ALGEBRA 2

ANELLI

- Se A è un anello finito allora $A = A^* \sqcup \mathcal{D}(A)$
- $f : A \to B$ allora 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 dominio) a primo $\implies$ a irriducibile
- (A UFD) a irriducibile $\implies$ a primo
- Se $H \subseteq A \times B$ è ideale allora $H = I \times J$ con $I \subseteq A$, $J \subseteq B$ ideali
- $A \cong A_1 \times A_2 \Leftrightarrow \exists e \in A, e \neq 0, 1 \quad e^2 = e$
- $\mathcal{D}(A) = \cup_{a \notin A^*}(0 : a) = \cup_{a \notin A^*} \sqrt{(0 : a)}$ e $\sqrt{\mathcal{D}(A)} = \mathcal{D}(A)$, 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 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**) $P_1, \ldots, P_n$ ideali primi. Sia $I \subseteq A$ ideale t.c. $I \subseteq \cup_{i=1}^n P_i$. Allora $\exists j$ t.c. $I \subseteq P_j$
- $I_1, \ldots, I_n$ ideali e P ideale primo. $\cap_{i=1}^n I_i \subseteq P \implies \exists j$ t.c. $I_j \subset P$. Inoltre se $P = \cap_i I_i$ allora $\exists j$ t.c. $I_j = P$
- (**Teorema cinese**) Siano $I_1, \ldots, I_n \subseteq A$ ideali tali che $I_i + I_j = 1$. Allora $\forall a_1, \ldots, a_n \in A \quad \exists a \in A$ t.c. $a \equiv a_i (I_i)$
- 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 $\phi : A \to B$ 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.
- (**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 $K[x_1, \ldots, x_n]$ è un ideale generato dai monomi

- (**Criterio di appartenenza**) Sia I un ideale monomiale e $f \in K[x_1, \ldots, x_n]$, $f = \sum_\beta c_\beta x^\beta$ con $c_\beta \in K$. Allora $f \in K \Leftrightarrow \forall \beta x^\beta \in I$
- (**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 $I_1 = (m_1, \ldots, m_k)$ e $I_2 = (n_1, \ldots, n_s)$ con m_i, n_j monomi. Allora si ha
  - $I_1 + I_2 = (m_1, \ldots, m_k, n_1, \ldots, n_s)$
  - $I_1 \cap I_2 = (\text{MCD}_{i,j}(m_i, n_j))$
  - $I_1 \cdot I_2 = (m_i \cdot n_j)_{i,j}$
  - (**Iatto**) $(I, m \cdot n) = (I, m) \cap (I, n)$ se MCD $(m, n) = 1$ come monomi
  - I primo $\Leftrightarrow$ $I = (x_{i_1}, \ldots, x_{i_k})$ (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 $\Leftrightarrow I = (x_{i_1}^{\alpha_1}, \ldots, x_{i_k}^{\alpha_k}, m_1, \ldots, m_s)$ dove $m_1, \ldots, m_s \in K[x_{i_1}, \ldots, x_{i_k}]$
- I è irriducibile $\Leftrightarrow I = (x_{i_1}^{\alpha_1}, \ldots, x_{i_k}^{\alpha_k})$
- $I \cdot J = I \cap J \Leftrightarrow \forall i, j \quad \text{MCD}\,(m_i, n_j) = 1$
- $I : J = \cap_i (I : n_i)$ 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 $x_1 > x_2 > \ldots > x_n$. Dico che $\alpha \geq \beta \Leftrightarrow$ In $\alpha - \beta$ la prima coordinata $\neq 0$ è positiva
- DEGLEX Sia $\mid \alpha \mid := \sum_i \alpha_i$. Allora $\alpha \geq \beta \Leftrightarrow$ si ha $\mid \alpha \mid \geq \mid \beta \mid$ oppure $\mid \alpha \mid = \mid \beta \mid$ e vale $\alpha \geq \beta$ con LEX
- DEGREVLEX $\alpha \geq \beta \Leftrightarrow \mid \alpha \mid > \mid \beta \mid$ oppure si ha $\mid \alpha \mid = \mid \beta \mid$ e in $\alpha - \beta$ l'ultima coordinata $\neq 0$ è negativa

