto di coordinate $[2, 1, 3]$ allora si ha che $f(P) = 2^2 + 1^2 - 2(3^2) = -13 = F(P)$. Sappiamo però che una scrittura equivalente di P è ad esempio $P' = [4, 2, 6]$, quindi $f(P) = f(P') = 4^2 + 2^2 - 2(6^2) = -52 \neq F(P)$. Dunque questa definizione di funzione regolare non è ben definita nel caso proiettivo.
Diamo qui di seguito la corretta definizione.

Definizione 3.3.1. Sia $X \subseteq \mathbb{P}^n_k$ una varietà proiettiva, e sia $F(t_0, \ldots, t_n) = \frac{g(t_0, \ldots, t_n)}{h(t_0, \ldots, t_n)}$ tale che g e h siano polinomi in $k[t_0, \ldots, t_n]$ omogenei dello stesso grado. Sia $x \in X$ con $h(x) \neq 0$, allora F definisce una funzione in un intorno di x. Diciamo quindi che F è *regolare in* x. F si dice *regolare* se è regolare in ogni $x \in X$.

Supponiamo che $deg\ g = deg\ h = d$, allora per ogni punto $P \in X$ si ha $F(\lambda P) = \frac{g(\lambda P)}{h(\lambda P)} = \frac{\lambda^d g(P)}{\lambda^d h(P)} = \frac{g(P)}{h(P)} = F(P)$.

Definizione 3.3.2. Siano $X \subseteq \mathbb{P}^n_k$, $Y \subseteq \mathbb{P}^m_k$ varietà proiettive, e siano $f_0, \ldots, f_m \in k[t_0, \ldots, t_n]$ polinomi omogenei dello stesso grado senza zeri comuni su X. La mappa $\phi : X \longrightarrow \mathbb{P}^m_k$ definita da $\phi([t_0, \ldots, t_n]) = [(f_0(t_0, \ldots, t_n), \ldots, f_m(t_0, \ldots, t_n))]$ è detta *morfismo proiettivo da* X *a* $\mathbb{P}^m_k$. Se l'immagine è contenuta in Y, diremo che è un morfismo (proiettivo) da X a Y.
Diremo che ϕ è un isomorfismo se esiste un morfismo proiettivo $\psi : Y \longrightarrow X$ tale che $\phi \circ \psi = id_Y$, $\psi \circ \phi = id_X$.

Esempio 3.3.3. Un famoso esempio di morfismo proiettivo è dato dall'*embedding di Segre*.

Siano $X \subseteq \mathbb{P}^n$ e $Y \subseteq \mathbb{P}^m$ due varietà proiettive. Vogliamo considerare l'insieme $X \times Y = \{[x, y] \in \mathbb{P}^N \mid x \in X,\ y \in Y\}$ come una varietà proiettiva in $\mathbb{P}^N$ con
$N = (n+1)(m+1) - 1 = nm + n + m$. Per poterlo fare occorre costruire una mappa $\phi:\ X \times Y \longrightarrow \mathbb{P}^N$.
Poniamoci nel caso in cui $X = \mathbb{P}^n$ e $Y = \mathbb{P}^m$ e chiamiamo w_{ij} le coordinate omogenee di $\mathbb{P}^N$ con $i = 0, \dots, n$ e $j = 0, \dots, m$. Definiamo quindi l'*embedding di Segre* come la mappa:

$$\begin{array}{cccc} \phi: & \mathbb{P}^n \times \mathbb{P}^m & \longrightarrow & \mathbb{P}^N \\ & ([x_0, \dots, x_n], [y_0, \dots, y_m]) & \longmapsto & [x_0 y_0, \dots, x_n y_m] \end{array}$$

Tale mappa è chiaramente morfismo proiettivo e la sua immagine viene denominata *varietà di Segre*.

Inoltre essa induce un isomorfismo tra $\mathbb{P}^n \times \mathbb{P}^m$ e $\phi(\mathbb{P}^n \times \mathbb{P}^m)$ e la varietà di Segre corrispondente è definita dal seguente sistema di equazioni:

$$w_{ij} w_{kl} - w_{il} w_{kj} = 0 \quad \forall\, i, k = 0, \dots, n, \ \ \forall j, l = 0, \dots, m \qquad (*)$$

Infatti la mappa di Segre è ben definita e iniettiva: presi due punti $P \in \mathbb{P}^n$ e $Q \in \mathbb{P}^m$ con coordinate rispettivamente uguali a $[a_0, \dots, a_n]$ e $[b_0, \dots, b_m]$, interpretiamo queste ultime come coefficienti di due forme lineari $L_1 = \sum_{i=0}^n a_i t_i$ e $L_2 = \sum_{j=0}^m b_j s_j$. Secondo questa interpretazione, l'immagine è la forma omogenea di grado 2 $L_1 L_2$. Poiché almeno un a_i e un b_j sono diversi da zero, allora sicuramente $L_1 L_2$ non è nullo.
Per l'iniettività si ragiona nel seguente modo: sia $\phi(x, y) = \phi(z, t)$ con $x = [x_0, \dots, x_n]$, $y = [y_0, \dots, y_m]$, $z = [z_0, \dots, z_n]$ e $t = [t_0, \dots, t_m]$. Notiamo anzitutto che $x_0 = 0$ se e solo se $z_0 = 0$; infatti se $x_0 = 0$ si avrebbe $0 = z_0 t_j$ per ogni $j = 0, \dots, m$, che è possibile solo se $z_0 = 0$. Poniamoci nel caso in cui $x_0 \neq 0$, e scriviamo $x = [1, x_1/x_0, \dots, x_n/x_0]$ analogamente $z = [1, z_1/z_0, \dots, z_n/z_0]$: si ha quindi per ipotesi che $x_0 y_j = z_0 t_j$ per ogni j e cioè $y_j = t_j$, concludendo che $y = t$. Procedendo al contrario si mostra che $x = z$ e quindi $(x, y) = (z, t)$.

