Publ. I.R.M.A. Strasbourg, 1993, 461/S–24
Actes 24^e Séminaire Lotharingien, p. 39–76

ALGORITMI COMBINATORI PER L'INTERPOLAZIONE POLINOMIALE IN DIMENSIONE ≥ 2

PER

LUIGI CERLIENCO e MARINA MURREDDU

1 Introduzione.

Sia K un campo, $X := \{x_1, x_2, \ldots, x_n\}$ un insieme di indeterminate e $K[X] := K[x_1, \ldots, x_n]$ l'usuale algebra dei polinomi nelle indetermiante x_j. Faremo uso delle notazioni: $\mathbf{i} := (i_1, \ldots, i_n) \in \mathbf{N}^n$ e $\mathbf{x}^{\mathbf{i}} := x_1^{i_1} \cdots x_n^{i_n}$. Consideriamo i problemi seguenti.

Problema 1. Dati N elementi distinti P_i $(i = 1, \ldots, N)$ dello spazio vettoriale K^n e fissati N valori $\alpha_i \in K$, si vuole determinare un polinomio $p(x_1, \ldots, x_n) \in K[X]$ tale che

$$p(P_i) = \alpha_i \qquad (i = 1, \ldots, N).$$

NB. Volutamente non ci si è riferiti a K^n come al K–spazio affine n–dimensionale A^n_K. Infatti alcuni aspetti rilevanti della trattazione che segue <u>non</u> hanno — nel caso $n \geq 2$ — carattere geometrico intrinseco. Rinviamo all'Appendice 1 per maggiori chiarimenti su questo aspetto. È pertanto solamente per comodità di linguaggio che chiameremo *punti* di K^n gli elementi P_i.

Problema 2. Analogo al Problema 1 ma nell'ipotesi che si conoscano oltre che i valori di p nei punti P_i anche di quelli di certe sue derivate parziali (derivate di ordine eventualmente variabile da punto a punto).

Occupiamoci dapprima del Problema 1. Nei termini enunciati esso è mal posto; occorre precisare ulteriormente la natura del polinomio cercato in modo tale che venga assicurata l'esistenza e l'unicità della soluzione. Infatti, è immediato osservare che se p è un polinomio che soddisfa alle condizioni richieste, tale è pure un qualunque altro polinomio p' congruo a p modulo l'ideale $\Im(\mathcal{P})$ di tutti i polinomi che si annullano sui punti dell'insieme $\mathcal{P} := \{P_1, \ldots, P_N\}$.

Tale ideale $\Im(\mathcal{P})$ è cofinito:

$$codim\Im(\mathcal{P}) := dim K[X]/\Im(\mathcal{P}) = N.$$

Se $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_N}$ sono monomi tali che le classi di equivalenza $[\mathbf{x}^{\mathbf{i}_1}], \ldots, [\mathbf{x}^{\mathbf{i}_N}]$ (modulo $\Im(\mathcal{P})$) formano una base per l'algebra quoziente $K[X]/\Im(\mathcal{P})$ — basi di questo tipo verranno dette *basi monomiali* — la classe di equivalenza $[p]$ di un qualunque polinomio $p \in K[X]$ contiene uno ed un solo polinomio $\overline{p}$ della forma

$$\overline{p} = a_1\mathbf{x}^{\mathbf{i}_1} + \cdots + a_N\mathbf{x}^{\mathbf{i}_N} \qquad (a_i \in K) \tag{1}$$

(che chiameremo "resto di p (mod. $\Im(\mathcal{P})$) rispetto alla base $\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_N}$ fissata"). Si può quindi affermare che esiste uno ed un solo polinomio della forma (1) soddisfacente alle condizioni poste.

Appare opportuno imporre un'altra ragionevole restrizione, atta a limitare la varietà delle possibili basi monomiali e quindi delle soluzioni al problema. È infatti naturale — ed è ciò che si fa *tacitamente* nel caso unidimensionale — privilegiare basi monomiali che siano "minimali" nel senso seguente. Indichiamo con M l'insieme dei *termini* (:= monomi monici) di $K[X]$ e con $\preceq$ un arbitrario *term-ordering* su M (ordine lineare compatibile con la sua struttura di monoide); ancora: "$\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{j}}$" sta per "$\mathbf{x}^{\mathbf{i}} \preceq \mathbf{x}^{\mathbf{j}}$ e $\mathbf{x}^{\mathbf{i}} \neq \mathbf{x}^{\mathbf{j}}$". La base monomiale $[\mathbf{x}^{\mathbf{i}_1}], \ldots, [\mathbf{x}^{\mathbf{i}_N}]$ di $K[X]/\Im(\mathcal{P})$ ($\mathbf{x}^{\mathbf{i}_1} \prec \ldots \prec \mathbf{x}^{\mathbf{i}_N}$) verrà detta *minimale* rispetto a $\preceq$ se, per qualunque altra base monomiale $[\mathbf{x}^{\mathbf{i}'_1}], \ldots, [\mathbf{x}^{\mathbf{i}'_N}]$ di $K[X]/\Im(\mathcal{P})$ (con $\mathbf{x}^{\mathbf{i}'_1} \prec \ldots \prec \mathbf{x}^{\mathbf{i}'_N}$) si ha $\mathbf{x}^{\mathbf{i}_j} \preceq \mathbf{x}^{\mathbf{i}'_j}$ per ogni $j = 1, \ldots, N$. Nel seguito chiameremo *base monomiale minimale* ogni base monomiale che sia minimale rispetto ad un qualche ordine lineare compatibile $\preceq$.

Come vedremo nei prossimi paragrafi, qualora si disponga di una base monomiale per $K[X]/\Im(\mathcal{P})$, il Problema 1 è di soluzione pressoché immediata. Esso viene così ricondotto a determinare algoritmi effettivi per trovare una base monomiale minimale per $K[X]/\Im(\mathcal{P})$.

Per tale questione verranno proposte soluzioni di tipo diverso: sia riconducendola alla ricerca di un minore non nullo di ordine N di una matrice a N righe; sia, dopo aver determinato un sistema di generatori per $\Im(\mathcal{P})$, facendo uso della teoria delle basi di Groebner; sia infine — e questo riteniamo essere il principale risultato del presente lavoro — attraverso un semplice algoritmo puramente combinatorio che fornisce direttamente la base monomiale, minimale rispetto all'ordine lessicografico inverso $\preceq_{i.l.}$, di $K[X]/\Im(\mathcal{P})$

Il Problema 2 richiederà ulteriori precisazioni, dopo di che la sua soluzione non si discosterà molto da quella del Problema 1. Ad esso sarà dedicato l'ultimo paragrafo della presente nota.

2 L'ideale $\Im(\mathcal{P})$ dell'insieme $\mathcal{P} := \{P_1, \ldots, P_N\}$.

2.1 Dato un ideale $I \subseteq K[X]$, sia $G = \{g_1, \cdots, g_s\}$ la *base di Groebner ridotta* (cfr. [1]) di I relativa all'ordine $\preceq$, in simboli:

$$G = \{g_1, \cdots, g_s\} := RGB_{\preceq}(I).$$

Detto t_i il *termine direttore* di g_i (cioè il termine di g_i più grande nell'ordine $\preceq$), poniamo

$$T_i := t_i \cdot M \qquad \text{e} \qquad B := M - \bigcup_{i=1}^{s} T_i.$$

È facile verificare che l'insieme delle classi di equivalenza, modulo I, dei termini in B costituisce una base monomiale per $K[X]/I$ che è minimale rispetto al term-ordering $\preceq$ considerato.

Osserviamo anche che l'insieme $\mathcal{F} := \mathcal{F}_{\prec}(I) := \{\mathbf{i} \in \mathbf{N}^n \mid \mathbf{x}^{\mathbf{i}} \in B\}$ è un diagramma di Ferrers (cfr. **4.6**) i cui elementi diedrali esterni $\mathbf{f}_1, \ldots, \mathbf{f}_s$ sono tali che $\mathbf{x}^{\mathbf{f}_i} = t_i$. Viceversa, è facile provare che se $\mathcal{F} \subseteq \mathbf{N}^n$ è tale che $\{[\mathbf{x}^{\mathbf{i}}]_I \mid \mathbf{i} \in \mathcal{F}\}$ costituisce una base monomiale, minimale rispetto al term-ordering $\preceq$, per $K[X]/I$ allora

a) $\mathcal{F}$ è un diagramma di Ferrers;

b) indicati con $\mathbf{f}_1, \ldots, \mathbf{f}_s$ gli elementi diedrali esterni di $\mathcal{F}$ e, per ogni $j = 1, \ldots, s$, con $p_j \in span_K\{\mathbf{x}^{\mathbf{i}} \mid \mathbf{i} \in \mathcal{F}_j\}$ (dove $\mathcal{F}_j := \{\mathbf{i} \in \mathcal{F} \mid \mathbf{i} \prec \mathbf{f}_j\}$) il polinomio univocamente determinato tale che $\mathbf{x}^{\mathbf{f}_j} - p_j \equiv 0 \; mod.I$, allora l'insieme $\{\mathbf{x}^{\mathbf{f}_1} - p_1, \ldots, \mathbf{x}^{\mathbf{f}_s} - p_s\}$ costituisce la base di Groebner ridotta $RGB_{\preceq}(I)$. Nel seguito queste osservazioni verranno spesso sfruttate tacitamente.

2.2 Per ogni sottoinsieme $T \subseteq M$, indichiamo con $T_{\prec}$ la sequenza

$$T_{\prec} := (t_0, t_1, \ldots, t_s, \ldots) \qquad (t_i \in T)$$

formata dagli elementi di T ordinati secondo l'ordine indotto da $\preceq$: $r < s \Rightarrow t_r \prec t_s$.

Se $P \in K^n$ poniamo

$$\begin{array}{rccl} v_P : K[x_1, \ldots, x_n] & \longrightarrow & K & \qquad \text{(valutazione in } P\text{)} \\ f & \longmapsto & f(P) & \end{array}$$

e indichiamo con $T_{\prec}(P)$ la lista

$$T_{\prec}(P) := (v_P(t_0), \ldots, v_P(t_s), \ldots).$$

Inoltre, in riferimento ad un insieme finito (lin. ordinato) $\mathcal{P} = \{P_1, \ldots, P_N\} \subseteq K^n$, indichiamo con $T_{\prec}(\mathcal{P})$ la matrice con $N' := \#T \leq \infty$ colonne ed N righe, la cui j-esima riga è $T_{\prec}(P_j)$.

2.3 Adottando anche nel presente lavoro la terminologia già utilizzata in [2], chiameremo *ideale elementare* un qualunque ideale $\Gamma = (\gamma_1(x_1), \dots, \gamma_n(x_n))$ di $K[x_1, \dots, x_n]$ generato da n polinomi, ciascuno in una sola variabile. Osserviamo che l'insieme dei generatori $(\gamma_1, \dots, \gamma_n)$ di Γ costituisce anche *la* sua base di Groebner ridotta (qualunque sia l'ordine lineare compatibile $\preceq$ adottato).

Conviene associare a $\mathcal{P} = \{P_1, \dots, P_N\}$ un ideale elementare Γ nel modo seguente. Dapprima associamo a $\mathcal{P}$ l'insieme $\tilde{\mathcal{P}}$ di tutti i punti $P(a_1, \dots, a_n)$ di K^n tale che, per ogni $1 \le j \le n$, a_j sia la j-esima coordinata di almeno uno dei punti $P_1, \dots, P_N$, e poniamo poi $\Gamma := \Im(\tilde{\mathcal{P}})$.

Osserviamo che se il complesso dei punti in $\mathcal{P}$ ha h_j valori distinti per j-esime coordinate allora $\#\tilde{\mathcal{P}} = h := h_1 \cdots h_n \ge N = \#\mathcal{P}$. Conveniamo inoltre di ordinare linearmente i punti in $\tilde{\mathcal{P}}$ assumendo che i primi N siano proprio i punti di $\mathcal{P} \subseteq \tilde{\mathcal{P}}$:

$$\tilde{\mathcal{P}} = \{P_1, \dots, P_N, P_{N+1}, \dots, P_h\} \qquad (h = h_1 \cdots h_n) .$$

Va notato che l'ideale $\Gamma := \Im(\tilde{\mathcal{P}})$ di $\tilde{\mathcal{P}}$, è l'ideale elementare generato dagli n polinomi quadrat-frei $\gamma_j(x_j)$, $j = 1, \dots, n$, definiti dalle condizioni

$$deg(\gamma_j) = h_j ,$$

$$\gamma_j(\rho) = 0 \Longleftrightarrow \rho \text{ è la j-esima coordinata di almeno uno dei punti } P_1, \dots, P_N .$$

Pertanto le classi di equivalenza mod.Γ dei termini in

$$H := \{\mathbf{x}^{\mathbf{i}} = x_1^{r_1} \cdots x_n^{r_n} \mid 0 \le r_j \le h_j - 1\}$$

costituiscono una base per $K[X]/\Gamma$.

Proposizione 1 *La matrice* $\mathcal{H} := H_{\prec}(\tilde{\mathcal{P}})$ *è non degenere.*

Dimostrazione. Facciamo uso della formula (vedi Appendice 2)

$$\begin{aligned} \mid A_1 \otimes A_2 \otimes \cdots \otimes A_n \mid \; &= \\ =\mid A_1 \mid^{h_2 \cdots h_n} \mid A_2 \mid^{h_1 h_3 \cdots h_n} \cdots \mid A_n \mid^{h_1 \cdots h_{n-1}} \; &= \; \frac{(\mid A_1 \mid \cdots \mid A_n \mid)^{h_1 h_2 \cdots h_n}}{\mid A_1 \mid^{h_1} \cdots \mid A_n \mid^{h_n}} \end{aligned} \tag{2}$$

dove A_j è una matrice quadrata d'ordine h_j.

L'enunciato discende dalla (2) non appena si osservi che la matrice $H_{\prec}(\tilde{\mathcal{P}})$ è il prodotto tensoriale di n matrici di Vandermonde, la j-esima delle quali è associata alle j-esime coordinate dei punti $P_1, \dots, P_N$. Anzi, posto $P_i \equiv (\rho_{i,1}, \dots, \rho_{i,n})$ con $P_i \in \mathcal{P}$, si ha

$$det\ H_{\prec}(\tilde{\mathcal{P}}) = \prod_{j=1}^{n} \Big[\prod_{\rho_{r,j} \neq \rho_{s,j}} (\rho_{r,j} - \rho_{s,j}) \Big]^{\overline{h}_j} \neq 0 \tag{3}$$

con $\overline{h}_j := h/h_j$. □

2.4 Per la Prop.1 la matrice $\mathcal{H} := H_{\prec}(\tilde{\mathcal{P}})$ è invertibile. Consideriamo la sua inversa $\mathcal{H}^{-1} = (\alpha_s^r)$ e, posto $H_{\prec} := \{\mathbf{x}^{\mathbf{i}_1}, \ldots, \mathbf{x}^{\mathbf{i}_h}\}$, associamo alla sua s-esima colonna il polinomio $p_s = \sum_{r=1}^h \alpha_s^r \mathbf{x}^{\mathbf{i}_r}$.

Proposizione 2 *L'ideale* $I := (p_{N+1}, \ldots, p_h, \gamma_1, \ldots, \gamma_n)$ *è l'ideale dell'insieme* $\mathcal{P} = \{P_1, \ldots, P_N\}$*:*

$$I := (p_{N+1}, \ldots, p_h, \gamma_1, \ldots, \gamma_n) = \Im(\mathcal{P}).$$

Dimostrazione Il fatto che $\mathcal{H}^{-1}$ sia inversa di $\mathcal{H}$ comporta che p_s assume il valore 1 in $P_s \in \tilde{\mathcal{P}}$ ed il valore zero in tutti gli altri punti di $\tilde{\mathcal{P}}$:

$$p_s(P_t) = v_{P_t}(p_s) = \delta_s^t.$$

Pertanto $\mathcal{V}(I) = \mathcal{P}$ ($\mathcal{V}(I)$ indica l'insieme algebrico dell'ideale I). Ne consegue che $I \subseteq \Im(\mathcal{V}(I)) = \Im(\mathcal{P})$ e quindi che *codim* $I \geq N =$ *codim* $\Im(\mathcal{P})$. Per concludere che $I = \Im(\mathcal{P})$ basta allora provare che *codim* $I = N$. È cioè sufficiente provare che in H esistono N monomi $\mathbf{x}^{\mathbf{i}_{\sigma(1)}}, \ldots, \mathbf{x}^{\mathbf{i}_{\sigma(N)}}$ tali che per ciascuno $\mathbf{x}^{\mathbf{i}_{\sigma(N+t)}}$ $(t = 1, \ldots, h-N)$ degli altri si abbia

$$\mathbf{x}^{\mathbf{i}_{\sigma(N+t)}} \equiv \sum_{r=1}^{N} \eta_{t,r}\, \mathbf{x}^{\mathbf{i}_{\sigma(r)}} \quad (\text{mod. } I). \tag{4}$$

Per la Prop. 1, la matrice (di tipo $N \times h$) $H_{\prec}(\mathcal{P})$ ha rango N. Fissato un suo minore non nullo L di ordine N, siano $\mathbf{x}^{\mathbf{i}_{\sigma(1)}}, \ldots, \mathbf{x}^{\mathbf{i}_{\sigma(N)}} \in H$ i monomi corrispondenti alle colonne di L e $\mathbf{x}^{\mathbf{i}_{\sigma(N+1)}}, \ldots, \mathbf{x}^{\mathbf{i}_{\sigma(h)}}$ gli altri; si ha:

$$p_s = \sum_{r=1}^{h} \alpha_s^{\sigma(r)}\, \mathbf{x}^{\mathbf{i}_{\sigma(r)}}$$

Riguardando i monomi $\mathbf{x}^{\mathbf{i}_{\sigma(r)}}$ come h indeterminate, consideriamo il sistema di $h-N$ equazioni lineari nelle $\mathbf{x}^{\mathbf{i}_{\sigma(r)}}$:

$$\sum_{r=1}^{h} \alpha_s^{\sigma(r)}\, \mathbf{x}^{\mathbf{i}_{\sigma(r)}} = 0 \quad (s = N+1, \ldots, h). \tag{5}$$

Il minore

$$\left|\alpha_s^{\sigma(r)}\right| \quad (r, s = N+1, \ldots, h)$$

della matrice dei coefficienti è, per l'identità di Jacobi (cfr. [3]), diverso da zero. Pertanto è possibile risolvere il sistema (5) esprimendo le incognite $\mathbf{x}^{\mathbf{i}_{\sigma(N+1)}}, \ldots$

$\ldots, \mathbf{x}^{\mathbf{i}_{\sigma(h)}}$ in funzione delle $\mathbf{x}^{\mathbf{i}_{\sigma(1)}}, \ldots, \mathbf{x}^{\mathbf{i}_{\sigma(N)}}$:

$$\mathbf{x}^{\mathbf{i}_{\sigma(N+t)}} = \sum_{r=1}^{N} \eta_{t,r} \, \mathbf{x}^{\mathbf{i}_{\sigma(r)}}. \tag{6}$$

Le operazioni formali che producono le (6) a partire dalle (5) possono essere anche utilizzate per ottenere le (4) a partire da

$$p_s = \sum_{r=1}^{h} \alpha_s^{\sigma(r)} \, \mathbf{x}^{\mathbf{i}_{\sigma(r)}} \equiv 0 \quad (\text{mod. } I) \quad (s = N+1, \ldots, h).$$

L'asserto resta pertanto provato. □

3 Basi di Groebner per $\Im(\mathcal{P})$ e algoritmi per il calcolo del polinomio interpolatore.

3.1 In generale l'insieme di generatori $(p_{N+1}, \ldots, p_h, \gamma_1, \ldots, \gamma_n)$ di $I = \Im(\mathcal{P})$, considerato nella Prop. 2, non costituisce una base di Groebner di I. In relazione a $I = \Im(\mathcal{P})$, assumiamo G e B come in **2.1**; si ha ora: $B \subseteq H$ e $\#B = N$. Posto $\{b_1, \ldots, b_N\} := B_\prec$, sia $\mathcal{B}^{-1}$ la matrice inversa della matrice $\mathcal{B} := B_\prec(\mathcal{P})$ d'ordine N (vengono usate, qui, le notazioni introdotte in **2.2**). Posto infine $\alpha := (\alpha_1, \ldots, \alpha_N)_{-1}$, il polinomio

$$p(x_1, \ldots, x_n) := \sum_{j=1}^{N} (\mathcal{B}^{-1}\alpha)_j \, b_j \tag{7}$$

è il polinomio interpolatore cercato.

