Metodi per la risoluzione di sistemi di equazioni polinomiali

Dato un sistema di equazioni polinomiali cercheremo di rispondere alle seguenti domande, nel modo più efficace possibile.

- Il sistema è risolubile?
- Quante soluzioni esistono
- Trovare o rappresentare le soluzioni in modo "pratico"

Preliminari e richiami
Ricordiamo alcuni risultati. Per le dimostrazioni si rimanda a [COX1].
Consideriamo un campo K di caratteristica 0, indichiamo con $\overline{K}$ la sua chiusura algebrica e con $K[X] = K[x_1, .., x_n]$ l'anello dei polinomi in n variabili.
Dato un sistema $\Sigma = \{f_i = 0\}$ di equazioni polinomiali, $f_i \in K[X]$, sia $I = (f_1, \ldots, f_k)$ l'ideale generato e con

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

Si ha allora che

$$\alpha \quad \text{soluzione di } \Sigma \Longleftrightarrow \alpha \in V(I)$$

Essendoci ricondotti all'ideale I possiamo usare:

1. Teorema della base di Hilbert (garantisce la finitezza di un insieme di generatori di I)
2. Il teorema degli zeri di Hilbert.

- $V(I) = \emptyset \Longleftrightarrow I = (1)$
- $I(V(I)) = \{f \in K[X] \mid f(\alpha) = 0, \forall \alpha \in V(I)\} = \sqrt{I}$

Possiamo allora rispondere al primo quesito: il sistema ha soluzione (in $\overline{K}^n$) se e solo se $I \neq (1)$.

Un modo effettivo per verificare questo è dato dalle Basi di Gróbner.

Definizione. Fissato un ordinamento monomiale $>$ un insieme di generatori $\{g_1, .., g_s\}$ per un ideale I è una base di Gróbner (BG) se $(Lt(I)) = (ltg_1, ..ltg_s)$.
Una base di Gröbner si può calcolare con l'algoritmo di Buchberger.
Dato che sono ben definiti la divisione e il resto rispetto ad una BG abbiamo

Proposizione (Ideal Membership) Se G è BG per un ideale I

$$f \in I \Longleftrightarrow f \longrightarrow_G 0$$

(dove $\longrightarrow_G$ indica il resto della divisione per l'insieme G).

Nota. Per verificare che $I = (1)$ il calcolo della base è sufficiente.

La conoscenza di una BG permette di rispondere anche al secondo quesito. Vale

Teorema 1. $\#V(I) < \infty \Longleftrightarrow \forall i \;\; {x_i}^{m_i} \in (Lt(I)) \Longleftrightarrow \exists g_i \in G \;\; lt(g_i) = {x_i}^{s_i}$

Vogliamo ora capire quante sono le soluzioni. Per questo studiamo $A = K[X]/I$. Dal teorema 1 otteniamo

Corollario $V(I)$ è finito se e solo se $\dim_K(A) = \dim_{\bar{K}}(A) < \infty$.

Definizione Dato un anello B chiamiamo *dimensione* di B il sup delle lunghezze delle catene di primi $p_0 \subsetneq .. \subsetneq p_d \subsetneq B$ in B. Definiamo dimensione di un ideale J la dimensione di B/J.
Quindi un ideale ha dimensione 0 se e solo se ogni primo che lo contiene è massimale, ossia $\sqrt{I} = \bigcap \mathfrak{m}_i$.
Inoltre dal corollario precedente segue anche che $V(I)$ è finito se e solo se $\dim(I) = 0$

Vale anche:
Proposizione Se $V(I)$ è finito si ha $\dim_K A \geq \#V(I)$. Inoltre $\dim_K A = \#V(I)$ se e solo se $I = \sqrt{I}$.
Dim. Consideriamo $\phi : A \longrightarrow K[X]/\sqrt{I} \cong (K[X]/I)/(\sqrt{I})/I)$, ϕ è un omomorfismo surgettivo, che è omomorfismo di K-algebre e quindi di spazi vettoriali. Inoltre è un isomorfismo se e solo se $\sqrt{I}/I = 0$.
Per concludere vediamo che $\dim K[X]/\sqrt{I} = \#V(I)$. Da $\sqrt{I} = \bigcap \mathfrak{m}_i$ otteniamo che $K[X]/\sqrt{I} \cong \bigcap K[X]\mathfrak{m}_i \cong K^d$.

