UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di
Scienze Matematiche
Fisiche e Naturali

Corso di Laurea in
Matematica

SIZIGIE E FUNZIONE DI HILBERT

Syzygies and Hilbert function

Relatore:
Prof. Giorgio Ottaviani

Candidato:
Federico Venturelli

Anno Accademico 2012/2013

Indice

Introduzione

Sia K un campo, $R{=}K[x_0, \ldots, x_n]$ e M un R-modulo finitamente generato. Può succedere che i generatori di M non siano R-linearmente indipendenti (cioè che siano in *relazione* tra loro), cosa che rende il problema '$a, b \in M$ sono uguali?' di soluzione non immediata. Per questo motivo è importante riuscire a descrivere l'insieme di tutte le relazioni tra i generatori di M, che è esso stesso un R-modulo N. Nel corso di questa tesi vedremo come sia possibile descrivere N grazie ad una generalizzazione per i moduli della teoria delle basi di Gröbner. Ma anche i generatori di N possono essere in relazione tra loro, e dunque dovremmo descrivere anche il modulo delle relazioni tra i generatori di N, e così via. Per trattare al meglio questo problema saranno introdotte le successioni esatte e le risoluzioni libere. L'ultima parte della tesi riguarderà lo studio degli R-moduli *graduati* e delle risoluzioni libere graduate, e condurrà ad una semplice formula per il calcolo della funzione di Hilbert di tali moduli. A conclusione del lavoro i concetti introdotti saranno applicati in alcuni esempi classici (varietà di Segre e di Veronese).

Gli elementi di R o di generici R-moduli saranno indicati con lettere non in grassetto, mentre lettere in grassetto indicheranno elementi di R^m; le lettere $\boldsymbol{e}_i$ indicheranno i vettori delle basi canoniche di R^m (quale che sia m ove esso è deducibile dal contesto).

1 Concetti base

Cominciamo col presentare il 'protagonista' di questa tesi:

Definizione 1.1. Sia M un R-modulo finitamente generato e siano $f_1, \ldots, f_t$ elementi di M; si dice una relazione (o una *sizigia*) tra gli f_i una t-upla $(a_1, \ldots, a_t)^T$ di elementi di R tale che:

$$a_1 f_1 + \cdots + a_t f_t = 0$$

E' immediato verificare che la somma di due sizigie è ancora una sizigia, così come il prodotto di una sizigia per un elemento $a \in R$; l'insieme delle sizigie di $f_1, \ldots, f_t$ costituisce dunque un sottomodulo di R^t, che si indica con $Syz(f_1, \ldots, f_t)$.

Poichè R è noetheriano ogni sottomodulo di R^t, in particolare $Syz(f_1, \ldots, f_t)$, è finitamente generato; ma come si individua un sistema di generatori per $Syz(f_1, \ldots, f_t)$? Per rispondere a questa domanda è necessario sviluppare in R^t la teoria delle basi di Gröbner; tuttavia, visto che essa si sviluppa in modo completamente analogo a quanto accade in R, qui ci limitiamo a definire cos'è un monomio in R^t e di conseguenza cosa sia un ordine monomiale.

Definizione 1.2. Un *monomio* in R^t è un elemento del tipo $x^\alpha \boldsymbol{e}_i$ e si dice che esso *contiene* il vettore $\boldsymbol{e}_i$.

Dalla definizione segue immediatamente che ogni elemento $\boldsymbol{f} \in R^t$ può essere scritto in modo unico come K-combinazione lineare di monomi $\boldsymbol{m}_i$.

Così come per gli ideali I di R, un R-modulo $M \subset R^t$ si dice *monomiale* se può essere generato da un insieme di monomi. Determinare dei generatori per il modulo delle sizigie di un ideale monomiale non è difficile; si ha infatti la seguente proposizione (per la dimostrazione vedere [1]):

Proposizione 1.1. *Sia $\{\boldsymbol{m}_1, \ldots, \boldsymbol{m}_s\}$ un insieme di generatori di un sottomodulo monomiale $M \subset R^t$. Definiamo $\boldsymbol{m}_{ij} = mcm(\boldsymbol{m}_i, \boldsymbol{m}_j)$, ponendo $\boldsymbol{m}_{ij} = \boldsymbol{0}$ se $\boldsymbol{m}_i$ e $\boldsymbol{m}_j$ non contengono lo stesso $\boldsymbol{e}_k$. Il modulo $Syz(\boldsymbol{m}_1, \ldots, \boldsymbol{m}_s)$ è generato dagli elementi $\boldsymbol{\sigma}_{ij} = (\boldsymbol{m}_{ij}/\boldsymbol{m}_i)\boldsymbol{e}_i - (\boldsymbol{m}_{ij}/\boldsymbol{m}_j)\boldsymbol{e}_j$ ove $1 \leq i < j \leq s$.*

La definizione di *ordine monomiale* è, per R^t, la stessa che si ha su R, dunque diamo solamente un esempio di come un ordine monomiale su R si estenda naturalmente ad un ordine monomiale su R^t.