3.2 Un ragionamento alternativo, ma facente uso di un *machinery* simile, è il seguente.

Supponiamo che i punti P_i dati abbiano coordinate $(\rho_{i,1}, \ldots, \rho_{i,n})$ ed associamo ad ogni P_i il punto $Q_i \in K^{n+1}$ di coordinate $(\rho_{i,1}, \ldots, \rho_{i,n}, \alpha_i)$. Sia $J \subseteq K[x_1, \ldots, x_n, y]$ l'ideale dell'insieme $\mathcal{Q} := \{Q_1, \ldots, Q_N\}$. Se fissiamo sul monoide dei termini di $K[x_1, \ldots, x_n, y]$ un ordine $\preceq$ per il quale la y abbia un peso infinito rispetto a ciascuna delle x_i, allora la base di Groebner ridotta $L := RGB_\preceq(J)$ di J rispetto a tale ordine conterrà — oltre che dei polinomi nelle variabili $x_1, \ldots, x_n$— uno ed un solo polinomio contenente effettivamente la variabile y, diciamolo $g(x_1, \ldots, x_n, y)$.

Poichè, comunque si assegnino le prime coordinate $\sigma_1, \ldots, \sigma_n \in K$ esiste al più un valore $\beta \in K$ tale che il punto di coordinate $(\sigma_1, \ldots, \sigma_n, \beta)$ stia in $\mathcal{Q}$, tale polinomio dovrà essere della forma

$$y - p(x_1, \ldots, x_n).$$

Il polinomio $p(x_1, \ldots, x_n)$ che qui compare sarà ovviamente quello cercato.

3.3 L'algoritmo descritto in **3.1** richiedeva la conoscenza di una base monomiale B di $K[X]/\Im(\mathcal{P})$ e ciò al fine di i) precisare la natura del polinomio p cercato: $p \in span_K(B)$ e ii) determinare la matrice $\mathcal{B} := B_{\prec}(\mathcal{P})$ che — via la (7) — consentiva di esprimere p. La procedura per trovare tale base prevedeva innanzitutto di a) determinare l'ideale $I := \Im(\mathcal{P})$ e b) trovare la base di Groebner ridotta per I.

Vogliamo qui osservare che si può anche procedere in modo diverso, in un certo senso invertendo quel ragionamento. Osserviamo in primo luogo che vi è una corrispondenza biunivoca tra le basi monomiali $B \subseteq H$ e i minori non nulli d'ordine N della matrice $H_{\prec}(\mathcal{P})$. Determinato uno di tali minori non nulli, diciamolo A, sia $B_A = \{b_1, \ldots, b_N\}$ l'insieme dei termini corrispondenti alle colonne di A. A questo punto, assunto $B = B_A$, possiamo procedere come in **3.1**, o anche semplicemente esprimere il polinomio $y = p(x_1, \ldots, x_n)$ cercato mediante la formula

$$\begin{vmatrix} b_1 & \ldots & b_N & y \\ & & & \alpha_1 \\ & A & & \vdots \\ & & & \alpha_N \end{vmatrix} = 0$$

dove $A = (a_{ij})$ con $a_{ij} := b_j(P_i) = v_{P_i}(b_j)$.

3.4 Aggiungiamo a quanto precede che se il minore non nullo A di cui in **3.3** viene scelto in modo conveniente, possiamo sfruttarlo anche per ottenere una procedura atta a determinare direttamente un sistema di generatori dell'ideale cofinito $\Im(\mathcal{P})$ che sia anche la sua base di Groebner ridotta rispetto ad un fissato term-ordering $\preceq$. Supponiamo infatti di aver scelto A in modo tale che, detto b il termine di B_A più grande in $\preceq$ e detto $D \subseteq H$, $D \neq B_A$ un insieme di N termini tutti minori o uguali a b, si abbia $det(D_{\prec}(\mathcal{P})) = 0$. Siano $b_1, \ldots, b_N$ (con $b_1 \prec \ldots \prec b_N$) i termini di H corrispondenti alle colonne di A e sia $\{\tau_1, \ldots, \tau_l\}$ il più piccolo sottoinsieme di $H - \{b_1, \ldots, b_N\}$ tale che, comunque si prenda $\tau \in H - \{b_1, \ldots, b_N\}$, esiste un $1 \leq i \leq l$ tale che $\tau_i | \tau$. Posto $C^i := \{b_1, \ldots, b_N, \tau_i\}$, sia D_i la matrice d'ordine $N+1$ la cui prima riga è $C^i_{\prec}$ e le cui righe successive sono quelle della matrice $C^i_{\prec}(\mathcal{P})$ di tipo $N \times (N+1)$; posto $g_i = det(D_i)$, l'insieme $\{g_1, \ldots, g_l\}$ è allora la base di Groebner ridotta di I rispetto all'ordine $\preceq$. Un procedimento sostanzialmente equivalente al precedente è descritto in [5].

Va notato che, posto $E_{\prec} := \{b_1, \ldots, b_s\}$, $E'_{\prec} := \{b_1, \ldots, b_s, \tau\}$, e $E''_{\prec} :=$

$\{b_1, \dots, b_s, \sigma\}$, con $b_i, \tau, \sigma \in M$, se $\tau | \sigma$ allora

$$rango(E_{\prec}(\mathcal{P})) = rango(E'_{\prec}(\mathcal{P})) = s \Longrightarrow rango(E''_{\prec}(\mathcal{P})) = s\,.$$

Questa osservazione ha due conseguenze immediate: a) da un lato essa consente di semplificare la precedente procedura per determinare A: una volta scartata la colonna corrispondente ad un termine τ, vengono automaticamente scartate anche quelle corrispondenti a tutti i multipli di τ; b) d'altro lato essa assicura che, in tale procedura, il riferimento alla matrice $H_{\prec}(\mathcal{P})$ — anziché, più in generale, alla matrice $M_{\prec}(\mathcal{P})$ — non è affatto restrittivo.

3.5 Un altro algoritmo per costruire — induttivamente sulla cardinalità di $\mathcal{P}$ — la base di Groebner ridotta $RGB_{\preceq}(\Im(\mathcal{P}))$ di $\Im(\mathcal{P})$ rispetto al term-ordering $\preceq$, si fonda sulle osservazioni seguenti.

Sia $\{[\mathbf{x}^{\mathbf{i}}]_{\Im(\mathcal{P})} \mid \mathbf{i} \in \mathcal{F}\}$ la base monomiale, minimale rispetto al term-ordering $\preceq$, di $K[X]/\Im(\mathcal{P})$ e siano $\mathbf{f}_1, \dots, \mathbf{f}_s$ ($\mathbf{f}_1 \prec \dots \prec \mathbf{f}_s$) gli elementi diedrali esterni del diagramma di Ferrers $\mathcal{F}$. Allora $G := RGB_{\preceq}(\Im(\mathcal{P}))$ sarà della forma

$$G = \{\mathbf{x}^{\mathbf{f}_1} - p_1, \dots, \mathbf{x}^{\mathbf{f}_s} - p_s\}$$

dove ciascuno dei polinomi $p_i \in K[X]$ contiene esclusivamente termini minori di $\mathbf{x}^{\mathbf{f}_i}$ nell'ordine $\preceq$.

Consideriamo ora il punto $P = (a_1, \dots, a_n) \notin \mathcal{P}$ e l'insieme $\mathcal{P}' := \mathcal{P} \cup \{P\}$, e siano $\mathcal{F}'$ e G' gli analoghi, relativamente a $\mathcal{P}'$, di $\mathcal{F}$ e G. Indichiamo con j, $1 \le j \le s$, il più piccolo indice tale che P non sia uno zero del polinomio $\mathbf{x}^{\mathbf{f}_j} - p_j$. È facile riconoscere che $\{[\mathbf{x}^{\mathbf{i}}]_{\Im(\mathcal{P}')} \mid \mathbf{i} \in \mathcal{F} \cup \{\mathbf{f}_j\}\}$ costituisce una base monomiale per $K[X]/\Im(\mathcal{P}')$ (si tenga presente che $codim\Im(\mathcal{P}') = N + 1 = \#(\mathcal{F} \cup \{\mathbf{f}_j\})$), che inoltre (giacché $\mathcal{F} \cup \{\mathbf{f}_j\}$ è un diagramma di Ferrers) è minimale rispetto ad un opportuno term-ordering. Proviamo che tale term-ordering è proprio quello considerato, cioè che si ha $\mathcal{F}' = \mathcal{F} \cup \{\mathbf{f}_j\}$, e nel contempo costruiamo la base di Groebner ridotta G'.

Iniziamo con l'osservare che gli elementi diedrali esterni di $\mathcal{F}$, diversi da $\mathbf{f}_j$, sono tali anche per il diagramma di Ferrers $\mathcal{F} \cup \{\mathbf{f}_j\}$. Gli eventuali altri elementi diedrali esterni di $\mathcal{F} \cup \{\mathbf{f}_j\}$ sono della forma $\mathbf{f}_j + \varepsilon_h$ (dove si è posto $\varepsilon_1 = (1, 0, \dots, 0), \dots, \varepsilon_n = (0, \dots, 0, 1)$). Supponiamo che siano tutti e soli quelli per i quali l'indice h appartiene all'insieme (eventualmente vuoto) $\{h_1, \dots, h_t\} \subseteq \{1, \dots, n\}$. (Va da sé che non è possibile precisare ulteriormente la natura di questo insieme, dipendendo essa da $\mathbf{f}_j$ e $\mathcal{F}$). Assumiamo pertanto che gli elementi diedrali esterni di $\mathcal{F} \cup \{\mathbf{f}_j\}$ siano quelli dell'insieme

$$\Phi = \{\mathbf{f}_1, \dots, \mathbf{f}_{j-1}, \mathbf{f}_{j+1}, \dots, \mathbf{f}_s, \mathbf{f}_j + \varepsilon_{h_1}, \dots, \mathbf{f}_j + \varepsilon_{h_t}\}$$

(con $0 \le t \le n$). Per provare che $\mathcal{F}' = \mathcal{F} \cup \{\mathbf{f}_j\}$ occorre dimostrare che per ogni $\mathbf{f} \in \Phi$ esiste in $\Im(\mathcal{P}')$ un polinomio della forma $\mathbf{x}^{\mathbf{f}} - p$, con p avente termini inferiori a $\mathbf{f}$ nel term-ordering $\preceq$ considerato. È facile controllare che tale polinomio è dato da

$$g_i := \mathbf{x}^{\mathbf{f}_i} - p_i - A_i/A_j\,(\mathbf{x}^{\mathbf{f}_j} - p_j) \qquad (i = 1, \ldots, s;\ i \neq j)$$

(dove A_l indica il valore che il polinomio $\mathbf{x}^{\mathbf{f}_l} - p_l$ assume in P) per ogni

$$\mathbf{f}_i \in \Phi_1 := \{\mathbf{f}_1, \ldots, \mathbf{f}_{j-1}, \mathbf{f}_{j+1}, \ldots, \mathbf{f}_s\},$$

mentre, per ogni elemento diedrale

$$\mathbf{f}_j + \varepsilon_{h_r} \in \Phi_2 := \{\mathbf{f}_j + \varepsilon_{h_1}, \ldots, \mathbf{f}_j + \varepsilon_{h_t}\},$$

è quello — diciamolo $\tilde{g}_r$ — che si ottiene operando una riduzione completa, a mezzo dei polinomi g_i, del polinomio

$$(x_r - a_r)(\mathbf{x}^{\mathbf{f}_j} - p_j).$$

Resta così provato che $\mathcal{F}' = \mathcal{F} \cup \{\mathbf{f}_j\}$ e che $G' := RGB_{\preceq}(\Im(\mathcal{P}'))$ è l'insieme

$$\{g_1, \ldots, g_{j-1}, g_{j+1}, \ldots, g_s, \tilde{g}_1, \ldots, \tilde{g}_r\}.$$

4 Un algoritmo combinatorio per determinare una base monomiale per $K[X]/\Im(\mathcal{P})$.

4.1 Nel seguito adotteremo le seguenti convenzioni. Con una notazione del tipo $\underline{\mathcal{P}} := \underline{\{P_1, \ldots, P_N, \ldots\}}$, denoteremo un insieme ordinato secondo l'ordine in cui gli elementi $P_1, \ldots, P_N, \ldots$ sono elencati, mentre $\mathcal{P} := \{P_1, \ldots, P_N, \ldots\}$ indicherà l'insieme sostegno dell'insieme ordinato $\underline{\mathcal{P}} := \underline{\{P_1, \ldots, P_N, \ldots\}}$. Conseguentemente, se $\underline{\mathcal{P}} := \underline{\{P_1, \ldots, P_N, \ldots\}}$ e $\underline{\mathcal{Q}} := \underline{\{Q_1, \ldots, Q_N, \ldots\}}$, la notazione $\underline{\mathcal{P}} = \underline{\mathcal{Q}}$ denoterà, oltre che $\mathcal{P} = \mathcal{Q}$, anche che $P_i = Q_i$ per ogni i. Infine, se $\underline{\phi}$ è un operatore tra insiemi di insiemi ordinati, denoteremo con $\phi(\underline{\mathcal{P}})$, o semplicemente con $\phi(\mathcal{P})$, l'insieme sostegno di $\underline{\phi}(\underline{\mathcal{P}})$.

In breve: la sottolineatura starà ad indicare che è necessario tener conto dell'ordine, mentre la mancanza di sottolineatura che, trascurando l'ordine, si prendono in considerazione solo gli aspetti insiemistici della questione.

4.2 Nel paragrafo precedente si sono descritti diversi algoritmi di soluzione del **Problema 1**. In ciascuno di essi la parte che decisamente comporta calcoli più pesanti è quella relativa alla determinazione di una base monomiale per $K[X]/I$ $\quad (I = \Im(\mathcal{P}))$. Nel presente paragrafo descriveremo un semplice algoritmo puramente combinatorio che consente di risolvere rapidamente tale problema.

Definiamo dapprima un operatore — l'operatore $\underline{\mathcal{D}}$ — che consente di associare ad un arbitrario insieme ordinato finito $\underline{\mathcal{P}} := \underline{\{P_1, \ldots, P_N\}}$ di punti dello spazio K^n un insieme ordinato, $\underline{\mathcal{D}}(\underline{\mathcal{P}}) := \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_N\}} \subset \mathbf{N}^n$ di cardinalità $\#\underline{\mathcal{D}}(\underline{\mathcal{P}}) = \#\underline{\mathcal{P}} = N$ tale che il sottoinsieme $\underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_s\}}$ sia, per ogni $s \leq N$, l'insieme $\underline{\mathcal{D}}(\underline{\{P_1, \ldots, P_s\}})$ associato a $\underline{\{P_1, \ldots, P_s\}}$. Resterà pertanto determinato anche un isomorfismo di insiemi ordinati

$$\begin{array}{rccc} \delta_{\underline{\mathcal{P}}}: & \underline{\mathcal{P}} & \longrightarrow & \underline{\mathcal{D}}(\underline{\mathcal{P}}) \\ & P_i & \longmapsto & \mathbf{d}_i. \end{array}$$

(Nel seguito useremo talvolta la notazione $\underline{\delta}_{\mathcal{P}}$ in luogo di $\delta_{\underline{\mathcal{P}}}$ quando ciò non darà adito a confusione.)

Proveremo quindi che i) in qualità di insieme non ordinato, $\mathcal{D}(\mathcal{P})$ non dipende dall'ordine fissato in $\underline{\mathcal{P}}$ (Prop. 3), ii) $\underline{\mathcal{D}}(\underline{\mathcal{P}})$ è un *diagramma di Ferrers* (ordinato, n-dimensionale) (Prop. 5), e iii) l'insieme

$$\{\mathbf{x}^{\mathbf{d}} \mid \mathbf{d} \in \mathcal{D}(\mathcal{P})\}$$

costituisce una base monomiale per l'algebra quoziente $K[X]/\mathfrak{I}(\mathcal{P})$ (Prop. 6) che è minimale per l'ordine lessicografico inverso (Prop. 7).

