

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 $\frac{A}{\frac{A}{J}} \cong \frac{A}{J}$
Si ha inoltre la corrispondenza tra gli ideali di $\frac{A}{J}$ 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 ϕ 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

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'escalier 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 $\beta \in \mathcal{V}(I_1)$. $f_i = c_i(x_2, \dots, x_n) \cdot x_1^{n_1} + \dots \in K[x_2, \dots, x_n][x_1]$. 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 β allora posso estendere β 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 $I = \cap_{i=1}^k P_i$ 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 α_i e le β_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 α . 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 $\Phi(s_i) = n_i$, Φ 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 φ . 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 SCHMIDT

- 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 $MM^* = (\det M)\text{id}$)

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.