Definizione 1.3. Sia $>$ un ordine monomiale su R; possiamo estenderlo ad un ordine monomiale su R^t ponendo:

a) (Estensione TOP) $x^\alpha \boldsymbol{e}_i >_{\text{TOP}} x^\beta \boldsymbol{e}_j$ se $x^\alpha > x^\beta$ o se $x^\alpha = x^\beta$ e $i < j$.

b) (Estensione POT) $x^\alpha \boldsymbol{e}_i >_{\text{POT}} x^\beta \boldsymbol{e}_j$ se $i < j$ o se $i = j$ e $x^\alpha > x^\beta$.

2 Il Teorema di Schreyer

Dopo il caso monomiale vediamo ora come calcolare un insieme di generatori per il modulo delle sizigie di un generico sottomodulo $M \subset R^t$. Per prima cosa fissiamo un ordine monomiale $>$ e calcoliamo (tramite l'algoritmo di Buchberger) una base di Gröbner $\boldsymbol{G} = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s\}$ per M. Il criterio di Buchberger ci assicura di poter scrivere, per ogni i,j

$$S(\boldsymbol{g}_i, \boldsymbol{g}_j) = \sum_{k=1}^{s} a_{ijk} \boldsymbol{g}_k$$

con $a_{ijk} \in R$ e $LM(a_{ijk}\boldsymbol{g}_k) \leq LM(S(\boldsymbol{g}_i, \boldsymbol{g}_j))$ per ogni k. Possiamo adesso definire gli elementi $\boldsymbol{a}_{ij} \in R^s$ come

$$\boldsymbol{a}_{ij} = \sum_{k=1}^{s} a_{ijk} \boldsymbol{\epsilon}_k$$

ove gli $\boldsymbol{\epsilon}_i$ indicano i vettori della base canonica di R^s. Infine, ponendo $\boldsymbol{m}_{ij} = mcm(LT(\boldsymbol{g}_i), LT(\boldsymbol{g}_j))$ (convenendo di nuovo che $\boldsymbol{m}_{ij}$ è zero se $LT(\boldsymbol{g}_i)$ e $LT(\boldsymbol{g}_j)$ non contengono lo stesso vettore della base canonica) possiamo definire, per gli i,j per cui $\boldsymbol{m}_{ij}$ è non nullo, gli elementi $\boldsymbol{s}_{ij} \in R^s$ come

$$\boldsymbol{s}_{ij} = (\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_i))\boldsymbol{\epsilon}_i - (\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_j))\boldsymbol{\epsilon}_j - \boldsymbol{a}_{ij}$$

Abbiamo adesso introdotto tutto il necessario per dimostrare il:

Teorema 2.1 (Teorema di Schreyer)**.** *Sia $\boldsymbol{G} \subset R^t$ una base di Gröbner di un sottomodulo $M \subset R^t$; gli $\boldsymbol{s}_{ij}$ formano una base di Gröbner per il modulo $N = Syz(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s)$ rispetto all'ordine monomiale $>_{\text{G}}$ su R^s così definito: $x^\alpha \boldsymbol{\epsilon}_i >_{\text{G}} x^\beta \boldsymbol{\epsilon}_j$ se $LM_>(x^\alpha \boldsymbol{g}_i) > LM_>(x^\beta \boldsymbol{g}_j)$ in R^t o se $LM_>(x^\alpha \boldsymbol{g}_i) = LM_>(x^\beta \boldsymbol{g}_j)$ e $i < j$.*

Dimostrazione. Che $>_{\text{G}}$ sia un ordine monomiale si dimostra facilmente, dunque passiamo alla seconda parte del teorema. Visto che $\boldsymbol{s}_{ij}$ e $\boldsymbol{s}_{ji}$ differiscono unicamente per il segno, è sufficiente considerare gli $\boldsymbol{s}_{ij}$ per $i < j$; allora, visto che negli S-vettori si ha una cancellazione dei leading term, vale

$$(\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_i))\boldsymbol{\epsilon}_i >_{\text{G}} (\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_j))\boldsymbol{\epsilon}_j.$$

Inoltre, come notato all'inizio di questa sezione,

$$LM_>(S(\boldsymbol{g}_i, \boldsymbol{g}_j)) \geq LM_>(a_{ijk}\boldsymbol{g}_k)$$

per ogni $k = 1, \ldots, s$ in R^t e dalla definizione di S-vettore si ha

$$LM_>((\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_i))\boldsymbol{g}_i > LM_>(S(\boldsymbol{g}_i, \boldsymbol{g}_j))$$

in R^t (ancora perchè negli S-vettori i leading term si cancellano). Di conseguenza vale

$$(\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_i))\boldsymbol{\epsilon}_i >_{\mathrm{G}} a_{ijk}\boldsymbol{\epsilon}_k$$

per ogni $k = 1, \ldots, s$ e quindi

$$LT_{>\mathrm{G}}(\boldsymbol{s}_{ij}) = (\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_i))\boldsymbol{\epsilon}_i.$$