4.3 Indichiamo con π_s e π^s le proiezioni

$$\begin{array}{rccc} \pi_s: & K^n & \longrightarrow & K^s \\ & (a_1, \ldots, a_n) & \longmapsto & (a_1, \ldots, a_s) \end{array}$$

e

$$\begin{array}{rccc} \pi^s: & K^n & \longrightarrow & K^{n-s+1} \\ & (a_1, \ldots, a_n) & \longmapsto & (a_s, \ldots, a_n); \end{array}$$

poniamo inoltre

$$\Pi_s(P, \mathcal{P}) := \{P_i \in \mathcal{P} \mid \pi_s(P_i) = \pi_s(P)\}$$
$$\Pi^s(P, \mathcal{P}) := \{P_i \in \mathcal{P} \mid \pi^s(P_i) = \pi^s(P)\}$$

con $P \in K^n$ e $\mathcal{P} \subseteq K^n$. Riguardando $\mathbf{N}^n$ come un sottoinsieme di K^n, risulta ovvio il significato da attribuire ai simboli $\pi_s(\mathbf{d})$, $\pi^s(\mathbf{d})$, $\Pi_s(\mathbf{d}, D)$ e $\Pi^s(\mathbf{d}, D)$ qualora $\mathbf{d} \in \mathbf{N}^n$ e $D \subseteq \mathbf{N}^n$. Queste, ed altre notazioni che introdurremo nel corso di questo paragrafo, vanno peraltro considerate con una certa duttilità che ci consentirà di evitare pignolerie tese ad un inutile rigore; ad esempio non staremo a precisare che cosa debba intendersi per "$\pi_s : K^m \longrightarrow K^s$" qualora $m \neq n$. Converremo inoltre tacitamente che l'ordine considerato su sottoinsiemi (o proiezioni di sottoinsiemi) di $\underline{\mathcal{P}}$ è quello indotto dall'ordine su $\underline{\mathcal{P}}$.

Se $P \notin \mathcal{P}$, diremo che s, $1 \leq s \leq n$, è il *σ-valore di $P \in K^n$ rispetto a $\mathcal{P} \subseteq K^n$* — in simboli: $s = \sigma(P, \mathcal{P})$ — se s è il più grande intero tale che $\Pi_{s-1}(P, \mathcal{P}) \neq \emptyset$ (si assume convenzionalmente che sia $\Pi_0(P, \mathcal{P}) \neq \emptyset$ per ogni $\mathcal{P}$ ed ogni P); poniamo inoltre

$$\Sigma(P, \mathcal{P}) := \{P_i \in \mathcal{P} \mid \pi_{s-1}(P_i) = \pi_{s-1}(P) \text{ con } s = \sigma(P, \mathcal{P})\} \qquad (P \notin \mathcal{P})$$

(in altri termini: $P_i \in \Sigma(P, \mathcal{P})$ sse P e P_i hanno esattamente le prime $s-1$ coordinate uguali). Queste notazioni vanno estese al caso $P \in \underline{P}$ — sia $P = P_j$ — nel modo seguente:

$$\sigma(P, \underline{P}) := \sigma(P, \{P_1, \ldots, P_{j-1}\}) \qquad (P \in \underline{P})$$

$$\Sigma(P, \underline{P}) := \Sigma(P, \{P_1, \ldots, P_{j-1}\}) \qquad (P \in \underline{P}).$$

4.4 L'operatore $\underline{D}$.

Ciò premesso, descriviamo — per induzione sulla cardinalità $N = \#\mathcal{P}$ — l'Algoritmo D che definisce l'operatore $\underline{D}$.

<u>**Algoritmo D.**</u>

1) Se $N = 1$, allora $\underline{D}(\underline{P}) := \{(0, \ldots, 0)\}$.

2) Se $\aleph_0 > N > 1$, facendo uso dell'ipotesi induttiva assumiamo di conoscere l'insieme $\underline{D}(\underline{\{P_1, \ldots, P_{N-1}\}}) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_{N-1}\}}$ e indichiamo come determinare l'elemento $\mathbf{d}_N \in \mathbf{N}^n$ corrispondente all'ultimo punto P_N di $\underline{P}$.

Posto $s = \sigma(P_N, \underline{P})$, dividiamo le componenti $d_{N,i}$ $(i = 1, \ldots, n)$ dell'elemento $\mathbf{d}_N \in \mathbf{N}^n$ cercato in tre diversi sottoinsiemi, a seconda che i sia maggiore, uguale o minore di s:

a) Per $i > s$, poniamo $d_{N,i} = 0$;

b) al fine di determinare $d_{N,s}$ consideriamo il più grande indice m, $1 \leq m < N$, tale che per il corrispondente punto P_m si abbia

$$\pi_{s-1}(P_m) = \pi_{s-1}(P_N) \qquad \pi^{s+1}(\mathbf{d}_m) = (0, \ldots, 0) = \pi^{s+1}(\mathbf{d}_N)$$

(cioè, posto $P_i = (a_{i,1}, \ldots, a_{i,n})$ e $\underline{\delta}_{\underline{P}}(P_i) = \mathbf{d}_i = (d_{i,1}, \ldots, d_{i,n})$, tale che

$$a_{m,1} = a_{N,1}, \ldots, a_{m,s-1} = a_{N,s-1} \qquad d_{m,s+1} = \ldots = d_{m,n} = 0\ )$$

[questo punto P_m verrà detto *σ-antecedente* di P_N *rispetto alla coppia di insiemi ordinati* $\underline{\{P_1, \ldots, P_{N-1}\}}$, $\underline{D}(\underline{\{P_1, \ldots, P_{N-1}\}})$] e si ponga

$$d_{N,s} := d_{m,s} + 1;$$

c) infine, per determinare i valori $d_{N,i}$ per $i < s$, consideriamo il sottoinsieme

$$\mathcal{L}(P_N, \underline{P}) := \underline{\{P_{j_1}, \ldots, P_{j_r}\}}$$

di $\underline{P}$, formato da tutti i punti di $\underline{P}$ cui $\underline{\delta_P}$ fa corrispondere un elemento $\mathbf{d} \in \underline{D}(\underline{P})$ tale che $\pi^s(\mathbf{d}) = (d_{N,s}, 0, \ldots, 0) = \pi^s(\mathbf{d}_N)$ [avente cioè $d_{N,s}, 0, \ldots, 0$ come ultime $n-s+1$ componenti]; in particolare: $P_{j_r} = P_N$. Poniamo

$$\underline{Q} := \pi_{s-1}(\mathcal{L}(P_N, \underline{P})) \subseteq K^{s-1}$$

(in altri termini: i punti di $\underline{Q}$ sono i punti di $\mathcal{L}(P_N, \underline{P})$ privati delle ultime $n-s+1$ coordinate). Va notato che se $h < r = \#\mathcal{L}(P_N, \underline{P})$ allora $\pi_{s-1}(P_{j_h}) \neq \pi_{s-1}(P_N)$; più in generale, il carattere induttivo della presente descrizione di $\underline{D}$ assicura che se $h < k \leq r$ allora $\pi_{s-1}(P_{j_h}) \neq \pi_{s-1}(P_{j_k})$; ne consegue che si ha: $\#\underline{Q} = \#\mathcal{L}(P_N, \underline{P}) = r$.

Poiché ovviamente $r = \#\underline{Q} < N$, per l'ipotesi induttiva si conosce l'insieme

$$\underline{D}(\underline{Q}) = \underline{\{\tilde{\mathbf{d}}_1, \ldots, \tilde{\mathbf{d}}_r\}}$$

e si ha

$$\tilde{\mathbf{d}}_i = \pi_{s-1}(\mathbf{d}_{j_i}) \qquad \text{per ogni } 1 \leq i < r.$$

Le prime $s-1$ componenti di $\mathbf{d}_N$ vengono allora definite da

$$\pi_{s-1}(\mathbf{d}_N) := \tilde{\mathbf{d}}_r.$$

3) Se $N = \aleph_0$, sia $\underline{P} = \underline{\{P_1, \ldots, P_N, \ldots\}}$ e $\underline{D}_N := \underline{D}(\underline{\{P_1, \ldots, P_N\}})$ e poniamo

$$\underline{D}(\underline{P}) := \bigcup \underline{D}_N.$$

4.5 Alcune proprietà di $\underline{D}(\underline{P})$.

Il seguente lemma giustifica alcuni passi nella descrizione precedente dell'Algoritmo D; in particolare dà senso all'applicazione $\underline{\delta_P}$.

Lemma 1 *Siano* $\underline{P} = \underline{\{P_1, \ldots, P_N\}}$ *e* $\underline{D}(\underline{P}) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_N\}}$. *Allora per ogni* $s \leq N$ *si ha* $\underline{D}(\underline{\{P_1, \ldots, P_s\}}) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_s\}}$.

Dimostrazione. Ovvia (per la natura induttiva dell'Algoritmo D). $\square$

Proposizione 3 *L'insieme sostegno* $\mathcal{D}(\mathcal{P})$ *di* $\underline{D}(\underline{P})$ *non dipende dall'ordine fissato in* $\underline{P}$.

Dimostrazione. Ci si convince facilmente che, posto

$$\underline{P}_1 := \underline{\{P_1, \ldots, P_N, P, P'\}}, \qquad \underline{P}_2 := \underline{\{P_1, \ldots, P_N, P', P\}},$$

è sufficiente provare che

$$\mathcal{D}(\mathcal{P}_1) = \mathcal{D}(\mathcal{P}_2).$$

Posto:

$$\mathbf{d} = (d_1, \ldots, d_n) := \underline{\delta}_{P_1}(P) \qquad \mathbf{d}' := (d'_1, \ldots, d'_n) := \underline{\delta}_{P_1}(P')$$

$$\mathbf{f} = (f_1, \ldots, f_n) := \underline{\delta}_{\mathcal{P}_2}(P) \qquad \mathbf{f}' := (f'_1, \ldots, f'_n) := \underline{\delta}_{\mathcal{P}_2}(P')$$

cioè

$$\underline{D}_1 := \underline{\mathcal{D}}(\underline{\mathcal{P}}_1) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_N, \mathbf{d}, \mathbf{d}'\}},$$

$$\underline{D}_2 := \underline{\mathcal{D}}(\underline{\mathcal{P}}_2) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_N, \mathbf{f}', \mathbf{f}\}},$$

occorre allora provare che o

$$(A) \qquad \mathbf{d} = \mathbf{f}', \quad \mathbf{d}' = \mathbf{f}$$

(nel qual caso $\underline{D}_1$ e $\underline{D}_2$ coincidono anche in quanto insiemi ordinati) oppure

$$(B) \qquad \mathbf{d} = \mathbf{f}, \quad \mathbf{d}' = \mathbf{f}'.$$

Indicate con a_i e a'_i $(i = 1, \ldots, n)$ le coordinate di P e P' rispettivamente, sia r, $1 < r \leq n$, tale che

$$d_r \neq d'_r, \; d_{r+1} = d'_{r+1}, \; \ldots, \; d_n = d'_n.$$

Non è difficile provare che ciò comporta che il valore assunto — nel calcolo di $\underline{D}_1 := \underline{\mathcal{D}}(\underline{\mathcal{P}}_1)$ — dalla $(n-r)$-upla $(d'_{r+1}, \ldots, d'_n)$ non dipende in alcun modo dal punto P che precede P' in $\underline{\mathcal{P}}_1$ e quindi deve coincidere con quello della analoga $(n-r)$-upla $(f'_{r+1}, \ldots, f'_n)$ ottenuta nel calcolo di $\underline{D}_2 := \underline{\mathcal{D}}(\underline{\mathcal{P}}_2)$:

$$d'_{r+1} = f'_{r+1}, \; \ldots, \; d'_n = f'_n.$$

Allo stesso modo si prova che

$$d_{r+1} = f_{r+1}, \; \ldots, \; d_n = f_n$$

e quindi si ha

$$d_{r+1} = d'_{r+1} = f_{r+1} = f'_{r+1}, \; \ldots, \; d_n = d'_n = f_n = f'_n.$$

Ne consegue che, ai fini di quanto si vuole dimostrare, non è restrittivo assumere $r = n$ e quindi $d_n \neq d'_n$. In tale ipotesi, è facile verificare che si presenterà il caso (A) o il caso (B) a seconda che si abbia $(a_1, \ldots, a_{n-1}) = (a'_1, \ldots, a'_{n-1})$ oppure $(a_1, \ldots, a_{n-1}) \neq (a'_1, \ldots, a'_{n-1})$. □

Lemma 2 *Siano $\mathcal{P}, \mathcal{P}' \subseteq K^n$ e sia $\mathcal{P} \subseteq \mathcal{P}'$; allora $\mathcal{D}(\mathcal{P}) \subseteq \mathcal{D}(\mathcal{P}')$.*

Dimostrazione. A causa della Prop.3 non è restrittivo supporre — ai fini del calcolo di $\mathcal{D}(\mathcal{P}')$ — che i punti appartenenti anche a $\mathcal{P}$ precedano, in $\underline{\mathcal{P}}'$, tutti gli altri: $\underline{\mathcal{P}}' = \underline{\{P_1, \ldots, P_N, P_{N+1}, \ldots, P_{N'}\}}$, con $\underline{\mathcal{P}} = \underline{\{P_1, \ldots, P_N\}}$. Da ciò e dal Lemma 1 consegue l'assunto. □

Dato un insieme (finito, ordinato) $\underline{\mathcal{P}} = \underline{\{P_1, \ldots, P_N\}} \subseteq K^n$, sia:

$$\underline{D} := \underline{\mathcal{D}}(\underline{\mathcal{P}})$$

$$h := max\{d_n \mid \mathbf{d} = (d_1, \ldots, d_n) \in \underline{D}\}$$
$$\underline{D}_r := \underline{\{\mathbf{d} = (d_1, \ldots, d_n) \in \underline{D} \mid d_n = r\}}$$
$$\underline{P}_r := \underline{\{P \in \underline{P} \mid \delta_{\underline{P}}(P) \in \underline{D}_r\}}.$$

Si ha il

Lemma 3 *Valgono le relazioni:*

$$r > r' \Longrightarrow \pi_{n-1}(\underline{P}_r) \subseteq \pi_{n-1}(\underline{P}_{r'}) \tag{8}$$
$$\underline{D}(\pi_{n-1}(\underline{P}_r)) = \pi_{n-1}(\underline{D}_r). \tag{9}$$

Dimostrazione. Per analisi diretta dell'Algoritmo D. □

Diremo che $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbf{N}^n$ precede $\mathbf{j} = (j_1, \ldots, j_n) \in \mathbf{N}^n$ nell'ordine *lessicografico inverso*, in simboli $\mathbf{i} \prec_{i.l.} \mathbf{j}$, se la prima non nulla delle differenze $j_n - i_n, \ldots, j_1 - i_1$ è positiva.

Lemma 4 *Sia* $\underline{P} = \underline{\{P_1, \ldots, P_N\}}$, $\underline{D}(\underline{P}) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_N\}}$, $\mathbf{d}_i = \delta_{\underline{P}}(P_i)$; *supponiamo che* $\mathbf{d}_{s+1} = \underline{\delta_{\underline{P}}(P_{s+1}) \prec_{i.l.} \mathbf{d}_s = \delta_{\underline{P}}(P_s)}$.

Posto allora

$$\underline{P}' = \underline{\{P_1, \ldots, P_{s+1}, P_s, \ldots, P_N\}},$$

si ha

$$\underline{D}(\underline{P}') = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_{s+1}, \mathbf{d}_s, \ldots, \mathbf{d}_N\}}.$$

Dimostrazione. (Traccia). Si ponga $P_s = (a_1, \ldots, a_n)$, $P_{s+1} = (b_1, \ldots, b_n)$; $\mathbf{d}_s = (j_1, \ldots, j_m, 0, \ldots, 0)$, $\mathbf{d}_{s+1} = (i_1, \ldots, i_r, 0, \ldots, 0)$ con $r \leq m \leq n$ e si distinguano i due casi $r < m$ e $r = m$ osservando che in entrambi deve accadere che $(a_1, \ldots, a_{m-1}) \neq (b_1, \ldots, b_{m-1})$ (pur senza poter escludere che nel primo si abbia $(a_1, \ldots, a_{r-1}) \neq (b_1, \ldots, b_{r-1})$) e ragionando per induzione sul numero $n \geq 2$ delle coordinate (per $n = 1$ le ipotesi del Lemma sono assurde) qualora $r = m$ e $i_r = j_r$. □

Proposizione 4 *Dato un insieme finito* $\underline{P} \subseteq K^n$, *è sempre possibile ordinarlo,* $\underline{P} = \underline{\{P_1, \ldots, P_N\}}$, *in modo tale che* $\underline{D}(\underline{P}) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_N\}}$ ($\mathbf{d}_i = \delta_{\underline{P}}(P_i)$) *sia ordinato secondo l'ordine lessicografico inverso:*

$$s < t \Longrightarrow \mathbf{d}_s = \delta_{\underline{P}}(P_s) \prec_{i.l.} \mathbf{d}_t = \delta_{\underline{P}}(P_t).$$

Dimostrazione. È una conseguenza diretta della Prop. 3 e del Lemma 4. □

4.6 Ulteriori proprietà di $\underline{D}(\underline{P})$.

Si consideri l'insieme $\mathbf{N}^n$ con l'ordine (parziale) prodotto indotto dall'ordine naturale su $\mathbf{N}$:

$$(i_1, \ldots, i_n) < (j_1, \ldots, j_n)$$

se e solo se

$$(i_1, \ldots, i_n) \neq (j_1, \ldots, j_n) \quad e \quad (\forall s)(i_s \leq j_s).$$

Un sottoinsieme $\mathcal{F} \subseteq \mathbf{N}^n$ verrà detto *diagramma di Ferrers n-dimensionale (standard)* se:

1) $\mathbf{0} := (0, \ldots, 0) \in \mathcal{F}$;

2) se $\mathbf{i} \in \mathcal{F}$ allora $[\mathbf{0}, \mathbf{i}] := \{\mathbf{j} \in \mathbf{N}^n \mid \mathbf{0} \leq \mathbf{j} \leq \mathbf{i}\} \subseteq \mathcal{F}$.

