

# ALGEBRA 2

## ANELLI

---

- Se  $A$  è un anello finito allora  $A = A^* \sqcup \mathcal{D}(A)$
- $f : A \rightarrow B$  allora  $\text{Im } f \cong \frac{A}{\text{Ker } f}$
- $I \subseteq A$  ideale,  $B \subseteq A$  sottoanello allora vale  $\frac{I+B}{I} \cong \frac{B}{I \cap B}$
- $I, J \subseteq A$  ideali e  $I \subseteq J$ . Allora vale  $\frac{\frac{A}{I}}{\frac{J}{I}} \cong \frac{A}{J}$   
Si ha inoltre la corrispondenza tra gli ideali di  $\frac{A}{I}$  e gli ideali  $J \subseteq A$  tali che  $I \subseteq J$ . In questa corrispondenza i primi ed i massimali si corrispondono
- $IJ \subseteq I \cap J$ . Se vale  $I + J = 1$  allora  $IJ = I \cap J$
- È FALSO che  $I \cap (J + K) = (I \cap J) + (I \cap K)$ . FALSO
- $I \subseteq \sqrt{I}$
- $(A \text{ dominio}) a \text{ primo} \implies a \text{ irriducibile}$
- $(A \text{ UFD}) a \text{ irriducibile} \implies a \text{ primo}$
- Se  $H \subseteq A \times B$  è ideale allora  $H = I \times J$  con  $I \subseteq A, J \subseteq B$  ideali
- $A \cong A_1 \times A_2 \Leftrightarrow \exists e \in A, e \neq 0, 1 \quad e^2 = e$
- $\mathcal{D}(A) = \cup_{a \notin A^*} (0 : a) = \cup_{a \notin A^*} \sqrt{(0 : a)} = \sqrt{\mathcal{D}(A)} = \mathcal{D}(A)$ , anche se non è necessariamente un ideale
- $\{E_\lambda\}_{\lambda \in \Lambda}$  sottoinsiemi di  $A$ . Allora  $\cup_{\lambda \in \Lambda} \sqrt{E_\lambda} = \sqrt{\cup_{\lambda \in \Lambda} E_\lambda}$
- Sia  $A$  dominio con un numero infinito di elementi e  $|A^*| < \infty$  allora  $A$  possiede infiniti ideali massimali
- $I$  massimale  $\implies I$  primo  $\implies I$  primario. Inoltre  $A \text{ dominio} \Leftrightarrow (0)$  ideale primo
- Sono equivalenti:
  - $A$  ha un unico ideale massimale
  - $\exists \mathfrak{m} \subseteq A$  ideale massimale t.c.  $\forall a \in A \setminus \mathfrak{m} \implies a \notin A^*$
  - $\exists \mathfrak{m} \subseteq A$  ideale massimale t.c. ogni elemento della forma  $1 + \mathfrak{m}$  è invertibile
- $a \in \mathcal{J}(A) \Leftrightarrow \forall b \in A \quad 1 - ab \in A^*$
- $\sqrt{I} = \cap_{I \subseteq P \text{ primi}} P$
- **(Lemma di Scansamento)**  $P_1, \dots, P_n$  ideali primi. Sia  $I \subseteq A$  ideale t.c.  $I \subseteq \cup_{i=1}^n P_i$ . Allora  $\exists j$  t.c.  $I \subseteq P_j$
- $I_1, \dots, I_n$  ideali e  $P$  ideale primo.  $\cap_{i=1}^n I_i \subseteq P \implies \exists j$  t.c.  $I_j \subseteq P$ . Inoltre se  $P = \cap_i I_i$  allora  $\exists j$  t.c.  $I_j = P$
- **(Teorema cinese)** Siano  $I_1, \dots, I_n \subseteq A$  ideali tali che  $I_i + I_j = 1$ . Allora  $\forall a_1, \dots, a_n \in A \quad \exists a \in A$  t.c.  $a \equiv a_i \pmod{I_i}$
- $A$  anello c.u. Allora si ha che
  - $f \in A[x]$  è un'unità  $\Leftrightarrow f = \sum_{i=0}^n a_i x^i$  con  $a_i \in A$  tali che  $a_0 \in A^*$  e  $a_i \in \mathcal{N}(A) \quad \forall i \geq 1$
  - $f \in A[x]$  è nilpotente  $\Leftrightarrow \forall i \quad a_i \in \mathcal{N}(A)$

- $f \in A[x]$  è divisore di zero  $\Leftrightarrow \exists c \in A, c \neq 0$  t.c.  $cf = 0$

Si ha inoltre per gli anelli di polinomi che

- $I$  primo  $\Leftrightarrow I[x]$  primo
- $I$  primario  $\Leftrightarrow I[x]$  primario

NON è vero che tutti gli ideali di  $A[x]$  sono del tipo  $I[x]$ , come ad esempio  $(x)$

- Gli ideali primi di  $\mathbb{Z}[x]$  sono dei seguenti tipi:
  - $(0)$
  - $(p)[x]$  con  $p \in \mathbb{P}$
  - $(f(x))$  con  $f$  irriducibile
  - $(p, f(x))$  con  $p \in \mathbb{P}$  e  $f$  irriducibile modulo  $p$  (Questi sono anche massimali)
- $u \in A^*, a \in \mathcal{N}(A)$ , allora  $u + a \in A^*$  (Somma di un nilpotente e di un invertibile è invertibile)
- $I$  primo  $\implies I$  irriducibile
- In  $A[x]$  si ha  $\mathcal{N}(A[x]) = \mathcal{J}(A[x])$  (Mentre in generale vale solo che  $\mathcal{N}(A) \subseteq \mathcal{J}(A)$ )
- Sia  $\phi : A \rightarrow B$  omomorfismo di anelli. Allora
  - $\phi(\mathcal{N}(A)) \subseteq \mathcal{N}(B)$
  - Se  $\phi$  è surgettivo allora  $\phi(\mathcal{J}(A)) \subseteq \mathcal{J}(B)$
  - $A$  semilocale (con un numero finito di ideali massimali)  $\implies \phi(\mathcal{J}(A)) = \mathcal{J}(B)$
- $A$  PID  $\implies \mathcal{J}(A) = \mathcal{N}(A)$
- $A$  t.c. ogni ideale è primo  $\implies A$  è un campo
- $A$  t.c. ogni ideale primo è principale  $\implies A$  è un anello ad ideali principali
- $\sqrt{I}$  massimale  $\implies I$  primario.
- $I$  primario,  $J \not\subseteq \sqrt{I} \implies \sqrt{I : J^i} = \sqrt{I} \forall i$
- $I = \sqrt{I}$  e  $h \notin I \implies I : h$  è radicale
- **(Teorema della base di Hilbert)** Se  $A$  è un anello Nötheriano, allora  $A[x]$  è Nötheriano
- Se  $A$  è locale,  $\mathfrak{m}$  il suo ideale massimale e  $Q$  è  $\mathfrak{m}$ -primario, allora si ha  $(\frac{A}{Q})_{\frac{\mathfrak{m}}{Q}} \cong \frac{A}{Q}$

## BASI DI GRÖBNER

---

### IDEALI MONOMIALI

Un ideale monomiale in  $K[x_1, \dots, x_n]$  è un ideale generato dai monomi

- **(Criterio di appartenenza)** Sia  $I$  un ideale monomiale e  $f \in K[x_1, \dots, x_n]$ ,  $f = \sum_{\beta} c_{\beta} x^{\beta}$  con  $c_{\beta} \in K$ . Allora  $f \in I \Leftrightarrow \forall \beta x^{\beta} \in I$
- **(Lemma di Dickson)** Ogni ideale monomiale è finitamente generato. (La frontiera minimale di un ideale monomiale è unica, e viene detta Escalièr)
- **(Operazioni con ideali monomiali)** Siano  $I_1 = (m_1, \dots, m_k)$  e  $I_2 = (n_1, \dots, n_s)$  con  $m_i, n_j$  monomi. Allora si ha
  - $I_1 + I_2 = (m_1, \dots, m_k, n_1, \dots, n_s)$
  - $I_1 \cap I_2 = (\text{MCD}_{i,j}(m_i, n_j))$

- $I_1 \cdot I_2 = (m_i \cdot n_j)_{i,j}$
- **(Iatto)**  $(I, m \cdot n) = (I, m) \cap (I, n)$  se  $\text{MCD}(m, n) = 1$  come monomi
- $I$  primo  $\Leftrightarrow I = (x_{i_1}, \dots, x_{i_k})$  (ed è massimale solo se le variabili compaiono tutte, ma DEVE essere monomiale)
- $I = \sqrt{I}$  (ovvero  $I$  è radicale)  $\Leftrightarrow \sqrt{m_i} = m_i \forall i$
- $I$  è primario  $\Leftrightarrow I = (x_{i_1}^{\alpha_1}, \dots, x_{i_k}^{\alpha_k}, m_1, \dots, m_s)$  dove  $m_1, \dots, m_s \in K[x_{i_1}, \dots, x_{i_k}]$
- $I$  è irriducibile  $\Leftrightarrow I = (x_{i_1}^{\alpha_1}, \dots, x_{i_k}^{\alpha_k})$
- $I \cdot J = I \cap J \Leftrightarrow \forall i, j \quad \text{MCD}(m_i, n_j) = 1$
- $I : J = \cap_i (I : n_i)$  e  $I : (n_i) = (\frac{m_j}{\text{MCD}(n_i, m_j)})_j$

- Notare che usando la terza relazione del punto precedente possiamo spezzare ogni ideale monomiale in ideali primari e utilizzando  $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$  si possono calcolare anche gli ideali primi associati. Inoltre con la decomposizione in primari si calcolano bene i divisori di zero, i nilpotenti, etc.