Sia ora $\boldsymbol{f} = \sum_{i=1}^{s} f_i\epsilon_i$ un elemento del modulo delle sizigie N; per dimostrare il teorema ci basta verificare che $LT_{>\mathrm{G}}(\boldsymbol{f})$ è divisibile per un qualche $LT_{>\mathrm{G}}(\boldsymbol{s}_{ij})$. Poniamo (per ogni $i = 1, \ldots, s$) $LT_{>\mathrm{G}}(f_i\epsilon_i) = m_i\epsilon_i$ per un certo termine m_i tra quelli che compaiono in f_i e sia inoltre $LT_{>\mathrm{G}}(\boldsymbol{f}) = m_v\epsilon_v$ per qualche v. Fissato questo v, definiamo
$S = \{u : LM_{>}(m_u\boldsymbol{g}_u) = LM_{>}(m_v\boldsymbol{g}_v)\} \subseteq \{1, \ldots, s\}$ e scriviamo

$$\boldsymbol{s} = \sum_{u \in S} m_u\boldsymbol{\epsilon}_u.$$

Notiamo subito che gli indici in S sono maggiori o uguali a v: infatti per ogni $j \in S$ vale $LM_{>}(m_j\boldsymbol{g}_j) = LM_{>}(m_v\boldsymbol{g}_v)$ e se valesse $j < v$ allora (per la definizione di $>_{\mathrm{G}}$) si avrebbe $LT_{>\mathrm{G}}(\boldsymbol{f}) = m_j\epsilon_j$ (il che è assurdo perchè $LT_{>\mathrm{G}}(\boldsymbol{f}) = m_v\epsilon_v$); di conseguenza $LT_{>\mathrm{G}}(\boldsymbol{s}) = LT_{>\mathrm{G}}(\boldsymbol{f})$. Poichè $\boldsymbol{f} \in M$ deve valere

$$\sum_{u \in S} m_u LT(\boldsymbol{g}_u) = 0$$

(altrimenti $\boldsymbol{f}$ non sarebbe una sizigia) e quindi $\boldsymbol{s} \in Syz(\{LT(\boldsymbol{g}_u) : u \in S\})$. Per la proposizione 1.1 $\boldsymbol{s}$ è una R-combinazione lineare degli elementi

$$\boldsymbol{\sigma}_{zw} = (\boldsymbol{m}_{zw}/LT_{>}(\boldsymbol{g}_z))\boldsymbol{\epsilon}_z - (\boldsymbol{m}_{zw}/LT_{>}(\boldsymbol{g}_w))\boldsymbol{\epsilon}_w$$

con $z < w$ e $z, w \in S$, e quindi il suo leading term è divisibile per il leading term di uno degli $\boldsymbol{s}_{ij}$, come volevamo dimostrare. □

Ricapitoliamo: grazie al teorema di Schreyer, dato un modulo $M \subset R^t$ ed una sua base di Gröbner $\boldsymbol{G} = \{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s\}$ siamo in grado di ricavare una base di Gröbner $\boldsymbol{G}_1 = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_l\}$ per $Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_s)$; tuttavia tra gli elementi di $\boldsymbol{G}_1$ possono ancora esserci delle relazioni (le cosiddette seconde sizigie), e possiamo di nuovo usare il teorema di Schreyer per calcolare una base di Gröbner di $Syz(\boldsymbol{g}_1, \ldots, \boldsymbol{g}_l)$ e così via. Otteniamo dunque una successione di generatori e di relazioni tra generatori per i vari moduli successivi delle sizigie di M; per studiare meglio questa situazione, è utile introdurre le successioni esatte e le risoluzioni libere.

3 Successioni esatte e risoluzioni libere

Definizione 3.1. Consideriamo una generica successione di R-moduli e di morfismi

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \longrightarrow \cdots$$

a) La successione è detta *esatta in* M_i se $im(\varphi_{i+1}) = ker(\varphi_i)$.

b) La successione è detta *esatta* se è esatta in ogni M_i che non sia all'inizio o alla fine di essa.

Le condizioni necessarie affinchè una successione sia esatta a prima vista possono sembrare molto stringenti, al punto da far sospettare che solo per certi moduli sia possibile costruirle; in realtà nel caso in esame, cioè $M \subset R^m$, vale esattamente il contrario. Il fatto che M sia finitamente generato garantisce infatti che:

Proposizione 3.1. *Per ogni R-modulo $M \subset R^m$ è possibile costruire una successione esatta del tipo*

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0$$

con s e t opportuni.

Una tale successione è detta una *presentazione* di M, e detti $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t$ e $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s$ i generatori rispettivamente di M e $Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_t)$ la si ottiene semplicemente ponendo $\varphi(\boldsymbol{e}_i) = \boldsymbol{f}_i$ e $\psi(\boldsymbol{\epsilon}_j) = \boldsymbol{g}_j$ per ogni $i = 1, \ldots, t$ e $j = 1, \ldots, s$ ($\boldsymbol{e}_i$ e $\boldsymbol{\epsilon}_j$ sono i vettori delle basi canoniche di R^t e R^s rispettivamente).

