Appunti di Algebra 2

Carlo Sircana

Indice

1 Moduli **1**
- 1.1 Definizioni e prime proprietà . . . 1
  - 1.1.1 Operazioni sui moduli . . . 2
- 1.2 Il teorema di Hamilton-Cayley . . . 4
- 1.3 Successioni esatte . . . 6
- 1.4 Moduli Proiettivi . . . 14
- 1.5 Forma normale di Smith . . . 16

2 Anelli di polinomi **21**
- 2.1 Ideali monomiali . . . 21
- 2.2 Algoritmo di divisione e basi di Gröbner . . . 24
- 2.3 Risultante . . . 29

3 Varietà algebriche **33**
- 3.1 Definizioni e prime proprietà . . . 33
- 3.2 Nullstellensatz e sue conseguenze . . . 34

4 Prodotto Tensore **41**
- 4.1 Definizione e proprietà fondamentali . . . 41
- 4.2 Moduli Piatti . . . 48

5 Anelli e Moduli di Frazioni **50**
- 5.1 Anelli di Frazioni . . . 50
- 5.2 Moduli di frazioni . . . 54
- 5.3 Proprietà locali . . . 58
- 5.4 Esercizi e Complementi . . . 60

6 Moduli Noetheriani e Artiniani **64**
- 6.1 Definizioni e prime proprietà . . . 64
- 6.2 Decomposizione Primaria . . . 68
- 6.3 Anelli Artiniani . . . 72
- 6.4 Complementi . . . 74

Capitolo 1

Moduli

1.1 Definizioni e prime proprietà

Definizione 1.1. Sia A un anello. M si dice un A-modulo se $(M, +)$ è un gruppo abeliano munito di una funzione

$$\begin{array}{rccc} f\colon & A \times M & \longrightarrow & M \\ & (a, m) & \longmapsto & a \cdot m \end{array}$$

che rispetta le seguenti proprietà:

- $(a + b) \cdot m = a \cdot m + b \cdot m$
- $a \cdot (m + n) = a \cdot m + b \cdot m$
- $ab \cdot m = a \cdot (b \cdot m)$
- $1_A \cdot m = m$

Esempio.

- Se A è un campo, gli A-moduli sono tutti gli A-spazi vettoriali.
- Se A è un anello, A è un modulo su sé stesso.
- Se $B \subseteq A$ è un sottoanello, allora A è un B-modulo.
- Ogni $\mathbb{Z}$-modulo è un gruppo abeliano.

Definizione 1.2. $N \subseteq M$ è un sottomodulo se è un sottogruppo additivo di M chiuso rispetto alle operazioni, cioè per il quale $\forall a \in A\ \forall n \in N\ a \cdot n \in N$.

Esempio.

- $\{0\}$ è sempre un sottomodulo.
- I sottomoduli di A come A-modulo sono tutti e soli gli ideali.
- Preso I un ideale di A, l'insieme $IM = \{\sum a_i m_i \mid a_i \in I\ m_i \in M\}$ è un sottomodulo di M.

Definizione 1.3. Sia S un sottoinsieme di M. Definiamo il sottomodulo generato da S come $\langle S \rangle = \{\sum a_i s_i \mid a_i \in A\ s_i \in S\}$. Se $\#S = 1$ e $\langle S \rangle = M$, M si dice ciclico. Se $\#S < \infty$ e $\langle S \rangle = M$, M si dice finitamente generato.

Come abbiamo detto, gli spazi vettoriali sono in particolare dei moduli; cerchiamo allora di generalizzare la nozione di base e indipendenza lineare.

Definizione 1.4. Un insieme $S = \{s_1, \dots, s_k\}$ si dice libero se

$$\sum_{i=1}^{k} a_i s_i = 0 \Rightarrow a_i = 0 \ \forall i = 1, \dots, k$$

Un insieme di generatori libero si dice una base.

Come sempre, dopo aver definito le strutture, definiamo le mappe tra di esse.

Definizione 1.5. Siano M, N A-moduli. $f\colon M \to N$ è un omomorfismo di A-moduli se

$$f(m+n) = f(m) + f(n) \qquad\qquad f(am) = af(m)$$

Dato un omomorfismo, individuiamo i sottomoduli:

$$\mathrm{Ker}(f) = \{m \in M \mid f(m) = 0\}$$
$$\mathrm{Im}(f) = \{n \in N \mid \exists m \in M \ t.c. \ f(m) = n\}$$

Proposizione 1.6. *Sia M un A-modulo. Allora* $\mathrm{Hom}_A(A, M) \simeq M$

Dimostrazione. Consideriamo

$$\begin{array}{rccc} f\colon & M & \longrightarrow & \mathrm{Hom}_A(A, M) \\ & m & \longmapsto & f_m \end{array}$$

dove $f_m(a) := a \cdot m$. Tale applicazione è iniettiva e surgettiva, dunque è un isomorfismo. □

1.1.1 Operazioni sui moduli

Dati $\{M_i \mid i \in I\}$, definiamo il modulo somma come

$$\sum_{i \in I} M_i := \{\sum_i m_i \mid m_i \neq 0 \textit{ per un numero finito di indici e } m_i \in M_i\}$$

Si può definire anche l'ideale quoziente:

$$(M : N) = \{a \in A \mid aN \subseteq M\}$$

che è un ideale di A. Nel caso in cui $M = 0$, si definisce l'annullatore di N come $\mathrm{Ann}(N) = (0 : N)$. In analogia con gli spazi vettoriali, possiamo definire la somma diretta:

$$\bigoplus_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i \textit{ e } m_i \neq 0 \textit{ per un numero finito di indici}\}$$

Togliendo il vincolo sugli elementi nulli, otteniamo invece il prodotto diretto:

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i\}$$

Mostriamo che il prodotto diretto e la somma diretta rispettano delle proprietà universali

Proposizione 1.7. *Sia M_i una famiglia di A-moduli, sia N un A-modulo. Supponiamo che esista per ogni i un omomorfismo $\varphi_i \colon M_i \to N$. Detto $M = \oplus M_i$, si ha allora che esiste un omomorfismo $\varphi \colon M \to N$ che fa commutare i diagrammi (j è l'inclusione canonica):*

$$\begin{tikzcd} M_i \arrow[r, "j"] \arrow[d, "\varphi_i"'] & M \arrow[dl, dashed, "\varphi"] \\ N & \end{tikzcd}$$

Dimostrazione. Definiamo φ come

$$\begin{array}{cccc} \varphi\colon & M & \longrightarrow & N \\ & (m_1, m_2, \dots) & \longmapsto & \sum_{i\in I} \varphi_i(m_i) \end{array}$$

φ è ben definita perchè la somma è in realtà finita. Mostriamo allora l'unicità. Sia ψ un omomorfismo che fa commutare i diagrammi. Allora:

$$\psi(m) = \psi(\sum_i j(m_i)) = \sum_i \psi(j(m_i)) = \sum_i \varphi_i(m_i)$$

e dunque $\psi = \varphi$. □

Proposizione 1.8. *Sia M_i una famiglia di A-moduli, sia N un A-modulo. Supponiamo che esista per ogni i un omomorfismo $\varphi_i \colon N \to M_i$. Detto $M = \prod M_i$, si ha allora che esiste un omomorfismo $\varphi \colon N \to M$ che fa commutare i diagrammi:*

$$\begin{tikzcd} M \arrow[r, "\pi_i"] & M_i \\ N \arrow[u, dashed, "\varphi"] \arrow[ur, "\varphi_i"'] & \end{tikzcd}$$

Dimostrazione. Definiamo φ come

$$\varphi(n) = (\varphi_1(n), \varphi_2(n), \dots, \varphi_k(n), \dots)$$

Tale φ è un omomorfismo che fa commutari i diagrammi. Mostriamo l'unicità. Sia ψ un omomorfismo che fa commutare i diagrammi. Sia $\psi(n) = (b_i)_{i\in I}$. Allora

$$b_i = \pi_i \circ \psi(n) = \varphi_i(n)$$

e dunque $\varphi = \psi$. □

Prima di continuare, osserviamo che dato M un A-modulo e I un ideale, non sempre possiamo canonicamente munire M della struttura di A/I-modulo. Nel caso in cui però $I \subseteq \mathrm{Ann}(M)$, questo è però possibile. Infatti, l'operazione

$$(a + I)m = am$$

risulta ben definita e indipendente dal rappresentante. Fatta questa osservazione, guidati ancora una volta dal caso particolare degli spazi vettoriali, ci domandiamo ora se nel caso di un modulo libero è ancora vero che è ben definita una sorta di dimensione. La risposta è affermativa, e vale

Teorema 1.9. *Sia M un A-modulo libero. Allora tutte le basi hanno la stessa cardinalità.*

Dimostrazione. Sia $\mathfrak{M}$ un ideale massimale di A e consideriamo il modulo quoziente ${}^{M}\!/_{\mathfrak{M}M}$. Tale modulo, per l'osservazione fatta sopra, può essere munito della struttura di ${}^{A}\!/_{\mathfrak{M}}$-modulo, cioè della struttura di spazio vettoriale. Sia ora $\mathcal{B} = \{v_1, \dots, v_n\}$ una base di M come A-modulo. Mostriamo che le immagini dei v_i tramite la proiezione sono una base di ${}^{M}\!/_{\mathfrak{M}M}$ come ${}^{A}\!/_{\mathfrak{M}}$-spazio vettoriale. Chiaramente generano. Supponiamo

$$\sum \bar{a}_i \bar{v}_i = 0 \ \bar{a}_i \in {}^{A}\!/_{\mathfrak{M}}$$

Scelti dei rappresentanti, questo significa che

$$\sum a_i v_i \in \mathfrak{M}M$$

Per definizione di $\mathfrak{M}M$ esistono dei coefficienti $b_i \in \mathfrak{M}$ per i quali

$$\sum a_i v_i = \sum b_i v_i \Rightarrow \sum (a_i - b_i) v_i = 0$$

Poichè $\mathcal{B}$ è una base, questa relazione implica che $b_i = a_i \ \forall i$ e dunque $a_i \in \mathfrak{M}$. Di conseguenza la relazione in ${}^{M}\!/_{\mathfrak{M}M}$ doveva essere banale, dunque la tesi. $\square$

1.2 Il teorema di Hamilton-Cayley

Teorema 1.10 (di Hamilton-Cayley)**.** *Sia M un A-modulo finitamente generato e sia I un ideale di A. Sia φ un endomorfismo di M tale che $\varphi(M) \subseteq IM$. Allora esistono $a_0, \dots a_{n-1} \in I$ tali che*

$$\varphi^n + \sum_{i=0}^{n-1} a_i \varphi^i \equiv 0$$

Dimostrazione. Supponiamo $M = \langle m_1, \dots, m_n \rangle$. Poichè $\varphi(m_i) \in IM$, si ha

$$\varphi(m_i) = \sum_{j=1}^{n} c_{ij} m_j \quad c_{ij} \in I$$

$$\Longrightarrow \varphi(m_i) - \sum_{j=1}^{n} c_{ij} m_j = 0 \Longrightarrow \sum_{j=1}^{n} (\delta_{ij}\varphi - c_{ij}) m_j = 0$$

Abbiamo allora ottenuto la seguente rappresentazione matriciale:

$$\begin{pmatrix} \varphi - c_{11} & -c_{12} & \cdots & -c_{1n} \\ -c_{21} & \varphi - c_{22} & & \vdots \\ \vdots & & \ddots & \\ -c_{n1} & \cdots & & \varphi - c_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Sia ora $\tilde{A}$ la matrice aggiunta di A, cioè la trasposta della matrice dei cofattori; la matrice cioè che realizza $\tilde{A}A = \det(A)I$. Allora, si ha che

$$\tilde{A}A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Longrightarrow \det(A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Di conseguenza, $\det(A)m_i = 0 \ \forall i = 1, \dots n$. Poichè $\det(A) = \varphi^n + \sum a_i \varphi^i$ è un endomorfismo che si annulla su ognuno dei generatori di M, coincide con l'omomorfismo nullo, da cui la tesi. □

Il teorema di Hamilton-Cayley estende il teorema analogo per gli spazi vettoriali. Nonostante in questa forma sembri di scarsa importanza, ha numerosi corollari importanti. Il primo è sicuramente il lemma di Nakayama, dovuto a Krull e Azumaya.

Corollario 1.11 (Lemma di Nakayama - I forma)**.** *Sia M un A-modulo finitamente generato e sia I un ideale tale che $M = IM$. Allora esiste un elemento $a \in A$ tale che $a \equiv 1 \ (I)$ e $aM = 0$.*

Dimostrazione. Applichiamo il teorema di Hamilton-Cayley all'omomorfismo $id\colon M \to M$. Otteniamo allora dei coefficienti $a_i \in I$ tali che

$$id + \sum_{i=0}^{n-1} a_i id \equiv 0$$

Di conseguenza, $\forall m \in M$, $(1 + \sum a_i)m = 0$. Detto allora $a := 1 + \sum a_i$, si ha $aM = 0$ e $a \equiv 1 \ (I)$. □

Corollario 1.12 (Lemma di Nakayama - II forma)**.** *Sia M un A-modulo finitamente generato e sia $I \subseteq \mathcal{J}(A)$ un ideale di A tale che $IM = M$. Allora $M = 0$.*

Dimostrazione. Per la prima forma del lemma di Nakayama, esiste un elemento a tale che $a \equiv 1 \ (I)$ e $aM = 0$. Di conseguenza, $1 + a \in I \subseteq \mathcal{J}(A)$ e dunque $a \in A^*$. Di conseguenza, da $aM = 0$ si ottiene $M = 0$. □

Corollario 1.13 (Lemma di Nakayama - III forma)**.** *Sia M un modulo finitamente generato, sia N un suo sottomodulo e sia $I \subseteq \mathcal{J}(A)$ un ideale di A. Supponiamo che $M = N + IM$. Allora $M = N$.*

Dimostrazione. Per la seconda forma del lemma di Nakayama, ci basta mostrare che

$$M/N = I\left(M/N\right)$$

Notiamo però che

$$I\left(M/N\right) = \{\sum a_i(m_i + N) \mid a_i \in I \ m_i \in M\} =$$
$$= \{\sum a_i m_i + N \mid a_i \in I \ m_i \in M\} = IM + N/N = M/N$$

□

Diamo ora una conseguenza del lemma di Nakayama su anelli locali. Abbiamo prima bisogno di un lemma:

Lemma 1.14. *Sia $(A, \mathfrak{M})$ un anello locale e sia M un A-modulo finitamente generato. Sia $\bar{m}_1, \dots, \bar{m}_k$ una base di ${}^{M}\!/_{\mathfrak{M}M}$. Allora, comunque presi $m_1, \dots, m_k \in M$ tali che $\pi(m_i) = \bar{m}_i$, si ha che $M = \langle m_1, \dots, m_k \rangle$.*

Dimostrazione. Sia $N = \langle m_1, \dots, m_k \rangle \subseteq M$ e consideriamo il diagramma:

$$N \longrightarrow M \longrightarrow {}^{M}\!/_{\mathfrak{M}M}$$

Per costruzione, la composizione è un omomorfismo surgettivo, dunque $M = N + \mathfrak{M}M$. Per località dell'anello, $\mathfrak{M} = \mathcal{J}(A)$ e dunque per la terza forma del lemma di Nakayama, $M = N$. □

Proposizione 1.15. *Sia $(A, \mathfrak{M})$ un anello locale e sia M un A-modulo finitamente generato. Allora ogni insieme di generatori minimale ha la stessa cardinalità.*

Dimostrazione. Sia $m_1, \dots, m_k$ un insieme di generatori minimale. Se per assurdo $\bar{m}_1, \dots, \bar{m}_k$ non fosse una base di ${}^{M}\!/_{\mathfrak{M}M}$, potremmo ricavare, per l'algoritmo di estrazione di una base per gli spazi vettoriali, una base come sottoinsieme di questi. Per il lemma, avremmo allora che un sottoinsieme di $m_1, \dots, m_k$ genererebbe ancora M, contro la minimalità. □

Per gli spazi vettoriali finitamente generati, sappiamo che ogni endomorfismo surgettivo o iniettivo è un isomorfismo. Nel caso dei moduli, ciò non è più vero; basta pensare a

$$\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & 1 & \longmapsto & 2 \end{array}$$

che è iniettivo ma non surgettivo. Vale però il seguente:

Proposizione 1.16. *Sia M un A-modulo finitamente generato e sia f un endomorfismo surgettivo. Allora f è un isomorfismo.*

Dimostrazione. Muniamo M della struttura di $A[x]$-modulo: dato $p = \sum a_i x^i \in A[x]$, definiamo $p \cdot m := \sum a_i f^i(m)$. In particolare, abbiamo allora $xm = f(m)$; cioè $xM = f(M) = M$. Per il lemma di Nakayama, esiste allora $q \in A[x]$ tale che $q \equiv 1\ (x)$ e $qM = 0$. Di conseguenza, esiste $h \in A[x]$ tale che $q = 1 + xh$. Mostriamo allora l'iniettività di f. Sia $m \in \mathrm{Ker}(f)$.

$$m = 1 \cdot m = qm - xhm = qm - hf(m) = 0$$

Abbiamo dimostrato allora che $\mathrm{Ker}(f) = \{0\}$ e dunque la tesi. □

1.3 Successioni esatte

Definizione 1.17. Sia $\{M_i\}$ una famiglia di A-moduli. Supponiamo che per ogni $i \in I$ sia definito un omomorfismo di A-moduli

$$\varphi_i\colon M_{i-1} \longrightarrow M_i$$

La successione

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

si dice esatta in M_i se $\mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i+1})$; si dice esatta se è esatta in ogni M_i.

Osservazione 1.18. $0 \to M \xrightarrow{f} N$ è esatta $\iff$ f è iniettiva.
$M \xrightarrow{f} N \longrightarrow 0$ è esatta $\iff$ f è surgettiva

Definiamo due semplici funtori. Dato $f \in \mathrm{Hom}(M, N)$ e $h \in \mathrm{Hom}(N, P)$, possiamo definire per composizione

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, dashed, "f^*(h)"'] & N \arrow[d, "h"] \\ & P \end{tikzcd}$$

la funzione $f^*(h)$. Risulta definito il seguente omomorfismo:

$$\begin{array}{rccc} f^*\colon & \mathrm{Hom}(N, P) & \longrightarrow & \mathrm{Hom}(M, P) \\ & h & \longmapsto & f^*(h) = h \circ f \end{array}$$

In modo simile, dato il diagramma

$$\begin{tikzcd} M \arrow[r, "f"] & N \\ & P \arrow[ul, "h"] \arrow[u, dashed, "f_*(h)"'] \end{tikzcd}$$

si ha il seguente omomorfismo:

$$\begin{array}{rccc} f_*\colon & \mathrm{Hom}(P, M) & \longrightarrow & \mathrm{Hom}(P, N) \\ & h & \longmapsto & f_*(h) = f \circ h \end{array}$$

Proposizione 1.19. *La successione*

$$M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0$$

è esatta se e solo se la successione

$$0 \to \mathrm{Hom}(M_2, N) \xrightarrow{g^*} \mathrm{Hom}(M, N) \xrightarrow{f^*} \mathrm{Hom}(M_1, N)$$

è esatta per ogni A-modulo N.

Dimostrazione. Supponiamo dapprima che la successione di partenza sia esatta.

- Mostriamo che g^* è iniettiva. Sia allora $h \in \mathrm{Hom}(M_2, N)$ e supponiamo che $g^*(h) = h \circ g = 0$. Per surgettività di g,

  $$\forall p \in M_2 \ \exists m \in M \ t.c. \ p = g(m)$$

  e dunque

  $$\forall p \in M_2 \ h(p) = h(g(m)) = 0$$

  e dunque $h = 0$. Di conseguenza, $\mathrm{Ker}(g^*) = \{0\}$.

- Mostriamo che $\mathrm{Im}(g^*) \subseteq \mathrm{Ker}(f^*)$. Sia $\varphi \in \mathrm{Im}(g^*)$. Per definizione, esiste allora η tale che $\varphi = g^*(\eta) = \eta \circ g$. Conseguentemente,

$$f^*(\varphi) = \varphi \circ f = \eta \circ g \circ f = 0$$

  per esattezza della successione.

- Mostriamo che $\mathrm{Ker}(f^*) \subseteq \mathrm{Im}(g^*)$. Sia allora $\eta \in \mathrm{Ker}(f^*)$, cioè $f \circ \eta = 0$. Dobbiamo allora definire $h \in \mathrm{Hom}(M_2, N)$ tale che $g^*(h) = h \circ g = \eta$. Sia $m_2 \in M_2$; esiste allora un elemento $m \in M$ tale che $m_2 = g(m)$ per surgettività di g. Definiamo allora $h(m_2) = \eta(m)$. Bisogna verificare ora che tale h sia ben definita; sappiamo per ipotesi che $\mathrm{Ker}(\eta) \supseteq \mathrm{Im}(f)$. Dunque, dati $m, n \in g^{-1}(m_2)$, si ha

$$g(m) - g(n) = g(m - n) = 0 \Rightarrow m - n \in \mathrm{Ker}(g) = \mathrm{Im}(f) \subseteq \mathrm{Ker}(\eta)$$

  da cui la buona definizione.

Mostriamo ora l'altra implicazione.

- Mostriamo che g è surgettiva. Consideriamo il diagramma:

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[d, dashed, "g^*(\pi)"'] & M_2 \arrow[dl, "\pi"] \\ M_2/\mathrm{Im}(g) & \end{tikzcd}$$

  Per costruzione, $g^*(\pi) = 0$. Per ipotesi, g^* è iniettiva, dunque $\pi = 0$ e dunque $M_2 = \mathrm{Im}(g)$

- Mostriamo che $\mathrm{Ker}(g) \supseteq \mathrm{Im}(f)$. Per esattezza della successione, $f^* \circ g^*(id_{M_2}) = 0$; da questo segue $g \circ f = 0$ e dunque $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$.

- Mostriamo che $\mathrm{Ker}(g) \subseteq \mathrm{Im}(f)$. Consideriamo il diagramma

$$\begin{tikzcd} M_1 \arrow[r, "f"] \arrow[d, dashed, "f^*(\pi)"'] & M \arrow[dl, "\pi"] \\ M/\mathrm{Im}(f) & \end{tikzcd}$$

  $f^*(\pi) = 0$ per costruzione e dunque $\pi \in \mathrm{Ker}(f^*) = \mathrm{Im}(g^*)$. Di conseguenza, esiste $h \in \mathrm{Hom}(M_2, M/\mathrm{Im}(f))$ tale che $g^*(h) = \pi$. Quindi

$$\mathrm{Im}(f) = \mathrm{Ker}(\pi) \supseteq \mathrm{Ker}(g)$$

$\square$

Proposizione 1.20. *La successione*

$$0 \to M_1 \xrightarrow{f} M \xrightarrow{g} M_2$$

è esatta se e solo se la successione

$$0 \to \mathrm{Hom}(N, M_1) \xrightarrow{f_*} \mathrm{Hom}(N, M) \xrightarrow{g_*} \mathrm{Hom}(N, M_2)$$

è esatta per ogni A-modulo N.

Dimostrazione. Supponiamo dapprima che la successione di partenza sia esatta.

- Mostriamo che f_* è iniettiva. Sia allora $h \in \mathrm{Hom}(N, M_2)$ e supponiamo che $f_*(h) = f \circ h = 0$. Per iniettività di f, $\mathrm{Im}(h) \subseteq \mathrm{Ker}(f) = \{0\}$ e dunque $h = 0$

- Mostriamo che $\mathrm{Im}(f_*) \subseteq \mathrm{Ker}(g_*)$. Sia $h \in \mathrm{Im}(f_*)$. Per definizione, esiste allora φ tale che $h = f \circ \varphi$. Conseguentemente,

  $$g_*(h) = g \circ h = g \circ f \circ \varphi = 0$$

  per esattezza della successione, e dunque il contenimento voluto.

- Mostriamo che $\mathrm{Im}(f_*) \supseteq \mathrm{Ker}(g_*)$. Sia allora $h \in \mathrm{Ker}(g_*)$, cioè $g \circ h = 0$. Dobbiamo allora definire $\varphi \in \mathrm{Hom}(N, M_1)$ tale che $f_*(\varphi) = h$. L'unico modo per far commutare il diagramma è definire $\varphi(n) = f^{-1}(h(n))$. Tale applicazione è ben definita perchè f è iniettiva e per ipotesi $\mathrm{Im}(h) \subseteq \mathrm{Ker}(g) = \mathrm{Im}(f)$

Mostriamo ora l'altra implicazione.

- Mostriamo che f è iniettiva. Consideriamo il diagramma:

  $$\begin{tikzcd} M_1 \arrow[r, "f"] & M \\ \mathrm{Ker}(f) \arrow[u, "i"] \arrow[ur, dashed, "f_*(i)"'] & \end{tikzcd}$$

  Per costruzione, $f_*(i) = 0$. Per ipotesi, f_* è iniettiva, dunque $i = 0$ e f è iniettiva.

- Mostriamo che $\mathrm{Ker}(g) \supseteq \mathrm{Im}(f)$. Per esattezza della successione, $f^* \circ g^*(id_{M_2}) = 0$; da questo segue $g \circ f = 0$ e dunque $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$.

- Mostriamo che $\mathrm{Ker}(g) \subseteq \mathrm{Im}(f)$. Consideriamo il diagramma

  $$\begin{tikzcd} M \arrow[r, "g"] & M_2 \\ \mathrm{Ker}(g) \arrow[u, "i"] \arrow[ur, dashed, "g_*(\pi)"'] & \end{tikzcd}$$

Per costruzione, $g_*(i) = 0$, cioè $i \in \mathrm{Ker}(g_*) = \mathrm{Im}(f_*)$. Dunque, esiste $h \in \mathrm{Hom}(\mathrm{Ker}(g), M_1)$ tale che $f_*(h) = f \circ h = i$. Di conseguenza,

$$\mathrm{Im}(f) \supseteq \mathrm{Ker}(g)$$

come voluto.

□

Definizione 1.21. Si dice che una successione esatta

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

spezza se esiste $f\colon M \oplus P \to N$ isomorfismo che fa commutare il seguente diagramma:

$$\begin{tikzcd}
 & & M \oplus P \arrow[dd, dashed, "f"] \arrow[dr, "\pi_P"] & & \\
0 \arrow[r] & M \arrow[ur, "i_M"] \arrow[r, "\alpha"'] & N \arrow[r, "\beta"'] & P \arrow[r] & 0
\end{tikzcd}$$

Proposizione 1.22. *Consideriamo una successione esatta:*

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

Sono equivalenti:

1. *La successione spezza*
2. *Esiste un omomorfismo $r\colon N \to M$ tale che $r \circ \alpha = id_M$*
3. *Esiste un omomorfismo $s\colon P \to N$ tale che $\beta \circ s = id_P$*

Dimostrazione.

(1) ⇒ (2) Mostriamo che definendo $r = \pi_M \circ f^{-1}$ otteniamo l'omomorfismo cercato.

$$r \circ \alpha = \pi_M \circ f^{-1} \circ \alpha = \pi_M \circ i_M = id_M$$

(1) ⇒ (3) Mostriamo che definendo $s = f \circ i_P$ otteniamo l'omomorfismo cercato.

$$\beta \circ s = \beta \circ f \circ i_P = \pi_P \circ i_P = id_P$$

(2) ⇒ (1) Per ogni elemento $n \in N$, consideriamo la scrittura

$$n = n - \alpha(r(n)) + \alpha(r(n))$$

Notiamo che $n - \alpha(r(n)) \in \mathrm{Ker}(r)$; infatti

$$r(n - \alpha(r(n))) = r(n) - r(\alpha(r(n))) = r(n) - r(n) = 0$$

Di conseguenza, $N \simeq \mathrm{Im}(\alpha) + \mathrm{Ker}(r)$. Mostriamo che tale somma è diretta. Sia $n \in \mathrm{Im}(\alpha) \cap \mathrm{Ker}(r)$. Allora esiste $m \in M$ tale che $\alpha(m) = n$. Quindi,

$$0 = r(n) = r(\alpha(m)) = m$$

e dunque $m = 0$; allora $n = 0$, come voluto. Poichè α è iniettiva, $\mathrm{Im}(\alpha) \simeq M$; per esattezza della successione, $\mathrm{Ker}(r) \simeq P$, dunque abbiamo ottenuto quanto desiderato.

(3) $\Rightarrow$ (1) Per ogni elemento $n \in N$, consideriamo la scrittura

$$n = n - s(\beta(n)) + s(\beta(n))$$

Notiamo che $n - s(\beta(n)) \in \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$; infatti

$$\beta(n - s(\beta(n))) = \beta(n) - \beta(s(\beta(n))) = \beta(n) - \beta(n) = 0$$

Di conseguenza, $N \simeq \mathrm{Im}(\alpha) + \mathrm{Im}(s)$. Mostriamo che tale somma è diretta. Sia $n \in \mathrm{Im}(\alpha) \cap \mathrm{Im}(s)$. Allora, esiste un $p \in P$ tale che $n = s(p)$. Poichè $n \in \mathrm{Ker}(\beta)$, si ha allora:

$$0 = \beta(n) = \beta(s(p)) = p$$

Poichè s è un omomorfismo, manda 0 in 0, dunque $n = 0$. Basta ora notare che $\mathrm{Im}(\alpha) \simeq M$ e $\mathrm{Im}(s) \simeq P$ perchè s è iniettiva.