## ORDINAMENTI MONOMIALI COMUNI

- LEX  $x_1 > x_2 > \dots > x_n$ . Dico che  $\alpha \geq \beta \Leftrightarrow$  In  $\alpha - \beta$  la prima coordinata  $\neq 0$  è positiva
- DEGLEX Sia  $|\alpha| := \sum_i \alpha_i$ . Allora  $\alpha \geq \beta \Leftrightarrow$  si ha  $|\alpha| \geq |\beta|$  oppure  $|\alpha| = |\beta|$  e vale  $\alpha \geq \beta$  con LEX
- DEGREVLEX  $\alpha \geq \beta \Leftrightarrow |\alpha| > |\beta|$  oppure si ha  $|\alpha| = |\beta|$  e in  $\alpha - \beta$  l'ultima coordinata  $\neq 0$  è negativa

## BASI DI GRÖBNER E ALGORITMO DI DIVISIONE

- **(Algoritmo di Divisione)** Siano  $f_1, \dots, f_k, f \in K[x_1, \dots, x_n]$  allora  $\exists a_1, \dots, a_k, r \in K[x_1, \dots, x_n]$  tali che  $f = \sum_i a_i f_i + r$  e  $\deg(a_i f_i) \leq \deg(f)$ . Inoltre se  $r = \sum_\alpha r_\alpha x^\alpha$  si ha che se  $r_\alpha \neq 0$  allora  $x^\alpha \in (\text{lt}(f_1), \dots, \text{lt}(f_k))$

Notiamo che posso fare dei passaggi "a mano" prima di partire con l'algoritmo di divisione e lui funzionerà comunque. La cosa importante è ricordarsi di soddisfare la condizione  $\deg(a_i f_i) \leq \deg(f)$  ad ogni passaggio.

- **(Base di Gröbner)** Un insieme di polinomi  $g_1, \dots, g_k$  generatori di un ideale  $I$  i cui leading term generano  $\text{lt}(I)$  si dicono base di Gröbner. Sono equivalenti inoltre:
  - $\forall f \quad \exists! r$  resto della divisione di  $f$  per  $\{g_1, \dots, g_k\}$
  - $\forall f \in I = (g_1, \dots, g_k)$  si ha  $r = 0$  dall'algoritmo di divisione
  - $\forall i, j \quad S(g_i, g_j)$  ha resto  $r = 0$  nell'algoritmo di divisione

Dove per divisione si intende un risultato che soddisfi le ipotesi dell'algoritmo di divisione

- **(Base di Gröbner ridotta)** Una BdG  $G = \{g_1, \dots, g_k\}$  si dice ridotta se è minimale per inclusione e inoltre
  - $\text{lc}(g_i) = 1 \quad \forall i$
  - $(\deg(g_1), \dots, \deg(g_k))$  sono un'escalière per  $\deg(I)$
  - $\forall g_i \quad g_i = \sum_\alpha c_\alpha x^\alpha$  allora  $x^\alpha \notin \text{lt}(G \setminus \{g_i\})$

Teorema: La base ridotta è unica. Per ridurre una BdG basta prendere ciascun elemento  $g$  ed effettuare la divisione per  $G \setminus \{g\}$

- **(S-polinomio)** Dati  $f, g \in K[x_1, \dots, x_n]$  e supponiamo  $f = c_\alpha x^\alpha + f_1$  e  $g = d_\beta x^\beta + g_1$  con  $\deg f = \alpha, \deg g = \beta$ . Allora dico S-polinomio tra  $f, g$  il polinomio definito da  $\gamma = (\gamma_1, \dots, \gamma_n)$  con  $\gamma_i = \max(\alpha_i, \beta_i)$

$$S(f, g) = \frac{x^\gamma}{c_\alpha x^\alpha} f - \frac{x^\gamma}{d_\beta x^\beta} g$$

## APPLICAZIONI E COMPUTAZIONI

- **(Eliminazione di LEX)**  $I \subseteq K[x_1, \dots, x_n]$  allora  $I_k = I \cap K[x_{k+1}, \dots, x_n]$  è il  $k$ -esimo ideale di eliminazione. Vale il teorema: Se  $G$  è una BdG rispetto a LEX con  $x_1 \geq \dots \geq x_n$  allora  $\forall k = 1, \dots, n-1$  si ha che  $G_k = G \cap K[x_{k+1}, \dots, x_n]$  è BdG di  $I_k$
- **(Cose calcolabili)** Dati  $I, J \subseteq K[x_1, \dots, x_n]$  e note le loro due BdG si ha
  - **(Intersezione)**  $I \cap J = (tI, (1-t)J) \cap K[x_1, \dots, x_n]$  dove quindi bisognerà usare l'ordinamento LEX con  $t$  come variabile più pesante per poter usare eliminazione
  - **(Colon)** Se  $\text{BdG}(J) = \{h_1, \dots, h_r\}$  allora  $I : J = \bigcap_{i=1}^r (I : h_i)$ .  
Se ora ho  $f \in K[x_1, \dots, x_n]$  e voglio calcolare  $I : (f) = \{g \mid gf \in I\}$  allora ho che  $I : (f) = \frac{1}{f} \cdot (I \cap (f))$ , ovvero se  $\text{BdG}(I \cap (f)) = \{g_1 f, \dots, g_k f\}$  allora ho  $\text{BdG}(I : (f)) = \{g_1, \dots, g_k\}$
  - **(Ker di morfismi)** Sia  $\Phi : K[x_1, \dots, x_n] \rightarrow K[y_1, \dots, y_n]$  tale che  $f_i(Y) := \Phi(x_i)$ . Allora si ha  $\text{Ker } \Phi = (x_1 - f_1(Y), \dots, x_n - f_n(Y)) \cap K[x_1, \dots, x_n]$  ovvero bisogna calcolare l'ideale di eliminazione senza le  $Y$
  - **(Appartenenza al radicale)**  $f \in \sqrt{I} \Leftrightarrow 1 \in (I, 1 - tf)$  e NON serve  $K$  algebricamente chiuso
- **(Sistemi di equazioni polinomiali)** Cerchiamo le soluzioni comuni di  $f_1 = 0, \dots, f_n = 0$  in  $K^n$ . Valgono:
  - **(Esistenza di soluzioni)** Se  $K$  è algebricamente chiuso, il sistema non ha soluzioni se e solo se  $1 \in I = (f_1, \dots, f_n)$ , che si vede subito se c'è o meno con una BdG
  - **(Teorema di Estensione)**  $I = (f_1, \dots, f_k)$  e supponiamo  $K$  algebricamente chiuso.  $I_1 = I \cap K[x_2, \dots, x_n]$  e  $\beta \in \mathcal{V}(I_1)$ .  $f_i = c_i(x_2, \dots, x_n) \cdot x_1^{n_i} + \dots \in K[x_2, \dots, x_n][x_1]$ . Se  $\beta \notin \mathcal{V}(c_1, \dots, c_k)$  allora  $\exists a \in K$  t.c.  $(a, \beta) \in \mathcal{V}(I)$ . Ovvero se i termini davanti alle potenze più alte di  $x_1$  non si annullano tutti su  $\beta$  allora posso estendere  $\beta$  ad una radice di  $I$ .
  - **(Conseguenza di Estensione)** Se la BdG è del tipo  $\{x_1^{N_1} + \dots, x_2^{N_2} + \dots, \dots, x_k^{N_k} + \dots\}$  (deve essere di questa forma in tutte le variabili) allora la varietà è finita.
  - **(Soluzioni finite)**  $K$  algebricamente chiuso.  $I \subseteq A$ . Allora sono fatti equivalenti:
    - \*  $|\mathcal{V}(I)| < \infty$  ( $\mathcal{V}(I)$  è costituita da un numero finito di punti)
    - \*  $\forall i = 1, \dots, n \quad \exists m_i$  t.c.  $x_i^{m_i} \in \text{lt}(I)$
    - \*  $G = \{g_1, \dots, g_r\}$  BdG di  $I$  allora  $\forall i = 1, \dots, n \quad \exists h_i \in \mathbb{N} \quad \exists g_r \in G$  t.c.  $\text{lt}(g_r) \mid x_i^{h_i}$
    - \*  $\dim_K \frac{A}{I} < \infty$
    - \*  $\dim I = 0$  (come dimensione di Krull)

Inoltre vale che una  $K$ -base di  $\frac{A}{I}$  è  $\{x^\alpha \text{ t.c. } x^\alpha \notin \text{lt}(I)\}$ , e anche  $\dim_K \frac{A}{I} = |\mathcal{V}(I)|$   
 Osservazione: Il nullstellensatz serve solo per la freccia che  $|\mathcal{V}(I)| < \infty$  implica una delle altre. Per le frecce inverse non serve.