Proviamo infine che l'insieme algebrico definito da (*) coincide proprio con la varietà di Segre. Chiaramente i punti della varietà di Segre soddisfano le equazioni; viceversa vediamo che un punto che soddisfa quelle equazioni sia proprio l'immagine tramite ϕ di un qualche $(x, y) \in \mathbb{P}^n \times \mathbb{P}^m$. Supponiamo che la prima coordinata del punto sia non nulla, possiamo quindi scrivere $w = [1, w_{01}, \ldots, w_{nm}]$; allora dal sistema di equazioni si ottiene $w_{ij} = w_{i0}w_{0j}$ per $i = 0, \ldots, n$ e $j = 0, \ldots, m$. Ma esso corrisponde proprio a $\phi(x, y)$ dove $x = [1, w_{10}, \ldots, w_{n0}]$ e $y = [1, w_{01}, \ldots, w_{0m}]$.

Questo embedding ci permette di dare una struttura di varietà proiettiva all'insieme $\mathbb{P}^n \times \mathbb{P}^m$ identificando quest'ultimo con la varietà di Segre.
Vediamo il caso in cui $n = m = 1$; allora la mappa di Segre corrispondente è :

$$\begin{array}{cccc} \phi : & \mathbb{P}^1 \times \mathbb{P}^1 & \longrightarrow & \mathbb{P}^3 \\ & ([x_0, x_1], [y_0, y_1]) & \longmapsto & [x_0y_0, x_0y_1, x_1y_0, x_1y_1] \end{array}$$

e la sua immagine $\phi(\mathbb{P}^1 \times \mathbb{P}^1)$ è la superficie di equazione $xt = yz$, dove x, y, z, t si intendono come coordinate di $\mathbb{P}^3_k$.
Questa superficie ha l'interessante proprietà di contenere due famiglie di rette dove, prese due rette distinte appartenenti allo stessa famiglia esse non si intersecano mai, mentre due rette appartenenti a famiglie diverse sono sempre incidenti. Per costruire queste famiglie basta fissare $[a, b] \in \mathbb{P}^1$ e fare l'immagine della retta $[a, b] \times \mathbb{P}^1$ tramite la mappa di Segre, ottenendo così :

$$\phi([a, b], [t_0, t_1]) = [at_0, at_1, bt_0, bt_1].$$

Notiamo che le equazioni cartesiane di questa retta sono date da

$$\begin{cases} bx = az \\ by = at \end{cases}$$

Al variare di $[a, b] \in \mathbb{P}^1$ si ottiene la prima famiglia di rette; la seconda si ottiene facendo l'immagine delle rette $\mathbb{P}^1 \times [a, b]$.

3.4 La mappa di Veronese

Un altro importante esempio di morfismo proiettivo è dato dall'embedding di Veronese.
Definiamo l'insieme $\mathcal{I} = \{(i_0, \ldots, i_n) \in \mathbb{N}^{n+1} \mid \sum_{j=0}^{n} i_j = m\}$; esso ha cardinalità $\binom{n+m}{m}$ e corrisponde al numero di tutti i monomi di grado m in $n+1$ variabili.
Sia $q = \binom{n+m}{m} - 1$ e considero $\mathbb{P}^q$
La *mappa di Veronese*, o *embedding di Veronese* si definisce nel modo seguente:

$$\begin{array}{cccc} \mathcal{V}_m : & \mathbb{P}^n & \longrightarrow & \mathbb{P}^q \\ & [x_0, \ldots, x_n] & \longmapsto & [x_0^m, x_0^{m-1}x_1, \ldots, x_n^m] \end{array}$$

Questa è chiaramente un morfismo proiettivo, infatti la q-pla $(x_0^m, x_0^{m-1}x_1, \ldots, x_n^m)$ include in particolare gli elementi del tipo x_i^m che si annullano contemporaneamente solo se sono tutti uguali a zero.
L'immagine del morfismo di Veronese $\mathcal{V}_m(\mathbb{P}^n) \subseteq \mathbb{P}^q$ viene chiamata *varietà di Veronese.*

Proposizione 3.4.1. Sia $\mathcal{V}_m : \mathbb{P}^n \longrightarrow \mathbb{P}^q$ un embedding di Veronese; l'applicazione $\mathcal{V}_m : \mathbb{P}^n \longrightarrow \mathcal{V}_m(\mathbb{P}^n)$ è un isomorfismo e la varietà $\mathcal{V}_m(\mathbb{P}^n)$ è definita dal seguente sistema di equazioni:

$$y_{i_0 \ldots i_n} y_{j_0 \ldots j_n} = y_{k_0 \ldots k_n} y_{l_0 \ldots l_n}, \qquad i_h + j_h = k_h + l_h \qquad \forall h = 0, \ldots, n \qquad (*)$$

.