$\square$

Concludiamo la sezione con un teorema di grande importanza, noto come *"Snake Lemma"*.

Teorema 1.23 (Lemma del serpente)**.** *Consideriamo due successioni esatte e degli omomorfismi α, β, γ che fanno commutare il seguente diagramma:*

$$\begin{tikzcd}
 & M \arrow[r, "f"] \arrow[d, "\alpha"'] & N \arrow[r, "g"] \arrow[d, "\beta"'] & P \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & M' \arrow[r, "f'"'] & N' \arrow[r, "g'"'] & P' &
\end{tikzcd}$$

Esiste allora una successione esatta come indicata tratteggiata nel seguente diagramma:

$$\begin{tikzcd}
 & \mathrm{Ker}(\alpha) \arrow[r, dashed, "\tilde{f}"] \arrow[d] & \mathrm{Ker}(\beta) \arrow[r, dashed, "\tilde{g}"] \arrow[d] & \mathrm{Ker}(\gamma) \arrow[d] \arrow[dddll, dashed, rounded corners] & \\
 & M \arrow[r, "f"] \arrow[d] & N \arrow[r, "g"] \arrow[d, "\partial"'] & P \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] \arrow[dd, dashed, rounded corners] & M' \arrow[r, "f'"'] \arrow[d] & N' \arrow[r, "g'"'] \arrow[d] & P' \arrow[d] & \\
 & \mathrm{Coker}(\alpha) \arrow[r, dashed, "\tilde{f}'"'] & \mathrm{Coker}(\beta) \arrow[r, dashed, "\tilde{g}'"'] & \mathrm{Coker}(\gamma) &
\end{tikzcd}$$

Dimostrazione. • L'unica idea sensata per definire $\tilde{f}$ è $\tilde{f} = f_{|_{\mathrm{Ker}(\alpha)}}$. Mostriamo che è ben definita. Sia $a \in \mathrm{Ker}(\alpha)$.

$$\alpha(a) = 0 \Rightarrow f'(\alpha(a)) = 0 \Rightarrow \beta(f(a)) = 0 \Rightarrow f(a) \in \mathrm{Ker}(\beta)$$

- Definiamo $\tilde{g} = g_{|_{\mathrm{Ker}(\beta)}}$. Mostriamo la buona definizione di tale mappa. Sia $b \in \mathrm{Ker}(\beta)$.

$$\beta(b) = 0 \Rightarrow g'(\beta(b)) = 0 \Rightarrow \gamma(g(b)) = 0 \Rightarrow g(b) \in \mathrm{Ker}(\gamma)$$

- Mostriamo che la mappa $\tilde{f})'$, che prendiamo come la mappa indotta da f' sui coker, è ben definita. Siano $a, a' \in M'$ tali che $a - a' \in \mathrm{Im}(\alpha)$. Esiste allora $m \in M$ tale che $\alpha(m) = a - a'$.

$$f'(\alpha(m)) = \beta(f(m)) \Rightarrow f'(\alpha(m)) \in \mathrm{Im}(\beta) \Rightarrow f'(a) - f'(a') \in \mathrm{Im}(\beta)$$

  come voluto.

- Mostriamo che $\tilde{g}'$, mappa indotta dal passaggio al coker da g', è ben definita. Siano $b, b' \in N'$ tali che $b - b' \in \mathrm{Im}(\beta)$. Allora esiste $n \in N$ tale che $\beta(n) = b - b'$.

$$g'(\beta(n)) = \gamma(g(n)) \Rightarrow g'(\beta(n)) \in \mathrm{Im}(\gamma) \Rightarrow g'(b) - g'(b') \in \mathrm{Im}(\gamma)$$

- Definiamo ora l'applicazione $\partial\colon \mathrm{Ker}(\gamma) \to \mathrm{Coker}(\alpha)$. Sia $p \in \mathrm{Ker}(\gamma)$. Per surgettività di g, esiste $n \in N$ tale che $g(n) = p$. Di conseguenza,

$$0 = \gamma(g(n)) = g'(\beta(n)) \Rightarrow \beta(n) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$$

  Per iniettività di f', esiste un'unica $a \in M'$ tale che $\beta(n) = f'(a)$. Definisco allora $\partial(p) = a + \mathrm{Im}(\alpha)$. Mostriamo la buona definizione: dimostriamo cioè che l'immagine di p tramite ∂ è indipendente dalla scelta di n. Siano n, n' tali che $g(n) = g(n') = p$. Dalla definizione, siano $a, a' \in M'$ tali che $f'(a) = \beta(n)$ e $f'(a') = \beta(n')$. Poiché $n - n' \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, esiste $x \in M$ tale che $f(x) = n - n'$. Notiamo ora che

$$f'(a - a') = \beta(n - n') = \beta(f(x)) = f'(\alpha(x))$$

  Per iniettività di f', $\alpha(x) = a - a'$ e dunque ∂ è ben definita, perché $a - a' \in \mathrm{Im}(\alpha)$.

Ora che abbiamo definito le mappe, mostriamo che la successione che abbiamo ottenuto è esatta.

- Dimostriamo che $\mathrm{Ker}(\tilde{g}) = \mathrm{Im}(\tilde{f})$. Intanto, $g \circ f = 0 \Rightarrow \tilde{g} \circ \tilde{f} = 0$ e dunque $\mathrm{Ker}(\tilde{g}) \supseteq \mathrm{Im}(\tilde{f})$. Sia ora $n \in \mathrm{Ker}(\beta)$ tale che $\tilde{g}(n) = 0$. Per esattezza della successione, esiste $m \in M$ tale che $f(m) = n$.

$$0 = \beta(f(m)) = f'(\alpha(m))$$

  e dunque $\alpha(m) = 0$ per iniettività di f'. Di conseguenza $m \in \mathrm{Ker}(\alpha)$ e $\mathrm{Ker}(\tilde{g}) \subseteq \mathrm{Im}(\tilde{f})$.

- Mostriamo che $\mathrm{Im}(\tilde{g}) = \mathrm{Ker}(\partial)$. Sia $n \in \mathrm{Ker}(\beta)$. Allora $\beta(n) = 0 = f'(0)$. Per definizione di ∂, abbiamo allora $\partial(g(n)) = 0 + \mathrm{Im}(\alpha)$ e dunque $\mathrm{Im}(\tilde{g}) \subseteq \mathrm{Ker}(\partial)$. Sia ora $p \in \mathrm{Ker}(\gamma)$ tale che $\partial(p) = 0$. Per surgettività di g, esiste $n \in N$ tale che $g(n) = p$.

$$g'(\beta(n)) = 0 \Rightarrow \beta(n) \in \mathrm{Ker}(g') = \mathrm{Im}(f') \Rightarrow \exists m \in M' \ t.c. \ f'(m) = \beta(n)$$

Poichè $p \in \mathrm{Ker}(\partial)$, $m \in \mathrm{Im}(\alpha)$, dunque $f'(m) = f'(\alpha(x))$. Notiamo ora che, per commutatività, $\beta(f(x)) = f'(\alpha(x)) = \beta(n)$ e quindi $n - f(x) \in \mathrm{Ker}(\beta)$. D'altronde,

$$\tilde{g}(n - f(x)) = g(n) - \underbrace{g(f(x))}_{=0} = p$$

e dunque $\mathrm{Ker}(\partial) \subseteq \mathrm{Im}(\tilde{g})$.

- Mostriamo ora che $\mathrm{Im}(\partial) = \mathrm{Ker}(\tilde{f'})$. Sia $x + \mathrm{Im}(\alpha) \in \mathrm{Im}(\partial)$, dunque esiste $y \in \mathrm{Ker}(\gamma)$ tale che $\partial(y) = x + \mathrm{Im}(\alpha)$. Per surgettività di g, esiste $n \in N$ tale che $g(n) = y$.

$$g'(\beta(n)) = \gamma(g(n)) = 0 \Rightarrow \beta(n) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$$

  Dunque $\beta(n) = f'(a)$ e $f'(a) \in \mathrm{Im}(\beta)$. Di conseguenza, $\partial(y) \in \mathrm{Ker}(\tilde{f'})$. Viceversa, sia $x + \mathrm{Im}(\alpha) \in \mathrm{Ker}(\tilde{f'})$. Allora $f'(x) \in \mathrm{Im}(\beta)$ e quindi esiste $n \in N$ tale che $\beta(n) = f'(x)$. Per costruzione allora $\partial(g(n)) = x + \mathrm{Im}(\alpha)$. Manca però da verificare che $g(n) \in \mathrm{Ker}(\gamma)$.

$$0 = g'(f'(x)) = g'(\beta(n)) = \gamma(g(n)) \Rightarrow g(n) \in \mathrm{Ker}(\gamma)$$

- Mostriamo ora che $\mathrm{Im}(\tilde{f'}) = \mathrm{Ker}(\tilde{g'})$. Sicuramente, poichè $g' \circ f' = 0$, si ha $\tilde{g'} \circ \tilde{f'} = 0$ e dunque $\mathrm{Im}(\tilde{f'}) \subseteq \mathrm{Ker}(\tilde{g'})$. Sia allora $x \in \mathrm{Ker}(\tilde{g'})$. Allora $g'(x) \in \mathrm{Im}(\gamma)$ e dunque esiste $p \in P$ tale che $\gamma(p) = g'(x)$. Per surgettività di g, esiste $n \in N$ tale che $g(n) = p$. Dunque,

$$g'(x) = \gamma(g(n)) = g'(\beta(n)) \Rightarrow x - \beta(n) \in \mathrm{Ker}(g') = \mathrm{Im}(f')$$

  Di conseguenza, esiste $a \in M'$ tale che $f'(a) = x - \beta(n)$ e dunque $\tilde{f'}(a + \mathrm{Im}(\alpha)) = x - \beta(n) + \mathrm{Im}(\beta) = x + \mathrm{Im}(\beta)$, come voluto.

□

Osservazione 1.24. Se f è iniettiva, allora anche $\tilde{f}$ è iniettiva perchè restrizione di una funzione iniettiva. Se g' è surgettiva, allora anche $\tilde{g'}$ è surgettiva, perchè non è altro che il passaggio al coker della mappa g.

Corollario 1.25 (Lemma dei Cinque)**.** *Consideriamo il diagramma*

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "\alpha"'] & N \arrow[r, "g"] \arrow[d, "\beta"'] & P' \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & M' \arrow[r, "f'"'] & N' \arrow[r, "g'"'] & P' \arrow[r] & 0
\end{tikzcd}$$

Se due dei tre omomorfismi α, β, γ sono isomorfismi, allora lo è anche il terzo.

Dimostrazione. Supponiamo che α, β siano isomorfismi, gli altri casi sono equivalenti. Per il lemma del serpente, otteniamo allora la successione:

$$0 \to \mathrm{Ker}(\alpha) = 0 \to \mathrm{Ker}(\beta) = 0 \to \mathrm{Ker}(\gamma) \to$$
$$\to \mathrm{Coker}(\alpha) = 0 \to \mathrm{Coker}(\beta) = 0 \to \mathrm{Coker}(\gamma) \to 0$$

Per esattezza della successione, $\mathrm{Ker}(\gamma) = 0$ (dunque γ è iniettiva) e $\mathrm{Coker}(\gamma) = 0$ (dunque γ è surgettiva), cioè γ è un isomorfismo. □

1.4 Moduli Proiettivi

Definizione 1.26. Un A-modulo P si dice proiettivo se per ogni $f\colon P \to N$ e $h\colon M \to N$ surgettiva esiste $\tilde{f}$ che fa commutare il seguente diagramma:

$$\begin{tikzcd} & P \arrow[dl, "\tilde{f}"'] \arrow[d, "f"] \\ M \arrow[r, "h"'] & N \end{tikzcd}$$

Lemma 1.27. *Sia P un modulo libero. Allora P è proiettivo.*

Dimostrazione. Consideriamo il diagramma

$$\begin{tikzcd} & P \arrow[d, "f"] \\ M \arrow[r, "h"'] & N \end{tikzcd}$$

dove h è surgettiva. Allora ha senso considerare il sottomodulo di M $h^{-1}(f(P))$ e prenderne un insieme di generatori $\{m_i \mid i \in I\}$. Definiamo allora $\tilde{f}(e_i) = m_i$ e tale $\tilde{f}$ è ben definita perchè P è libero e fa commutare il diagramma. $\square$

Proposizione 1.28. *Sono fatti equivalenti:*

1. *P proiettivo*
2. *Ogni successione esatta $0 \to M \to N \to P \to 0$ spezza*
3. *P è addendo diretto di un modulo libero*
4. *Il funtore $F\colon M \mapsto \mathrm{Hom}_A(P, M)$ è esatto, cioè manda successioni esatte corte in successioni esatte corte*

Dimostrazione.

(1) $\Rightarrow$ (2) Consideriamo una successione esatta

$$0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P \to 0$$

Mostriamo che esiste una sezione $s\colon P \to N$ tale che $\beta \circ s = id_P$. Poichè P è proiettivo, esiste la s che fa commutare il seguente diagramma:

$$\begin{tikzcd} & P \arrow[dl, "s"'] \arrow[d, "id"] \\ N \arrow[r, "\beta"'] & P \end{tikzcd}$$

e dunque la successione spezza, poichè per commutatività $\beta \circ s \simeq id_P$

(2) $\Rightarrow$ (3) Sicuramente P è quoziente di un modulo libero F. Abbiamo allora la successione esatta:

$$0 \to \mathrm{Ker}(\pi) \xrightarrow{i} F \xrightarrow{\pi} P \to 0$$

che per ipotesi spezza, dunque $F \simeq P \oplus \mathrm{Ker}(\pi)$, come voluto.

(3) $\Rightarrow$ (4) Consideriamo la successione esatta

$$0 \to N_1 \xrightarrow{f} M \xrightarrow{g} N_2 \to 0$$

Applicando il funtore, otteniamo la successione

$$0 \to \mathrm{Hom}_A(P, N_1) \xrightarrow{f_*} \mathrm{Hom}_A(P, M) \xrightarrow{g_*} \mathrm{Hom}_A(P, N_2)$$

Ci basta allora mostrare che g_* è surgettiva. Consideriamo il diagramma

$$\begin{tikzcd}
 & P \oplus M' \arrow[d, "\pi"] \arrow[dl, "\eta"'] \\
 & P \arrow[d, "\varphi"] \\
M \arrow[r, "g"'] & N_2
\end{tikzcd}$$

dove M' è un modulo tale che $M' \oplus P$ sia libero. L'omomorfismo η del diagramma esiste perchè $P \oplus M'$ è libero, quindi proiettivo. Sappiamo allora che $g \circ \eta = \varphi \circ \pi$. D'altronde, esiste l'immersione i di P in $P \oplus M'$. Consideriamo allora $s = \eta \circ i$. Verifichiamo che tale s faccia commutare il diagramma; questo darebbe la surgettività di g_*.

$$g \circ s = g \circ \eta \circ i = \varphi \circ \underbrace{\pi \circ i}_{id_P} = \varphi$$

e dunque la tesi.

(4) $\Rightarrow$ (1) Poichè g_* è surgettiva, comunque data $\varphi\colon P \to N$, esiste $s\colon P \to N_1$ tratteggiata che fa commutare il diagramma:

$$\begin{tikzcd}
 & P \arrow[d, "\varphi"] \arrow[dl, dashed, "s"'] \\
N_1 \arrow[r, "g"'] & N
\end{tikzcd}$$

e quindi la tesi.

□

Proposizione 1.29. *Sia $M = \oplus_{i \in I} M_i$. Allora M è proiettivo se e solo se M_i è proiettivo per ogni i.*

Dimostrazione. $\Rightarrow$ Poichè M è proiettivo, esiste un modulo P per il quale $P \oplus M = F$ dove F è libero. Di conseguenza, $\forall i$, $(P \oplus \sum_{j \neq i} M_j) \oplus M_i = F$, dunque M_i è proiettivo.

$\Leftarrow$ Poichè ogni M_i è proiettivo, esiste un modulo P_i tali che $M_i \oplus P_i$ sia libero. Detto $P = \oplus_i P_i$, si ha allora che $M \oplus P$ è libero, dunque M è proiettivo. □

Proposizione 1.30. *P è proiettivo se e solo se P è addendo diretto di ogni modulo di cui è quoziente.*

Dimostrazione. La successione

$$0 \to \mathrm{Ker}(\pi) \to M \to P \to 0$$

è esatta; poichè P è proiettivo spezza, dunque $M \simeq P \oplus \mathrm{Ker}(\pi)$. □

1.5 Forma normale di Smith

Si potrebbe pensare che, come nel caso degli spazi vettoriali, i sottomoduli di un modulo libero siano liberi. In realtà questo non è vero:

Esempio. Sia $A = K[x, y]$ e consideriamo il suo sottomodulo $N =< x, y >$. N non è libero; infatti $yx + (-x)y = 0$.

Nel caso l'anello sia un PID abbiamo però il seguente:

Teorema 1.31. *Sia A un PID, sia M un A-modulo libero finitamente generato e sia N un suo sottomodulo non banale. Allora N è libero.*

Dimostrazione. Mostriamo l'enunciato per induzione sul rango (la cardinalità di una base) di M. Se M è ciclico, $M \simeq A$, e dunque i suoi sottomoduli non nulli sono ideali di A. Poiché A è un PID, $N = (x)$. $x \neq 0$ e poichè A è un dominio, $ax = 0$ implica $a = 0$. Dunque N è libero. Supponiamo ora che M abbia rango $n + 1$ e assumiamo vera la tesi per tutti i moduli di rango minore o uguale a n. Sia $\{m_1, \cdots, m_{n+1}\}$ una base di M e definiamo $N_n = N \cap \langle m_1, \cdots, m_n \rangle$. Se $N_n = N$, per ipotesi induttiva N è libero. Supponiamo allora $N_n \neq N$. Dato $u \in N$, si ha

$$u = a_1 m_1 + \cdots a_n m_n + a_u m_{n+1}$$

Possiamo allora definire l'ideale $I = \{a_u \in A \mid u \in N\}$. Poichè A è un PID, $I = (d)$, cioè esiste $w \in N$ tale che $w = \alpha_1 m_1 + \cdots + d m_{n+1}$. Mostriamo allora che $N = N_n \oplus \langle w \rangle$.
Sia $p \in N$. Allora $a_p \in I$, e dunque $a_p = dk$. Di conseguenza, $p - kw \in N_n$, come volevasi dimostrare. □

Osservazione 1.32. Ripercorrendo la dimostrazione, si ottiene che necessariamente $\mathrm{rk}(N) \leq \mathrm{rk}(M)$.

Corollario 1.33. *Sia A un PID.*

1. *P proiettivo $\iff$ P libero*
2. *N sottomodulo di M, M finitamente generato $\Rightarrow$ N è finitamente generato.*

Dimostrazione.

1. Poichè P è proiettivo, P è addendo diretto di un modulo libero, dunque è isomorfo a un sottomodulo di un libero.

2. Poichè M è finitamente generato, esiste un omomorfismo surgettivo

$$A^n \xrightarrow{f} M \to 0$$

Dunque, $f^{-1}(N)$ è un sottomodulo di A^n, dunque è libero e finitamente generato. Di conseguenza, N è finitamente generato.

□

Sia ora M un A-modulo finitamente generato, con A un PID. Allora M è quoziente di un modulo libero finitamente generato:

$$0 \to \mathrm{Ker}(f) \xrightarrow{i} A^n \xrightarrow{f} M$$

$\mathrm{Ker}(f)$ è libero; sia allora $v_1, \cdots v_m$ una base di $\mathrm{Ker}(f)$. Considerata l'applicazione

$$\begin{array}{rccc} \psi\colon & A^m & \longrightarrow & A^n \\ & e_i & \longmapsto & v_i \end{array}$$

si ha allora che $\mathrm{Ker}(f) = \mathrm{Im}(\psi)$ e dunque $M \simeq \mathrm{Coker}(\psi)$. Ci siamo ridotti allora a studiare le applicazioni tra moduli liberi e i loro Coker per classificare i moduli finitamente generati su un PID. Fissate rispettivamente due basi $\mathcal{B}_1$ e $\mathcal{B}_2$ di A^m e A^m, si ha che un qualsiasi omomorfismo tra questi può essere rappresentato da una matrice, secondo la regola

$$M_{ij} = ([f(b_i)^{(m)}]_{\mathcal{B}^n})$$

Definizione 1.34. Siano $X, Y \in M(n, m, A)$. X e Y si dicono equivalenti se esistono due matrici $S \in GL(n, A)$ e $T \in GL(m, A)$ tali che $X = SYT$.

Proposizione 1.35. *Sia $X \in M(n, m, A)$, con A un PID. Allora X è equivalente a una matrice D in forma diagonale, cioè $d_{ij} = 0\ \forall i \neq j$.*

Dimostrazione. Mostriamo l'enunciato per una matrice $X \in M(2, A)$

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Poichè siamo in un PID, $(a, c) = (x)$; di conseguenza, esistono $s, t \in A$ tali che $as + ct = x$. Consideriamo allora la matrice:

$$M = \begin{pmatrix} s & t \\ -\frac{c}{x} & \frac{a}{x} \end{pmatrix}$$

M è invertibile perchè $\det M = 1$; inoltre

$$MX = \begin{pmatrix} x & * \\ 0 & * \end{pmatrix}$$

Lo stesso si ha poi nel caso generale agendo con matrici del tipo

$$\begin{pmatrix} M & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

Analogamente possiamo agire a destra per rendere la matrice X in forma triangolare inferiore. Mostriamo ora che con queste operazioni introdotte, e con permutazioni di righe, possiamo portare una matrice in forma diagonale. Supponiamo $x_{11} \neq 0$. Possiamo allora trovare delle matrici $S_1, \cdots S_{n-1}$ tali che la prima colonna di X sia tutta nulla eccetto il primo elemento, x_{11}. Allo stesso modo, si può fare per la prima riga; in questo modo si sporca però la prima colonna. Iterando questo procedimento si arriva però a termine; infatti, considerando a ogni passo il valore di x_{11}, si ha che questi creano una catena ascendente di ideali, perchè l'azione delle matrici sopra indicate porta sempre in posizione $(1,1)$ il generatore dell'ideale. Poichè siamo in un PID, una catena ascendente di ideali è stazionaria, e dunque il processo deve terminare. Arriviamo allora alla matrice

$$\begin{pmatrix} x_{11} & 0 \\ 0 & \tilde{X} \end{pmatrix}$$

e per ipotesi induttiva si ha la tesi, agendo sulla matrice $\tilde{X}$. □

Definizione 1.36. Una matrice D diagonale si dice in forma di Smith se $d_{11} \mid d_{22} \mid \cdots \mid d_{nn}$.

Proposizione 1.37. *Sia D una matrice in forma diagonale. Allora D è equivalente a una matrice $\tilde{D}$ in forma normale di Smith.*

Dimostrazione. Consideriamo una matrice in forma diagonale $D \in M(n, m, A)$

$$D = \begin{pmatrix} d_1 & & & 0 & \cdots & 0 \\ & \ddots & & \vdots & & \vdots \\ & & d_n & 0 & \cdots & 0 \end{pmatrix}$$

Sia i il minimo degli indici tali che $d_1 \nmid d_i$ e sia $a = (d_1, d_i)$. Di conseguenza, esistono $s, t \in A$ tali che $sd_1 + td_i = a$. A meno di permutazioni, possiamo supporre che $i = 2$. Consideriamo allora le matrici:

$$S = \begin{pmatrix} s & t & \\ \frac{-d_2}{a} & \frac{d_1}{a} & \\ & & I_{n-2} \end{pmatrix} \qquad T = \begin{pmatrix} 1 & -\frac{td_i}{a} & \\ 1 & \frac{sd_1}{a} & \\ & & I_{m-2} \end{pmatrix}$$

Il prodotto $X = SDT$ genera una matrice ancora in forma diagonale

$$X = \begin{pmatrix} a & & & & & 0 & \cdots & 0 \\ & \frac{d_1 d_2}{a} & & & & 0 & \cdots & 0 \\ & & d_3 & & & 0 & \cdots & 0 \\ & & & \ddots & & \vdots & & \vdots \\ & & & & d_n & 0 & \cdots & 0 \end{pmatrix}$$

in cui però $x_{11} \mid x_{22}$. Iterando il procedimento, otteniamo la tesi. □

Definizione 1.38. Data X una matrice, definiamo
$\Delta_i(X) = (\{\text{determinante dei minori } i \times i\})$

Proposizione 1.39. *Siano $X \in M(n, m, A)$ e $S \in GL(m, A)$. Allora $\Delta_i(X) = \Delta_i(SX)$ per ogni i.*

Dimostrazione. Sia $Y = SX$. Le righe di Y sono combinazioni lineari delle righe di X; per multilinearità del determinante, si ha allora che $\Delta_i(X) \supset \Delta_i(Y)$. D'altronde, S è invertibile, dunque come sopra $\Delta_i(S^{-1}Y) = \Delta_i(Y)$. Ma $S^{-1}Y = X$. quindi $\Delta_i(X) = \Delta_i(Y)$, come voluto. □

Corollario 1.40. *La forma di Smith è unica a meno di associati.*

Dimostrazione. Siano q_i gli elementi diagonali di X in forma di Smith, e siano d_i gli elementi diagonali di Y anch'essa in forma di Smith. Supponiamo che $X \sim Y$. Procediamo per induzione su i. Per $i = 1$, $(q_1) = \Delta_1(X) = \Delta_1(Y) = (d_1)$. Mostriamo il passo induttivo. Sviluppando i determinanti, otteniamo

$$\begin{aligned} \Delta_{i+1}(X) &= \Delta_i(X)(q_{i+1}) \\ \Delta_{i+1}(Y) &= \Delta_i(Y)(d_{i+1}) \end{aligned}$$

Di conseguenza, poichè $X \sim Y$,

$$\Delta_i(X)(q_{i+1}) = \Delta_i(Y)(d_{i+1})$$

Poichè A è un PID, $\Delta_i(X) = \Delta_i(Y) = (s)$ e quindi $(sd_{i+1}) = (sq_{i+1})$ e per cancellazione $(d_{i+1}) = (q_{i+1})$, come voluto. □

Da quanto mostrato fino ad ora, non possiamo ancora affermare di aver classificato i moduli finitamente generati su un PID; infatti, la forma di Smith dipende a priori dall'omomorfismo di A-moduli scelto. Mostriamo allora che in realtà la struttura trovata è indipendente dall'omomorfismo.

Lemma 1.41. *Supponiamo che M si scriva come somma diretta*

$$M = A/J_1 \oplus A/J_2$$

dove J_1, J_2 sono ideali di A. Sia I un ideale di A. Allora

$$M/IM \simeq A/J_1 + I \oplus A/J_2 + I$$

Dimostrazione. Per il secondo teorema di isomorfismo, IM si scrive come:

$$IM \simeq I(A/J_1 \oplus A/J_2) \simeq I + J_1/J_1 \oplus I + J_2/J_2$$

Dunque:

$$M/IM \simeq \left(A/J_1\right)\Big/\left(J_1 + I/J_1\right) \oplus \left(A/J_2\right)\Big/\left(J_2 + I/J_2\right) \simeq A/J_1 + I \oplus A/J_2 + I$$

□

Lemma 1.42. *Sia $M = A/J$ e sia $a \in A$. Allora $aM \simeq A/(J : a)$*

Dimostrazione. Consideriamo l'omomorfismo di A-moduli

$$\begin{array}{rccc} f\colon & A & \longrightarrow & aM \\ & a & \longmapsto & a(1+J) \end{array}$$

Chiaramente f è surgettiva; d'altronde $\mathrm{Ker}(f) = \{a \in A \mid am \in J\} = (J : a)$ e per il primo teorema di omomorfismo abbiamo la tesi. □

Lemma 1.43. *Sia B un anello e sia $f\colon B^n \to B^m$ un omomorfismo surgettivo, con $m > n \;\Rightarrow\; B = \{0\}$*

Dimostrazione. Abbiamo ovviamente la decomposizione $B^m = B^n \oplus B^{m-n}$. Consideriamo allora gli omomorfismi:

$$B^n \oplus B^{m-n} \xrightarrow{\pi} B^n \xrightarrow{f} B^m$$

$f \circ \pi$ è un endomorfismo surgettivo, dunque è anche iniettivo, ma allora $\mathrm{Ker}(\pi) = \{0\}$. Ma $\mathrm{Ker}(\pi) = B^{m-n}$, dunque la tesi. □

Teorema 1.44. *Sia A un anello. Supponiamo esistano due catene di ideali:*

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$$
$$J_1 \supseteq J_2 \supseteq \cdots \supseteq J_m$$

con $m > n$ e supponiamo che

$$M \simeq \bigoplus_{k=1}^{n} A/I_k \simeq \bigoplus_{k=1}^{m} A/J_k$$

Allora $J_1 = J_2 = \cdots = J_{m-n} = A$ e $\forall i = 1, \cdots n$ $J_{m-n+i} = I_i$.