## IDEALI E VARIETÀ

Siano  $I, J, H \subseteq K[x_1, \dots, x_n]$  ideali e  $V$  varietà affine. Allora vale

- $I \subseteq J \implies \mathcal{V}(J) \subseteq \mathcal{V}(I)$
- $I \subseteq \mathcal{I}(\mathcal{V}(I))$
- $\mathcal{V}(\mathcal{I}(V)) = V$
- $\mathcal{V}(I) \subseteq \mathcal{V}(J) \implies \mathcal{I}(\mathcal{V}(J)) \subseteq \mathcal{I}(\mathcal{V}(I))$
- $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$
- $\mathcal{V}(I \cdot J) = \mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$
- $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$

- $\mathcal{V}(I, JH) = \mathcal{V}(I, J) \cup \mathcal{V}(I, H)$

Valgono inoltre i seguenti fatti:

- $V$  è irriducibile  $\implies \exists$  primo t.c.  $V = \mathcal{V}(\mathfrak{p})$  (il viceversa è vero se  $K$  è algebricamente chiuso)
- Ogni varietà affine si decompone come unione di un numero finito di varietà irriducibili. Tale decomposizione si può minimizzare nel modo seguente: se compaiono due varietà irriducibili una contenuta dentro l'altra si toglie dall'unione la più piccola. La decomposizione minimalizzata è unica a meno dell'ordine con cui compaiono i fattori irriducibili
- $V = \{\alpha\}$  con  $\alpha = (\alpha_1, \dots, \alpha_n)$  allora  $\mathcal{I}(V) = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$  è un ideale massimale. (Se  $K$  è algebricamente chiuso allora  $I$  è massimale se e solo se è di quella forma)
- **(Nullstellensatz)**  $K$  algebricamente chiuso. Allora  $I \subseteq K[x_1, \dots, x_n]$  e si ha:
  - **(Forma debole)**  $\mathcal{V}(I) = \emptyset \Leftrightarrow 1 \in I$
  - **(Forma forte)**  $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$
- **(Normalizzazione di Nöther)**  $K$  infinito. Se  $f$  è un polinomio in  $K[x_1, \dots, x_n]$  t.c.  $f \notin I_1 = K[x_2, \dots, x_n]$  (ovvero  $x_1$  compare) allora  $\exists \phi$  cambio lineare di coordinate tale che  $\phi(f) = c \cdot x_1^N + \bar{f}$  con  $\deg_{x_1} \bar{f} < N$  e  $c \neq 0$  costante.
- $K$  algebricamente chiuso. Se  $I$  è radicale allora  $I = \bigcap_{i=1}^k P_i$  con  $P_i$  primi. (Basta decomporre la varietà)

## RISULTANTE

- **(Definizione di Risultante)** Sia  $R$  un dominio d'integrità,  $f, g \in R[x]$  e  $f = \sum_{i=0}^n a_i x^i$ ,  $g = \sum_{i=0}^m b_i x^i$ . Definiamo allora la matrice di Sylvester come

$$\text{Sylv}(f, g) = \begin{bmatrix} a_0 & a_1 & \dots & \dots & a_n & 0 & \dots & \dots & \dots & 0 \\ 0 & a_0 & a_1 & \dots & \dots & a_n & 0 & \dots & \dots & 0 \\ \vdots & & & \ddots & & & \ddots & & & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & \dots & a_n & \dots & 0 \\ \hline b_0 & b_1 & \dots & b_m & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_m & 0 & \dots & \dots & \dots & 0 \\ 0 & 0 & b_0 & b_1 & \dots & b_m & 0 & \dots & \dots & 0 \\ \vdots & & & \ddots & & & \ddots & & & \vdots \\ 0 & \dots & \dots & 0 & b_0 & b_1 & \dots & \dots & b_m & 0 \end{bmatrix}$$

Ed il risultante di  $f$  e  $g$  è  $\text{Ris}(f, g) = \det \text{Sylv}(f, g)$

- **(Definizione alternativa)**  $\text{Ris}(f, g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j) = a_n^m \cdot \prod_{f(\alpha_i)=0} g(\alpha_i) = (-1)^{mn} b_m^n \cdot \prod_{g(\beta_j)=0} f(\beta_j)$  dove le  $\alpha_i$  e le  $\beta_j$  sono le radici rispettivamente di  $f$  e di  $g$ , con molteplicità
- **(Proprietà del risultante)** Valgono le seguenti proprietà:
  - $\text{Ris}(f, g) = (-1)^{mn} \text{Ris}(g, f)$
  - $\text{Ris}(af, g) = a^n \text{Ris}(f, g)$  con  $a \in R$  scalare
  - $\text{Ris}(f, ag) = a^m \text{Ris}(f, g)$  con  $a \in R$  scalare
  - $\text{Ris}(a, b) = 1$  dove  $a, b \in R$  sono scalari
  - $\text{Ris}(f, g) = 0 \Leftrightarrow \exists \alpha \in \overline{R}$  t.c.  $f(\alpha) = g(\alpha) = 0$  (ovvero il risultante è nullo se e solo se  $f$  e  $g$  hanno una radice in comune nella chiusura algebrica del campo delle frazioni di  $R$ ). Inoltre, se  $R$  è UFD allora le due precedenti sono equivalenti a  $\exists h \in R[x]$  t.c.  $\deg h > 0, h \mid f, h \mid g$
  - $f, g \in R[x]$  e  $\deg f = n, \deg g = m$ , allora  $\text{Ris}(f, g) = Af + Bg$  con  $A, B \in R[x]$  e  $\deg A < m, \deg B < n$

- $\text{Ris}(f, h_1 \cdot h_2) = \text{Ris}(f, h_1) \cdot \text{Ris}(f, h_2)$
- $\text{Ris}(f, hf + g) = a_m^{\deg(hf+g)} \cdot \text{Ris}(f, g)$  [ATTENZIONE: della formula a fianco non sono completamente sicuro]
- In molti casi vale che  $\text{Ris}(f, g)|_\alpha = \text{Ris}(f|_\alpha, g|_\alpha)$  dove con  $|_\alpha$  si intende la valutazione in  $\alpha$ . Bisogna solo stare attenti che almeno uno dei coefficienti direttivi valutati sia non nullo, altrimenti cambia la dimensione della matrice di Sylvester e di conseguenza anche il polinomio che definisce il risultante
- Può essere comodo sapere che, detti  $a_i$  e  $b_j$  i coefficienti di  $f$  e di  $g$ , si ha che  $\text{Ris}(f, g) \in \mathbb{Z}[a_i, b_j]$
- **(Trucchi utili con il risultante)** Dati  $f = \prod_i (x - \alpha_i)$  e  $g = \prod_j (x - \beta_j)$ , allora si possono costruire i seguenti polinomi:
  - $\text{Ris}_y(f(x - y), g(y))$  ha radici  $\gamma_{i,j} = \alpha_i + \beta_j$
  - $\text{Ris}_y(f(x + y), g(y))$  ha radici  $\gamma_{i,j} = \alpha_i - \beta_j$
  - $\text{Ris}_y(y^{\deg f} f(\frac{x}{y}), g(y))$  ha radici  $\gamma_{i,j} = \alpha_i \cdot \beta_j$
  - Se  $g(0) \neq 0$  allora  $\text{Ris}_y(f(xy), g(y))$  ha radici  $\gamma_{i,j} = \frac{\alpha_i}{\beta_j}$