Se calcoliamo quindi il radicale di I conosciamo $\#V(I)$.
Come si può calcolare $\sqrt{I}$? Ci sono vari modi, uno può essere il seguente, (per ideali di dimensione 0).
Proposizione Sia $I \subset A$ un ideale. Se $\dim(I) = 0$ e $(h_i(x_i)) = I \cap K[x_i]$, indichiamo con $\overline{h}_i = \dfrac{h_i}{(h_i, h_i')}$ le parti libere da quadrati dei polinomi h_i, allora

$$\sqrt{I} = (I, \overline{h}_1, ..\overline{h}_n)$$

Dim. Proviamo un lemma.
Lemma Ogni ideale J che contiene un ideale radicale Q di dimensione 0 è radicale o $J = (1)$.
Dim. Sia $Q = \sqrt{Q} = \cap \mathfrak{m}_i \subset J = (g_1, ...g_r)$. La tesi segue immediatamente da $Q \subset (Q, g_1) \subset (Q, g_1, g_2) \subset ... \subset$ e osservando che $(Q, g_1) = \cap(\mathfrak{m}_i, g_1)$ e che $(\mathfrak{m}_i, g_1) = \mathfrak{m}_i$ o (1) a seconda che $g_1 \in \mathfrak{m}_i$ o no.

Dimostriamo ora la proposizione. Per il lemma, se proviamo che $Q = (\overline{h}_1, ..\overline{h}_n)$ è radicale abbiamo finito. Se $n = 1$ $(\overline{h}_1)$ è radicale (infatti in $K[x_1]/(\overline{h}_1)$ non ci sono nilpotenti diversi da zero). Inoltre, $K[x_1]/(\overline{h}_1) \cong \prod F_i$ è un prodotto di campi.
Consideriamo $K[x_1, x_2]/(\overline{h}_1, \overline{h}_2) \cong (K[x_1]/(\overline{h}_1))[x_2]/(\overline{h}_2)$. Poiché char $K = 0$, $\overline{h}_2$ è ancora libero da quadrati su $K[x_1]/(\overline{h}_1)$ quindi possiamo ripetere il ragionamento precedente, su ognuno degli F_i.

Basi di Gröbner di Ideali zero dimensionali primi e radicali. Shape lemma.

La BG-lex ridotta di un ideale zero dimensionale ha una forma particolare:

Proposizione Sia G la base lessicografica ridotta $(x_1 > x_2.. > x_n)$ di un ideale 0-dimensionale I allora G ha la seguente forma:

$$G = (g_{11}(x_1, .., x_n), ...g_{1s_1}(x_1, ..x_n), g_{21}(x_2, .., x_n), .., g_{2s_2}(x_2, ..x_n), ..., g_{n1}(x_n))$$

dove:

i) $g_{ij}(x_i, .., x_n) \in I \cap K[x_i, .., x_n]$

ii) $lt(g_{i1}(x_i, .., x_n)) = x_i^{m_i}$

iii) Se $I = \sqrt{I}$, $g_{n1}(x_n)$ è libero da quadrati.