Dimostrazione. Sia $B = A/J_1$. Mostriamo che $B = 0$. Notiamo subito che nelle ipotesi date, $J_1 + J_i = J_1$.

$$B^m \simeq \bigoplus_{i=1}^{m} A/J_1 \simeq \bigoplus_{i=1}^{m} A/(J_i + J_1) \simeq M/J_1M \simeq \bigoplus_{i=1}^{n} A/J_1 + I_i \twoheadleftarrow B^n$$

Di conseguenza, per il lemma, $B = 0$ e dunque $J_1 = A$. Possiamo iterare il ragionamento e quindi $J_1 = J_2 = \cdots = J_{m-n} = A$.
Per il secondo punto, possiamo supporre $m = n$. Per simmetria, basta mostrare che $I_k \subseteq J_k$ $\forall k$. Sia $a \in I_k$.

$$aM \simeq a\left(\bigoplus_{i=1}^{n} A/I_i\right) \simeq \bigoplus_{i=1}^{n} A/(I_i : a)$$

Poichè $I_k \supset I_{k-1}$, si ha che $a \in I_s$ $\forall s \leq k$ e dunque $(I_s : a) = A$. Di conseguenza,

$$aM \simeq \bigoplus_{i=k+1}^{n} A/(I_i : a)$$

D'altra parte,

$$aM \simeq a\left(\bigoplus_{i=1}^{n} A/J_i\right) \simeq \bigoplus_{i=1}^{n} A/(J_i : a)$$

Per il punto 1, si ha allora che $(J_s : a) = A$ $\forall s \leq k$ e dunque $a \in J_k$. □

Capitolo 2

Anelli di polinomi

2.1 Ideali monomiali

Definizione 2.1. Sia $I \subseteq \mathbb{K}[x_1, \cdots, x_n]$. I si dice monomiale se $\exists A \subseteq \mathbb{N}^n$ tale che $I = (x^\alpha \mid \alpha \in A)$.

Gli ideali monomiali sono i più semplici e godono di proprietà particolarmente vantaggiose, come la seguente:

Proposizione 2.2. *Sia I un ideale monomiale, $I = (x^\alpha \mid \alpha \in A \subseteq \mathbb{N}^n)$. Sia $f = \sum_\gamma c_\gamma x^\gamma$.*

$$f \in I \iff \forall \gamma \quad c_\gamma x^\gamma \in I$$

Dimostrazione. Chiaramente, se $c_\gamma \in I$ $\forall \gamma$, $f \in I$. Viceversa, supponiamo che $f \in I$. Allora f si scrive in termini dei generatori di I:

$$f = \sum_{\alpha \in A} p_\alpha x^\alpha = \sum_{\alpha \in A} (\sum_\beta g_\beta x^\beta) x^\alpha = \sum_{\alpha, \beta} a_{\alpha,\beta} x^{\alpha+\beta}$$

Per il principio di identità dei polinomi, i monomi devono coincidere termine a termine, e dunque ogni monomio di f appartiene a I, poichè $\forall \beta \; x^{\alpha+\beta} \in I$. $\square$

Dato un monomio, possiamo associargli un vettore $\alpha \in \mathbb{N}^n$ contenente i gradi nelle singole variabili. Studiare un ideale monomiale diventa allora equivalente a studiare particolari sottoinsiemi di $\mathbb{N}^n$:

Definizione 2.3. $A \subseteq \mathbb{N}^n$ si dice un E-sottoinsieme se $A \neq 0$ e se vale

$$x \in A \Longrightarrow \forall \gamma \in \mathbb{N}^n \; x + \gamma \in A$$

$F \subseteq A$ si dice una frontiera di A se

$$\forall a \in A \; \exists f \in F \; \exists \gamma \in \mathbb{N}^n \; t.c. \; a = f + \gamma$$

Lemma 2.4. *Sia A un E-sottoinsieme di $\mathbb{N}^n$ e sia $\pi \colon \mathbb{N}^n \to \mathbb{N}^{n-1}$ la proiezione su $n-1$ componenti. Allora $\pi(A)$ è un E-sottoinsieme di $\mathbb{N}^{n-1}$.*

Dimostrazione. Sia $\alpha \in A$. Dobbiamo mostrare che $\forall \gamma \in \mathbb{N}^{n-1}$ $\pi(\alpha) + \gamma \in \pi(A)$. Dato γ, per surgettività della proiezione, $\exists \tilde{\gamma} \in \mathbb{N}^n$ *t.c.* $\pi(\tilde{\gamma}) = \gamma$. Di conseguenza, $\gamma + \pi(\alpha) = \pi(\alpha + \tilde{\gamma})$, da cui la tesi. $\square$

Lemma (di Dickson). *Ogni E-sottoinsieme ammette una frontiera finita.*

Dimostrazione. Dobbiamo mostrare che dato A un E-sottoinsieme di $\mathbb{N}^n$, esiste una frontiera finita; affrontiamo la dimostrazione per induzione su n.
Nel caso n=1, A non è altro che una semiretta di $\mathbb{N}$; è sufficiente allora considerare $n_0 = \min A$ per ottenere una frontiera finita.
Supponiamo ora l'enunciato vero per ogni naturale minore o uguale a n, e mostriamo la tesi per n+1. Consideriamo la proiezione $\pi\colon \mathbb{N}^{n+1} \to \mathbb{N}^n$ sulle ultime n componenti. Per il lemma, $\pi(A)$ è un E-sottoinsieme di $\mathbb{N}^n$, dunque per ipotesi induttiva esiste $\tilde{F}_0$ frontiera finita di $\pi(A)$. Scegliamo allora delle controimmagini e chiamiamo $F_0 = \{a_{1,0}, \cdots a_{n_0,0}\}$ gli elementi scelti in questo modo, cioè $a_{i,0} = (a_{i,0}^{(1)}, \cdots a_{i,0}^{(n+1)}) \in A$. Abbiamo in questo modo preso una frontiera di 'quasi tutto' A; ci mancano solo una quantità finita di sezioni da coprire. Per questo, sia $\bar{a} = \max\{a_{i,0}^{(1)} \mid i \in \{1 \cdots n\}\}$ e consideriamo, $\forall a < \bar{a}$, il sottoinsieme $A_a = A \cap (\{a\} \times \mathbb{N}^n)$. Tali sezioni sono E-sottoinsiemi, dunque per ipotesi induttiva ammettono una frontiera finita $F_a = \{a_{1,a}, \cdots a_{n_a,a}\}$.
Verifichiamo allora che $F = F_0 \cup \bigcup_{a<\bar{a}} F_a$ si una frontiera finita di A. Sia $\alpha = (\alpha_1, \cdots, \alpha_{n+1}) \in A$. Distinguiamo due casi:

($\alpha_1 < \bar{a}$) In questo caso, $\exists a < \bar{a}$ *t.c.* $a = \alpha_1$. Ma allora, $\exists i \in \{1, \cdots, n_a\}$ *t.c.* $\alpha - a_{i,a} \geq 0$, come si voleva.

($\alpha_1 \geq \bar{a}$) Questa volta, considerata $\pi(\alpha)$ la proiezione, $\exists i \in \{1, \cdots, n_0\}$ *t.c.* $\pi(\alpha) - \tilde{a}_{i,0} \geq 0$. Passando alle controimmagini, allora, $\alpha - a_{i,0} \geq 0$ perché per ipotesi $a_{i,0}^{(1)} \leq \bar{a} \leq \alpha_1$.

Abbiamo allora trovato una frontiera finita di A, come richiesto.

□

Grazie a questo teorema, otteniamo il seguente

Corollario 2.5. *Ogni ideale monomiale è finitamente generato.*

Siamo ora interessati a caratterizzare in maniera più precisa le frontiere di un E-sottoinsieme; in particolare, siamo interessati a indagare sull'esistenza di frontiere minimali, che corrisponderebbero a un insieme di generatori non ridondanti di un ideale monomiale.

Proposizione 2.6. *Dato A un E-sottoinsieme, esiste un'unica frontiera di cardinalità minimale di A.*

Dimostrazione. Supponiamo per assurdo che esistano due frontiera di cardinalità minimale $F_1 = \{a_1 \cdots a_n\}$, $F_2 = \{b_1 \cdots b_n\}$. Abbiamo allora che

$$\forall i \in \{1, \cdots, n\}\ \exists j_i \text{ t.c. } a_i \in b_{j_i} + \mathbb{N}^n$$

Ciò definisce una applicazione $f\colon \{1, \cdots, n\} \to \{1, \cdots, n\}$. Tale applicazione è iniettiva per la supposta minimalità delle frontiere; se infatti non fosse iniettiva,

$$j_i = j_k \Rightarrow a_i \in b_{j_i} + \mathbb{N}^n \ \wedge\ a_k \in b_{j_i} + \mathbb{N}^n$$

e dunque sostituendo a a_j, a_k l'elemento b_{j_i} avremmo trovato una frontiera di cardinalità minore. Dunque, f è una permutazione; a meno di riordinare gli

elementi possiamo allora supporre che sia l'identità. Il procedimento attuato sopra può allora essere invertito, cioè

$$\forall i \in \{1, \cdots, n\} \ \exists j_i \ t.c. \ b_i \in a_{j_i} + \mathbb{N}^n$$

Otteniamo allora un'altra permutazione; se questa non fosse l'identità, avrei che

$$a_i \in b_i + \mathbb{N}^n \ \wedge \ b_i \in a_{j_i} + \mathbb{N}^n$$

e questo negherebbe ancora una volta la minimalità delle frontiere. Dunque, $F_1 = F_2$. □

Concludiamo la sezione con alcuni lemmi utili sugli ideali monomiali:

Proposizione 2.7. *Siano I, J ideali monomiali, $I = (m_1, \cdots, m_k)$. Allora:*

1. *$I \cap J$ è monomiale*
2. *Se $m_k = uv$, con $(u, v) = 1 \Rightarrow \ I = (I, u) \cap (I, v)$*

Dimostrazione.

1. Sia $f = \sum c_\alpha x^\alpha \in I \cap J$. Per quanto dimostrato, poichè $f \in I$ ogni monomio di f appartiene a I; poichè $f \in J$, ogni monomio di f sta in J. Di conseguenza ogni monomio di f sta in $I \cap J$, e dunque $I \cap J$ è monomiale (è generato da tutti i monomi dei polinomi che ci appartengono)
2. Chiaramente, $I \subseteq (I, u) \cap (I, v)$. Mostriamo l'altra inclusione. Sia $m \in (I, u) \cap (I, v)$ un monomio.

$$m \in (I, u) \iff m_i \mid m \ \vee \ u \mid m$$
$$m \in (I, v) \iff m_i \mid m \ \vee \ v \mid m$$

Se $m_i \mid m$, abbiamo finito. In caso contrario,

$$(u \mid m) \wedge (v \mid m) \Rightarrow uv \mid m \Rightarrow m \in I$$

□

Lemma 2.8. *Sia I un ideale tale che $\sqrt{I}$ è massimale. Allora I è primario.*

Dimostrazione. Ricordiamo che un ideale è primario se e solo se i divisori di 0 nel quoziente sono tutti nilpotenti.
Poichè $\sqrt{I} = \mathfrak{M}$ è massimale, $\mathfrak{M}$ è l'unico primo che contiene I. Allora, per corrispondenza, in A/I esiste un solo primo. Dunque tutti gli elementi non invertibili sono nilpotenti perchè sono contenuti nell'unico primo di A/I. Poichè questo vale in particolare per i divisori di 0, si ha la tesi. □

Proposizione 2.9. *Sia $I = (m_1, \cdots, m_k)$ un ideale monomiale con una base minimale.*

1. *I primo $\iff \forall i \ \exists x_{j_i}$ t.c. $m_i = x_{j_i}$*
2. *I radicale $\iff \forall i \ m_i = x_{i_1} \dots x_{i_k}$ con $i_k \neq i_h$ se $h \neq k$*
3. *I primario $\iff I = (x_{i_1}^{\alpha_1}, \dots, x_{i_k}^{\alpha_k}, m_1, \dots m_s)$ con $m_i \in \mathbb{K}[x_{i_1}, \dots, x_{i_k}]$*

Dimostrazione. 1. Se $I = (x_{i_1}, \dots, x_{i_k})$ è primo perchè il quoziente è un dominio. Viceversa, sia $m_i = x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \dots x_{i_h}^{\alpha_h}$ un generatore minimale di I, con I primo. Poichè I è primo, vale $x_{i_1} \in I$ oppure $x_{i_1}^{\alpha_1 - 1} x_{i_2}^{\alpha_2} \dots x_{i_h}^{\alpha_h} \in I$. Iterando, si ottiene che una variabile pura deve stare in I.

2. ($\Leftarrow$) Chiaramente $\sqrt{I} \supseteq I$. Mostriamo l'altra inclusione. Sia $f \in \sqrt{I} \Rightarrow f^k \in I$. Poichè I è monomiale, ogni monomio di f^k deve appartenere a I. In particolare, le potenze pure dei monomi di f devono stare in I. Allora

$$m^k \in I \Rightarrow \exists i \text{ t.c. } m_i \mid m^k \Rightarrow m_i \mid m \textit{ perchè } \deg m_i = 1$$

Di conseguenza, $m \in I$ e dunque $f \in I$.
($\Rightarrow$) $m_i = x_{i_h}^a n$, dove n dipende dalle altre variabili. Di conseguenza, $x_{i_h}^a n^a \in I = \sqrt{I}$, dunque $x_{i_h} n \in I$. di conseguenza, $a = 1$.

3. ($\Rightarrow$) Sia $m_i = x_h n$. Poichè la base è ridotta, possiamo supporre che $n \notin I$; di conseguenza, esiste $r \in \mathbb{N}$ tale che $x_i^r \in I$, dunque x_i^r sta nei generatori.
($\Leftarrow$) Supponiamo che le variabili in questione siano $x_1, \dots, x_k$. Consideriamo l'omomorfismo

$$f \colon \mathbb{K}[x_1, \dots, x_n] \longrightarrow \mathbb{K}(x_{k+1}, \dots, x_n)[x_1, \dots, x_k]$$

Notiamo che $\sqrt{I^e}$ è massimale, dunque I^e è primario. Di conseguenza, I^{ec} è primario. Basta ora notare che $I^{ec} = I$.

□

2.2 Algoritmo di divisione e basi di Gröbner

Siamo ora interessati ad approfondire la conoscenza degli ideali negli anelli di polinomi; la generalizzazione della teoria svolta per gli ideali monomiali è però non semplice. Abbiamo infatti visto che decidere l'appartenenza di un polinomio ad un ideale monomiale è facile; lo stesso non si può dire in generale. Per prima cosa, abbiamo necessità allora di estendere al caso in più variabili l'algoritmo di divisione euclidea; in particolare, è allora necessario scegliere un criterio per determinare un ordinamento dei monomi dei polinomi.

Definizione 2.10. Un ordinamento monomiale è una relazione d'ordine su $\mathbb{N}^n$ che rispetta le seguenti proprietà:

- è un buon ordine
- $\forall \alpha, \beta, \gamma \in \mathbb{N}^n \ \alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma$

Per facilità di verifica, ricordiamo il seguente lemma di teoria degli insiemi:

Lemma 2.11. $(\mathbb{N}^n, \leq)$ *è un buon ordine* $\iff$ *ogni catena discendente è stazionaria.*

Tra gli ordinamenti più utilizzati, vi sono i seguenti:

1. Ordinamento lessicografico:

$$\alpha \geq \beta \Rightarrow \textit{il primo termine non nullo di } \alpha - \beta \textit{ è maggiore di 0}$$

2. Ordinamento totale lex: detto $|\alpha| = \alpha_1 + \cdots + \alpha_n$,

$$\alpha \geq \beta \Rightarrow |\alpha| \geq |\beta| \ \vee \ \alpha \geq \beta \textit{ per l'ordinamento lessicografico}$$

3. Ordinamento reverse lex: detto $|\alpha| = \alpha_1 + \cdots + \alpha_n$,

$$\alpha \geq \beta \Rightarrow |\alpha| \geq |\beta| \ \vee \ |\alpha| = |\beta| \textit{ e l'ultimo termine non 0 in } \alpha - \beta \textit{ è } < \textit{ di 0}$$

Diamo ora delle notazioni comode per trattare i polinomi in più variabili:

Definizione 2.12. Sia $f \in \mathbb{K}[x_1 \cdots, x_n]$, $f = \sum_\alpha c_\alpha x^\alpha$, dove $c_\alpha \in \mathbb{K}$. Fissato un ordinamento monomiale, definiamo:

- Il multigrado di un polinomio è $\deg(f) := \max\{\alpha \mid c_\alpha \neq 0\}$
- Il coefficiente direttore è $lc(f) = c_\alpha$, dove $\alpha = \deg(f)$
- Il termine di testa è $lt(f) = c_\alpha x^\alpha$, dove $\alpha = \deg(f)$
- Il monomio di testa è $lm(f) = x^\alpha$ dove $\alpha = \deg(f)$

Possiamo ora illustrare l'algoritmo di divisione:

Teorema 2.13. *Consideriamo $R = \mathbb{K}[x_1, \cdots, x_n]$ con un fissato ordinamento monomiale, siano $p, f_1 \cdots, f_k \in R$. $\Rightarrow \exists a_1 \cdots a_k \in R \ \exists r \in R$ t.c*

$$p = \sum_{i=1}^{k} a_i f_i + r$$

dove

- $\forall i \ \deg(p) \geq \deg(a_i f_i)$
- $r = 0 \ \vee \ r = \sum r_\alpha x^\alpha$ *in modo tale che* $\forall \alpha \ x^\alpha \notin (lt(f_1) \cdots lt(f_k))$

Dimostrazione.

```
p ← f
r ← 0
a_i ← 0 ∀i
while p ≠ 0 do
    i ← 1
    diviso ← false
    while i ≤ k & diviso == false do
        if lt(f_i) | lt(p) then
            c_i ← lt(p)/lt(f_i)
            p ← p − c_i f_i
            diviso ← true
            a_i ← a_i + c_i
        else
            i++
        end if
    end while
    if diviso == false then
```

$r \leftarrow r + lt(p)$
$p \leftarrow p - lt(p)$
end if
end while

Mostriamo che l'algoritmo illustrato nello pseudocodice è effettivamente corretto e termina. Dimostriamo che ad ogni passo vale che $f = a_1 f_1 + \cdots + a_k f_k + p + r$. Sicuramente questo è vero in fase di input. Supponiamo che sia vero al passo $n-1$-esimo. Ci sono 2 casi possibili:

- Se $lt(f_i) \mid lt(p)$, vale che

$$a_i f_i + p = (a_i + \frac{lt(p)}{lt(f_i)}) f_i + p - \frac{lt(p)}{lt(f_i)} f_i$$

  e dunque $a_i f_i + p$ rimane invariato, dunque la relazione continua a valere

- Se invece si aggiorna il resto, vale invece

$$p + r = (r + lt(p)) + (p - lt(p))$$

Mostriamo ora la terminazione dell'algoritmo. Per questo, basta mostrare che il grado di p cala ad ogni iterazione; ciò è vero perchè ad ogni passo si ammazza il termine di testa di p. Mostriamo ora la condizione sul grado di $a_i f_i$. Ogni a_i è somma di termini $\frac{lt(p)}{lt(f_i)}$, inoltre $lt(p) < lt(f)$ e dunque $\deg(a_i f_i) \leq \deg(f)$, come voluto. □

Purtroppo l'algoritmo di divisione così enunciato non garantisce l'unicità del resto; è necessario allora trovare delle proprietà degli f_i che rendano efficace l'algoritmo. Dato un ideale I, possiamo associargli l'ideale $lt(I) = (\{lt(f) \mid f \in I\})$. Per definizione, $lt(I)$ è monomiale, dunque possiamo trovare un insieme di generatori finito. Di conseguenza, esistono dei polinomi $g_1, \cdots g_k$ tali che $(lt(g_1), \cdots, lt(g_k)) = lt(I)$.

Teorema 2.14. *Sia I un ideale di $\mathbb{K}[x_1, \cdots, x_n]$ e siano $g_1, \cdots g_k \in I$ tali che $lt(I) = (lt(g_1), \ldots, lt(g_k))$. Allora:*

- $I = (g_1, \cdots, g_k)$
- $f \in I \iff$ *il resto della divisione di f per $\{g_i \mid i \in \{1 \cdots k\}\}$ è 0*

Dimostrazione. Chiaramente, poichè $g_i \in I \ \forall i = 1 \cdots k$, $(g_1, \cdots, g_k) \subseteq I$. Sia allora $f \in I$. Per l'algoritmo di divisione,

$$f = \sum_{i=1}^{k} a_i g_i + r$$

Necessariamente $r \in I$. Se $r \neq 0$, allora $lt(r) \in lt(I) = (lt(g_1), \cdots, lt(g_k))$; ma questo è assurdo per l'algoritmo di divisione, perchè $\deg(r) < \deg g_i \ \forall i$. Di conseguenza $r = 0$ e $I = (g_1, \cdots, g_k)$. □

Corollario 2.15. *Ogni ideale di $\mathbb{K}[x_1, \cdots, x_n]$ è finitamente generato.*

Definizione 2.16. $(g_1, \cdots, g_k)$ si dice una base di Gröbner di I se $g_i \in I \ \forall i$ e $lt(I) = (lt(g_1), \cdots, lt(g_k))$.

Per indicare il resto della divisione di un polinomio f per una base di Gröbner G scriveremo d'ora in poi $\overline{f}^G$. Siamo così riusciti a utilizzare quanto sappiamo sugli ideali monomiali nello studio di un ideale qualunque. Quello che manca però in questa definizione è l'unicità di una base di Gröbner; aggiungiamo allora delle richieste sui polinomi in modo da trovare l'unicità dei generatori.

Definizione 2.17. Una base di Gröbner $(g_1, \cdots, g_k)$ si dice ridotta se

- $(lt(g_1), \cdots, lt(g_k))$ è la frontiera di cardinalità minimale di $lt(I)$
- $\forall i = 1, \cdots, k \; lc(g_i) = 1$
- $\forall i = 1, \cdots k \; \overline{g_i}^{G-\{g_i\}} = g_i$

Se valgono solo le prime due condizioni, la base di Gröbner si dice invece minimale.

Teorema 2.18. *Sia I un ideale di $\mathbb{K}[x_1, \cdots, x_n]$. Allora I ammette un'unica base di Gröbner ridotta.*

Dimostrazione. Siano $G = \{g_1, \cdots, g_k\}$ e $\tilde{G} = \{\tilde{g}_1, \cdots, \tilde{g}_k\}$. A meno di permutare gli elementi, possiamo supporre che $lt(g_i) = lt(\tilde{g}_i)$ $\forall i$. Fissato i, siano $g_i = \sum c_\alpha x^\alpha$ e $\tilde{g}_i = \sum d_\alpha x^\alpha$. Consideriamo allora il polinomio $g_i - \tilde{g}_i = \sum (c_\alpha - d_\alpha) x^\alpha$. Chiaramente $\deg(g_i - \tilde{g}_i) < deg(g_i) = deg(\tilde{g}_i)$. I monomi di $g_i - \tilde{g}_i$ derivano però o da monomi di g_i o da monomi di $\tilde{g}_i$; per ipotesi, poichè le basi son ridotte, questi monomi non appartengono all'ideale generato da $lt(G \setminus \{g_i\}) = lt(\tilde{G} \setminus \{\tilde{g}_i\})$ e dunque nell'algoritmo di divisione $\overline{g_i - \tilde{g}_i}^G = \overline{g_i - \tilde{g}_i}^{\tilde{G}} = g_i - \tilde{g}_i$. Poichè G e $\tilde{G}$ sono basi di Gröbner di I e il resto per la divisione deve stare in I, si ha $g_i - \tilde{g}_i = 0$.

□

Diamo ora un algoritmo per il calcolo di una base di Gröbner.

Definizione 2.19. Siano f, g polinomi di $\mathbb{K}[x_1, \cdots x_n]$, siano $\alpha = \deg f$ e $\beta = \deg g$. Detto $\gamma \in \mathbb{N}^n$ il vettore di componenti $\gamma_i = \max(\alpha_i, \beta_i)$, definiamo l'S-polinomio tra f e g come:

$$S(f, g) = \frac{x^\gamma}{lt(f)} f - \frac{x^\gamma}{lt(g)} g$$

Vale il seguente teorema, che enunciamo senza dimostrazione:

Teorema 2.20. *Sia $I = (g_1, \cdots, g_k)$ un ideale di $\mathbb{K}[x_1, \cdots, x_n]$.*

$$\{g_1, \cdots, g_k\} \text{ è una base di Gröbner} \iff \forall i = 1, \cdots, k \; \forall j \neq i \; \overline{S(g_i, g_j)}^G = 0$$

L'idea è allora quella di calcolare gli S-polinomi di un insieme di generatori e aggiungerli fino a quando tutti gli S-polinomi non vengono ridotti a 0. Diamo ora lo pseudocodice di questo algoritmo, detto Algoritmo di Buckberger:

$F \leftarrow \{f_1, \cdots, f_k\}$
$G \leftarrow F$
$G' \leftarrow \emptyset$
while $G \neq G'$ **do**

```
    G' ← G
    for i = 1; i ≤ #G; i++ do
        for j = 1; j ≤ #G; j++ do
            s ← S(f_i, f_j)^{G'}
            if s ≠ 0 then
                G ← G ∪ {s}
            end if
        end for
    end for
end while
```

Lemma 2.21. *Ogni catena ascendente di ideali di $\mathbb{K}[x_1, \cdots, x_n]$ è stazionaria.*

Dimostrazione. Consideriamo una catena di ideali:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

Consideriamo l'ideale $I = \bigcup_{i \in \mathbb{N}} I_i$. Per quanto dimostrato, I è finitamente generato, dunque $I = (f_1, \cdots, f_k)$. Poichè i generatori sono in numero finito, esiste $n \in \mathbb{N}$ tale che $f_i \in I_n$ $\forall i$. Dunque,

$$I = (f_1, \cdots, f_k) \subseteq I_n \subseteq I$$

da cui l'uguaglianza cercata. □

Proposizione 2.22. *L'algoritmo di Buckberger termina ed è corretto.*

Dimostrazione. Sicuramente l'algoritmo è corretto, perchè la condizione di terminazione è che $\overline{S(f_i, f_j)}^G = 0$ e questo, per il teorema precedentemente enunciato, garantisce che l'output sia effettivamente una base di Gröbner. D'altronde, se l'algoritmo non terminasse, la catena degli ideali $lt(G)$ ad ogni passo dell'algoritmo non sarebbe stazionaria, contro il lemma precedente. □

Definizione 2.23. Sia I un ideale di $\mathbb{K}[x_1, \cdots, x_n]$. Definiamo il k-esimo ideale di eliminazione come $I_k := I \cap \mathbb{K}[x_{k+1}, \cdots, x_n]$.

Teorema 2.24. *Sia G una base di Gröbner di un ideale I rispetto all'ordinamento lessicografico $x_1 > x_2 > \cdots > x_n$. Sia $G_k = G \cap \mathbb{K}[x_{k+1}, \cdots, x_n]$. Allora G_k è una base di Gröbner di I_k.*

Dimostrazione. Mostriamo l'enunciato nel caso di $k = 1$; induttivamente si ha la tesi per k generico. Sia $G = \{g_1, \cdots, g_l\}$ e supponiamo senza perdita di generalità che $G_1 = \{g_1, \cdots g_s\}$ con $s < n$. Chiaramente $(G_1) \subseteq I_1$, perchè $\forall i$ $g_i \in I$. Mostriamo allora l'altro contenimento. Sia $f \in I_1$. Per l'algoritmo di divisione,

$$f = \sum_{i=1}^{s} a_i g_i + \sum_{i=s+1}^{n} a_i g_i$$

con resto 0 perchè in particolare $f \in I$. Sappiamo però che $\deg f \geq \deg a_i g_i$; poichè $\forall i \geq s+1$ g_i contiene un monomio di grado non nullo in x_1, si ha che questa disuguaglianza è verificata se e solo se $a_i = 0$ $\forall i \geq s+1$. Abbiamo allora

$$f = \sum_{i=1}^{s} a_i g_i$$

e dunque G_1 genera I_1. G_1 è anche una base di Gröbner, perchè con la stessa dimostrazione si vede che il resto nella divisione di un polinomio per G_1 è sempre 0, e questo vale in particolare per gli S-polinomi. □

2.3 Risultante

Definizione 2.25. Sia R un dominio di integrità e siano $f, g \in R[x]$.

$$f = a_n x^n + \cdots + a_0$$
$$g = b_m x^m + \cdots + b_0$$

Definiamo la matrice di Sylvester come:

$$Syl(f,g) = \begin{pmatrix} a_n & \cdots & a_0 & & & \\ & \ddots & & & \ddots & \\ & & a_n & & \cdots & a_0 \\ b_m & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \\ & & b_m & & \cdots & b_0 \end{pmatrix}$$

Definiamo il risultante di f, g come $\mathrm{Ris}(f,g) = \det(Syl(f,g))$.