L'osservazione conclusiva della sezione precedente, insieme a quest'accenno di dimostrazione, ci fa capire che è possibile estendere a sinistra la successione esatta

$$R^s \xrightarrow{\psi} R^t \xrightarrow{\varphi} M \longrightarrow 0$$

ad una successione esatta comprendente il modulo delle seconde sizigie, quello delle terze sizigie e così via. Si ottiene in questo modo una risoluzione libera di M, la cui definizione è la seguente:

Definizione 3.2. Una *risoluzione libera* di un R-modulo M è una successione esatta della forma

$$\cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

ove $F_i \cong R^{d_i}$ per ogni i. Se esiste un l per cui $F_{l+1} = F_{l+2} = \cdots = 0$ ma $F_l \neq 0$ allora la risoluzione è detta *finita* di *lunghezza* l e si scriverà

$$0 \longrightarrow F_l \longrightarrow F_{l-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

Come già detto il teorema di Schreyer consente di trovare delle basi di Gröbner per i vari moduli delle sizigie di un R-modulo $M \subset R^t$, e di ottenere quindi una sua risoluzione libera; è adesso naturale chiedersi se per ogni R-modulo sia possibile trovare una risoluzione libera finita, o quali condizioni debbano essere soddisfatte affinchè ciò sia possibile.

4 Il teorema delle sizigie di Hilbert

Per rispondere alla domanda della sezione precedente sono necessari due lemmi:

Lemma 4.1. *Sia $\boldsymbol{G}$ una base di Gröbner di un R-modulo $M \subset R^t$ rispetto ad un ordine monomiale qualsiasi, e ordiniamo gli elementi di $\boldsymbol{G}$ in modo da formare una s-upla ordinata $G = (\boldsymbol{g}_1, \ldots, \boldsymbol{g}_s)$ tale che ogni volta in cui $LT(\boldsymbol{g}_i)$ e $LT(\boldsymbol{g}_j)$ contengono lo stesso vettore della base canonica $\boldsymbol{e}_k$ e $i < j$, allora $LM(\boldsymbol{g}_i)/\boldsymbol{e}_k >_{\text{lex}} LM(\boldsymbol{g}_j)/\boldsymbol{e}_k$, ove $>_{\text{lex}}$ indica l'ordine monomiale lessicografico su R con $x_0 > \cdots > x_n$. Se le indeterminate $x_1, \ldots, x_m$ non compaiono nei leading term di $\boldsymbol{G}$, allora $x_1, \ldots, x_{m+1}$ non compaiono nei leading term degli elementi $\boldsymbol{s}_{ij} \in Syz(\boldsymbol{G})$ rispetto all'ordine monomiale $>_{\text{G}}$.*

Nell'enunciato del lemma, l'espressione $LM(\boldsymbol{g}_j)/\boldsymbol{e}_k$ indica il leading monomial dell'elemento $f \in R$ presente nella riga k-esima di $\boldsymbol{g}_j$.

Dimostrazione. Utilizzando le stesse notazioni del teorema di Schreyer, sappiamo che

$$LT_{>\mathrm{G}}(\boldsymbol{s}_{ij}) = (\boldsymbol{m}_{ij}/LT(\boldsymbol{g}_i))\boldsymbol{\epsilon}_i$$

ove $\boldsymbol{\epsilon}_i$ indica un vettore della base canonica di R^s. Di nuovo, è sufficiente considerare gli $\boldsymbol{s}_{ij}$ tali che $LT(\boldsymbol{g}_i)$ e $LT(\boldsymbol{g}_j)$ contengono lo stesso vettore della base canonica $\boldsymbol{e}_k$ in R^t (altrimenti $\boldsymbol{s}_{ij} = \boldsymbol{0}$) e con $i < j$ (per $j > i$ cambia solo il segno di $\boldsymbol{s}_{ij}$). Per come abbiamo ordinato gli elementi di G, vale $LM(\boldsymbol{g}_i)/\boldsymbol{e}_k >_{\mathrm{lex}} LM(\boldsymbol{g}_j)/\boldsymbol{e}_k$ e poichè $x_1, \ldots, x_m$ non compaiono nei leading term di $\boldsymbol{G}$ possiamo scrivere

$$LM(\boldsymbol{g}_i)/\boldsymbol{e}_k = x_{m+1}^{\alpha} n_i$$

$$LM(\boldsymbol{g}_j)/\boldsymbol{e}_k = x_{m+1}^{\beta} n_j$$

con $\alpha \geq \beta$ e n_i, n_j monomi in R contenenti solo $x_{m+2}, \ldots, x_n$. Ma allora $mcm(LT(\boldsymbol{g}_i), LT(\boldsymbol{g}_j))$ contiene x_{m+1}^{α} e quindi, per quanto scritto all'inizio, $LT_{>\mathrm{G}}(\boldsymbol{s}_{ij})$ non contiene $x_1, \ldots, x_m, x_{m+1}$. □

Lemma 4.2. *Sia $M \subset R^t$ e $\boldsymbol{G} = (\boldsymbol{g}_1, \ldots, \boldsymbol{g}_l)$ una sua base di Gröbner ridotta (dunque i leading term degli elementi di $\boldsymbol{G}$ sono vettori della base canonica di R^t); allora*

a) Se $\boldsymbol{e}_i$ è il leading term di un qualche elemento di $\boldsymbol{G}$, allora è il leading term di esattamente un elemento di $\boldsymbol{G}$.

b) $Syz(\boldsymbol{G}) = \{0\} \subset R^l$ e dunque M è un modulo libero.

