UNIVERSITÀ DI PISA

Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Triennale in Matematica

Tesi di Laurea Triennale

Il Teorema di Quillen-Suslin

Candidato:

Carlo Sircana

Relatore:

Prof.ssa Patrizia Gianni

Anno Accademico 2013/2014

Indice

Introduzione

Nel 1955 Serre, nel suo articolo *"Faisceaux Algébriques Cohérents"*, si domandò se ogni fibrato vettoriale algebrico localmente banale su uno spazio affine fosse globalmente banale, problema da allora noto come "Congettura di Serre". Poiché i fibrati vettoriali algebrici corrispondono ai fasci coerenti localmente liberi, fu possibile riformulare la congettura in termini puramente algebrici: è vero che ogni modulo proiettivo finitamente generato su un anello di polinomi su un campo è libero? Il primo passo verso la soluzione del problema lo fece lo stesso Serre, che introdusse la nozione di modulo *stabilmente libero*, ovvero nucleo di un omomorfismo tra moduli liberi. Dimostrò che ogni modulo proiettivo su un anello di polinomi è stabilmente libero, utilizzando i concetti di anello *regolare* e di *risoluzione*; tale risultato è noto come teorema di Serre. Il teorema di Serre legò quindi i concetti di anelli regolari, cioè anelli noetheriani per i quali ogni modulo su di essi ammette una risoluzione libera finita, moduli proiettivi e moduli stabilmente liberi sugli anelli di polinomi. Tale risultato permise di compiere un passo decisivo verso la risoluzione della congettura, traducendo il problema in forma matriciale. L'equivalenza tra moduli stabilmente liberi e moduli liberi divenne analoga alla proprietà di completamento a base dei vettori *unimodulari*, vettori le cui componenti generano tutto l'anello.

In questa tesi, verranno trattate con particolare attenzione le proprietà delle risoluzioni e il teorema di Serre, fino ad arrivare alla soluzione della congettura, raggiunta nel 1976 Daniel Quillen e Andrei Suslin [4]. Si esporranno le dimostrazioni di Suslin e una dimostrazione successiva di Vaserstein [5]. Tali prove sono di carattere astratto; si terminerà con una dimostrazione algoritmica del teorema, che permette di ottenere esplicitamente un isomorfismo tra il modulo dato e un modulo libero. Tale dimostrazione è dovuta a Sturmfels e Logar [1], che esplicitarono ogni passaggio della prova di Va-

serstein. La dimostrazione procede risolvendo il problema su anelli locali e effettuando poi un "patching" delle informazioni per ottenere quanto voluto. L'algoritmo si fonda sull'utilizzo di una risoluzione libera finita del modulo proiettivo dato; si suggeriscono due metodi per il calcolo di quest'ultima, entrambi incentrati sul calcolo del modulo delle *sizigie*. Il primo è diretto ed è basato sulla dimostrazione del teorema delle *sizigie di Hilbert*; il secondo invece calcola prima una forma monomiale della risoluzione e la rielabora per trovare la successione esatta richiesta.

Quillen e Suslin non si fermarono al caso di anelli di polinomi su un campo, ma ottennero lo stesso risultato per anelli di polinomi su domini a ideali principali (PID). Si contemplerà anche questo caso, sviluppando la teoria per garantire la possibilità di agire mediante trasformazioni invertibili su un vettore unimodulare fino ad ottenere un polinomio monico tra i coefficienti di un vettore unimodulare. Tale obiettivo viene raggiunto mediante il teorema del *polinomio monico di Suslin*.

Capitolo 1

Il teorema di Serre

1.1 Risoluzioni

Il concetto di modulo proiettivo è stato fondamentale negli ultimi 50 anni, soprattutto per la sua importanza in geometria algebrica e in algebra omologica e per i legami con le successioni esatte. Questo è chiaro fin dalla definizione; un modulo P si dice infatti proiettivo se vale una delle seguenti condizioni equivalenti:

- Ogni successione esatta $0 \to N \to M \to P \to 0$ spezza
- P è addendo diretto di un modulo libero

Notiamo anche che un modulo libero è sempre proiettivo. Una domanda interessante è capire quando è vero il viceversa, cioè sotto quali condizioni un modulo proiettivo è libero. Sappiamo che questo è vero quando si considerano moduli su un campo $\mathbb{K}$ e anche per moduli su un dominio a ideali principali o su anelli locali. Ciò che vorremmo ottenere è una generalizzazione dell'equivalenza proiettivo-libero su anelli di polinomi. Per questo, ci serve intanto approfondire due concetti fondamentali: la nozione di risoluzione e quella di modulo stabilmente libero.

Definizione 1.1. Sia M un A-modulo. Una *risoluzione* di M è una successione esatta di A-moduli del tipo

$$\cdots \to E_n \to E_{n-1} \to \cdots \to E_0 \to M \to 0$$

Se ogni E_i è libero e finitamente generato, la successione si dice *risoluzione libera*. Una risoluzione si dice *finita* se esiste un indice $n \in \mathbb{N}$ tale che $E_i = 0 \ \forall i \geq n$.

Indicheremo con E_i i moduli che compongono una risoluzione. Notiamo che ogni modulo ammette una risoluzione con gli E_i liberi non necessariamente finitamente generati. Infatti ogni modulo è quoziente di un modulo libero E_0,

$$E_0 \xrightarrow{\varphi} M \to 0$$

e possiamo continuare la costruzione all'indietro ragionando su $\operatorname{Ker}\varphi$. Se aggiungiamo l'ipotesi che l'anello A sia noetheriano, allora possiamo anche scegliere la risoluzione in modo tale che ogni E_i sia libero e finitamente generato. Non abbiamo condizioni sulla finitezza di una risoluzione libera: siamo allora interessati a capire quando un modulo ammette una risoluzione libera finita.

Definizione 1.2. Un A-modulo E si dice *stabilmente libero* se esiste un modulo libero F finitamente generato tale che $E \oplus F$ è libero e finitamente generato.

In altre parole, i moduli stabilmente liberi possono essere visti come il nucleo di un omomorfismo tra due moduli liberi finitamente generati. Infatti, considerato un omomorfismo $\varphi\colon A^n \to A^m$, si può considerare la successione esatta corta

$$0 \to \operatorname{Ker}(\varphi) \to A^n \xrightarrow{\varphi} A^m$$

che spezza (perché A^m è proiettivo), da cui $A^n \simeq \operatorname{Ker}(\varphi) \oplus A^m$ e dunque $\operatorname{Ker}(\varphi)$ è stabilmente libero.

Su un anello a ideali principali (PID), per esempio, la nozione di modulo stabilmente libero coincide con quella di modulo libero: sappiamo infatti che su tali anelli un sottomodulo di un modulo libero è libero. Ciò non accade sempre; vedremo un controesempio nel Capitolo 3, dopo aver sviluppato la teoria.

Osservazione 1.3. Un modulo stabilmente libero è necessariamente proiettivo e finitamente generato, perché addendo diretto di un modulo libero finitamente generato.

Alcune domande possono sorgere in maniera spontanea. Per esempio: perché nella definizione di modulo stabilmente libero si richiede che il mo-

dulo libero F sia finitamente generato? La risposta risiede nella seguente proposizione:

Proposizione 1.4. *Sia P un A-modulo proiettivo. Allora esiste F libero tale che $P \oplus F$ è libero.*

Dimostrazione. Poiché P è proiettivo, esiste Q tale che $P \oplus Q = E$, dove E è un A-modulo libero. Sia allora $F = \oplus_{\mathbb{N}} E$. Pertanto,

$$\begin{aligned} P \oplus F \simeq & P \oplus E \oplus E \cdots \\ \simeq & P \oplus (Q \oplus P) \oplus (Q \oplus P) \cdots \\ \simeq & (P \oplus Q) \oplus (P \oplus Q) \oplus \cdots \\ \simeq & E \oplus E \oplus \cdots \\ \simeq & F \end{aligned}$$

Dunque, come voluto, $P \oplus F \simeq F$. □

Dunque, il caso di un modulo libero non finitamente generato è più semplice. A questo punto, ha senso chiedersi cosa succede se si rimuove l'ipotesi che il modulo E sia finitamente generato. Anche in questo caso, la risposta è sorprendente:

Proposizione 1.5. *Sia P un A-modulo non finitamente generato tale che $P \oplus A^m \simeq F$, con F libero. Allora P è libero.*

Dimostrazione. Supponiamo $P \oplus A^m \simeq F$, con F modulo libero. F non può essere finitamente generato; se lo fosse infatti, si avrebbe che le immagini dei generatori di F tramite l'omomorfismo

$$\pi \colon F \simeq A^m \oplus P \longrightarrow P$$

genererebbero P, che invece per ipotesi non è finitamente generato. Sia allora $\{e_i \mid i \in I\}$ una base di F e consideriamo la successione:

$$0 \to P \xrightarrow{i} F \xrightarrow{\pi} A^n \to 0$$

Poichè A^m è finitamente generato, esiste un insieme $I_0 \subseteq I$ di cardinalità finita tale che, detto $F_0 = \mathrm{Span}\{e_i \mid i \in I_0\}$, $\pi_{|_{F_0}}$ sia surgettiva. Di conseguenza, abbiamo $F = P + F_0$. Sia $Q = P \cap F_0$. Abbiamo le due successioni

esatte:

$$0 \to Q \to P \to {}^{P}\!/_{Q} \to 0$$
$$0 \to Q \to F_0 \to A^m \to 0$$

Utilizzando il terzo teorema di isomofismo,

$${}^{F}\!/_{F_0} \simeq {}^{P+F_0}\!/_{F_0} \simeq {}^{P}\!/_{P \cap F_0} \simeq {}^{P}\!/_{Q}$$

e dunque ${}^{P}\!/_{Q}$ è libero, di rango infinito. Possiamo scrivere ${}^{P}\!/_{Q} \simeq A^m \oplus F_1$, dove F_1 è un A-modulo libero. Le successioni spezzano, dunque

$$P \simeq {}^{P}\!/_{Q} \oplus Q \simeq A^m \oplus F_1 \oplus Q \simeq F_0 \oplus F_1$$

Abbiamo mostrato che P è libero, come voluto. □

Restringiamo la nostra attenzione ai moduli proiettivi finitamente generati. Notiamo che se un modulo ammette una risoluzione libera finita, deve essere necessariamente finitamente generato; è allora possibile che un modulo stabilmente libero ammetta una risoluzione libera finita. In realtà, questo è sempre vero e vale anche di più.

Teorema 1.6. *Sia M un A-modulo proiettivo.*

M è stabilmente libero $\iff$ M ammette una risoluzione libera finita

Dimostrazione. Supponiamo dapprima che M sia stabilmente libero. Per definizione, esiste F modulo libero finitamente generato tale che $F \oplus M \simeq A^n$. Di conseguenza, la successione

$$0 \to F \to A^n \to M \to 0$$

è una risoluzione libera finita di M.
Viceversa, supponiamo M ammetta una risoluzione libera finita. Dimostriamo l'enunciato per induzione sulla lunghezza della risoluzione. Se $n = 0$, abbiamo la successione

$$0 \to E_0 \to M \to 0$$

e dunque $M \simeq E_0$, cioè M è libero e finitamente generato e dunque stabilmente libero. Supponiamo ora di avere una risoluzione libera di lunghezza

n

$$0 \to E_n \xrightarrow{f_n} E_{n-1} \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M \to 0$$

Sia $P = \operatorname{Ker} f_0$; possiamo allora considerare la successione esatta

$$0 \to P \to E_0 \to M \to 0$$

Poichè M è proiettivo, la successione spezza, dunque $E_0 \simeq M \oplus P$. Per costruzione allora, P ammette una risoluzione libera di lunghezza $n-1$

$$0 \to E_n \xrightarrow{f_n} E_{n-1} \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_2} E_1 \xrightarrow{f_1} P \to 0$$

Inoltre P è proiettivo e finitamente generato perché addendo diretto di un modulo libero finitamente generato. Dunque, per ipotesi induttiva, P è stabilmente libero; per definizione esiste un modulo libero finitamente generato F tale che $P \oplus F \simeq A^n$. Allora, $A^n \oplus M \simeq P \oplus F \oplus M \simeq E_0 \oplus F$, che è libero e finitamente generato. □

Si potrebbe pensare ora che l'esistenza di una risoluzione libera finita di un modulo sia allora una proprietà non banale. Proviamo allora a considerare delle risoluzioni in cui i moduli E_i sono stabilmente liberi, meno pretenziose a prima vista rispetto a quelle libere. In realtà, se un modulo ammette l'una, ammette anche l'altra:

Proposizione 1.7. *Sia M un A-modulo. Sono equivalenti:*

- *M ammette una risoluzione libera di lunghezza n*
- *M ammette una risoluzione stabilmente libera di lunghezza n.*

Dimostrazione. Un'implicazione è ovvia, perché i moduli liberi finitamente generati sono in particolare stabilmente liberi. Mostriamo ora l'altra implicazione iterativamente, illustrando un procedimento per ottenere una risoluzione libera di lunghezza n da quella di partenza. Supponiamo quindi di avere una risoluzione stabilmente libera:

$$0 \to E_n \xrightarrow{f_n} E_{n-1} \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M \to 0$$

E_i è stabilmente libero, dunque esiste un modulo libero F_i tale che $E_i \oplus F_i$ è libero. Detto $F = F_i \oplus F_{i+1}$, possiamo allora considerare la risoluzione:

$$0 \to E_n \xrightarrow{f_n} \dots \xrightarrow{f_{i-1}} E_i \oplus F \xrightarrow{f_i \oplus id} E_{i+1} \oplus F \xrightarrow{f_{i+1}} \dots \xrightarrow{f_1} E_0 \xrightarrow{f_0} M \to 0$$

Iterativamente, possiamo sostituire tutti i moduli con dei moduli liberi, da cui la tesi. □

Chiaramente, un modulo può ammettere diverse risoluzioni. Se però ammette una risoluzione libera finita, può essere interessante considerare il minimo delle lunghezze di tali risoluzioni:

Definizione 1.8. Sia M un A-modulo. Definiamo la *dimensione stabilmente libera* di M come la minima delle lunghezze di una risoluzione stabilmente libera finita di M.

Osservazione 1.9. Nel caso la dimensione stabilmente libera sia 0, il modulo considerato è banalmente stabilmente libero.

L'obiettivo è ora quello di sviluppare la teoria in modo che si possano affrontare delle dimostrazioni per induzione sulla dimensione stabilmente libera. Il prossimo lemma sarà fondamentale nella strada verso questo risultato.

Lemma 1.10 (di Schaunel)**.** *Consideriamo le successioni esatte*

$$0 \to K \to P \to M \to 0$$
$$0 \to K' \to P' \to M \to 0$$

e supponiamo che P e P' siano proiettivi. Allora $K \oplus P' \simeq K' \oplus P$.

Dimostrazione. Consideriamo il diagramma:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \xrightarrow{f} & P & \xrightarrow{g} & M & \longrightarrow & 0 \\ & & & & \varphi \downarrow & & id \downarrow & & \\ 0 & \longrightarrow & K' & \xrightarrow[f']{} & P' & \xrightarrow[g']{} & M & \longrightarrow & 0 \end{array}$$

Dato che P è proiettivo, esiste l'omomorfismo φ del diagramma che fa commutare il quadrato a destra. Costruiamo ora una $\psi \colon K \to K'$ che faccia commutare anche l'altra parte. L'unico modo sensato per far questo è definire

la funzione in questo modo:

$$\begin{array}{rccc} \psi\colon & K & \longrightarrow & K' \\ & k & \longmapsto & (f')^{-1}(\varphi(f(k))) \end{array}$$

Verifichiamo la buona definizione di tale funzione. Notiamo che f' è iniettiva, quindi effettivamente a un elemento del dominio viene associato al più un elemento del codominio. Bisogna ora verificare che $\mathrm{Im}(\varphi \circ f) \subseteq \mathrm{Im}(f')$. Per commutatività della parte destra del diagramma, $g' \circ \varphi \circ f = id \circ g \circ f = 0$, dunque $\mathrm{Im}(\varphi \circ f) \subseteq \mathrm{Ker}\, g' = \mathrm{Im}(f')$, quindi ψ è ben definita. Da questo diagramma, ricaviamo la successione:

$$0 \to K \xrightarrow{s_1} P \oplus K' \xrightarrow{s_2} P' \to 0$$

dove $s_1(k) = (f(k), \psi(k))$ e $s_2(p,k) = \varphi(p) - f'(k)$. Mostriamo che tale successione è esatta.

- s_1 è iniettiva perché f è iniettiva.
- s_2 è surgettiva, perché f' è surgettiva.
- $\mathrm{Im}(s_1) \subseteq \mathrm{Ker}\, s_2$, perché

  $$s_2(s_1(x)) = s_2(f(x), \psi(x)) = \varphi(f(x)) - f'(\psi(x)) = 0$$

  per commutatività del diagramma.
- $\mathrm{Ker}\, s_2 \subseteq \mathrm{Im}(s_1)$; infatti, sia $(x,y) \in \mathrm{Ker}\, s_2$.

  $$s_2(x,y) = \varphi(x) - f'(y) = 0 \Rightarrow \varphi(x) = f'(y)$$

  Per iniettività di f, $\exists! k \in K$ t.c. $f(k) = x$. Notiamo ora che $\varphi(f(k)) = f'(\psi(k)) = f'(y)$. Per iniettività di f', $\psi(k) = y$, e dunque $s_1(k) = (x,y)$.

Dato che la successione è esatta e P' è proiettivo, spezza, e dunque $K \oplus P' \simeq P \oplus K'$. □

Definizione 1.11. Siano P e Q due A-moduli. P e Q si dicono *stabilmente isomorfi* se esistono due moduli liberi finitamente generati F_1 e F_2 tali che $F_1 \oplus P \simeq F_2 \oplus Q$.

Notiamo che questa è una generalizzazione della definizione di modulo stabilmente libero; due moduli stabilmente liberi sono sempre stabilmente isomorfi.

Proposizione 1.12. *Siano M_1, M_2 moduli stabilmente isomorfi e siano*

$$0 \to N_1 \to E_1 \to M_1 \to 0$$
$$0 \to N_2 \to E_2 \to M_2 \to 0$$

due successioni esatte, con E_1 ed E_2 stabilmente liberi. Allora N_1 è stabilmente isomorfo a N_2.