quindi il sistema può essere risolto con un procedimento di sostituzione "all'indietrò.
Problemi: difficoltà del calcolo della BG lessicografica e calcoli in estensioni algebriche.
Se $I = \sqrt{I}$ la forma precedente si può semplificare notevolmente.
Facciamo un esempio. Consideriamo il caso in cui il grado del polinomio $p_n(x_n) = I \cap K[x_n]$ sia uguale al numero di punti in $V(I) = \dim A = d$. Allora $1, x_n, ..., x_n^{d-1}$ sono linearmente indipendenti e quindi sono una base di A e in I per ogni i si ha $x_i = p_i(x_n)$ con $\deg(p_i(x_n)) < d$. Quindi si ottiene che la base lessicografica ridotta è della forma $G = (x_1 - p_1(x_n), \ldots, x_{n-1} - p_{n-1}(x_n), p_n(x_n))$. In questo modo si semplifica il calcolo delle soluzioni.
Ci possiamo sempre ridurre a questo caso. Vale
Teorema-Shape Lemma Se I è zero dimensionale radicale per quasi tutte le trasformazioni lineari di coordinate la base lessicografica ridotta è della forma $G = (x_1 - p_1(x_n), .., x_{n-1} - p_{n-1}(x_n), p_n(x_n))$.
Dim. Per l'osservazione precedente basta che vediamo che per quasi tutte le trasformazioni lineari le ultime coordinate dei punti di $V(I)$ sono distinte. Cerchiamo una trasformazione lineare $L : K^n \longrightarrow K$ tale che $L(P_i)$ siano tutti distinti, ossia coefficienti $\mathbf{c} = (c_1, .., c_n) \in K^n$ tali $L(P_i) = \mathbf{c} \cdot P_i \neq L(P_j) = \mathbf{c} \cdot P_j$. Affinché le coppie siano a due a due distinte è quindi sufficiente escludere i valori $\mathbf{c}$ tali che $\mathbf{c} \cdot (P_i - P_j) = 0$. Si tratta di una condizione lineare le cui

soluzioni sono K^{n-1}, dato che ci sono $\binom{m}{2}$ coppie otteniamo una unione finita di spazi vettoriali di dimensione K^{n-1} che quindi non possono ricoprire K^n. Allora a meno di operare con la trasformazione $y_1 = x_1, .., y_{n-1} = x_{n-1}, y_n = L(x_1, .., x_n)$ otteniamo la forma desiderata.
Esempio $I = (x^2 - y, y^2 - 1)$ operando con la trasformazione $x_1 = x, y_1 = x + y$ otteniamo che la base lex è $(x_1 + \frac{2}{5}y_1^3 - \frac{1}{5}y_1^2 - \frac{1}{5}y_1 - 1, y_1^4 - 2y_1^2 - 4y_1)$

La seguente proposizione "costruisce" una trasformazione lineare di coordinate che separa gli elementi di un insieme finito di punti.
Proposizione Siano $\alpha_1, .., \alpha_m$ punti in $\overline{K}^n$. Definiamo $u_i(X) = x_1 + ix_2 + .. + i^{n-1}x_n$, allora nell'insieme $\{u_i \mid 0 \leq i \leq \binom{m}{2}(n-1)\}$ esiste un elemento tale che $u_i(\alpha_k) \neq u_(\alpha_l)$ per ogni $k \neq l$.
Dim. Per ogni $k \neq l$ definiamo $r(l,k) = \#\{i \mid u_i(\alpha_k) = u_i(\alpha_l)\}$. Gli elementi di $r(k,l)$ sono le radici del polinomio $(\alpha_{k,1} - \alpha_{l,1}) + .. + (\alpha_{k,n} - \alpha_{l,n})t^{n-1}$ che ha grado $n-1$. Dato che ci sono $\binom{m}{2}$ coppie da considerare la tesi segue.
Corollario. Dati $\{a_1, .., \alpha_m\}$ punti in $\overline{K}^n$ èpossibile costruire una famiglia di polinomi $\{g_i(X)\}$ tali che $g_i(\alpha_i) = 1$ e $g_i(\alpha_j) = 0$.
Dalla proposizione precedente segue che esiste un polinomio lineare $u(X)$ tale che tale che $u(\alpha_i) \neq u(\alpha_j)$ se $i \neq j$. Se definiamo $g_i(X) = \prod_{i \neq j} \frac{u(X) - u(\alpha_j)}{u(\alpha_i) - u(\alpha_j)}$, questi elementi soddisfano le proprietà richieste.