Dimostrazione. Fissiamo un indice i_0 e sia $LT(\boldsymbol{g}_{i_0}) = \boldsymbol{e}_{j_0}$; se esistesse un altro $\boldsymbol{g}_{i_1} \in \boldsymbol{G}$ tale che $LT(\boldsymbol{g}_{i_1}) = \boldsymbol{e}_{j_0}$ allora i due leading term sarebbero associati, ma questo è assurdo perchè $\boldsymbol{G}$ è ridotta. Questo prova il punto a). Siano ora $\{i_1, \ldots, i_l\} \subset \{1, \ldots, t\}$ gli indici dei vettori della base canonica di R^t costituenti i vari $LT(\boldsymbol{g}_i)$. Poichè $\boldsymbol{G}$ è ridotta gli elementi i_k-esimi dei $\boldsymbol{g}_i$ (quando diversi da $LT(\boldsymbol{g}_i)$) devono essere nulli. Sia ora $(a_1, \ldots, a_l) \in R^l$ tale che

$$\sum_{i=1}^{l} a_i \boldsymbol{g}_i = \boldsymbol{0}$$

in particolare varrà

$$\sum_{i=1}^{l} a_i g_{i_k} = 0$$

per ogni $k = 1, \ldots, l$; ma questo significa $a_i = 0$ per ogni $i = 1, \ldots, l$, dunque $Syz(\boldsymbol{G}) = \{0\}$ cioè M è libero. □

Siamo ora in grado di dimostrare il

Teorema 4.3 (Teorema delle sizigie di Hilbert)**.** *Ogni R-modulo M finitamente generato ha una risoluzione libera finita di lunghezza al più n+1.*

Dimostrazione. Visto che M è finitamente generato, la proposizione 3.1 ci garantisce che M ha una presentazione del tipo

$$F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0$$

ottenuta scegliendo un insieme di generatori $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{r_0}\}$ di M e una base di Gröbner $\boldsymbol{G}_0 = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_{r_1}\}$ per $Syz(\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{r_0}) = im(\varphi_1) \subset F_0 = R^{r_0}$ rispetto ad un ordine

monomiale qualsiasi su F_0. Ordiniamo gli elementi di $\boldsymbol{G}_0$ in modo che soddisfino l'ipotesi del lemma 4.1, ottenendo un vettore $\overline{\boldsymbol{G}}_0$, ed usiamo il Teorema di Schreyer per trovare una base di Gröbner $\boldsymbol{G}_1$ di $Syz(\overline{\boldsymbol{G}}_0) \subset F_1 = R^{r_1}$; possiamo supporre che $\boldsymbol{G}_1$ sia ridotta. Allora almeno x_0 non sarà presente nei leading term di $\boldsymbol{G}_1$, e avremo ottenuto la successione esatta

$$F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0$$

dove $F_2 = R^{r_2}$ e $im(\varphi_2) = Syz(\overline{\boldsymbol{G}}_1)$; r_2 sarà il numero di elementi di $\boldsymbol{G}_1$, che possiamo ordinare di nuovo come nel lemma 4.1.

Iterando questo procedimento, per un generico i otteniamo $\varphi_i : F_i \longrightarrow F_{i-1}$ dove $im(\varphi_i) = Syz(\overline{\boldsymbol{G}}_{i-1})$ e $\boldsymbol{G}_i \subset R^{r_i}$ è una base di Gröbner per $Syz(\overline{\boldsymbol{G}}_{i-1})$, a patto di ordinare ogni volta gli elementi della base di Gröbner $\boldsymbol{G}_{i-1}$ per ottenere un vettore $\overline{\boldsymbol{G}}_{i-1}$ soddisfacente le ipotesi del lemma 4.1.

Il numero di indeterminate presente nei leading term degli elementi delle varie basi di Gröbner decresce di almeno 1 ad ogni passo, dunque di sicuro per un certo $l \leq n+1$ i leading term della base di Gröbner $\boldsymbol{G}_l$ non conterranno nessuna x_i. A questo punto, la successione esatta iniziale sarà diventata

$$F_l \xrightarrow{\varphi_l} F_{l-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0 \tag{4.1}$$

e i leading term degli elementi di $\boldsymbol{G}_l$ (che possiamo supporre ridotta) saranno vettori della base canonica di F_l.

Usando il lemma 4.2, possiamo concludere che $Syz(\overline{\boldsymbol{G}}_{l-1})$ è un modulo libero e dunque la successione 4.1 può essere estesa ad una successione esatta tramite l'inclusione $0 \longrightarrow F_l$; la successione esatta così ottenuta è proprio una risoluzione libera di M di lunghezza $l \leq n+1$. □

Le risoluzioni libere rivestono particolare importanza nello studio degli ideali omogenei $I = \boldsymbol{I}(V)$ di varietà proiettive $V \subset \mathbb{P}^n$, perchè risoluzioni di ideali (e quindi di moduli) di questo tipo possiedono una struttura aggiuntiva derivante dalla *graduazione* su R. Vedremo cosa questo significhi nella prossima sezione.