Diremo invece che $\mathcal{F} \subseteq \mathbf{N}^n$ è un *diagramma di Ferrers n-dimensionale generalizzato* se

$$\mathbf{i}, \mathbf{h} \in \mathcal{F} \Rightarrow [\mathbf{i}, \mathbf{h}] := \{\mathbf{j} \in \mathbf{N}^n \mid \mathbf{i} \leq \mathbf{j} \leq \mathbf{h}\} \subseteq \mathcal{F}.$$

È immediato provare che:

Lemma 5 *i) Se $\mathcal{F} \subseteq \mathbf{N}^n$ è tale che, per ogni $1 \leq j \leq n$, si ha*

$$(i_1, \ldots, i_n) \in \mathcal{F} \Longrightarrow (i_1, \ldots, i_j - 1, \ldots, i_n) \in \mathcal{F}$$

allora $\mathcal{F}$ è un diagramma di Ferrers.
ii) Sia $\mathcal{F}$ un diagramma di Ferrers n-dimensionale (standard). Considerato il sottoinsieme $\{r_1, \ldots, r_m\} \subseteq \{1, \ldots, n\}$ e la proiezione

$$\begin{array}{cccc} \psi: & \mathbf{N}^n & \longrightarrow & \mathbf{N}^m \\ & (i_1, \ldots, i_n) & \longmapsto & (i_{r_1}, \ldots, i_{r_m}), \end{array}$$

allora $\psi(\mathcal{F})$ è un diagramma di Ferrers m-dimensionale (standard). □

Sia $\mathcal{F} \subseteq \mathbf{N}^n$ un diagramma di Ferrers. Un elemento $\mathbf{j} \in \mathbf{N}^n$ verrà detto *diedrale esterno* per $\mathcal{F}$ se

$$a) \quad \{\mathbf{i} \in \mathbf{N}^n \mid \mathbf{i} < \mathbf{j}\} \subseteq \mathcal{F}$$

$$b) \quad \{\mathbf{i} \in \mathbf{N}^n \mid \mathbf{j} \leq \mathbf{i}\} \cap \mathcal{F} = \emptyset$$

(equivalentemente se a) e c) $\mathbf{j} \notin \mathcal{F}$); verrà invece detto *diedrale interno* se

$$a') \quad \{\mathbf{i} \in \mathbf{N}^n \mid \mathbf{i} \leq \mathbf{j}\} \subseteq \mathcal{F}$$

$$b') \quad \{\mathbf{i} \in \mathbf{N}^n \mid \mathbf{j} > \mathbf{i}\} \cap \mathcal{F} = \emptyset$$

(equivalentemente se b') e c') $\mathbf{j} \in \mathcal{F}$).

Un elemento diedrale $\mathbf{f} = (f_1, \ldots, f_n)$ di $\mathcal{F}$ sarà detto essere *di livello l* $(1 \leq l \leq n)$ se $f_l \neq 0$, $f_{l+1} = \ldots = f_n = 0$.

È immediato riconoscere che un diagramma di Ferrers n-dimensionale non vuoto ha almeno un elemento diedrale interno ed almeno n elementi diedrali esterni e che l'insieme degli uni o degli altri caratterizza $\mathcal{F}$. Indicando con $\mathbf{f}_1, \ldots, \mathbf{f}_s$ (rispettivamente ${}_1\mathbf{f}, \ldots, {}_t\mathbf{f}$) gli elementi diedrali esterni (risp. interni) di $\mathcal{F}$, esprimeremo questo fatto con la notazione

$$\mathcal{F} = \; > \mathbf{f}_1, \ldots, \mathbf{f}_s < \; = \; < {}_1\mathbf{f}, \ldots, {}_t\mathbf{f} > .$$

Dati due diagrammi di Ferrers $\mathcal{F} \subset \mathcal{F}'$ tali che $\mathcal{F}' - \mathcal{F} = \{\mathbf{f}\}$ (differenza insiemistica), allora $\mathbf{f}$ è un elemento diedrale esterno per $\mathcal{F}$ (rispett. diedrale interno per $\mathcal{F}'$). Ne consegue che un diagramma di Ferrers può accrescersi (di un elemento alla volta) solo tramite aggiunta di elementi diedrali esterni.

Consideriamo: $\underline{\mathcal{P}} := \{P_1, \ldots, P_N\}$, $\underline{\mathcal{P}'} := \{P_1, \ldots, P_N, P_{N+1}\}$, $\underline{\mathcal{D}(\mathcal{P})} := \{\mathbf{d}_1, \ldots, \mathbf{d}_N\}$ e $\underline{\mathcal{D}(\mathcal{P}')} := \{\mathbf{d}_1, \ldots, \mathbf{d}_N, \mathbf{d}_{N+1}\}$; è facile provare che se $\underline{\mathcal{D}(\mathcal{P})}$ è un diagramma di Ferrers allora $\mathbf{d}_{N+1}$ è un suo elemento diedrale esterno. Se ne deduce, ragionando per induzione sulla cardinalità di $\mathcal{P}$, che vale la

Proposizione 5 *L'insieme $\mathcal{D}(\mathcal{P})$ è un diagramma di Ferrers.* □

Proposizione 6 *Sia $D := \mathcal{D}(\mathcal{P})$; allora $\{[\mathbf{x}^{\mathbf{d}}]_{\Im(\mathcal{P})} \mid \mathbf{d} \in D\}$ costituisce una base monomiale per $K[X]/\Im(\mathcal{P})$.*

Dimostrazione. Ragioniamo per induzione sulla dimensione n di K^n. Per $n = 1$ si ha $\mathcal{P} = \{\rho_1, \ldots, \rho_N\}$ e $I := \Im(\mathcal{P}) = (g)$ con

$$g = \prod_{i=1}^{N} (x - \rho_i).$$

Applicando l'Algoritmo D a $\mathcal{P}$ si ottiene $\mathcal{D}(\mathcal{P}) = \{0, 1, \ldots, N-1\}$; pertanto $\{[\mathbf{x}^{\mathbf{d}}]_{\Im(\mathcal{P})} \mid \mathbf{d} \in D\} = \{[1], [x], \ldots, [x^{N-1}]\}$, che è, banalmente, una base monomiale per $K[X]/\Im(\mathcal{P})$.

Supponiamo ora che la Proposizione sia vera per ogni sottoinsieme finito di $K^{n'}$, con $n' < n$, e dimostriamola per l'insieme $\mathcal{P} = \{P_1, \ldots, P_N\} \subseteq K^n$. Poiché $dim(K[X]/\Im(\mathcal{P})) = N = \#\mathcal{D}(\mathcal{P})$, è sufficiente provare che le classi di equivalenza, modulo $\Im(\mathcal{P})$, dei monomi associati agli elementi di $\mathcal{D}(\mathcal{P})$ sono linearmente indipendenti in $K[X]/\Im(\mathcal{P})$, cioè che, dato un polinomio $p(x_1, \ldots, x_n)$ della forma

$$p(x_1, \ldots, x_n) = \sum_{\mathbf{d} \in \mathcal{D}(\mathcal{P})} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}},$$

se $p(x_1, \ldots, x_n) \in \Im(\mathcal{P})$ allora $p(x_1, \ldots, x_n)$ è identicamente nullo.

Supposto pertanto $p(x_1, \ldots, x_n) \in \Im(\mathcal{P})$, poniamo

$$p(x_1, \ldots, x_n) = \sum_{r=0}^{h} p_r(x_1, \ldots, x_{n-1}) \cdot x_n^r$$

con

$$p_r(x_1, \ldots, x_{n-1}) := \sum_{(d_1, \ldots, d_{n-1}) \in \pi_{n-1}(D_r)} \alpha_{(d_1, \ldots, d_{n-1}, r)} \cdot x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}. \tag{10}$$

Il polinomio $p(x_1, \ldots, x_n)$ deve annullarsi per ogni punto $P = (a_1, \ldots, a_n) \in \mathcal{P}$; se, in particolare, $P \in \mathcal{P}_h$, ciò comporta che

$$p_h(a_1, \ldots, a_{n-1}) = 0 \quad \text{con} \quad (a_1, \ldots, a_{n-1}) \in \pi_{n-1}(\mathcal{P}_h)$$

(giacché il polinomio $p(a_1, \ldots, a_{n-1}, x_n)$ — dovendo ammettere $h+1$ radici [si tenga presente che per ogni $P \in \mathcal{P}_h$ esistono in $\mathcal{P}$ altri h punti aventi le stesse prime $n-1$ coordinate di P] — deve essere identicamente nullo). Avendo presente la (9) e la (10), da quest'ultima si trae — per l'ipotesi induttiva — che il polinomio $p_h(x_1, \ldots, x_{n-1})$ deve annullarsi identicamente.

Iterando, per $r = h-1, h-2, \ldots, 0$, il ragionamento appena fatto per $r = h$ — e sfruttando la (8) — si perviene a concludere che, per ogni $0 \leq r \leq h$, il polinomio $p_r(x_1, \ldots, x_{n-1})$ è identicamente nullo e quindi tale è anche $p(x_1, \ldots, x_n)$. □

Proposizione 7 *La base monomiale* $\{[\mathbf{x}^{\mathbf{d}}]_{\Im(\mathcal{P})} \mid \mathbf{d} \in \mathcal{D}(\mathcal{P})\}$ *di* $K[X]/\Im(\mathcal{P})$ *è minimale rispetto all'ordine lessicografico inverso* $\prec_{i.l.}$.

Dimostrazione. A causa della Prop. 4, possiamo supporre di aver ordinato l'insieme $\underline{\mathcal{P}} := \{P_1, \ldots, P_N\}$ in modo tale che per $\underline{D} := \underline{\mathcal{D}}(\underline{\mathcal{P}}) := \{\mathbf{d}_1, \ldots, \mathbf{d}_N\}$, con $\mathbf{d}_i := \underline{\delta_{\mathcal{P}}}(P_i)$, si abbia $\mathbf{d}_i \prec_{i.l.} \mathbf{d}_{i+1}$ $(i = 1, \ldots, N-1)$. Nel corso della presente dimostrazione, tale ipotesi verrà sfruttata ripetutamente, e talvolta tacitamente.

Sia $C := \mathcal{C}(\mathcal{P}) \subseteq \mathbf{N}^n$ tale che $\{[\mathbf{x}^{\mathbf{i}}]_{\Im(\mathcal{P})} \mid \mathbf{i} \in \mathcal{C}(\mathcal{P})\}$ costituisca una base monomiale di $K[X]/\Im(\mathcal{P})$ minimale rispetto all'ordine lessicografico inverso $\prec_{i.l.}$. Dobbiamo provare che $C := \mathcal{C}(\mathcal{P}) = D := \mathcal{D}(\mathcal{P})$.

Ragioniamo per induzione sulla cardinalità $\#\mathcal{P} = \#C = \#D = codim \Im(\mathcal{P})$. L'enunciato è ovvio per $\#\mathcal{P} = 1$; proviamolo per $\#\mathcal{P} = N$ supposto che valga per $\#\mathcal{P} < N$.

Supponiamo per assurdo che l'assunto sia falso e indichiamo con $\mathbf{f} = (f_1, \ldots \ldots, f_s, 0, \ldots, 0)$ (con $1 \leq s \leq n$ e $f_s \neq 0$) il più piccolo (rispetto a $\prec_{i.l.}$) tra gli elementi di $D \cup C - D \cap C$. Allora o $\mathbf{f} \in C$, $\mathbf{f} \notin D$, oppure $\mathbf{f} \in D$, $\mathbf{f} \notin C$. Escludiamo, in primo luogo, la seconda di tali eventualità. La relazione $\mathbf{f} \notin C$ comporta che si abbia

$$\mathbf{x}^{\mathbf{f}} \equiv \sum_{\mathbf{d} \in C, \mathbf{d} \prec_{i.l.} \mathbf{f}} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} \qquad mod.\Im(\mathcal{P})$$

per opportuni coefficienti $\alpha_{\mathbf{d}} \in K$ non tutti nulli (la restrizione "$\mathbf{d} \prec_{i.l.} \mathbf{f}$" è da imputare alla minimalità di C rispetto a $\preceq_{i.l.}$); ma, per definizione di $\mathbf{f}$, ogni indice $\mathbf{d} \in C$ per cui $\mathbf{d} \prec_{i.l.} \mathbf{f}$ appartiene anche a D e quindi si ha

$$\mathbf{x}^{\mathbf{f}} \equiv \sum_{\mathbf{d} \in D, \mathbf{d} \prec_{i.l.} \mathbf{f}} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} \qquad mod.\Im(\mathcal{P})$$

in contraddizione con $\mathbf{f} \in D$.

Resta da analizzare il caso in cui $\mathbf{f} \in C$ e $\mathbf{f} \notin D$. Iniziamo col provare che non è restrittivo supporre che ogni elemento $\mathbf{d} = (d_1, \ldots, d_n) \in D$ sia tale che (a) $d_{s+1} = \ldots = d_n = 0$. Indichiamo infatti con $\underline{\hat{D}}$ il sottoinsieme di $\underline{D}$ formato con gli elementi soddisfacenti alla (a); per l'ipotesi fatta all'inizio di questa dimostrazione, $\hat{\underline{\mathcal{D}}}$ risulta essere un segmento iniziale dell'insieme ordinato $\underline{\mathcal{D}} = \{\mathbf{d}_1, \dots, \mathbf{d}_N\}$: $\hat{\underline{\mathcal{D}}} = \{\mathbf{d}_1, \dots, \mathbf{d}_t\}$. Posto $\hat{\underline{\mathcal{P}}} = \{P_1, \dots, P_t\}$, si ha $\hat{\underline{\mathcal{D}}} = \underline{\mathcal{D}}(\hat{\underline{\mathcal{P}}})$; ovviamente $\mathbf{f} \notin \hat{\mathcal{D}}$. Osserviamo che, per ogni punto $P \in \underline{\mathcal{P}} - \hat{\underline{\mathcal{P}}}$ esiste qualche punto in $\hat{\underline{\mathcal{P}}}$ che ha le stesse prime s coordinate di P. Ciò premesso, notiamo che la relazione $\mathbf{f} \in C$ comporta che ogni polinomio della forma

$$\mathbf{x}^{\mathbf{f}} - \sum_{\mathbf{d} \prec_{i.l.} \mathbf{f}} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}}$$

(e quindi nelle sole variabili $x_1, \dots, x_s$) <u>non</u> viene annullato da almeno uno dei punti in $\underline{\mathcal{P}}$ e quindi — per l'osservazione fatta più sopra — da almeno uno dei punti in $\hat{\underline{\mathcal{P}}}$. Ne consegue che $\mathbf{f} \in \hat{C} := C(\hat{\underline{\mathcal{P}}})$ e siamo così ricondotti — considerando $\hat{\underline{\mathcal{P}}}$ in luogo di $\underline{\mathcal{P}}$ — al caso in cui la (a) è soddisfatta. Supponiamo pertanto che siano nulle le ultime $n - s$ componenti di ogni elemento di D.

Ciò premesso, osserviamo che $\mathbf{f}$ è necessariamente un elemento diedrale esterno per D e, per la Prop. 6, esiste in $\Im(\mathcal{P})$ uno ed un solo polinomio della forma

$$\mathbf{x}^{\mathbf{f}} - \sum_{\mathbf{d} \in D} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} \qquad (\alpha_{\mathbf{d}} \in K) \tag{11}$$

che, per quanto appena visto, non è restrittivo supporre nelle sole variabili $x_1, \dots, x_s$. Va provato che in (11) si annullano i coefficienti $\alpha_{\mathbf{d}}$ tali che $\mathbf{d} \succ_{i.l.} \mathbf{f}$, ottenendo così

$$\mathbf{x}^{\mathbf{f}} \equiv \sum_{\mathbf{d} \in D,\, \mathbf{d} \prec_{i.l.} \mathbf{f}} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} \qquad (mod.\Im(\mathcal{P})) \tag{12}$$

che è in contraddizione con $\mathbf{f} \in C$ giacché nelle attuali ipotesi ogni elemento $\mathbf{d} \in D$, $\mathbf{d} \prec_{i.l.} \mathbf{f}$ appartiene anche a C.

Proviamo dapprima che il polinomio (11) è di grado f_s in x_s. Supposto per assurdo che sia di grado $d_s > f_s$ in x_s, scriviamolo nella forma

$$\mathbf{x}^{\mathbf{f}} - p(x_1, \dots, x_{s-1}) \cdot x_s^{d_s} - q(x_1, \dots, x_s)$$

con $q(x_1, \dots, x_s)$ di grado minore di d_s in x_s. Per provare che $p(x_1, \dots, x_{s-1})$ è identicamente nullo, consideriamo l'insieme $\check{\underline{\mathcal{D}}} \subseteq \underline{\mathcal{D}}$ formato da tutti gli elementi $\mathbf{d} \in \underline{\mathcal{D}}$ la cui s-esima componente è d_s e sia $\check{\underline{\mathcal{P}}} := \delta_{\underline{\mathcal{P}}}^{-1}(\check{\underline{\mathcal{D}}})$. Per ogni punto $P \in \check{\underline{\mathcal{P}}}$ esistono in $\underline{\mathcal{P}}$ altri d_s punti aventi le stesse prime $s - 1$ coordinate di P, per cui (in particolare) $p(x_1, \dots, x_{s-1})$ deve annullarsi nei punti di $\check{\underline{\mathcal{P}}}$ e quindi di $\check{\underline{\mathcal{Q}}} := \pi_{s-1}(\check{\underline{\mathcal{P}}})$; cioè, $p(x_1, \dots, x_{s-1}) \in \Im(\check{\underline{\mathcal{Q}}})$. D'altra parte, i termini $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_{s-1}^{i_{s-1}}$ in $p(x_1, \dots, x_{s-1})$ sono solo quelli per cui $\mathbf{i} \in \pi_{s-1}(\check{\underline{\mathcal{D}}}) = \underline{\mathcal{D}}(\check{\underline{\mathcal{Q}}})$, cioè costituiscono un sistema di rappresentanti per una base monomiale per $K[x_1, \dots, x_{s-1}]/\Im(\check{\underline{\mathcal{Q}}})$. Ne consegue che $p(x_1, \dots, x_{s-1})$ è identicamente nullo.