Matrici di moltiplicazione e loro autovalori e autovettori

Per questa parte rimandiamo a (COX2). Sia $I \subset K[X]$, $K = \overline{K}$, un ideale zero dimensionale e indichiamo con $A = K[X]/I$. Sia $f \in A$ e sia L_f l'endomorfismo di A definito dalla moltiplicazione per f, $L_f(g) = fg$.
Osserviamo che se $f, g \in A$ allora $L_f = L_g$ se e solo se $f = g$, inoltre vale $L_{f+g} = L_f + L_g$ e $L_{fg} = L_f \circ L_g$ quindi otteniamo un omomorfismo iniettivo di anelli, $\mathfrak{L} : A \longrightarrow End(A)$. Da questo segue anche che, fissata una base di A, ad ogni $f \in A$ si può associare una matrice m_f e che per ogni polinomio $h(t) \in K[t]$ vale $m_{h(f)} = h(m_f)$.

Fissiamo un elemento $f \in A$, dato che A ha dimensione finita esiste un polinomio $h \in K[t]$ tale che $h(f) = 0$, e quindi la stessa relazione vale per L_f, da cui segue che $h(t)$ deve essere divisibile per h_f, il polinomio minimo di L_f, che ha le stesse radici del polinomio caratteristico.

Teorema Sia I ideale di dimensione 0, $f \in A$, h_f il polinomio minimo di L_f e $\lambda \in K$; sono fatti equivalenti:

i) $h_f(\lambda) = 0$, ossia λ è un autovalore di L_f

ii) esiste $\alpha \in V(I)$ tale che $f(\alpha) = \lambda$

Dim. Sia λ un autovalore di L_f e sia $0 \neq g \in A$ un autovettore associato a λ, ossia $L_{(f-\lambda)}(g) = 0$. Supponiamo per assurdo che $\forall \alpha \in V(I)$, $f(\alpha) \neq \lambda$, allora $L_{(f-\lambda)}(g)(\alpha) = (f - \lambda)g(\alpha) \neq 0 \ \forall \alpha \in V(I)$. Se proviamo che $f - \lambda$

è invertibile in A, dato $g \neq 0$, abbiamo un assurdo. Esiste una famiglia di polinomi g_i separatori cosi' se definiamo $p(X) = \sum_i \frac{g_i(X)}{(f-\lambda)(X)}$ otteniamo che $1 - p(\alpha)(f(\alpha) - \lambda) = 0$ su $V(I)$ da cui $(1 - p(X)(f - \lambda))^r = 0$ in A, e quindi la svluppando la potenza esiste $q(X) \in A$ tale che $1 = (f - \lambda)q$.
Viceversa dato che $h_f(f) = 0$ in A, per definizione di $V(I)$ $h_f(f)$ si annulla su tutti i punti di $V(I)$ e quindi $\lambda = f(\alpha)$ è un autovalore di L_f.

Corollario Se consideriamo $f_i = x_i$ gli autovalori di L_{x_i} sono esattamente i valori delle i-esime coordinate dei punti di $V(I)$ e $(h_{x_i}(x_i)) = I \cap K[x_i]$.

Possiamo anche mettere in relazione gli autovettori sinistri delle matrici m_f con i punti di $V(I)$. Ricordiamo che un elmento $0 \neq v \in K^n$ si dice autovettore sinistro per una matrice M se esiste $\lambda \in K$ tale che $vM = \lambda v$.

Proposizione Sia I ideale radicale 0-dimensionale e sia $f \in K[X]$, tale che $f(\alpha) \neq f(\beta)$ per $\alpha, \beta \in V(I)$, $\alpha \neq \beta$. Indichiamo con $\mathfrak{B} = \{X^{d_1}, ..., X^{d_s}\}$ una base monomiale di $A = K[X]/I$, $(\dim_K(A) = s)$, allora gli autospazi sinistri di m_f, la matrice di moltiplicazione per f rispetto alla base $\mathfrak{B}$, hanno dimensione 1 e sono generati dagli elementi $(\alpha^{d_1}, .., \alpha^{d_s}), \alpha \in V(I)$.
Dim. Consideriamo $m_f = (m_{ij})$ la matrice associata a L_f rispetto alla base $\mathfrak{B}$. La j-ma colonna di m_f è data da $[L_f(X^{d_j})]_{\mathfrak{B}}$ e quindi $L_f(X^{d_j}) = X^{d_j} f = \sum_i m_{ij} X^{d_i}$. Valutando questa espressione in α otteniamo $\alpha^{d_j} f(\alpha) = \sum_i m_{ij} \alpha^{d_i}$ e quindi $(\alpha^{d_1}, .., \alpha^{d_m}) f(\alpha) = (\alpha^{d_1}, .., \alpha^{d_m}) m_f$. Per concludere osserviamo che essendo l'ideale 0-dimensionale, $1 \in \mathfrak{B}$ e quindi $(\alpha^{d_1}, .., \alpha^{d_s}) \neq 0$, inoltre dato che $f(\alpha) \neq f(\beta)$ per $\alpha \neq \beta \in V(I)$, gli autovalori sinistri di m_f sono tutti distinti e quindi gli autospazi corrispondenti hanno dimensione 1.