5 Risoluzioni graduate

Ricordiamo che l'anello R può essere scritto come

$$R = \bigoplus_{s \geq 0} R_s$$

ove gli R_s indicano i sottogruppi additivi cui appartengono gli elementi di R di grado totale s (oltre all'elemento neutro 0). Anche i moduli possono avere una simile decomposizione, e quelli che la ammettono sono detti graduati.

Definizione 5.1. Si definisce *R-modulo graduato* un modulo M avente una famiglia di sottogruppi $\{M_t : t \in \mathbb{Z}\}$ del proprio gruppo additivo (detti *elementi omogenei di grado t*) soddisfacenti le seguenti condizioni:

a) $M = \bigoplus_{t \in \mathbb{Z}} M_t$ come gruppi additivi.

b) $R_s M_t \subset M_{s+t}$ per ogni $s \geq 0$ e $t \in \mathbb{Z}$ (cioè la decomposizione di M al punto precedente è compatibile con la moltiplicazione per elementi di R).

Osserviamo subito due cose: la prima è che ogni M_t è chiaramente un K-sottospazio vettoriale di M e quindi se M è finitamente generato gli M_t hanno dimensione finita su K; la seconda è che gli R-moduli graduati sono meno rari di quanto la definizione non sembri suggerire: gli ideali omogenei $I \subset R$, per esempio, sono moduli graduati (gli elementi omogenei di grado t di I sono $I_t = I \cap R_t$); un esempio anche più semplice di R-modulo graduato è R^m, visto che si ottiene una graduazione semplicemente ponendo $(R^m)_t = (R_t)^m$. La struttura di R-modulo graduato inoltre si conserva per somma diretta e quoziente.

Nei moduli graduati finora citati la graduazione rispetta il grado polinomiale (elementi di grado polinomiale t appartengono agli elementi omogenei di grado t del modulo), tuttavia non è affatto necessario che questo accada; infatti non è difficile verificare che traslando la graduazione di un modulo graduato M possiamo ottenere un modulo graduato N con graduazione diversa ma isomorfo ad M.

Proposizione 5.1. *Sia M un R-modulo graduato e sia $d \in \mathbb{Z}$. Sia $M(d)$ la somma diretta*

$$M(d) = \bigoplus_{t \in \mathbb{Z}} M(d)_t$$

dove $M(d)_t = M_{d+t}$; allora anche $M(d)$ è un R-modulo graduato.

Ad esempio, i moduli $(R^m)(d) = R(d)^m$ sono detti R-moduli graduati liberi *traslati* (dall'inglese *twisted*); i vettori $\boldsymbol{e}_i$ sono ancora una base per $R(d)^m$, ma sono elementi omogenei di grado $-d$, non 0 (visto che $R(d)_{-d} = R_0$). D'ora in avanti tratteremo spesso R-moduli graduati liberi traslati del tipo

$$R(-d_1) \oplus \cdots \oplus R(-d_m)$$

ove gli elementi $\boldsymbol{e}_i$ hanno grado d_i.

La struttura aggiuntiva che i moduli graduati possiedono si riflette anche sui morfismi tra di essi; in particolare possiamo definire i morfismi graduati:

Definizione 5.2. Siano M, N R-moduli graduati. Un morfismo $\varphi : M \longrightarrow N$ è detto un *morfismo graduato di grado d* se $\varphi(M_t) \subset N_{t+d}$ per ogni $t \in \mathbb{Z}$.

Ad esempio sia $M = (f_1, \ldots, f_m)$ con $deg f_i = d_i$ per ogni $i = 1, \ldots, m$. Abbiamo già visto che per ottenere un morfismo $\varphi : R^m \longrightarrow M$ basta porre $\varphi(\boldsymbol{e}_i) = f_i$ per ogni $i = 1, \ldots, m$, tuttavia il morfismo così costruito è chiaramente non graduato. Possiamo però ottenere un morfismo graduato (di grado 0) $\psi : R(-d_1) \oplus \cdots \oplus R(-d_m) \longrightarrow M$ ponendo di nuovo $\psi(\boldsymbol{e}_i) = f_i$ per ogni $i = 1, \ldots, m$ (si noti che ψ è anche suriettivo). Ora che abbiamo definito i morfismi graduati, possiamo definire le risoluzioni graduate:

Definizione 5.3. Sia M un R-modulo graduato. Una *risoluzione graduata* di M è una risoluzione

$$\cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow M \longrightarrow 0$$

in cui ogni F_i è un R-modulo libero graduato traslato del tipo $R(-d_1) \oplus \cdots \oplus R(-d_m)$ e ciascun morfismo φ_i è graduato di grado 0. Una risoluzione graduata si dice inoltre *minimale* se per ogni $i \geq 1$ gli elementi non nulli della matrice di φ_i hanno grado positivo.

Ci sono alcune cose da osservare sulla condizione di minimalità:

a. Innanzitutto, essa è equivalente alla scelta di insiemi di generatori minimali per i moduli presenti nella risoluzione graduata; la definizione è qui riportata perchè il

programma Macaulay2 (con cui saranno illustrati degli esempi nella parte conclusiva di questo lavoro) tramite il comando RESOLUTION calcola proprio risoluzioni minimali.

b. Le risoluzioni minimali di un modulo graduato M sono uniche a meno di isomorfismi (fatto la cui dimostrazione esula dagli obbiettivi di questa tesi); di conseguenza possiamo definire senza ambiguità i *numeri di Betti* di M come i ranghi dei moduli liberi che appaiono in una risoluzione graduata minimale di M (anch'essi calcolabili con Macaulay2 grazie al comando BETTI).