Dimostrazione. Per una dimostrazione rigorosa si rimanda a [3].
Per prima cosa mostriamo che il morfismo di Veronese è ben definito: sia $P \in \mathbb{P}^n$ un punto di coordinate $(a_0, \ldots, a_n)$ ed interpretiamo queste ultime come i coefficienti di una forma lineare $L = \sum_{i=0}^{n} a_i x_i$, la quale è ben definita in quanto almeno un a_i è diverso da zero. Quindi le coordinate di $\mathcal{V}_m(P)$ sono i coefficienti del polinomio omogeneo L^m, a meno di coefficienti binomiali. Poiché $L \neq 0$ allora anche $L^m \neq 0$, dunque $(a_0, \ldots, a_n) \neq 0$ implica che anche le coordinate di $\mathcal{V}_m(P)$ siano diverse da zero.
Proviamo ora che $\mathcal{V}_m$ è iniettiva. Per quanto visto in precedenza, siano P e Q due punti differenti in $\mathbb{P}^n$ e siano L_1 ed L_2 due forme lineari che hanno per coefficienti le coordinate rispettivamente di P e Q. Ricordiamo che $k[t_0, \ldots, t_n]$ è un dominio a fattorizzazione

unica e perciò $L_1 \neq L_2$ implica che $L_1^m \neq L_2^m$. Da cui $\mathcal{V}_m$ è iniettiva.
Quindi questa mappa rappresenta un isomorfismo coristretta all'immagine.
Chiaramente l'immagine è formata da punti che soddisfano $(*)$, mentre l'inclusione opposta è un po' più difficile da provare. $\square$

Definizione 3.4.2. Per $n = 1$ e quindi $q = m + 1$, la varietà di Veronese definita dalla mappa $\mathcal{V}_m : \mathbb{P}^1 \longrightarrow \mathbb{P}^{m+1}$ prende il nome di *curva razionale normale.*

Vediamo qualche esempio:

Esempio 3.4.3. Per $n = 1$ e $m = 1$ la mappa di Veronese corrispondente è :

$$\begin{array}{rccc} \mathcal{V}_1 : & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ & [x_0, x_1] & \longmapsto & [x_0, x_1] \end{array}$$

che è banalmente l'identità sulla retta proiettiva.

Poniamo $n = 1$ e $m = 2$, allora $q = 2$. La mappa di Veronese in questo caso è :

$$\begin{array}{rccc} \mathcal{V}_2 : & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^2 \\ & [x_0, x_1] & \longmapsto & [x_0^2, x_0x_1, x_1^2] \end{array}$$

Ponendo $(x_0^2, x_0x_1, x_1^2) = (y_0, y_1, y_2)$ si vede subito che l'immagine della mappa in questione corrisponde alla curva in $\mathbb{P}^2$ di equazione $y_0y_2 = y_1^2$.

Siano ora $n = 1$ e $m = 3$, allora $q = 4$. La mappa di Veronese in tal caso è :

$$\begin{array}{rccc} \mathcal{V}_3 : & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^3 \\ & [x_0, x_1] & \longmapsto & [x_0^3, x_0^2x_1, x_0x_1^2, x_1^3] \end{array}$$

Questa varietà prende il nome di *cubica gobba* ed è parametrizzata dal seguente sistema di equazioni:

$$\begin{cases} y_0 = t^3 \\ y_1 = t^2 s \\ y_2 = ts^2 \\ y_3 = s^3 \end{cases} \qquad (*)$$

con $[t, s] \in \mathbb{P}^1$.

Si può dimostrare che la cubica gobba è intersezione di queste tre quadriche:

$$\begin{cases} y_0y_2 = y_1^2 \\ y_0y_3 = y_1y_2 \\ y_1y_3 = y_2^2 \end{cases} \qquad (**)$$

Infatti sostituendo in $(**)$ i parametri (t, s) alle incognite y_i, si ottiene

$$\begin{cases} t^3ts^2 = (t^2s)^2 \\ t^3s^3 = t^2sts^2 \\ t^2ss^3 = (ts^2)^2 \end{cases}$$

e cioè

$$\begin{cases} t^4s^2 = t^4s^2 \\ t^3s^3 = t^3s^3 \\ t^2s^4 = t^2s^4 \end{cases}$$

Viceversa, sia $P = [a_0, a_1, a_2, a_3] \in \mathbb{P}^3$ appartenente all'intersezione delle tre quadriche $(**)$. Proviamo che P appartiene alla cubica gobba, cioè che P soddifa il sistema di equazioni parametriche $(*)$.

Se $a_0 = 0$ allora sostituendo le coordinate di P in (**): $\begin{cases} 0a_2 = a_1^2 \Rightarrow a_1 = 0 \\ 0a_3 = 0a_2 \\ 0a_3 = a_2^2 \Rightarrow a_2 = 0 \end{cases}$, cioè $P = [0, 0, 0, 1]$. Quindi (*) diventa: $\begin{cases} 0 = t^3 \\ 0 = t^2s \\ 0 = ts^2 \\ 1 = s^3 \end{cases}$, ossia P appartiene alla cubica gobba per $[t, s] = [0, 1]$.