Proposizione 2.26. *Siano $f, g \in R[x]$ e $a, b \in R$. Allora:*

1. $\mathrm{Ris}(f,g) = (-1)^{mn}\,\mathrm{Ris}(g,f)$
2. $\mathrm{Ris}(af,g) = a^m\,\mathrm{Ris}(f,g)$ *e* $\mathrm{Ris}(f,ag) = a^n\,\mathrm{Ris}(f,g)$

Dimostrazione. I risultati discendono dalle proprietà di multilinearità del determinante. □

Sia ora $y = (y_1, \cdots y_m)$ e sia

$$f_m(x,y) := \prod_{i=1}^{m}(x - y_i) = \sum_{i=0}^{m} a_i^{(m)} x^i$$

I coefficienti di f_m sono le funzioni simmetriche nelle variabili $y_1, \cdots y_m$.

$$a_m^{(m)} = 1$$
$$a_{m-1}^{(m)} = -(y_1 + \cdots + y_m)$$
$$a_{m-2}^{(m)} = y_1 y_2 + \cdots + y_{m-1} y_m$$
$$\vdots$$
$$a_0^{(m)} = (-1)^m y_1 y_2 \cdots y_m$$

Notiamo che sono funzioni lineari di ogni y_i; inoltre, $f_m(x,y) = f_{m-1}(x,y)(x - y_m)$ e dunque

$$a_{i-1}^{(m-1)}(y_1, \cdots, y_{m-1}) - y_m a_i^{(m-1)}(y_1, \cdots, y_{m-1}) = a_i^{(m)}(y_1, \cdots, y_{m-1}, y_m)$$

Valutando per $y_m = 0$, si ottiene:

$$a_{i-1}^{(m-1)}(y_1, \cdots, y_{m-1}) = a_i^{(m)}(y_1, \cdots, y_{m-1}, 0)$$

Dimostriamo ora il teorema fondamentale sul risultante, che lo caratterizza fortemente in termini delle radici dei polinomi.

Teorema 2.27. *Sia R un dominio, $g \in R[x]$ un polinomio di grado $n > 0$.*

$$\Rightarrow \mathrm{Ris}_x(f_m(x,y), g(x)) = g(y_m)\,\mathrm{Ris}_x(f_{m-1}(x,y), g(x))$$

Dimostrazione. Sia $g = b_n x^n + \cdots + b_0$. La matrice di Sylvester in questo caso è:

$$Syl(f_m, g) = \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & \\ & \ddots & & & \ddots & \\ & & a_m^{(m)} & & \cdots & a_0^{(m)} \\ b_n & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \\ & & b_n & & \cdots & b_0 \end{pmatrix}$$

Le operazioni elementari su righe e colonne non influenzano il valore del determinante, poiché hanno determinante 1. Possiamo allora sommare all'ultima colonna il valore $y_m^{m+n-i} C_i$ $\forall i$, dove C_i è l'i-esima colonna di $Syl(f_m, g)$. Otteniamo allora:

$$\mathrm{Ris}(f_m, g) = \det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & y_m^{n-1} f_m(y_m) \\ & \ddots & & & \ddots & \vdots \\ & & a_m^{(m)} & & \cdots & f_m(y_m) \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} g(y_m) \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & g(y_m) \end{pmatrix}$$

Per costruzione, $f_m(y_m) = 0$, dunque

$$\mathrm{Ris}(f_m, g) = det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & 0 \\ & \ddots & & & \ddots & \vdots \\ & & a_m^{(m)} & & \cdots & 0 \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} g(y_m) \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & g(y_m) \end{pmatrix}$$

Procediamo ora al calcolo del risultante; per multilinearità del determinante, possiamo raccogliere dall'ultima colonna la costante $g(y_m)$:

$$\mathrm{Ris}(f_m, g) = g(y_m) \det \begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & 0 \\ & \ddots & & & \ddots & \vdots \\ & & a_m^{(m)} & & \cdots & 0 \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & 1 \end{pmatrix}$$

Osserviamo che $\deg_{y_m} \operatorname{Ris}(f_m, g) = \deg_{y_m} g(y_m) = n$ e R è un dominio. Di conseguenza, per additività del grado, il grado in y_m del determinante deve essere 0. Dunque possiamo valutare y_m in 0 senza influire sul valore del determinante; ricordando la relazione sui coefficienti, allora,

$$\begin{pmatrix} a_m^{(m)} & \cdots & a_0^{(m)} & & & 0 \\ & \ddots & & & \ddots & \vdots \\ & & a_m^{(m)} & & \cdots & 0 \\ b_n & \cdots & b_1 & b_0 & & y_m^{m-1} \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & 1 \end{pmatrix} \sim \begin{pmatrix} a_{m-1}^{(m-1)} & \cdots & a_0^{(m-1)} & & & 0 \\ & \ddots & & & \ddots & \vdots \\ & & a_{m-1}^{(m-1)} & & \cdots & 0 \\ b_n & \cdots & b_1 & b_0 & & \vdots \\ & \ddots & & & \ddots & 0 \\ & & b_n & & \cdots & 1 \end{pmatrix}$$

Dunque, il determinante della matrice è proprio $\operatorname{Ris}(f_{m-1}, g)$ e dunque siamo arrivati alla relazione cercata. □

Nonostante questo teorema possa sembrare a prima vista di scarsa utilità, i corollari sono in realtà notevolissimi.

Corollario 2.28.

(1) Siano $f, g \in \mathbb{K}[x]$.

$$\operatorname{Ris}(f, g) = 0 \iff \exists \alpha \in \overline{\mathbb{K}} \text{ t.c. } f(\alpha) = g(\alpha) = 0$$

(2) Siano $f, g \in R[x]$, sia a_m il coefficiente direttore di f e siano z_i le radici di f.

$$\operatorname{Ris}(f, g) = a_m^n \prod g(z_i)$$

Corollario 2.29. *Sia R un dominio, $f, h, g, h_1, h_2 \in R[x]$.*

(1) $\operatorname{Ris}(f, h_1 h_2) = \operatorname{Ris}(f, h_1) \operatorname{Ris}(f, h_2)$

(2) $\operatorname{Ris}(f, hf + p) = a_n^{N - \deg p} \operatorname{Ris}(f, p)$, *dove* $N = \deg hf$

Dimostrazione.

(1) Sia a_n il coefficiente di testa di f e siano z_i le sue radici. Sia $m = \deg h_1 + \deg h_2$.

$$\operatorname{Ris}(f, h_1 h_2) = a_n^m \prod_{i=1}^{n} h_1(z_i) h_2(z_i) =$$

$$= \left(a_n^{\deg h_1} \prod_{i=1}^{n} h_1(z_i) \right) \left(a_n^{\deg h_2} \prod_{i=1}^{n} h_2(z_i) \right) = \operatorname{Ris}(f, h_1) \operatorname{Ris}(f, h_2)$$

(2)

$$\operatorname{Ris}(f, hf + p) = a_m^N \prod_{i=1}^{n} (hf + p)(\alpha_i) = a_m^N \prod_{i=1}^{n} p(\alpha_i) = a_m^{N - deg(p)} \operatorname{Ris}(f, p)$$

□

Proposizione 2.30. *Siano* $f, g \in R[x]$

$$\Rightarrow \mathrm{Ris}(f,g) = Af + Bg, \textit{ dove } \deg A < \deg g \textit{ e } \deg B < \deg f$$

Dimostrazione. Come nella dimostrazione del teorema sopra, possiamo agire sulla matrice di Sylvester con trasformazioni elementari, arrivando alla matrice:

$$\begin{pmatrix} a_m & \cdots & a_0 & & & x^{n-1}f(x) \\ & \ddots & & & \ddots & \vdots \\ & & a_m & & \cdots & f(x) \\ b_n & \cdots & b_1 & b_0 & & x^{m-1}g(x) \\ & \ddots & & & \ddots & \vdots \\ & & b_n & & \cdots & g(x) \end{pmatrix}$$

Per ottenere la tesi, basta allora svulippare il determinante rispetto all'ultima colonna e notare che f risulta moltiplicato per un polinomio di grado al più $n-1$, mentre g ha un fattore di grado al più $m-1$ a moltiplicarlo.

□

Concludiamo questa sezione con un lemma, fondamentale nelle prossime dimostrazioni:

Lemma 2.31. *Sia* $\varphi\colon R[x] \to R[x]$ *un omomorfismo di R-moduli e siano* $f, g \in R[x]$ *due polinomi tali che* $\deg(f) = \deg(\varphi f)$ *e* $\deg(g) = \deg(\varphi g)$.

$$\Longrightarrow \varphi(\mathrm{Ris}(f,g)) = \mathrm{Ris}(\varphi f, \varphi g)$$

Dimostrazione. Mostriamo la tesi per induzione sulla taglia della matrice del risultante. Se n=2,

$$\varphi\left(det\begin{pmatrix} a_1 & a_0 \\ b_1 & b_0 \end{pmatrix}\right) = \varphi(a_1b_0 - a_0b_1)$$

Al contrario,

$$det\begin{pmatrix} \varphi(a_1) & \varphi(a_0) \\ \varphi(b_1) & \varphi(b_0) \end{pmatrix} = \varphi(a_1)\varphi(b_0) - \varphi(a_0)\varphi(b_1)$$

e dunque abbiamo provato l'enunciato per n=2, poichè φ è un omomorfismo. Supponiamo ora la tesi vera per matrici di ordine n-1, e mostriamo che vale anche per matrici di ordine n. Il passo induttivo è però banale: è sufficiente infatti sviluppare mediante il metodo di Laplace rispetto alla prima colonna. Chiamando A, B i complementi algebrici:

$$\varphi(\mathrm{Ris}(f,g)) = \varphi(a_n det(A) \pm b_m det(B)) =$$
$$\varphi(a_n)\varphi(det(A)) \pm \varphi(b_m)\varphi(det(B)) = \varphi(a_n)det(\varphi(A)) \pm \varphi(b_m)det(\varphi(B)) =$$
$$\mathrm{Ris}(\varphi(f), \varphi(g))$$

e dunque la tesi. □

Capitolo 3

Varietà algebriche

3.1 Definizioni e prime proprietà

Definizione 3.1. Sia $I \subseteq \mathbb{K}[x_1, \dots x_n]$ un ideale; definiamo la varietà affine di I

$$\mathcal{V}(I) = \{\alpha \in \mathbb{K}^n \mid f(\alpha) = 0 \ \forall f \in I\}$$

Data una varietà affine V, definiamo $\mathcal{I}(V) := \{f \in \mathcal{K}[x] \mid f(\alpha) = 0 \ \forall \alpha \in V\}$

Proposizione 3.2. *Siano I, J ideali e V, W varietà affini. Allora:*

1. $I \subseteq J \Rightarrow \mathcal{V}(I) \supseteq \mathcal{V}(J)$
2. $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) = \mathcal{V}(I)$
3. $V \subseteq W \iff \mathcal{I}(V) \supseteq \mathcal{I}(W)$
4. $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$
5. $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$
6. $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$

Dimostrazione.

1. $$a \in \mathcal{V}(J) \Rightarrow f(a) = 0 \ \forall f \in J \Rightarrow f(a) = 0 \ \forall f \in I \Rightarrow a \in \mathcal{V}(I)$$
2. Chiaramente $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) \supseteq \mathcal{V}(I)$. Per l'altro contenimento, basta notare che $\mathcal{I}(\mathcal{V}(I)) \supseteq I$ e dunque, dal punto (1), $\mathcal{V}(\mathcal{I}(\mathcal{V}(I))) \subseteq \mathcal{V}(I)$.
3. Mostriamo prima che $V \subseteq W \Rightarrow \mathcal{I}(V) \supseteq \mathcal{I}(W)$

   $$f \in \mathcal{I}(W) \Rightarrow \forall a \in W \ f(a) = 0 \Rightarrow \forall a \in V \ f(a) = 0 \Rightarrow f \in \mathcal{I}(V)$$

   Viceversa, supponiamo che $\mathcal{I}(V) \supseteq \mathcal{I}(W)$.

   $$a \in V \Rightarrow f(a) = 0 \ \forall f \in \mathcal{I}(V) \Rightarrow$$
   $$\Rightarrow f(a) = 0 \ \forall f \in \mathcal{I}(W) \Rightarrow a \in \mathcal{V}(\mathcal{I}(W)) = W$$

4. Sicuramente, $I + J \supseteq I$, $I + J \supseteq J$ e dunque $\mathcal{V}(I + J) \subseteq \mathcal{V}(I) \cap \mathcal{V}(J)$. Viceversa, sia $a \in \mathcal{V}(I) \cap \mathcal{V}(J)$.

$$(f(a) = 0 \ \forall f \in I) \ \wedge \ (f(a) = 0 \ \forall f \in J) \Rightarrow f(a) = 0 \ \forall f \in I + J$$

   e dunque $a \in \mathcal{V}(I + J)$.

5. Per contenimento, $I \supseteq IJ$, $J \supseteq IJ$ e dunque $\mathcal{V}(IJ) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J)$. Viceversa, sia $a \in V(IJ)$. Allora $fg(a) = 0 \ \forall f \in I \ \forall g \in J$. Supponiamo $a \notin \mathcal{V}(I)$. Sia $f \in I$ *t.c.* $f(a) \neq 0$. Allora, $\forall g \in J$ $f(a)g(a) = 0$ e dunque $g(a) = 0$.

6. Ancora per contenimento di ideali, $I \supseteq I \cap J$, $J \supseteq I \cap J$ e dunque $\mathcal{V}(I \cap J) \supseteq \mathcal{V}(I) \cup \mathcal{V}(J)$. Viceversa, sappiamo che $IJ \subseteq I \cap J$ e dunque, dal punto precedente, $\mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$.

□

Corollario 3.3. *Se V, W sono varietà affini, allora $V \cap W$ e $V \cup W$ sono varietà affini.*

Teorema 3.4 (Teorema di estensione)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso. Sia $I = (f_1, \dots f_k)$ un ideale di $\mathbb{K}[x_1, \dots x_n]$. Siano $g_i(x_2, \dots x_n) = lt(f_i)$, intendendo $f_i \in \mathbb{K}[x_2, \dots x_n][x_1]$.*

$$\Rightarrow \forall a = (a_2, \dots a_n) \in (\mathcal{V}(I_1) \setminus \mathcal{V}(g_1, \dots g_k)) \ \exists b \in \mathbb{K} \ t.c. \ (b, a_2, \dots a_n) \in \mathcal{V}(I)$$

Dimostrazione. Per semplicità, ci riduciamo a dimostrare l'enunciato nel caso $k = 2$; supponiamo cioè $I = (f, g)$.

$$f = a_s(x_2, \dots x_n)x_1^s + \dots + a_0(x_2, \dots x_n)$$
$$g = b_r(x_2, \dots x_n)x_1^r + \dots + b_0(x_2, \dots x_n)$$

Sia $c \in \mathcal{V}(I_1)$ tale che $(a_s(c) \neq 0) \ \vee \ (b_r(c) \neq 0)$. Dimostriamo prima il caso in cui $(a_s(c) \neq 0) \ \wedge \ (b_r(c) \neq 0)$. Sia $h(x_2, \dots x_n) = \mathrm{Ris}_{x_1}(f, g)$. Per le proprietà del risultante, $h \in \mathbb{K}[x_2, \dots x_n] \cap I = I_1$. Dunque, $h(c) = 0$, ma allora $f(x_1, c), g(x_1, c) \in \mathbb{K}[x_1]$ hanno un fattore in comune. Grazie all'ipotesi che il campo sia algebricamente chiuso, $\exists b \in \mathbb{K}$ *t.c.* $f(b, c) = g(b, c) = 0$; allora $(b, c) \in \mathcal{V}(I)$, come si voleva dimostrare.
Supponiamo ora che $(a_s(c) = 0) \ \wedge \ (b_r(c) \neq 0)$. Consideriamo allora $p = x_1^n g + f$, dove n è scelto in modo tale che $\deg_{x_1}(x_1^n g + f) = \deg_{x_1}(x_1^n g)$. Allora chiaramente $I = (f, g) = (p, g)$, e in questo modo ci siamo ricondotti al caso precedente. □

3.2 Nullstellensatz e sue conseguenze

Siamo pronti per dimostrare il famoso Teorema degli Zeri di Hilbert, che fornisce una corrispondenza tra le varietà affini e gli ideali radicali dell'anello di polinomi.

Teorema 3.5 (Nullstellensatz - forma debole)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $A = \mathbb{K}[x_1, x_2, \dots x_n]$ e sia I un ideale di A.*

$$\mathcal{V}(I) = \emptyset \iff I = A$$

Dimostrazione. Dimostriamo la tesi per induzione sul numero di variabili. Per n=1, $\mathbb{K}[x]$ è un PID, dunque $I = (f)$ e poichè $\mathbb{K}$ è algebricamente chiuso, gli unici polinomi senza radici sono costanti e quindi $I = A$. Supponiamo la tesi vera per ogni $i < n$ e mostriamo che vale per n. Fissiamo un insieme di generatori $I = (f_1 \dots f_k)$. Se i generatori non dipendono da x_1, possiamo usare l'ipotesi induttiva e concludere. Supponiamo allora che esista f_i che dipenda da x_1. Ordinando il polinomio per ordinamento lessicografico, otteniamo

$$f_i = g_1(x_2, \dots, x_n)x_1^N + \tilde{f} \qquad\qquad deg_{x_1}\tilde{f} < N$$

Supponiamo dapprima che g_1 sia costante. Allora necessariamente $\mathcal{V}(I_1) = \emptyset$; in caso contrario, per il Teorema di Estensione 3.4, otterrei $\mathcal{V}(I) \neq \emptyset$ e dunque un assurdo. Allora, per l'ipotesi induttiva, $1 \in I_1 \subseteq I$ e dunque la tesi. Supponiamo allora che g_1 non sia costante. Consideriamo l'isomorfismo di $\mathbb{K}$-algebre:

$$\begin{array}{rccccl} \varphi: & \mathbb{K}[x_1, \dots, x_n] & \longrightarrow & \mathbb{K}[x_1, \dots, x_n] & & \\ & x_1 & \longmapsto & x_1 & & \\ & x_i & \longmapsto & x_i + a_i x_1 & & \forall i = 2 \dots n \end{array}$$

Vogliamo determinare gli a_j in modo tale che l'immagine di f_i abbia termine di testa costante. In questo modo, ci siamo ricondotti al caso studiato prima, poichè φ è un isomorfismo e quindi manda radici in radici. Sia g_j il j-esimo coefficiente di f_i.

$$\varphi(g_j(x_2, \dots, x_n))) = \varphi\left(\sum_\alpha c_\alpha x_2^{\alpha_2} \dots x_n^{\alpha_n}\right) =$$
$$= \sum_\alpha c_\alpha (x_2 + a_2 x_1)^{\alpha_2} \dots (x_n + a_n x_1)^{\alpha_n} = \sum_\alpha c_\alpha x_1^{\sum \alpha_j} a_1^{\alpha_1} \dots a_n^{\alpha_n} + \tilde{g}_\alpha$$

dove $\tilde{g}_\alpha$ ha grado in x_1 minore di $\sum \alpha_j$. Di conseguenza, riordinando i termini secondo x_1,

$$\varphi(f) = s(a_2, \dots a_n)x_1^N + \tilde{h}$$

s è un polinomio in $a_2 \dots a_n$ e dunque, per il principio di identità dei polinomi (notando che l'ipotesi che $\mathbb{K}$ sia algebricamente chiuso garantisce che la cardinalità del campo sia infinita), esistono $\bar{a}_2 \dots \bar{a}_n$ tali che $s \neq 0$, e dunque concludiamo. □

Teorema 3.6 (Nullstellensatz - forma forte)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $A = \mathbb{K}[x_1, x_2, \dots x_n]$ e sia I un ideale di A.*

$$\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$$

Dimostrazione. Mostriamo la tesi per doppia inclusione. Sia $f \in \sqrt{I}$. Allora esiste $n \in \mathbb{N}$ tale che $f^n \in I$. Di conseguenza,

$$f^n(a) = 0 \ \forall a \in \mathcal{V}(I) \Rightarrow (f(a))^n = 0 \Rightarrow f(a) = 0 \Rightarrow f \in \mathcal{I}(\mathcal{V}(I))$$

Viceversa, sia $f \in \mathcal{I}(\mathcal{V}(I))$ e consideriamo $J = (I, 1 - tf) \subseteq \mathbb{K}[t, x_1, \dots x_n]$. Mostriamo che $\mathcal{V}(J) = \emptyset$.

$$(\alpha_1 \dots \alpha_n) \in \mathcal{V}(J) \Rightarrow (\alpha_1 \dots \alpha_n) \in \mathcal{V}(I) \Rightarrow f(\alpha) = 0$$

Ma allora $(1-tf)(\alpha) = 1 \neq 0$ e dunque $\mathcal{V}(J) = \emptyset$. Per la forma debole del Nullstellensatz 3.5, allora, $1 \in (I, 1-tf)$. Fissiamo un insieme di generatori di $I = (g_1, \dots, g_s)$.

$$1 = \sum_{i=1}^{s} a_i(x,t)g_i(x) + h(x,t)(1-tf)$$

Valutiamo l'espressione per $t = 1/f$; otteniamo allora

$$1 = \sum_{i=1}^{s} a_i(x, \frac{1}{f})g_i(x) = \sum_{i=1}^{n} \frac{\tilde{a}_i(x)}{f^{k_i}} g_i(x)$$

Detto $k = \max k_i$, si ricava la relazione

$$f^k = \sum_{i=1}^{s} \overline{a}_i(x)g_i(x)$$

e dunque $f \in \sqrt{I}$, come voluto. □

Il Teorema degli Zeri ha molteplici applicazioni. La prima è di tipo computazionale; fornisce infatti un metodo per dire se un sistema di equazioni polinomiali ammette soluzione:

Corollario 3.7. *Sia K un campo algebricamente chiuso e siano $f_1, \dots, f_k \in K[x_1, \dots, x_n]$. Allora il sistema polinomiale*

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_k = 0 \end{cases}$$

ha soluzioni se e solo se $1 \notin (f_1 \dots f_k)$.

La forma forte invece individua un metodo per determinare se un polinomio appartiene al radicale di un dato ideale:

Corollario 3.8.

$$f \in \sqrt{I} \iff (1-tf, I)\mathbb{K}[t,x] = (1)$$

A livello più astratto, invece, il Nullstellensatz mostra che gli ideali massimali di un anello di polinomi a coefficienti in un campo algebricamente chiuso sono particolarmente semplici:

Lemma 3.9. *Sia $\alpha = (\alpha_1 \dots \alpha_n) \in \mathbb{K}^n$. Allora $\mathfrak{M} = (x_1 - \alpha_1, \dots x_n - \alpha_n)$ è un ideale massimale.*

Dimostrazione. Consideriamo l'omomorfismo di anelli

$$\begin{array}{rccc} \varphi\colon & \mathbb{K}[x] & \longrightarrow & \mathbb{K} \\ & f(x) & \longmapsto & f(\alpha) \end{array}$$

Chiaramente φ è surgettiva, perchè le costanti vengono mandate in loro stesse. Sicuramente poi $\operatorname{Ker}\varphi \supseteq \mathfrak{M}$. D'altronde, i generatori di $\mathfrak{M}$ sono una base di Gröbner, dunque, dato $f \in \mathbb{K}[x]$,

$$f(x) = \sum p_i(x)(x_i - \alpha_i) + r \Rightarrow f(\alpha) = \sum p_i(\alpha)0 + r = r$$

e dunque $f \in \operatorname{Ker}\varphi \iff f \in \mathfrak{M}$. □

Proposizione 3.10. *Sia $\mathbb{K}$ un campo algebricamente chiuso. Allora $\mathfrak{M}$ è un ideale massimale se e solo se esiste $\alpha \in \mathbb{K}^n$ tale che $\mathfrak{M} = (x_1 - \alpha_1 \dots x_n - \alpha_n)$*

Dimostrazione. Una implicazione è stata dimostrata nel Lemma precedente 3.9. Viceversa, sia $\mathfrak{M}$ un ideale massimale. Per la forma debole del Nullstellensatz, $\mathcal{V}(\mathfrak{M}) \neq \emptyset$; sia allora $\alpha \in \mathcal{V}(\mathfrak{M})$.

$$(x_1 - \alpha_1, \dots, x_n - \alpha_n) = \mathcal{I}(\{\alpha\}) \supseteq \mathcal{I}(\mathcal{V}(\mathfrak{M})) = \sqrt{\mathfrak{M}} = \mathfrak{M}$$

Per massimalità di $\mathfrak{M}$ si ha l'uguaglianza. □

I risultati maggiori si hanno però nell'ambito della Geometria Algebrica.

Definizione 3.11. Sia S un sottoinsieme di $\mathbb{K}^n$. $\overline{S} = \mathcal{V}(\mathcal{I}(S))$ è la chiusura di Zariski di S.

Lemma 3.12. *La chiusura di Zariski è la più piccola varietà affine che contiene S.*

Dimostrazione. Sicuramente $\overline{S} = \mathcal{V}(\mathcal{I}(S))$ è una varietà affine. Sia allora $W \supseteq S$ una varietà affine.

$$\mathcal{I}(W) \subseteq \mathcal{I}(S) \Rightarrow W = \mathcal{V}(\mathcal{I}(W)) \supseteq \mathcal{V}(\mathcal{I}(S))) = \overline{S}$$

e dunque $\overline{S}$ è l'intersezione di tutte le varietà affine che contengono S. □

Proposizione 3.13. *Sia I un ideale, sia $V = \mathcal{V}(I)$ e sia*

$$\begin{array}{rccc} \pi_k\colon & \mathbb{K}^n & \longrightarrow & \mathbb{K}^{n-k} \\ & (\alpha_1 \dots \alpha_n) & \longmapsto & (\alpha_{n-k+1} \dots \alpha_n) \end{array}$$

Allora $\overline{\pi_k(V)} = \mathcal{V}(I_k)$

Dimostrazione. Mostriamo che $\overline{\pi_k(V)} \subseteq \mathcal{V}(I_k)$. Supponiamo per semplicità $k = 1$. Dal teorema di estensione,

$$\mathcal{V}(I_1) = \pi_1(V) \cup (\mathcal{V}(g_1, \dots, g_s) \cap \mathcal{V}(I_1))$$

dove g_i è il termine di testa dell'i-esimo generatore di I. Ma allora

$$\mathcal{V}(I_1) \supseteq \pi_1(V) \Rightarrow \mathcal{V}(\mathcal{I}(\mathcal{V}(I_1))) \supseteq \mathcal{V}(\mathcal{I}\pi_1(V))$$

Viceversa, sia $f \in \mathcal{I}(\pi_k(V))$.

$$\forall \bar{\alpha} \in \pi_k(V)\ f(\bar{\alpha}) = 0\ \bar{\alpha} = \pi_k(\alpha)\ \alpha \in V \Rightarrow f(\alpha) = 0 \Rightarrow$$
$$\Rightarrow f \in \mathbb{K}[x_{k+1}, \dots, x_n] \cap \sqrt{I} \Rightarrow f^n \in I_k \Rightarrow \mathcal{I}(\pi_k(V)) \subseteq \sqrt{I_k} \Rightarrow \overline{\pi_k(V)} \supseteq \mathcal{V}(I_k)$$

□

Lemma 3.14. *Siano V, W varietà affini e sia $V \subseteq W$.*

$$W = V \cup (\overline{W \setminus V})$$

Proposizione 3.15. *Ogni catena discendente di varietà affini è stazionaria.*

Dimostrazione. Data $V_1 \supseteq V_2 \supseteq \dots$ catena discendente di varietà affini, possiamo fargli corrispondere la catena ascendente di ideali $\mathcal{I}(V_1) \subseteq \mathcal{I}(V_2) \subseteq \dots$. Poichè $K[x_1, \dots, x_n]$ è noetheriano, tale catena è stazionaria; necessariamente allora, anche la catena $\mathcal{V}(\mathcal{I}(V_1)) \supseteq \mathcal{V}(\mathcal{I}(V_2)) \supseteq \dots$ è stazionaria. La dimostrazione termina notando che $\mathcal{V}(\mathcal{I}(V)) = V$. □

Definizione 3.16. Una varietà V si dice irriducibile se, date V_1 e V_2 varietà,

$$V = V_1 \cup V_2 \Rightarrow (V_1 = V) \vee (V_2 = V)$$

Proposizione 3.17. *Sia V una varietà. Allora V è irriducibile se e solo se $\mathcal{I}(V)$ è un ideale primo.*

Dimostrazione.