- (**Algoritmo di Divisione**) Siano $f_1, \ldots, f_k, f \in K[x_1, \ldots, x_n]$ allora $\exists a_1, \ldots, x_k, r \in K[x_1, \ldots, x_n]$ 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 $x^\alpha \in (\text{lt}\,(f_1), \ldots, \text{lt}\,(f_k))$
  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 $g_1, \ldots, g_k$ 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 $\{g_1, \ldots, g_k\}$
  - $\forall f \in I = (g_1, \ldots, g_k)$ 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 $G = \{g_1, \ldots, g_k\}$ si dice ridotta se è minimale per inclusione e inoltre
  - $\text{lc}\,(g_i) = 1 \quad \forall i$
  - $(\deg\,(g_1), \ldots, \deg\,(g_k))$ sono un'escalièr 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 $f, g \in K[x_1, \ldots, x_n]$ 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 $\gamma = (\gamma_1, \ldots, \gamma_n)$ con $\gamma_i = \max(\alpha_i, \beta_i)$
$$S(f, g) = \frac{x^\gamma}{c_\alpha x^\alpha} f - \frac{x^\gamma}{d_\beta x^\beta} g$$
- (**Eliminazione di LEX**) $I \subseteq K[x_1, \ldots, x_n]$ allora $I_k = I \cap K[x_{k+1}, \ldots, x_n]$ è il k-esimo ideale di eliminazione. Vale il teorema: Se G è una BdG rispetto a LEX con $x_1 \geq \ldots \geq x_n$ allora $\forall k = 1, \ldots, n-1$ si ha che $G_k = G \cap K[x_{k+1}, \ldots, x_n]$ è BdG di I_k
- (**Cose calcolabili**) Dati $I, J \subseteq K[x_1, \ldots, x_n]$ e note le loro due BdG si ha

- (**Intersezione**) $I \cap J = (tI, (1-t)J) \cap K[x_1, \ldots, x_n]$ dove quindi bisognerà usare l'ordinamento LEX con t come variabile più pesante per poter usare eliminazione
- (**Colon**) Se BdG $(J) = \{h_1, \ldots, h_r\}$ allora $I : J = \cap_{i=1}^{r}(I : h_i)$.
  Se ora ho $f \in K[x_1, \ldots, x_n]$ e voglio calcolare $I : (f) = \{g \mid gf \in I\}$ allora ho che $I : (f) = \frac{1}{f} \cdot (I \cap (f))$, ovvero se BdG $(I \cap (f)) = \{g_1 f, \ldots, g_k f\}$ allora ho BdG $(I : (f)) = \{g_1, \ldots, g_k\}$
- (**Ker di morfismi**) Sia $\Phi : K[x_1, \ldots, x_n] \to K[y_1, \ldots, y_n]$ tale che $f_i(Y) := \Phi(x_i)$. Allora si ha Ker $\Phi = (x_1 - f_1(Y), \ldots, x_n - f_n(Y)) \cap K[x_1, \ldots, x_n]$ 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 $f_1 = 0, \ldots, f_n = 0$ in K^n. Valgono:
  - (**Esistenza di soluzioni**) Se K è algebricamente chiuso, il sistema non ha soluzioni se e solo se $1 \in I = (f_1, \ldots, f_n)$, che si vede subito se c'è o meno con una BdG
  - (**Teorema di Estensione**) $I = (f_1, \ldots, f_k)$ e supponiamo K algebricamente chiuso. $I_1 = I \cap K[x_2, \ldots, x_n]$ e $\beta \in \mathcal{V}(I_1)$. $f_i = c_i(x_2, \ldots, x_n) \cdot x_1^{n_1} + \ldots \in K[x_2, \ldots, x_n][x_1]$. Se $\beta \notin \mathcal{V}(c_1, \ldots, c_k)$ 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 $\{x_1^{N_1} + \ldots, x_2^{N_2} + \ldots, \ldots, x_k^{N_k} + \ldots\}$ (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:
    - $\mid \mathcal{V}(I) \mid < \infty$
    - $\forall i = 1, \ldots, n \quad \exists m_i$ t.c. $x_i^{m_i} \in \text{lt}\,(I)$
    - $G = \{g_1, \ldots, g_r\}$ BdG di I allora $\forall i = 1, \ldots, n \quad \exists h_i \in \mathbb{N} \quad \exists g_r \in G$ t.c. lt $(g_r) \mid x_i^{h_i}$
    - dim $_K \frac{A}{I} < \infty$

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

IDEALI E VARIETÀ

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

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

Valgono inoltre i seguenti fatti:

- V è irriducibile $\Leftrightarrow \mathcal{I}(V)$ è primo
- Ogni varietà affine si decompone come unione di un numero finito di varietà irriducibili
- I, J, H ideali. Allora $\mathcal{V}(I, JH) = \mathcal{V}(I, J) \cup \mathcal{V}(I, H)$
- $V = \{\alpha\}$ con $\alpha = (\alpha_1, \ldots, \alpha_n)$ allora $\mathcal{I}(V) = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ 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 $I \subseteq K[x_1, \ldots, x_n]$ 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 $K[x_1, \ldots, x_n]$ t.c. $f \notin I_1 = K[x_2, \ldots, x_n]$ (ovvero x_1 compare) allora $\exists \phi$ cambio lineare di coordinate tale che $\phi(f) = c \cdot x_1^N + \overline{f}$ con $\deg_{x_1} \overline{f} < N$ 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)