Altrimenti moltiplichiamo P per a_0^2: $[a_0^3, a_0^2a_1, a_0^2a_2, a_0^2a_3]$ e, come prima, sostituiamo le nuove coordinate in (**): $\begin{cases} a_0^5a_2 = a_0^4a_1^2 & \Rightarrow a_0a_2 = a_1^2 \\ a_0^5a_3 = a_0^4a_1a_2 & \Rightarrow a_0a_3 = a_1a_2 \\ a_0^4a_1a_3 = a_0^4a_2^2 & \Rightarrow a_2^2 = a_1a_3 \end{cases}$ da cui si ottiene:

$a_0^2a_3 = a_0a_1a_2 = a_1^3$, $a_0^2a_2 = a_0a_1^2$, quindi le nuove coordinate di P sono $[a_0^3, a_0^2a_1, a_0a_1^2, a_1^3]$ e quindi P appartiene alla cubica gobba per $[t, s] = [a_0, a_1]$.

Esempio 3.4.4. Siano $n = 2$ e $m = 2$, allora $q = 5$ e l'embedding di Veronese che si ottiene è :

$$\begin{array}{rccc} \mathcal{V}_2 : & \mathbb{P}^2 & \longrightarrow & \mathbb{P}^5 \\ & [x_0, x_1, x_2] & \longmapsto & [x_0^2, x_1^2, x_2^2, x_0x_1, x_1x_2, x_0x_2] \end{array}$$

L'immagine di tale mappa viene denominata *superficie di Veronese.*

Capitolo 4

Prodotti tensoriali e introduzione al problema di Waring

4.1 Prodotto tensoriale di moduli

Definiamo di seguito il prodotto tensoriale tra moduli e vediamo alcune sue proprietà utili.

Definizione 4.1.1. Sia R un anello e M, N, P tre R-moduli. L'applicazione $\psi : M \times N \longrightarrow P$ si dice *mappa bilineare di R-moduli* se, per ogni $x, y \in M$, per ogni $z, t \in N$ e per ogni $r \in R$ valgono le seguenti affermazioni:

$$\psi(x + y, z) = \psi(x, z) + \psi(y, z)$$

$$\psi(x, z + t) = \psi(x, z) + \psi(x, t)$$

$$\psi(rx, z) = r\psi(x, z)$$

$$\psi(x, rz) = r\psi(x, z)$$

Proposizione-Definizione 4.1.2. Sia R un anello e M, N due R-moduli. Esiste una coppia (T, ψ), con T R-modulo e ψ applicazione bilineare tale che $\psi : M \times N \longrightarrow T$, per cui vale la proprietà universale seguente:
Per ogni R-modulo P e per ogni applicazione bilineare $\phi : M \times N \longrightarrow P$, esiste

$\xi : \ T \longrightarrow P$ tale che ϕ si fattorizza mediante ψ secondo il seguente diagramma:

$$\begin{tikzcd} M \times N \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & T \arrow[dl, "\xi"] \\ & P & \end{tikzcd}$$

Inoltre se due coppie (T, ψ) e (T', ψ') verificano la proprietà enunciata sopra, si ha che esiste un isomorfismo $f : \ T \longrightarrow T'$ tale che il seguente diagramma commuti:

$$\begin{tikzcd} M \times N \arrow[rr, "\psi"] \arrow[dr, "\psi'"'] & & T \arrow[dl, "f(\cong)"] \\ & T' & \end{tikzcd}$$

L'R-modulo T è denominato *prodotto tensoriale di* M *e* N e viene denotato con $M \otimes_R N$.

Dimostrazione. Vediamo come poter costruire questa struttura appena definita per provare la sua esistenza: siano M e N due R-moduli e sia $R^{M\times N}$ l'R-modulo libero con base $M \times N$. Ogni elemento di $R^{M\times N}$ può essere espresso nella forma $\sum_{i=1}^{n} r_i(x_i, y_i)$ con $r_i \in R$, $x_i \in M$ e $y_i \in N$.
Sia infine S il sottomodulo di $R^{M\times N}$ generato dagli elementi del tipo:

$$(x + y, z) - (x, y) - (x, z)$$

$$(x, z + t) - (x, z) - (x, t)$$

$$(rx, z) - r(x, z)$$

$$(x, rz) - r(x, z)$$

con $x, y \in M$; $\ z, t \in N$ e $r \in R$. Definiamo $T = M \otimes_R N = R^{M\times N}/S$ e scriviamo $x \otimes y$ per la classe (x, y) in $M \otimes_R N$.
Definiamo quindi la mappa ψ come:

$$\begin{array}{rccc} \psi : & M \times N & \longrightarrow & M \otimes_R N \\ & (x, y) & \longmapsto & x \otimes y \end{array}$$