- $\Rightarrow$ Sia $fg \in \mathcal{I}(V)$. Vogliamo mostrare che $f \in \mathcal{I}(V)$ oppure $g \in \mathcal{I}(V)$. Consideriamo le varietà

  $$V_1 = V \cap \mathcal{V}(f) \qquad\qquad V_2 = V \cap \mathcal{V}(g)$$

  Mostriamo che $V_1 \cup V_2 = V$.

  $$V_1 \cup V_2 = (V \cap \mathcal{V}(f)) \cup (V \cap \mathcal{V}(g)) = V \cup (\mathcal{V}(f) \cap \mathcal{V}(g)) = V \cup (\mathcal{V}(fg)) = V$$

  Di conseguenza, per irriducibilità di V, $(V = V_1) \vee (V = V_2)$. Ma allora $f \in \mathcal{I}(V) \ \vee \ g \in \mathcal{I}(V)$.

- $\Leftarrow$ Sia $V = V_1 \cup V_2$. Passando agli ideali, $\mathcal{I}(V) = \mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$. Poichè $\mathcal{I}(V)$ è primo, è anche irriducibile, dunque $\mathcal{I}(V_1) = \mathcal{I}(V)$ oppure $\mathcal{I}(V_2) = \mathcal{I}(V)$. Sfruttando il fatto che $\mathcal{V}(\mathcal{I}(V)) = V$, si ha che $V_1 = V$ oppure $V_2 = V$, e dunque V è irriducibile.

□

Teorema 3.18. *Sia V una varietà affine. Allora esistono $V_1 \dots V_n$ varietà irriducibili tali che $V = \bigcup_{i=1}^n V_i$*

Dimostrazione. Sia $\Sigma = \{V \mid V \text{ non è unione finita di varietà irriducibili}\}$, ordinato per inclusione. Supponiamo per assurdo che Σ sia non vuoto. Allora Σ ammette un elemento minimale V. V non è irriducibile, quindi $V = A \cup B$ con $A \neq V \ \wedge \ B \neq V$. Per minimalità di V, $A = \bigcup_{i=1}^m W_i$ e $B = \bigcup_{i=1}^k Z_i$ con Z_i, W_i irriducibili. Ma allora $V = \bigcup_{i=1}^m W_i \cup \bigcup_{i=1}^k Z_i$, assurdo. □

Proposizione 3.19. *Sia V una varietà affine e sia $V = \bigcup_{i=1}^n V_i$ una sua decomposizione in varietà irriducibili. Se $\forall i = 1 \dots n \ \forall j \neq i \ V_i \not\subseteq V_j$, allora la decomposizione è unica.*

Dimostrazione. Supponiamo $V = \bigcup_{i=1}^n V_i = \bigcup_{i=1}^m W_i$. Allora:

$$V_i = V_i \cap V = \bigcup_{j=1}^m V_i \cap W_j$$

Per irriducibilità di V_i, $\exists r$ *t.c.* $V_i = V_i \cup W_r$ e dunque $V_i \subseteq W_r$. Allo stesso modo, $W_r \subseteq V_j$. Per irridondanza della decomposizione, $j = i$ e $V_i = W_r$. Dunque le due decomposizioni sono uguali a meno di permutazione dei fattori.

□

Fino ad ora, abbiamo studiato le varietà algebriche senza definire alcuna nozione di mappe tra di esse. La maniera più naturale di far questo è considerare le seguenti:

Definizione 3.20. Una mappa $\varphi\colon \mathbb{K}^n \to \mathbb{K}^m$ si dice polinomiale se esistono $f_1 \dots f_m \in \mathbb{K}[x]$ taali che $\varphi(a) = (f_1(a), \dots f_m(a))$

Siano $\psi, \varphi\colon \mathbb{K}^n \to \mathbb{K}^m$ mappe polinomiali e supponiamo che $\forall a \in V$ $\varphi(a) = \psi(a)$. Sotto queste ipotesi, $(\varphi - \psi)(a) = 0$ e dunque $\varphi - \psi \in \mathcal{I}(V)$. Questo ci spinge a studiare l'anello $\mathbb{K}[V] := {}^{\mathbb{K}[x]}\!/_{\mathcal{I}(V)}$, che chiamiamo *anello delle coordinate di V*. La teoria svolta sulle basi di Gröbner permette di trovare dei rappresentanti delle classi di resto privilegiati:

Proposizione 3.21. *Sia $A = \mathbb{K}[x_1 \dots x_n]$, sia $\leq$ un ordinamento monomiale su A e sia I un ideale di A. Allora*

1. *$\forall f \in A$ esiste un'unico $\bar{f}$ tale che $f \cong \bar{f}$ (mod I) e $\bar{f} = \sum c_\beta x^\beta$, dove $x^\beta \notin lt(I)$*
2. *$\{x^\alpha \mid x^\alpha \notin lt(I)\}$ è una base di ${}^{A}\!/_{I}$ come $\mathbb{K}$-spazio vettoriale.*

Dimostrazione. Sia $(G, \leq)$ una base di Gröbner di I. Per l'algoritmo di divisione, allora,

$$f = \sum a_i g_i + r \quad r = \sum r_\alpha x^\alpha \; x^\alpha \notin lt(I).$$

Per unicità del resto della divisione per una base di Gröbner, abbiamo la tesi. □

Teorema 3.22. *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $A = \mathbb{K}[x_1 \dots x_n]$, sia $\leq$ un ordinamento monomiale su A e sia I un ideale di A. Sono equivalenti:*

1. *$\#\mathcal{V}(I) < \infty$*
2. *$\forall i = 1 \dots n \; \exists m_i \in \mathbb{N}$ t.c. $x_i^{m_i} \in lt(I)$*
3. *Data $(G, \leq)$ una base di Gröbner di I, per ogni i esiste $h \in \mathbb{N}$ ed esiste $g_k \in G$ tale che $lt(g_k) \mid x_i^h$*
4. *$\dim_{\mathbb{K}} {}^{A}\!/_{I} < \infty$*

Dimostrazione.

(1) ⇒ (2) Se $V = \emptyset$, la tesi discende facilmente dalla forma debole del Nullstellensatz. Sia allora $V = \{P_1, \dots P_k\}$. $\forall i = 1 \dots k$, $P_i = (a_1^{(i)}, \dots, a_n^{(i)})$. Allora:

$$f_j(x) = \prod_{i=1}^{k} (x_j - a_j^{(i)} \in \mathcal{I}(V) = \sqrt{I} \Rightarrow f_j^{n_j} \in I \text{ è monico in } x_j$$

e dunque abbiamo provato (2).

(2) ⇔ (3) L'equivalenza è ovvia, basta ricordare che data $(G, \leq)$ una base di Gröbner di I, $lt(I) = (lt(g_1), \dots, lt(g_k))$.

(3) ⇒ (4) Per la proposizione precedente, è sufficiente dimostrare che l'insieme $\{\alpha \in \mathbb{N}^n \mid x^\alpha \notin lt(I)\}$ è finito. Sia $\alpha \in \mathbb{N}^n$. Se $x^\alpha \notin lt(I)$, necessariamente deve valere $\alpha_1 < m_1 \dots \alpha_n < m_n$, dunque la base è finita.

(4) $\Rightarrow$ (1) Sia $n = \dim_{\mathbb{K}} {}^{A}\!/_{I}$. Allora $\{\bar{1}, \bar{x}_i \dots \bar{x}_i^n\}$ è un insieme di vettori linearmente dipendenti, dunque $\exists c_j \in \mathbb{K}$ *t.c.* $\sum_{j=1}^{n} c_j \bar{x}_i^j = 0$. Dunque $\sum c_j x_i^j \in I$, e dunque ogni coordinata deve soddisfare un polinomio di grado finito. Di conseguenza, il luogo degli zeri deve essere finito.

□

Osservazione 3.23. Nella dimostrazione del teorema, l'ipotesi che $\mathbb{K}$ fosse algebricamente chiuso è stata utilizzata solo nell'implicazione (1) $\Rightarrow$ (2).

Proposizione 3.24. *Sia $\mathbb{K}$ un campo algebricamente chiuso, sia I un ideale radicale di $\mathbb{K}[x_1 \dots x_n]$. Supponiamo che $\#\mathcal{V}(I) = s$. Allora:*

$$\dim_{\mathbb{K}} {}^{\mathbb{K}[x]}\!/_{I} = s$$

Dimostrazione. Sia $V = \{Q_1 \dots Q_s\}$. Per quanto visto,

$$I = \sqrt{I} = \mathcal{I}(V) = \bigcap_{i=1}^{s} \mathcal{I}(Q_i)$$

Notiamo che $\mathcal{I}(Q_i)$ è un ideale massimale; detto allora $\mathfrak{M}_i = \mathcal{I}(Q_i)$, per il teorema cinese del resto si ha:

$$\mathbb{K}[x]\!/_{I} \simeq \mathbb{K}[x]\!/_{\prod_{i=1}^{s} \mathfrak{M}_i} \simeq \prod_{i=1}^{s} \mathbb{K}[x]\!/_{\mathfrak{M}_i} \simeq \mathbb{K}^s$$

□

Lemma 3.25. *Sia $I = (f, g)$ un ideale di $\mathbb{C}[x, y]$.*

$$\mathrm{Ris}(f, g) \neq 0 \Rightarrow \#\mathcal{V}(f, g) < \infty$$

Dimostrazione. Basta notare che $\mathrm{Ris}_x(f, g) = h(y) \in \mathbb{C}[y] \setminus \{0\}$, $\mathrm{Ris}_y(f, g) = p(x) \in \mathbb{C}[x] \setminus \{0\}$ e dunque

$$\mathcal{V}(f, g) = \mathcal{V}(f, g, h, p)$$

Dal teorema fondamentale dell'algebra, h,p hanno un numero finito di radici, e quindi il luogo di zeri di I è finito. □

Capitolo 4

Prodotto Tensore

4.1 Definizione e proprietà fondamentali

Definizione 4.1. Siano M, N, P A-moduli. $f\colon M \times N \to P$ si dice bilineare se:

- $f(m_1 + m_2, n_1 + n_2) = f(m_1, n_1) + f(m_1, n_2) + f(m_2, n_1) + f(m_2, n_2)$
- $f(am, bn) = abf(m, n)$

Dato $M \times N$, consideriamo $A^{M \times N} = C$ il modulo libero generato dagli elementi di $M \times N$. Sia D il sottomodulo di C generato dagli elementi della forma:

$$\begin{aligned} (m_1 + m_2, n) - (m_1, n) - (m_2, n) \qquad & (m, n_1 + n_2) - (m, n_1) - (m, n_2) \\ a(m - n) - (am, n) \qquad & a(m, n) - (m, an) \end{aligned}$$

Definiamo il prodotto tensore tra M e N come $M \otimes N = {}^{C}\!/_{D}$.

Osservazione 4.2. Poichè C è generato dalle coppie $(m, n) \in M \otimes N$, si ha che $\overline{(m, n)} = m \otimes n$ è un insieme di generatori per $M \otimes_A N$.

Vediamo come si comporta questo modulo rispetto alle operazioni.

Lemma 4.3. *1.* $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$

2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$

3. $a(m \otimes n) = am \otimes n = m \otimes (an)$

Dimostrazione. Mostriamo che vale (1).

$$\begin{gathered} (m_1 + m_2) \otimes n = (m_1 + m_2, n) + D = \\ ((m_1, n) + D) + ((m_2, n) + D) = m_1 \otimes n + m_2 \otimes n \end{gathered}$$

Allo stesso modo si dimostra (2).

$$\begin{aligned} a(m, n) = a((m, n) + D) = (am, an) + D \ (caso\ 1) &= (am, n) + D = am \otimes n \\ (caso\ 2) &= (m, an) + D = m \otimes an \end{aligned}$$

□

Corollario 4.4.

$$\begin{array}{rccc} g\colon & M \times N & \longrightarrow & M \otimes_A N \\ & (m,n) & \longmapsto & m \otimes n \end{array}$$

è una mappa bilineare.

Caratterizziamo ora il prodotto tensore in termini categoriali. Fissiamo M, N due A-moduli. Consideriamo la categoria $\mathcal{C}$ nella quali gli oggetti sono i prodotti bilineari $f : M \times N \to P$ dove P è un qualsiasi A-modulo e nel quale i morfismi sono le mappe che fanno commutare il seguente diagramma:

$$\begin{tikzcd} & P_1 \arrow[dd, "\tilde{g}"] \\ M \times N \arrow[ur, "g"] \arrow[dr, "f"'] & \\ & P_2 \end{tikzcd}$$

Si ha allora che in questa categoria il prodotto tensore è un oggetto universale, come chiarito nelle seguenti proposizioni:

Proposizione 4.5. *Siano M, N, P A-moduli e sia $f\colon M \times N \to P$ una mappa bilineare.*
$\Rightarrow \exists! \tilde{f}\colon M \otimes_A N \to P$ omomorfismo di A-moduli che fa commutare il diagramma:

$$\begin{tikzcd} M \times N \arrow[rr, "f"] \arrow[dr, "g"'] & & P \\ & M \otimes_A N \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Dimostrazione. Con la notazione usata in precedenza, sia

$$\begin{array}{rccc} F\colon & C & \longrightarrow & P \\ & (m,n) & \longmapsto & f(m,n) \end{array}$$

F è per costruzione un omomorfismo di A-moduli. Inoltre, $\forall a \in D$,

$$F(a) = f \circ g(a) = 0 \Rightarrow D \subseteq \operatorname{Ker} f$$

Allora è ben definito il passaggio al quoziente $\tilde{f} : M \otimes_A N = {}^{C}\!/_{D} \to P$. Per commutatività del diagramma, $\tilde{f}(m \otimes n) = f(m,n)$. Mostriamo allora che tale $\tilde{f}$ è unica. Sia h un omomorfismo che fa commutare il diagramma. Allora:

$$h(m \otimes n) = f(m,n) = \tilde{f} \circ g(m,n) = \tilde{f}(m \otimes n) \Rightarrow \tilde{f} = h$$

□

Proposizione 4.6. *$M \otimes_A N$ è l'unico A-modulo che soddisfa la proprietà universale della proposizione precedente.*

Dimostrazione. Sia (T, h) una coppia modulo-funzione che soddisfa le proprietà della proposizione precedente. Mostriamo che $T \simeq M \otimes_A N$ Consideriamo i diagrammi:

$$\begin{tikzcd} M \times N \arrow[rr, "h"] \arrow[dr, "g"'] & & T \\ & M \otimes_A N \arrow[ur, "\tilde{h}"'] & \end{tikzcd} \qquad \begin{tikzcd} M \times N \arrow[rr, "g"] \arrow[dr, "h"'] & & M \otimes_A N \\ & T \arrow[ur, "\tilde{g}"'] & \end{tikzcd}$$

Per commutatività, $\tilde{h} \circ g = h$ e $\tilde{g} \circ h = g$. Si ottiene allora $\tilde{h} \circ \tilde{g} \circ h = h$ e $\tilde{g} \circ \tilde{h} \circ g = g$. Dunque, il seguente diagramma commuta:

$$\begin{tikzcd} M \times N \arrow[rr, "h"] \arrow[dr, "h"'] & & T \\ & T \arrow[ur, "\tilde{h} \circ \tilde{g}"'] & \end{tikzcd}$$

ma commuterebbe anche con l'identità. Allora, per unicità della mappa, dimostrata nella proposizione precedente, si ha $\tilde{h} \circ \tilde{g} = id_T$. Analogamente, si ottiene $\tilde{g} \circ \tilde{h} = id_{M \otimes_A N}$, e quindi l'isomorfismo. □

Corollario 4.7. *Siano $u\colon M \to M'$, $v\colon N \to N'$ omomorfismi di A-moduli.*

$$\Rightarrow \exists! \varphi\colon \quad \begin{array}{ccc} M \otimes_A N & \longrightarrow & M' \otimes_A N' \\ m \otimes n & \longmapsto & u(m) \otimes v(n) \end{array}$$

Ora che abbiamo caratterizzato il prodotto tensore, vediamo come si comporta con le altre operazioni introdotte sui moduli.

Proposizione 4.8. *Siano M, N, P A-moduli.*

1. $A \otimes_A M \simeq M$
2. $M \otimes_A N \simeq N \otimes_A M$
3. $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$
4. $(M \oplus N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$

Dimostrazione.

(1) Consideriamo l'omomorfismo di A-moduli

$$f\colon \quad \begin{array}{ccc} A \times M & \longrightarrow & M \\ (a, m) & \longmapsto & am \end{array}$$

f è una mappa bilineare surgettiva, dunque per la proprietà universale passa al prodotto tensore:

$$\tilde{f}\colon \quad \begin{array}{ccc} A \otimes_A M & \longrightarrow & M \\ a \otimes m & \longmapsto & am \end{array}$$

Per commutatività del diagramma, $\tilde{f}$ è surgettiva. Per mostrare l'iniettività, notiamo che un elemento di $A \otimes_A M$ si può scrivere meglio:

$$\sum_{i=1}^{n} a_i \otimes m_i = \sum_{i=1}^{n} 1 \otimes a_i m_i = 1 \otimes \sum_{i=1}^{n} a_i m_i = 1 \otimes \tilde{m}$$

Dunque,

$$\tilde{f}(1 \otimes m) = 0 \iff 1m = 0 \iff m = 0 \iff 1 \otimes m = 0$$

e quindi l'iniettività.

(2) Con lo stesso metodo, definiamo:

$$\begin{array}{rccc} f\colon & N \times M & \longrightarrow & M \otimes_A N \\ & (n, m) & \longmapsto & m \otimes n \end{array}$$

f è una mappa bilineare, dunque passa al prodotto tensore:

$$\begin{array}{rccc} \varphi\colon & N \otimes_A M & \longrightarrow & M \otimes_A N \\ & n \otimes m & \longmapsto & m \otimes n \end{array}$$

D'altronde, possiamo anche definire

$$\begin{array}{rccc} g\colon & M \times N & \longrightarrow & N \otimes_A M \\ & (m, n) & \longmapsto & n \otimes m \end{array}$$

Anche questa è una mappa bilineare, dunque passa al prodotto tensore:

$$\begin{array}{rccc} \psi\colon & M \otimes_A N & \longrightarrow & N \otimes_A M \\ & m \otimes n & \longmapsto & n \otimes m \end{array}$$

Verifichiamo ora che $\psi \circ \varphi = id_{M \otimes_A N}$ e $\varphi \circ \psi = id_{N \otimes_A M}$. Poichè sono omomorfismi di A-moduli, è sufficiente controllarlo sui generatori.

$$\psi(\varphi(n \otimes m)) = \psi(m \otimes n) = n \otimes n$$
$$\varphi(\psi(m \otimes n)) = \varphi(n \otimes m) = m \otimes n$$

Dunque sono isomorfismi tra i moduli $M \otimes_A N$ e $N \otimes_A N$, come voluto.

(3) Utilizziamo la stessa tecnica del punto 2. Definiamo:

$$\begin{array}{rccc} f\colon & M \times (N \otimes_A P) & \longrightarrow & (M \otimes_A N) \otimes_A P \\ & (m, n \otimes p) & \longmapsto & (m \otimes n) \otimes p \end{array}$$

Verifichiamo che f è ben definita. Consideriamo la mappa:

$$\begin{array}{rccc} g\colon & M \times N \times P & \longrightarrow & (M \otimes_A N) \otimes_A P \\ & (m, n, p) & \longmapsto & (m \otimes n) \otimes p \end{array}$$

Tale mappa è ben definita, dunque possiamo considerare le m-sezioni:

$$\begin{array}{rccc} g_m\colon & N \times P & \longrightarrow & (M \otimes_A N) \otimes_A P \\ & (n, p) & \longmapsto & (m \otimes n) \otimes p \end{array}$$

g_m è A-bilineare, dunque passa al tensore:

$$\begin{array}{rccc} \tilde{g}_m\colon & N \otimes_A P & \longrightarrow & (M \otimes_A N) \otimes_A P \\ & n \otimes p & \longmapsto & (m \otimes n) \otimes p \end{array}$$

Abbiamo allora che la f introdotta all'inizio è in realtà:

$$\begin{array}{rccc} f\colon & M \times (N \otimes_A P) & \longrightarrow & (M \otimes_A N) \otimes_A P \\ & (m, n \otimes p) & \longmapsto & \tilde{g}_m(n,p) \end{array}$$

e notando che $\tilde{g}_{am} = a\tilde{g}_m$ si ha la buona definizione. f è A-bilineare, e dunque passa al prodotto tensore:

$$\begin{array}{rccc} \varphi\colon & P \otimes_A (N \otimes_A M) & \longrightarrow & (P \otimes_A M) \otimes_A N \\ & p \otimes (n \otimes m) & \longmapsto & (p \otimes m) \otimes n \end{array}$$

Allo stesso modo, si ottiene:

$$\begin{array}{rccc} \psi\colon & (P \otimes_A N) \otimes_A M & \longrightarrow & P \otimes_A (M \otimes_A N) \\ & (p \otimes n) \otimes m & \longmapsto & p \otimes (m \otimes n) \end{array}$$

Dunque,

$$\psi(\varphi(p \otimes (n \otimes m))) = \psi((p \otimes m) \otimes n) = p \otimes (n \otimes m)$$
$$\varphi(\psi((p \otimes m) \otimes n)) = \varphi(p \otimes (n \otimes m)) = (p \otimes m) \otimes n$$

e dunque l'isomorfismo cercato.

(4) Consideriamo le mappe:

$$\begin{array}{rccc} f\colon & M \times N_1 & \longrightarrow & M \otimes_A (N_1 \oplus N_2) \\ & (m, n_1) & \longmapsto & m \otimes (n_1, 0) \\ g\colon & M \times N_2 & \longrightarrow & M \otimes_A (N_1 \oplus N_2) \\ & (m, n_2) & \longmapsto & m \otimes (0, n_2) \end{array}$$

f, g sono entrambe bilineari, dunque per la proprietà universale del prodotto tensore otteniamo gli omomorfismi

$$\begin{array}{rccc} \tilde{f}\colon & M \otimes_A N_1 & \longrightarrow & M \otimes_A (N_1 \oplus N_2) \\ & m \otimes n_1 & \longmapsto & m \otimes (n_1, 0) \\ \tilde{g}\colon & M \otimes_A N_2 & \longrightarrow & M \otimes_A (N_1 \oplus N_2) \\ & m \otimes n_2 & \longmapsto & m \otimes (0, n_2) \end{array}$$

Per definizione di somma diretta otteniamo allora

$$\begin{array}{rccc} \varphi\colon & (M \otimes_A N_1) \oplus (M \otimes_A N_2) & \longrightarrow & M \otimes_A (N_1 \oplus N_2) \\ & (m_1 \otimes n_1, m_2 \otimes n_2) & \longmapsto & m_1 \otimes (n_1, 0) + m_2 \otimes (0, n_2) \end{array}$$

Mostriamo ora l'inversa, con lo stesso metodo. La mappa

$$\begin{array}{rccc} h\colon & M \times (N_1 \oplus N_2) & \longrightarrow & (M \otimes_A N_1) \oplus (M \otimes_A N_2) \\ & (m, (n_1, n_2)) & \longmapsto & (m \otimes n_1, m \otimes n_2) \end{array}$$

è bilineare, dunque passa al tensore:

$$\begin{array}{rccc} \psi\colon & M \otimes_A (N_1 \oplus N_2) & \longrightarrow & (M \otimes_A N_1) \oplus (M \otimes_A N_2) \\ & m \otimes (n_1, n_2) & \longmapsto & (m \otimes n_1, m \otimes n_2) \end{array}$$

Dunque,

$$\psi(\varphi(m \otimes n_1, m \otimes n_2)) = \psi(m \otimes (n_1, n_2)) = (m \otimes n_1, m \otimes n_2)$$
$$\varphi(\psi(m \otimes (n_1, n_2))) = \varphi(m \otimes n_1, m \otimes n_2) = (m \otimes (n_1, n_2))$$

e quindi ψ, φ sono isomorfismi.

□

Vediamo ora qualche lemma utile per caratterizzare, a meno di isomorfismo, i prodotti più semplici.

Corollario 4.9. $A^n \otimes_A A^m \simeq A^{mn}$

Dimostrazione.

$$A^n \otimes_A A^m \simeq (\oplus_{i=1}^n A) \otimes_A (\oplus_{i=1}^m A) \simeq \oplus_{i=1}^n \oplus_{j=1}^m (A \otimes_A A) \simeq$$
$$\simeq \oplus_{i=1}^n \oplus_{j=1}^m (A) \simeq A^{mn}$$

□

Proposizione 4.10. *Sia A un anello e siano I, J ideali di A.*

$$A/I \otimes_A A/J \simeq A/I + J$$

Dimostrazione. Consideriamo la mappa bilineare:

$$\begin{array}{rccc} f\colon & A/I \times A/J & \Longrightarrow & A/(I+J) \\ & (a+I, b+J) & \longmapsto & ab+I+J \end{array}$$

Per la proprietà universale del prodotto tensore, esiste l'omomorfismo di A-moduli

$$\begin{array}{rccc} \varphi\colon & A/I \otimes_A A/J & \Longrightarrow & A/(I+J) \\ & a+I \otimes b+J & \longmapsto & ab+I+J \end{array}$$

φ è surgettiva perchè f lo è. Mostriamo allora che φ è iniettiva. Notiamo prima che ogni elemento del prodotto tensore ammette una scrittura più semplice.

$$(x+I) \otimes (y+J) = x((1+I) \otimes (y+J) = (1+I) \otimes (xy+J)$$

Mostriamo, con questa scrittura, che $\operatorname{Ker} \varphi = \{0\}$.

$$\varphi((1+I) \otimes (xy+J)) = 0 \iff xy \in I+J \iff \exists i \in I\ \exists j \in J \text{ t.c. } i+j = xy$$
$$\Rightarrow I \otimes (xy+J) = I \otimes i + J = 0$$

□

Cerchiamo ora di capire come si comporta il prodotto tensore con le successioni esatte; per questo abbiamo prima bisogno del seguente teorema:

Teorema 4.11. *Siano M, N, P A-moduli.*

$$Bil(M \times N, P) \simeq Hom_A(M \otimes_A N, P) \simeq Hom_A(M, Hom_A(N, P))$$

Dimostrazione. Il primo isomorfismo è solo questione di linguaggio; infatti la definizione del prodotto tensore induce l'omomorfismo:

$$\begin{array}{rccccc} \Phi\colon & Bil(M \times N, P) & \longrightarrow & Hom_A(M \otimes_A N, P) & & \\ & f & \longmapsto & \Psi(f)\colon M \otimes_A N & \to & P \\ & & & m \otimes n & \mapsto & f(m,n) \end{array}$$

che è surgettivo per costruzione del prodotto tensore e iniettivo per unicità della mappa.
Mostriamo ora che $Bil(M \times N, P) \simeq Hom_A(M, Hom_A(N, P))$. Definiamo le mappe:

$$\begin{array}{llllll} F\colon & Bil(M \times N, P) & \longrightarrow & Hom_A(M, Hom_A(N,P)) & & \\ & f & \longmapsto & F(f)\colon M & \to & Hom_A(N,P) \\ & & & m & \mapsto & F(f)(m) \end{array}$$

$$\begin{array}{llllll} G\colon & Hom_A(M, Hom_A(N,P)) & \longrightarrow & Bil(M \times N, P) & & \\ & \varphi & \longmapsto & G(\varphi)\colon M \times N & \to & P \\ & & & (m,n) & \mapsto & \varphi(m)(n) \end{array}$$

F e G sono una l'inversa dell'altra, da cui la tesi. □

Corollario 4.12.

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ è esatta}$$
$$\Longleftrightarrow$$
$$\forall N \text{ A-modulo } M' \otimes N \xrightarrow{f \otimes id} M \otimes N \xrightarrow{g \otimes id} M'' \otimes N \to 0 \text{ è esatta}$$

Lemma 4.13. *Sia A un anello, I un ideale di A e M un A-modulo$\Rightarrow$ ${}^{A}\!/_{I} \otimes_A M$ si può munire della struttura di ${}^{A}\!/_{I}$-modulo.*

Dimostrazione. E' sufficiente notare che $I \subseteq \mathrm{Ann}({}^{A}\!/_{I} \otimes_A M)$. □

Dato un A-modulo M e B un anello, definiamo $M_B = M \otimes_A B$. Abbiamo così ottenuto un B-modulo; chiamiamo questa operazione estensione di scalari.