## MODULI

### PRIMI FATTI

- **(Fregatura dei Moduli)** Attenzione che le seguenti cose non sono sempre vere su moduli generici:
  - Non sempre esiste una base
  - Un sistema di generatori minimale non è necessariamente una base
  - Un insieme libero massimale non è necessariamente una base
  - Due sistemi di generatori minimali non hanno necessariamente la stessa cardinalità (e nemmeno gli insiemi liberi massimali)
- **(Omomorfismi di A-Moduli)** Dati due  $A$ -Moduli  $M$  ed  $N$ , allora si ha che anche  $\text{Hom}_A(M, N)$  è un  $A$ -modulo con le operazioni di somma e di prodotto scalare effettuate in arrivo. (Notare che questa proprietà è particolarmente strana e ci tornerà utile più volte).  
Inoltre si può notare come dato un omomorfismo  $f : M \rightarrow N$  di  $A$ -moduli si ha che  $\text{Ker } f = \{m \in M \mid f(m) = 0\}$  ed  $\text{Im } f = \{f(m) \mid m \in M\}$  sono entrambi due sottomoduli rispettivamente di  $M$  e di  $N$ . Allora possiamo anche sempre definire  $\text{coKer } f = \frac{N}{\text{Im } f}$
- **(Fatti di base e definizioni di operazioni importanti)** Valgono le seguenti cose:
  - $\text{Hom}_A(A, M) \cong_{A\text{-mod}} M$ . Infatti conoscere il valore di  $f(1)$  caratterizza tutto l'omomorfismo  $f$ , visto che è di  $A$ -moduli
  - $L \subseteq N \subseteq M$  allora vale  $\frac{M}{N} \cong_{A\text{-mod}} \frac{\frac{M}{L}}{\frac{N}{L}}$
  - $M_1, M_2 \subseteq M$  sottomoduli.  $M_1 + M_2 := \{m_1 + m_2 \mid m_1 \in M_1, m_2 \in M_2\}$  allora vale che  $\frac{M_1 + M_2}{M_2} \cong_{A\text{-mod}} \frac{M_1}{M_1 \cap M_2}$
  - **( $\frac{A}{I}$ -moduli)** Dato  $I \subseteq A$  ideale ed  $M$  modulo si può definire  $IM = \{\sum_i a_i m_i \mid a_i \in I, m_i \in M\}$  e si verifica che è un sottomodulo di  $M$ . Inoltre vale che  $\frac{M}{IM}$  è anche un  $\frac{A}{I}$ -modulo.  
Possiamo invece notare che  $M$  non è sempre un  $\frac{A}{I}$ -modulo. Ci possiamo però riuscire se  $I \subseteq (0 : M) = \{a \in A \mid aM \subseteq (0)\}$ .
  - **(Somma diretta e prodotto)** Dati  $\{M_i\}_{i \in I}$  una famiglia di  $A$ -moduli si definisce

$$\oplus_i M_i = \{(a_i)_{i \in I} \mid a_i \in M_i, a_i \neq 0 \text{ solo per un numero finito di indici}\}$$

Inoltre si definisce

$$\prod_i M_i = \{(a_i)_{i \in I} \mid a_i \in M_i\}$$

senza la condizione di sopra.

Se l'insieme  $I$  di indici è finito allora si ha che  $\oplus_i M_i = \prod_i M_i$ . Valgono inoltre le seguenti proprietà universali per somma diretta e prodotto:

- \* Dati  $\{M_i\}_{i \in I}$   $A$ -moduli, si hanno  $M_i \hookrightarrow^{j_i} \oplus_i M_i$  date da  $m_i \mapsto (0, \dots, 0, m_i, 0, \dots)$ . Allora per ogni assegnamento di  $\{\varphi_i\}_{i \in I}$  con  $\varphi_i : M_i \rightarrow N$  omomorfismi di  $A$ -moduli, esiste unico  $\tilde{\phi} : \oplus_i M_i \rightarrow N$  tale che  $\varphi_i = \tilde{\phi} \circ j_i$
- \* Dati  $\{M_i\}_{i \in I}$   $A$ -moduli, si hanno  $\prod_i M_i \twoheadrightarrow^{\pi_i} M_i$  le proiezioni date da  $m = (m_j)_{j \in I} \mapsto m_i$ . Allora per ogni assegnamento di  $\{\varphi_i\}_{i \in I}$  con  $\varphi_i : N \rightarrow M_i$  omomorfismi di  $A$ -moduli, esiste unico  $\tilde{\phi} : N \rightarrow \prod_i M_i$  tale che  $\varphi_i = \pi_i \circ \tilde{\phi}$
- **(Morfismi da un modulo libero)** Sia  $M$  un  $A$ -modulo libero e sia  $S = \{s_1, \dots, s_k\}$  una sua base. Allora dati  $n_1, \dots, n_k \in N$  ( $N$  è un altro  $A$ -modulo) si ha che  $\exists! \Phi : M \rightarrow N$  tale che  $\Phi(s_i) = n_i$ ,  $\Phi$  morfismo di  $A$ -moduli
- **(Rango di un modulo libero)** Sia  $M$  un  $A$ -modulo libero con base  $B = \{b_1, \dots, b_k\}$  finita. Allora ogni altra base di  $M$  ha cardinalità  $k$ . Se  $M$  è libero con base di cardinalità  $k$  si dice che  $M$  ha rango  $k$  ( $\text{rk } M = k$ )
- $\text{Hom}_A(A^n, M) \cong M^n$ .
- $M$  è un  $A$ -modulo finitamente generato  $\Leftrightarrow M \cong \frac{A^k}{\text{Ker } \varphi}$  per un certo  $k \in \mathbb{N}$  e per un certo  $\varphi$ . Se  $M = \langle m_1, \dots, m_k \rangle$  si ha  $\varphi : A^k \rightarrow M$  definito da  $e_i \mapsto m_i$ . Allora  $M \cong \frac{A^k}{\text{Ker } \varphi}$ . Il viceversa è ovvio.
- **(Hamilton-Cayley)** Sia  $M$  un  $A$ -modulo finitamente generato,  $I \subseteq A$  ideale. Sia  $\varphi \in \text{Hom}_A(M, M)$  endomorfismo tale che  $\phi(M) \subseteq IM$ . Allora  $\exists b_0, \dots, b_{n-1} \in I$  t.c.  $\phi^n + \sum_{i=0}^{n-1} a_i \phi^i = 0$  in  $\text{Hom}_A(M, M)$
- **(Nakayama)** Come corollario di Hamilton-Cayley si ottengono le seguenti tre versioni di Nakayama:
  - Sia  $M$  un  $A$ -modulo finitamente generato,  $I \subseteq A$  ideale t.c.  $M = IM$ . Allora  $\exists a \in A$  t.c.  $a \equiv 1 \pmod{I}$  e  $a \cdot M = 0$  (Basta applicare HC a  $\varphi = \text{id}$ )
  - Sia  $M$  un  $A$ -modulo finitamente generato,  $\mathcal{J}(A)$  radicale di Jacobson,  $I \subseteq \mathcal{J}(A)$  ideale di  $A$  tale che  $M = IM$ . Allora  $M = 0$  (Usiamo il Nakayama precedente ed usiamo la caratterizzazione del radicale di Jacobson)
  - Sia  $M$  un  $A$ -modulo finitamente generato,  $N$  un sottomodulo,  $I \subseteq \mathcal{J}(A)$  ideale di  $A$ . Se  $M = N + IM$  allora  $M = N$  (Usando il Nakayama precedente basta mostrare che  $\frac{M}{N} = I(\frac{M}{N})$  così che  $\frac{M}{N} = (0) \Rightarrow M = N$  e questo è piuttosto semplice)

Come corollario otteniamo che se  $A$  è un anello locale e  $\mathfrak{m}$  un suo ideale massimale,  $M$  un  $A$ -modulo finitamente generato. Allora se  $n_1, \dots, n_k$  sono elementi di  $M$  tali che si ha che  $\overline{n_1}, \dots, \overline{n_k}$  generato  $\frac{M}{\mathfrak{m}M}$  allora  $n_1, \dots, n_k$  generano  $M$  (considerare  $N \hookrightarrow M \twoheadrightarrow \frac{M}{\mathfrak{m}M}$ )

- Sia  $M$  un  $A$ -modulo finitamente generato,  $f \in \text{End}_A(M)$  surgettivo  $\Rightarrow f$  è un isomorfismo.
- **(Functori  $f^*$  e  $g_*$ )** Se ho  $f : P \rightarrow M$  allora posso considerare  $f^* : \text{Hom}_A(M, N) \rightarrow \text{Hom}_A(P, N)$  definito da  $\phi \mapsto \phi \circ f$ . Notiamo che è contravariante. Inoltre dato  $g : M \rightarrow P$  si ha  $g_* : \text{Hom}_A(N, M) \rightarrow \text{Hom}_A(N, P)$  definito da  $\psi \mapsto g \circ \psi$ , che è covariante.