Dimostrazione. Per ipotesi, esistono $n, m \in \mathbb{N}$ tali che $M_1 \oplus A^n$ e $M_2 \oplus A^m$ siano isomorfi. Otteniamo allora le successioni esatte:

$$0 \to N_1 \to E_1 \oplus A^n \to M_1 \oplus A^n \to 0$$
$$0 \to N_2 \to E_2 \oplus A^m \to M_2 \oplus A^m \to 0$$

Di conseguenza, per il lemma di Schaunel 1.10, $N_1 \oplus E_2 \oplus A^m \simeq N_2 \oplus E_1 \oplus A^n$. Poichè E_1 e E_2 sono stabilmente liberi, esiste $k \in \mathbb{N}$ per il quale $E_1 \oplus A^k$ e $E_2 \oplus A^k$ sono entrambi liberi e finitamente generati. Di conseguenza, $N_1 \oplus E_2 \oplus A^k \oplus A^m \simeq N_2 \oplus E_1 \oplus A^k \oplus A^n$ e quindi N_1 è stabilmente isomorfo a N_2. □

Disporre di una risoluzione stabilmente libera di un modulo permette anche di completare altre risoluzioni:

Proposizione 1.13. *Sia M un modulo che ammette una risoluzione stabilmente libera di lunghezza n*

$$0 \to E_n \to \dots E_0 \to M \to 0$$

Sia

$$F_m \to \dots F_0 \to M \to 0$$

una successione esatta dove ogni F_i è stabilmente libero.

1. *$\forall m < n-1$ esiste F_{m+1} stabilmente libero tale che estende la successione:*

$$F_{m+1} \to F_m \to \dots F_0 \to M \to 0$$

2. *Se* $m = n - 1$, *detto* $F_n = \mathrm{Ker}(F_{n-1} \to F_{n-2})$, *si ha che* F_n *è stabilmente libero e*

$$0 \to F_n \to F_{n-1} \to \dots F_0 \to M \to 0$$

è una risoluzione stabilmente libera.

Dimostrazione. Consideriamo i sottomoduli $K_i = \mathrm{Ker}(E_i \to E_{i-1})$, $K_0 = \mathrm{Ker}(E_0 \to M)$, $K'_i = \mathrm{Ker}(F_i \to F_{i-1})$ e $K'_0 = \mathrm{Ker}(F_0 \to M)$. Mostriamo induttivamente che K_i è stabilmente isomorfo a K'_i. Il passo base è semplice, poiché M è isomorfo tramite l'identità a M. Supponiamo allora che ogni modulo K_i per $i < m$ sia stabilmente isomorfo a K'_i. Abbiamo le successioni esatte:

$$0 \to K_m \to E_m \to K_{m-1} \to 0$$
$$0 \to K'_m \to F_m \to K'_{m-1} \to 0$$

Per la proposizione 1.12, abbiamo allora che K_m è stabilmente isomorfo a K'_m, come voluto. Di conseguenza, esistono due moduli liberi F e F' finitamente generati tali che

$$K_m \oplus F \simeq K'_m \oplus F'$$

1. Se $m < n-1$, K_m è una immagine omomorfa di E_{m+1}; dunque $K_m \oplus F$ è immagine omomorfa di $E_{m+1} \oplus F$; di conseguenza lo è anche $K'_m \oplus F'$. Dunque K'_m è immagine omomorfa di $E_{m+1} \oplus F$; allora $F_{m+1} = E_{m+1} \oplus F$ è il modulo cercato.

2. Se $m = n - 1$, $K_m = E_n$ a meno di isomorfismo e dunque K_m è stabilmente libero. Di conseguenza, $K_m \oplus F$ è stabilmente libero e, poiché abbiamo mostrato che $K_m \oplus F \simeq K'_m \oplus F'$, si ha che anche $K'_m \oplus F'$ è stabilmente libero. Allora, poiché F' è libero, anche K'_m è stabilmente libero, dunque definendo $F_n = K'_m$ si ha la tesi.

□

La proposizione può sembrare fine a se stessa; il corollario è però utilissimo e ci permette di indurre nelle prossime dimostrazioni sulla dimensione stabilmente libera di un modulo:

Corollario 1.14. *Sia E un modulo stabilmente libero e supponiamo che M abbia dimensione stabilmente libera n. Sia*

$$0 \to N \to E \to M \to 0$$

una successione esatta. Allora N ha dimensione stabilmente libera $\leq n-1$.

Dimostrazione. Dalla proposizione 1.13, possiamo completare l'omomorfismo

$$E \xrightarrow{f} M$$

a una risoluzione stabilmente libera di lunghezza n:

$$0 \to E_n \to \ldots \xrightarrow{g} E \xrightarrow{f} M \to 0$$

Poichè $\mathrm{Ker}(f) \simeq N$, si ha che N ammette la risoluzione stabilmente libera

$$0 \to E_n \to \ldots \xrightarrow{g} N \to 0$$

e dunque la tesi. □

Cerchiamo ora un legame tra le successioni esatte e l'esistenza di date risoluzioni libere finite: in particolare, vogliamo mostrare che se due moduli di una successione esatta corta ammettono una risoluzione libera finita, allora la ammette anche il terzo. Per questo, mostriamo intanto che il pull-back esiste nella categoria dei moduli noetheriani su anelli noetheriani:

Lemma 1.15. *Sia A un anello noetheriano e siano M, M', N A-moduli finitamente generati. Siano $f\colon M \to N$ e $g\colon M' \to N$ due omomorfismi surgettivi. Allora esiste un modulo stabilmente libero P e due omomorfismi surgettivi $\tilde{f}$ e $\tilde{g}$ che fanno commutare il seguente diagramma:*

$$\begin{array}{ccccc} & \tilde{f} & P & \tilde{g} & \\ & \swarrow & & \searrow & \\ M & & & & M' \\ & f \searrow & & \swarrow g & \\ & & N & & \end{array}$$

Dimostrazione. Consideriamo l'omomorfismo di A-moduli

$$\begin{array}{rccc} s\colon & M \times M' & \longrightarrow & N \\ & (m, m') & \longmapsto & f(m) - g(m') \end{array}$$

e sia $E = \mathrm{Ker}(s)$. Notiamo che per ipotesi di noetherianità, E è finitamente generato. Sia P un modulo stabilmente libero che ammette un omomorfismo surgettivo h su E (per esempio, basta prendere un modulo libero finitamente generato). Definiamo allora $\tilde{f} = \pi_M \circ h$ e $\tilde{g} = \pi_{M'} \circ h$. Mostriamo che $f \circ \tilde{f} = g \circ \tilde{g}$. Sia $x \in P$. Allora $h(x) = (a, b) \in E$. Di conseguenza, poiché $E = \mathrm{Ker}(s)$, dopo aver composto con le proiezioni, si ottiene $f(a) = g(b)$, dunque il diagramma commuta. □

Lemma 1.16. *Sia A un anello noetheriano; consideriamo una successione esatta di A-moduli finitamente generati*

$$0 \to M' \to M \to M'' \to 0$$

Allora esistono dei moduli stabilmente liberi E', E, E'' e dei moduli finitamente generati N, N', N'' per i quali il seguente diagramma commuti:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Dimostrazione. Sia E'' un modulo stabilmente libero che ammette un omomorfismo surgettivo su M''. Per il lemma 1.15, esiste un modulo E_1 che rende commutativo il seguente diagramma:

$$\begin{array}{ccccccccc}
 & & & & E_1 & \longrightarrow & E'' & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

Sia ora E_2 un modulo stabilmente libero che ammette un omomorfismo surgettivo su M' e definiamo $E = E_1 \oplus E_2$. Possiamo allora estendere gli

omomorfismi $E \to M$ e $E \to E''$ affinché il diagramma commuti. Sia allora $E' = \mathrm{Ker}(E \to E'')$. Per costruzione, $E_2 \subseteq E'$ e dunque abbiamo ottenuto il diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

A questo punto, i candidati N, N', N'' sono $\mathrm{Ker}(E \to M)$, $\mathrm{Ker}(E' \to M')$ e $\mathrm{Ker}(E'' \to M'')$. Ma questa riga è proprio l'inizio della successione esatta data dal lemma del serpente, e dunque abbiamo ottenuto il diagramma cercato. □

Teorema 1.17. *Sia A un anello noetheriano e consideriamo una successione esatta di A-moduli*

$$0 \to M' \to M \to M'' \to 0$$

Se due moduli della successione ammettono una risoluzione libera finita, allora anche il terzo la ammette.

Dimostrazione. Ricordiamo che se un modulo ammette una risoluzione libera finita, allora è necessariamente finitamente generato. Nelle ipotesi di noetherianità dell'anello, in ogni caso due moduli della successione risultano noetheriani e questo è sufficiente a fornire la noetherianità del terzo. Per il lemma 1.16, abbiamo allora il diagramma:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

dove E, E', E'' sono stabilmente liberi. Discutiamo ora i tre possibili casi:

- Assumendo che M, M' ammettano una risoluzione libera finita, dimostriamo in questo caso l'enunciato per induzione sulla dimensione stabilmente libera di M. Se M è stabilmente libero, che è il caso base, si ha la successione

$$0 \to M' \to M \to M'' \to 0$$

Poiché per ipotesi M' ammette una risoluzione libera finita,

$$0 \to F_1 \to \cdots \to F_s \to M' \to 0$$

la seguente (sfruttando l'iniettività della mappa $M' \to M$)

$$0 \to F_1 \to \cdots \to F_s \to M \to M'' \to 0$$

è una risoluzione stabilmente libera di M''. Il passo induttivo è ora semplice; basta infatti notare che la dimensione stabilmente libera di N è $\leq n-1$ e che la dimensione stabilmente libera di N' è finita. Per ipotesi induttiva N'' ammette una risoluzione stabilmente libera finita

$$0 \to P_m \to P_{m-1} \to \cdots \to P_0 \to N'' \to 0$$

e da questa la risoluzione

$$0 \to P_m \to P_{m-1} \to \cdots \to P_0 \to E'' \to M'' \to 0$$

che è stabilmente libera poiché E'' è stabilmente libero.

- Supponiamo ora che M', M'' ammettano una risoluzione libera finita. Procediamo per induzione sul massimo tra la dimensione stabilmente libera di M' e quella di M''. Nel caso base, sia M' che M'' sono stabilmente liberi, dunque sono proiettivi e la successione spezza: $M \simeq M' \oplus M''$ e quindi M è stabilmente libero. Per il passo induttivo, notiamo che la dimensione stabilmente libera di N' e N'' è rispettivamente minore di quella di M' e di M''; per ipotesi induttiva allora N ammette una risoluzione stabilmente libera e dunque come prima possiamo produrne una per M.

- Supponiamo che M, M'' ammettano una risoluzione libera finita. Di-

mostriamo l'enunciato per induzione sul massimo tra la dimensione stabilmente libera di M e quella di M''. Il passo base discende direttamente dalla proposizione 1.13. Il passo induttivo è automatico: infatti la dimensione stabilmente libera di N'' e N è rispettivamente minore di quella di M'' e M. Per ipotesi induttiva, N' ammette una risoluzione stabilmente libera

$$0 \to Q_m \to Q_{m-1} \to \cdots \to Q_0 \to N' \to 0$$

e da questa ricaviamo la risoluzione cercata:

$$0 \to Q_m \to Q_{m-1} \to \cdots \to Q_0 \to E' \to M' \to 0$$

□

1.2 Il gruppo di Grothendieck K_0

Sia A un anello commutativo con identità. Sappiamo che le classi di isomorfismo di moduli proiettivi su A formano un monoide (commutativo) grazie all'operazione di somma diretta; dato un A-modulo proiettivo P, indichiamo con (P) la sua classe di isomorfismo. Consideriamo il gruppo abeliano libero generato da (P) al variare di P tra i moduli proiettivi finitamente generati su A. Intuitivamente vorremmo però imporre le relazioni del tipo:

$$(P \oplus Q) = (P) + (Q)$$

Possiamo allora considerare H il sottogruppo generato da tutte queste relazioni. Definiamo il *gruppo di Grothendieck* $K_0(A)$ come il gruppo quoziente G/H. Un generico elemento del gruppo di Grothendieck $[P]$ si può scrivere come $[P] = [Q] - [T]$. Le classi di equivalenza di $K_0(A)$ sono strettamente collegate alla nozione di moduli stabilmente liberi introdotta nella sezione precedente. Abbiamo infatti la seguente caratterizzazione:

Proposizione 1.18. *Siano P e Q due moduli proiettivi finitamente generati. Sono equivalenti:*

1. *Esiste un modulo proiettivo finitamente generato T tale che $P \oplus T \simeq Q \oplus T$.*

2. $[P] = [Q]$

3. Esiste $t \in \mathbb{N}$ *tale che* $P \oplus A^t \simeq Q \oplus A^t$

Dimostrazione.

$1 \Rightarrow 2$ Se $P \oplus T \simeq Q \oplus T$, si ha:

$$[Q] + [T] = [Q \oplus T] = [P \oplus T] = [P] + [T] \Rightarrow [Q] = [P]$$

$2 \Rightarrow 1$ Se $[P] = [Q]$, allora $(P) - (Q) \in H$, e dunque

$$(P) - (Q) = \sum_i (P_i \oplus Q_i) - (P_i) - (Q_i) - \sum_j (P'_j \oplus Q'_j) - (P'_j) - (Q'_j)$$

Di conseguenza,

$$(P) + \sum (P'_j \oplus Q'_j) + \sum (P_i) + (Q_i) = (Q) + \sum (P_i \oplus Q_i) + \sum (P'_j) + (Q'_j)$$

Poichè G è libero, si ha che $\sum(M_\alpha) = \sum(N_\beta)$ implica $\oplus M_\alpha \simeq \oplus N_\beta$. Sia $T = \sum P'_j \oplus Q'_j \oplus \sum P_i \oplus Q_i$; allora $P \oplus T \simeq Q \oplus T$, come voluto.

$3 \Rightarrow 1$ Basta ricordare che i moduli liberi sono proiettivi.

$1 \Rightarrow 3$ Supponiamo $P \oplus T \simeq Q \oplus T$. Poichè T è proiettivo e finitamente generato, esiste un modulo S tale che $T \oplus S \simeq A^n$. Di conseguenza, $P \oplus A^n \simeq Q \oplus A^n$.

□

Dalla proposizione 1.18, discende direttamente il seguente:

Corollario 1.19. *Due moduli proiettivi che stanno nella stessa classe del gruppo di Grothendieck sono stabilmente isomorfi.*

La conoscenza del gruppo di Grothendieck di un anello caratterizza in maniera univoca i moduli stabilmente liberi su di esso:

Proposizione 1.20. *P è stabilmente libero* $\iff [P] \in \langle [A] \rangle$

Dimostrazione. Supponiamo che P sia stabilmente libero. Allora $P \oplus A^m \simeq A^n$ per oppurtuni $n, m \in \mathbb{N}$. Allora

$$[P] + [A^m] = [A^n] \Rightarrow [P] = [A^{m-n}] = (m-n)[A]$$

e dunque $P \in \langle [A] \rangle$. Viceversa, se $[P] = [A^s]$, per la proposizione 1.18 esiste $t \in \mathbb{N}$ tale che $P \oplus A^t \simeq A^{s+t}$, e quindi P è stabilmente libero. □

Dunque, le nozioni di modulo proiettivo e modulo stabilmente libero coincidono se e solo se il gruppo di Grothendieck $K_0(A)$ è isomorfo a $\mathbb{Z}$. Il gruppo di Grothendieck di un campo $\mathbb{K}$ è allora sicuramente $\mathbb{Z}$, poiché tutti i moduli proiettivi sono liberi e dunque banalmente appartengono a $\langle [\mathbb{K}] \rangle$. Non sappiamo dire però nulla su anelli più complicati: scopo della prossima sezione sarà indagare sul gruppo di Grothendieck di anelli di polinomi.

1.3 Il teorema di Serre

In questa sezione, ci proponiamo di dimostrare che, se A un PID, ogni modulo proiettivo finitamente generato su $A[x_1, \dots x_n]$ è stabilmente libero. Questo è il primo passo verso la risoluzione della congettura: ci basterà infatti mostrare che i moduli stabilmente liberi sono liberi. In termini di gruppo di Grothendieck, il teorema di Serre equivale a dire che $K_0(A[x_1, \dots, x_n]) \simeq \mathbb{Z}$, generato dalla classe di $A[x_1, \dots, x_n]$. Dimostreremo cioè che esiste un isomorfismo tra $K_0(A)$ e $K_0(A[x])$; questo argomento applicato induttivamente ci porterà alla tesi. Considereremo i seguenti anelli:

Definizione 1.21. Un anello A si dice *regolare* se è noetheriano e se ogni A-modulo finitamente generato ammette una risoluzione libera finita.

Se ogni A-modulo ammette una risoluzione libera finita, in base alla proposizione 1.6, in particolare si ha che i moduli proiettivi sono stabilmente liberi. Inoltre, se l'anello non fosse noetheriano, potrebbe accadere che il nucleo di un omomorfismo tra moduli liberi che compongono una risoluzione non sia finitamente generato. Quello che vogliamo dimostrare è allora che se A è regolare, allora lo è anche $A[x]$. Useremo come strumento le filtrazioni di un modulo:

Proposizione 1.22. *Sia M un A-modulo che ammette una filtrazione*

$$M = M_n \supseteq M_{n-1} \supseteq \cdots \supseteq M_1 \supseteq M_0 = 0$$

dove $M_{i+1}/M_i \simeq A/P_i$, $P_i \in Spec(A)$. Se A/P ammette una risoluzione finita $\forall P \in Spec(A)$, allora M ammette una risoluzione libera finita.

Dimostrazione. Mostriamo iterativamente che se l'enunciato vale per M_i, allora vale anche per M_{i+1}. Al primo passo, $M_0 = 0$ e dunque ammette banalmente una risoluzione libera finita. Utilizzando la successione esatta:

$$0 \to M_i \to M_{i+1} \to {}^{M_i}\!/_{M_{i+1}} \simeq {}^{A}\!/_{P_i} \to 0$$

si ha che per ipotesi ${}^{A}\!/_{P_i}$ ammette una risoluzione libera finita, per ipotesi induttiva la ammette anche M_i. Per la proposizione 1.17 la tesi. □

Come corollario, otteniamo una definizione equivalente di anello regolare, più maneggevole per le dimostrazioni.