Questa mappa risulta essere bilineare; infatti dalla definizione abbiamo che:

$$(x+y)\otimes z = x\otimes z + y\otimes z$$

$$x\otimes(z+t) = x\otimes z + x\otimes t$$

$$r(x\otimes z) = (rx)\otimes z = x\otimes(rz)$$

per ogni $x, y \in M, \quad z, t \in N$ e $r \in R$.
Vediamo che vale la proprietà universale per la coppia (T, ψ): sia P un R-modulo e $g: M\times N \longrightarrow P$ un'applicazione bilineare. Consideriamo il morfismo

$$\begin{array}{rccc} F: & R^{M\times N} & \longrightarrow & P \\ & (x,y) & \longmapsto & g(x,y) \end{array}$$

Si ha che $S \subseteq ker\ F$; infatti:

- $F((x+y,z)-(x,y)-(x,z)) = F(x+y,z)-F(x,z)-F(y,z) = g(x+y,z)-g(x,z)-g(y,z) = 0$

- $F((x,z+t)-(x,z)-(x,t)) = F(x,z+t)-F(x,z)-F(x,t) = g(x,z+t)-g(x,z)-g(x,t) = 0$

- $F((rx,z)-r(x,z)) = F(rx,z)-rF(x,z) = g(rx,z)-rg(x,z) = 0$

- $F((x,rz)-r(x,z)) = F(x,rz)-rF(x,z) = g(x,rz)-rg(x,z) = 0.$

cioè F si annulla sui generatori di S e quindi su tutto S.
Allora F induce un morfismo α

$$\begin{tikzcd} R^{M\times N} \arrow[rr, "F"] \arrow[dr, "\pi"'] & & P \\ & T \arrow[ur, "\alpha"'] & \end{tikzcd}$$

tale che $\alpha(x \otimes y) = F(x, y) = g(x, y)$, e quindi il seguente diagramma commuta:

$$\begin{tikzcd} M \times N \arrow[r, "\psi"] \arrow[dr, "g"'] & T \arrow[d, "\alpha"] \\ & P \end{tikzcd}$$

Se β è un altro morfismo che fa commutare il diagramma, allora $\beta(\psi(x, y)) = g(x, y)$ per ogni $(x, y) \in M \times N$, quindi α e β coincidono.

Proviamo ora la seconda parte della Proposizione: siano (T, ψ) e (T', ψ') due coppie che soddisfano la proprietà universale. Allora esistono due morfismi ξ e ξ' tali che $\psi' = \xi \circ \psi$:

$$\begin{tikzcd} M \times N \arrow[r, "\psi"] \arrow[dr, "\psi'"'] & T \arrow[d, "\xi"] \\ & T' \end{tikzcd}$$

e $\psi = \xi' \circ \psi'$:

$$\begin{tikzcd} M \times N \arrow[r, "\psi'"] \arrow[dr, "\psi"'] & T' \arrow[d, "\xi'"] \\ & T \end{tikzcd}$$

Quindi $\psi' = \xi \circ \xi' \circ \psi'$ e $\psi = \xi' \circ \xi \circ \psi$, cioè si hanno i due seguenti diagrammi commutativi:

$$\begin{tikzcd} M \times N \arrow[r, "\psi'"] \arrow[dr, "\psi'"'] & T' \arrow[d, "\xi \circ \xi'"] \\ & T' \end{tikzcd}$$

$$\begin{tikzcd} M \times N \arrow[r, "\psi"] \arrow[dr, "\psi"'] & T \arrow[d, "\xi' \circ \xi"] \\ & T \end{tikzcd}$$

ma poiché la proprietà universale dice che tale morfismo è unico, si conclude che $\xi \circ \xi' = id_{T'}$ e che $\xi' \circ \xi = id_T$ e cioè ξ è un isomorfismo.

$\square$

Quando è chiaro l'anello R in questione, scriveremo semplicemente $M \otimes N$ al posto di $M \otimes_R N$.
Con la seguente proposizione enunciamo qualche isomorfismo canonico:

Proposizione 4.1.3. Siano M, N e P tre R-moduli. Allora le seguenti applicazioni sono degli isomorfismi:

1.
$$\begin{array}{ccc} M \otimes N & \longrightarrow & N \otimes M \\ x \otimes y & \longmapsto & y \otimes x \end{array}$$

2.
$$\begin{array}{ccccc} (M \otimes N) \otimes P & \longrightarrow & M \otimes (N \otimes P) & \longrightarrow & M \otimes N \otimes P \\ (x \otimes y) \otimes z & \longmapsto & x \otimes (y \otimes z) & \longmapsto & x \otimes y \otimes z \end{array}$$

3.
$$\begin{array}{ccc} R \otimes M & \longrightarrow & M \\ r \otimes x & \longmapsto & rx \end{array}$$

Dimostrazione. 1. Dimostriamo la commutatività tra i due R-moduli: sia $\psi' : M \times N \longrightarrow M \otimes N$ tale che $\psi'(x, y) = y \otimes x$ e consideriamo il diagramma commutativo

$$\begin{tikzcd} M \times N \arrow[rr, "\psi"] \arrow[dr, "\psi'"'] & & M \otimes N \arrow[dl, "\xi"] \\ & N \otimes M & \end{tikzcd}$$

che esiste poiché ψ' è bilineare. Dunque per la Proposizione precedente esiste una unica mappa ξ tale che

$$\begin{array}{rccc} \xi : & M \otimes N & \longrightarrow & N \otimes M \\ & x \otimes y & \longmapsto & y \otimes x \end{array}$$

Il diagramma simile costruito invertendo i ruoli di $M \otimes N$ e $N \otimes M$ mi garantisce l'esistenza di

$$\begin{aligned} \xi' : \quad N \otimes M &\longrightarrow M \otimes N \\ y \otimes x &\longmapsto x \otimes y \end{aligned}$$

Entrambe le composizioni di ξ e ξ' sono ovviamente l'identità , e dunque concludiamo che $\xi : \ M \otimes N \longrightarrow N \otimes M$ è un isomorfismo.