Proposizione 4.14. *Sia M un A-modulo, P un B-modulo e N un A- e B-modulo.*

$$\Rightarrow (M \otimes_A N) \otimes_B P \simeq M \otimes_A (N \otimes_B P)$$

Dimostrazione. Definiamo l'applicazione:

$$\begin{array}{llll} F\colon & (M \otimes_A N) \times P & \longrightarrow & M \otimes_A (N \otimes_B P) \\ & (\sum m_i \otimes n_i, p) & \longmapsto & \sum m_i \otimes (n_i \otimes p) \end{array}$$

Poichè è B-bilineare, passa al tensore su B:

$$\begin{array}{llll} \varphi\colon & (M \otimes_A N) \otimes_B P & \longrightarrow & M \otimes_A (N \otimes_B P) \\ & (a \otimes b) \otimes c & \longmapsto & a \otimes (b \otimes c) \end{array}$$

Allo stesso modo, possiamo ottenere:

$$\begin{array}{llll} \psi\colon & M \otimes_A (N \otimes_B P) & \longrightarrow & (M \otimes_A N) \otimes_B P \\ & a \otimes (b \otimes c) & \longmapsto & (a \otimes b) \otimes c \end{array}$$

Come già fatto vedere in precedenza, φ e ψ sono l'una l'inversa dell'altra, e dunque sono isomorfismi. □

Lemma 4.15. *Sia A un anello, I un ideale di A e sia M un A-modulo.*

$$\Rightarrow {}^{A}\!/_{I} \otimes_A M \simeq {}^{M}\!/_{IM}$$

Dimostrazione. Consideriamo la successione esatta:

$$0 \to I \xrightarrow{i} A \xrightarrow{\pi} {}^{A}\!/_{I} \to 0$$

Tensorizzando per M, si ottiene:

$$I \otimes_A M \xrightarrow{i \otimes id} A \otimes_A M \xrightarrow{\pi \otimes id} {}^{A}\!/_{I} \otimes_A M \to 0$$

Sappiamo però che $A \otimes_A M \simeq M$; otteniamo allora la successione:

$$I \otimes_A M \xrightarrow{f} M \xrightarrow{g} {}^{A}\!/_{I} \otimes_A M \to 0$$

E' sufficiente allora studiare il $\mathrm{Ker}(g)$, che per esattezza coincide con $\mathrm{Im}(f)$. Vediamo allora l'immagine di $I \otimes A$ in M.

$$\begin{array}{rccc} f\colon & I \otimes_A M & \longrightarrow & M \\ & i \otimes m & \longmapsto & im \end{array}$$

Per doppia inclusione, $\mathrm{Im}(f) = IM$ e dunque la tesi. □

Proposizione 4.16. *Sia A un anello locale, siano M,N A-moduli finitamente generati.*

$$M \otimes_A N = 0 \Longrightarrow (M = 0) \vee (N = 0)$$

Dimostrazione. Sappiamo che, detto $K = {}^{A}\!/_{\mathfrak{M}}$, si ha

$$\begin{aligned} {}^{M}\!/_{\mathfrak{M}M} &\simeq {}^{A}\!/_{\mathfrak{M}} \otimes_A M = M_K \\ {}^{N}\!/_{\mathfrak{M}N} &\simeq {}^{A}\!/_{\mathfrak{M}} \otimes_A N = N_K \end{aligned}$$

Dunque,

$$\begin{aligned} M_K \otimes_K N_K = (M \otimes_A K) \otimes_K (N \otimes_A K) \simeq ((M \otimes_A K) \otimes_K K) \otimes_A N \simeq \\ \simeq (M \otimes_A K) \otimes_A N \simeq (M \otimes_A N) \otimes_A K = 0 \end{aligned}$$

Di conseguenza, $M_K \otimes_K N_K = 0$. Ma M_K e N_K sono spazi vettoriali su K e dunque $M_K \simeq K^n$ e $N_K \simeq K^m$. Allora, per quanto visto per i moduli liberi,

$$M_K \otimes_K N_K \simeq K^{nm} \simeq 0 \iff (n = 0) \vee (m = 0)$$

Supponiamo $n = 0$; il caso $m = 0$ è analogo. Se $m = 0$, $M_K \simeq {}^{M}\!/_{\mathfrak{M}M} = 0$, dunque $M = \mathfrak{M}M$. Ma allora, per il lemma di Nakayama, $M = 0$, che è quello che dovevamo dimostrare. □

4.2 Moduli Piatti

Definizione 4.17. Un A-modulo N si dice piatto se per ogni successione esatta corta,

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ è esatta}$$

$$\iff$$

$$0 \to N \otimes_A M' \xrightarrow{id \otimes f} N \otimes_A M \xrightarrow{id \otimes g} N \otimes_A M'' \to 0 \text{ è esatta}$$

I moduli piatti sembrano rivestire lo stesso ruolo dei moduli proiettivi nella teoria del prodotto tensore. Proviamo a ripercorrere la stessa strada e vediamo se riusciamo a ottenere risultati simili.

Lemma 4.18. *N_1, N_2 A-moduli.*

$$N_1 \oplus N_2 \text{ è piatto} \iff N_1, N_2 \text{ sono piatti}$$

Dimostrazione. Supponiamo dapprima che N_1, N_2 siano piatti.

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ è esatta}$$

$$\implies 0 \to N_1 \otimes_A M' \xrightarrow{id \otimes f} N_1 \otimes_A M \xrightarrow{id \otimes g} N_1 \otimes_A M'' \to 0 \text{ è esatta}$$

e anche

$$\implies 0 \to N_2 \otimes_A M' \xrightarrow{id \otimes f} N_2 \otimes_A M \xrightarrow{id \otimes g} N_2 \otimes_A M'' \to 0 \text{ è esatta}$$

Di conseguenza, sommando,

$$0 \to (N_1 \oplus N_2) \otimes_A M' \to (N_1 \oplus N_2) \otimes_A M \to (N_1 \oplus N_2) \otimes_A M'' \to 0 \text{ è esatta}$$

Viceversa, supponiamo che $N_1 \oplus N_2$ sia piatto.

$$0 \to (N_1 \oplus N_2) \otimes_A M' \to (N_1 \oplus N_2) \otimes_A M \to (N_1 \oplus N_2) \otimes_A M'' \to 0 \text{ è esatta}$$

Usando la proprietà distributiva del prodotto tensore rispetto alla somma,

$$0 \to (N_1 \otimes_A M') \oplus (N_2 \otimes_A M') \to$$
$$\to (N_1 \otimes_A M) \oplus (N_2 \otimes_A M) \to (N_1 \otimes_A M'') \oplus (N_2 \otimes_A M'') \to 0 \text{ è esatta}$$

Notando la particolare natura delle mappe, e usando le proprietà della somma diretta si ha allora la tesi. □

Proposizione 4.19. *Sia M un A-modulo libero. Allora M è piatto.*

Dimostrazione. M è libero, dunque $M = \oplus_i A$. Allora,

$$0 \to N_1 \otimes M \to N \otimes M \to N_2 \otimes M \to 0 \text{ è esatta}$$
$$\iff$$
$$0 \to N_1 \otimes (\oplus_i A) \to N \otimes (\oplus_i A) \to N_2 \otimes (\oplus_i A) \to 0 \text{ è esatta}$$
$$\iff$$
$$0 \to \oplus_i (N_1 \otimes A) \to \oplus_i (N \otimes A) \to \oplus_i (N_2 \otimes A) \to 0 \text{ è esatta}$$
$$\iff$$
$$0 \to \oplus_i (N_1) \to \oplus_i (N) \to \oplus_i (N_2) \to 0 \text{ è esatta}$$

e quest'ultima è esatta per ipotesi. □

Proposizione 4.20. *Sia M un A-modulo proiettivo. Allora M è piatto.*

Dimostrazione. Basta ricordare che un modulo proiettivo è addendo diretto di un A-modulo libero, e dunque usare il lemma. □

Capitolo 5

Anelli e Moduli di Frazioni

5.1 Anelli di Frazioni

Definizione 5.1. Sia A un anello. Un sottoinsieme $S \subseteq A$ si dice moltiplicativamente chiuso se:

- $1 \in S$
- $s, t \in S \Rightarrow \ st \in S$

Dato un sottoinsieme moltiplicativo di A, costruiamo un altro anello, detto anello delle frazioni. Muniamo l'insieme $A \times S$ della seguente relazione:

$$(a, s) \sim (b, t) \iff \exists u \in S \ t.c. \ u(at - bs) = 0$$

Lemma 5.2. *$\sim$ è una relazione di equivalenza*

Dimostrazione.

- Riflessività: $(a, s) \sim (a, s) \iff \exists u \in S \ t.c. \ u(at - at) = 0$ e questo è banalmente vero.
- Simmetria: supponiamo $(a, s) \sim (b, t)$; mostriamo che $(b, t) \sim (a, s)$. Per ipotesi, $\exists u \in S \ t.c. \ u(as - bt) = 0 \ \Rightarrow u(bt - as) = 0$, come voluto.
- Transitività: supponiamo $(a, s) \sim (b, t)$ e $(b, t) \sim (c, r)$. Vogliamo mostrare che $(a, s) \sim (c, r)$. Sappiamo che:

  $$\exists u \in S \ t.c. \ u(at - bs) = 0$$
  $$\exists v \in S \ t.c. \ v(br - ct) = 0$$

  Allora:

  $$vru(at - bs) = 0$$
  $$vus(br - ct) = 0$$

  Sommando, si ottiene: $vruat - vusct = 0 \iff vut(ar - sc) = 0$, come voluto, perchè $vut \in S$.

$\square$

Definiamo allora $S^{-1}A := {}^{A \times S}\!/_{\sim}$. Muniamo questo insieme di due operazioni:

$$\frac{a}{s} + \frac{b}{t} = \frac{at + sb}{st} \qquad\qquad \frac{a}{s} + \frac{b}{t} = \frac{ab}{st}$$

Proposizione 5.3. *$S^{-1}A$ è un anello con le operazioni sopra introdotte.*

Dimostrazione. E' sufficiente dimostrare che le operazioni sono ben definite; l'esistenza dell'elemento neutro per somma e prodotto, associatività, distributività e commutatività si ricavano direttamente da quelle di A. Supponiamo $\frac{a}{s} = \frac{a'}{s'}$ e $\frac{b}{t} = \frac{b'}{t'}$. Mostriamo che $\frac{at+sb}{st} = \frac{a't'+s'b'}{s't'}$. Per ipotesi,

$$\begin{aligned} &\exists u \in S \ t.c. \ u(as' - a's) = 0 \\ &\exists v \in S \ t.c. \ v(bt' - b't) = 0 \end{aligned}$$

Da questo segue:

$$\begin{aligned} &uvtt'(as' - a's) = 0 \\ &uvss'(bt' - b't) = 0 \end{aligned}$$

Sommando, si ottiene quanto richiesto. La stessa verifica si può fare per il prodotto. □

Abbiamo un omomorfismo canonico

$$\begin{aligned} f : &A \longrightarrow S^{-1}A \\ &a \longrightarrow \frac{a}{1} \end{aligned}$$

Lemma 5.4. *1.* $S^{-1}A = 0 \iff 0 \in S$

2. *f è iniettiva* $\iff S \cap \mathcal{D}(A) = \emptyset$

Dimostrazione. 1. $0 \in S \Rightarrow \forall a \in A \ \frac{a}{1} = \frac{0}{1}$ per come è definita la relazione di equivalenza.
$S^{-1}A = 0 \Rightarrow \frac{0}{1} = \frac{1}{1} \Rightarrow \exists u \in S \ t.c. \ u1 = 0 \Rightarrow u = 0$

2. $f(a) = 0 \iff \frac{a}{1} = \frac{0}{1} \iff \exists u \in S \ t.c. \ ua = 0 \iff a \in S \cap \mathcal{D}(A)$

□

Caratterizziamo ora l'anello di frazioni $S^{-1}A$ mediante una proprietà universale. Fissato un anello A e un suo sottoinsieme moltiplicativo S, definiamo $\mathcal{C}$ la categoria in cui gli oggetti sono gli anelli e i morfismi sono gli omomorfismi di anelli $f : A \to B$ tali che $f(S) \subseteq B^*$. $S^{-1}A$ risulta essere universale in tale categoria; vale cioè la seguente

Proposizione 5.5. *Sia S un sottoinsieme moltiplicativamente chiuso di un anello A e sia $f : A \to S^{-1}A$ l'omomorfismo canonico. Sia $\varphi : A \to B$ un omomorfismo di anelli tale che $\varphi(S) \subseteq B^*$. Allora $\exists! h : S^{-1}A \to B$ che fa commutare il seguente diagramma:*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "f"'] & B \\ S^{-1}A \arrow[ur, "h"'] & \end{tikzcd}$$

Dimostrazione. Mostriamo che se tale h esiste, è unica. Per commutatività del diagramma,

$$h\Big(\frac{a}{s}\Big) = h\Big(\frac{a}{1}\Big)h\Big(\frac{1}{s}\Big) = h(f(a))h(f(s))^{-1} = \varphi(a)\varphi(s)^{-1}$$

e dunque h è determinata univocamente da φ. Mostriamo ora che tale h è ben definita.

$$\frac{a}{s} = \frac{b}{t} \iff \exists u \in S \ t.c \ u(at - bs) = 0 \Rightarrow \ \varphi(u)(\varphi(a)\varphi(t) - \varphi(b)\varphi(s)) = 0$$

Per ipotesi, $\varphi(u)$ è invertibile in B e dunque

$$\varphi(a)\varphi(t) = \varphi(b)\varphi(s) \Rightarrow \varphi(a)\varphi(s)^{-1} = \varphi(b)\varphi(t)^{-1}$$

come volevasi dimostrare. □

Proposizione 5.6. *Sia $\varphi : A \to B$ che soddisfa:*

1. $\varphi(S) \subseteq B^*$
2. $\varphi(a) = 0 \Rightarrow \exists s \in S \ t.c. \ as = 0$
3. $\forall b \in B \ \exists a \in A \ \exists s \in S \ t.c \ b = \varphi(a)\varphi(s)^{-1}$

$\implies B \simeq S^{-1}A$

Dimostrazione. Per la proposizione precedente, è sufficiente mostrare che l'omomorfismo h che fa commutare il diagramma è iniettiva e surgettiva. Per definizione di h e per il punto (3), h è surgettiva. Sia allora $\frac{a}{s} \in S^{-1}A \ t.c. \ h(\frac{a}{s}) = 0$. Allora $\varphi(a)\varphi(s)^{-1} = 0 \Rightarrow \ \varphi(a) = 0$. Per ipotesi allora, $\exists t \in S \ t.c. \ at = 0 \Rightarrow \frac{a}{s} = \frac{at}{st} = \frac{0}{st} = 0$ da cui l'iniettività. □

Localizzazione Un caso particolare di questo procedimento è rappresentato dalla localizzazione. Sia $P \in Spec(A)$; $S = A \setminus P$ è allora un sottoinsieme moltiplicativamente chiuso. Infatti, $1 \in S$ perchè un ideale primo è proprio per definizione; inoltre, se $x, y \in S \ \Rightarrow x, y \notin P \ \Rightarrow xy \notin P \ \Rightarrow xy \in S$. Definiamo allora $A_P := S^{-1}A$.

Lemma 5.7. *A_P è un anello locale, con ideale massimale $\mathfrak{M} = \{\frac{a}{s} \mid a \in P\}$*

Dimostrazione. Mostriamo che $\mathfrak{M}$ è un ideale.

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \in \mathfrak{M} \qquad \frac{a}{s} \in \mathfrak{M} \ \frac{\alpha}{\beta} \in S^{-1}A \Rightarrow \ \frac{a\alpha}{s\beta} \in \mathfrak{M}$$

Mostriamo ora che ogni elemento non contenuto in $\mathfrak{M}$ è invertibile.
Sia $\frac{a}{s} \notin \mathfrak{M} \ \Rightarrow \ a \in S \Rightarrow \ \frac{s}{a} \in S^{-1}A$ □

Questo lemma ci spinge a cercare di capire meglio che cosa succede agli ideali di A quando vengono estesi in $S^{-1}A$.

Proposizione 5.8.

1. *Ogni ideale di $S^{-1}A$ è l'estensione di un ideale di A.*
2. *$\forall I$ ideale di A $I^{ec} = \cup_{s \in S}(I : s)$*

3. *I è un ideale contratto* $\iff \forall s \in S \;\; s + I \notin \mathcal{D}(A/I)$
4. $\{P \in Spec(A) \mid P \cap S = \emptyset\}$ *è in corrispondenza biunivoca con* $Spec(S^{-1}A)$

Dimostrazione. 1. Sia J un ideale di $S^{-1}A$. Sicuramente $J^{ce} \subseteq J$. Mostriamo il viceversa.

$$\frac{a}{t} \in J \;\Rightarrow\; \frac{t}{1}\frac{a}{t} = \frac{a}{1} \in J \;\Rightarrow\; a \in J^c \;\Rightarrow \frac{a}{t} \in J^{ce}$$

2. Sia $\alpha \in I^{ec}$.

$$f(\alpha) = \frac{\alpha}{1} \in I^e \;\Rightarrow \frac{\alpha}{1} = \frac{a}{s},\; a \in I,\; s \in S$$

Per la definizione della relazione di equivalenza,

$$\exists u \in S \text{ t.c. } u\alpha s = ua \Rightarrow\; ua \in I \;\Rightarrow\; u\alpha s \in I \;\Rightarrow\; \alpha \in (I : us)$$

Viceversa, sia $\alpha \in (I : t)$.

$$\alpha t \in I \;\Rightarrow \frac{\alpha t}{1} \in I^e \;\Rightarrow \frac{\alpha t}{t} \in I^e \;\Rightarrow \frac{\alpha}{1} \in I^e \;\Rightarrow\; \alpha \in I^{ec}$$

3.

$$I = J^c \iff I^{ec} = I \iff \forall s \in S\; \forall \alpha \in (I : s)\; \alpha \in I$$

Nel quoziente allora,

$$\overline{\alpha s} = 0\ (I) \iff \overline{\alpha} = 0\ (I)$$

4. Consideriamo la mappa

$$\begin{aligned} \{P \in Spec(A) \mid P \cap S = \emptyset\} &\longrightarrow Spec(S^{-1}A) \\ P &\longrightarrow S^{-1}P \end{aligned}$$

Mostriamo che tale mappa è ben definita, cioè che $S^{-1}P$ è primo.

$$\frac{a}{s}\frac{b}{t} \in S^{-1}P \;\Rightarrow\; \frac{ab}{st} = \frac{p}{r} \in S^{-1}P \;\Rightarrow\; \exists u \in S\; u(abr - pst) = 0$$

Di conseguenza,

$$urab = upst \in P \;\Rightarrow\; ab \in P \text{ perchè } u, r \in S$$

Mostriamo la surgettività. Dato $Q \in Spec(S^{-1}A)$, $Q^c \in Spec(A)$; bisogna però mostrare che $Q^c \cap S = \emptyset$.

$$s \in Q^c \cap S \;\Rightarrow\; \frac{s}{1} \in Q \;\Rightarrow\; \frac{s}{1}\frac{1}{s} \in Q \;\Rightarrow 1 \in Q$$

e questo è assurdo. Mostriamo l'iniettività. Supponiamo $S^{-1}P_1 = S^{-1}P_2$; mostriamo che $P_1 = P_2$.

$$a \in P_1 \;\Rightarrow\; \frac{a}{1} \in S^{-1}P_1 = S^{-1}P_2 \;\Rightarrow\; \frac{a}{1} = \frac{b}{t} \quad b \in P_2$$

Come al solito, per la definizione della relazione di equivalenza,

$$uat - ub = 0 \;\Rightarrow uat = ub \in P_2 \Rightarrow a \in P_2 \;\Rightarrow\; P_1 \subseteq P_2$$

Allo stesso modo, si mostra l'altra inclusione.

□

5.2 Moduli di frazioni

La costruzione descritta per gli anelli può essere generalizzata al caso di un modulo. Dato S sottoinsieme moltiplicativo di A, definiamo la seguente relazione su $M \times S$:

$$(m,s) \sim (n,t) \iff \exists u \in S \ t.c \ u(mt - sn) = 0$$

Come prima, si verifica che questa è una relazione di equivalenza e l'insieme ottenuto, che chiamiamo $S^{-1}M$ può essere dotato della struttura di $S^{-1}A$-modulo:

$$\frac{m}{s}, \frac{n}{t} \in S^{-1}M \ \Rightarrow \ \frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st}$$
$$\frac{a}{s} \in S^{-1}A \ \ \frac{m}{t} \in S^{-1}M \ \Rightarrow \ \frac{a}{s}\frac{m}{t} = \frac{am}{st}$$

La teoria può essere sviluppata in maniera analoga a quanto fatto per gli anelli; una proprietà rilevante di queste strutture riguarda le mappe di A-moduli.

Lemma 5.9. *Siano M,N A-moduli e sia $\varphi : M \to N$ un omomorfismo di A-moduli$\Rightarrow$ φ induce un omomorfismo di $S^{-1}A$-moduli*

$$s^{-1}\varphi : S^{-1}M \longrightarrow S^{-1}N$$
$$\frac{m}{s} \longrightarrow \frac{\varphi(m)}{s}$$

Dimostrazione. Mostriamo che l'omomorfismo è ben definito.

$$\frac{m}{s} = \frac{n}{t} \ \Rightarrow \ \exists u \in S \ t.c. \ u(mt - ns) = 0$$

Sfruttando il fatto che φ è un omomorfismo di A-moduli, si ottiene:

$$\varphi(u(mt - ns)) = 0 \iff u(t\varphi(m) - s\varphi(n)) = 0 \iff \frac{\varphi(m)}{s} = \frac{\varphi(n)}{t}$$

□

Corollario 5.10. *Siano M,N,P A-moduli, $\varphi : M \to N$ e $\psi : N \to P$ omomorfismi di A-moduli $\Rightarrow$ $s^{-1}(\psi \circ \varphi) = s^{-1}\psi \circ s^{-1}\varphi$*

Questo semplice risultato ci induce a indagare il comportamento dei moduli di frazioni rispetto a una successione esatta.

Proposizione 5.11. *Sia*

$$M \xrightarrow{\varphi} N \xrightarrow{\psi} P$$

una successione esatta di A-moduli e sia S un sottoinsieme moltiplicativamente chiuso. Allora la successione

$$S^{-1}M \xrightarrow{s^{-1}\varphi} S^{-1}N \xrightarrow{s^{-1}\psi} S^{-1}P$$

è esatta

Dimostrazione. Mostriamo che $\mathrm{Im}(s^{-1}\varphi) = \mathrm{Ker}(s^{-1}\psi)$.

- $\mathrm{Im}(s^{-1}\varphi) \subseteq \mathrm{Ker}(s^{-1}\psi)$

$$\psi \circ \varphi = 0 \ \Rightarrow \ s^{-1}\psi \circ s^{-1}\varphi = 0 \ \Rightarrow \mathrm{Im}(s^{-1}\varphi) \subseteq \mathrm{Ker}(s^{-1}\psi)$$

- $\mathrm{Im}(s^{-1}\varphi) \supseteq \mathrm{Ker}(s^{-1}\psi)$

  $$\frac{n}{s} \in \mathrm{Ker}(s^{-1}\psi) \;\Rightarrow\; \frac{\psi(n)}{s} = \frac{0}{1} \;\Rightarrow\; \exists u \in S \text{ t.c. } u\psi(n) = \psi(un) = 0$$

  Per l'esattezza della successione, allora,

  $$un \in \mathrm{Im}(\varphi) = \mathrm{Ker}(\psi) \;\Rightarrow\; \exists m \in M \text{ t.c. } \varphi(m) = un$$

  A questo punto,

  $$\frac{n}{s} = \frac{un}{us} = \frac{\varphi(m)}{us} = s^{-1}\varphi\Big(\frac{m}{us}\Big)$$

□

Corollario 5.12. *M,N A-moduli, $N \subset M \;\Rightarrow\; S^{-1}N \hookrightarrow S^{-1}M$ in modo canonico.*

Il corollario ci porta allora a vedere come si comportano i sottomoduli e le operazioni più comuni tra di loro.

Proposizione 5.13. *M,N,P A-moduli. $M, N \subset P$*

1. $S^{-1}(M+N) = S^{-1}M + S^{-1}N$
2. $S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N$
3. $S^{-1}(P/M) \simeq S^{-1}P/S^{-1}M$

Dimostrazione. 1. Mostriamo che $S^{-1}(M+N) \subseteq S^{-1}M + S^{-1}N$

$$\alpha \in S^{-1}(M+N) \;\Rightarrow\; \alpha = \frac{m+n}{s} = \underbrace{\frac{m}{s}}_{\in S^{-1}M} + \underbrace{\frac{n}{s}}_{\in S^{-1}N}$$

Viceversa,

$$\alpha \in S^{-1}M + S^{-1}N \;\Rightarrow\; \alpha = \frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st} \in S^{-1}(M+N)$$

2.

$$a \in S^{-1}(M \cap N) \;\Rightarrow\; a = \frac{m}{s}\; m \in M \cap N \;\Rightarrow \frac{m}{s} \in S^{-1}M \cap S^{-1}N$$

Viceversa,

$$a \in S^{-1}M \cap S^{-1}N \;\Rightarrow\; a = \frac{m}{s} = \frac{n}{t}\; m \in M \;\; n \in N$$

Per la definizione della relazione di equivalenza,

$$\exists u \in S \text{ t.c. } u(mt - ns) = 0 \;\Rightarrow\; umt = uns \in M \cap N$$

Da questo segue

$$\frac{m}{s} = \frac{utm}{uts} = \frac{uns}{uts} \in S^{-1}(M \cap N)$$

3. Consideriamo la successione esatta $0 \to M \xrightarrow{f} P \xrightarrow{g} P/M \to 0$ Allora $0 \to S^{-1}M \xrightarrow{s^{-1}f} S^{-1}P \xrightarrow{s^{-1}g} S^{-1}(P/M) \to 0$ è esatta. Definiamo la successione

$$0 \to S^{-1}M \xrightarrow{\tilde{f}} S^{-1}P \xrightarrow{\tilde{g}} S^{-1}P/S^{-1}M \to 0$$

dove $\tilde{g}$ è la funzione definita da:

$$\begin{aligned} \tilde{g}\colon S^{-1}P &\longrightarrow S^{-1}P/S^{-1}M \\ \frac{p}{s} &\longrightarrow \frac{p}{s} + S^{-1}M \end{aligned}$$

Definisco allora

$$\begin{aligned} \gamma\colon S^{-1}(P/M) &\longrightarrow S^{-1}P/S^{-1}M \\ \frac{p+M}{s} &\longrightarrow \frac{p}{s} + S^{-1}M \end{aligned}$$

$$\begin{tikzcd} 0 \arrow[r] & S^{-1}M \arrow[r, "s^{-1}f"] \arrow[d, "\alpha"'] & S^{-1}P \arrow[r, "s^{-1}g"] \arrow[d, "\beta"'] & S^{-1}(M/P) \arrow[r] \arrow[d, "\gamma"'] & 0 \\ 0 \arrow[r] & S^{-1}M \arrow[r, "\tilde{f}"'] & S^{-1}P \arrow[r, "\tilde{g}"'] & S^{-1}P/S^{-1}M \arrow[r] & 0 \end{tikzcd}$$

Per il lemma dei cinque, utilizzando $\alpha = id_{S^{-1}M}$ e $\beta = id_{S^{-1}P}$ si ha $S^{-1}(P/M) \simeq S^{-1}P/S^{-1}M$

□

I moduli di frazioni possono essere visti come un'estensione degli scalari che possono agire sugli elementi del modulo; visto che anche il prodotto tensore agiva similarmente, è opportuno sperare che esistano delle connessioni tra le due strutture. In effetti,

Proposizione 5.14. $S^{-1}M \simeq S^{-1}A \otimes_A M$

Dimostrazione. Definiamo:

$$\begin{aligned} f\colon M \times S^{-1}A &\longrightarrow S^{-1}M \\ (m, \frac{a}{s}) &\longrightarrow \frac{am}{s} \end{aligned}$$

f è bilineare, dunque dalla proprietà universale del prodotto tensore,

$$\begin{aligned} \exists!\varphi\colon M \otimes S^{-1}A &\longrightarrow S^{-1}M \\ m \otimes \frac{a}{s} &\longrightarrow \frac{am}{s} \end{aligned}$$

φ è surgettiva perchè f lo è. Mostriamo l'iniettività.

$$\alpha \in S^{-1}A \otimes M \;\Rightarrow\; \alpha = \sum_i m_i \otimes \frac{a_i}{s_i}$$

Sia $s = \prod s_i$ e sia $t_i = \dfrac{s}{s_i}$.

$$\alpha = \sum_i \frac{a_i t_i}{t_i s_i} \otimes m_i = \frac{1}{s} \otimes n$$

Con questa forma più comoda, mostriamo che $\operatorname{Ker} \varphi = \{0\}$.

$$\varphi(\frac{1}{s} \otimes m) = 0 \;\Rightarrow\; \frac{m}{s} = \frac{0}{1} \;\Rightarrow\; \exists u \in S \text{ t.c. } um = 0$$

Da quest'ultima uguaglianza,

$$\frac{1}{s} \otimes m = \frac{u}{us} \otimes m = \frac{1}{us} \otimes um = 0 \;\Rightarrow\; \operatorname{Ker} \varphi = \{0\}$$

□

Proposizione 5.15. *$S^{-1}A$ è un A-modulo piatto*

Dimostrazione. Sia $0 \to M \xrightarrow{f} N$ una successione esatta. Vale che

$$0 \to M \otimes_A S^{-1}A \xrightarrow{f \otimes id} N \otimes_A S^{-1}A \text{ esatta} \iff 0 \to S^{-1}M \xrightarrow{s^{-1}f} S^{-1}N \text{ esatta}$$

e quest'ultima è esatta per quanto mostrato prima. □

Proposizione 5.16. *Siano M, N A-moduli, $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso.*

$$\implies S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq S^{-1}(M \otimes_A N)$$

Dimostrazione.

$$\begin{aligned} S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq & S^{-1}M \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \simeq \\ \simeq (S^{-1}M \otimes_{S^{-1}A} S^{-1}A) \otimes_A N \simeq & S^{-1}M \otimes_A N \simeq \\ \simeq (S^{-1}A \otimes_A M) \otimes_A N \simeq & S^{-1}A \otimes_A (M \otimes_A N) \simeq S^{-1}(M \otimes_A N) \end{aligned}$$

□

Corollario 5.17.

$$M_P \otimes_A N_P \simeq (M \otimes_A N)_P$$

Corollario 5.18.

$$S^{-1}(M \oplus N) \simeq S^{-1}M \oplus S^{-1}N$$

Dimostrazione.

$$S^{-1}(M \oplus N) \simeq S^{-1}A \otimes_A (M \oplus N) \simeq S^{-1}M \oplus S^{-1}N$$

per distributività del prodotto tensore rispetto alla somma diretta.