Corollario 1.23. *Sia A un anello noetheriano. A è regolare $\iff \forall P \in Spec(A)$, ${}^{A}\!/_{P}$ ammette una risoluzione libera finita.*

Dimostrazione. Chiaramente, se A è regolare, ${}^{A}\!/_{P}$ ammette una risoluzione libera finita per definizione. Mostriamo l'altra implicazione. Sia M un A-modulo; poiché A è noetheriano, possiamo trovare una sua filtrazione [5, pag. 419]

$$M = M_{n+1} \supseteq M_n \supseteq \cdots \supseteq M_0 = (0)$$

dove ogni quoziente ${}^{M_i}\!/_{M_{i+1}}$ è isomorfo a ${}^{A}\!/_{P}$, $P \in Spec(A)$. Dalla proposizione 1.22 segue la tesi. □

Siamo allora pronti per il primo passo verso il teorema di Serre. Poiché l'obiettivo è mostrare che ogni modulo proiettivo ammette una risoluzione libera finita, vogliamo mostrare che la regolarità di un anello viene ereditata da un anello di polinomi. Questo basterebbe poiché sappiamo che per un modulo proiettivo ammettere una risoluzione libera finita è equivalente ad essere stabilmente libero.

Teorema 1.24 (di Swan)**.** *Sia A un anello regolare. Allora $A[x]$ è regolare.*

Dimostrazione. Notiamo che $A[x]$ è noetheriano per il teorema della base di Hilbert. In virtù del corollario 1.23, basta allora mostrare che ${}^{A[x]}\!/_{P}$ ammette una risoluzione libera finita $\forall P \in Spec(A[x])$. Dato $P \in Spec(A[x])$, possiamo considerare la successione esatta:

$$0 \to P \to A[x] \to {}^{A[x]}\!/_{P} \to 0$$

Dunque, per mostrare che ${}^{A[x]}\!/_{P}$ ammette una risoluzione libera finita, è sufficiente esibirne una per P per la proposizione 1.17. Supponiamo per assurdo che esistano dei primi per i quali ${}^{A[x]}\!/_{P}$ non ammetta tale risoluzione. Consideriamo l'insieme:

$$\Sigma = \{P \cap A \mid P \in Spec(A[x]) \wedge {}^{A[x]}\!/_{P} \textit{ non ha risoluzioni libere finite}\}$$

Poiché A è noetheriano, esiste un elemento massimale I per Σ e sia $P \in Spec(A[x])$ un primo che realizza tale massimo. Per ipotesi, I ammette una risoluzione libera finita,

$$0 \to E_n \to \cdots \to E_0 \to I \to 0$$

Tensorizzando per $A[x]$, si ottiene:

$$0 \to E_n[x] \to \cdots \to E_0[x] \to I[x] \to 0$$

Dunque $I[x]$ ammette una risoluzione libera finita come $A[x]$-modulo. Notiamo che I è la contrazione di P tramite l'omomorfismo

$$A \to A[x]$$

e dunque I è primo poiché contrazione di un primo: l'anello $A_0 \coloneqq {}^{A}\!/_{I}$ è dunque un dominio. $A_0[x]$, come $A[x]$ modulo, rende esatta la successione

$$0 \to I[x] \to A[x] \to A_0[x] \to 0$$

quindi anche $A_0[x]$ ammette una risoluzione libera finita. Sia $P_0 = {}^{P}\!/_{I[x]}$. Notiamo che ${}^{A[x]}\!/_{P}$ ammette non solo la struttura di $A[x]$-modulo, ma anche quella di $A_0[x]$-modulo, in quanto isomorfo a ${}^{A_0[x]}\!/_{P_0}$. Se mostriamo che P_0 ammette una risoluzione libera finita, otteniamo un assurdo, poiché la successione

$$0 \to I[x] \to P \to P_0 \to 0$$

è esatta e P_0, $I[x]$ ammettono una risoluzione libera finita.
Poichè $A_0[x]$ è noetheriano, esistono $f_1, \ldots, f_n$ dei generatori di P_0 e consideriamo f un polinomio di grado minimo in P_0. A_0 è un dominio e ammette un campo dei quozienti K_0, dove vale la divisione euclidea. Possiamo allora

scrivere, per ogni i:

$$f_i = q_i f + r_i$$

dove $q_i, r_i \in K_0[x]$. Sia d_0 denominatore comune di q_i, r_i al variare di i. Otteniamo allora la relazione in $A_0[x]$:

$$d_0 f_i = q_i' f + r_i'$$

Per le proprietà dell'algoritmo di divisione, poiché $r_i' \in P_0$, $\deg(r_i') < \deg(f)$ e f ha grado minimo in P_0, si ottiene $r_i' = 0\ \forall i$, e dunque:

$$d_0 P_0 \subseteq A_0[x] f = (f)$$

Definiamo il modulo $N = {}^{P_0}\!/_{(f)}$, che può essere visto sia come $A[x]$-modulo, sia come $A_0[x]$-modulo. Per quanto visto sopra, $d_0 \in \mathrm{Ann}(N)$ visto come $A_0[x]$-modulo. Sia ora $d \in A$ tale che $d \equiv d_0\ (I)$. Poiché $d_0 \notin I$, anche $d \notin I$. Come fatto in precedenza, possiamo trovare una filtrazione di N come $A_0[x]$-modulo:

$$N = N_k \supseteq N_{k-1} \supseteq \cdots \supseteq N_0 = (0)$$

dove ${}^{N_{i+1}}\!/_{N_i} \simeq {}^{A_0[x]}\!/_{Q_i}$ e ogni Q_i è un primo associato a N. Siano $\tilde{Q}_i$ le contrazioni dei Q_i tramite la proiezione:

$$\pi \colon A[x] \longrightarrow A_0[x]$$

Tali primi sono dei primi associati a N come $A[x]$-modulo. Ogni $\tilde{Q}_i$ contiene I ed è primo. Inoltre

$$d_0 \in \mathrm{Ann}_{A_0[x]}(N) \Rightarrow d \in \mathrm{Ann}_{A[x]}(N) \Rightarrow d \in \bigcap_{Q \in \mathrm{Ass}(N)} Q$$

Quindi ogni $\tilde{Q}_i$ contiene d. Di conseguenza, i $\tilde{Q}_i$ non possono essere elementi di Σ per massimalità di P. Ne segue che ogni modulo della filtrazione di N ammette una risoluzione libera finita, dunque anche N la ammette per il lemma 1.22.

Inoltre, poiché A_0 è un dominio, $(f) \simeq A_0[x]$ come $A[x]$-moduli e dunque

ammette una risoluzione libera finita. L'esattezza della successione

$$0 \to (f) \to P_0 \to N \to 0$$

implica allora che P_0 ammette una risoluzione libera finita, assurdo. □

Induttivamente, otteniamo il seguente corollario:

Corollario 1.25. *Sia A un anello regolare. Allora $A[x_1, \dots, x_n]$ è regolare.*

Come già anticipato, procediamo ora induttivamente per ottenere il risultato voluto.

Teorema 1.26 (di Serre)**.** *Sia A un PID. Allora ogni modulo proiettivo finitamente generato su $A[x_1, \dots, x_n]$ è stabilmente libero.*

Dimostrazione. Procediamo per induzione sul numero di variabili. Dato che A è un PID, ogni modulo proiettivo finitamente generato è libero, dunque in particolare stabilmente libero. Supponiamo la tesi vera per $A[x_1, \dots, x_n]$, e dimostriamola per $A[x_1, \dots, x_{n+1}]$. $A[x_1, \dots, x_{n+1}]$ è regolare per il teorema di Swan 1.24, dunque ogni modulo finitamente generato ammette una risoluzione libera finita. Per i moduli proiettivi questo è equivalente ad essere stabilmente liberi per il teorema 1.6, come voluto. □

Come anticipato, il teorema di Serre può anche essere visto in termini del gruppo di Grothendieck K_0. Un omomorfismo di anelli $f\colon A \to B$ induce funtorialmente un omomorfismo di gruppi

$$\begin{array}{rccc} \tilde{f}\colon & K_0(A) & \longrightarrow & K_0(B) \\ & [P] & \longmapsto & [P \otimes_A B] \end{array}$$

che sappiamo essere ben definito perché $P \otimes_A B$ è un B-modulo proiettivo. Possiamo vedere allora il gruppo di Grothendieck come un funtore tra la categoria degli anelli e la categoria dei gruppi abeliani. Quindi:

Teorema 1.27 (di Serre)**.** *Sia A un PID. Allora l'omomorfismo di gruppi $\tilde{\imath}\colon K_0(A) \to K_0(A[x])$ è un isomorfismo.*

Dimostrazione. Notiamo che, detta $\pi : A[x] \to A$ la valutazione in 0, si ha $\pi \circ i = id_A$ e dunque, funtorialmente, $\tilde{\pi} \circ \tilde{\imath} = id_{K_0(A)}$. Ci basta allora

mostrare la surgettività. Sia P un modulo proiettivo finitamente generato su $A[x]$; per il primo enunciato del teorema di Serre 1.26, P è stabilmente libero. Di conseguenza, $K_0(A[x]) \simeq \mathbb{Z}$ e un suo generatore è $[A[x]]$. Per mostrare la tesi, è sufficiente vedere che $[A[x]]$ stia nell'immagine di $\tilde{\imath}$. D'altronde,

$$\tilde{\imath}([A]) = [A \otimes_A A[x]] = [A[x]]$$

e dunque la surgettività. □

Abbiamo allora mostrato che su $A[x_1, \ldots, x_n]$ la nozione di modulo stabilmente libero coincide con quella di modulo proiettivo. Questo non è altro che il primo passo verso la risoluzione della congettura di Serre: quello che rimane da mostrare è che un modulo stabilmente libero è libero, ma di questo ci occuperemo nel capitolo 3.

Capitolo 2

Risoluzioni: un approccio algoritmico

Abbiamo visto nel primo capitolo come le risoluzioni rivestano un ruolo importante nella caratterizzazione di un modulo ma finora le abbiamo trattate solo in astratto. Il problema che ci poniamo è quello di trovare esplicitamente una risoluzione libera finita di un modulo finitamente generato su un anello di polinomi: sarà fondamentale infatti, nella dimostrazione algoritmica del teorema di Quillen-Suslin, disporre di una risoluzione libera finita di un dato modulo proiettivo. È necessario trattare la nozione di base di Gröbner di un sottomodulo di un modulo libero e del modulo delle sizigie; daremo quindi due algoritmi per il calcolo di una risoluzione.

2.1 Basi di Gröbner e Sizigie

Ordinamenti monomiali Sia $S = \mathbb{K}[x_1, \ldots, x_n]$ un anello di polinomi su un campo $\mathbb{K}$, munito di un ordinamento monomiale $<$ fissato. Dato un modulo libero S^p, $p \in \mathbb{N}$, definiamo un monomio di S^p come un elemento della forma:

$$m = t \cdot e$$

dove $t \in S$ è un monomio ed e è un vettore della base canonica di S^p.

Definizione 2.1. Un *ordine monomiale* su S^p è un buon ordine sui monomi tale che:

- Se m, n sono monomi di F tali che $m < n$, allora $\forall t \in S \; t \cdot m < t \cdot n$

- Se $s < t$ sono monomi di S e e è un elemento della base di S^p, allora $s \cdot e < t \cdot e$.

Fissato un ordinamento monomiale, abbiamo allora che ogni elemento $f \in F$ si scrive in modo unico come somma di monomi:

$$f = c_1 m_1 + c_2 m_2 + \cdots + c_k m_k$$

dove $c_i \in \mathbb{K}^*$ e $m_1 > m_2 > \cdots > m_k$. Analogamente a quanto si fa con i polinomi, se $m_1 = t \cdot e$, dove e è un elemento della base canonica, definiamo

- $lc(f) = c_1 \in \mathbb{K}^*$ il coefficiente di testa o leading coefficient
- $lm(f) = m_1 \in S^p$ il monomio di testa o leading monomial
- $lpp(f) = t \in S$ il leading power product

La scelta di un ordine monomiale sul modulo S^p permette di estendere l'algoritmo di divisione, che utilizzeremo in continuazione nel corso del capitolo. Ricordiamo l'enunciato:

Teorema 2.2. *Siano $f, f_1, \ldots, f_n \in S^p$ e sia $<$ un fissato ordinamento monomiale. Allora esistono unici $g_1, \ldots, g_n \in S$ e $r \in S^p$ tali che*

$$f = \sum_{i=1}^{n} g_i f_i + r$$

con le seguenti condizioni:

- $lm(g_i f_i) \leq lm(f)$
- $lm(r) < lm(f_i)$ *oppure* $r = 0$

Basi di Gröbner Dato $G \subseteq F$, possiamo allora associargli il sottomodulo di F

$$in(G) = \langle \{ lm(f) \mid f \in G \} \rangle$$

$in(G)$ non è altro che la generalizzazione al caso dei moduli dell'ideale $lt(I)$ associato all'ideale I. Come in quel caso, possiamo introdurre la nozione di base di Gröbner:

Definizione 2.3. $G = \{g_1, \ldots, g_k\} \subseteq I \subseteq F$ è una *base di Gröbner* del sottomodulo I di F se $\langle\{lm(g_1), \ldots, lm(g_k)\}\rangle = in(I)$.
Una base di Gröbner si dice *minimale* se $\{lm(g_1), \ldots, lm(g_k)\}$ è un insieme di generatori minimale di $in(I)$; si dice invece ridotta se il leading term di g_j non divide nessun monomio di g_i $\forall j \neq i$.

Le proprietà di una base di Gröbner di un sottomodulo sono simili a quelle delle basi di Gröbner nel caso degli ideali; molte delle proprietà sono infatti legate all'ordine monomiale più che alla struttura algebrica. Per esempio:

Proposizione 2.4. *Sia I un sottomodulo di S^p e sia $G = \{g_1, \ldots, g_k\}$ una base di Gröbner di I. Allora $I = \langle G\rangle$.*

Dimostrazione. Supponiamo per assurdo che esista un $f \in I \setminus \langle g_1, \ldots, g_k\rangle$. Poichè l'ordinamento monomiale è un buon ordine, possiamo supporre che ogni elemento minore di f stia in $\langle G\rangle$. Sappiamo che f ammette una scrittura in monomi:

$$f = c_1 m_1 + \cdots + c_n m_n$$

tale che $m_1 > m_2 > \cdots > m_n$. Per ipotesi, $lm(f) = c_1 m_1 \in in(I) = \langle lm(G)\rangle$. Esiste allora un elemento $g \in \langle G\rangle$ tale che $lm(g) = lm(f)$. Di conseguenza, $f - g \in I$ e $f - g < f$. Per l'ipotesi di minimalità di f, $f - g \in \langle G\rangle$, da cui un assurdo. □

Sizigie Nel nostro caso, le basi di Gröbner sono solo uno strumento per il calcolo di una risoluzione; il nostro problema è infatti equivalente al calcolo del modulo delle sizigie:

Definizione 2.5. Sia M un S-modulo e siano $m_1, \ldots, m_k \in M$. Definiamo

$$Syz(m_1, \ldots, m_k) = \{(f_1, \ldots, f_k) \in S^k \mid \sum_{i=1}^{k} f_i m_i = 0\} \subseteq S^k$$

come il *modulo delle sizigie* del sottomodulo generato da $m_1, \ldots, m_k$.

Scelto dunque un insieme di generatori $m_1, \ldots, m_k$ di M, il modulo delle sizigie rende esatta la successione

$$0 \to Syz(m_1, \ldots, m_k) \longrightarrow S^k \xrightarrow{f} M \to 0$$

dove $f(e_i) = m_i$. Poichè S è un anello noetheriano, S^k è noetheriano e dunque lo è anche il modulo $Syz(m_1, \ldots, m_k)$. Spostiamo allora il nostro interesse verso il calcolo effettivo di un insieme di generatori finito per tale modulo; ciò risolverebbe a livello computazionale il problema del calcolo di una risoluzione.

Il caso monomiale Come spesso accade in queste situazioni, si decide di partire dal caso più semplice: il caso monomiale. Consideriamo $m_1, \ldots, m_n$ monomi di S^m e definiamo l'omomorfismo

$$\begin{array}{rccc} f\colon & S^n & \longrightarrow & S^m \\ & e_i & \longmapsto & m_i \end{array}$$

Chiaramente possiamo identificare $Syz(m_1, \ldots, m_n) = \mathrm{Ker}(f)$. Cerchiamo allora un metodo per determinare un insieme di generatori del nucleo.

Definizione 2.6. Siano $m_1, \ldots, m_n$ monomi di S^m, quindi $m_i = c_i x^{\alpha_i} e_{k(i)}$. Per ogni coppia di indici (i, j) per i quali $k(i) = k(j)$ sia

$$m_{ij} = \frac{mcm(x^{\alpha_i}, x^{\alpha_j})}{c_j x^{\alpha_j}}$$

Definiamo allora

$$\tau_{ij} \coloneqq m_{ji} e_i - m_{ij} e_j \in \mathrm{Ker}(f) = Syz(m_1, \ldots, m_n)$$

L'idea è che questi elementi siano sufficienti a generare il modulo delle sizigie; effettivamente è cosi. Identifichiamo con T il sottomodulo $\langle \tau_{ij} \mid i, j \rangle$. Ciò che vogliamo mostrare è che $T = Syz(m_1, \ldots, m_n)$.