E' naturale ora chiedersi, come abbiamo fatto per gli R-moduli, se ogni R-modulo graduato finitamente generato ammetta una risoluzione graduata finita (la definizione di finitezza è la stessa del caso non graduato). La risposta è di nuovo sì, ed è data da un ulteriore teorema di Hilbert (di cui diamo solo l'enunciato).

Teorema 5.2 (Teorema delle sizigie di Hilbert nel caso graduato)**.** *Ogni R-modulo graduato finitamente generato ammette una risoluzione graduata finita di lunghezza al più $n+1$.*

6 La funzione di Hilbert

Come già detto nella sezione precedente, se M è un R-modulo graduato finitamente generato i suoi elementi omogenei M_t sono K-spazi vettoriali di dimensione finita. E' allora possibile definire la funzione di Hilbert di M.

Definizione 6.1. Se M è un R-modulo graduato finitamente generato, la *funzione di Hilbert* $H_M(t)$ di M è data da

$$H_M(t) = dim_K M_t$$

dove dim_K indica la dimensione come K-spazio vettoriale.

Dalla definizione segue chiaramente che

$$H_R(t) = \binom{t+n}{n}$$

ed è immediato verificare che $H_{R(d)}(t) = H_R(t+d)$; di conseguenza si ha pure

$$H_{R(d)}(t) = \binom{t+n+d}{n}.$$

Se M non coincide con R (o con un suo traslato $R(d)$) il calcolo della sua funzione di Hilbert non è così semplice; tuttavia il seguente risultato fornisce una semplificazione del problema:

Proposizione 6.1. *Sia M un R-modulo graduato. Per ogni risoluzione graduata finita di M*

$$0 \longrightarrow F_s \longrightarrow \ldots \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

vale

$$H_M(t) = dim_K M_t = \sum_{j=0}^{s} (-1)^j dim_K (F_j)_t = \sum_{j=0}^{s} (-1)^j H_{F_j}(t) \tag{6.1}$$

Dimostrazione. In una risoluzione graduata tutti i morfismi hanno grado 0, dunque restringendoli agli elementi omogenei di grado t dei vari moduli graduati otteniamo, per ogni $t \in Z$, una successione esatta di K-spazi vettoriali

$$0 \longrightarrow (F_s)_t \longrightarrow \cdots \longrightarrow (F_0)_t \longrightarrow M_t \longrightarrow 0.$$

La somma alterna delle dimensioni è 0 per le proprietà delle successioni esatte dunque vale

$$dim_K M_t = \sum_{j=0}^{s} (-1)^j dim_K (F_j)_t$$

e la proposizione segue dalla definizione di funzione di Hilbert. □

Visto che sappiamo calcolare la funzione di Hilbert di un generico modulo libero traslato (per 6.1), e che ogni R-modulo graduato finitamente generato ammette una risoluzione graduata finita (per il teorema delle sizigie di Hilbert), la proposizione precedente ci consente di calcolare la funzione di Hilbert di un qualsiasi R-modulo graduato finitamente generato. In particolare, se I è un ideale omogeneo di R allora R/I ammette la risoluzione graduata finita

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

e dunque si ha

$$H_{R/I}(t) = H_R(t) - H_I(t) \tag{6.2}$$

che possiamo calcolare facilmente usando la proposizione precedente.

7 Esempi

7.1 Varietà di Segre

Sia M una matrice $m \times n$ i cui elementi sono indeterminate distinte; la *varietà di Segre* di M è il luogo dei punti di $\mathbb{P}^{nm-1}$ che annullano tutti i minori 2×2 di M (cioè il luogo degli zeri delle matrici $m \times n$ di rango 1). Il seguente codice di Macaulay2 calcola la risoluzione dell'ideale omogeneo I della varietà di Segre di matrici quadrate; inoltre mostra i numeri di Betti di I e i gradi dei generatori dei moduli liberi presenti nella risoluzione.

```
i=3
s=i^2-1
R=QQ[x_0..x_s]
M=genericMatrix(R,i,i)
I=minors(2,M)
rM=resolution I
betti rM
```

Vediamo come funziona per una matrice 3×3.

```
i1 : i=3

o1 = 3

i2 : s=i^2-1

o2 = 8
```

```
i3 : R=QQ[x_0..x_s]

o3 = R

o3 : PolynomialRing

i4 : M=genericMatrix(R,i,i)

o4 = | x_0 x_3 x_6 |
     | x_1 x_4 x_7 |
     | x_2 x_5 x_8 |

             3       3
o4 : Matrix R  <--- R

i5 : I=minors(2,M)

o5 = ideal (- x x  + x x , - x x  + x x , - x x  + x x , - x x  + x x , - x x
               1 3    0 4     2 3    0 5     2 4    1 5     1 6    0 7     2 6
     ------------------------------------------------------------------------
     + x x , - x x  + x x , - x x  + x x , - x x  + x x , - x x  + x x )
       0 8     2 7    1 8     4 6    3 7     5 6    3 8     5 7    4 8

o5 : Ideal of R

i6 : rM=resolution I

      1      9      16      9      1
o6 = R  <-- R  <-- R   <-- R  <-- R  <-- 0

     0      1      2       3      4      5

o6 : ChainComplex

i7 : betti rM

            0 1  2 3 4
o7 = total: 1 9 16 9 1
         0: 1 .  . . .
         1: . 9 16 9 .
         2: . .  . . 1

o7 : BettiTally
```