□

5.3 Proprietà locali

Definizione 5.19. Sia M un A-modulo. Una proprietà $\mathcal{P}$ si dice locale se

$$M \textit{ soddisfa } \mathcal{P} \iff M_P \textit{ soddisfa } \mathcal{P}\ \forall P \in Spec(A)$$

E' chiaro che allora tali proprietà diventano centrali nella teoria della localizzazione; verificare alcune proprietà su un anello locale è spesso più semplice che controllarle sull'anello di partenza.

Proposizione 5.20. *Sia M un A-modulo. Sono equivalenti:*

1. $M = 0$
2. $M_P = 0\ \forall P \in Spec(A)$
3. $M_{\mathfrak{M}} = 0\ \forall \mathfrak{M} \in SpecM(A)$

Dimostrazione. Chiaramente è sufficiente mostrare che (3) $\Rightarrow$ (1). Supponiamo per assurdo che $M \neq 0$. Allora

$$\exists m \in M \textit{ t.c. } \mathrm{Ann}(m) \neq A \Rightarrow \exists \mathfrak{M} \in SpecM(A) \textit{ t.c. } \mathrm{Ann}(m) \subseteq \mathfrak{M}$$

Poichè $\mathfrak{M}$ è massimale, possiamo usare l'ipotesi e dunque

$$M_{\mathfrak{M}} = 0 \Rightarrow \frac{m}{1} = \frac{0}{1} \Rightarrow \exists u \in S = A \setminus \mathfrak{M} \textit{ t.c. } um = 0$$

Notando allora che per quanto detto, $u \notin \mathrm{Ann}(m)$, si ha un assurdo.

□

Corollario 5.21. *Sia $\varphi\colon M \to N$ un omomorfismo di A-moduli. Sono equivalenti:*

1. *φ iniettivo*
2. *$\varphi_P\colon M_P \to N_P$ iniettivo $\forall P \in Spec(A)$*
3. *$\varphi_{\mathfrak{M}}\colon M_{\mathfrak{M}} \to N_{\mathfrak{M}}$ iniettivo $\forall \mathfrak{M} \in SpecM(A)$*

Dimostrazione. In virtù della proposizione precedente, è sufficiente dimostrare che $S^{-1}(\mathrm{Ker}\,\varphi) = \mathrm{Ker}\, s^{-1}\varphi$.

$$\frac{a}{s} \in \mathrm{Ker}\, s^{-1}\varphi \Rightarrow \frac{\varphi(a)}{s} = \frac{0}{1} \Rightarrow \exists u \in S \textit{ t.c. } \varphi(au) = 0 \Rightarrow au \in \mathrm{Ker}\,\varphi$$

Di conseguenza,

$$\frac{a}{s} = \frac{au}{su} \in S^{-1}(\mathrm{Ker}\,\varphi)$$

Viceversa,

$$\frac{a}{s} \in S^{-1}(\mathrm{Ker}\,\varphi) \Rightarrow s^{-1}\varphi\left(\frac{a}{s}\right) = \frac{\varphi(a)}{s} = \frac{0}{1} \Rightarrow \frac{a}{s} \in \mathrm{Ker}\, s^{-1}\varphi$$

□

Corollario 5.22. *Sia $\varphi\colon M \to N$ un omomorfismo di A-moduli. Sono equivalenti:*

1. *φ surgettivo*
2. *$\varphi_P \colon M_P \to N_P$ surgettivo $\forall P \in Spec(A)$*
3. *$\varphi_{\mathfrak{M}} \colon M_{\mathfrak{M}} \to N_{\mathfrak{M}}$ surgettivo $\forall \mathfrak{M} \in SpecM(A)$*

Dimostrazione. Basta applicare la proposizione 5.20 a $\mathrm{Coker}(\varphi)$ □

Corollario 5.23. *Sono fatti equivalenti:*

1. *M piatto*
2. *M_P piatto $\forall P \in Spec(A)$*
3. *$M_{\mathfrak{M}}$ piatto $\forall \mathfrak{M} \in SpecM(A)$*

Dimostrazione. Chiaramente se M è piatto, $M_P = S^{-1}A \otimes_A M$ è piatto perchè il prodotto tensore di moduli piatti è piatto. Dunque basta mostrare che (3) $\Rightarrow$ (1). Sia $0 \to N' \xrightarrow{f} N$ esatta. Bisogna mostrare che $0 \to N' \otimes_A M \xrightarrow{f \otimes id} N \otimes_A N$ è esatta. A questo punto, basta allora applicare la proposizione 5.20 a $Ker(f \otimes id)$ per ottenere la tesi. □

Lemma 5.24. *Sia A un anello, sia S un sottoinsieme moltiplicativamente chiuso e sia I un ideale di A.*

$$S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$$

Dimostrazione. Basta ricordare che $\sqrt{I} = \bigcap_{P \supseteq I, P \in Spec(A)} P$ e dunque invocare la corrispondenza tra gli ideali di $S^{-1}A$ e A. □

Proposizione 5.25. *Sono fatti equivalenti:*

1. *M ridotto*
2. *M_P ridotto $\forall P \in Spec(A)$*
3. *$M_{\mathfrak{M}}$ ridotto $\forall \mathfrak{M} \in SpecM(A)$*

Dimostrazione. In virtù del lemma e della proposizione precedente,

$$\mathfrak{N}(A) = 0 \iff (\mathfrak{N}(A))_{\mathfrak{M}} = 0 \ \forall \mathfrak{M} \in SpecM(A) \iff \mathfrak{N}(A_{\mathfrak{M}}) = 0 \ \forall \mathfrak{M}$$

□

Osservazione 5.26. L'essere un dominio non è una proprietà locale. Basta considerare $A = \mathbb{Z} \times \mathbb{Z}$ e considerare $S = A \setminus (P \times \mathbb{Z})$. A non è un dominio ma il localizzato si.

Osservazione 5.27. L'essere un anello noetheriano non è una proprietà locale. Sia infatti

$$A = {}^{\mathbb{F}_2[x_1, x_2 \cdots]}\!/_{I} \qquad\qquad I = (x_i^2 - x_i \ \forall i \in \mathbb{N})$$

Sicuramente A non è noetheriano. Sia però $\mathfrak{M}$ un ideale massimale. Allora $A_{\mathfrak{M}}$ è un anello locale; dalla definizione di I e dal fatto che siamo su un campo a caratteristica 2 si ha però che ogni elemento è idempotente. In un anello locale, però, gli unici elementi idempotenti sono $0, 1$; da questo segue che $A_{\mathfrak{M}} = \mathbb{F}_2$ che chiaramente è noetheriano.

5.4 Esercizi e Complementi

Proposizione 5.28. *Sia A un anello.*

$$\mathfrak{N}(A) = \bigcap_{P \in Spec(A)} P$$

Dimostrazione. Sia $x \in \mathfrak{N}(A)$. Allora $x^n = 0 \in \bigcap_{P \in Spec(A)} \Rightarrow x \in \bigcap_{P \in Spec(A)}$ Viceversa, sia $x \notin \mathfrak{N}(A)$. Allora il sottoinsieme moltiplicativo $S = \{x^n\}$ non contiene lo 0, dunque $S^{-1}A \neq 0$. Di conseguenza, esiste un ideale massimale di $S^{-1}A$ la cui contrazione non contiene x. Ma la contrazione di un ideale primo è un ideale primo. □

Osservazione 5.29. Formalizziamo ora il trucco di Rabinowitsch, utilizzato nella dimostrazione della forma forte del Nullstellensatz. Arrivati all'uguaglianza

$$1 = \sum_{i=1}^{s} a_i(x,t)g_i(x) + h(x,t)(1 - tf)$$

si vorrebbe porre $t = \frac{1}{f}$. Per rendere rigoroso questo passaggio, è sufficiente considerare l'insieme moltiplicativamente chiuso $S = \{f^n \mid n \in \mathbb{N}\}$ e ripetere i passaggi della dimostrazione nell'anello delle frazioni $S^{-1}A$. Arrivati a

$$\frac{f^k}{1} = \sum_{i=1}^{s} \frac{\overline{a}_i(x)}{1} \frac{g_i(x)}{1}$$

ricordando che A è un dominio e $S \cap \mathcal{D}(A) = \emptyset$ (e dunque la mappa da A in $S^{-1}A$ è iniettiva), si ottiene l'uguaglianza in A.

Ci chiediamo ora se esiste una sorta di corrispondenza tra i possibili sottoinsiemi moltiplicativi di A e gli anelli di frazioni. La risposta è negativa; vale infatti il seguente:

Lemma 5.30. *Siano S, T sottoinsiemi moltiplicativamente chiusi, $S \subseteq T$. Sia*

$$\begin{aligned} f \colon S^{-1}A &\to T^{-1}A \\ \frac{a}{s} &\to \frac{a}{s} \end{aligned}$$

Allora f è un isomorfismo $\iff \forall t \in T \ \frac{t}{1} \in (S^{-1}A)^*$

Dimostrazione. Supponiamo che f sia un isomorfismo. Sia $t \in T$. Per surgettività, allora,

$$\exists \frac{a}{s} \in S^{-1}A \text{ t.c. } \frac{1}{t} = f\left(\frac{a}{s}\right) \Rightarrow \ f\left(\frac{at}{s}\right) = \frac{t}{1} f\left(\frac{a}{s}\right) = 1$$

Poichè f è un isomorfismo, in particolare è iniettiva, e dunque

$$\frac{t}{1} f\left(\frac{a}{s}\right) = 1 \ \Rightarrow \ \frac{t}{1} \in (S^{-1}A)^*$$

Viceversa, supponiamo ora che $\forall t \in T$ $\frac{t}{1} \in (S^{-1}A)^*$ e mostriamo che f è un isomorfismo. Mostriamo prima la surgettività.

$$\frac{b}{t} \in T^{-1}A \Rightarrow \frac{b}{t} = \frac{1}{t}\frac{b}{1} = \left(\frac{t}{1}\right)^{-1} f\left(\frac{b}{1}\right) = f\left(\frac{b}{1}\left(\frac{t}{1}\right)^{-1}\right)$$

Mostriamo ora l'iniettività.

$$f\left(\frac{a}{s}\right) = 0 \Rightarrow \exists u \in T \text{ t.c. } ta = 0 \Rightarrow \frac{a}{s} = \frac{a}{s}\frac{t}{1}\left(\frac{t}{1}\right)^{-1} = 0$$

□

Più in particolare, assume interesse lavorare con i sottoinsiemi moltiplicativi più semplici tra tutti quelli che generano lo stesso anello delle frazioni.

Definizione 5.31. Un sottoinsieme moltiplicativamente chiuso si dice saturato se $xy \in S \Rightarrow x \in S \ \wedge y \in S$

Proposizione 5.32.

$$S \text{ è saturato} \iff \exists \{P_i\}_i \text{ ideali primi t.c. } S = A \setminus \bigcup_i P_i$$

Dimostrazione. Supponiamo dapprima che S sia il complementare dell'unione di primi. Allora

$$xy \in S \Rightarrow xy \notin P_i \ \forall i = 1 \cdots n \Rightarrow x, y \notin P_i \ \forall i = 1 \cdots n \Rightarrow x, y \in S$$

Viceversa, sia $\Sigma = \{P \in Spec(A) \mid P \cap S = \emptyset\}$ e sia $B = \cup_{P \in \Sigma} P$. Se $x \in \bigcup P_i$, allora chiaramente $x \notin S$.
Per mostrare l'altra inclusione, sia $x \in B \setminus \bigcup P_i$. Chiaramente se $x \in A^*$, allora $\exists y \in A$ *t.c.* $xy = 1 \in S$ e dunque per definizione di saturato $x \in S$. Se invece $x \notin A^*$, supponiamo per assurdo che $x \notin S$. Allora x genera un ideale proprio che non interseca S; allora esiste un ideale massimale $\mathfrak{M}$ di $S^{-1}A$ che contiene $(x)^e$. Di conseguenza, $\mathfrak{M}^c \supset (x)$, ma il contratto di un massimale è primo. Siamo allora arrivati a un assurdo, perchè avevamo supposto $x \in B$. □

Proposizione 5.33. *Sia A un dominio, e siano $P_1, \cdots P_r \in Spec(A)$, con $P_i \not\subset P_j$ $\forall i \neq j$. Detto $Q(A) = (A \setminus \mathcal{D}(A))^{-1}A$, si ha:*

$$Q\left(A/P_1 \cap \cdots \cap P_r\right) = Q\left(A/P_1\right) \times \cdots Q\left(A/P_r\right)$$

Dimostrazione. Per semplicità di notazione, denotiamo con B l'anello $A/\bigcap_i P_i$. I divisori di zero di B sono gli elementi appartenenti alle immagini dei primi nel quoziente. Mostriamolo per doppia inclusione.

$$x \in P_i \Rightarrow \forall i = 1 \cdots r \ \exists x_i \in P_i \setminus \bigcup_{\substack{j=1 \\ j \neq i}}^{r} P_i \Rightarrow x(x_1 x_2 \cdots x_{r-1}) \in \bigcap_{i=1}^{r} P_i$$

Viceversa, sia

$$(\overline{xy} = 0) \wedge (\overline{y} \neq 0) \Rightarrow xy \in P_i \ \forall i = 1 \cdots r \Rightarrow \exists i \text{ t.c. } x \in P_i$$

e dunque abbiamo ottenuto l'uguaglianza cercata. Di conseguenza, otteniamo

$$S = B \setminus (\pi(P_1) \cup \pi(P_2) \cup \cdots \pi(P_r) \text{ e } Q(A) = S^{-1}B$$

Vorremmo applicare il teorema cinese del resto; ma per far questo dobbiamo mostrare che $S^{-1}(\pi(P_i)) + S^{-1}(\pi(P_j)) = S^{-1}B$ Per questo, mostriamo che tali ideali sono massimali. Sia $S^{-1}I \in S^{-1}B$ un ideale massimale.

$$I \cap S = \emptyset \Rightarrow (S^{-1}I)^c \subseteq \bigcup_{i=1}^{r} P_i \overset{Scansamento}{\Longrightarrow} \exists i \text{ t.c. } (S^{-1}I)^c \subseteq \pi(P_i)$$

da cui la massimalità dei primi P_i ri-estendendo gli ideali. Possiamo allora applicare il teorema cinese del resto, ottenendo:

$$S^{-1}B \simeq \prod_{i=1}^{r} {Q(B)}/{S^{-1}(\pi(P_i))} \simeq \prod_{i=1}^{r} Q\left({B}/{\pi(P_i)}\right)$$

□

Proposizione 5.34. *Sia M un A-modulo finitamente generato. Allora*

$$S^{-1}(\mathrm{Ann}(M)) = \mathrm{Ann}(S^{-1}M)$$

Dimostrazione. Mostriamo la tesi per induzione sul numero di generatori di M. Supponiamo dapprima $M = \langle m \rangle$.

$$0 \to \mathrm{Ann}(M) \to A \to M \to 0 \text{ è esatta}$$
$$\Rightarrow\ 0 \to S^{-1}(\mathrm{Ann}(M)) \to S^{-1}A \to S^{-1}M \to 0 \text{ è esatta}$$

Notiamo però che anche la successione

$$0 \to \mathrm{Ann}(S^{-1}M) \to S^{-1}A \to S^{-1}M \to 0 \text{ è esatta}$$

In quanto nuclei dello stesso omomorfismo, $\mathrm{Ann}(S^{-1}M) \simeq S^{-1}(\mathrm{Ann}(M))$ Mostriamo ora che se la tesi vale per M, N A-moduli finitamente generati, vale anche per $M + N$.

$$S^{-1}(\mathrm{Ann}(M+N)) = S^{-1}(\mathrm{Ann}(M) \cap \mathrm{Ann}(N)) =$$
$$\overset{hp\ ind}{=} \mathrm{Ann}(S^{-1}M) \cap \mathrm{Ann}(S^{-1}N) = \mathrm{Ann}(S^{-1}(M+N))$$

□

Osservazione 5.35. Nel caso di un modulo non finitamente generato, non vale l'uguaglianza. Sia infatti $A = \mathbb{K}[x]$ e sia $p_i(x)$ una famiglia numerabile di polinomi irriducibili con termine noto diverso da 0.
Sia M il modulo $\langle m_i \mid p_i m_i = 0 \rangle$ (abbiamo indicato le relazioni tra i generatori). Allora $\mathrm{Ann}(M) = (0)$ e dunque $S^{-1}(\mathrm{Ann}(M)) = 0$. Localizzando per l'ideale generato da x invece, si ha $S^{-1}M = 0$ perchè
$\forall i\ p_i(x) \notin (x)$ e dunque $\mathrm{Ann}(M) = A_{(x)}$.

Grazie a questa proposizione possiamo ottenere un criterio che ci aiuti a dire se un prodotto tensore sia nullo.

Teorema 5.36. *Siano M, N A moduli finitamente generati.*

$$M \otimes_A N = 0 \iff \mathrm{Ann}(M) + \mathrm{Ann}(N) = A$$

Dimostrazione. Supponiamo dapprima che $\mathrm{Ann}(M) + \mathrm{Ann}(N) = A$. Allora $\exists a \in \mathrm{Ann}(M)$ $\exists b \in \mathrm{Ann}(N)$ *t.c.* $a + b = 1$. Di conseguenza,

$$m \otimes n = 1(m \otimes n) = (a + b)(m \otimes n) = (am) \otimes n + m \otimes (bn) = 0$$

e dunque $M \otimes_A N = 0$.
Viceversa, supponiamo per assurdo che $\mathrm{Ann}(M) + \mathrm{Ann}(N) = I \subsetneq A$. Allora $\exists \mathfrak{M} \in SpecM(A)$ *t.c.* $I \subseteq \mathfrak{M}$. Consideriamo allora la localizzazione $A_{\mathfrak{M}}$.

$$\begin{aligned} \mathrm{Ann}(M_{\mathfrak{M}}) &= \mathrm{Ann}(M)_{\mathfrak{M}} \neq A_{\mathfrak{M}} \\ \mathrm{Ann}(N_{\mathfrak{M}}) &= \mathrm{Ann}(N)_{\mathfrak{M}} \neq A_{\mathfrak{M}} \end{aligned}$$

Di conseguenza, i due moduli localizzati sono non nulli. Dunque,

$$N_{\mathfrak{M}} \otimes_{A_{\mathfrak{M}}} M_{\mathfrak{M}} = 0 \Rightarrow {}^{A_{\mathfrak{M}}}\!/_{\mathfrak{M}} \otimes_{A_{\mathfrak{M}}} N_{\mathfrak{M}} \otimes_{A_{\mathfrak{M}}} M_{\mathfrak{M}} = 0$$

Dai lemmi sul prodotto tensore, si ottiene allora

$${}^{N_{\mathfrak{M}}}\!/_{\mathfrak{M}N_{\mathfrak{M}}} \otimes_{A_{\mathfrak{M}}} {}^{M_{\mathfrak{M}}}\!/_{\mathfrak{M}M_{\mathfrak{M}}} = 0$$

che, poichè siamo su un anello locale, implica che uno dei due moduli deve essere nullo. Per il lemma di Nakayama allora vale $N_{\mathfrak{M}} = 0 \vee M_{\mathfrak{M}} = 0$, contro quanto affermato in precedenza. Siamo allora arrivati a un assurdo e dunque doveva valere $\mathrm{Ann}(M) + \mathrm{Ann}(N) = A$. $\square$

Capitolo 6

Moduli Noetheriani e Artiniani

6.1 Definizioni e prime proprietà

E' chiaro che per molti risultati riguardanti gli anelli e i moduli siano necessarie ipotesi di finita generatezza. Cerchiamo allora di approfondire lo studio di anelli e moduli che hanno questi requisiti.

Definizione 6.1. Sia M un A-modulo. M si dice Noetheriano se ogni catena ascendente di sottomoduli è stazionaria.

Vale la seguente proposizione di teoria degli insiemi che semplifica le dimostrazioni.

Proposizione 6.2. *Sia $(\Sigma, \leq)$ un insieme parzialmente ordinato. Sono equivalenti:*

1. *Ogni catena ascendente di Σ è stazionaria*
2. *Ogni sottoinsieme non vuoto di Σ ammette un elemento massimale.*

Dimostrazione. (1) $\Rightarrow$ (2)
Supponiamo che $A \subseteq \Sigma$ non ammetta un elemento massimale. Sia $x \in A$ e sia f una funzione di scelta sui sottoinsiemi non vuoti di A. Definisco allora:

$$\begin{cases} a_0 = x \\ a_i = f\left(\{a \in A \mid a > a_{i-1}\}\right) \end{cases}$$

La funzione è ben definita perchè per ipotesi A non ammette elemento massimale. L'immagine della funzione forma una catena ascendente non stazionaria. (2) $\Rightarrow$ (1) Sia $A_1 \leq A_2 \leq A_3 \dots$ una catena ascendente. L'insieme $\{A_i\}$ ammette un elemento massimale $A_{\bar{n}} \;\Rightarrow\; \forall i \geq \bar{n}\; A_i = A_{\bar{n}}$ $\square$

Esempio. $\mathbb{Z}$ è uno $\mathbb{Z}$-modulo noetheriano, mentre $\mathbb{K}[x_1, x_2, \dots]$ non lo è.

Proposizione 6.3. *Sia M un A-modulo.*

$$M \text{ è noetheriano} \iff \forall N \subseteq M \;\; N \text{ è finitamente generato}$$

Dimostrazione. Supponiamo che M sia un A-modulo noetheriano. Sia N un sottomodulo di M e sia $X = \{P \subseteq N \mid \text{P è finitamente generato}\}$.

$$(0) \in X \Rightarrow X \neq \emptyset \Rightarrow \ \exists N_0 \text{ massimale in A}$$

Supponiamo per assurdo che $N \neq N_0$. Allora esiste $n \in N \setminus N_0$

$$N_0 \subsetneq N_0 + \langle n \rangle = N_1 \subseteq N$$

Ciò nega la massimalità di N_0, dunque $N = N_0$ e dunque N è finitamente generato. Viceversa, sia $M_0 \subseteq M_1 \dots$ una catena ascendente in M.

$$\tilde{M} := \bigcup M_i \text{ è finitamente generato} \Rightarrow \ \tilde{M} = \langle m_1, m_2 \dots, m_n \rangle$$

Di conseguenza,

$$\exists \bar{n} \in \mathbb{N} \ t.c. \ \{m_1, m_2 \dots, m_n\} \subseteq M_{\bar{n}} \Rightarrow \ M_{\bar{n}} = \tilde{M} \Rightarrow \forall n \geq \bar{n} \ M_n = M_{\bar{n}}$$

□

Indaghiamo ora il comportamento delle funzioni su moduli noetheriani.

Teorema 6.4. *Siano M,N,P A-moduli e sia*

$$0 \to N \xrightarrow{f} M \xrightarrow{g} P \to 0$$

una successione esatta. Vale allora

$$M \text{ è noetheriano} \iff N, P \text{ sono noetheriani}$$

Dimostrazione. ($\Rightarrow$) Supponiamo dapprima che M sia noetheriano. Sia $N_0 \subseteq N_1 \dots$ una catena ascendente di sottomoduli di N. Allora $f(N_0) \subseteq f(N_1) \dots$ è una catena ascendente in M, dunque stazionaria. Per iniettività di f, la catena è stazionaria anche in N e dunque N è noetheriano. Sia ora $P_0 \subseteq P_1 \dots$ una catena ascendente in P. Allora $g^{-1}(P_0) \subseteq g^{-1}(P_1) \dots$ è una catena ascendente di M, dunque è stazionaria. Di conseguenza, $g(g^{-1}(P_0)) = P_0 \subseteq g(g^{-1}(P_1)) = P_1 \dots$ è stazionaria, e anche P è noetheriano.

($\Leftarrow$) Mostriamo ora l'altra implicazione; supponiamo cioè che N e P siano noetheriani e mostriamo che M è noetheriano. Sia $M_0 \subseteq M_1 \dots$ una catena ascendente in M. Definiamo:

$$N_i = f^{-1}(f(N) \cap M_i) \qquad\qquad P_i = g(M_i)$$

La catena degli N_i è stazionaria, dunque $\exists n_1 \in \mathbb{N}$ *t.c.* $\forall n \geq n_1 \ N_n = N_{n_1}$. La catena dei P_i è stazionaria, dunque $\exists n_2 \in \mathbb{N}$ *t.c.* $\forall n \geq n_2 \ P_n = P_{n_2}$. Sia allora $n = max\{n_1, n_2\}$ e sia $i \geq n$. Definiamo la successione

$$0 \to N_i \xrightarrow{f_i} M_i \xrightarrow{g_i} P_i \to 0$$

dove $g_i = g|_{M_i}$ e $f_i = f|_{N_i}$. Sicuramente dunque f_i è iniettiva e g_i è surgettiva. Mostriamo che la successione è esatta in M_i.

$$g_i \circ f_i = g|_{M_i} \circ f|_{N_i} = 0 \Rightarrow \ \mathrm{Im}(f_i) \subseteq \mathrm{Ker}\, g_i$$

Sia ora $m_i \in \operatorname{Ker} g_i$.

$$m_i \in \operatorname{Ker} g_i \subseteq \operatorname{Ker} g = \operatorname{Im}(f) \Rightarrow \ \exists n \in N \ t.c. \ f(n) = m_i \in M_i \Rightarrow n \in N_i$$

Dunque la successione è esatta.

$$\begin{tikzcd}
0 \arrow[r] & N_i \arrow[r, "f_i"] \arrow[d, "id_{N_i}"'] & M_i \arrow[r, "g_i"] \arrow[d, "i"'] & P_i \arrow[r] \arrow[d, "id_{P_i}"'] & 0 \\
0 \arrow[r] & N_n \arrow[r, "f_n"'] & M_n \arrow[r, "g_n"'] & P_n \arrow[r] & 0
\end{tikzcd}$$

Per il Lemma dei Cinque, con $id\colon N_i \to N_n$, $id\colon P_i \to P_n$ e $i\colon M_i \to M_n$, ottengo la tesi.

□

Corollario 6.5. *Sia* $M = \oplus_{i=1}^{n} M_i$

$$M \text{ noetheriano} \iff M_i \text{ noetheriano } \forall i$$

Dimostrazione. Una implicazione è ovvia, perchè i sottomoduli di un modulo noetheriano sono noetheriani. Mostriamo il viceversa per induzione sul numero di addendi della somma diretta. Se n=2, consideriamo

$$0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$$

e dunque basta applicare la proposizione precedente. Supponiamo ora che la tesi sia vera per ogni somma diretta di n termini, e mostriamo che vale per quelli di n+1 addendi.

$$0 \to M_1 \to M_1 \oplus (\bigoplus_{i=2}^{n+1} M_i) \to \bigoplus_{i=2}^{n+1} M_i \to 0$$

M_1 è noetheriano, $\oplus_{i=2}^{n+1} M_i$ è noetheriano per ipotesi induttiva, e dunque per la proposizione precedente otteniamo la tesi.

□

Definizione 6.6. Un anello A si dice noetheriano se è noetheriano come modulo su sé stesso.

Dato che i sottomoduli di un modulo noetheriano sono gli ideali, la definizione è equivalente a dire che ogni ideale è finitamente generato.