Proposizione 2.7. *Gli elementi τ_{ij} generano $Syz(m_1, \ldots, m_n)$.*

Dimostrazione. È sufficiente ridursi al caso di $m = 1$, dove quindi $m_1, \ldots, m_n$ sono monomi di S. Dato $h = (h_1, \ldots, h_n) \in Syz(m_1, \ldots, m_n)$, definiamo la funzione

$$\delta(h) = \max_i \deg(h_i m_i)$$

Supponiamo per assurdo che $Syz(m_1, \ldots, m_n) \supsetneq T$ e sia h un minimo di δ in $Syz(m_1, \ldots, m_n) \setminus T$. Consideriamo l'insieme J degli indici per i quali

$\deg(h_j m_j) = \delta(h)$. Si ottiene

$$\sum_{j \in J} lt(h_j) m_j = 0$$

Se mostrassimo che $h' = \sum_{j \in J} lt(h_j) e_j \in T$ avremmo finito; in tal caso infatti $\delta(h - h') \leq \delta(h)$ e $h - h' \notin T$, contraddicendo la minimalità di h in $Syz(m_1, \ldots, m_n) \setminus T$.
Sia $lt(h_j) = \phi_j lm(h_j)$ e $m_j = c_j lpp(m_j)$. Per ipotesi $\sum \phi_j c_j = 0$. Per ogni coppia di indici $j_1, j_2 \in J$, definiamo

$$x^{\gamma_{j_1 j_2}} = mcm(lt(h_{j_1}), lt(h_{j_2}))$$

e dunque, dalla definizione 2.6, si ottiene

$$m_{j_1 j_2} = \frac{x^{\gamma_{j_1 j_2}}}{c_{j_2} lm(m_{j_2})}$$

Di conseguenza,

$$\tau_{j_1 j_2} = \frac{x^{\gamma_{j_2 j_1}} e_{j_1}}{c_{j_1} lpp(m_{j_2})} - \frac{x^{\gamma_{j_1 j_2}} e_{j_2}}{c_{j_2} lpp(m_{j_2})}$$

Da questa relazione si ricava

$$x^{\delta - \gamma_{j_1 j_2}} \tau_{j_1 j_2} = \frac{lm(h_{j_1}) e_{j_1}}{c_{j_1}} - \frac{lm(h_{j_2}) e_{j_2}}{c_{j_2}}$$

Per semplicità, supponiamo $J = \{1, \ldots, k\}$. Pertanto,

$$\begin{aligned} h' = \sum_{j \in J} lt(h_j) e_j = \sum_{j \in J} \phi_j lm(h_j) e_j = \sum_{j \in J} \phi_j c_j \frac{lm(h_j) e_j}{c_j} = \\ = \sum_{j \in J} \phi_j c_j \left(\sum_{t=1}^{j} \frac{lm(h_t) e_t}{c_t} - \frac{lm(h_{t-1}) e_{t-1}}{c_{t-1}} \right) = \\ = \sum_{t=1}^{k} \left(\frac{lm(h_t) e_t}{c_t} - \frac{lm(h_{t-1}) e_{t-1}}{c_{t-1}} \right) \sum_{j=t}^{k} c_j \phi_j \end{aligned}$$

Poichè per ipotesi $\sum \phi_j c_j = 0$, si ha che l'addendo per $j = 1$ è nullo. Dunque

$$h' = \sum_{t=1}^{k} x^{\delta - \gamma_{t\ t-1}} \tau_{j\ j-1} \sum_{j=t}^{k} c_j \phi_j \in T$$

come voluto. □

Dunque abbiamo visto come il caso di un sottomodulo generato da monomi sia particolarmente semplice. Quanto fatto utilizza solo marginalmente i più potenti mezzi computazionali disponibili per maneggiare i polinomi: l'ordinamento e le basi di Gröbner.

Il caso generale Generalizziamo allora quanto fatto al caso di un sottomodulo qualunque. Consideriamo un modulo $M \subseteq S^m$ e una sua base di Gröbner $\{g_1, \dots, g_k\}$ rispetto a un fissato ordine monomiale $<$. Consideriamo l'omomorfismo

$$\begin{array}{rccc} f\colon & S^k & \longrightarrow & S^m \\ & e_i & \longmapsto & g_i \end{array}$$

Detto $lt(g_i) = c_i x^{\alpha_i} e_{k(i)}$, definiamo

$$m_{ij} = \frac{mcm(x^{\alpha_i}, x^{\alpha_j})}{c_j x^{\alpha_j}}$$

Dal criterio di Buchberger,

Proposizione 2.8. *$G = \{g_1, \dots, g_k\}$ è una base di Gröbner del sottomodulo M* $\iff \overline{S(g_i, g_j)}^G = 0$

si ottiene che $S(g_i, g_j) = m_{ij} g_j - m_{ji} g_i$ si scrive in modo unico, per l'algoritmo di divisione, come combinazione dei g_i

$$S(g_i, g_j) = \sum_{s=1}^{k} f_s^{i,j} g_s$$

Di conseguenza, $m_{ij} g_j - m_{ji} g_i - \sum f_s^{i,j} g_s = 0$. Definiamo allora

$$\tau_{ij} \coloneqq m_{ij} e_j - m_{ji} e_i - \sum_{s=1}^{k} f_s^{i,j} e_s \in Syz(g_1, \dots, g_k)$$

i candidati generatori del modulo delle sizigie. La prima domanda che uno potrebbe porsi è se qualche τ_{ij} può essere banale; notiamo però che, dall'algoritmo di divisione,

$$lm(f_s^{i,j} g_s) \leq lm(S(g_i, g_j)) < lm(m_{ij} g_j) = lm(m_{ji} g_i)$$

e dunque le relazioni trovate sono non banali.

Osservazione 2.9. La nozione di base di Gröbner si fonda sull'esistenza di un ordinamento monomiale; è allora necessario trovare un ordinamento monomiale coerente con l'omomorfismo dato. Dato l'omomorfismo

$$\begin{array}{rccc} f\colon & S^k & \longrightarrow & S^m \\ & e_i & \longmapsto & g_i \end{array}$$

muniamo così S^k dell'ordinamento

$$me_i < ne_j \iff \begin{cases} lt(mg_i) < lt(ng_j) \\ lt(mg_i) = lt(ng_j) \ \wedge \ i > j \end{cases}$$

Tale ordinamento monomiale indotto riveste un ruolo fondamentale a livello algoritmico, come chiaro dal seguente:

Teorema 2.10 (**Schreyer**). *Sia $G = \{g_1, \dots, g_k\}$ una base di Gröbner di un modulo $M \subseteq S^m$ e supponiamo S^k munito dell'ordinamento monomiale indotto da f. Allora $\{\tau_{ij} \mid i < j\}$ sono una base di Gröbner di $Syz(g_1, \dots, g_k) \subseteq S^k$.*

Dimostrazione. Abbiamo già notato che $lt(m_{ij}g_j) = lt(m_{ji}g_i) > lt(f_s^{i,j}g_s)$ e dunque $lt(\tau_{ij}) = m_{ji}e_i$. È allora sufficiente mostrare che, dato un qualsiasi elemento $\eta = \sum_{i=1}^{t} p_i e_i$, esistono i, j per i quali $m_{ji}e_i \mid lt(\eta)$.
Sia $n_j e_j = lt(p_j e_j)$ e sia $lt(\eta) = lt(p_{\tilde{\jmath}} e_{\tilde{\jmath}})$. Consideriamo l'insieme di indici J per i quali $lm(p_j g_j) = lm(p_{\tilde{\jmath}} g_{\tilde{\jmath}})$; gli indici contenuti in J devono essere, in base all'ordinamento considerato, tutti $\geq \tilde{\jmath}$. Pertanto $\sum_{j\in J} n_j lt(g_j) = 0$ e dunque $\sum_{j\in J} n_j e_j$ è una sizigia sul sottomodulo generato da $\{lt(g_j) \mid j \in J\}$. Per la proposizione 2.7, tale sizigia appartiene al sottomodulo generato da $m_{ij}e_j - m_{ji}e_i$ con $i, j \geq \tilde{\jmath}$ e dunque $n_{\tilde{\jmath}}$ appartiene all'ideale generato da $m_{j\tilde{\jmath}}$, $j > \tilde{\jmath}$, come voluto. □

Questo teorema permette di elaborare un semplice algoritmo per il calcolo di una risoluzione libera: è infatti sufficiente calcolare ad ogni passo la base di Gröbner del modulo delle sizigie e iterare.

Criterio di terminazione Quanto visto dimostra la correttezza dell'algoritmo. Rimane ancora il problema della terminazione di questo processo.

Questo viene risolto dal teorema delle sizigie di Hilbert, o meglio dalla sua dimostrazione.

Lemma 2.11. *Con la notazione dei teoremi precedenti, ordiniamo $g_1, \dots, g_s$ in modo che, se $lt(g_i) = p_i e_{k(i)}$ e $lt(g_j) = p_j e_{k(j)}$ con $k(i) = k(j)$, allora $i < j$ se e solo se $p_i < p_j$ secondo l'ordinamento lessicografico di S. Se $lt(g_i)$ non dipende da $x_1, \dots, x_l$, allora $lt(\tau_{ij})$ non dipende da $x_1, \dots, x_{l+1}$ per $i < j$.*

Dimostrazione. Per l'ordine scelto della base di Gröbner, si ha che se $lt(g_i)$ non dipende da $x_1, \dots, x_l$, allora non vi dipendono neanche $lt(g_j)$ per tutti gli indici $j \leq i$. Ciò che dobbiamo mostrare è che x_{l+1} non appare in m_{ji}; poiché abbiamo scelto l'ordinamento lex su $\mathbb{K}[x_1, \dots, x_n]$, si ha che la potenza di x_{l+1} che appare in $lt(g_i)$ è maggiore di quella che appare in $lt(g_j)$. Per la definizione di m_{ji}, si ha allora la tesi. □

Procediamo allora alla dimostrazione della terminazione dell'algoritmo:

Teorema 2.12 (**delle sizigie di Hilbert**)**.** *Sia M un $\mathbb{K}[x_1, \dots, x_n]$-modulo noetheriano. Allora M ammette una risoluzione libera di lunghezza $\leq n$.*

Dimostrazione. Poichè M è noetheriano, ammette un insieme finito di generatori $\{m_1, \dots, m_t\}$. Consideriamo allora l'omomorfismo

$$\begin{array}{rccc} f\colon & S^t & \longrightarrow & M \\ & e_i & \longmapsto & m_i \end{array}$$

Sia $g_1^{(1)}, \dots, g_{t_1}^{(1)}$ una base di Gröbner per $\mathrm{Ker}(f)$ rispetto all'ordinamento indotto da f; abbiamo allora la successione esatta

$$0 \to Syz(g_1^{(1)}, \dots, g_{t_1}^{(1)}) \longrightarrow S^{t_1} \longrightarrow S^t \xrightarrow{f} M \longrightarrow 0$$

Per il lemma 2.11 x_1 non appare nei leading term di $\{g_1^{(1)}, \dots, g_{t_1}^{(1)}\}$. Iterando il procedimento, all'n-esimo passo, ottengo che i leading term di $\{g_1^{(n)}, \dots, g_{t_n}^{(n)}\}$ sono costanti. Di conseguenza, il modulo delle sizigie è generato da alcuni elementi della base canonica ed è libero, da cui la tesi. □

Abbiamo dunque ottenuto un criterio per la terminazione dell'algoritmo: una risoluzione ottenuta con esso non può essere lunga più di n. Riassumendo, dunque, abbiamo il seguente algoritmo: preso in input un modulo

M ed una sua presentazione $f\colon S^{t_0} \to M$, si calcola una base di Gröbner $G_1 = \{g_1^{(1)}, \ldots, g_{t_1}^{(1)}\}$ di $\mathrm{Ker}(f)$. Si ottiene così un omomorfismo

$$\begin{array}{rccc} g_1\colon & S^{t_1} & \longrightarrow & S^{t_0} \\ & e_i & \longmapsto & g_i^{(1)} \end{array}$$

A questo punto il teorema di Schreyer permette di trovare una base di Gröbner di $\mathrm{Ker}(g_1)$ tramite il calcolo dei τ_{ij} e si itera.
Sotto il punto di vista astratto, il teorema è interessante allo stesso modo; dice infatti che la dimensione stabilmente libera di un $\mathbb{K}[x_1, \ldots, x_n]$-modulo è al più n. Tale teorema può anche essere considerato equivalente al teorema di Serre nel caso di $\mathbb{K}[x_1, \ldots, x_n]$: dimostra infatti che ogni modulo finitamente generato su $\mathbb{K}[x_1, \ldots, x_n]$ ammette una risoluzione libera finita e abbiamo visto che questo, per i moduli proiettivi, è equivalente ad essere stabilmente liberi.

2.2 Calcolo di risoluzioni e cornici di Schreyer

Illustriamo ora un altro algoritmo per ricavare una risoluzione libera finita di un S-modulo M, più efficiente. L'algoritmo sarà basato sul trovare prima una sorta di risoluzione monomiale per poi estenderla a una vera e propria. Consideriamo un S-modulo $M = \langle m_1, \ldots, m_k \rangle$. Possiamo vedere allora M come quoziente di $F_0 = S^k$ per un dato sottomodulo I. Denoteremo nel seguito con $\mathcal{E}_i$ la base canonica dell'i-esimo modulo libero che compone una risoluzione.

Definizione 2.13. Siano $(F_i)_{i=1,\ldots,l}$ moduli liberi su S. Una *risoluzione di Schreyer* di un S-modulo $M \simeq {}^{F_0}\!/_I$ è una risoluzione libera:

$$\Phi\colon 0 \to F_l \xrightarrow{\varphi_l} F_{l-1} \xrightarrow{\varphi_{l-1}} \ldots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0$$

munita di un ordinamento monomiale tale che

- $\mathrm{Coker}(\varphi_1) = M$
- $\varphi_i(\mathcal{E}_i)$ è una base di Gröbner minimale di $\mathrm{Im}(\varphi_i)$

Una *cornice di Schreyer* di un S-modulo $M = {}^{F_0}\!/_I$ è una risoluzione libera:

$$\Xi\colon 0 \to F_l \xrightarrow{\xi_l} F_{l-1} \xrightarrow{\xi_{l-1}} \ldots \xrightarrow{\xi_2} F_1 \xrightarrow{\xi_1} F_0$$

nella quale ogni colonna della matrice che rappresenta ξ_i è a entrate monomiali e munita di un ordinamento rispetto al quale:

- $\xi_1(\mathcal{E}_1)$ è un insieme di generatori minimale per $in(I)$
- $\xi_i(\mathcal{E}_i)$ è un insieme di generatori minimale di $in(\mathrm{Ker}(\xi_{i-1}))$

Trovare una cornice L'idea è quella di trovare prima una cornice e successivamente ricavare da questa una risoluzione di Schreyer. Il seguente lemma è fondamentale per raggiungere il primo di questi obiettivi:

Lemma 2.14. *Sia Ξ una cornice di Schreyer di un S-modulo M. Nelle notazioni introdotte in precedenza, sia $\mathcal{E}_i(e) = \{s \in \mathcal{E}_i \mid \xi_i(s) = t \cdot e\}$, ordinato in modo crescente. Allora*

$$\bigcup_{e \in \mathcal{E}_{i-1}} \bigcup_{j=2}^{r_e} mingen(t_1, \ldots, t_{j-1} : t_j) \cdot s_j$$

è un insieme di generatori minimale per $in(\mathrm{Ker}(\xi_i))$, dove t_j sono gli elementi tali che, se $\mathcal{E}_i(e) = \{\epsilon_1 < \cdots < \epsilon_r\}$ allora $\xi_i(\epsilon_j) = t_j e$ mentre mingen restituisce l'insieme dei generatori minimali dell'ideale monomiale.

Dimostrazione. Fissiamo $e \in \mathcal{E}_{i-1}$ e siano $m_1, \ldots, m_r$ le immagini ordinate degli elementi di $\mathcal{E}_{i-1}$, dove $m_j = t_j e$. Siano allora dei $g_j \in S$ tali che

$$\sum_{j=1}^{r} g_j m_j = 0$$

Otteniamo

$$\sum_{j=1}^{r} g_j \epsilon_j \in \mathrm{Ker}(\xi_i)$$

Sia $s_k \epsilon_k$ il leading monomial di questa relazione, dove quindi $s_k = lm(g_k)$. Vi sono ora due casi.

- Se $s_k \epsilon_k$ appartiene a $\mathrm{Ker}(\xi_i)$, allora $\xi_i(s_k \epsilon_k) = s_k \xi_i(\epsilon_k) = s_k m_k = 0$. Dunque, $s_k t_k = 0$ e questo è assurdo, poiché $\mathbb{K}[x_1, \ldots, x_n]$ è un dominio.
- Se invece $s_k m_k = -\sum_{j=1}^{r} s_j m_j$, si ottiene che $s_k \in (t_1, \ldots, t_{k-1} : t_k)$.

da cui la tesi. □

Grazie a questo lemma, possiamo descrivere facilmente un algoritmo per ricavare una cornice di Schreyer. Consideriamo $M \simeq {}^{F_0}\!/_I$. Dopo aver calcolato un insieme di generatori minimale per $in(I) = (g_1, \dots, g_k)$, consideriamo $F_1 = S^k$ e definiamo $\xi_1(e_i) = g_i$. Come spiegato nel lemma, troviamo un insieme di generatori minimale per $in(\mathrm{Ker}(\xi_1))$ e iteriamo il ragionamento. In pseudocodice,

$B_i = \emptyset$
$B_1 = \{g_1, \cdots, g_k\}$
$i = 0$
while $B_i \neq \emptyset$ **do**
  $rk = \#B_i$
  for $j = 1; j \leq rk; j++$ **do**
    Calcola $\mathcal{E}_i(e_j) = \{s_1, \cdots, s_{k_j}\}$
    for $h = 1; h \leq k_j; h++$ **do**
      Calcola generatori minimali di $(t_1, \dots, t_{h-1} : t_h) = \{f_1, \dots f_l\}$
      $B_{i+1} \leftarrow B_{i+1} \cup f_1 s_h, \dots, f_l s_h$
    end for
  end for
  $i++$
end while

Per una migliore comprensione, forniamo un esempio:

Esempio. Consideriamo $S = \mathbb{K}[x_1, x_2, x_3]$ con l'ordinamento lessicografico e sia $I = (x_1x_2, x_2x_3, x_1x_3)$. Cerchiamo una risoluzione del modulo $M = {}^{S}\!/_I$.

I Iterazione Poichè $I = in(I)$ (I è monomiale), prendiamo $F_1 = S^3$. I generatori di $in(\mathrm{Ker}(\xi_1))$ sono x_1e_2, x_2e_3, x_3e_3.