Resta così provato che il polinomio (nelle sole variabili $x_1, \dots, x_s$) (11) è di grado f_s in x_s. Scriviamolo ora nelle due forme seguenti

$$\mathbf{x}^{\mathbf{f}} - \sum_{\mathbf{d} \in D_1} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} - \sum_{\mathbf{d} \in D_2} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} - \sum_{\mathbf{d} \in D_3} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}} \tag{13}$$

dove

$$D_1 := \{\mathbf{d} \in D \mid \mathbf{d} \succ_{i.l.} \mathbf{f},\ d_s = f_s\}, \qquad D_2 := \{\mathbf{d} \in D \mid \mathbf{d} \prec_{i.l.} \mathbf{f},\ d_s = f_s\},$$

$$D_3 := \{\mathbf{d} \in D \mid d_s < f_s\},$$

e

$$p_{f_s}(x_1,\dots,x_{s-1})\cdot x_s^{f_s} + p_{f_s-1}(x_1,\dots,x_{s-1})\cdot x_s^{f_s-1} + \cdots + p_0(x_1,\dots,x_{s-1}). \quad (14)$$

Osservato che, in (13), tutti e soli i termini di grado f_s in x_s sono concentrati nei primi tre addendi, deve aversi

$$p_{f_s}(x_1,\dots,x_{s-1}) := x_1^{f_1}\cdots x_{s-1}^{f_{s-1}} - p_{(1)} - p_{(2)} \quad (15)$$

con

$$p_{(1)}\cdot x_s^{f_s} = \sum_{\mathbf{d}\in D_1} \alpha_{\mathbf{d}}\cdot \mathbf{x}^{\mathbf{d}} \quad e \quad p_{(2)}\cdot x_s^{f_s} = \sum_{\mathbf{d}\in D_2} \alpha_{\mathbf{d}}\cdot \mathbf{x}^{\mathbf{d}}. \quad (16)$$

Per provare il nostro assunto occorre dimostrare che il secondo addendo in (13) è identicamente nullo o, equivalentemente, che tale è $p_{(1)}$. A tal fine, poniamo $\tilde{\mathcal{P}} := \underline{\delta_{\mathcal{P}}}^{-1}(D_1 \cup D_2)$. Il polinomio (14) deve annullarsi su tutti i punti di $\tilde{\mathcal{P}} \subseteq \mathcal{P}$; osservato che per ogni punto in $\tilde{\mathcal{P}}$ se ne trovano in $\mathcal{P}$ altri f_s aventi le stesse prime $s-1$ coordinate di quello, il fatto che il polinomio (14) è di grado f_s in x_s comporta che i polinomi $p_{f_s}(x_1,\dots,x_{s-1}),\dots,p_0(x_1,\dots,x_{s-1})$ devono annullarsi nei punti di $\tilde{\mathcal{P}}$, e quindi anche nei punti dell'insieme $\tilde{\mathcal{Q}} := \pi_{s-1}(\tilde{\mathcal{P}}) \subseteq K^{s-1}$. In particolare, il polinomio (15) deve appartenere all'ideale $\Im(\tilde{\mathcal{Q}})$ di $K[x_1,\dots,x_{s-1}]$:

$$p_{f_s}(x_1,\dots,x_{s-1}) := x_1^{f_1}\cdots x_{s-1}^{f_{s-1}} - p_{(1)} - p_{(2)} \equiv 0 \quad (mod.\Im(\tilde{\mathcal{Q}})). \quad (17)$$

Poiché $\#\tilde{\mathcal{Q}} < \#\mathcal{P}$, per l'ipotesi induttiva la proposizione vale per l'insieme $\tilde{\mathcal{Q}} \subseteq K^{s-1}$; pertanto, osservato che $\tilde{\mathbf{f}} := (f_1,\dots,f_{s-1}) = \pi_{s-1}(\mathbf{f})$ è un elemento diedrale esterno per $\mathcal{D}(\tilde{\mathcal{Q}}) = \pi_{s-1}(D_1 \cup D_2)$, deve aversi

$$x_1^{f_1}\cdots x_{s-1}^{f_{s-1}} \equiv \sum_{\tilde{\mathbf{d}}:=(d_1,\dots,d_{s-1})\in\mathcal{D}(\tilde{\mathcal{Q}}),\tilde{\mathbf{d}}\prec_{i.l.}\tilde{\mathbf{f}}} \beta_{\tilde{\mathbf{d}}}\cdot x_1^{d_1}\cdots x_{s-1}^{d_{s-1}} \quad (mod.\Im(\tilde{\mathcal{Q}})).$$

dove i coefficienti $\beta_{\tilde{\mathbf{d}}}$ sono *univocamente* determinati. Dal confronto di quest'ultima con (16) e (17) si deduce facilmente che $p_{(1)}$ è identicamente nullo, che è quanto restava da provare. □

5 Algoritmi derivati.

5.1 In questo paragrafo illustriamo una proprietà (Prop. 8) che — in molti casi — costituisce una sensibile semplificazione dell'Algoritmo D.

Posto infatti $\mathcal{P} \subseteq K^n$ e $\mathcal{Q} := \pi_{n-1}(\mathcal{P}) \subseteq K^{n-1}$, tale proprietà riconduce il calcolo del diagramma di Ferrers (non ordinato) $\mathcal{D}(\mathcal{P})$ a quello del diagramma di Ferrers (ordinato!) $\underline{\mathcal{D}}(\underline{\mathcal{Q}})$, avendo preventivamente ordinato $\underline{\mathcal{Q}} := \underline{\{Q_1, \ldots, Q_m\}}$ in modo tale che, posto $h_i := \# \overset{-1}{\pi}_{n-1}(Q_i)$ (cioè, h_i è il numero dei punti in $\mathcal{P}$ aventi le prime $n-1$ coordinate uguali a quelle di Q_i), si abbia $i < j \to h_i \geq h_j$.

Va subito notato che — proprio a causa del ruolo che gioca in questo contesto l'ordine considerato in $\underline{\mathcal{D}}(\underline{\mathcal{Q}})$ — non ha senso iterare l'uso di questa proprietà. Tuttavia nel caso bidimensionale essa fornisce anche una versione alternativa dell' Algoritmo D (Prop. 9).

Proposizione 8 *Con riferimento alle notazioni introdotte più sopra e posto inoltre*

$$\underline{\mathcal{D}}(\underline{\mathcal{Q}}) := \underline{\{\tilde{\mathbf{d}}_1, \ldots, \tilde{\mathbf{d}}_m\}} \subseteq \mathbf{N}^{n-1}$$

e

$$\tilde{\mathbf{d}}_i = (\tilde{d}_{i,1}, \ldots, \tilde{d}_{i,n-1}) = \underline{\delta}_{\mathcal{Q}}(Q_i) \qquad (1 \leq i \leq m)$$

si ha

$$\mathcal{D}(\mathcal{P}) = \{(\tilde{d}_{i,1}, \ldots, \tilde{d}_{i,n-1}, e_i) | 1 \leq i \leq m \text{ e } 0 \leq e_i < h_i\}.$$

Dimostrazione La dimostrazione si riduce ad applicare l'Alg.D dopo aver dotato $\mathcal{P}$ di un ordine opportuno.

Operiamo una partizione di $\mathcal{P}$ distribuendone gli elementi in una famiglia ordinata di h_1 blocchi $B_0, B_1, \ldots, B_{h_1-1}$ nel modo seguente: scelti successivamente a caso gli elementi di $\mathcal{P}$, l'elemento P via via considerato verrà messo nel primo dei blocchi che non contiene alcun elemento P' tale che $\pi_{n-1}(P) = \pi_{n-1}(P')$. È chiaro che un elemento Q_i apparterrà a $\pi_{n-1}(B_s)$ se e solo se $s < h_i$, per cui si ha

$$\pi_{n-1}(B_0) = \pi_{n-1}(\mathcal{P}) = \{Q_1, \ldots, Q_m\}$$

e

$$\pi_{n-1}(B_0) \supseteq \pi_{n-1}(B_1) \supseteq \ldots \supseteq \pi_{n-1}(B_h) \qquad \text{con} \qquad h := h_1 - 1.$$

Ordiniamo ciascuno degli insiemi $\pi_{n-1}(B_s) \subseteq \mathcal{Q}$ secondo l'ordine indotto da $\underline{\mathcal{Q}}$; ciò determina un ordine anche in ciascuno dei blocchi B_s:

$$\underline{B}_s = \underline{\{P_1^s, \ldots, P_{m_s}^s\}} \qquad \text{con} \qquad \pi_{n-1}(P_t^s) = Q_t.$$

Infine introduciamo un ordine $\underline{\mathcal{P}}$ in $\mathcal{P}$ semplicemente incollando ordinatamente i diversi blocchi ordinati $\underline{B}_0, \underline{B}_1, \ldots, \underline{B}_h$: dati due punti $P, P' \in \underline{\mathcal{P}}$, P precederà P' se, posto $P = P_{r_i}^i$ e $P' = P_{r_j}^j$ si ha o $i < j$ oppure $i = j$ e $r_i < r_j$.

È sufficiente ora applicare a $\underline{P}$ ordinato in questo modo l'operatore $\underline{D}$ per ottenere il risultato enunciato. □

Come diretta conseguenza della proposizione precedente si ottiene la:

Proposizione 9 *Sia $\mathcal{P} \subseteq K^2$. Se i punti in $\mathcal{P}$ hanno, complessivamente, m ascisse diverse $\rho_1, \ldots, \rho_m$ e ve ne sono h_i di ascissa ρ_i:*

$$\mathcal{P} := \{(\rho_1, \sigma_{1,1}), \ldots (\rho_1, \sigma_{1,h_1}), \ldots, (\rho_m, \sigma_{m,1}), \ldots, (\rho_m, \sigma_{m,h_m})\},$$

allora — assumendo che $h_1 \geq \ldots \geq h_m$ — il diagramma di Ferrers $M_{\mathcal{P}}$ dei monomi associati a $\mathcal{D}(\mathcal{P})$ è quello rappresentato nella tavola

$$\begin{array}{ccccc}
1 & x & \ldots & x^{m-2} & x^{m-1} \\
y & xy & \ldots & x^{m-2}y & x^{m-1}y \\
\vdots & \vdots & \ldots & \vdots & \vdots \\
y^{h_m-1} & xy^{h_m-1} & \ldots & x^{m-2}y^{h_m-1} & x^{m-1}y^{h_m-1} \\
y^{h_m} & xy^{h_m} & \ldots & x^{m-2}y^{h_m} & \\
\vdots & \vdots & \ldots & \vdots & \\
 & & & & \\
\vdots & \vdots & & & \\
y^{h_2-1} & xy^{h_2-1} & & & \\
y^{h_2} & & & & \\
\vdots & & & & \\
y^{h_1-1} & & & &
\end{array}$$

□

6 Generalizzazione al caso dei punti multipli.

6.1 Corretta impostazione del Problema 2.

Nel corso del presente paragrafo generalizzeremo — seguendone la falsariga — quanto esposto nei paragrafi precedenti, al fine di precisare prima e poi di risolvere il Problema 2.

Iniziamo con l'introdurre alcune nozioni — in particolare quelle di *diagramma algebrico* e di *multiinsieme algebrico* — che svolgeranno un ruolo centrale in quanto segue.

Consideriamo l'applicazione lineare

$$\begin{array}{rccc}
\mathbf{D_i} : & K[X] & \longrightarrow & K[X] \\
 & \mathrm{x^h} & \longmapsto & \binom{\mathrm{h}}{\mathrm{i}}\mathrm{x^{h-i}}
\end{array}$$

e la sua composizione $v_P^{\mathbf{i}} = v_P \circ \mathbf{D}_{\mathbf{i}}$ con l'operatore di valutazione v_P:

$$\begin{array}{rcl} v_P^{\mathbf{i}} : K[X] & \longrightarrow & K \\ q & \longmapsto & (\mathbf{D}_{\mathbf{i}} q)(P). \end{array}$$

Osserviamo che se K è un campo di caratteristica zero allora

$$\mathbf{D}_{\mathbf{i}} = \frac{1}{\mathbf{i}!}\mathbf{D}^{\mathbf{i}} = \frac{1}{\mathbf{i}!}\frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1}\cdots\partial x_n^{i_n}}$$

dove $\mathbf{i} = (i_1, \ldots, i_n)$ e $\mathbf{i}! = i_1! \cdots i_n!$.

Sia J un ideale di $K[x_1, \ldots, x_n]$ e sia $P \in \mathcal{V}(J)$. Consideriamo l'insieme

$$\mathcal{F}(P) := \left\{ \mathbf{i} \in \mathbf{N}^n \middle| \, (\forall p \in J) \left(v_P^{\mathbf{i}}(p) = 0 \right) \right\}$$

Utilizziamo la nota formula:

$$\mathbf{D}_{\mathbf{i}}(f \cdot g) = \sum_{\mathbf{h}+\mathbf{k}=\mathbf{i}} \mathbf{D}_{\mathbf{h}}(f) \cdot \mathbf{D}_{\mathbf{k}}(g) \tag{18}$$

per dimostrare la seguente

Proposizione 10 *a) $\mathcal{F}(P)$ è un diagramma di Ferrers; b) se $(g_1, \ldots, g_s)$ è un sistema di generatori per J allora $\mathcal{F}(P)$ è il più grande diagramma di Ferrers contenuto nell'insieme*

$$\left\{ \mathbf{i} \in \mathbf{N}^n \middle| \, v_P^{\mathbf{i}}(g_j) = 0 \textit{ per ogni } 1 \leq j \leq s \right\}$$

Dimostrazione.

a) Sia $\mathbf{i} \in \mathcal{F}(P)$; per la prima parte del Lemma 5 è sufficiente dimostrare che $\mathbf{i}' := (i_1, \ldots, i_j - 1, \ldots, i_n)$ appartiene a $\mathcal{F}(P)$. Supponiamo per assurdo che $\mathbf{i}' \notin \mathcal{F}(P)$; allora per qualche polinomio $q \in J$ deve aversi

$$v_P^{\mathbf{i}'}(q) \neq 0. \tag{19}$$

Consideriamo il polinomio $x_j \cdot q \in J$; poiché $\mathbf{i} \in \mathcal{F}(P)$ si ha:

$$\begin{aligned} 0 &= v_P^{\mathbf{i}}(x_j \cdot q) = (\mathbf{D}_{\mathbf{i}}(x_j \cdot q))(P) = \left(\sum_{\mathbf{h}+\mathbf{k}=\mathbf{i}} \mathbf{D}_{\mathbf{h}} x_j \cdot \mathbf{D}_{\mathbf{k}} q \right)(P) = \\ &= (x_j \mathbf{D}_{\mathbf{i}} q + \mathbf{D}_{\mathbf{i}'} q)(P) = (\mathbf{D}_{\mathbf{i}'} q)(P) \end{aligned}$$

in contrasto con la (19).

b) La seconda parte dell'enunciato è una diretta conseguenza della prima parte e della (18).

□

Il diagramma di Ferrers $\mathcal{F}(P)$ verrà detto il *diagramma algebrico* di P in $\mathcal{V}(J)$ (o relativamente all'ideale J).

Un insieme finito $\wp := \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$ di coppie $(P_j, \mathcal{F}_j)$, costituite da un punto P_j di K^n (con $i \neq j \Rightarrow P_i \neq P_j$) e da un diagramma di Ferrers $\mathcal{F}_j$ di $\mathbf{N}^n$, verrà detto essere un *multiinsieme algebrico n-dimensionale* sul campo K. Gli elementi P_j verranno detti *punti* del multiinsieme algebrico $\wp$ — e scriveremo $P_j \in \wp$ — e il diagramma di Ferrers $\mathcal{F}_j$ si dirà il *diagramma algebrico* di P_j nel multiinsieme algebrico $\wp$. Diremo inoltre che P_j è *semplice* se $\mathcal{F}_j = \{(0, \ldots, 0)\}$. Talvolta, nel seguito, identificheremo tacitamente il multiinsieme algebrico $\wp$ con il sottoinsieme di $K^n \times \mathbf{N}^n$ costituito da tutte le coppie della forma $(P, \mathbf{i})$ con $P \in \wp$ e $\mathbf{i}$ elemento del diagramma algebrico $\mathcal{F}$ di P. In accordo con ciò, useremo anche la notazione $(P, \mathbf{i}) \in \wp$ per denotare tale situazione e chiameremo *cardinalità* $\#\wp$ del multinsieme algebrico $\wp$ l'intero $\#\wp := \sum_{j=1}^{N} \#\mathcal{F}_j$. Inoltre, dati due multiinsiemi algebrici $\wp$ e $\wp'$, la relazione $(P, \mathbf{i}) \in \wp \Rightarrow (P, \mathbf{i}) \in \wp'$ verrà espressa con la notazione $\wp \subseteq \wp'$. Diremo che $\wp := \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$ è il *multiinsieme algebrico dell'ideale cofinito* J — e scriveremo $\wp = \wp(J)$ — se $V(J) = \{P_1, \ldots, P_N\}$ e se $\mathcal{F}_j$ è il diagramma algebrico di P_j relativamente all'ideale J.

Consideriamo ora l'insieme

$$\Im(\wp) := \left\{ p \in K[X] \mid (\forall j)(\forall \mathbf{i} \in \mathcal{F}_j) \left(v^{\mathbf{i}}_{P_j}(p) = 0 \right) \right\}.$$

Sfruttando ancora una volta la (18) e il fatto che $\mathcal{F}_j$ è un diagramma di Ferrers si prova che $\Im(\wp)$ è un ideale di $K[x_1, \ldots, x_n]$, che diremo essere l'*ideale del multiinsieme algebrico* $\wp$. Ovviamente il diagramma algebrico $\mathcal{F}_j$ di P_j in $\wp$ coincide con il diagramma algebrico di P_j relativamente all'ideale $\Im(\wp)$. Si può dimostrare (cfr. [2]) che si ha

$$\mathit{codim}\ \Im(\wp) = \#\wp.$$

Siamo ora in grado di precisare il:

Problema 2. Dato un multiinsieme algebrico $\wp := \{(P_1, \mathcal{F}_1), \ldots, (P_N, \mathcal{F}_N)\}$ si vuole determinare un polinomio $p \in K[x_1, \ldots, x_n]$ tale che, per ogni $1 \leq j \leq n$ ed ogni $\mathbf{i} \in \mathcal{F}_j$, si abbia

$$v^{\mathbf{i}}_{P_j}(p) = \alpha_{\mathbf{i};j}$$

dove le $\alpha_{\mathbf{i};j}$ sono dei valori assegnati in K.