2. Mostriamo l'associatività dei tre R-moduli: siano

$$(M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} (M \otimes N) \otimes P$$

tali che $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ e $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$ per ogni $x \in M$, $y \in N$ e $z \in P$.

Per costruire f fissiamo z; allora la mappa $M \times N \longrightarrow M \otimes N \otimes P$ che alla coppia (x, y) associa $x \otimes y \otimes z$ è bilineare e quindi induce un omomorfismo

$$\begin{aligned} \bar{f}_z : \quad M \otimes N &\longrightarrow M \otimes N \otimes P \\ x \otimes y &\longmapsto x \otimes y \otimes z \end{aligned}$$

Consideriamo ora la mappa

$$\begin{aligned} h : (M \otimes N) \times P &\longrightarrow M \otimes N \otimes P \\ (t, z) &\longmapsto \bar{f}_z(t) \end{aligned}$$

anch'essa è bilineare in t e z quindi induce un omomorfismo

$$\begin{aligned} f : \quad (M \otimes N) \otimes P &\longrightarrow M \otimes N \otimes P \\ (x \otimes y) \otimes z &\longmapsto x \otimes y \otimes z \end{aligned}$$

Costruiamo ora g: prendiamo la mappa

$$\begin{aligned} l : M \times N \times P &\longrightarrow (M \otimes N) \otimes P \\ (x, y, z) &\longmapsto (x \otimes y) \otimes z \end{aligned}$$

che è lineare in ogni variabile e quindi induce un omomorfismo

$$\begin{aligned} g : \quad M \otimes N \otimes P &\longrightarrow (M \otimes N) \otimes P \\ x \otimes y \otimes z &\longmapsto (x \otimes y) \otimes z \end{aligned}$$

Entrambe le composizioni $f \circ g$ e $g \circ f$ sono l'identità , allora sono due isomorfismi.

3. Infine vediamo la moltiplicazione per scalari: prendiamo il diagramma

$$\begin{tikzcd} R \times M \arrow[r, "\psi"] \arrow[dr, "\psi'"'] & R \otimes M \arrow[d, "\xi"] \\ & M \end{tikzcd}$$

Per definizione sappiamo che $r \otimes x = r(1 \otimes x) = 1 \otimes (rx)$; d'altra parte $\psi'(r,x) = rx$. Dunque l'isomorfismo ξ può essere visto come la proiezione sul secondo fattore.

$\square$

Poniamoci ora nel caso in cui R sia un campo k algebricamente chiuso di caratteristica zero:

Proposizione 4.1.4. Siano $V_1, \ldots, V_n$ spazi vettoriali di dimensione finita rispettivamente $\dim V_i = d_i$, allora lo spazio vettoriale $V_1 \otimes \ldots \otimes V_n$ ha dimensione uguale al prodotto delle dimensioni dei V_i.

Dimostrazione. Dimostriamo questo fatto solo nel caso in cui $n = 2$, poiché la dimostrazione è facilmente estendibile ai casi successivi.
Mostriamo che, date $\mathcal{B}_1 = \{v_1, \ldots, v_{d_1}\}$ e $\mathcal{B}_2 = \{w_1, \ldots, w_{d_2}\}$ basi rispettivamente di V_1 e V_2, $\mathcal{B} = \{v_1 \otimes w_1, \ldots, v_{d_1} \otimes w_{d_2}\}$ è base di $V_1 \otimes V_2$. Chiaramente una scrittura del tipo

$$a_1 \tilde{v}_1 \otimes \tilde{w}_1 + \ldots + a_s \tilde{v}_s \otimes \tilde{w}_s$$

può essere ricondotta ad una combinazione lineare degli elementi di $\mathcal{B}$ tramite le proprietà di linearità del prodotto tensoriale, dunque $\mathcal{B}$ è un insieme di generatori.
Per mostrare che gli elementi sono linearmente indipendenti basta notare che

$$0 = \sum_{i,j} a_{ij} v_i \otimes w_j = \sum_i v_i \otimes (\sum_j a_{ij} w_j)$$

da cui segue che $a_{ij} = 0$.

$\square$

Proposizione-Definizione 4.1.5. Sia $V =< v_1, \ldots, v_n >$ uno spazio vettoriale di dimensione n e sia H il sottospazio di $V \otimes V$ generato dagli elementi del tipo $v \otimes w - w \otimes v$.

Gli elementi dello spazio quoziente $Sym_2(V) := V \otimes V/H$ sono detti *tensori simmetrici.* Inoltre $Sym_2(V)$ è isomorfo a $k[t_1, \dots, t_n]_2$, dove questo è l'anello dei polinomi omogenei di grado 2.