II Iterazione In questo caso, $F_2 = S^3$ e

$$\begin{array}{rccc} \xi_2\colon & F_2 & \longrightarrow & F_1 \\ & e_1 & \longmapsto & x_1e_2 \\ & e_2 & \longmapsto & x_2e_3 \\ & e_3 & \longmapsto & x_3e_3 \end{array}$$

Per il lemma, abbiamo che $in(\mathrm{Ker}(\xi_2))$ è ciclico, generato da x_2e_3

III Iterazione Chiaramente, $F_3 = S$ e l'applicazione ξ_3 è iniettiva, dunque abbiamo

trovato una cornice:

$$0 \to S \xrightarrow{\xi_3} S^3 \xrightarrow{\xi_2} S^3 \xrightarrow{\xi_1} S \to M \to 0$$

Trovare una risoluzione Dimostriamo ora una proposizione che ci conforti riguardo alla possibilità che il metodo scelto per la soluzione del problema sia effettivamente sensato:

Proposizione 2.15. *Sia Ξ una cornice di Schreyer per un S-modulo M. Allora esiste una risoluzione di Schreyer Φ tale che $\Xi = in(\Phi)$.*

Dimostrazione. Diamo un processo iterativo per costruire la risoluzione a partire dalla cornice. Per definizione di cornice, $\xi_1(\mathcal{E}_1)$ è un insieme di generatori minimale per $in(I)$. Troviamo allora una base di Gröbner C_1 minimale $\{g_1, \ldots, g_k\}$ tale che $lm(g_i) = \xi_1(e_i)$. Esiste un unico modo sensato per definire φ_1 su F_1:

$$\begin{array}{rccc} \varphi_1 \colon & F_1 & \longrightarrow & F_0 \\ & e_i & \longmapsto & g_i \end{array}$$

Per iterare il procedimento, basta mostrare che $in(\mathrm{Ker}(\varphi_1)) = in(\mathrm{Ker}(\xi_1))$, ma questo discende direttamente dal teorema 2.10. □

Descriviamo ora l'algoritmo per il calcolo di una risoluzione di Schreyer di un S-modulo $M = {}^{F_0}\!/_{I}$. Supponiamo di avere in input una base di Gröbner minimale $\bar{C}_i$ del sottomodulo I e una cornice di Schreyer Ξ di M. Per comodità, consideriamo $B = B_1 \cup \cdots \cup B_n$ l'unione dei generatori minimali di $in(\mathrm{Ker}(\xi_i))$. In output, produrremo le basi di Gröbner C_i di $\mathrm{Ker}(\varphi_i)$ e le sizigie minimali H_i.

$C_i, H_i \leftarrow \emptyset \ \forall i$
while $B \neq \emptyset$ **do**
  $m \leftarrow \mathbf{min}B$
  $B \leftarrow B \setminus \{m\}$
  $i \leftarrow \mathbf{lev}(m)$
  if $i = 1$ **then**
    $g \leftarrow$ l'elemento di $\bar{C}_i$ tale che $lm(g) = m$
    $C_i \leftarrow C_i \cup \{g\}$
    $H_i \leftarrow H_i \cup \{g\}$
  else

$(f, g) \leftarrow$ **Reduce**(m, C_{i-1})
$C_i \leftarrow C_i \cup \{g\}$
if $f \neq 0$ **then**
$C_{i-1} \leftarrow C_{i-1} \cup \{f\}$
$B \leftarrow B \setminus \{lm(f)\}$
else
$H_i \leftarrow H_i \cup \{g\}$
end if
end if
end while
return C_i

Rimangono ancora da illustrare le funzioni ausiliarie **Reduce** e **Min**. La funzione **Reduce** è la seguente:

Reduce$(t \cdot \epsilon, C_{i-1})$
$f \leftarrow t \cdot k$, dove $\varphi_{i-1}(\epsilon) = k$
$g \leftarrow t \cdot \epsilon$
while $(f \neq 0) \wedge (lm(f) \in in\langle C_{i-1} \rangle)$ **do**
Scegli $h \in C_{i-1}$ tale che $lm(h) \mid lm(f)$
$f \leftarrow f - \dfrac{lc(f)lpp(f)}{lc(h)lpp(h)}h$
$g \leftarrow g - \dfrac{lc(f)lpp(f)}{lc(h)lpp(h)}e$, dove $\varphi_{i-1}(e) = h$
end while
if $f \neq 0$ **then**
$g \leftarrow g - e$, dove $\varphi_{i-1}(e) = f$
end if
return f, g

La funzione **min** è invece una funzione di scelta del monomio da utilizzare nell'algoritmo; seleziona il minimo di B secondo un ordinamento totale per il quale, $\forall m, n \in B$, se vale una delle seguenti

1. $\deg(m) - lev(m) \leq \deg(n) - lev(n)$ e $lev(m) < lev(n)$
2. $\deg(m) < \deg(n)$ e $lev(m) = lev(n)$
3. $\deg(m) = \deg(n)$ e $lev(m) > lev(n)$

allora $m < n$. Verifichiamo la correttezza dell'algoritmo.

Teorema 2.16. *La risoluzione Φ del modulo M fornita in output dall'algoritmo proposto è una risoluzione di Schreyer di M.*

Dimostrazione. Procediamo per induzione su i. Supponiamo cioè che al termine dell'algoritmo l'insieme C_i sia una base di Gröbner minimale del sottomodulo $\mathrm{Ker}(\varphi_{i-1})$. Dobbiamo mostrare che C_{i+1} è una base di Gröbner minimale di $\mathrm{Ker}(\varphi_i)$. Chiaramente, per come è fatto l'algoritmo, abbiamo un'inclusione:

$$B_{i+1} \subseteq in(C_{i+1})$$

e quindi C_{i+1} è una base di Gröbner di $\mathrm{Ker}(\varphi_i)$. Bisogna quindi mostrare la minimalità. Sia $f \in C_{i+1}$ un elemento ottenuto in un passo dell'algoritmo da un monomio $m \in B$. Mostriamo che $lm(f) \in B_{i+1}$. Vi sono due casi:

- Se $m \in B_{i+1}$ allora $lm(f) = m$ per costruzione perché è stato inserito in C_{i+1} senza essere modificato dalla funzione **Reduce**.
- Se $m \in B_{i+2}$, allora f è ottenuto dalla funzione **Reduce** tramite riduzione di m. Sia g un elemento di C_{i+1} calcolato a un passo precedente. Per costruzione, abbiamo che $lm(g) \nmid lm(f)$. Per ipotesi induttiva, possiamo supporre che $lm(g) \in B_{i+1}$. Per minimalità di B_{i+1}, abbiamo allora che $lm(f) \nmid lm(g)$.

Di conseguenza, C_{i+1} è una base di Gröbner minimale di $\mathrm{Ker}(\varphi_{i-1})$ e dunque Φ è una risoluzione di Schreyer. □

L'algoritmo è allora corretto; il vero vantaggio è che procede al calcolo della risoluzione producendo le basi di Gröbner minimali durante l'esecuzione. Uno dei maggiori rischi dell'algoritmo presentato nella prima sezione è infatti quello che le basi di Gröbner coinvolte abbiano cardinalità grandi; ciò rallenta in maniera esagerata l'esecuzione. L'algoritmo di Schreyer è invece ottimale sotto questo punto di vista, anche se il calcolo della base di Gröbner è più difficoltoso.

Utilizzeremo quanto fatto nella dimostrazione algoritmica del teorema di Quillen-Suslin: l'esistenza di una risoluzione giocherà nell'algoritmo lo stesso ruolo che il teorema di Serre gioca nella dimostrazione astratta.

Capitolo 3

Il teorema di Quillen-Suslin

Abbiamo visto nel Capitolo 1 come un modulo proiettivo finitamente generato su $A[x_1, \dots, x_n]$ sia stabilmente libero. In questo capitolo daremo alcune dimostrazioni del secondo passo: mostreremo cioè che un modulo stabilmente libero su $A[x_1, \dots, x_n]$ è libero, risolvendo quindi in positivo la congettura di Serre. Le dimostrazioni sono tutte basate su proprietà matriciali dei moduli stabilmente liberi: anche da questo si vede la grandezza del teorema di Serre, che ha permesso di trasportare il problema sul campo dell'algebra lineare. Vediamo quindi una condizione necessaria e sufficiente affinché un modulo stabilmente libero, cioè il nucleo di un omomorfismo di moduli liberi, sia libero:

Proposizione 3.1. *Sia $f\colon A^n \to A^m$ un omomorfismo surgettivo di A-moduli. Allora* $\mathrm{Ker}(f)$ *è un modulo libero se e solo se f si solleva a un isomorfismo $\tilde{f}\colon A^n \to A^m \oplus A^r$ che rende commutativo il seguente diagramma:*

$$\begin{array}{ccc} & & A^m \oplus A^r \\ & \overset{\tilde{f}}{\nearrow} & \big\downarrow \pi \\ A^n & \xrightarrow[f]{} & A^m \end{array}$$

Dimostrazione. Se tale isomorfismo esiste, allora $\mathrm{Ker}(f) \simeq \mathrm{Ker}(\pi) = A^r$. Viceversa, supponiamo che $\mathrm{Ker}(f)$ sia libero. Allora $\mathrm{Ker}(f) \simeq A^r$. La successione

$$0 \to \mathrm{Ker}(f) \to A^n \to A^m \to 0$$

spezza, dunque $A^n \simeq \mathrm{Ker}(f) \oplus A^m \simeq A^r \oplus A^m$ e quindi la tesi. □

Interpretiamo la proposizione fissando delle basi dei moduli; questo permette di rappresentare le applicazioni tramite matrici. Consideriamo le matrici $X \in M(m,n,A)$, $Y \in M(m+r,n,A)$ che rappresentano rispettivamente f e $\tilde{f}$. La condizione $\pi \circ \tilde{f} = f$ ci dice che X è una sottomatrice di Y, mentre il fatto che $\tilde{f}$ sia un isomorfismo implica che la matrice Y sia invertibile. Dunque la possibilità di sollevare f a $\tilde{f}$ è equivalente al fatto che X sia completabile a una matrice invertibile. Studiamo allora le matrici più semplici che ambiscono a soddisfare tali proprietà:

Definizione 3.2. Sia A un anello. Un vettore $(f_1, \cdots f_k)$ di A^k si dice *unimodulare* se le sue componenti generano l'ideale (1). Si dice che tale vettore ha la proprietà di estensione (unimodulare) se esiste una matrice $M \in GL(k,A)$ che ha $(f_1, \cdots, f_k)^t$ come prima colonna.

L'interpretazione matriciale permette quindi di spostare l'attenzione sui vettori unimodulari:

Corollario 3.3. *Sono fatti equivalenti:*

1. *Ogni vettore unimodulare di A^k ha la proprietà di estensione*
2. *Ogni A-modulo stabilmente libero è libero.*

Per verificare la veridicità della congettura sarà allora sufficiente mostrare che ogni vettore unimodulare di A^k ha la proprietà di estensione. Ci concentreremo dapprima nel caso di un campo $\mathbb{K}$; troveremo poi il modo di generalizzare al caso di un anello A PID. In realtà otterremo qualcosa di più, cioè che l'equivalenza tra moduli liberi e stabilmente liberi vale su tutti gli anelli di dimensione di Krull ≤ 1. Questo significa, per esempio, che tutti i moduli stabilmente liberi su un dominio di Dedekind sono in realtà liberi; purtroppo in generale su questi anelli manca l'equivalenza tra moduli proiettivi finitamente generati e moduli stabilmente liberi.

3.1 La dimostrazione di Suslin

Diamo ora una prima dimostrazione del teorema di Quillen-Suslin, fornita da Suslin nel 1976. Chiaramente, possiamo agire sulla base del dominio e del codominio tramite matrici invertibili. Dato A anello commutativo,

introduciamo una relazione di equivalenza sui vettori di $A[x]^n$.

$$f \sim g \iff \exists M \in GL(n, A) \text{ t.c. } Mg = f$$

e diciamo in questo caso che f e g sono equivalenti su A. In virtù di questa relazione, siamo portati a dimostrare che, sotto opportune ipotesi, ogni vettore unimodulare è equivalente a un vettore della base canonica; questo ci porterebbe alla tesi. Effettivamente, è proprio quello che ci accingiamo a fare. In questa dimostrazione, faremo attenzione ai sottogruppi che utilizzeremo nell'azione: vedremo infatti che non tutte le matrici invertibili saranno necessarie. In particolare, faremo distinzione tra

- $E(n, A)$ le matrici elementari di Gauss
- $GL(n, A)$ le matrici invertibili
- $SL(n, A)$ le matrici invertibili a determinante 1

Iniziamo con qualche lemma. Avremo intanto bisogno nella dimostrazione di contrarre gli ideali mediante l'omomorfismo

$$i \colon A \longrightarrow A[x]$$

Il seguente lemma è un'osservazione interessante che sfrutta l'integralità di una data estensione:

Lemma 3.4. *Sia A un anello commutativo, e sia I un ideale in $A[x]$ che contiene un polinomio monico. Sia J un ideale in A tale che*

$$J[x] + I = A[x]$$

Allora $A \cap I + J = A$.

Dimostrazione. Consideriamo l'anello $S = {}^{A[x]}\!/_{I}$. Consideriamo gli omomorfismi:

$$A \xrightarrow{\pi} {}^{A}\!/_{A \cap I} \xrightarrow{\imath} S$$

Chiamiamo $\overline{J}$ l'immagine di J tramite la proiezione e $\overline{J}^e$ la sua estensione in S. Per le ipotesi, $\overline{J}^e = S$. Notiamo che l'ipotesi che I contenga un polinomio monico garantisce che S sia intero su ${}^{A}\!/_{A \cap I}$, in quanto modulo

finitamente generato. Per il teorema del Going-Up [7, pag. 62], si ha allora che $\overline{J} = {}^{A}\!/_{A \cap I}$, cioè $(A \cap I) + J = A$, come voluto. □

Suslin cercò di risolvere il problema per passi successivi. Il primo problema fu allora quello di risolvere il caso più facile:

Lemma 3.5. *Sia A un dominio e sia $f = (f_1, f_2) \in A[x]^2$. Sia $c \in A \cap (f_1, f_2)$. Allora per ogni A-algebra R, dati comunque $b, b' \in R$,*

$$b \equiv b' \ (c) \ \Rightarrow \ f(b) \sim f(b') \text{ tramite una matrice in } SL(2, A)$$

Dimostrazione. Per ipotesi, possiamo scrivere c come $c = h_1 f_1 + h_2 f_2$. Per l'ipotesi di integrità dell'anello, possiamo lavorare su A_c; su questo anello, consideriamo la matrice:

$$M = \frac{1}{c} \begin{pmatrix} h_1(b) & -f_2(b) \\ g_2(b) & f_1(b) \end{pmatrix} \begin{pmatrix} f_1(b') & f_2(b') \\ -g_2(b') & g_1(b') \end{pmatrix}$$

Mostriamo che $M \in SL(2, A)$. Intanto notiamo che $\det(M) = \frac{1}{c^2} \cdot c \cdot c = 1$. Dobbiamo però mostrare che gli elementi di M stiano in A. Per far questo, basta vedere che gli elementi di $c \cdot M$ siano 0 modulo (c). Svolgiamo il prodotto:

$$\begin{pmatrix} h_1(b) & -f_2(b) \\ h_2(b) & f_1(b) \end{pmatrix} \begin{pmatrix} f_1(b') & f_2(b') \\ -h_2(b') & h_1(b') \end{pmatrix} =$$
$$= \begin{pmatrix} h_1(b)f_1(b') + f_2(b)g_2(b') & h_1(b)f_2(b') - f_2(b)h_1(b') \\ f_1(b')h_2(b) - f_1(b)h_2(b') & h_2(b)f_2(b') + f_1(b)h_1(b') \end{pmatrix} =: X$$

Ragionando modulo c, si ha per ipotesi che $b \equiv b'$, dunque

$$X \equiv \begin{pmatrix} h_1(b)f_1(b) + f_2(b)h_2(b) & h_1(b)f_2(b) - f_2(b)h_1(b) \\ f_1(b)h_2(b) - f_1(b)h_2(b) & h_2(b)f_2(b) + f_1(b)h_1(b) \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$$

e quindi $M \in SL(2, A)$. Ci rimane da mostrare che M realizzi quanto voluto.

$$\begin{aligned} f(b) \cdot M &= \frac{1}{c}(f_1(b), f_2(b)) \begin{pmatrix} h_1(b) & -f_2(b) \\ h_2(b) & f_1(b) \end{pmatrix} \begin{pmatrix} f_1(b') & f_2(b') \\ -h_2(b') & h_1(b') \end{pmatrix} = \\ &= \frac{1}{c}(c, 0) \begin{pmatrix} f_1(b') & f_2(b') \\ -h_2(b') & h_1(b') \end{pmatrix} = e_1^t \begin{pmatrix} f_1(b') & f_2(b') \\ -h_2(b') & h_1(b') \end{pmatrix} = \\ &= (f_1(b'), f_2(b')) \end{aligned}$$

e questo termina la dimostrazione. □

Il seguente lemma ci ispirerà per il seguito:

Lemma 3.6. *Sia A un anello commutativo e sia $f \in A[x]^n$. Per ogni A-algebra commutativa R e ogni sottogruppo $G < GL(n, A)$*

$$I_{f,G,R} = \{a \in A \mid \forall b, b' \in A \left(b \equiv b' \ (a) \Rightarrow f(b) \sim_G f(b')\right)\}$$

è un ideale di A.

Dimostrazione. Siano $c, c' \in I$ e $r, r' \in A$. Mostriamo che $rc + r'c' \in I$. Siano $b, b' \in A$ tali che $b \equiv b' \ (rc + r'c')$. Di conseguenza, $b - b' = (rc + r'c)a$, e quindi $b - rca = b' + r'c'a$. Poiché $c \in I$, si ha $f(b) \sim_G f(b - rca)$, dato che $b \equiv b - rca \ (c)$. Allo stesso modo, $f(b') \sim_G f(b' + r'c'a)$. Segue allora che

$$f(b') \sim_G f(b' + r'c'a) = f(b - rca) \sim_G f(b)$$

e dunque I è un ideale. □

Se trovassimo un sottogruppo di $GL(n, A)$ per il quale l'ideale introdotto nel lemma è A, saremmo a buon punto. Potremmo valutare infatti il vettore unimodulare f in 0 rispetto a una delle variabili e concludere per induzione.