Facendo considerazioni analoghe a quelle del paragrafo 1, si vede che — così riformulato — il Problema 2 ammette una soluzione — determinata univocamente modulo $\Im(\wp)$ — e quindi che, per ogni base monomiale $\{\mathbf{x}^{\mathbf{i}_j} \mid 1 \leq j \leq \#\wp\}$ di $K[X]/\Im(\wp)$, esiste uno ed un solo polinomio $p = \sum p_j \mathbf{x}^{\mathbf{i}_j}$ soddisfacente alle condizioni richieste.

6.2 Soluzione del Problema 2. Vediamo ora — generalizzando al caso attuale quanto, nei paragrafi **2** e **3**, si è già fatto per gli insiemi algebrici — come possa essere determinata una base monomiale minimale $\{\mathbf{x}^{\mathbf{i}_j} \mid 1 \leq j \leq \#\wp\}$ di $K[X]/\Im(\wp)$ e quindi un polinomio $p = \sum p_j \mathbf{x}^{\mathbf{i}_j}$.

Associamo dapprima al multiinsieme algebrico $\wp$ un ideale elementare $\Gamma = (\gamma_1(x_1), \ldots, \gamma_n(x_n))$ di generatori

$$\gamma_i(x_i) := \prod_{j=1}^{t_i} (x_i - \rho_{i,j})^{h_{i,j}}$$

dove si è indicato con $\{\rho_{i,1}, \ldots, \rho_{i,t_i}\}$ l'insieme delle i–esime coordinate dei punti di $\wp$ e le molteplicità $h_{i,j}$ sono state determinate nel modo seguente. Indichiamo con $P_{s_1}, \ldots, P_{s_m}$ i punti di $\wp$ aventi $\rho_{i,j}$ come i-esima coordinata e, per ogni $r \in \{1, \ldots, m\}$, sia $\mathbf{f}_{s_r} = (f_{s_r,1}, \ldots, f_{s_r,n})$ l'estremo superiore del diagramma algebrico $\mathcal{F}_{s_r} \subseteq \mathbf{N}^n$ di P_{s_r}; allora $h_{i,j}$ è definito come il $\sup\{f_{s_r,i} | 1 \leq r \leq m\}$. Poniamo inoltre $h_i := \sum_{j=1}^{t_i} h_{i,j} = deg(\gamma_i)$, $h := h_1 \cdots h_n$ e $\mathbf{h} := (h_1 - 1, \ldots, h_n - 1)$. È immediato verificare che l'insieme

$$H := \{\mathbf{x}^{\mathbf{s}} \mid \mathbf{s} \leq \mathbf{h}\}$$

costituisce un sistema di rappresentanti per una base monomiale (minimale rispetto ad un qualunque ordine lineare compatibile $\preceq$) per $K[X]/\Gamma$.

All'ideale elementare Γ così definito associamo un multiinsieme algebrico $\wp_\Gamma$ nel nodo seguente: la coppia $(P, \mathcal{F})$ è un elemento di $\wp_\Gamma$ sse, posto $P = (\sigma_1, \ldots, \sigma_n)$, si ha $\gamma_i(\sigma_i) = 0$ ed inoltre, indicata con s_i la molteplicità di σ_i in γ_i, si ha

$$\mathcal{F} = \{\mathbf{i} \in \mathbf{N}^n \mid \mathbf{i} \leq (s_1 - 1, \ldots s_n - 1)\}.$$

È facile verificare (cfr. [2]) che si ha: $\wp \subseteq \wp_\Gamma$, $\wp_\Gamma = \wp(\Gamma)$ e $\#\wp_\Gamma = codim(\Gamma)$.

Generalizzando quanto contenuto in **2.2**, dato un insieme ordinato di monomi

$$T_\prec := (t_0, t_1, \ldots, t_s, \ldots),$$

ed una coppia $(P, \mathbf{i})$, $P \in K^n$ e $\mathbf{i} \in \mathbf{N}^n$, poniamo

$$T_\prec(P, \mathbf{i}) := (v_P^{\mathbf{i}}(t_0), \ldots, v_P^{\mathbf{i}}(t_s), \ldots).$$

Fissato un arbitrario multiinsieme algebrico $\Re$ ed avendone ordinato linearmente gli elementi $(P, \mathbf{i})$, sia $T_\prec(\Re)$ la matrice di tipo $\#\Re \times \#T_\prec$ la cui $(P, \mathbf{i})$-esima riga è $T_\prec(P, \mathbf{i})$.

Considerato di nuovo il multiinsieme algebrico $\wp$ e quello $\wp_\Gamma$ associato a Γ, assumiamo di aver ordinato gli elementi $(P, \mathbf{i})$ di $\wp_\Gamma$ in modo tale che quelli appartenenti anche a $\wp$ precedano gli altri e consideriamo le matrici $\tilde{H} := H_\prec(\wp_\Gamma)$ e $H_\prec(\wp)$ (la seconda essendo formata con le prime $\#\wp$ righe della prima). Ancora si può dimostrare che $\tilde{H}$ è non degenere (esattamente come per la Prop. 1, non appena si riconosca che $\tilde{H}$ è il prodotto tensoriale di n matrici di Vandermonde *generalizzate*, ciascuna associata alle radici di uno dei generatori $\gamma_i(x_i)$ di Γ) e si può, in ultima analisi, ripetere quanto ottenuto, nei paragrafi **2** e **3**, per gli insiemi algebrici $\{P_1, \ldots, P_n\}$.

Nel paragrafo seguente, infine, mostreremo come generalizzare al caso dei multiinsiemi algebrici l'operatore $\mathcal{D}$, ottenendo tramite esso una base monomiale minimale per l'algebra quoziente $K[X]/\Im(\wp)$.

6.3 Diagramma di Ferrers associato ad un multiinsieme algebrico.

Consideriamo la bigezione (*"rappresentazione umbrale"*)

$$\begin{array}{rcl} u: K^n \times \mathbf{N}^n & \longrightarrow & (K \times \mathbf{N})^n \\ ((a_1, \ldots, a_n), (i_1, \ldots, i_n)) & \longmapsto & ((a_1, i_1), \ldots, (a_n, i_n)); \end{array}$$

chiameremo *"valutazione umbrale"* l'applicazione inversa $U := u^{-1}$.

Dato il multiinsieme algebrico $\wp := \{(P_1, F_1), \ldots, (P_N, F_N)\}$ ad ogni coppia $(P, \mathbf{i}) \in \wp$ associamo la sua rappresentazione umbrale $u(P, \mathbf{i})$ e chiamiamo *rappresentazione umbrale* $\mathcal{R}(\wp)$ *di* $\wp$ l'insieme

$$\mathcal{R} = \mathcal{R}(\wp) := \{u(P, \mathbf{i}) \mid (P, \mathbf{i}) \in \wp\}.$$

Estendiamo l'operatore $\mathcal{D}$ ai multiinsiemi algebrici definendo il diagramma di Ferrers $\mathcal{D}(\wp)$ come il diagramma di Ferrers associato all'insieme $\mathcal{R}$ dall'Algoritmo D:

$$\mathcal{D}(\wp) := \mathcal{D}(\mathcal{R}).$$

Vale la seguente

Proposizione 11 *L'insieme* $B := \{[\mathbf{x}^{\mathbf{i}}]_{\Im(\wp)} \mid \mathbf{i} \in \mathcal{D}(\wp)\}$ *costituisce una base lineare monomiale (minimale) per l'algebra quoziente* $K[X]/\Im(\wp)$.

Prima di dimostrare la Prop. 11 conviene provare il seguente Lemma 6. Poniamo:

$$D := \mathcal{D}(\mathcal{R}) = \mathcal{D}(\wp)$$

$$h := max\{d_n \mid (d_1, \ldots, d_n) \in D\},$$

e, per ogni $r \in \{0, \ldots, h\}$,

$$D_r := \{\mathbf{d} = (d_1, \ldots, d_n) \in D \mid d_n = r\}$$

$$\mathcal{R}_r := \{R \in \mathcal{R} \mid \underline{\delta_{\mathcal{R}}}(R) \in D_r\}$$

$$\wp_r := U(\pi_{n-1}(\mathcal{R}_r)).$$

Osserviamo che, pur dipendendo $\mathcal{R}_r$ e, quindi, $\wp_r$ dall'ordine considerato nell'insieme $\mathcal{R}$, tale dipendenza non gioca alcun ruolo in quanto segue e verrà pertanto sottaciuta.

Lemma 6 *Per ogni* $r \in \{0, \ldots, h\}$, $\wp_r$ *è un multiinsieme algebrico* $(n-1)$*-dimensionale e si ha*

$$r > r' \Rightarrow \wp_r \subseteq \wp_{r'}; \tag{20}$$

$$\mathcal{D}(\wp_r) = \pi_{n-1}(D_r). \tag{21}$$

Dimostrazione. La (20) e la (21) sono conseguenza diretta delle (8) e (9), rispettivamente, del Lemma 3 non appena si osservi (per quanto riguarda la (20)) che $\mathcal{R} \subseteq \mathcal{S} \Rightarrow U(\mathcal{R}) \subseteq U(\mathcal{S})$ e, (per quanto riguarda la (21)), che l'operatore $\mathcal{D}$ che agisce sui multiinsiemi è in effetti la composizione dell'operatore di rappresentazione umbrale u con l'operatore $\mathcal{D}$ che agisce sugli insiemi:

$$\pi_{n-1}(D_r) = \mathcal{D}(\pi_{n-1}(\mathcal{R}_r)) = \mathcal{D}(u(\wp_r)) = \mathcal{D}(\wp_r).$$

□

Dimostrazione della Prop. 11. Ovviamente si ha $\#B = \#\wp$; poiché *codim* $\Im(\wp) = \#\wp$, è quindi sufficiente provare che nessuna combinazione lineare (non banale) dei monomi in B sia un elemento dell'ideale $\Im(\wp)$. Seguendo la falsariga della dimostrazione della Prop. 6, dimostriamo — ragionando per induzione sulla dimensione n — che se un polinomio $p(x_1, \ldots, x_n)$ della forma

$$p(x_1, \ldots, x_n) = \sum_{\mathbf{d} \in \mathcal{D}(\wp)} \alpha_{\mathbf{d}} \cdot \mathbf{x}^{\mathbf{d}},$$

appartiene a $\Im(\wp)$ allora è identicamente nullo. Si ha

$$p(x_1, \ldots, x_n) = \sum_{r=0}^{h} p_r(x_1, \ldots, x_{n-1}) \cdot x_n^r$$

con

$$p_r(x_1, \ldots, x_{n-1}) := \sum_{(d_1, \ldots, d_{n-1}) \in \pi_{n-1}(D_r)} \alpha_{(d_1, \ldots, d_{n-1}, r)} \cdot x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}.$$

Posto

$$D_h = \{\mathbf{d}^{(1)}, \ldots, \mathbf{d}^{(s)}\}$$

(con $\mathbf{d}^{(j)} = (d_1^{(j)}, \ldots, d_{n-1}^{(j)}, h)$, $j = 1, \ldots, s$), si ha

$$\mathcal{R}_h = \{R^{(j)} \mid \underline{\delta_{\mathcal{R}}}(R^{(j)}) = \mathbf{d}^{(j)};\ j = 1, \ldots, s\}.$$

Per ogni $R^{(j)} \in \mathcal{R}_h$ vi sono esattamente $h+1$ punti $R \in \mathcal{R}$ tale che $\pi_{n-1}(R^{(j)}) = \pi_{n-1}(R)$. Indicato con $\mathcal{T}_h^{(j)}$ il complesso di tali $h+1$ punti, poniamo $\mathcal{T}_h := \cup_{j=1}^{s} \mathcal{T}_h^{(j)}$. Non è difficile riconoscere che $\pi_{n-1}(\mathcal{T}_h) = \pi_{n-1}(\mathcal{R}_h)$ e quindi che $U(\pi_{n-1}(\mathcal{T}_h)) = \wp_h$. Vi è inoltre una ovvia corrispondenza biunivoca

$$\tau : \wp_h \to \{\mathcal{T}_h^{(j)} \mid j = 1, \ldots s\}.$$

Sia $(Q,\mathbf{j}) \in \wp_h$, $Q \in K^{n-1}$ e $\mathbf{j} \in \mathbf{N}^{n-1}$, e sia $\tau(Q,\mathbf{j}) = \mathcal{T}_h^{(l)}$ per un opportuno intero $l \in \{1,\ldots,s\}$. Posto $Q = (c_1,\ldots,c_{n-1})$ e $\mathbf{j} = (j_1,\ldots,j_{n-1})$, valutiamo umbralmente i punti in $\tau(Q,\mathbf{j}) = \mathcal{T}_h^{(l)} \subseteq \mathcal{R}$. [Questi punti sono della forma $((c_1,j_1),\ldots,(c_{n-1},j_{n-1}),(c,j))$; due di essi differiscono quindi solo nell'ultima componente (c,j)]. Risulta che un certo numero — diciamolo $q_1 \geq 1$ — di questi si trasformano in un punto $Q_1 = (c_1,\ldots,c_{n-1},c_{(1)})$, un altro gruppo — diciamo $q_2 \geq 1$ di essi — nel punto $Q_2 = (c_1,\ldots,c_{n-1},c_{(2)})$, etc., con $q_1+q_2+\cdots = h+1$ e tali inoltre che al diagramma algebrico $\mathcal{F}_r$ associato — in $\wp$ — a Q_r appartengano le q_r n-uple $(j_1,\ldots,j_{n-1},0),\ldots,(j_1,\ldots,j_{n-1},q_r-1)$. Ne consegue che ogni polinomio $f(x_1,\ldots,x_n)$ appartenente a $\Im(\wp)$ dovrà essere tale che per ogni $(Q,\mathbf{j}) \in \wp_h$, $Q = (c_1,\ldots,c_{n-1})$, $\mathbf{j} = (j_1,\ldots,j_{n-1})$, il polinomio $\tilde{f}(x_n) := \vartheta_Q^{\mathbf{j}}(f(x_1,\ldots,x_n))$ dovrà ammettere le radici $c_{(1)},c_{(2)},\ldots$ con le molteplicità $q_1, q_2, \ldots$ rispettivamente e quindi dovrà avere almeno grado $q_1+q_2+\cdots = h+1$. Ne consegue che il polinomio $p(x_1,\ldots,x_n) = \sum_{r=0}^{h} p_r(x_1,\ldots,x_{n-1})\cdot x_n^r \in \Im(\wp)$ considerato — essendo di grado al più h in x_n — dovrà essere tale che i polinomi

$$p_0(x_1,\ldots,x_{n-1}),\ldots,p_h(x_1,\ldots,x_{n-1})$$

appartengono all'ideale $\Im(\wp_h) \subseteq K[x_1,\ldots,x_{n-1}]$. Poiché p_h è della forma

$$p_h(x_1,\ldots,x_{n-1}) = \sum_{(d_1,\ldots,d_{n-1})\in\pi_{n-1}(D_h)} \alpha_{(d_1,\ldots,d_{n-1},h)}\cdot x_1^{d_1}\cdots x_{n-1}^{d_{n-1}}.$$

e poiché, per la (21), $\mathcal{D}(\wp_h) = \pi_{n-1}(D_h)$, dall'ipotesi induttiva si trae che $p_h(x_1,\ldots,x_{n-1})$ deve essere identicamente nullo.

Iterando per $r = h-1, h-2,\ldots,1,0$ il ragionamento fatto per $r = h$, si perviene a concludere che $p(x_1,\ldots,x_n)$ è identicamente nullo e quindi che $\{[\mathbf{x}^{\mathbf{i}}]_{\Im(\wp)} \mid \mathbf{i} \in \mathcal{D}(\wp)\}$ costituisce una base lineare monomiale per $K[X]/\Im(\wp)$. □

References

[1] B. Buchberger, *An Algorithmic Method in Polynomial Ideal Theory*, in "N. K. Bose (ed): Recent Trends in Multidimensional System Theory", D. Reidel Publishing Co. , 1985, pp. 184-232

[2] L. Cerlienco, F. Piras *On the Continuous Dual of a Polynomial Bialgebra.* (preprint)

[3] J.P.S. Kung *Jacobi's identity and the König-Egerváry theorem*, Discrete Math. 49(1984) 75-77

[4] L. Robbiano *Introduzione all'algebra computazionale.* Appunti per il corso INDAM. (Roma 1986/87)

[5] H.M. Möller, B. Buchberger *The construction of multivariate polynomials with preassigned zeros*, in "Computer Algebra (Marseille, 1982)", Lecture Notes in Comp. Sci., 144, Springer, Berlin-New York, 1982, pp.24-31

Indirizzo degli autori:
Luigi Cerlienco, Marina Mureddu
Dipartimento di Matematica.
Via Ospedale 72 — I-09124 Cagliari
Tel. 070-2000456/7
Fax 070-2000467

Appendice 1 – All'analisi condotta del problema dell'interpolazione in più variabili occorre aggiungere qualche ulteriore considerazione rivolta a mettere in evidenza alcune limitazioni intrinseche — cui già si è fatto cenno nell'introduzione — che non si presentano nel caso unidimensionale. Va chiarito che mentre in quest'ultimo caso la soluzione al problema ha un significato *geometrico* intrinseco, di contro nel caso $n \geq 2$ questa caratteristica viene a mancare. Infatti, se $n = 1$, la soluzione $y = p(x)$ privilegiata (soddisfacente cioè alla condizione $deg(p) < N$) dei Problemi 1 e/o 2 rappresenta nel piano (xy) una curva C che è invariante per cambiamenti di riferimento affine sull'asse x; nel caso n–dimensionale, invece, non solo vengono privilegiate più soluzioni $y = p_1(x_1, \ldots, x_n)$, ..., $y = p_r(x_1, \ldots, x_n)$ — dipendenti dalle diverse possibili scelte della base monomiale minimale — cui corrispondono diverse superfici $\Sigma_1, \ldots, \Sigma_r$ dello spazio affine $(x_1, \ldots, x_n, y)$, ma risulta anche che il complesso di tali superfici *non è invariante rispetto al gruppo delle trasformazioni affini dello spazio* $(x_1, \ldots, x_n)$. Detto in altri termini: mentre a) nel caso unidimensionale il problema: "trovare una funzione polinomiale che in certi punti P_i della retta affine assuma valori assegnati α_i" equivale (insieme con la sua soluzione) al problema: "trovare un polinomio (di dato grado) che per certi ρ_i [coordinate di P_i rispetto ad un arbitrario sistema di riferimento affine sulla retta] assuma valori assegnati α_i"; di contro b) non si può affermare qualcosa di simile nel caso multidimensionale.