Con questa osservazione possiamo calcolare gli elementi di $V(I)$.

i) ci riduciamo a I radicale.

ii) Calcoliamo una base monomiale $\mathfrak{B}$ di A. Dal fatto che I ha dimensione zero, $1 \in \mathfrak{B}$. Inoltre esistono $k \leq n$ variabili x_{i_j} tali che $x_{i_j} \in \mathfrak{B}$, quindi possiamo assumere (eventualmente riordinando le variabili) $\mathfrak{B} = \{1, x_1, \ldots, x_k, b_{k+1}, .., b_s\}$.

iii) Consideriamo un polinomio lineare f che assuma valori distinti su $V(I)$, (ad esempio consideriamo $f = \sum_{1=1}^{n} c_i x_i$ con $c_i \in K$ scelti random).

iv) Costruiamo la matrice m_f di moltiplicazione per f rispetto a $\mathfrak{B}$

v) Troviamo autovalori e autovettori sinistri di m_f

vi) Per ogni autovalore $\lambda = f(\gamma)$, $\gamma = (\gamma_1, .., \gamma_n) \in V(I)$ se $v_\gamma = (v_0, .., v_{s-1})$ l'autovettore associato, esiste $c_\gamma \in K$ tale che $v_\gamma = \mathbf{c}_\gamma(\gamma^{d_1}, \ldots, \gamma^{d_s})$.

Per ricavare il valore delle coordinate γ_i del punto γ, dalla scelta di $\mathfrak{B}$ ricaviamo che, $v_0 = \mathbf{c}_\gamma$ e $\gamma_i = \dfrac{v_i}{v_0}$, per $i \leq k$. Infine se $k < i \leq n$ allora

esistono in I relazioni moniche della forma $x_i = p_i(x_1, \ldots, x_k)$ e quindi i valori delle coordinate corrispondenti possono essere ricavate sostituendo i valori trovati precedentemente.

In questo modo abbiamo trovato gli zeri, ma abbiamo perso le informazioni sulla molteplicità. Vediamo come ricavare questa informazione: dobbiamo studiare meglio la struttura di A.
Ricordiamo che se $I = \cap_i^m \mathfrak{q}_i$ zero dimensionale, usando il CRA (dato che $(\mathfrak{q}_i, \mathfrak{q}_j) = (1)$) si decompone $A = K[X]/I \cong \prod K[X]/\mathfrak{q}_i = \prod R_i$. Gli anelli R_i sono anelli locali con ideale massimale $\mathfrak{m}_i$, e quindi ogni elemento non invertibile è nilpotente. Inoltre ogni $f \notin \mathfrak{m}_i$ è invertibile in R_i.
Se $\alpha \in K^n$ è il punto tale che $\mathfrak{m}_i = \sqrt{q}_i = \{f \in A \quad | f(\alpha) = 0\}$, allora $R_i = S_\alpha^{-1} A = A_\alpha$ con $S_\alpha = A \setminus \mathfrak{m}_i = \{f \in A |\ f(\alpha) \neq 0\}$ e $A \cong \prod A_\alpha$; definiamo $\mu_\alpha = \dim_K(A_\alpha)$ la molteplicità di α.
Per caratterizzare ulteriormente i fattori A_α costruiamo una famiglia di polinomi $\{e_\alpha\}$ detti *idempotenti* di A.