Proposizione 3.7. *Sia A un anello semilocale e sia $f = (f_1, \ldots, f_n)$ un vettore unimodulare ($n \geq 3$). Allora esiste una matrice $M \in E(n, A)$ tale che $f \cdot M = e_1^t$.*

Dimostrazione. Sia $I = (f_2, \ldots, f_n)$. Dimostriamo preliminarmente che $f_1 + I = \{f_1 + i \mid i \in I\}$ contiene un invertibile. A meno di quozientare, possiamo supporre che $\mathcal{J}(A) = 0$. In tal caso, per il teorema cinese del resto, A è un

prodotto di campi, $A = \mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_m$. Consideriamo allora la scrittura di f_1 nel prodotto: $f_1 = (f_{1,1}, \ldots, f_{1,n})$. Poiché f_1 non è invertibile, esistono delle componenti di f_1 nulle. Dato che f è unimodulare, per ogni componente $f_{1,i} = 0$ si ha che esiste un elemento di I s_i che abbia componente i-esima 1 e le altre 0. Allora $f_1 + \sum s_i$ è invertibile.

Sia allora c un invertibile di tale insieme $c = f_1 + \sum_{i=2}^{n} c_i f_i$. Possiamo portare f_1 in un elemento invertibile tramite la matrice

$$\begin{pmatrix} 1 & & & \\ c_2 & 1 & & \\ \vdots & & \ddots & \\ c_n & & & 1 \end{pmatrix} \in E(n, A)$$

e poi ridurre tutti gli altri f_i a 0 . □

Uniamo ora tutti i risultati ottenuti per dimostrare che l'ideale I introdotto è tutto l'anello: ci basterà dopo indurre sul numero di variabili per ottenere la tesi.

Teorema 3.8 (di Suslin)**.** *Sia A un anello commutativo con identità, e sia $f = (f_1, \ldots, f_n) \in A[x]^n$ un vettore unimodulare, con f_1 monico. Allora per ogni A-algebra R e per ogni $b, b' \in R$ abbiamo*

$$f(b) \sim_G f(b')$$

dove $G = \langle Sl(2, A), E(n, A) \rangle \subseteq GL(n, A)$, intendendo con $SL(2, A)$ l'immersione:

$$M \longrightarrow \begin{pmatrix} M & \\ & I_{n-2} \end{pmatrix}$$

Dimostrazione. Proviamo che $I = A$, dove I è l'ideale introdotto nel lemma 3.6. Mostriamo allora che per ogni ideale massimale $\mathfrak{M}$ di A, esiste $c \in I \setminus \mathfrak{M}$. Quozientiamo per l'ideale $\mathfrak{M}[t] + (f_1)$; otteniamo allora un vettore unimodulare $(\bar{f}_2, \ldots, \bar{f}_n)$ sull'anello quoziente. Notiamo che per il secondo teorema di omomorfismo,

$$A[t]/(f_1) + \mathfrak{M}[t] \simeq A/\mathfrak{M}[t]/\bar{f}_1$$

è un'algebra di dimensione finita su $A/\mathfrak{M}$; di conseguenza, è un anello semilocale. Per la proposizione 3.7, esiste una matrice elementare $\overline{M} \in E\left(n-1, A[t]/(f_1)+\mathfrak{M}[t]\right)$ per la quale

$$(\bar{f}_2, \dots, \bar{f}_n)\overline{M} = (\bar{1}, \bar{0}, \dots, \bar{0})$$

Sia $M \in E(n-1, A[x])$ tale che $\pi(M) = \overline{M}$. Siano allora $g_2, \dots, g_n$ tali che $(f_2, \dots, f_n) \cdot M = (g_2, \dots, g_n)$. Si ha che $g_2 \equiv 1$ $(\mathfrak{M}[t] + (f_1))$, dunque $(f_2, g_2) + \mathfrak{M}[t] = A[t]$. Poiché f_1 è monico, per il lemma 3.4, abbiamo allora che $(f_2, g_2) \cap A + \mathfrak{M} = A$; in particolare, esiste $c \in ((f_2, g_2) \cap A) \setminus \mathfrak{M}$. Mostriamo allora che $c \in I$. Siano $b, b' \in A$ tali che $b \equiv b'$ (c). Notiamo che

$$g_i(b) - g_i(b') \in (b - b') \subseteq (c) \subseteq (f_1, g_2) \cap A$$

Allora,

$$\begin{aligned}
f(b) &\sim_{E(n,A)} (f_1(b), g_2(b), \dots g_n(b)) \\
&\sim_{E(n,A)} (f_1(b), g_2(b), g_3(b') \dots g_n(b')) && \textit{Per il lemma } 3.7 \\
&\sim_{SL(2,A)} (f_1(b'), g_2(b'), g_3(b') \dots g_n(b')) && \textit{Per il lemma } 3.5 \\
&\sim_{E(n,A)} (f_1(b'), f_2(b'), f_3(b') \dots f_n(b')) \\
&= f(b')
\end{aligned}$$

da cui la tesi. □

Mostriamo ora che ogni vettore unimodulare ha la proprietà di estensione:

Teorema 3.9 (di Quillen-Suslin)**.** *Sia $\mathbb{K}$ un campo e sia f un vettore unimodulare in $\mathbb{K}[x_1, \cdots, x_n]^r$. Allora f ha la proprietà di estensione.*

Dimostrazione. Dimostriamo il teorema per induzione su n. Se $n = 1$, l'enunciato è ovvio poiché $\mathbb{K}[x]$ è un PID e dunque si può utilizzare l'algoritmo di divisione euclidea. Supponiamo allora l'enunciato vero per n e dimostriamo che vale per $n+1$. Consideriamo ora f come un vettore di polinomi in x_{n+1} a coefficienti in $\mathbb{K}[x_1, \cdots x_n]$. Se f ha una componente con termine di testa 1, possiamo applicare la proposizione 3.8, dunque $f(x_{r+1}) \sim f(0)$ e concludere per ipotesi induttiva. Supponiamo allora che ogni componente abbia termine di testa non invertibile. Consideriamo l'isomorfismo di $\mathbb{K}$-algebre

(trucco di Nagata):

$$\begin{aligned} x_1 &\to \tilde{x}_1 + \tilde{x}_{r+1}^{M_1} \\ &\vdots \\ x_r &\to \tilde{x}_r + \tilde{x}_{r+1}^{M_r} \\ x_{r+1} &\to \tilde{x}_{r+1} \end{aligned}$$

con gli M_i da determinare. Mostriamo che nelle nuove coordinate una componente ha coefficiente di testa invertibile. Fissato i, sia $f_i = \sum c_\alpha x^\alpha$. Allora,

$$f_i(\tilde{x}_1 + \tilde{x}_{r+1}^{M_1}, \cdots, \tilde{x}_{r+1}) = \sum_\alpha c_\alpha (\tilde{x}_1 + \tilde{x}_{r+1}^{M_1})^{\alpha_1} \cdots (\tilde{x}_r + \tilde{x}_{r+1}^{M_r})^{\alpha_r} \tilde{x}_{r+1}^{\alpha_{r+1}} =$$
$$= \sum_\alpha c_\alpha x_{r+1}^{\alpha_{r+1} + \sum \alpha_j M_j} + g_\alpha$$

dove $\deg(g_\alpha) < (\alpha_{r+1} + \sum \alpha_j M_j)$. Scegliamo allora gli M_i in modo tale che le potenze $\alpha_{r+1} + \sum \alpha_j M_j$ siano tutte distinte al variare di α. Per far questo, possiamo per esempio scegliere $M_i = s^{i-1}$, dove s è un naturale maggiore di ogni componente di α. Di conseguenza, non ci saranno cancellazioni tra i termini; abbiamo così trovato un polinomio con termine di testa invertibile, e dunque possiamo applicare la proposizione 3.21, valutare in 0 la variabile x_{n+1} e concludere per ipotesi induttiva. □

Unendo il risultato con quanto dimostrato nel primo capitolo, abbiamo allora dimostrato la veridicità della congettura:

Teorema (Congettura di Serre)**.** *Sia $\mathbb{K}$ un campo. Allora ogni modulo proiettivo finitamente generato su $\mathbb{K}[x_1, \ldots, x_n]$ è libero.*

Notiamo che la dimostrazione seguita illustra come a livello teorico sia sufficiente agire con le matrici elementari di Gauss e matrici 2×2 a determinante 1. Purtroppo non è chiaro dalla dimostrazione come trovare le matrici che agiscono sul vettore. Un altro problema è rappresentato dal fatto che la dimostrazione fallisce sui PID. Il trucco di Nagata è infatti efficace nel trovare un polinomio che contenga una potenza pura di una indeterminata, ma non riesce a lavorare sui coefficienti dei monomi. Abbiamo allora bisogno di sostituire il trucco di Nagata con un altro automorfismo: il *teorema del polinomio monico* di Suslin fa proprio questo.

3.2 Il teorema del Polinomio Monico di Suslin

Fino ad ora, abbiamo visto che la congettura di Serre è valida su anelli di polinomi su un campo. Rivisitando le dimostrazioni, si nota che tale risultato si può estendere ai PID, a patto di avere dei coefficienti invertibili nelle componenti del vettore unimodulare. In realtà, ci si può sempre ricondurre a questo caso ed è esattamente quanto mostrato da Suslin nella seconda parte della sua dimostrazione. Questo ci permetterà di ottenere un risultato più forte, legato all'hermitianetà dell'anello:

Definizione 3.10. Un anello si dice *d-Hermitiano* se ogni modulo stabilmente libero di rango $> d$ è libero.

Per quanto visto, $\mathbb{K}[x_1, \dots, x_n]$ è 0-Hermitiano. Per ottenere quanto voluto, dimostreremo che, dato A un PID, $A[x_1, \dots, x_n]$ è 1-Hermitiano. Infatti, per i moduli stabilmente liberi di rango 1, vale il seguente:

Proposizione 3.11. *Sia A un anello commutativo e sia P un A-modulo tale che $P \oplus A^{n-1} \simeq A^n$. Allora $P \simeq A$.*

Dimostrazione. Possiamo vedere P come il nucleo di un omomorfismo da A^n in A^{n-1}. In particolare, esiste una matrice $M \in M(n-1, n, A)$ che rappresenta tale applicazione. Notiamo che basta mostrare che i determinanti dei minori $n-1 \times n-1$ di M, $b_1, \dots, b_n \in A$, formano un vettore unimodulare. In tal caso, esistono $a_1, \dots, a_n \in A$ tali che $a_1 b_1 + \cdots + a_n b_n = 1$; detto allora

$$f_n = (a_1, -a_2, a_3, \dots, (-1)^{n+1} a_n)$$

si ottiene, completando la matrice con questa riga, una matrice invertibile e dunque la tesi. Supponiamo allora per assurdo che $b_1, \dots, b_n$ non generino l'ideale unità. Allora esiste un ideale massimale $\mathfrak{M}$ tale che $(b_1, \dots, b_n) \subseteq \mathfrak{M}$. Lavorando sul quoziente per $\mathfrak{M}$, per il teorema di completamento a base per spazi vettoriali, la matrice si completa a una matrice invertibile X. Sviluppando il determinante lungo l'ultima riga, otteniamo però che $\det(X) = 0$, un assurdo. □

Altezza di un ideale Trattiamo ora il caso dei moduli di rango superiore; per questo, è necessario utilizzare la nozione di altezza di un ideale. Ricordiamo che l'altezza ht di un ideale primo P è definita come la massima lunghezza

di una catena di primi contenuti in P. Per un ideale I qualsiasi, l'altezza ht è definita come il minimo delle lunghezze dei primi che contengono I. Abbiamo bisogno del seguente teorema, riportato senza dimostrazione:

Teorema 3.12 (di Krull)**.** *Sia A un anello noetheriano e sia I un ideale primo di altezza m. Allora m è il minimo naturale per il quale esiste un ideale J generato da m elementi tale che I è un primo minimale di A/J.*

Il teorema è una caratterizzazione molto utile a livello pratico; grazie a questo possiamo per esempio dimostrare il seguente lemma, che collega l'altezza di un ideale di $A[x]$ con l'altezza della sua contrazione in A.

Lemma 3.13. *Sia A un anello noetheriano e sia P un ideale primo di $A[x]$. Detto $I = P \cap A$, si ha*

$$ht(P) = \begin{cases} ht(I) \text{ se } P = I[x] \\ ht(I) + 1 \text{ se } P \supsetneq I[x] \end{cases}$$

Dimostrazione. La disuguaglianza $\geq$ è banale. Mostriamo che vale anche l'altra disuguaglianza. Sia $m = ht(I)$ e sia $J = (a_1, \ldots, a_m)$ un ideale per il quale I è un primo minimale di A/J. Per definizione di $I[x]$ e $J[x]$, $I[x]$ è un primo minimale di $A[x]/J[x]$, dove $J[x]$ è generato da almeno m elementi. Conseguentemente, $ht(I[x]) \leq m$. Se $I[x] = P$ abbiamo ottenuto l'uguaglianza cercata. Supponiamo allora che valga il contenimento stretto. Sia allora $f \in P \setminus I[x]$. Mostriamo che P è minimale su $I[x] + (f)$. Sia Q un primo tale che $I[x] \subseteq Q \subseteq P$. Allora necessariamente $Q \cap A = P \cap A$. A meno di quozientare, possiamo supporre $I = (0)$ e che I sia un dominio (ricordiamo che la contrazione di un primo è primo). Consideriamo l'anello di frazioni $S^{-1}A[x]$ ottenuto per $S = A \setminus \{0\}$. Tale anello è un PID, dunque di dimensione 1. Pertanto, otteniamo che $S^{-1}P = S^{-1}Q$. Per la corrispondenza biunivoca esistente tra gli ideali primi di $S^{-1}A$ e gli ideali primi di A che non intersecano S, $P = Q$ e dunque la tesi. □

Questo lemma, oltre a essere fondamentale nelle prossime dimostrazioni, ha anche un interessante corollario:

Corollario 3.14. *Sia A un anello noetheriano. Allora* $\dim(A[x_1, \ldots, x_n]) = n + \dim(A)$.

Quello che ci servirà nella dimostrazione del teorema del polinomio monico sarà un modo per ridurre il numero di variabili nel passo induttivo. Una strategia classica è quella di considerare l'ideale dei *leading coefficient*. Il problema è però dimostrare che l'altezza di un ideale e dell'ideale dei leading coefficient viene quasi conservata.

Lemma 3.15. *Sia A un anello noetheriano e sia I un ideale di $A[x]$. Allora $ht(lc(I)) \geq ht(I)$.*

Dimostrazione. Supponiamo prima che I sia un ideale primo. Sia $P = I \cap A$. Se $I = P[x]$, in tal caso $lc(I) = P$, e dunque, per il lemma 3.13,

$$ht(lc(I)) = ht(P) = ht(P[x]) = ht(I)$$

Se invece $I \supsetneq P[x]$, vale che $lc(I) \supseteq P$; dunque, ancora per il lemma 3.13,

$$ht(lc(I)) > ht(P) = ht(I) - 1 \Rightarrow ht(lc(I)) \geq ht(I)$$

Supponiamo ora che I sia un ideale qualunque e siano $P_1, \ldots, P_k$ i primi associati a I. Poiché l'anello è noetheriano, dato che $\prod P_i \subseteq \cap P_i$, esiste $n \in \mathbb{N}$ per il quale $(\prod P_i)^n \subseteq I$. Inoltre, visto che $lc(IJ) \subseteq lc(I)lc(J)$, $(\prod lc(P_i))^n \subseteq lc(I)$. Sia ora Q un primo di A tale che $ht(lc(I)) = ht(Q)$. Dalla relazione

$$(\prod lc(P_i))^n \subseteq lc(I) \subseteq Q$$

segue per il lemma di scansamento che esiste un indice i per il quale $lc(P_i) \subseteq Q$. Dunque,

$$ht(I) \leq ht(P_i) \leq ht(lc(P_i)) \leq ht(Q) = ht(lc(I))$$

come voluto. □

Il teorema del polinomio monico Possiamo ora sfruttare i risultati ottenuti per dimostrare il *teorema del polinomio monico di Suslin*, che in pratica sostituirà il trucco di Nagata nella dimostrazione del teorema di Quillen-Suslin:

Teorema 3.16. *Sia A un anello noetheriano di dimensione finita d. Sia I un ideale di $A[x_1, \ldots, x_n]$, con $ht(I) > d$. Allora esiste un automorfismo di*

A-algebre di $A[x_1, \ldots, x_n]$ per il quale, nell'immagine, esista un polinomio di I monico.

Dimostrazione. Procediamo per induzione sul numero di variabili. Se $n = 0$, $ht(I) > d$ implica che $I = A$ e dunque l'enunciato è ovvio. Assumiamo vera la tesi per $n-1$ e mostriamo che vale per n. Per comodità, sia $B = A[x_1, \ldots, x_{n-1}]$. Vediamo allora I come un ideale in $B[x_n] = A$, e dunque $lc(I) \subseteq B$. Per il lemma 3.15, $ht(lc(I)) \geq ht(I) > d$; per ipotesi induttiva, possiamo supporre allora che B contenga un polinomio g monico in x_1 in $lc(I)$,

$$g = x_1^N + g_{N-1}(x_2, \ldots, x_{n-1})x_1^{N-1} + \cdots + g_0(x_2, \ldots, x_{n-1})$$

Per definizione di $lc(I)$, esiste allora un polinomio $f \in I$

$$f = g \cdot x_n^m + b_{m-1}x_n^{m-1} + \cdots + b_0$$

Sia M la massima potenza di x_1 che compare nei polinomi $b_{m-1}, \ldots, b_0$. Attuiamo il cambio di variabile

$$x_i \longmapsto \tilde{x}_i \ \forall i < n$$
$$x_n \longmapsto \tilde{x}_n + x_1^K$$

con K da determinare. In seguito a questo cambio di variabile, otteniamo che il grado massimo in $\tilde{x}_1$ di $b_{m-1}x_n^{m-1} + \cdots + b_0$ è $\leq M + (m-1)K$. D'altra parte, il grado di $g \cdot x_m^n$ è esattamente $n + mK$. Scelto allora $K = M - n + 1$, si ha che f risulta monico in $\tilde{x}_1$, come voluto. □

Per poter utlizzare il teorema efficacemente, bisogna prima trovare prima avere delle informazioni sull'altezza dell'ideale generato dai segmenti iniziali di un vettore unimodulare. In particolare, è necessaria una sorta di pre-processing del vettore per portarlo in una forma conveniente:

Lemma 3.17. *Sia A un anello commutativo noetheriano e consideriamo $f = (f_1, \ldots, f_n)$ un vettore unimodulare su A^n. Allora esiste un vettore unimodulare $f' = (f'_1, \ldots, f'_n)$ tale che*

$$f \sim_{E(n,A)} f'$$

e per ogni $r \leq n$, $ht(f'_1, \ldots, f'_r) \geq r$.