Chiariamo meglio, e giustifichiamo, le affermazioni precedenti. Nel caso unidimensionale la situazione è la seguente: dati sulla retta N punti P_i, sia $\mathcal{S}$ la famiglia di funzioni polinomiali che assumono in P_i il valore α_i. Fissato sulla retta un sistema di riferimento affine R, rispetto al quale chiameremo x la coordinata del generico punto P, resta determinato l'ideale $\Im(\mathcal{P}) \subseteq K[x]$ dell'insieme $\mathcal{P} = \{P_1, \ldots, P_N\}$ e $\mathcal{S}$ è rappresentata da un laterale S di $\Im(\mathcal{P})$; questo laterale a sua volta viene rappresentato dall'unico polinomio p di grado minore di N contenuto in esso. Adottando poi un nuovo sistema di riferimento R' e chiamando x', $\Im'(\mathcal{P}) \subseteq K[x']$, S', p' gli analoghi dei precedenti, la trasformazione di coordinate affini $x' = \alpha \cdot x + \beta$ non solo trasforma $\Im'(\mathcal{P}) \subseteq K[x']$ in $\Im(\mathcal{P}) \subseteq K[x]$ e S' in S ma anche p' in p. Se ripetiamo ora, per il caso n–dimensionale, queste considerazioni — con l'unica differenza che ora i laterali S ed S' vengono rappresentati, al variare della base monomiale minimale scelta, da uno degli elementi di tutta una famiglia, $p_1, \ldots, p_r$ e $p'_1, \ldots, p'_{r'}$, rispettivamente, contenuta in essi — succede che una generica trasformazione affine $x' = \sum \alpha_{ij} x_j + \beta_i$, $(i, j = 1, \ldots, n)$ fa corrispondere $\Im'(\mathcal{P})$ a $\Im(\mathcal{P})$ e S' a S ma non trasforma il generico p_i in uno dei p'_j bensì, in generale, in un diverso rappresentante di S'. La ragione di ciò sta in quanto segue: il fatto che basi monomiali minimali calcolate rispetto a R non corrispondono a basi monomiali minimali calcolate rispetto a R' ha — nel caso $n > 1$ — effetti perversi che non si presentano invece nel caso unidimensionale. Tali effetti sono da imputare al fatto che un monomio $x_1^{i_1} \cdots x_n^{i_n}$ viene trasformato dall'affinità considerata in una combinazione lineare di (tutti) i monomi $x'^{j_1}_1 \cdots x'^{j_n}_n$ di grado $j_1 + \ldots + j_n \leq i_1 + \ldots + i_n$.

Appendice 2 – Dimostrazione della formula

$$\begin{aligned} | A_1 \otimes A_2 \otimes \cdots \otimes A_n | &= | A_1 |^{h_2 \cdots h_n} \cdot | A_2 |^{h_1 h_3 \cdots h_n} \cdots | A_n |^{h_1 \cdots h_{n-1}} \\ &= \frac{(| A_1 | \cdots | A_n |)^{h_1 h_2 \cdots h_n}}{| A_1 |^{h_1} \cdots | A_n |^{h_n}} \end{aligned}$$

È immediato convincersi che la formula in oggetto può essere provata facilmente ragionando per induzione sul numero s dei fattori tensoriali una volta provata per s=2. Poiché se $B_1 \sim A_1$ e $B_2 \sim A_2$ allora $A_1 \otimes A_2 \sim B_1 \otimes B_2$, è sufficiente provarla nel caso in cui A_1 e A_2 siano in forma canonica di Jordan (passando eventualmente alla chiusura algebrica del campo K).

Considerate la matrici $A = (a^i_j)$ e $B = (b^h_k)$, con $i, j = 0, \ldots, n-1$, e $h, k = 0, \ldots, m-1$, la matrice

$$A \otimes B = C = (c^\alpha_\beta) \qquad \alpha, \beta = 0, \ldots, mn-1$$

è data da

$$(*) \qquad c^\alpha_\beta = a^r_{\tilde{r}} \cdot b^q_{\tilde{q}} \qquad \text{con } \alpha = qn + r,\ \beta = \tilde{q}n + \tilde{r} \text{ e } r, \tilde{r} < n$$

Se A e B sono triangolari inferiori ($a^i_j = 0$ per $i < j$ e $b^h_k = 0$ per $h < k$) allora da $(*)$ consegue che anche $A \otimes B = C$ è triangolare inferiore (infatti $c^\alpha_\beta = a^r_{\tilde{r}} \cdot b^q_{\tilde{q}}$ è diverso da zero solo a patto che $r \geq \tilde{r}$ e $q \geq \tilde{q}$ e quindi che $\alpha = nq + r \geq n\tilde{q} + \tilde{r} = \beta$). Si verifica inoltre che gli elementi della diagonale di $A \otimes B$ sono dati dai prodotti degli elementi della diagonale di A per quelli della diagonale di B. Con ciò la formula considerata resta provata. □

Seconda dimostrazione della Prop. 1 La matrice di Vandermonde V_j associata alle radici di γ_j è la matrice che esprime il cambiamento di base, nello spazio S_j delle s.r.l. di scala γ_j, dalla base delle s.r.l. fondamentali (chiamiamola $b_{j,1}, \ldots, b_{j,h_j}$) alla base delle radici (chiamiamola $c_{j,1}, \ldots, c_{j,h_j}$). Orbene il sottospazio $S \subseteq K[X]^\circ$ delle forme ricorrenti n-lineari associate all'ideale $\Gamma = (\gamma_1, \ldots, \gamma_n) \subseteq K[X]$ è il prodotto tensoriale degli spazi S_j:

$$S = S_1 \otimes \cdots \otimes S_n$$

e la matrice

$$H_\prec(\tilde{\mathcal{P}}) = V_1 \otimes \cdots \otimes V_n$$

esprime il cambiamento dalla base delle forme ricorrenti n-lineari fondamentali

$$b_{1,t_1} \otimes \cdots \otimes b_{n,t_n} \qquad (1 \leq t_j \leq h_j)$$

alla base delle valutazioni v_P, $P \in \tilde{\mathcal{P}}$. Ne consegue l'enunciato in quanto la matrice in oggetto è la matrice di un cambiamento di base. □

Appendice 3 – Sulla dimostrazione della Prop. 7.

Chiariamo la dimostrazione della Prop. 7 ripetendone — con riferimento ad un esempio concreto — alcuni dei passi principali.

Per comodità, chiamiamo le variabili x, y, z, t in luogo di x_1, x_2, x_3, x_4 e identifichiamo $\mathcal{D}(\mathcal{P})$ con $\{\mathbf{x}^{\mathbf{d}} \mid \mathbf{d} \in \mathcal{D}(\mathcal{P})\}$. Supponiamo che si abbia $\underline{\mathcal{P}} = \underline{\{P_1, \dots, P_{33}\}}$, cui corrisponda il diagramma $\mathcal{D}(\underline{\mathcal{P}}) = \underline{\{\mathbf{d}_1, \dots, \mathbf{d}_{33}\}}$ seguente:

$$\begin{bmatrix} \mathbf{d}_1 = 1 & \mathbf{d}_2 = x & \mathbf{d}_3 = x^2 & \mathbf{d}_4 = x^3 & \mathbf{d}_5 = x^4 & \mathbf{d}_6 = x^5 \\ \mathbf{d}_7 = y & \mathbf{d}_8 = xy & \mathbf{d}_9 = x^2y & \mathbf{d}_{10} = x^3y & \mathbf{d}_{11} = x^4y & \\ \mathbf{d}_{12} = y^2 & \mathbf{d}_{13} = xy^2 & \mathbf{d}_{14} = x^2y^2 & \mathbf{d}_{15} = x^3y^2 & & \\ \mathbf{d}_{16} = y^3 & \mathbf{d}_{17} = xy^3 & & & & \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{d}_{18} = z & \mathbf{d}_{19} = xz & \mathbf{d}_{20} = x^2z & \mathbf{d}_{21} = x^3z \\ \mathbf{d}_{22} = yz & \mathbf{d}_{23} = xyz & \mathbf{d}_{24} = x^2yz & \\ \mathbf{d}_{25} = y^2z & \mathbf{d}_{26} = xy^2z & & \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{d}_{27} = z^2 & \mathbf{d}_{28} = xz^2 \\ \mathbf{d}_{29} = yz^2 & \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{d}_{30} = t & \mathbf{d}_{31} = xt \\ \mathbf{d}_{32} = yt & \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{d}_{33} = zt \end{bmatrix}$$

Per la Prop. 4, inoltre, possiamo supporre di aver ordinato $\underline{\mathcal{P}}$ in modo tale che gli elementi di $\underline{D} := \mathcal{D}(\underline{\mathcal{P}})$ vengano determinati nell'ordine lessicografico inverso, che è quello con cui sono stati numerati.

Supponiamo per assurdo che $D \cup C - D \cap C \neq \emptyset$ e che il più piccolo fra gli elementi appartenenti a $D \cup C - D \cap C$ sia, ad esempio, $\mathbf{f} = x^3yz \notin D$ (e quindi $\mathbf{f} \in C$). Si ha ora $s = 3$ e $f_s = f_3 = 1$.

In primo luogo mostriamo che non è restrittivo far riferimento a $\hat{\underline{\mathcal{P}}} := \underline{\{P_1, \dots, P_{29}\}}$, $\hat{\underline{D}} := \mathcal{D}(\hat{\underline{\mathcal{P}}}) = \underline{\{\mathbf{d}_1, \dots, \mathbf{d}_{29}\}}$ e $\hat{C} := C(\hat{\underline{\mathcal{P}}})$ (anziché a $\underline{\mathcal{P}}$, $\mathcal{D}(\underline{\mathcal{P}})$ e C). Se infatti $\mathbf{f} = x^3yz \notin \hat{C}$ allora si avrebbe

$$(*) \qquad x^3yz \equiv p[\mathbf{d}_1 = 1, \mathbf{d}_2 = x, \dots, \mathbf{d}_{29} = yz^2] \qquad mod.\Im(\hat{\mathcal{P}})$$

(con la notazione a secondo membro si denota una combinazione lineare dei monomi entro parentesi quadre) e il polinomio

$$(**) \qquad x^3yz - p[\mathbf{d}_1 = 1, \mathbf{d}_2 = x, \dots, \mathbf{d}_{29} = yz^2]$$

si annullerebbe per ciascuno dei punti $P_1, \dots, P_{29}$ e quindi — poiché, a causa della struttura di $\mathcal{D}(\underline{\mathcal{P}})$, risulta che le prime tre coordinate di uno qualunque dei punti $P_{30}, \ldots, P_{33}$ sono anche quelle di qualcuno dei punti $P_1, \ldots, P_{29}$ — si annullerebbe su tutto $\mathcal{P}$ e pertanto la congruenza $(*)$ sarebbe soddisfatta anche $mod.\Im(\mathcal{P})$, contro l'ipotesi che $\mathbf{f} = x^3yz \in C$.

Siamo quindi legittimati ad assumere che fin dall'inizio si sia posto $\underline{\mathcal{P}} = \underline{\{P_1, \ldots, P_{29}\}}$ e $\mathcal{D}(\underline{\mathcal{P}}) = \underline{\{\mathbf{d}_1, \ldots, \mathbf{d}_{29}\}}$. Proviamo ora che ogni polinomio della forma $(**)$ (e quindi nelle sole variabili x, y, z) appartenente a $\Im(\mathcal{P})$ è di grado $f_s = f_3 = 1$ in z cioè che i coefficienti dei termini in $\check{\mathcal{D}} := \{\mathbf{d}_{27} = z^2, \mathbf{d}_{28} = xz^2, \mathbf{d}_{29} = yz^2\}$ sono nulli. Indichiamo con $(a + bx + cy)z^2$ il complesso di tali termini. Per ogni punto P in $\check{\underline{\mathcal{P}}} := \underline{\{P_{27}, P_{28}, P_{29}\}} = \underline{\delta_{\mathcal{P}}}^{-1}(\check{\mathcal{D}})$ devono trovarsi in $\mathcal{P}$ altri $d_s = d_3 = 2$ punti aventi le stesse prime $s-1 = 2$ coordinate di P; pertano sostituendo tali prime due coordinate a x e y in $(**)$ si ottiene un polinomio nella sola z che — ammettendo $d_s+1 = 3$ radici distinte ed essendo di grado $d_s = 2$ — deve annullarsi identicamente. In particolare tali prime due coordinate (quelle dei punti dell'insieme $\check{\underline{\mathcal{Q}}} := \{\pi_2(P_{27}), \pi_2(P_{28}), \pi_2(P_{29})\}$) devono annullare il polinomio $a+bx+cy \in K[x, y]$, cioè $a+bx+cy \in \Im(\check{\underline{\mathcal{Q}}})$. Ma ciò è possibile solo a patto che $a = b = c = 0$ perché, come è facile dedurre dalla struttura di $\mathcal{D}(\underline{\mathcal{P}})$, si ha $\{1, x, y\} = \mathcal{D}(\{P_{27}, P_{28}, P_{29}\}) = \mathcal{D}(\{\pi_2(P_{27}), \pi_2(P_{28}), \pi_2(P_{29})\})$ e quindi $1, x, y$ costituiscono un sistema di rappresentanti per una base monomiale di $K[x, y]/\Im(\check{\underline{\mathcal{Q}}})$.

Pertanto un eventuale polinomio $(**)$ appartenente a $\Im(\mathcal{P})$ deve essere della forma

$$(***) \qquad x^3yz - p[\mathbf{d}_1 = 1, \mathbf{d}_2 = x, \ldots, \mathbf{d}_{26} = xy^2z].$$

Ripartiamo i termini (diversi da x^3yz) in $(***)$ nei tre sottoinsiemi $D_1 := \{\mathbf{d}_{25}, \mathbf{d}_{26}\}$, $D_2 := \{\mathbf{d}_{18}, \ldots, \mathbf{d}_{24}\}$ e $D_3 := \{\mathbf{d}_1, \ldots, \mathbf{d}_{17}\}$ (a seconda che $\mathbf{d}_j$ sia maggiore di $\mathbf{f} = x^3yz$ oppure, pur avendo lo stesso esponente in z, sia minore o infine abbia un esponente in z inferiore) e proviamo che anche i coefficienti di $\mathbf{d}_{25}$ e $\mathbf{d}_{26}$ devono annullarsi. Posto $\tilde{\mathcal{P}} := \underline{\delta_{\mathcal{P}}}^{-1}(D_1 \cup D_2) = \{P_{18}, \ldots, P_{26}\}$ e osservato che per ogni punto in $\tilde{\mathcal{P}}$ ne esistono in $\underline{\mathcal{P}}$ altri $f_s = 1$ aventi le stesse prime $s - 1 = 2$ coordinate di quello, il fatto che il polinomio $(***)$ è di grado $f_s = 1$ in z comporta che, sostituendo in $(***)$ a x e y le prime due coordinate di uno qualunque dei punti in $\tilde{\mathcal{P}}$ (e quindi di uno qualunque dei punti in $\tilde{\mathcal{Q}} := \pi_2(\tilde{\mathcal{P}})$) si ottiene un polinomio in z che deve annullarsi identicamente. In particolare i punti di $\tilde{\mathcal{Q}}$ devono annullare il polinomio in x, y che costituisce il coefficiente di z in $(***)$, diciamolo

$$(\#) \qquad x^3y - p_{(1)} - p_{(2)}$$

con

$$p_{(1)} := a_{25}y^2 + a_{26}xy^2$$

$$p_{(2)} := a_{18} + a_{19}x + a_{20}x^2 + a_{21}x^3 + a_{22}y + a_{23}xy + a_{24}x^2y.$$

In altri termini, il polinommio $(\#)$ appartiene $\Im(\tilde{\mathcal{Q}})$. D'altra parte i termini in $(\#)$ diversi da x^3y sono, come è facile controllare, gli elementi di $\mathcal{D}(\tilde{\mathcal{Q}}) = \pi_2(D_1 \cup$

D_2) e $x^3y = \pi_2(x^3yz)$ è un elemento diedrale di $\mathcal{D}(\tilde{\mathcal{Q}})$. Quindi $x^3y \notin \mathcal{D}(\tilde{\mathcal{Q}}) = \mathcal{C}(\tilde{\mathcal{Q}})$ (quest'ultima uguaglianza è garantita dall'ipotesi induttiva). La relazione $x^3y \notin \mathcal{C}(\tilde{\mathcal{Q}})$ e il fatto che $\mathcal{C}(\tilde{\mathcal{Q}})$ sia minimale rispetto all'ordine lessicografico inverso comportano che, modulo $\Im(\tilde{\mathcal{Q}})$, x^3y sia esprimibile, *in uno ed un sol modo*, come combinazione lineare dei termini in $\mathcal{C}(\tilde{\mathcal{Q}}) = \mathcal{D}(\tilde{\mathcal{Q}})$ *più piccoli* di x^3y, cioè che in (#) si abbia $a_{25} = a_{26} = 0$, che è quanto restava da provare per concludere che $\mathbf{f} = x^3yz \notin \mathcal{C}(\mathcal{P})$ in contraddizione con $\mathcal{D}(\mathcal{P}) \neq \mathcal{C}(\mathcal{P})$. □

Appendice 4 – Sulla Prop. 9.

Diamo una dimostrazione diretta del fatto che i monomi nella tabella della Prop. 9 costituiscono un sistema di rappresentati per una base monomiale rispetto all'ideale del multiisieme algebrico là considerato.