Corollario 6.7. *Sia A un anello noetheriano e sia M un A-modulo. Allora M è finitamente generato se e solo se M è noetheriano*

Dimostrazione.

$$0 \to \operatorname{Ker} \varphi \to A^n \to M \to 0$$

Per il corollario precedente, A^n è noetheriano e per la proposizione, M è noetheriano. □

Corollario 6.8. *A anello noetheriano, I ideale di A. Allora A/I è noetheriano.*

Dimostrazione.

$$0 \to I \to A \to {}^{A}\!/_{I} \to 0$$

Poichè A è noetheriano, ${}^{A}\!/_{I}$ è noetheriano come A modulo, ma allora è noetheriano come ${}^{A}\!/_{I}$ -modulo. □

Corollario 6.9. *Sia A un anello e sia M un A-modulo noetheriano. Allora ${}^{A}\!/_{\mathrm{Ann}(M)}$ è noetheriano.*

Dimostrazione. La tesi è equivalente a mostrare che se M è un A-modulo noetheriano con $\mathrm{Ann}(M) = 0$, A è noetheriano. M è noetheriano, dunque $M = \langle m_1 \dots m_n \rangle$. Sia I un ideale di A; mostriamo che I è finitamente generato. Consideriamo:

$$\begin{aligned} f : I &\longrightarrow M^n \\ i &\longrightarrow (im_1 \dots im_n) \end{aligned}$$

f è un omomorfismo iniettivo perchè $\mathrm{Ann}(M) = 0$, dunque $I \simeq f(I)$. Ma $f(I)$ è un sottomodulo di un modulo noetheriano, quindi $f(I)$ è finitamente generato e visto l'isomorfismo lo è anche I. □

Proposizione 6.10. *A anello noetheriano, S sottoinsieme moltiplicativamente chiuso. Allora $S^{-1}A$ è noetheriano.*

Dimostrazione. Mostriamo che ogni ideale di $S^{-1}A$ è finitamente generato. Sia J un ideale di $S^{-1}A$. Per quanto visto sugli anelli di frazioni, $J = S^{-1}I$ con I ideale di A tale che $S \cap I = \emptyset$. Poichè A è noetheriano, $I = (a_1 \dots a_n)$ e dunque $J = \left(\frac{a_1}{1} \dots \frac{a_n}{1}\right)$. □

Ci chiediamo ora se un anello di polinomi su un anello noetheriano rimane ancora noetheriano. In generale questo è falso; infatti $\mathbb{K}[x_1, x_2, \dots]$ non è noetheriano; d'altro canto, abbiamo già mostrato con la trattazione delle basi di Gröbner che $\mathbb{K}[x_1, \dots x_n]$ è noetheriano. Il seguente teorema di Hilbert risponde a questa domanda:

Teorema (della base di Hilbert). *Sia A un anello noetheriano. Allora $A[x]$ è noetheriano.*

Dimostrazione. Sia $I \subseteq A[x]$ un ideale. Mostriamo che è finitamente generato. Sia $lc(I) = \{a \in A \mid \exists f \in I \text{ t.c. } lc(f) = a\}$. $lc(I)$ è un ideale di A, dunque è finitamente generato, ma allora possiamo considerare un insieme di generatori $lc(I) = (a_1, \dots a_k)$. Di conseguenza, per ogni indice $i = 1 \dots k$ esiste f_i tale che $lc(f_i) = a_i$. Sia $d = \max\{deg(f_i)\}$. L'idea è ora quella di attuare una sorta di divisione per questi polinomi e aggiungere ai generatori i resti.
Sia $h \in I$. Poichè gli f_i generano l'ideale dei coefficienti di testa, è possibile sottrarre a h una combinazione degli f_i in modo da abbassare il grado. Più precisamente, sia $h = ax^n + \tilde{h}$ con $deg(\tilde{h}) < n$ e $n \geq d$. Allora $a \in lc(I)$ e dunque $a = \sum_{i=1}^{k} b_i a_i$. Di conseguenza, preso $g = \sum_{i=1}^{k} b_i x^{n-n_i} f_i$, si ha che $g \in I$ e quindi $h - g \in I$ e $deg(h-g) < n$. Iterando, posso allora trovare un $\tilde{g} \in (f_1 \dots f_k)$ tale che $deg(h - \tilde{g}) < d$. Considero allora l'A-modulo $M = \langle 1, x, x^2 \dots x^{d-1} \rangle$. M è finitamente generato su un anello noetheriano e dunque è noetheriano. Se considero allora $M \cap I$, questo è finitamente generato in quanto sottomodulo

di un modulo noetheriano, e dunque $\exists\{g_1, \dots g_l\} \subseteq I$ *t.c.* $M \cap I = (g_1, \dots g_l)$. Questi polinomi generano i "resti" della divisione; cioè $h - \tilde{g} \in M \cap I$ e dunque $I = (f_1, \dots f_k, g_1, \dots g_l)$ □

6.2 Decomposizione Primaria

Ispirati da quando ottenuto nel caso degli anelli di polinomi su un campo, vorremmo vedere se negli anelli noetheriani è possibile decomporre un ideale come intersezione di ideali primari.

Proposizione 6.11. *Sia A un anello noetheriano.*

$$I \text{ irriducibile} \Rightarrow I \text{ primario}$$

Dimostrazione. Supponiamo, senza perdita di generalità, che $I = (0)$ (possiamo ridurci a questo caso a meno di quozientare per I). Ci chiediamo se

$$xy = 0 \; y \neq 0 \overset{?}{\Rightarrow} x^n = 0$$

Consideriamo la catena

$$\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \cdots \subseteq \mathrm{Ann}(x^n)$$

Poiche A è noetheriano, la catena è stazionaria, cioè $\exists n \in \mathbb{N}$ *t.c.* $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1})$ Mostriamo allora che $(x^n) \cap (y) = (0)$. In tal caso, poichè (0) è irriducibile, $x^n = 0$. Sia $a \in (x^n) \cap (y)$.

$$a = by = cx^n \Rightarrow ax = bxy = cx^{n+1} \; ma \; xy = 0 \Rightarrow$$
$$\Rightarrow cx^{n+1} = 0 \Rightarrow c \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n) \Rightarrow cx^n = a = 0$$

Di conseguenza, $x^n = 0$ e dunque (0) è primario. □

Proposizione 6.12. *Sia A un anello noetheriano e sia I un ideale di A.*

$$\Longrightarrow \exists Q_1 \dots Q_n \text{ irriducibili t.c. } I = \bigcap_{i=1}^{n} Q_i$$

Dimostrazione. Per semplicità, chiamiamo $\mathcal{P}$ la proprietà che vogliamo dimostrare. Sia $X = \{I \text{ ideali di } A \mid \neg\mathcal{P}(I)\}$. Per assurdo, supponiamo che X sia non vuoto. Allora, poichè A è noetheriano, esiste un ideale $P \in X$ massimale. Chiaramente P non è irriducibile, dunque $P = L \cap J$, con $P \subsetneq L$ e $P \subsetneq J$. Per massimalità di P, L e J sono intersezione di irriducibili, cioè:

$$\exists Q_1 \dots Q_k \text{ irriducibili t.c. } L = \bigcap_{i=1}^{k} Q_i$$
$$\exists T_1 \dots T_l \text{ irriducibili t.c. } J = \bigcap_{i=1}^{l} T_i$$
$$\Longrightarrow P = \bigcap_{i=1}^{k} Q_i \cap \bigcap_{i=1}^{l} T_i$$

e dunque siamo arrivati a un assurdo, perchè abbiamo scritto P come intersezione finita di irriducibili. □

Definizione 6.13. Sia I un ideale di A. Una decomposizione primaria di I è una scrittura $I = \bigcap_{i=1}^{n} Q_i$ dove ogni Q_i è un ideale primario. Una decomposizione primaria si dice minimale se $Q_i \not\supset \bigcap_{j \neq i} Q_j$ e se, detti $P_i = \sqrt{Q_i}$, si ha $P_i \neq P_j \ \forall i \neq j$.

Lemma 6.14. *Siano Q_1, Q_2 ideali P-primari e sia $Q = Q_1 \cap Q_2$. Allora Q è P-primario.*

Dimostrazione. Mostriamo intanto che $\sqrt{Q} = P$.

$$\sqrt{Q} = \sqrt{Q_1 \cap Q_2} = \sqrt{Q_1} \cap \sqrt{Q_2} = P \cap P = P$$

Mostriamo ora che Q è primario. Sia $ab \in Q$ e supponiamo $a \notin Q$. Vogliamo mostrare che $b \in P$. Per quanto supposto, $(a \notin Q_1) \vee (a \notin Q_2)$. Supponiamo che valga la prima delle due condizioni. Allora, poichè Q_1 è P-primario, $b \in P$ e dunque la tesi. □

Lemma 6.15. *Sia A un anello noetheriano e sia I un ideale di A. Allora esiste $m \in \mathbb{N}$ tale che $(\sqrt{I})^m \subseteq I$*

Dimostrazione. A è noetheriano, dunque l'ideale $\sqrt{I}$ è finitamente generato, $\sqrt{I} = (f_1 \dots f_k)$.

$$\forall i = 1 \dots k \ \exists m_i \in \mathbb{N} \ t.c. \ f_i^{m_i} \in I$$

Sia $m = \sum_{i=1}^{k} m_i$ e sia $f = \sum_{i=1}^{k} a_i f_i \in \sqrt{I}$. Per la formula del binomio di Newton, $f^m \in I$ e dunque la tesi.

□

Lemma 6.16. *Sia Q un ideale P-primario e sia $a \in A$.*

1. $a \in Q \Rightarrow (Q : a) = A$
2. $a \notin Q \Rightarrow (Q : a)$ *è P-primario*
3. $a \notin P \Rightarrow (Q : a) = Q$

Dimostrazione.

(1) Segue dalla definizione di ideale e di quoziente.

(2) Mostriamo che $\sqrt{(Q : a)} = P$.

$$x \in \sqrt{(Q : a)} \Rightarrow x^n \in (Q : a) \Rightarrow ax^n \in Q \ ma \ Q \ è \ primario$$
$$\Rightarrow x^n \in P \Rightarrow x \in P$$

Viceversa, supponiamo $x \in P$.

$$\sqrt{Q} = P \Rightarrow \exists n \in \mathbb{N} \ t.c. \ x^n \in Q \Rightarrow x^n \in (Q : a) \Rightarrow x \in \sqrt{(Q : a)}$$

Mostriamo ora che $(Q : a)$ è primario. Sia $xy \in (Q : a)$. Supponiamo $x \notin P$; ricordando che $a \notin Q$,

$$axy \in Q \Rightarrow ay \in Q \Rightarrow y \in (Q : a)$$

(3) Chiaramente $Q \subseteq (Q : a)$; viceversa,

$$x \in (Q : a) \Rightarrow ax \in Q \ ma \ a \notin P \Rightarrow x \in Q$$

□

Teorema 6.17 (Unicità della decomposizione primaria)**.** *Sia $I = \bigcap Q_i$ una decomposizione primaria minimale di I.*

1. $\{P_i \mid \sqrt{Q_i} = P_i\} = \{\sqrt{(I : a)} \mid \sqrt{(I : a)}$ *è primo*$\}$
2. *Se A è noetheriano,* $\{P_i \mid \sqrt{Q_i} = P_i\} = \{(I : a) \mid (I : a)$ *è primo*$\}$

Dimostrazione.

(1) Esibiamo un elemento $a \in A$ tale che $\sqrt{(I : a)} = P_i$. Poichè abbiamo supposto che la decomposizione fosse minimale, $\exists a \in \bigcap_{j \neq i} Q_j$ *t.c.* $a \notin Q_i$

$$(I : a) = (\bigcap_{k=1}^{n} Q_k : a) = \bigcap_{k=1}^{n} (Q_k : a) = (Q_i : a)$$

che per il lemma è P_i-primario, e dunque $\sqrt{(I : a)} = \sqrt{(Q_i : a)} = P_i$. Mostriamo allora che i P_i sono i soli che si possono realizzare in questo modo. Sia $P = \sqrt{(I : a)}$.

$$\sqrt{(I : a)} = \sqrt{(\bigcap_{i=1}^{n} Q_i : a)} = \bigcap_{i=1}^{n} \sqrt{(Q_i : a)} = \bigcap P_j$$

Per il lemma di scansamento, allora, $\exists i$ *t.c.* $P = P_i$

(2) Sia $P_i = \sqrt{Q_i}$. Poichè A è noetheriano, $\exists k \in \mathbb{N}$ *t.c.* $P_i^k \subseteq Q_i$. Sia allora $m \in \mathbb{N}$ il minimo tale che $P_i^m(\bigcap_{j \neq i} Q_j) \subseteq I$ e sia $a \in (P^{m-1}(\bigcap_{j \neq i} Q_j)) \setminus I$. Per come è stato scelto a, si ha che $aP_i \subseteq I$ e di conseguenza $(I : a) \supseteq P_i$ d'altronde, per il lemma, $(I : a)$ è P_i-primario, e dunque si ha l'uguaglianza.

□

Corollario 6.18. *I primi P_i di una decomposizione minimale sono indipendenti dalla decomposizione scelta.*

Definizione 6.19. Sia $I = \bigcap Q_i$. Gli ideali P_i si dicono primi associati di I. I P_i si dicono minimali se sono minimali tra i primi associati, altrimenti si dicono immersi.

Lemma 6.20. *I primi associati minimali sono minimali nell'insieme dei primi che contengono I.*

Dimostrazione. Sia P un primo che contiene I. Allora $P \supseteq \sqrt{I} = P_1 \cap \cdots \cap P_n$. Per il lemma di scansamento, $\exists i$ *t.c.* $P_i \subseteq P$. □

Proposizione 6.21. *Sia $I = \bigcap Q_i$ una decomposizione primaria minimale. Allora*

$$\bigcup P_i = \{a \in A \mid (I : a) \neq I\}$$

Dimostrazione. A meno di quozientare per l'ideale I, possiamo considerare $I = (0)$ e dunque dimostrare che $\mathcal{D}(A) = \bigcup_{i=1}^{n} P_i$. Per il teorema precedente, ricordando che $\mathcal{D}(A) = \bigcup_{a \neq 0} \sqrt{(0:a)}$, si ha

$$\forall i \ \exists a_i \in A \ t.c. \ P_i = \sqrt{(0:a_i)} \Rightarrow \forall i \ P_i \subseteq \mathcal{D}(A) \Rightarrow \bigcup_{i=1}^{n} P_i \subseteq \mathcal{D}(A)$$

Per mostrare l'altra inclusione, basta notare che, $\forall a \in A \setminus \{0\}$,

$$\sqrt{(0:a)} = \bigcap_{i=1}^{n} \sqrt{(Q_i:a)} = \bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} P_i \subseteq \bigcup_{i=1}^{n} P_i$$

□

Occupiamoci ora di caratterizzare in qualche modo gli ideali primari di una decomposizione. Per farlo, dobbiamo però ricorrere alla teoria degli anelli di frazioni.

Teorema 6.22. *Sia $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso e sia Q un ideale P-primario.*

1. *Se $S \cap P \neq \emptyset$ allora $S^{-1}Q = S^{-1}A$*
2. *Se $S \cap P = \emptyset$ allora $S^{-1}Q$ è $S^{-1}P$-primario e $(S^{-1}Q)^c = Q$*

Dimostrazione.

(1) Sia $a \in S \cap P \Rightarrow \exists n \in \mathbb{N} \ t.c. \ a^n \in Q \cap S \Rightarrow S^{-1}Q = S^{-1}A$.

(2) $\sqrt{S^{-1}Q} = S^{-1}\sqrt{Q} = S^{-1}P$. Mostriamo allora che $S^{-1}Q$ è primario.

$$\frac{a}{s}\frac{b}{t} \in S^{-1}Q \Rightarrow \frac{ab}{st} = \frac{c}{u} \ c \in Q \ u \in S$$
$$\Rightarrow \exists v \in S \ t.c. \ \underbrace{uv}_{\notin P} ab = cvst \in Q \Rightarrow ab \in Q \Rightarrow \left(\frac{a}{s} \in S^{-1}Q\right) \vee \left(\frac{b}{t} \in S^{-1}P\right)$$

Rimane da mostrare che $(S^{-1}Q)^c = Q$.

$$\frac{b}{t} \in S^{-1}Q \Rightarrow \left(\frac{b}{t} = \frac{a}{1} \iff \exists s \in S \ t.c. \ ats = bs \in Q\right)$$
$$\iff a \in Q \ perchè \ st \notin P$$

□

Proposizione 6.23. *Sia $S \subseteq A$ un sottoinsieme moltiplicativamente chiuso, sia $I = \bigcap_{i=1}^{m} Q_i \cap \bigcap_{i=m+1}^{n} Q_i$ una decomposizione primaria minimale. Supponiamo che*

1. $S \cap P_i = \emptyset \ \forall i = 1 \dots m$
2. $S \cap P_i \neq \emptyset \ \forall i = m+1 \dots n$

$$\Longrightarrow (S^{-1}I)^c = \bigcap_{i=1}^{m} Q_i$$

Dimostrazione.

$$S^{-1}I = S^{-1}(\bigcap_{i=1}^{n} Q_i \overset{th\ prec}{=} S^{-1} \bigcap_{i=1}^{m} Q_i$$

$$\Longrightarrow (S^{-1}I)^c = \bigcap_{i=1}^{m} Q_i$$

□

In virtù di quest'ultima proposizione, i Q_i minimali sono univocamente determinati dalla contrazione delle localizzazioni di I per i primi associati.

6.3 Anelli Artiniani

Nella definizione di modulo noetheriano, abbiamo considerato l'insieme dei sottomoduli ordinato per inclusione. Possiamo però ordinare questo insieme rispetto all'inclusione inversa. Abbiamo allora la seguente definizione:

Definizione 6.24. M si dice Artiniano se ogni catena discendente di sottomoduli è stazionaria.

Ripetendo le dimostrazioni eseguite per i moduli noetheriani, si ottiene che un quoziente e un sottomodulo di un modulo artiniano è artiniano.

Indaghiamo ora sulla struttura degli anelli artiniani.

Proposizione 6.25. *Sia A un anello artiniano. Allora ogni primo è massimale.*

Dimostrazione. Sia P un primo di A. Allora A/P è un dominio. Mostriamo che in realtà è un campo. Sia $\bar{a} \neq 0$.

$$(\bar{a}) \supseteq (\bar{a}^2) \supseteq \dots$$

è una catena discendente, e dunque, poichè A/P è artiniano, è stazionaria. Dunque $\exists n \in \mathbb{N}$ *t.c.* $(\bar{a}^n) = (\bar{a}^{n+1})$. Dunque, sfruttando l'inclusione non banale, $\bar{a}^n = \bar{b}\bar{a}^{n+1}$ Di conseguenza, $\bar{a}^n(\bar{1} - \bar{a}\bar{b}) = 0$. Poichè A/P è un dominio e $\bar{a} \neq 0$, necessariamente $\bar{a}\bar{b} = 1$. □

Proposizione 6.26. *Sia A un anello artiniano. Allora A ha finiti massimali.*

Dimostrazione. Sia $\Sigma = \{\mathfrak{M}_1 \cap \dots \cap \mathfrak{M}_k \mid \mathfrak{M}_i \in SpecM(A)\}$; questo è l'insieme di tutte le possibili intersezioni finite di ideali massimali di A. Sicuramente $\Sigma \neq \emptyset$ perchè esiste sicuramente un massimale di A. Allora esiste un elemento minimale per Σ; cioè esistono $\mathfrak{M}_1 \dots \mathfrak{M}_n$ che hanno intersezione minimale. Mostriamo che questi sono tutti i massimali di A. Sia $\mathfrak{N}$ un massimale di A. Allora $\mathfrak{N} \cap \mathfrak{M}_1 \dots \cap \mathfrak{M}_n \subseteq \mathfrak{M}_1 \cap \dots \cap \mathfrak{M}_n$. Dunque, per minimalità, $\mathfrak{N} \supseteq \mathfrak{M}_1 \cap \dots \cap \mathfrak{M}_n$ e per scansamento, $\exists i$ *t.c.* $\mathfrak{N} = \mathfrak{M}_i$ □

Definizione 6.27. Sia A un anello.

$$\dim(A) := \max\{\textit{lunghezze di catene di primi}\}$$

Sia I un ideale.

$$\dim(I) := \dim\left({}^{A}\!/_{I}\right)$$

Esempio. Se $\mathbb{K}$ è un campo, $\dim(\mathbb{K}) = 0$. Se A è un PID che non è un campo, $\dim(A) = 1$.

Lemma 6.28. *Sia A un anello artiniano. Allora esiste $n \in \mathbb{N}$ tale che $\mathfrak{N}(A)^n = 0$*

Dimostrazione. Consideriamo la catena:

$$\mathfrak{N}(A) \supseteq \mathfrak{N}(A)^2 \supseteq \mathfrak{N}(A)^3 \supseteq \dots$$

Poichè A è artiniano, tale catena è stazionaria; dunque $\exists n \in \mathbb{N}$ *t.c.* $\mathfrak{N}(A)^n = \mathfrak{N}(A)^{n+1}$. Chiamiamo ora $I = \mathfrak{N}(A)^n$ e mostriamo che deve essere 0. Supponiamo per assurdo che $I \neq 0$. Consideriamo l'insieme

$$\Sigma = \{J \subseteq A \mid JI \neq (0)\}$$

$\Sigma \neq \emptyset$ perchè $I \in \Sigma$; allora, visto che A è artiniano, esiste $J \in \Sigma$ minimale. J è principale; infatti se $J = (f_k \mid k \in K)$, allora $\exists k \in K$ *t.c.* $(f_k)I \neq (0)$ e dunque per minimalità $J = (f_k)$. Notiamo ora che $JI = J$. Infatti $(JI)I = JI^2 = JI$; poichè $JI \subseteq J$ e $JI \in \Sigma$, per minimalità di J, $J = IJ$. Notiamo ora che $J = (f_k)$ è un A-modulo finitamente generato (è un ideale principale); per il lemma di Nakayama, $J = 0$ perchè $I \subseteq \mathfrak{N}(A) \subseteq \mathfrak{J}(A)$. □

Teorema 6.29. *A artiniano $\iff$ A è prodotto diretto finito di anelli locali artiniani.*

Dimostrazione.

($\Leftarrow$) La tesi segue dal fatto che un prodotto diretto finito di artiniani è artiniano.

($\Rightarrow$) Ricordiamo che il nilradicale è l'intersezione di tutti gli ideali primi; visto che A è artiniano, questa coincide con l'intersezione di tutti gli ideali massimali. Ma allora, dal lemma precedente:

$$0 = \mathfrak{N}(A)^n = (\mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_m)^n = \mathfrak{M}_1^n \mathfrak{M}_2^n \dots \mathfrak{M}_m^n$$

per comassimalità dei massimali. Dunque, dal teorema cinese del resto,

$$A = {}^{A}\!/_{\mathfrak{N}(A)} = \prod_{i=1}^{m} {}^{A}\!/_{\mathfrak{M}_i^n}$$

che sono locali e artiniani.

□

Lemma 6.30. *Sia A un anello nel quale esistono $\mathfrak{M}_1, \dots, \mathfrak{M}_n$ ideali massimali tali che $\mathfrak{M}_1 \dots \mathfrak{M}_n = (0)$.*

$$A \text{ artiniano} \iff A \text{ noetheriano}$$

Dimostrazione. Consideriamo la catena:

$$A \supset \mathfrak{M}_1 \supset \mathfrak{M}_1 \cap \mathfrak{M}_2 \supset \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \mathfrak{M}_3 \supset \dots \supset \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \dots \cap \mathfrak{M}_n = (0)$$

Supponiamo che A sia artiniano; il caso noetheriano è equivalente. Vogliamo risalire la catena dall'ideale (0) fino ad A; mostriamo allora iterativamente che se un elemento della catena è artiniano, allora lo è anche il precedente. Il primo passo è chiaro, perché $\mathfrak{M}_1 \dots \mathfrak{M}_{n-1} / \mathfrak{M}_1 \dots \mathfrak{M}_n \simeq \mathfrak{M}_1 \dots \mathfrak{M}_{n-1}$ è un $A/\mathfrak{M}_n$-spazio vettoriale artiniano, dunque è finitamente generato ma allora è anche noetheriano come $A/\mathfrak{M}_n$-spazio vettoriale. A maggior ragione, lo è come A-modulo.
Consideriamo ora un qualsiasi modulo $\mathfrak{M}_1 \dots \mathfrak{M}_{j-1}$ della catena e supponiamo di aver mostrato che tutti gli elementi successioni siano noetheriani e artiniani.. $\mathfrak{M}_1 \dots \mathfrak{M}_{j-1} / \mathfrak{M}_1 \dots \mathfrak{M}_j$ è un $A/\mathfrak{M}_j$-spazio vettoriale artiniano. Come per il passo base, l'artinianità dello spazio vettoriale implica la sua noetherianità come $A/\mathfrak{M}_j$-modulo e quindi quella come A-modulo. Allora, poiché per ipotesi induttiva $\mathfrak{M}_1 \dots \mathfrak{M}_j$ è noetheriano come $A/\mathfrak{M}_j$-modulo, anche $\mathfrak{M}_1 \dots \mathfrak{M}_{j-1}$ è noetheriano come $A/\mathfrak{M}_j$-modulo, e dunque come A-modulo. L'induzione ci da allora la tesi. □

Teorema 6.31. *A artiniano $\iff$ (A noetheriano)* $\wedge$ $(\dim(A) = 0)$

Dimostrazione.

($\Rightarrow$) Per il primo dei due lemmi precedenti, $\mathfrak{N}(A)^n = \mathfrak{M}_1^n \dots \mathfrak{M}_m^n = \mathfrak{M}_1^m \cap \dots \cap \mathfrak{M}_m^n = 0$. Dunque, per il secondo dei due lemmi, A è noetheriano. Per quanto dimostrato sopra, poi, ogni primo è massimale e dunque $\dim A = 0$.

($\Leftarrow$) Poichè $\dim A = 0$, ogni primo è massimale, dunque $\mathfrak{N}(A) = \mathfrak{M}_1 \mathfrak{M}_2 \dots \mathfrak{M}_n$. Inoltre, poichè A è noetheriano, $\mathfrak{N}(A)^m = 0$ e dunque siamo nelle ipotesi del lemma precedente; di conseguenza A è artiniano.

□

6.4 Complementi

Per definizione, abbiamo che una qualsiasi catena di ideali di un anello noetheriano è stazionaria. Questo non ci fornisce tuttavia un limite superiore alla lunghezza delle catene di primi; mostriamo allora che esiste un anello noetheriano di dimensione infinita. Abbiamo prima necessità di un lemma:

Lemma 6.32. *Sia A un anello che soddisfa le seguenti condizioni:*

- $\forall P \in Spec(A)$ A_P *è noetheriano*
- $\forall x \neq 0$ *esistono finiti massimali $\mathfrak{M}_1, \dots, \mathfrak{M}_k$ che contengono x.*

Allora A è noetheriano.

Dimostrazione. Sia I un ideale di A. Per ottenere la tesi, ci basta mostrare che I è finitamente generato. Per ipotesi, abbiamo che esistono finiti massimali che contengono I. Infatti, fissato $x \in I$, esistono solo finiti massimali che contengono x, e di conseguenza solo un sottoinsieme di questi può contenere I. Siano $\mathfrak{M}_1, \dots, \mathfrak{M}_r$ questi massimali. Consideriamo allora $\forall i$ l'ideale $IA_{\mathfrak{M}_i}$ l'ideale esteso nella localizzazione. Per ipotesi, $A_{\mathfrak{M}_i}$ è noetheriano, dunque

$$IA_{\mathfrak{M}_i} = \left(\frac{a_{i,1}}{1}, \dots, \frac{a_{i,n_i}}{1}\right)$$

Sia allora $B = \{a_{i,j} \mid i = 1, \dots, r \; j = 1, \dots, n_r\}$. Per ogni $b \in B$ esistono $M_{b,1}, \dots, M_{b,n_b}$ che contengono b. Per ognuno di questi massimali, scegliamo $x_{b_i} \in I \setminus M_{b_i}$. Consideriamo allora $B' = B \cup \{x_{b_i}\}$ e mostriamo che questo è un insieme di generatori per I. Mostriamo cioè che $\left({}^{I}\!/_{\langle B' \rangle}\right)_{\mathfrak{M}} = 0$ per ogni massimale $\mathfrak{M}$. Localizzando per un massimale che contiene I, gli elementi di B mi garantiscono che ${}^{A_{\mathfrak{M}}}\!/_{B'^e} = 0$. Se localizziamo invece per un massimale che non contiene I, $S^{-1}I = S^{-1}A$. Per gli elementi di $B' \setminus B$, si ha che in questo caso anche $S^{-1}B' = S^{-1}A$ e dunque la tesi. $\square$

Siamo ora pronti a fornire un esempio di un anello noetheriano di dimensione infinita. Consideriamo l'anello $A = \mathbb{K}[x_1, x_2, \dots]$ e sia m_i una successione di naturali crescente tale che

$$m_{i+1} - m_i > m_i - m_{i-1}$$

Consideriamo allora gli ideali:

$$I_n = (x_{m_n+1}, \dots, x_{m_{n+1}})$$

Ognuno di questi ideali è primo; sia allora $S = A \setminus (\cup I_n)$. Poichè S è il complementare di una unione di primi, si ha che esso è un sottoinsieme moltiplicativamente chiuso. Possiamo allora considerare l'anello $S^{-1}A$. In questo anello, ogni elemento non nullo o invertibile è contenuto in un numero finito di massimali; inoltre $(S^{-1}A)_P$ è noetheriano per ogni ideale primo. Di conseguenza, $S^{-1}A$ è noetheriano. D'altronde, tale anello ha dimensione infinita; fissato $n \in \mathbb{N}$, troviamo un elemento della successione m_i tale che $m_i - m_{i-1} > n$. Troviamo allora la catena di ideali primi $(x_{m_i}) \subseteq (x_{m_i+1}) \subseteq \dots \subseteq (x_{m_i+1}, \dots, x_{m_{i+1}})$. Abbiamo allora trovato l'esempio cercato.