Dimostrazione. Supponiamo $ht(f_1, \ldots, f_r) \geq r$ e mostriamo che a meno di agire con matrici elementari $ht(f_1, \ldots, f_{r+1}) \geq r+1$ (stiamo procedendo per induzione, ma il passo base è equivalente a quello induttivo). Consideriamo l'anello $A/(f_1, \ldots, f_r)$ e l'ideale J generato da $(\bar{f}_{r+2}, \ldots, \bar{f}_n)$. Mostriamo che in $\bar{f}_{r+1} + J$ vi è un elemento che non sta nell'unione dei primi minimali del quoziente; da questo seguirebbe la tesi. Consideriamo i primi minimali $P_1, \ldots, P_k$ che contengono $(f_1, \ldots, f_r)$. Possiamo considerare il sottoinsieme moltiplicativo $S = A \setminus (P_1 \cup \cdots \cup P_k)$ e ottenere allora un anello di frazioni semilocale. Procedendo come nella dimostrazione della proposizione 3.7, si ottiene la tesi. □

Vedremo che a livello algoritmico il lemma appena mostrato sarà fondamentale per risolvere dei casi particolari. Abbiamo sviluppato la teoria necessaria per dimostrare il teorema anticipato a inizio capitolo:

Teorema 3.18. *Sia A un anello noetheriano di dimensione d. Allora l'anello $A[x_1, \ldots, x_n]$ è d-hermitiano.*

Dimostrazione. Dimostriamo intanto che le ipotesi garantiscono che A è d-hermitiano. Come al solito, possiamo rappresentare matricialmente il problema; ci basta cioè provare che un vettore unimodulare $f = (f_1, \ldots, f_k)$ con $k \geq d+2$ ha la proprietà di estensione. Siano $P_1, \ldots, P_h$ i primi minimali di A. Possiamo supporre, a meno di agire come nel lemma 3.17, che $f_1 \notin \cup_i P_i$. Se $d = 0$, allora a_1 è invertibile e dunque A è chiaramente hermitiano. Se $d \geq 1$, consideriamo l'anello $A/(f_1)$. Poichè la dimensione di questo anello è minore di d, per ipotesi induttiva otteniamo che

$$(\bar{f}_2, \ldots, \bar{f}_k) \sim_{E(n-1, A/(f_1))} (\bar{1}, \bar{0}, \ldots, \bar{0})$$

e questo basta per dire che $f \sim_{E(n,A)} e_1$. Mostriamo ora che la stessa proprietà vale per $A[x_1, \ldots, x_n]$. Visto che quanto detto fino ad ora corrisponde al passo base, procediamo per induzione sul numero di variabili. Per il lemma 3.17, possiamo supporre che $\forall r \leq k$ $ht(f_1, \ldots, f_r) \geq r$. In particolare, abbiamo che $(f_1, \ldots, f_{k-1})$ ha altezza maggiore di d. Per il teorema del polinomio monico di Suslin, mediante un isomorfismo di A-algebre, otteniamo

un polinomio $g = \sum c_i f_i$ monico in x_1. Detto $n = \deg_{x_1}(f_k)$, possiamo allora agire mediante la matrice

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ c_1 x_1^n & \cdots & c_{k-1} x_1^n & 1 \end{pmatrix} \in E(k, A[x])$$

e ottenere un polinomio monico in x_1 tra gli elementi del vettore unimodulare. Per quanto visto nel teorema 3.8, possiamo allora valutare in 0 e concludere per ipotesi induttiva. □

Con questo teorema abbiamo ottenuto dunque la generalizzazione richiesta: sugli anelli noetheriani di dimensione 1 la nozione di modulo stabilmente libero su $A[x_1, \ldots, x_n]$ coincide con quella di modulo libero; i nuclei degli omomorfismi tra moduli liberi sono cioè liberi. Questo vale quindi non solo per i PID, ma anche per i domini di Dedekind. Inoltre, abbiamo dimostrato che per un anello noetheriano di dimensione finita, vale lo stesso. Abbiamo dunque ampliato notevolmente il campo di validità dell'equivalenza libero-stabilmente libero. La prossima sezione ci mostrerà però che non possiamo essere troppo ottimisti sulla possibilità di estendere ulteriormente il teorema a classi di anelli più ampie.

3.3 Un controesempio

Mostriamo ora con un controesempio che le ipotesi non possono essere indebolite troppo; diamo cioè un esempio di un modulo stabilmente libero non libero. Consideriamo l'anello

$$A = \mathbb{R}[x, y, z] \big/ (x^2 + y^2 + z^2 - 1)$$

Notiamo che A non è un PID, ma è noetheriano ed è un dominio. Inoltre A ha dimensione 2; in base al teorema dimostrato, ogni modulo stabilmente libero di rango ≥ 3 è libero. Poichè abbiamo visto che il risultato è sempre vero per modulo stabilmente liberi di rango 1, possiamo cercare il controesempio tra i modulo stabilmente liberi di rango 2. Consideriamo allora il sottomodulo $T = \{(f, g, h) \in A^3 \mid fx + gy + hz = 0 \ in \ R\}$ e mostriamo allora che $A \oplus T \simeq$

A^3. Su A è ben definito il prodotto scalare standard $(a,b,c)\cdot(\alpha,\beta,\gamma) = a\alpha + b\beta + c\gamma$. Dato $v \in A^3$, sia $r = v\cdot(x,y,z)$. Allora

$$(v - r(x,y,z))\cdot(x,y,z) = v\cdot(x,y,z) - r(x,y,z)\cdot(x,y,z) = r - r = 0$$

di conseguenza $v - r(x,y,z) \in T$. Ogni elemento ammette la scrittura

$$v = \underbrace{v - r(x,y,z)}_{\in T} + \underbrace{r(x,y,z)}_{\in(x,y,z)}$$

e quindi $A^3 \simeq T + \langle(x,y,z)\rangle$. Mostriamo ora che la somma è diretta. Sia $a \in \langle(x,y,z)\rangle \cap T$; allora $a = r(x,y,z)$, con $r \in A$. Poiché $a \in T$, si ottiene che $a\cdot(x,y,z) = 0$, per definizione di T. Svolgendo il conto,

$$r(x,y,z)\cdot(x,y,z) = r(x^2+y^2+z^2) = r = 0$$

dunque $a = 0$. La somma è allora diretta:

$$A^3 \simeq \langle(x,y,z)\rangle \oplus T$$

Notiamo però che $a(x,y,z) = (0,0,0) \Rightarrow a = 0$; di conseguenza, l'omomorfismo

$$\begin{array}{rccc} f\colon & A & \longrightarrow & \langle(x,y,z)\rangle \\ & a & \longmapsto & a(x,y,z) \end{array}$$

è un isomorfismo di A-moduli, dunque

$$A^3 \simeq A \oplus T$$

Supponiamo ora per assurdo che $T \simeq A^2$. Esiste quindi una base di T, (f,g,h), (a,b,c). Una base di A^3 è quindi (x,y,z), (f,g,h), (a,b,c). La matrice

$$\begin{pmatrix} x & f & a \\ y & g & b \\ z & h & c \end{pmatrix}$$

è invertibile, cioè

$$\det\begin{pmatrix} x & f & a \\ y & g & b \\ z & h & c \end{pmatrix} \in A^*$$

Consideriamo l'applicazione:

$$\begin{array}{rccc} \varphi\colon & S^2 & \longrightarrow & \mathbb{R}^3 \\ & v & \longmapsto & (f(v), g(v), h(v)) \end{array}$$

Tale applicazione è ben definita, perché presi altri rappresentanti della classe di f, g, h, questi assumono lo stesso valore su S^2. Inoltre, poiché il determinante della matrice sopra è sempre invertibile, questo implica che $(f(v), g(v), h(v)) \neq (0,0,0)$ per ogni $v \in S^2$. Normalizzando, otteniamo

$$\begin{array}{rccc} \varphi\colon & S^2 & \longrightarrow & S^2 \\ & v & \longmapsto & (\frac{f(v)}{\|f(v)\|}, \frac{g(v)}{\|g(v)\|}, \frac{h(v)}{\|h(v)\|}) \end{array}$$

Dobbiamo verificare che il campo vettoriale sia tangente, cioè che

$$\left(\frac{f(v)}{\|f(v)\|}, \frac{g(v)}{\|g(v)\|}, \frac{h(v)}{\|h(v)\|}\right) \cdot v = 0$$

Questa condizione è però garantita dalla definizione del modulo T. Abbiamo allora trovato un campo vettoriale tangente su S^2 mai nullo e questo è assurdo, in quanto S^2 non è pettinabile [8]. Siamo allora riusciti a trovare il controesempio di rango più basso possibile; abbiamo dimostrato quindi che su A il teorema di Quillen-Suslin non vale.

3.4 La dimostrazione di Vaserstein

Vediamo ora un'altra dimostrazione della congettura, fornita da Vaserstein nell'ottobre del 1976, pubblicata mesi dopo quelle fornite da Quillen e Suslin. Tale dimostrazione si basa sull'idea di lavorare su anelli locali e riunire le informazioni per arrivare alla matrice voluta. Inoltre, il percorso seguito per arrivare alla tesi ci guiderà dopo nella dimostrazione algoritmica, che per l'appunto trarrà vantaggio dalle prove fornite.

Vaserstein iniziò il suo lavoro dagli anelli locali:

Teorema 3.19 (di Horrocks)**.** *Sia $(A, \mathfrak{M})$ un anello locale e sia $A[x]$ l'anello dei polinomi in una variabile su A. Sia $f = (f_1, \cdots f_n)$ un vettore unimodulare di $A[x]^n$ tale che almeno una componente abbia coefficiente di testa 1. Allora f ha la proprietà di estensione.*

Dimostrazione. Se $n = 1$ il teorema è banale. Supponiamo $n = 2$, cioè $f = (f_1, f_2)$. Poiché $(f_1, f_2) = 1$, esistono $h_1, h_2 \in A[x]$ tali che $f_1h_1 + f_2h_2 = 1$. Di conseguenza possiamo esibire direttamente la matrice:

$$\begin{pmatrix} f_1 & -h_2 \\ f_2 & h_1 \end{pmatrix}$$

che è invertibile poiché ha determinante 1, ed ha come prima colonna f. Supponiamo allora $n \geq 3$. Procediamo per induzione sul minimo grado d delle componenti di f che hanno termine di testa 1. Se $d = 0$, l'enunciato è ovvio: le componenti del vettore unimodulare sono tutti elementi di A. Poichè A è locale, almeno un elemento di f deve essere invertibile; di conseguenza, esiste $M \in E(n, A)$ tale che $f \cdot M = e_1^t$. Mostriamo ora il passo induttivo. Grazie alla divisione euclidea e al fatto che la moltiplicazione del vettore per una matrice invertibile conserva la proprietà di essere unimodulare, possiamo supporre che f_1 abbia coefficiente di testa 1, grado d e che le altre componenti abbiano grado minore di d. Poiché f è unimodulare, esistono dei polinomi $h_1, \cdots, h_n$ tali che

$$\sum_{i=1}^{n} h_i f_i = 1$$

Questa relazione deve continuare a valere anche dopo la riduzione modulo $\mathfrak{M}$, quindi almeno un coefficiente di $f_2, \cdots f_n$ non appartiene all'ideale massimale, e dunque è invertibile perché l'anello è locale. A meno di permutare gli f_i, possiamo supporre che f_2 abbia un coefficiente che sia un'unità. Abbiamo allora:

$$f_1(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$
$$f_2(x) = b_s x^s + b_{s-1}x^{s-1} + \cdots + b_0$$

dove, per quanto detto, almeno un b_i è una unità. Sia ora

$$I = \{lt(h) \mid h \in (f_1, f_2) \wedge \deg(h) \leq d - 1\}$$

I è un ideale di A; infatti:

- Siano $a, b \in I$. Per definizione, esistono dei polinomi $f, g \in (f_1, f_2)$ di grado $\leq d - 1$ tali che $lt(f) = a$ e $lt(g) = b$. Supponiamo che

$\deg(f) = n \geq deg(g) = m$. Allora, $lt(f + x^{n-m}g) = a + b$ e $\deg(f + x^{n-m}g) = n \leq d - 1$, come voluto.

- Sia $a \in I$ e sia $s \in A$. Per definizione, esiste un polinomio $f \in (f_1, f_2)$ di grado $\leq d - 1$ per il quale $lt(f) = a$. Di conseguenza, $lt(sf) = sa$ e dunque la tesi.

Mostriamo che $I = (1)$ o equivalentemente che $b_i \in I \ \forall i$. Chiaramente, $b_s \in I$. Detto $g_1 = x^{d-s}f_2 - b_s f_1$, si ha $lc(g_1) = a_{d-1}b_s + b_{s-1}$, e poiché I è un ideale e $b_s \in I$, si ha che $b_{s-1} \in I$. In generale, detto $g_{i+1} = lm(g_i)f_1 - x^{d-\deg(g_i)}g_i$, si verifica allo stesso modo che, sfruttando il fatto che I sia un ideale, $b_i \in I \ \forall i$. Di conseguenza, esiste una combinazione lineare $g_1 f_1 + g_2 f_2$ di grado $\leq d-1$ e coefficiente di testa 1. Possiamo allora sfruttare questo polinomio per abbassare il grado dei polinomi $f_3, \cdots, f_n$ tramite operazioni di riga e fare in modo che uno di questi abbia grado $d-1$ e coefficiente di testa 1. Per ipotesi induttiva, la tesi. □

Il teorema appena dimostrato ci dice quindi che, dato A un anello locale, un vettore unimodulare f di $A[x]^n$ con una componente avente coefficiente direttore 1 è equivalente al vettore della base canonica e_1. Poiché almeno uno dei termini noti delle componenti deve essere invertibile, possiamo anche dire che $f(x)$ è equivalente al vettore $f(0)$, dove cioè ogni componente viene valutata in $x = 0$. Cerchiamo ora di sollevare le informazioni ricavate dalle localizzazioni all'anello di partenza.

Lemma 3.20. *Sia A un dominio di integrità e sia S un sottoinsieme moltiplicativamente chiuso. Sia $f \in A[x]^n$. Se $f(x) \sim f(0)$ su $(S^{-1}A)[x]$, esiste $c \in S$ tale che $f(x + cy) \sim f(x)$ su $A[x, y]$.*

Dimostrazione. Dalla definizione della relazione di equivalenza, sappiamo che esiste una matrice $M(x) \in GL(n, (S^{-1}A)[x])$ tale che

$$M(x)f(0) = f(x)$$

Di conseguenza, $f(0) = M(x)^{-1}f(x)$ è costante e dunque invariante per traslazione. Vale quindi anche $f(0) = M(x + y)^{-1}f(x + y)$. Definiamo $G(x, y) = M(x)M(x + y)^{-1}$. Notiamo allora che

$$G(x, y)f(x + y) = M(x)M(x + y)^{-1}f(x + y) = M(x)f(0) = f(x)$$

Inoltre, $G(x,0) = I$ e dunque possiamo scrivere $G(x,y) = I + yH(x,y)$ separando le componenti in y della matrice, dove $H(x,y) \in M(n, (S^{-1}A)[x,y])$. Per ogni entrata della matrice, esiste dunque $s_{ij} \in S$ tale che $s_{ij}H_{ij} \in A[x,y]$. Sia allora $c = \prod_{i,j} s_{ij}$. Allora

$$G(x,cy) = I + cyH(x,cy) \in M(n, A[x,y])$$

Di conseguenza,

$$G(x,cy)f(x+cy) = M(x)M(x+cy)^{-1}f(x+cy) = M(x)f(0) = f(x)$$

e dunque $f(x+cy) \sim f(x)$, come voluto. □

Abbiamo preparato il campo per il mezzo fondamentale della dimostrazione del teorema: la possibilità di 'eliminare' una variabile.

Proposizione 3.21. *Sia A un dominio di integrità e sia f un vettore unimodulare in $A[x]^n$ tale che una componente abbia coefficiente di testa 1. Allora $f(x) \sim f(0)$ su $A[x]$.*

Dimostrazione. Sia $J = \{c \in A \mid f(x+cy) \sim f(x) \text{ su } A[x,y]\}$. J è un ideale di A; infatti

- Se $a, b \in J$, mostriamo che $a + b \in J$. Poiché $f(x) \sim f(x+ay)$, per traslazione $x \to x + by$, si ha $f(x+ay+by) \sim f(x+by)$ (dato che l'immagine tramite la valutazione di un invertibile è invertibile) e per ipotesi $f(x+by) \sim f(x)$. Per transitività della relazione di equivalenza, $f(x+ay+by) \sim f(x)$.

- Sia $a \in J$ e sia $b \in A$. Per ipotesi, $f(x+ay) \sim f(x)$, cioè esiste una matrice $M \in GL(n, A[x,y])$ tale che $M(x,y)f(x+ay) = f(x)$. Mediante un cambio di coordinate $y \to by$, si ha la relazione $M(x,by)f(x+aby) = f(x)$ (sempre perché l'immagine di un invertibile è invertibile), e dunque $f(x+aby) \sim f(x)$.

Sia P un ideale primo di A. Sappiamo allora che $f(x) \sim f(0)$ su $A_P[x]$ per il teorema di Horrocks 3.19. Per il lemma 3.20, esiste $c \in A \setminus P$ tale che $f(x+cy) \sim f(0)$ in $A[x,y]$. Dunque $J \not\subseteq P$; poiché possiamo ripetere

il ragionamento per ogni ideale massimale di A, si ottiene che $1 \in J$. Per definizione di J, allora, esiste una matrice $M \in GL(n, A[x, y])$ tale che

$$M(x, y)f(x + y) = f(x)$$

Possiamo allora valutare in 0 la variabile x e ottenere la tesi. □

La proposizione appena dimostrata è analoga a quella data da Suslin nel teorema 3.8 e dunque possiamo ripetere la dimostrazione per induzione fornita nel teorema 3.9. Sfruttiamo ora il background astratto che abbiamo costruito per fornire un algoritmo.