Proposizione Sia I 0-dimensionale e sia $m = \#V(I)$ allora $\forall \alpha \in V(I)$ esiste un elemento $e_\alpha \in A$, detto idempotente associato ad α e valgono le seguenti:

1. ${e_\alpha}^2 = e_\alpha$
2. $\sum_\alpha e_\alpha = 1$
3. $e_\alpha e_\beta = 0$ se $\alpha \neq \beta$
4. $e_\alpha(\alpha) = 1$.

Dim. Abbiamo dimostrato che, dati m punti, è sempre possibile costruire un elemento *separatore* ossia un polinomio u tale che $u(\alpha) \neq u(\beta)$ se $\alpha \neq \beta$. Definiamo allora $s_\alpha(X) = \prod_{\alpha \neq \beta} \frac{u(X)-u(\beta)}{u(\alpha)-u(\beta)} \in K[X]$. Osserviamo che, se $\alpha \neq \beta$ $s_\alpha s_\beta(\gamma) = 0$, $\forall \gamma \in V(I)$ quindi fissato α per ogni β esiste r_β tale che $(s_\alpha s_\beta)^{r_\beta} = 0$ in A. Indichiamo con $r = max_{\alpha \neq \beta}\{r_\beta\}$ e con $t_\alpha = s_\alpha^r$. Dalla definizione segue che $t_\alpha t_\beta = 0$ in A, $t_\alpha(\alpha) = 1$ e $t_\alpha(\beta) = 0$ se $\alpha \neq \beta$. Valgono le ultime due condizioni, per soddisfare anche le prime, consideriamo l'ideale $J = (I, (t_\alpha)$, per costruzione si ha che $V(J) = \emptyset$ quindi per HN $J = 1$ e si ha $1 = \sum h_i f_i + \sum c_\alpha t_\alpha 2$. Se definiamo $e_\alpha = c_\alpha t_\alpha$ otteniamo gli elementi desiderati.

Proposizione $A_\alpha \cong e_\alpha A$.
Dim. Lo dimostriamo sfruttando le proprietà universali della localizzazione. Definiamo $\phi : A \longrightarrow e_\alpha A$ ponendo $\phi(f) = e_\alpha f$. Proviamo che se $s \in S_\alpha$ allora $\phi(s)$ è invertibile. Osserviamo che l'elemento $(e_\alpha(s(x) - s(\alpha)) = e_\alpha v(x) \in A$ è nilpotente, infatti si annulla su tutti gli elementi di $V(I)$ e quindi l'elemento $e_\alpha(s(\alpha) + v(x))$ è invertibile in $e_\alpha A$. Dato che $s(\alpha) + v(x) = s(x)$ otteniamo che $e_\alpha s(x) = \varphi(s)$ è invertibile in $e_\alpha A$.

Per vedere che se $e_\alpha g = 0$ allora esiste $s \in S_\alpha$ tale che $sg = 0$ in A, basta considerare la relazione $e_\alpha e_\alpha g = e_\alpha g = 0$.
Infine dobbiamo vedere che ogni elemento di $e_\alpha A$ si scrive come $\phi(a)\phi(s)^{-1}$, con $s \in S_\alpha$. Dato che $\phi(a) = e_\alpha a = \phi(a)\phi(1)^{-1}$, la tesi è provata.

Usiamo ora la decomposizione ottenuta per studiare gli endomorfismi di A.

Teorema(Stickelberger) Sia $f \in A$, L_f l'endomorfismo associato. Allora per ogni $\alpha \in V(I)$, $L_f(A_\alpha) \subset A_\alpha$, ossia A_α è un autospazio per L_f.
Inoltre la restrizione ad A_α di L_f ha un unico autovalore $f(\alpha)$ con molteplicità $\mu_\alpha = \dim_K(A_\alpha)$.
Dim. Dato che $A_\alpha \cong e_\alpha A$, $L_f(A_\alpha) = L_f(e_\alpha A) = e_\alpha L_f(A) \subset e_\alpha A$. Inoltre dato che $e_\alpha(f - f(\alpha))$ si annulla su tutti i punti di $V(I)$ la restrizione di $L_{(f-f(\alpha))}$ ad A_α è nilpotente e quindi la tesi.