## OMOMORFISMI TRA MODULI LIBERI E FORMA NORMALE DI SMITH

- Ogni elemento di  $\text{Hom}_A(A^m, A^n)$  si può rappresentare in modo unico come matrice, quindi mi basta sapere dove vanno gli  $e_i$  base di  $A^m$  per sapere dove vanno tutti gli altri elementi. Inoltre una matrice sarà invertibile se e solo se il suo determinante è un elemento invertibile dell'anello (Basta usare l'aggiunta sapendo che  $MM^* = (\det M)\text{id}$ )
- $S, T$  matrici si dicono equivalenti per righe se  $\exists P$  invertibile tale che  $PS = T$ , equivalenti per colonne se  $\exists Q$  invertibile tale che  $SQ = T$  e si dicono equivalenti se  $\exists P, Q$  tali che  $PSQ = T$

- Se  $A$  è PID, allora si ha che ogni matrice è equivalente ad una matrice diagonale ( $D$  si dice diagonale se  $D_{ij} = 0$  quando  $i \neq j$ ).  
Il trucco fondamentale è che sui blocchetti  $2 \times 2$  riesco a triangularli. Infatti, usando che  $A$  è PID si ha  $d = \text{MCD}(a, b)$  e quindi  $\exists s, t$  t.c.  $d = as + bt$  ovvero

$$\begin{pmatrix} a & b \\ u & v \end{pmatrix} \cdot \begin{bmatrix} s & -\frac{b}{d} \\ t & \frac{a}{d} \end{bmatrix} = \begin{pmatrix} d & 0 \\ w & x \end{pmatrix}$$

e trasponendo la relazione si riesce anche a portare in forma triangolare superiore.

Il modo generale di procedere è piuttosto semplice: con il metodo precedente si pongono a zero tutti i numeri sulla prima riga tranne il primo, a questo punto si mettono a zero tutti i numeri sulla prima colonna tranne il primo, e si procede riga-colonna fino a quando non sono nulli sia tutti i numeri sulla prima riga che sulla prima colonna (tranne ovviamente il primo). Questa cosa deve succedere prima o poi. Quando accade si ricorre per induzione sulla sottomatrice  $(n-1) \times (n-1)$  che si ottiene levando la prima riga e la prima colonna.

- **(Forma normale di Smith)**  $A$  PID. Vogliamo dare una forma canonica alle matrici che rappresentano gli omomorfismi tra moduli liberi. Una matrice diagonale  $D$  si dice in forma di Smith se  $d_1 \mid d_2 \mid \dots \mid d_n$  con  $D =$

$$D = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{pmatrix}$$

- **(Ogni matrice diagonale si può portare in forma di Smith)** Infatti data  $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$  e detto  $d = \text{MCD}(a, b) = as + bt$  si computa  $\begin{pmatrix} s & t \\ -\frac{b}{d} & \frac{a}{d} \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 1 & -\frac{tb}{d} \\ 1 & \frac{sa}{d} \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & \frac{ab}{d} \end{pmatrix}$

- **(Caratterizzazione tramite ideali determinanti)** Se  $S$  è una matrice definiamo  $\Delta_i(S)$  come l'ideale generato dai determinanti delle sottomatrici  $i \times i$  di  $S$ . Se  $S, T$   $m \times n$  sono equivalenti allora  $\Delta_i S = \Delta_i T \quad \forall i$ . Se  $D_1$  e  $D_2$  sono matrici in forma di Smith allora  $D_1$  è equivalente a  $D_2$  se e solo se  $d_i^{(1)}$  e  $d_i^{(2)}$  differiscono di un invertibile (ovvero sono associati)

- **(Sottomoduli di moduli liberi su PID)** Se  $M$  è un  $A$ -modulo libero con  $A$  PID e  $N \subseteq M$  sottomodulo, allora  $N$  è libero e inoltre vale che  $\text{rk } N \leq \text{rk } M$

- **(Teorema di struttura di moduli f.g. su PID)** Ogni modulo finitamente generato su PID si scrive come somma diretta di moduli ciclici.  $M$  f.g. su PID (ovvero è quoziente di un modulo libero).  $M = \langle m_1, \dots, m_k \rangle$ . Allora  $A^n \xrightarrow{f} M \rightarrow 0$  con  $f(e_i) = m_i$  e  $f(a_1, \dots, a_n) = \sum_i a_i m_i$  ovvero  $M \cong \frac{A^n}{\text{Ker } f}$  e  $\text{Ker } f \subseteq A^n$  è un sottomodulo di modulo libero.

Sapendo che ogni sottomodulo di modulo libero su PID è libero abbiamo che  $A^m \xrightarrow{\phi} A^k \xrightarrow{f} M \rightarrow 0$  allora  $M \cong \frac{A^m}{\text{Ker } f} \cong \frac{A^k}{\text{Im } \phi} \cong \text{coKer } \phi \cong \bigoplus_i \frac{A}{(d_i)} \cong \bigoplus_i \langle z_i \rangle$  con  $d_i = \text{Ann}(z_i)$

- Se  $M = \langle m \rangle$  è un  $A$ -modulo ciclico allora  $M \cong \frac{A}{\text{Ann}(m)}$
- $M = \frac{A}{J}$  come  $A$ -modulo. Dato  $a \in A$  si ha  $(a) \cdot M \cong \frac{A}{(J \cdot (a))}$
- $A^n \cong A^m \Leftrightarrow n = m$
- $\phi: A^m \rightarrow A^n$  surgettivo e  $m < n \implies A = 0$
- $M = \frac{A}{J_1} \oplus \frac{A}{J_2}$ , con  $I \subseteq A$  ideale. Allora valgono:

$$\begin{aligned} - IM &\cong \frac{I+J_1}{J_1} \oplus \frac{I+J_2}{J_2} \\ - \frac{M}{IM} &\cong \frac{A}{I+J_1} \oplus \frac{A}{I+J_2} \end{aligned}$$

- Sia  $M$  un  $A$ -modulo finitamente generato su PID allora  $M$  si scrive come somma diretta di moduli ciclici  $M = \langle m_1 \rangle \oplus \dots \oplus \langle m_k \rangle$



- Se ho due catene di ideali  $I_n \subseteq \dots \subseteq I_1, J_m \subseteq \dots \subseteq J_1$  con  $n \geq m$ , e supponiamo  $M = \bigoplus_{k=1}^n \frac{A}{I_k} = \bigoplus_{i=1}^m \frac{A}{J_i}$  allora  $J_1 = \dots = J_{n-m} = A$  e  $I_i = J_{n-m+i}$
- Se  $A$  è un dominio ed  $M$  un  $A$ -modulo, allora chiamiamo sottomodulo di torsione  $\tau(M) = \{m \in M \mid \text{Ann}(m) \neq 0\} \subseteq M$ .
  - $f \in \text{Hom}_A(M, N) \implies f(\tau(M)) \subseteq \tau(N)$
  - Data  $0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$  esatta  $\implies 0 \rightarrow \tau(M) \rightarrow \tau(N) \rightarrow \tau(P) \rightarrow 0$  è esatta ma non a destra
  - $M$  f.g. su  $A$  PID. Allora  $M \cong \tau(M) \oplus A^k$  per un qualche  $k$
- $M$  si dice modulo  $p$ -primario se  $\text{Ann}(M) = (p^s)$
- **(Riassunto di tutto)**  $M$  f.g. su  $A$  PID. allora valgono:
  - $M = (\bigoplus_{i=1}^m \frac{A}{(d_i)}) \oplus A^k$  con  $d_1 \mid \dots \mid d_m$  non necessariamente distinti, unicamente determinati a meno di associati. Tali  $d_i$  si chiamano fattori invarianti di  $M$ .
  - $M \cong (\bigoplus_{p_i} M_{p_i}) \oplus A^k$  dove gli  $M_{p_i}$  sono moduli ciclici  $p_i$ -primari di torsione. Tutti i  $p_1^{s_1} \dots p_r^{s_r}$  si chiamano divisori elementari di  $M$ .  
 Infatti se  $\tau(M) = \bigoplus_i \frac{A}{(d_i)}$  con  $d_i \in A$  PID allora se  $d_i = p_{i_1}^{s_{i_1}} \dots p_{i_k}^{s_{i_k}} \implies \frac{A}{(d_i)} = \bigoplus_{j=1}^k \frac{A}{p_{i_j}^{s_{i_j}}}$