Il codice mostra che i numeri di Betti di I sono 9, 16, 9 e 1, e che i generatori dei moduli liberi (non banali) della risoluzione sono di grado rispettivamente 2, 3, 4 e 6. La risoluzione graduata minimale di I è dunque

$$0 \longrightarrow R(-6) \longrightarrow R(-4)^9 \longrightarrow R(-3)^{16} \longrightarrow R(-2)^9 \longrightarrow I \longrightarrow 0.$$

Di conseguenza la funzione di Hilbert di R/I è (usando 6.1 e 6.2)

$$H_{R/I}(t) = \binom{t+8}{8} - 9\binom{t-2+8}{8} + 16\binom{t-3+8}{8} - 9\binom{t-4+8}{8} + \binom{t-6+8}{8}$$

e semplificando si ottiene

$$H_{R/I}(t) = (1/4)t^4 + (3/2)t^3 + (13/4)t^2 + 3t + 1$$

7.2 Varietà di Veronese

Sia M una matrice quadrata simmetrica di dimensione n contenente $n(n+1)/2$ indeterminate distinte; la *Varietà di Veronese* di M è il luogo dei punti di $\mathbb{P}^{n(n+1)/2-1}$ che annullano tutti i minori 2×2 di M (cioè il luogo degli zeri delle matrici simmetriche di dimensione n e rango 1). Il seguente codice è un adattamento del precedente che fornisce le stesse informazioni sull'ideale omogeneo I di tale varietà: risoluzione, grado dei generatori dei moduli liberi e numeri di Betti.

```
i=3
s=0
for j from 1 to i do s=s+j
R=QQ[x_0..x_(s-1)]
M=genericSymmetricMatrix(R,i)
I=minors(2,M)
rM=resolution I
betti rM
```

Consideriamo il caso $n = 3$.

```
i1 : i=3

o1 = 3

i2 : s=0

o2 = 0

i3 : for j from 1 to i do s=s+j

i4 : R=QQ[x_0..x_(s-1)]

o4 = R

o4 : PolynomialRing

i5 : M=genericSymmetricMatrix(R,i)

o5 = | x_0 x_1 x_2 |
     | x_1 x_3 x_4 |
     | x_2 x_4 x_5 |
```

```
             3       3
o5 : Matrix R  <--- R

i6 : I=minors(2,M)

               2                                                        2
o6 = ideal (- x  + x x , - x x  + x x , - x x  + x x , - x x  + x x , - x  +
               1    0 3     1 2    0 4     2 3    1 4     1 2    0 4     2
     ------------------------------------------------------------------------
                                                        2
     x x , - x x  + x x , - x x  + x x , - x x  + x x , - x  + x x )
      0 5     2 4    1 5     2 3    1 4     2 4    1 5     4    3 5

o6 : Ideal of R

i7 : rM=resolution I

      1      6      8      3
o7 = R  <-- R  <-- R  <-- R  <-- 0

     0      1      2      3      4

o7 : ChainComplex

i8 : betti rM

            0 1 2 3
o8 = total: 1 6 8 3
         0: 1 . . .
         1: . 6 8 3

o8 : BettiTally
```

Dal codice si ricava che i numeri di Betti di I sono 6, 8 e 3, e che i generatori dei moduli (non banali) della risoluzione sono di grado rispettivamente 2, 3 e 4. La risoluzione graduata minimale di I è dunque

$$0 \longrightarrow R(-4)^3 \longrightarrow R(-3)^8 \longrightarrow R(-2)^6 \longrightarrow I \longrightarrow 0.$$

Di conseguenza la funzione di Hilbert di R/I è

$$H_{R/I} = \binom{t+5}{5} - 6\binom{t+3}{5} + 8\binom{t+2}{5} - 3\binom{t+1}{5} = 2t^2 + 3t + 1$$

Riferimenti bibliografici

[1] D. Cox, J. Little, D. O'Shea - Using algebraic geometry - Springer-Verlag - New York - 2005.

[2] D. Cox, J. Little, D. O'Shea - Ideals, varieties and algorithms - Springer-Verlag - New York - 2007.

[3] D. Eisenbud - Commutative algebra with a view towards algebraic geometry - Springer-Verlag - New York - 1995.

[4] J. Harris - Algebraic geometry: a first course - Springer-Verlag - New York - 1992

[5] G. Ottaviani - Introduzione alle varietà algebriche. Un punto di vista costruttivo. - disponibile all'indirizzo `http://web.math.unifi.it/users/ottavian/groebner/groebner.pdf`