Possiamo riassumere i risultati provati:

Teorema Sia $f \in A = K[X]/I$ e sia $L_f \in End(A)$ l'omomorfismo di moltiplicazione per f. Vale:

1. $Tr(L_f) = \sum_\alpha \mu_\alpha f(a)$
2. $det(L_f) = \prod_\alpha f(\alpha)^{\mu_\alpha}$
3. il polinomio caratteristico $\chi_f(t) = \prod_\alpha (t - f(\alpha))^{\mu_\alpha}$

Per concludere riportiamo alcuni risultati senza dimostrazione.
Vogliamo usare le informazioni fornite dal polinomio caratteristico dell'endomorfismo di moltiplicazione per costruire una parametrizzazione razionale delle coordinate degli elementi di $V(I)$.
Sia $u \in A$, $\chi_u(t)$ il suo polinomio caratteristico, per ogni $f \in A$ definiamo il polinomio

$$g_u(f,t) = \sum_\alpha \mu(\alpha) f(\alpha) \prod_{\beta \neq \alpha} (t - u(\beta))$$

Proposizione I polinomi g_u soddisfano le seguenti proprietà:

1. $g_u(f,t) \in K[t]$
2. Se u è un elemento separatore, e $\beta \in V(I)$, $f(\beta) = \frac{g_u(f,u(\beta))}{g_u(1,u(\beta))}$

Corollario (RUR) Sia $u \in A$ un elemento separatore e $\chi_u(t)$ il suo polinomio caratteristico, sia $\alpha \in V(I)$:

1. Se $\alpha \in V(I)$ allora $u(\alpha)$ è una radice di $\chi_u(t)$.

2. la molteplicità $\mu(\alpha)$ di α come radice è uguale alla molteplicità di $u(\alpha)$ come radice di $\chi_u(t)$.

3. Il numero di fattori irriducibili di $\chi_u(t)$ è uguale a $\#V(I)$.

4. Se $\bar{t}$ è una radice di $\chi_u(t)$ allora:

$$\left(\frac{g_u(x_1,\bar{t})}{g_u(1,\bar{t})}, \frac{g_u(x_2,\bar{t})}{g_u(1\bar{t})}, ..., \frac{g_u(x_n,\bar{t})}{g_u(1,\bar{t})}\right)$$

   è una radice del sistema con la stessa molteplicità.

Defininizione Se $f \in A$ definiamo l'applicazione bilineare $T_f : A \times A \longrightarrow K$ data da $T_f(h,g) = tr(L_{fgh})$. La forma quadratica associata a T_f, data da $Q_f(g) = tr(L_{fg^2})$ si dice forma quadratica di Hermite associata ad f.

Valgono i seguenti risultati:

Teorema

$$f \in \sqrt{I} \Longleftrightarrow T_1(f,g) = 0 \ \ \forall g \in A$$

Teorema Sia $f \in A$ e Q_f la forma quadratica di Hermite associata:

$$\text{rank}(Q_f) = \#\{\alpha \in V(I) \ \mid \ f(\alpha) \neq 0\}$$

in particolare per $f = 1$ otteniamo che $\text{rank}(Q_1) = \#V(I)$.

Infine vediamo le informazioni che possiamo ottenere riguardo alle radici reali del sistema, (se $k \subset \mathbb{R}$).
Le matrici associate alle forme bilinerari sono matrici simmetriche a coefficienti in $\mathbb{R}$ e quindi hanno tutti autovalori reali. Vale:

Teorema Sia $I \subset k[X]$ ideale zero dimensionale, $k \subset \mathbb{R}$, se $f \in k[X]$, allora la segnatura della matrice associata a Q_f soddisfa la seguente:

$$\sigma(Q_f) = \#\{\alpha \in V(I) \cap \mathbb{R}^n \mid f(\alpha) > 0\} - \#\{\alpha \in V(I) \cap \mathbb{R}^n \mid f(\alpha) < 0\}$$

Riferimenti

[COX1]- Cox, Little, O'Shea, "Ideals Varieties and Algorithms"
[COX2] - Cox, Little, O'Shea, "Using Algebraic Geometry".