## PRODOTTO TENSORE

- **(Proprietà universale)** Sia  $R$  un anello,  $M, N$  due  $R$ -moduli. Un prodotto tensore di  $M$  e  $N$  è un  $R$ -modulo denotato con  $M \otimes_R N$  con una mappa  $\tau : M \times N \rightarrow M \otimes_R N$  bilineare tale che  $\forall \phi : M \times N \rightarrow P$  bilineare (con  $P$  un generico  $R$ -modulo)  $\exists! \tilde{\phi} : M \otimes_R N \rightarrow P$  tale che  $\phi = \tilde{\phi} \circ \tau$   
 Deriva dalla definizione che se un tale modulo esiste allora è unico a meno di unico isomorfismo.  
 Si può costruire in maniera piuttosto semplice sui moduli prendendo l' $R$ -modulo libero generato dagli elementi di  $M \times N$  e quotientando per il sottomodulo delle relazioni, ovvero il generato da  $i(m_1 + m_2, n) - i(m_1, n) - i(m_2, n), i(m, n_1 + n_2) - i(m, n_1) - i(m, n_2), i(r \cdot m, n) - r i(m, n), i(m, r n) - r i(m, n)$
- **(Tensori semplici)** Una cosa della forma  $m \otimes n$  in  $M \otimes_R N$  è detto tensore semplice. L'insieme dei tensori semplici genera  $M \otimes_R N$  come  $R$ -modulo. Inoltre se  $\{m_\alpha\}$  genera  $M$  e  $\{n_\beta\}$  genera  $N$ , allora  $\{m_\alpha \otimes n_\beta\}$  genera  $M \otimes_R N$
- **(Formule di uguaglianza)** Valgono le seguenti cose, alcune ovvie alcune meno:
  - $R \otimes_R M \cong M$
  - $M \otimes_R N \cong N \otimes_R M$
  - $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P)$
  - $(M \oplus N) \otimes_R P \cong (M \otimes_R P) \oplus (N \otimes_R P)$  (vale anche per somme dirette infinite)
  - $\frac{R}{I} \otimes_R M \cong \frac{M}{IM}$
  - $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} = (M \otimes_A N)_{\mathfrak{p}}$
- **(Aggiunzione con Hom)**  $M, N, P$  tre  $R$ -moduli. Allora vale che  $\text{Hom}_R(M \otimes_R N, P) \cong \text{Hom}_R(M, \text{Hom}_R(N, P))$  dove l'isomorfismo è naturale (e vale in particolare anche a livello di  $R$ -moduli)
- **(Esattezza a destra)** Essendo aggiunto sinistro il funtore  $-\otimes_R M$  (o anche  $M \otimes_R -$ , che è canonicamente equivalente al primo) è esatto a destra, cioè:  
 $M \rightarrow N \rightarrow P \rightarrow 0$  è esatta  $\iff \forall Q \quad M \otimes Q \rightarrow N \otimes Q \rightarrow P \otimes Q \rightarrow 0$  è esatta
- **(Implicazioni varie)**
  - $M, N$  f.g.  $\implies M \otimes_R N$  f.g.
  - $M, N$  liberi  $\implies M \otimes_R N$  libero

## ANELLO E MODULO DELLE FRAZIONI

- **(Anello delle frazioni)**  $A$  anello ed  $S \subseteq A$  moltiplicativamente chiuso ( $1 \in S, s, t \in S \implies st \in S$ ). Allora l'insieme  $A \times S$  quozientato per la relazione di equivalenza  $(a, s) \sim (b, t) \iff \exists u \neq 0 \in S$  t.c.  $u(at - bs) = 0$  è un anello dotato di una mappa  $A \rightarrow \frac{A \times S}{\sim}$  tale per cui ogni elemento di  $S$  va a finire in un invertibile.  
Gode inoltre della proprietà universale per la quale per ogni altro anello  $B$  e morfismo di anelli  $g : A \rightarrow B$  tale che tutti gli elementi di  $S$  vadano a finire in elementi invertibili di  $B$ , allora questo morfismo si spezza in modo unico attraverso il passaggio per  $S^{-1}A := \frac{A \times S}{\sim}$
- **(Nullità dell'anello delle frazioni)**  $0 \in S \iff S^{-1}A = 0$
- **(Ideali di  $S^{-1}A$ )** Valgono le seguenti affermazioni sugli ideali di  $S^{-1}A$ :
  - Ogni ideale di  $S^{-1}A$  è un ideale esteso
  - Sia  $I \subseteq A$  ideale. Allora  $I^e = 1 \iff I \cap S \neq \emptyset$
  - $I^{ec} = \bigcup_{s \in S} (I : s)$
  - C'è una corrispondenza biunivoca tra gli ideali primi di  $A$  che non intersecano  $S$  ed i primi di  $S^{-1}A$ . Infatti:
    - \* Se  $Q$  è primo in  $S^{-1}A$  allora  $Q^c$  è primo in  $A$  (e questo è sempre vero)
    - \*  $P$  primo in  $A, P \cap S = \emptyset \implies S^{-1}P$  primo
  - $P_1, P_2$  ideali primi. Allora si ha  $S^{-1}P_1 = S^{-1}P_2 \implies P_1 = P_2$
  - $Q \subseteq A$  ideale  $P$ -primario. Allora se  $S \cap P \neq \emptyset$  si ha  $S^{-1}Q = S^{-1}A$   
Se  $S \cap P = \emptyset$  allora  $S^{-1}Q$  è  $S^{-1}P$ -primario ed inoltre  $(S^{-1}Q)^c = Q$
- **( $S^{-1}$  e le altre operazioni)** Potremmo dire in linea di massima che  $S^{-1}$  commuta con tutte le operazioni principali, purché siano finite:
  - $S^{-1}(I + J) = S^{-1}I + S^{-1}J$
  - $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$
  - $S^{-1}(I \cdot J) = (S^{-1}I) \cdot (S^{-1}J)$
  - $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$
- **(Modulo delle frazioni)** Sia  $M$  un  $A$ -modulo ed  $S \subseteq A$  un insieme moltiplicativamente chiuso. Allora definiamo  $S^{-1}M := \frac{S \times M}{\sim}$  dove  $(m, s) \sim (m', s') \iff \exists u \in S \quad u(s'm - sm') = 0$  ed indicheremo con  $\frac{m}{s}$  la classe di equivalenza.  
 $S^{-1}M$  ha una struttura di  $S^{-1}A$ -modulo. Inoltre si può facilmente verificare che  $S^{-1}$  è un funtore dalla categoria degli  $A$ -moduli a quella degli  $S^{-1}A$ -moduli, dove dato  $f : M \rightarrow N$  morfismo si può definire  $S^{-1}f : S^{-1}M \rightarrow S^{-1}N$  come  $(S^{-1}f)(\frac{m}{s}) = \frac{f(m)}{s}$
- **( $S^{-1}$  è un funtore esatto)** Si ha che  $S^{-1}$  è esatto, ovvero se  $M \xrightarrow{f} N \xrightarrow{g} P$  è una sequenza esatta di  $A$ -moduli allora  $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$  è una sequenza esatta di  $S^{-1}A$ -moduli.  
In particolare omomorfismi iniettivi o surgettivi rimangono rispettivamente iniettivi o surgettivi
- **( $S^{-1}$  e le altre operazioni)** Siano  $M, P \subseteq N$  sotto- $A$ -moduli,  $S \subseteq A$  moltiplicativamente chiuso. Allora  $S^{-1}$  commuta con somme finite, intersezioni finite e quozienti, ovvero vale che
  - $S^{-1}(M + P) = S^{-1}M + S^{-1}P$
  - $S^{-1}(M \cap P) = S^{-1}M \cap S^{-1}P$
  - $S^{-1}(\frac{N}{M}) \cong \frac{S^{-1}N}{S^{-1}M}$  dove l'isomorfismo è come  $S^{-1}A$ -moduli
  - Se  $M$  è f.g. allora  $\text{Ann}(S^{-1}M) = S^{-1}\text{Ann}(M)$
  - Sapendo che  $(N : P) = \text{Ann}(\frac{N+P}{N})$  si può mostrare che se  $P$  è f.g. allora  $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$

Valgono inoltre le seguenti uguaglianze furbe:

- $S^{-1}A \otimes_A M = S^{-1}M$
- $S^{-1}(M \otimes_A N) \cong S^{-1}M \otimes_{S^{-1}A} S^{-1}N$
- **(Correlazione tra anello e modulo delle frazioni e prodotto tensore)** Vale che  $S^{-1}A \otimes_A M = S^{-1}M$ . Inoltre abbiamo anche dimostrato che  $S^{-1}A$  è un  $A$ -modulo piatto, ovvero  $0 \rightarrow M \xrightarrow{f} N$  rimane iniettiva tensorizzando per il piatto, cioè  $0 \rightarrow S^{-1}A \otimes_A M \xrightarrow{S^{-1}A \otimes_A f} S^{-1}A \otimes_A N$  per l'osservazione precedente.
- **(Altri fatti)**
  - $f : A \rightarrow B$  omomorfismo di anelli,  $S \subseteq A$  moltiplicativamente chiuso e  $T = f(S)$ . Allora  $S^{-1}B \cong T^{-1}B$  come  $S^{-1}A$ -moduli
  - $S \subseteq A$  molt. chiuso. Diciamo che  $S$  è saturato se  $xy \in S \implies x \in S, y \in S$ . Si ha allora che:
    - \*  $S$  saturato  $\Leftrightarrow S = A \setminus \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$
    - \* Se  $S$  è un sistema molt. chiuso allora  $\exists! \bar{S} \subseteq \overline{S}$  con  $\bar{S}$  saturato e minimale rispetto alla proprietà di contenere  $S$ .
    - \*  $\bar{S}^{-1}A \cong S^{-1}A$

## LOCALIZZAZIONE E PROPRIETÀ LOCALI

- **(Definizione)**  $A$  anello,  $\mathfrak{p} \subseteq A$  ideale primo e consideriamo  $S = A \setminus \mathfrak{p}$  che è moltiplicativamente chiuso. Allora  $A_{\mathfrak{p}} := S^{-1}A$  si dice localizzazione a  $\mathfrak{p}$ . Si ha che  $A_{\mathfrak{p}}$  è un anello locale, dove l'unico ideale massimale è  $\mathfrak{p}_{\mathfrak{p}} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$
- **(Proprietà locali)**  $P$  è una proprietà per  $A$  anello oppure per  $M$  modulo si dice che è locale se  $P$  vale per  $A$  (o per  $M$ )  $\Leftrightarrow P$  vale per  $A_{\mathfrak{p}}$  (o  $M_{\mathfrak{p}}$ )  $\forall \mathfrak{p}$  primo
- **(Essere nullo è una proprietà locale (e anche massimale))**  $M$  un  $A$ -modulo. TFAE:
  - $M = 0$
  - $M_{\mathfrak{p}} = 0 \quad \forall \mathfrak{p}$  primo
  - $M_{\mathfrak{m}} = 0 \quad \forall \mathfrak{m}$  massimale
- **(Per un omomorfismo essere iniettivo (o surgettivo) è una proprietà locale (e anche massimale))** Sia  $f : M \rightarrow N$ . TFAE:
  - $f$  iniettivo (surgettivo)
  - $f_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$  iniettivo (surgettivo)  $\forall \mathfrak{p}$  primo
  - $f_{\mathfrak{m}} : M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$  iniettivo (surgettivo)  $\forall \mathfrak{m}$  massimale

Per l'iniettività basta mostrare che  $\text{Ker } f_{\mathfrak{p}} = (\text{Ker } f)_{\mathfrak{p}}$  e usare che  $M = 0$  è locale. Uguale per la surgettività con i  $\text{coKer}$
- **(Essere ridotto è una proprietà locale)** Un anello infatti è ridotto se  $\mathcal{N}(A) = 0$  e abbiamo mostrato che  $S^{-1}\mathcal{N}(A) = \mathcal{N}(S^{-1}A)$ , ovvero  $\mathcal{N}(A) = 0 \Leftrightarrow \mathcal{N}(A)_{\mathfrak{p}} = \mathcal{N}(A_{\mathfrak{p}}) = 0 \quad \forall \mathfrak{p}$  primo
- **(Dominio NON è una proprietà locale)**

## SUCCESSIONI ESATTE DI MODULI

- La successione  $M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \rightarrow 0$  è esatta  $\Leftrightarrow$  la successione  $0 \rightarrow \text{Hom}_A(M_2, N) \xrightarrow{g^*} \text{Hom}_A(M, N) \xrightarrow{f^*} \text{Hom}_A(M_1, N)$  è esatta  $\forall N$   $A$ -moduli.
- La successione  $0 \rightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2$  è esatta  $\Leftrightarrow$  la successione  $\text{Hom}_A(N, M_1) \xrightarrow{f^*} \text{Hom}_A(N, M) \xrightarrow{g^*} \text{Hom}_A(N, M_2) \rightarrow 0$  è esatta  $\forall N$   $A$ -moduli.
- **(Successioni che spezzano)** Data una successione esatta corta di  $A$ -moduli  $0 \rightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \rightarrow 0$  si ha TFAE:

- $N \cong M \oplus P$
- $\exists r : N \rightarrow M$  t.c.  $r \circ \alpha = \text{id}_M$
- $\exists s : P \rightarrow N$  t.c.  $\beta \circ s = \text{id}_P$
- **(Proprietà estremi-intermedio)** Sia  $0 \rightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} P \rightarrow 0$  una successione esatta di  $A$ -moduli. Allora valgono le seguenti:

- $M, P \text{ f.g.} \implies N \text{ f.g.}$
- **(Moduli Proiettivi)**  $P$  si dice proiettivo se vale una delle seguenti, tutte equivalenti:
  - Data  $\phi : M \rightarrow N$  surgettivo si ha  $\forall f : P \rightarrow N, \exists g : P \rightarrow M$  tale che  $f = \phi \circ g$
  - $\forall g : M \rightarrow N$  surgettiva l'omomorfismo indotto  $\text{Hom}_A(P, M) \xrightarrow{g^*} \text{Hom}_A(P, N)$  è surgettivo
  - Ogni successione esatta corta  $0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$  spezza
  - $P$  è sommando diretto di un modulo libero (ovvero  $\exists F$  libero t.c.  $F = P \oplus C$ )
  - $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$  esatta  $\Leftrightarrow 0 \rightarrow \text{Hom}_A(P, K) \rightarrow \text{Hom}_A(P, M) \rightarrow \text{Hom}_A(P, N) \rightarrow 0$  esatta
  - Ovvero anche  $\text{Hom}_A(P, -)$  è un funtore esatto

Hanno inoltre le seguenti proprietà rispetto ad alcune costruzioni:

- $P_1 \oplus P_2$  proiettivo  $\Leftrightarrow P_1$  e  $P_2$  sono proiettivi
- $P_1, P_2$  proiettivi  $\implies P_1 \otimes_R P_2$  proiettivo (il viceversa non vale)
- **(Moduli Iniettivi)**  $Q$  si dice modulo iniettivo se vale una delle seguenti, tutte equivalenti:
  - Per ogni  $f : N \hookrightarrow M$  iniettiva e  $g : N \rightarrow Q$  si ha  $\exists G : M \rightarrow Q$  tale che  $g = G \circ f$
  - Ogni successione esatta  $0 \rightarrow Q \rightarrow M \rightarrow N \rightarrow 0$  spezza
  - Per ogni  $I \subseteq A$  ideale vale la caratterizzazione (1) con  $N = I$  e  $M = A$   
Si può dire anche per ogni  $I$  ideale di  $A$  si ha che ogni  $f : I \rightarrow Q$  si estende ad una funzione  $\tilde{f} : A \rightarrow Q$
  - $0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0$  esatta  $\Leftrightarrow 0 \rightarrow \text{Hom}_A(N, Q) \rightarrow \text{Hom}_A(M, Q) \rightarrow \text{Hom}_A(K, Q) \rightarrow 0$  esatta
  - Ovvero anche  $\text{Hom}_A(-, Q)$  è un funtore esatto
- **(Moduli Piatti)**  $N$  è un  $R$ -modulo piatto se il funtore  $N \otimes_R -$  è esatto  
Valgono le seguenti proprietà rispetto alle costruzioni:
  - $N, M$  piatti  $\Leftrightarrow N \oplus M$  piatto
  - $N, M$  piatti  $\implies N \otimes_R M$  piatto (il viceversa non vale)
  - $S^{-1}R$  è un  $R$ -modulo piatto  $\forall S \subseteq R$  moltiplicativamente chiusi

Per quozienti si può controllare la piatezza sapendo che le seguenti sono equivalenti:

- $a \in a^2 A$
- $aA$  è sommando diretto di  $A$
- $\frac{A}{aA}$  è  $A$ -piatto
- **(Implicazioni varie)**
  - Libero  $\implies$  Proiettivo (Il viceversa vale se  $A$  è PID oppure anche se  $A$  è locale e  $P$  f.g.)
  - Proiettivo  $\implies$  Piatto (Viene da Libero  $\implies$  Piatto, piuttosto semplice da mostrare usando che  $L = \bigoplus_{\mathbb{N}} R^{(\mathbb{N})}$  se  $L$  è libero ed utilizzando il fatto che un modulo proiettivo è un sommando diretto di un modulo libero).
  - Il viceversa non vale. Ad esempio  $\mathbb{Q}$  come  $\mathbb{Z}$ -modulo
- **(Lemma del Serpente)**
- **(Lemma dei cinque)**