Dimostrazione. Mostriamo anzitutto che la dimensione di $Sym_2(V) = \binom{n+1}{2}$ ovvero pari alla dimensione dei polinomi omogenei di grado 2. Infatti una base per $Sym_2(V)$ è data da $\mathcal{B} = \{v_i \otimes v_j \in Sym_2(V) \mid i \leq j\}$ perché in questo quoziente $v_j \otimes v_i$ con $i \leq j$ è equivalente a $v_i \otimes v_j$. Dunque un isomorfismo definito sugli elementi di una base ed esteso per linearità è :

$$\begin{array}{rccc} \phi : & Sym_2(V) & \longrightarrow & k[t_1, \dots, t_n]_2 \\ & v_i \otimes v_j & \longmapsto & t_i t_j \end{array}$$

□

Nella dimostrazione precedente abbiamo fatto un leggero abuso di notazione utilizzando la scrittura $v_i \otimes v_j$ sia nel caso in cui l'elemento appartenga a $V \otimes V$ che nel caso in cui appartenga a $Sym_2(V)$. In seguito renderemo sempre esplicito l'ambiente in cui si opererà per evitare confusione.

Osservazione 4.1.6. Possiamo estendere questo risultato al caso in cui il prodotto tensoriale sia $\underbrace{V \otimes \dots \otimes V}_{d}$ quozientato con l'opportuno sottospazio generato da tutte le differenze tra due tensori i cui indici differiscono per una permutazione. Esso risulta isomorfo a $k[t_1, \dots, t_n]_d$.

4.2 Problema di Waring e rango di tensori

Poniamoci in un campo k algebricamente chiuso e di caratteristica zero.

Definizione 4.2.1. Siano $V_1, \dots, V_t$ dei sottospazi vettoriali di dimensione finita sul campo k. Allora esiste una funzione così definita:

$$\begin{array}{ccc} V_1 \times \dots \times V_t & \longrightarrow & V_1 \otimes \dots \otimes V_t \\ (v_1, \dots, v_t) & \longmapsto & v_1 \otimes \dots \otimes v_t \end{array}$$

Gli elementi appartenenti all'immagine vengono detti *tensori irriducibili o di rango 1.* In altre parole un tensore irriducibile è un elemento di $V_1 \otimes \ldots \otimes V_t$ che può essere scritto semplicemente come $v_1 \otimes \ldots \otimes v_t$ con $v_i \in V_i$.

Definizione 4.2.2. Sia $w \in V_1 \otimes \ldots \otimes V_t$. Si dice che il rango di w è N se N è il minimo intero per cui esistono $z_1, \ldots, z_N$ tensori irriducibili di $V_1 \otimes \ldots \otimes V_t$ tali che $w = \sum_{i=1}^{N} z_i$. Se il rango di w è N scriviamo *rank* $w = N$.

Il problema di Waring è un quesito di teoria dei numeri proposto da Edward Waring e dimostrato in seguito da Hilbert, che precisamente dice:

Per ogni intero $d \geq 2$ esiste un intero positivo $g(d)$ tale che ogni $n \in \mathbb{Z}^+$ può essere scritto come $n = a_1^d + \ldots + a_{g(d)}^d$ con $a_i \geq 0,\ i = 1, \ldots, g(d)$.

Daremo ora la sua formulazione in termini di polinomi omogenei: poniamoci in un campo k algebricamente chiuso di caratteristica zero e sia $\mathbb{P}_k^n$ lo spazio proiettivo n-dimensionale sul campo k. Sia inoltre $k[t_0, \ldots, t_n]$ l'anello dei polinomi in $n+1$ variabili, che sappiamo essere un anello graduato. Quindi

$$k[t_0, \ldots, t_n] = \bigoplus_{d \geq 0} R_d$$

dove $R_d =< x_0^d, x_0^{d-1}x_1, \ldots, x_n^d >$ è generato dagli elementi omogenei di grado d e, come detto, la sua dimensione è $\binom{n+d}{d}$. Allora il problema di Waring è formulato come segue:

Qual è il minimo $z \in \mathbb{Z}^+$ tale che una generica forma $f \in R_d$ si possa scrivere come combinazione di z potenze d-esime di forme lineari, ossia come $f = L_1^d + \ldots + L_z^d$?

Definizione 4.2.3. Sia $p \in k[t_0, \ldots, t_n]$ un polinomio omogeneo di grado d. Definiamo *rango di p* il più piccolo intero positivo z tale che p si possa scrivere come combinazione lineare di z potenze d-esime di forme lineari.

Per risolvere la questione, dobbiamo studiare l'immagine della mappa

$$\phi : \underbrace{R_1 \times \cdots \times R_1}_{z} \longrightarrow R_d, \quad \phi(L_1, \ldots, L_z) = L_1^d + \ldots + L_z^d$$

Il primo oggetto geometrico legato al nostro problema è la mappa di Veronese. Ricordiamo la sua definizione:

$$\begin{array}{cccc} \mathcal{V}_d: & \mathbb{P}^n & \longrightarrow & \mathbb{P}^q \\ & [x_0,\ldots,x_n] & \longmapsto & [x_0^d, x_0^{d-1}x_1,\ldots,x_n^d] \end{array}$$

Come visto nella dimostrazione di 3.4.1, possiamo vedere la varietà di Veronese come la varietà che parametrizza le potenze d-esime delle forme lineari, ovvero i punti appartenenti all'immagine della Veronese rappresentano i polinomi omogenei di grado d e rango 1.