Dimostrazione. Per ogni $1 \leq i \leq m$ associamo al monomio $x^{m-i}y^{h_{m-i+1}-1}$ l'insieme

$$M_i := \cup_{j=1}^{i} S_{m-j,h_{m-j+1}-1}$$

come pure (se $i \neq m$) l'insieme

$$A_{i+1} := S_{m-1,h_{m-i}-1} - M_{i+1}$$

dove si è indicato con $S_{i,j}$ l'insieme $S_{i,j} := \{x^{i'}y^{j'} | i' \leq i \text{ e } j' \leq j\}$; poniamo inoltre $M_0 = A_1 := \emptyset$. Osserviamo che si ha

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots \subseteq M_m = M_{\mathcal{P}}$$

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots \subseteq A_m$$

$$\#M_m = \#M_{\mathcal{P}} = \#\mathcal{P}.$$

Nei calcoli che seguono denoteremo le *funzioni simmetriche elementari* delle variabili $\rho_1, \ldots, \rho_n$ mediante le notazioni

$$[\rho_1, \ldots, \rho_n]_0 := -1$$

$$[\rho_1, \ldots, \rho_n]_1 := \rho_1 + \ldots + \rho_n$$

$$[\rho_1, \ldots, \rho_n]_2 := -(\rho_1\rho_2 + \ldots + \rho_{n-1}\rho_n)$$

$$\ldots\ldots\ldots\ldots$$

$$[\rho_1, \ldots, \rho_n]_n := (-1)^{n-1}\rho_1\rho_2 \cdots \rho_n$$

cioè

$$[\rho_1, \ldots, \rho_n]_i := (-1)^{i-1} \sum_{1 \leq j_1 < \ldots < j_i \leq n} \rho_{j_1}\rho_{j_2} \cdots \rho_{j_i}.$$

Poiché $\#M_m = \#M_{\mathcal{P}} = \#\mathcal{P} = \textit{codim}\ \Im(\mathcal{P})$ è sufficiente dimostrare che le classi di equivalenza (modulo $\Im(\mathcal{P})$) dei monomi in M_m costituiscono un insieme di generatori per l'algebra quoziente $K[X]/\Im(\mathcal{P})$. Ciò discende subito dalle congruenze

$$(C_s) \qquad x^s y^{h_{s+1}} \equiv \sum_{i=1}^{s} [\rho_1, \rho_2, \ldots, \rho_s]_i \, x^{s-i} y^{h_{s+1}} + \sum_{\tau \in M_{m-s}} \mu_\tau \tau$$

$$(C'_s) \qquad x^i y^j \equiv \sum_{\tau \in M_{m-s+1}} \alpha_\tau \tau \qquad se \qquad x^i y^j \in A_{m-s+1}$$

(con $\mu_\tau, \alpha_\tau \in K$) per $s = m, m-1, \ldots, 1, 0$ ed avendo assunto $h_{m+1} := 0$.

È facile verificare che la (C'_s) è una diretta conseguenza di (C_t) per $m \geq t \geq s$. Proviamo quest'ultima ragionando induttivamente sui valori decrescenti di s. Per $s = m$ essa è banalmente vera, giacché esprime semplicemente il fatto che il polinomio

$$\prod_{i=1}^{m} (x - \rho_i) = -\sum_{i=0}^{m} [\rho_1, \ldots, \rho_m]_i \, x^{m-i}$$

appartiene a $I = \Im(\mathcal{P})$.

Supponiamo pertanto che la (C_s) sia vera per ogni $m \geq s \geq t$ e proviamola per $s = t - 1$.

Consideriamo il polinomio contenuto in $\Im(\mathcal{P})$

$$\begin{aligned}
p_t \;:=\;& \prod_{i \neq t} (x - \rho_i) \cdot \prod_{j=1}^{h_t} (y - \sigma_{t,j}) = \\
=\;& -\sum_{i=0}^{m-1} [\rho_1, \ldots, \rho_{t-1}, \rho_{t+1}, \ldots, \rho_m]_i \, x^{m-1-i} y^{h_t} + \\
& + \sum_{\tau \in A_{m-t+1}} \beta_\tau \tau + \sum_{\tau \in M_{m-t+1}} \gamma_\tau \tau \equiv \\
& \text{(usando la } (C'_t) \text{ per inglobare la seconda sommatoria nella terza)} \\
\equiv\;& x^{m-1} y^{h_t} - \sum_{i=1}^{m-1} [\rho_1, \ldots, \rho_{t-1}, \rho_{t+1}, \ldots, \rho_m]_i \, x^{m-1-i} y^{h_t} + \\
& + \sum_{\tau \in M_{m-t+1}} \delta_\tau \tau \equiv \\
& \text{(usando prima la } (C_{m-1}) \text{ e successivamente la } (C'_t) \text{ per ridurre} \\
& \text{il primo termine)} \\
\equiv\;& \sum_{i=1}^{m-1} \{[\rho_1, \ldots, \rho_{m-1}]_i - [\rho_1, \ldots, \rho_{t-1}, \rho_{t+1}, \ldots, \rho_m]_i\} \, x^{m-1-i} y^{h_t} + \\
& + \sum_{\tau \in M_{m-t+1}} \varepsilon_\tau \tau =
\end{aligned}$$

$$= \quad (\rho_t - \rho_m) \sum_{i=1}^{m-1} -[\rho_1, \ldots, \rho_{t-1}, \rho_{t+1}, \ldots, \rho_{m-1}]_{i-1}\, x^{m-1-i} y^{h_t} +$$

$$+ \sum_{\tau \in M_{m-t+1}} \varepsilon_\tau \tau =$$

(posto i in luogo di $i-1$)

$$= \quad (\rho_t - \rho_m)\{x^{m-2} y^{h_t} - \sum_{i=1}^{m-2} [\rho_1, \ldots, \rho_{t-1}, \rho_{t+1}, \ldots, \rho_{m-1}]_i\, x^{m-2-i} y^{h_t}\} +$$

$$+ \sum_{\tau \in M_{m-t+1}} \varepsilon_\tau \tau \equiv$$

(utilizzando ora la (C_{m-2}) e successivamente la (C'_t) per ridurre il primo termine e operando le semplificazioni come nei passaggi precedenti)

$$\equiv \quad (\rho_t - \rho_m)(\rho_t - \rho_{m-1})\{x^{m-3} y^{h_t} +$$

$$- \sum_{i=1}^{m-3} [\rho_1, \ldots, \rho_{t-1}, \rho_{t+1}, \ldots, \rho_{m-2}]_i\, x^{m-3-i} y^{h_t}\} + \sum_{\tau \in M_{m-t+1}} \eta_\tau \tau \equiv$$

....

$$\equiv \quad (\rho_t - \rho_m)(\rho_t - \rho_{m-1}) \cdots (\rho_t - \rho_{t+1})\{x^{t-1} y^{h_t} +$$

$$- \sum_{i=1}^{t-1} [\rho_1, \ldots, \rho_{t-1}]_i\, x^{t-1-i} y^{h_t}\} + \sum_{\tau \in M_{m-t+1}} \varsigma_\tau \tau$$

$$\equiv \quad 0 \quad (\text{modulo } \Im(\mathcal{P}))$$

da cui la (C_{t-1}). □

Appendice 5 – Sulla dimostrazione della Prop. 11.

A titolo chiarificatore, ripercorriamo — facendo riferimendo ad un caso concreto — il ragionamento fatto nella dimostrazione della Prop. 11.

Sia dato il multiinsieme algebrico $\wp$:

$$P_1 = (0,0,0) \quad \begin{bmatrix} (0,0,0) & (1,0,0) & & (0,0,1) & & \\ (0,1,0) & & & & & \end{bmatrix}$$

$$P_2 = (0,0,1) \quad \begin{bmatrix} (0,0,0) & (1,0,0) & (2,0,0) & (0,0,1) & (1,0,1) & \end{bmatrix}$$

$$P_3 = (1,1,0) \quad \begin{bmatrix} (0,0,0) & (1,0,0) & & (0,0,1) & (1,0,1) & (0,0,2) \\ (0,1,0) & (1,1,0) & & (0,1,1) & & (0,1,2) \end{bmatrix}$$

$$P_4 = (1,1,1) \quad \begin{bmatrix} (0,0,0) \\ (0,1,0) \end{bmatrix}$$

La sua rappresentazione umbrale $\mathcal{R} = \mathcal{R}(\wp)$ (qui, volutamente, gli elementi di $\mathcal{R}$ vengono elencati secondo un ordine casuale) ed il corrispondente diagramma $\mathcal{D}(\mathcal{R})$ sono dati dalla tabella

$\mathcal{R}$	$\longleftrightarrow$	$\mathcal{D}(\mathcal{R})$
$R_1 = (10,\ 10,\ 02)$	$\longleftrightarrow$	$\mathbf{d}_1 = (0,\ 0,\ 0)$
$R_2 = (10,\ 11,\ 02)$	$\longleftrightarrow$	$\mathbf{d}_2 = (0,\ 1,\ 0)$
$R_3 = (01,\ 00,\ 11)$	$\longleftrightarrow$	$\mathbf{d}_3 = (1,\ 0,\ 0)$
$R_4 = (11,\ 10,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_4 = (2,\ 0,\ 0)$
$R_5 = (00,\ 00,\ 11)$	$\longleftrightarrow$	$\mathbf{d}_5 = (3,\ 0,\ 0)$
$R_6 = (10,\ 10,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_6 = (0,\ 0,\ 1)$
$R_7 = (02,\ 00,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_7 = (4,\ 0,\ 0)$
$R_8 = (01,\ 00,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_8 = (1,\ 0,\ 1)$
$R_9 = (10,\ 10,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_9 = (0,\ 0,\ 2)$
$R_{10} = (00,\ 01,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{10} = (1,\ 1,\ 0)$
$R_{11} = (00,\ 00,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{11} = (2,\ 0,\ 1)$
$R_{12} = (00,\ 00,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_{12} = (1,\ 0,\ 2)$
$R_{13} = (10,\ 11,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{13} = (0,\ 1,\ 1)$
$R_{14} = (11,\ 10,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{14} = (3,\ 0,\ 1)$
$R_{15} = (00,\ 00,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{15} = (0,\ 0,\ 3)$
$R_{16} = (10,\ 11,\ 01)$	$\longleftrightarrow$	$\mathbf{d}_{16} = (0,\ 1,\ 2)$
$R_{17} = (11,\ 11,\ 00)$	$\longleftrightarrow$	$\mathbf{d}_{17} = (2,\ 1,\ 0)$
$R_{18} = (01,\ 00,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{18} = (2,\ 0,\ 2)$
$R_{19} = (10,\ 11,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{19} = (1,\ 0,\ 3)$
$R_{20} = (10,\ 10,\ 10)$	$\longleftrightarrow$	$\mathbf{d}_{20} = (0,\ 1,\ 3)$

Dobbiamo dimostrare che l'insieme delle classi di equivalenza (modulo $\Im(\wp)$) dei monomi

$$\begin{array}{lllll} 1 & x_1 & x_1^2 & x_1^3 & x_1^4 \\ x_2 & x_1x_2 & x_1^2x_2 & & \end{array} \qquad \begin{array}{llll} x_3 & x_1x_3 & x_1^2x_3 & x_1^3x_3 \\ x_2x_3 & & & \end{array}$$

$$\begin{array}{lll} x_3^2 & x_1x_3^2 & x_1^2x_3^2 \\ x_2x_3^2 & & \end{array} \qquad \begin{array}{ll} x_3^3 & x_1x_3^3 \\ x_2x_3^3 & \end{array}$$

costituisce una base monomiale per $K[X]/\Im(\wp)$, cioè che ogni polinomio

$$\begin{aligned} p(x_1,\ldots,x_n) \;\; = \;\; & p_0[1,x_1,x_1^2,x_1^3,x_1^4,x_2,x_1x_2,x_1^2x_2]+p_1[1,x_1,x_1^2,x_1^3,x_2]\cdot x_3+ \\ & +p_2[1,x_1,x_1^2,x_2]\cdot x_3^2+p_3[1,x_1,x_2]\cdot x_3^3 \in \Im(\wp) \end{aligned}$$

(qui le parentesi quadre stanno ad indicare che il polinomio $p[\eta,\varsigma,\ldots]$ è una combinazione lineare dei monomi $\eta,\varsigma,\ldots$) è identicamente nullo.

In $\mathcal{D}(\mathcal{R})$ il massimo valore assunto dalla terza componente è $h=3$; consideriamo pertanto l'insieme

$$D_3=\{\mathbf{d}^{(1)}=\mathbf{d}_{15}=(0,0,3), \quad \mathbf{d}^{(2)}=\mathbf{d}_{19}=(1,0,3), \quad \mathbf{d}^{(3)}=\mathbf{d}_{20}=(0,1,3)\}$$

e l'insieme delle sue controimmagini tramite $\underline{\delta}_{\mathcal{R}}$:

$$\begin{aligned} \mathcal{R}_3 \;\; = \;\; & \{R^{(1)}=R_{15}=(00,00,10), \qquad R^{(2)}=R_{19}=(10,11,10), \\ & R^{(3)}=R_{20}=(10,10,10)\}. \end{aligned}$$

[NB. Se, inizialmente, avessimo considerato i punti in $\mathcal{R}$ in un diverso ordine, l'insieme $\mathcal{R}_3$ sarebbe stato diverso da quello qui effettivamente ottenuto ma tutta l'analisi che segue si sarebbe potuta ripetere esattamente allo stesso modo. In effetti un diverso ordine in $\mathcal{R}$ provocherebbe — al più — una permutazione degli indici in alto degli insiemi $\mathcal{T}_3^{(j)}$ e lascerebbe quindi inalterato l'insieme $\mathcal{T}_3$.]
Consideriamo $R^{(1)}=R_{15}=(00,00,10)\in\mathcal{R}_3$; poiché l'ultima coordinata di $\underline{\delta}_{\mathcal{R}}(R^{(1)})=\mathbf{d}^{(1)}=\mathbf{d}_{15}=(0,0,3)$ è "3", devono esservi in $\mathcal{R}$ altri tre punti — che precedono $R_{15}=R^{(1)}$ — le cui coordinate sono della forma $(00,00,--)$; l'insieme di questi punti viene indicato con $\mathcal{T}_3^{(1)}$; in effetti si tratta dell'insieme

$$\begin{aligned} \mathcal{T}_3^{(1)} \;\; = \;\; & \{R_5=(00,\ 00,\ 11), \qquad R_{11}=(00,\ 00,\ 00), \\ & R_{12}=(00,\ 00,\ 01), \qquad R_{15}=(00,\ 00,\ 10)\}. \end{aligned}$$

Analogamente, in corrispondenza agli altri due punti di $\mathcal{R}_3$, si trovano gli insiemi

$$\begin{aligned} \mathcal{T}_3^{(2)} \;\; = \;\; & \{R_2=(10,\ 11,\ 02), \qquad R_{13}=(10,\ 11,\ 00), \\ & R_{16}=(10,\ 11,\ 01), \qquad R_{15}=(10,\ 11,\ 10)\}, \end{aligned}$$

$$\begin{aligned} \mathcal{T}_3^{(3)} \;\; = \;\; & \{R_1=(10,\ 10,\ 02), \qquad R_6=(10,\ 10,\ 01), \\ & R_9=(10,\ 10,\ 00), \qquad R_{20}=(10,\ 10,\ 10)\}. \end{aligned}$$

Posto

$$\mathcal{T}_3 := \mathcal{T}_3^{(1)} \cup \mathcal{T}_3^{(2)} \cup \mathcal{T}_3^{(3)},$$

si ha

$$\pi_2(\mathcal{T}_3) = \pi_2(\mathcal{R}_3) = \{(00,00),\ (10,11),\ (10,10)\}$$

$$\begin{aligned} \wp_3 = U(\pi_2(\mathcal{T}_3)) &= \{((0,0),(0,0)) \quad ((1,1),(0,0)) \quad ((1,1),(0,1))\} = \\ &= \{(0,0),[(0,0)]; \quad (1,1),[(0,0),(0,1)]\} \end{aligned}$$

e

$$\tau: \quad ((0,0),(0,0)) \mapsto \mathcal{T}_3^{(1)}; \quad ((1,1),(0,0)) \mapsto \mathcal{T}_3^{(3)}; \quad ((1,1),(0,1)) \mapsto \mathcal{T}_3^{(2)}.$$

NB. All'elemento $((a_1,a_2),(i_1,i_2)) \in \wp_3$ la bigezione τ fa corrispondere il $\mathcal{T}_3^{(j)}$ i cui elementi sono della forma $((a_1,i_1),(a_2,i_2),(-,-))$.

Consideriamo ora un polinomio $f(x_1,x_2,x_3) \in \Im(\wp)$ e fissiamo la nostra attenzione — ad esempio — sul punto $(Q,\mathrm{j}) = ((1,1),(0,1))$ di $\wp_3$, sulla sua immagine $\mathcal{T}_3^{(2)}$ in τ e sulla valutazione umbrale

$$U(\mathcal{T}_3^{(2)}) = \{(1,1,0),\ [(0,1,0),(0,1,1),(0,1,2)]; \quad (1,1,1),\ [(0,1,0)]\}.$$

La relazione $U(\mathcal{T}_3^{(2)}) \subseteq \wp$ garantisce che, valutando in $x_1 = x_2 = 1$ la derivata rispetto ad x_2 di f si ottiene un polinomio in x_3 che deve ammettere la radice tripla $x_3 = 0$ e la radice $x_3 = 1$ e quindi deve essere almeno di quarto grado. Similmente, se fissiamo l'attenzione sugli altri due punti $(Q,\mathrm{j}) = ((1,1),(0,0))$ e, rispettivamente, $(Q,\mathrm{j}) = ((0,0),(0,0))$ di $\wp_3$, otteniamo che anche le valutazioni di f in $x_1 = x_2 = 1$ e in $x_1 = x_2 = 0$ devono essere polinomi in x_3 almeno di quarto grado.

Nel caso in cui $f(x_1,x_2,x_3) = p(x_1,x_2,x_3)$ ciò comporta che il coefficiente $p_3[1,x_1,x_2]$ di x_3^3 in p deve annullarsi in $(1,1)$ insieme con la sua derivata prima dispetto a x_2 ed in $(0,0)$, cioè deve appartenere all'ideale del multiinsieme algebrico $\wp_3$. Poiché la base monomiale che l'operatore $\mathcal{D}$ associa a $\wp_3$ è proprio costituita dai monomi $1, x_1, x_2$, si può — applicando l'ipotesi induttiva — concludere che $p_3[1,x_1,x_2]$ è identicamente nullo.

A questo punto abbiamo quindi

$$\begin{aligned} p(x_1,\ldots,x_n) &= p_0[1,x_1,x_1^2,x_1^3,x_1^4,x_2,x_1x_2,x_1^2x_2] + p_1[1,x_1,x_1^2,x_1^3,x_2]\cdot x_3 + \\ &\quad + p_2[1,x_1,x_1^2,x_2]\cdot x_3^2; \end{aligned}$$

considerando ora D_2 (in luogo di D_3) possiamo ripercorrere tutto il ragionamento precedente fino ad ottenere $p_2[1,x_1,x_1^2,x_2] \equiv 0$, etc. etc. □