## MODULI NÖTHERIANI ED ARTINIATI

---

- **(Definizione)** Se  $(\Sigma, \leq)$  è un insieme parzialmente ordinato allora sono equivalenti:

- Ogni catena ascendente è stazionaria
- Ogni sottoinsieme diverso dal vuoto ha un elemento massimale

Sia ora  $A$  un anello,  $M$  un  $A$ -modulo e  $\Sigma = \{N \subseteq M \text{ sottomodulo}\}$ . Se  $(\Sigma, \subseteq)$  soddisfa una delle due condizioni equivalenti di cui sopra,  $M$  viene detto  $A$ -modulo Nötheriano [ACC]

Se invece è  $(\Sigma, \supseteq)$  a soddisfare una delle due condizioni,  $M$  viene detto  $A$ -modulo Artiniano [DCC]

Un anello  $A$  si dice Artiniano (Nötheriano) se è Artiniano (Nötheriano) come  $A$ -modulo su sè stesso

- **(Condizione equivalente alla Nötherianità)**  $M$  è un  $A$ -modulo Nötheriano  $\Leftrightarrow$  ogni sottomodulo è f.g.
- **(Passaggio per sequenze esatte)** Sia  $0 \rightarrow M \rightarrow N \rightarrow P \rightarrow 0$  una sequenza esatta corta. Allora vale che:
  - $N$  Nötheriano  $\Leftrightarrow M, P$  Nötheriani
  - $N$  Artiniano  $\Leftrightarrow M, P$  Artiniani

Come corollari si ottengono i seguenti:

- $M_1, \dots, M_n$  Nötheriani  $\Leftrightarrow \oplus_i M_i$  Nötheriano
- $A$  Nötheriano e  $M$   $A$ -modulo f.g.  $\Rightarrow M$  Nötheriano
- $A$  Nötheriano e  $I \subseteq A$  ideale  $\Rightarrow \frac{A}{I}$  Nötheriano
- $f: A \twoheadrightarrow B$  surgettiva. Allora  $A$  Nötheriano  $\Rightarrow B$  Nötheriano
- $A$  Nötheriano  $\Rightarrow S^{-1}A$  Nötheriano (per la corrispondenza tra ideali)
- Vale inoltre che  $A$  Nötheriano  $\Rightarrow A[x]$  Nötheriano (Base di Hilbert)
- **(Lemmi per i Nötheriani)** Valgono le seguenti cose a caso:
  - $A$  Nötheriano. Ogni ideale contiene allora una potenza del suo radicale, ovvero  $\forall I \subseteq A \quad \exists n \text{ t.c. } (\sqrt{I})^n \subseteq I$
  - $A$  Nötheriano,  $\mathfrak{m}$  ideale massimale. Allora TFAE:
    - \*  $Q$  è  $\mathfrak{m}$ -primario
    - \*  $\sqrt{Q} = \mathfrak{m}$
    - \*  $\exists n \quad \mathfrak{m}^n \subseteq Q \subseteq \mathfrak{m}$
- **(Teoremi per gli Artiniani)**
  - $A$  è Artiniano  $\Leftrightarrow A$  è Nötheriano e  $\dim A = 0$  [Non dimostrato]
  - **(Teorema di Struttura per anelli artiniani)**  $A$  è Artiniano  $\Leftrightarrow A = \oplus_i A_i$  con gli  $A_i$  Artiniani e Locali. La decomposizione è unica a meno di isomorfismi [Non dimostrato]
  - $A$  Artiniano  $\Rightarrow A$  semilocale

## DECOMPOSIZIONE PRIMARIA

---

- **(Decomposizione primaria di un ideale)**  $I \subseteq A$  ideale si dice decomponibile se si può scrivere come intersezione di un numero finito di ideali primari  $Q_1, \dots, Q_n$  come  $I = \cap_i Q_i$ . (Definiamo inoltre primi associati ad una decomposizione  $P_i := \sqrt{Q_i}$ )
- **(Minimalizzazione di una decomposizione)** Se  $P_i = P_j$  in una decomposizione allora vale che  $Q_i \cap Q_j$  è ancora primario e posso quindi sostituirlo al posto di  $Q_i$  e  $Q_j$  (Vale ancora che  $\sqrt{Q_i \cap Q_j} = P_i = P_j$ ). Una decomposizione si dice minimale o irridondante se  $P_i \neq P_j \quad \forall i \neq j$  e  $\cap_{i \neq j} Q_j \not\subseteq Q_i$

- **(Proposizione tecniche)**  $Q$  primario e  $P = \sqrt{Q}$ ,  $a \in A$ . Allora valgono le seguenti:
  - Se  $a \in Q$  si ha  $(Q : a) = 1$
  - Se  $a \notin Q$  allora  $(Q : a)$  è  $P$ -primario, ovvero  $Q : a$  è primario e  $\sqrt{Q : a} = P$
  - Se  $a \notin P$  allora  $(Q : a) = Q$
- **(Unicità dei primi associati)** Sia  $I = \cap_{i=1}^n Q_i$  con  $\sqrt{Q_i} = P_i$  e supponiamo la scrittura minimale. Allora i  $P_i$  sono indipendenti dalla decomposizione ed inoltre vale che  $\{P_1, \dots, P_n\} = \{\sqrt{I : a} \text{ primi} \mid a \in A\}$  (Ovvero  $\forall a \in A$  faccio  $\sqrt{I : a}$ . Se  $\sqrt{I : a}$  è primo allora lo prendo).
- **(Primi minimali)** Data una decomposizione minimale di  $I$ , considero i primi associati  $P_i$ . Tra questi posso considerare i primi minimali per inclusione (detti primi minimali). In particolare i primi minimali associati ad  $I$  sono quelli tali che  $\forall P$  primo tale che  $I \subseteq P$  allora si ha  $\exists i$  tale che  $P_i \subseteq P$  dove  $P_i$  è un primo minimale.
- **(Nilradicale)** In particolare se  $(0)$  è decomponibile allora  $\mathcal{N}(A) = \cap_{P_i \text{ minimali di } (0)} P_i$
- **(Caratterizzazione dell'unione dei primi associati)**  $I = \cap_i Q_i$  minimale con  $P_i = \sqrt{Q_i}$  allora  $\{a \in A \mid (I : a) \neq I\} = \cup_i P_i$
- **(Divisori di Zero)** Se  $(0)$  è decomponibile allora si ha  $\mathcal{D}(A) = \cup_{0 \neq a \in A} \sqrt{0 : a}$  e se  $(0) = \cap_i Q_i$  allora  $\sqrt{0 : a} = \cap_{a \notin Q_i} \sqrt{Q_i : a} = \cap_{a \notin Q_i} P_i \subseteq P_i$ , ovvero  $\mathcal{D}(A) \subseteq \cup_i P_i$  e visto che  $P_i = \sqrt{0 : a}$  si ha  $P_i \subseteq \mathcal{D}(A)$
- **(Decomposizione Primaria con  $S^{-1}$ )**  $S \subseteq A$  e  $I = \cap_i Q_i$  minimale. Siano inoltre  $P_1, \dots, P_m, P_{m+1}, \dots, P_n$  i primi associati ordinati in modo che  $S \cap P_i = \emptyset$  con  $i \leq m$  e che  $S \cap P_j \neq \emptyset$  se  $j \geq m+1$ . Allora si ha che  $S^{-1}I = \cap_i S^{-1}Q_i = \cap_{i \leq m} S^{-1}Q_i$  e quindi  $(S^{-1}I)^c = Q_1 \cap \dots \cap Q_m$ . "Facendo così abbiamo ucciso le componenti i cui primi intersecano  $S$ "
- **(Unicità dei primari minimali)** Per il lemma di sopra abbiamo l'unicità dei primari minimali. Infatti visto che  $P_i$  è minimale si ha  $S = A \cap P_i$  e allora  $S \cap P_j \neq \emptyset \quad \forall j \neq i$  e quindi  $Q_i$  non dipende dalla decomposizione perché anche i  $P_i$  non dipendono dalla decomposizione.
- **(Esistenza della Decomposizione Primaria)** Mostriamo che in un anello Nötheriano ogni ideale è decomponibile, nei seguenti due step:
  - Dimostriamo prima che  $I \subseteq A$  ideale, con  $A$  Nötheriano, allora  $I = \cap_i I_i$  dove gli  $I_i$  sono ideali irriducibili (ovvero tali che  $I_i = J \cap K \implies I_i = J$  oppure  $I_i = K$ )
  - Ogni irriducibile in un Nötheriano è primario