Definizione 4.2.4. Sia $X \subseteq \mathbb{P}^n$ una varietà proiettiva di dimensione n; denotiamo con $\sigma_s(X)$ l's-esima varietà secante di X e la definiamo nel modo seguente:

$$\sigma_s(X) := \overline{\bigcup_{P_1,\ldots,P_s \in X} < P_1,\ldots,P_s >}$$

dove $< P_1,\ldots,P_s >$ è il più piccolo spazio proiettivo che contiene $P_1,\ldots,P_s$.

Esempio 4.2.5. Sia $\mathcal{V}_d(\mathbb{P}^n)$ l'immagine della varietà di Veronese. L'insieme

$$\sigma_2(\mathcal{V}_d(\mathbb{P}^n)) := \overline{\bigcup_{P_1,P_2 \in \mathcal{V}_d} < P_1,P_2 >}$$

rappresenta la seconda varietà secante di $\mathcal{V}_d$. Un punto generico P che appartiene a $\sigma_2(\mathcal{V}_d(\mathbb{P}^n))$ può essere scritto come $P = aP_1 + bP_2$ con $P_1,P_2 \in \mathcal{V}_d(\mathbb{P}^n)$ e $a,b \in k$. Per quello che abbiamo detto in precedenza sappiamo però che P_1 e P_2 rappresentano polinomi omogenei di rango 1, e cioè si possono scrivere come potenza d-esima di un polinomio in 2 variabili. Quindi la forma omogenea di grado d che rappresenta P può essere scritta come $L_1^d+L_2^d$ (scegliendo opportunamente le forme lineari), ovvero il polinomio omogeneo di grado d che rappresenta P ha rango uguale a 2.

Questo esempio illustra come rispondere al Problema di Waring equivalga a studiare le dimensioni delle s-esime varietà secanti della Veronese. Purtroppo queste secanti non hanno sempre la dimensione che ci si aspetta, ovvero:

Proposizione 4.2.6. Sia $X = \sigma_s(\mathcal{V}_d(\mathbb{P}^n))$, allora la dimensione attesa di X è

$$\dim(X) = \min\left\{\binom{n+d}{d} - 1,\ s(n+1)-1\right\}$$

.

Dimostrazione. Per una dimostrazione si rimanda a [6].
Il primo numero rappresenta esattamente la dimensione dello spazio ambiente in cui X è contenuto, mentre il secondo si ottiene pensando di prendere s punti su uno spazio di dimensione $n+1$.

□

Concludiamo l'elaborato con il Teorema di Alexander-Hirschowitz che risponde completamente al problema di Waring:

Teorema 4.2.7 (Alexander-Hirschowitz)**.** Sia $X = \sigma_s(\mathcal{V}_d(\mathbb{P}^n))$ con $d \geq 2$, allora la dimensione di X è quella attesa, tranne nei casi:

- $d = 2,\ 2 \leq s \leq n$
- $d = 3,\ n = 4,\ s = 7$
- $d = 4,\ n = 2,\ s = 5$
- $d = 4,\ n = 3,\ s = 9$
- $d = 4,\ n = 4,\ s = 14$

Dimostrazione. Per una trattazione completa si vedano i lavori citati in [6]. □

Bibliografia

[1] Igor R. Shafarevich, Basic Algebraic Geometry 1, Varieties in Projective Space, Springer, 2013.

[2] Hartshorne R., Algebraic Geometry, Springer-Verlag, 1977.

[3] J. Milne, Algebraic Geometry, Note del 2009.

[4] Atiyah M. F. and Macdonald I. G., Introduction to Commutative Algebra, Addison-Wesley Publishing Company, 1969.

[5] C. Cascioli, Varietà algebriche affini, Tesi di Laurea in Geometria Algebrica, 2015.

[6] A. Bernardi, Waring Problems, Secant Varieties and Sylvester Algorithm, Note del 2013.

[7] D. Vanzo, Curve razionali normali e loro proiezioni, Tesi di Laurea in Geometria Proiettiva, 2010.

Ringraziamenti

Ringrazio gli insegnanti Monica, Lucia e Davide per la loro comprensione e pazienza, e per avermi trasmesso parte della loro conoscenza.
Ringrazio tutta la mia famiglia, quella stretta, quella allargata, quella che non c'è più . Quella che non lo è di sangue, ma che ha fatto parte della mia vita.
In particolare ringrazio Giovanni, Laura e Giulia per il costante sostegno.
Ringrazio i miei Amici, di Bologna Fano Pesaro Padova e di ogni dove. Quelli d'infanzia e di scuola, quelli con cui ho vissuto, quelli con cui ho condiviso esperienze importanti e quelli con cui mi sono semplicemente divertita.
Infine l'ultimo grazie va alla sartoria: a chi me l'ha fatta scoprire, a chi me la insegna con dedizione e a chi condivide questa passione con me.