3.5 Una dimostrazione algoritmica

Cerchiamo ora di ricavare un algoritmo che ci permetta di trovare una base di un modulo proiettivo da una sua presentazione. Per semplicità, proveremo il teorema nella forma

Teorema 3.22. *Sia $A \in M(l, m, \mathbb{C}[x_1, \ldots, x_n])$ una matrice unimodulare. Allora esiste una matrice $U \in GL(m, \mathbb{C}[x_1, \ldots, x_n])$ tale che*

$$AU = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 & \ldots & 0 \end{pmatrix}$$

Come nel caso astratto, ci possiamo ridurre a dimostrare l'enunciato nel caso di un vettore unimodulare:

Teorema 3.23. *Sia $f = (f_1, \ldots, f_m)$ una riga unimodulare di $\mathbb{C}[x_1, \ldots, x_n]$. Allora esiste una matrice $A \in M(m, \mathbb{C}[x_1, \ldots x_n])$ tale che $fA = e_1^t$.*

Procederemo per induzione sul numero di variabili.

I casi semplici Notiamo subito che ci sono dei casi particolarmente semplici. Abbiamo già visto durante la dimostrazione del teorema di Horrocks 3.19 che il caso $m = 2$ si risolve esplicitamente. Nel caso $n = 1$, invece, possiamo agire per divisione euclidea sul vettore, portando ogni componente a una costante. Chiaramente il vettore f è equivalente al vettore e_1 e quindi

anche questo caso è risolto banalmente.
Un altro caso particolare è quello in cui $m > n + 1$. In tal caso infatti, il lemma 3.17 ci permette di supporre, a meno di agire tramite trasformazioni elementari, che l'ideale generato da $f_1, \ldots, f_{n+1}$ sia l'ideale unità. Tramite il calcolo della base di Gröbner, possiamo trovare degli elementi $g_1, \ldots g_{n+1} \in \mathbb{C}[x_1, \cdots, x_n]$ tali che

$$g_1 f_1 + \ldots g_{n+1} f_{n+1} = 1$$

dunque possiamo direttamente esibire la matrice $U \in GL(m, \mathbb{C}[x_1, \ldots, x_n])$. In realtà, questo suggerisce di tenere sempre disponibili delle informazioni sugli ideali generati da ogni sottoinsieme proprio di elementi del vettore unimodulare. Se infatti uno di questi generasse l'ideale unità, potremmo agire come sopra mediante trasformazioni elementari e risolvere in maniera diretta il problema.

Descrizione del main cycle Supponiamo allora di non essere in nessuno di questi casi particolari e procediamo al passo induttivo. Per chiarezza di esposizione, chiamiamo $t \coloneqq x_n$. Possiamo supporre che uno dei polinomi $f_i(x_1, \ldots, x_{n-1}, t)$ sia monico in t. Se non siamo in questa situazione, possiamo infatti considerare il cambiamento di variabili (il trucco di Nagata, lemma di Normalizzazione di Noether)

$$\begin{array}{ccc} x_1 & \longmapsto & \tilde{x}_1 + \tilde{t}^{M_1} \\ & \vdots & \\ x_{n-1} & \longmapsto & \tilde{x}_{n-1} + \tilde{t}^{M_{n-1}} \\ t & \longmapsto & \tilde{t} \end{array}$$

con gli M_i sufficientemente grandi e ottenere nelle nuove coordinate un polinomio monico in $\tilde{t}$. Entriamo ora nel main cycle dell'algoritmo. Supponiamo all'inizio del ciclo di avere i polinomi $r_1, \ldots r_{k-1} \in \mathbb{C}[x_1, \ldots, x_{n-1}]$ che corrispondono ai polinomi ottenuti nelle iterazioni precedenti e $a_k \in \mathbb{C}$. All'inizializzazione, $a_0 = 0$.

- L'ideale $\mathcal{I}(\{a_k\})$ è massimale, e lo denotiamo con $\mathfrak{M}_k$. Per le proprietà dei vettori unimodulari, $f(a_k, t) = (f_1(a_k, t), \ldots, f_m(a_k, t))$ è un vettore unimodulare di $\mathbb{C}[t]$; di conseguenza, detto p un generatore

dell'ideale $(f_2(a_k,t),\dots,f_m(a_k,t))$ ($\mathbb{C}[t]$ è un PID), si ha

$$(p)+(f_1(a_k,t))=\mathbb{C}[t]$$

Tramite l'algoritmo euclideo, possiamo allora trovare una matrice $E_k \in GL(m-1,\mathbb{C}[t])$ tale che

$$(f_2(a_k,t),\dots,f_m(a_k,t))\cdot E_k = p(t)\cdot e_1^t$$

- La valutazione commuta con la moltiplicazione di matrici e dunque

$$f(x,t)\underbrace{\begin{pmatrix}1 & 0\\ 0 & E_k\end{pmatrix}}_{A_k} = (f_1(x,t),p(t)+q_2(x,t),q_3(x,t),\dots,q_m(x,t))$$

dove ogni q_i appartiene a $\mathfrak{M}_k$. Calcoliamo ora il risultante r_k dei polinomi f_1 e $p+q_2$ rispetto alla variabile t; per le proprietà del risultante ([3]), $r_k \in (f_1(x,t),p(t)+q_2(x,t))$ e quindi esistono $v,w\in\mathbb{C}[x_1,\dots,x_{m-1},t]$ tali che

$$v(x,t)f_1(x,t)+w(x,t)(p(t)+q_2(x,t))=r_k(x)$$

- Poiché f_1 è monico, vale il teorema di estensione, dunque

$$r_k(x_0)=0 \iff \exists t_0\in\mathbb{C}\ t.c.\ f_1(x_0,t_0)=p(t_0)+q_2(x_0,t_0)=0$$

Di conseguenza, $r_k(a_k)\neq 0$; localizzando per $\mathfrak{M}_k$, si ha allora che r_k è invertibile, e dunque la matrice

$$U_k(x,t) \coloneqq A_k \underbrace{\begin{pmatrix} vr_k^{-1} & -p-q_2 & & & \\ wr_k^{-1} & f_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}}_{B_k} \underbrace{\begin{pmatrix}1 & 0 & -q_3 & \dots & -q_m\\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}}_{C_k}$$

è invertibile su $(\mathbb{C}[x_1,\dots x_{m-1}])_{\mathfrak{M}_k}[t]$.

- La matrice U_k è tale che

$$\begin{aligned} f(x,t)U_k(x,t) &= f(x,t)\cdot A_k \cdot B_k \cdot C_k \\ &= (f_1(x,t), p(t)+q_2(x,t), q_3(x,t), \dots, q_m(x,t))\cdot B_k \cdot C_k \\ &= (1,0,q_3(x,t),\dots,q_m(x,t))\cdot C_k \\ &= e_1^t \end{aligned}$$

- Calcolando la base di Gröbner di $(r_1,\dots,r_k)$, si determina se l'ideale è (1) oppure no; in caso di risposta positiva, si esce dal ciclo, altrimenti si rinizia.

Per una migliore comprensione, diamo ora lo pseudocodice del ciclo:

$R \leftarrow \emptyset$
$a \leftarrow a_0 \in \mathbb{C}^{m-1}$
$k \leftarrow 0$
$finito \leftarrow false$
Tramite cambio di coordinate, trova f_1 monico in t
while $finito == false$ **do**
  $k++$
  Trova E tale che $(f_2(a,t),\dots,f_m(a,t))E = p(t)\cdot e_1^t$ tramite divisione euclidea
  Calcola i q_i di $(f_2(x,t),\dots f_m(x,t))E = (p(t)+q_2(x,t),\dots,q_m(x,t))$
  Calcola $r_k = \mathrm{Ris}_t(f_1, p+q_2)$
  $R \leftarrow R \cup \{r_k\}$
  Calcola $U_k(x,t)$
  $finito \leftarrow ((R) == \mathbb{C}[x_1,\dots,x_{m-1},t])$
  if $finito == false$ **then**
    Calcola una soluzione a_k di $R = 0$
    $a \leftarrow a_k$
  end if
end while

Si noti che il ciclo termina poiché $\mathbb{C}[x_1,\dots,x_{m-1},t]$ è noetheriano per il teorema della base di Hilbert, e ad ogni passo $r_k \notin (r_1,\dots r_{k-1})$.

Patching Il problema delle matrici trovate è che non sono a coefficienti in $\mathbb{C}[x_1,\dots,x_{m-1},t]$; l'obiettivo è allora quello di unire le informazioni trovate

sui localizzati per ottenere la matrice voluta.

Al termine del ciclo, poiché $(r_1, \dots, r_k) = \mathbb{C}[x_1, \dots x_{m-1}, t]$, si ha anche $(r_1^m, \dots, r_k^m) = \mathbb{C}[x_1, \dots x_{m-1}, t]$, dunque possiamo trovare dei g_i tali che

$$g_1 r_1^m + \cdots + g_k r_k^m = 1$$

Introduciamo ora le variabili y e s e definiamo le matrici:

$$A_i(s, z) \coloneqq U_i(x, s) U_i^{-1}(x, s + z)$$

A_i è a coefficienti in $(\mathbb{C}[x_1, \dots, x_{m-1}])_{\mathfrak{M}_i}[s, z]$. Per definizione di U, $r_i U_i \in \mathbb{C}[x_1, \dots, x_{m-1}, s, z]$ e, dalla formula dell'aggiunta per il calcolo dell'inversa, si ha che la matrice $r_i^{m-1} U_i^{-1} \in \mathbb{C}[x_1, \dots, x_{m-1}, s, z]$. Di conseguenza, $r_i^m A_i$ è una matrice di $\mathbb{C}[x_1, \dots, x_{m-1}, s, z]$.

Separando le componenti di A_i non dipendenti da z, si ottiene:

$$A_i(s, z) = I + z H_i(s, z)$$

dove l'identità si ottiene poiché $A_i(s, 0) = U_i U_i^{-1}$. Valutando la relazione trovata in $z r_i^m$, si ottiene allora:

$$A_i(s, z r_i^m) = I + z r_i^m H_i(s, z r_i^m)$$

in $\mathbb{C}[x_1, \cdots, x_{m-1}, s, z]$. Allora,

$$\begin{aligned} f(s) A_i(s, z r_i^m) =& f(s) U_i(s) U_i(s + r_i^m z) f(s + z r_i^m) \\ =& e_i^t U_i^{-1}(s + r_i^m z) \\ =& f(s + r_i^m z) \end{aligned}$$

Definiamo allora

$$\begin{aligned} U(x, t) \coloneqq& A_1(t, -t g_1 r_1^m) \cdot A_2(t - t g_1 r_1^m, -t g_2 r_2^m) \\ & \cdot A_3(t - t g_1 r_1^m - t g_2 r_2^m, -t g_3 r_3^m) \\ & \vdots \\ & \cdot A_k(t - \sum_{i=1}^{k-1} t g_i r_i^m, -t g_k r_k^m) \end{aligned}$$

La matrice U è proprio quella cercata; infatti:

$$\begin{aligned}
f(t)U(t) =& f(t)A_1(t, -tg_1r_1^m)\cdots A_k(t-\sum_{i=1}^{k-1} tg_ir_i^m, -tg_kr_k^m)\\
=& f(t-tg_1r_1^m)A_2(t-tg_1r_1^m, -tg_2r_2^m)\cdots A_k(t-\sum_{i=1}^{k-1} tg_ir_i^m, -tg_kr_k^m)\\
=& \dots\\
=& f(t-\sum_{i=1}^{k-1} tg_ir_i^m)A_k(t-\sum_{i=1}^{k-1} tg_ir_i^m, -tg_kr_k^m)\\
=& f(t-\sum_{i=1}^{k} tg_ir_i^m) = f(0)
\end{aligned}$$

A questo punto, $f(0)$ è unimodulare in $n-1$ variabili. Possiamo allora concludere per ipotesi induttiva.

Algoritmo Consideriamo ora un modulo proiettivo presentato come immagine, nucleo o conucleo di una matrice polinomiale. Diamo ora un procedimento per il calcolo di una base di P.

Tramite il procedimento descritto nel secondo capitolo, possiamo trovare una risoluzione libera finita:

$$0 \to A^{n_s} \xrightarrow{M_s} A^{n_{s-1}} \xrightarrow{M_{s-1}} \dots \xrightarrow{M_1} A^{n_0} \xrightarrow{\Phi} P \to 0$$

dove ogni $M_i \in M(n_{i-1}, n_i, A)$. Poiché P è proiettivo, la successione

$$0 \to \mathrm{Ker}(\Phi) \to A^{n_0} \to P \to 0$$

spezza, e dunque $\mathrm{Ker}(\Phi) = \mathrm{Im}(M_1)$ è proiettivo. Induttivamente, si trova allora che $\mathrm{Im}(M_s)$ è proiettivo e la successione

$$0 \to A^{n_s} \xrightarrow{M_s} A^{n_{s-1}} \xrightarrow{M_{s-1}} \mathrm{Im}(M_{s-1}) \to 0$$

spezza. Esiste allora una retrazione B_s tale che $B_sM_s = I_{n_s}$; M_s è di conseguenza unimodulare. Possiamo utilizzare l'algoritmo sopra descritto per calcolare una matrice $U_{s-1} \in GL(n_{s-1}, A)$ che estende M_s. Le prime n_s colonne di U_{s-1} sono uguali alle colonne di M_s. Le colonne che completano

M_s a una matrice invertibile sono una base di $\mathrm{Ker}(B_s)$; denotiamo questa sottomatrice con V_{s-1}. Definiamo $C_{s-1} = M_{s-1}V_{s-1}$.

Proposizione 3.24. *La successione*

$$0 \to A^{n_{s-1}-n_s} \xrightarrow{C_{s-1}} A^{n_{s-2}} \xrightarrow{M_{s-2}} \dots \xrightarrow{M_1} A^{n_0} \xrightarrow{\Phi} P \to 0$$

è una risoluzione libera finita di P.

Dimostrazione. Consideriamo il diagramma

$$\begin{array}{ccccc} & & \overset{B_s}{\curvearrowleft} & & \\ 0 \to A^{n_s} & & A^{n_{s-1}} & \xrightarrow{M_{s-1}} & \mathrm{Im}(M_{s-1}) \to 0 \\ & & \underset{M_s}{\curvearrowright} & \uparrow V_{s-1} & \\ & & & A^{n_{s-1}-n_s} & \\ & & & \uparrow & \\ & & & 0 & \end{array}$$

Per mostrare l'enunciato basta mostrare che $M_{s-1}V_{s-1}$ rappresenta un isomorfismo da $A^{n_{s-1}-n_s}$ in $\mathrm{Im}(M_{s-1})$. Per costruzione, $\mathrm{Im}(V_{s-1}) = \mathrm{Ker}(B_s)$; per esattezza della successione, M_{s-1} è un isomorfismo tra i moduli $\mathrm{Ker}(B_s)$ e $\mathrm{Im}(M_{s-1})$. Poiché V_{s-1} è iniettiva, abbiamo la tesi. □

Come conseguenza della proposizione, possiamo ripetere il procedimento s volte fino ad arrivare alla successione

$$0 \to A^s \xrightarrow{\Phi \circ C_0} P \to 0$$

A questo punto, l'immagine della base di A^s è una base di P, e questo termina la dimostrazione algoritmica del teorema di Quillen-Suslin. La dimostrazione è chiaramente adattabile al caso di un PID a patto di saper risolvere i seguenti problemi:

- Trovare un polinomio monico in una delle variabili
- Trovare un ideale massimale che contiene un ideale dato (se esiste)
- Trovare una risoluzione libera finita del modulo proiettivo dato

L'algoritmo non determina solo se un modulo è libero, ma ne determina una base e dunque il rango. Inoltre, se prendesse in ingresso un modulo non proiettivo, fallirebbe uno dei passi di riduzione della lunghezza della

risoluzione. Dunque, anche se poco efficiente, può essere utilizzato anche come test per verificare se un modulo è proiettivo. A livello computazionale, il problema maggiore di questo algoritmo è la difficoltà nel determinarne il costo computazionale. Non esistono stime sulla lunghezza del main cycle e anzi, in generale si può verificare che esso dipende dall'ideale massimale scelto.

Conclusioni In questo lavoro abbiamo esaminato quindi il percorso che in 40 anni ha portato dalla formulazione della congettura alla sua risoluzione, fino ad arrivare a una sua soluzione in senso algoritmico. Come spesso accade, infatti, rendere esplicito il lavoro svolto in astratto richiede anni, indipendentemente dalla sua importanza. Siamo partiti dalla nozione di modulo proiettivo, abbiamo considerato il caso particolare dei moduli stabilmente liberi e le risoluzioni libere finite, legando i tre concetti con il teorema di Serre. Abbiamo poi notato che la nozione di base di Gröbner risolve a livello algoritmico il problema dell'equivalenza proiettivo-stabilmente libero, enunciando il teorema delle sizigie di Hilbert, che in pratica traduce il teorema di Serre in termini computazionali. Il seguito è stata solo una conseguenza del lavoro svolto nella prima parte: la nozione di modulo stabilmente libero ci ha permesso di portare il problema sul campo dell'algebra lineare. Abbiamo così visto le dimostrazioni di Vaserstein e Suslin e in particolare la d-hermitianità di $A[x_1, \ldots, x_n]$ nel caso di A noetheriano di dimensione d. Tutta la teoria trattata è stata poi riutilizzata nell'algoritmo risolvente, dove alcuni accorgimenti utili per raffinare l'algoritmo sono derivati da lemmi e proposizioni dimostrate precedentemente. La risoluzione trovata viene allora accorciata fino a trovare l'isomorfismo del modulo proiettivo con un modulo libero.

Bibliografia

[1] B. Sturmfels A. Logar. *Algorithms for the Quillen-Suslin Theorem*. 1992.

[2] K. Conrad. *Stably Free Modules*.

[3] D. O'Shea D. Cox, J. Little. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 2006.

[4] T. Y. Lam. *Serre's Conjecture*. 1978.

[5] S. Lang. *Algebra*. 2005.

[6] L. Robbiano M. Kreuzer. *Computational Commutative Algebra 1*. 2000.

[7] I.G. MacDonald M.F. Atiyah. *Introduction to commutative algebra*. 1969.

[8] J. W. Milnor. *Topology from the Differentiable Viewpoint*. 1997.

[9] M. Stillman R. La Scala. *Strategies for Computing Minimal Free Resolutions*. 1998.