Sulla bialgebra duale
della bialgebra dei polinomi in più variabili.

DI

LUIGI CERLIENCO E FRANCESCO PIRAS

Dipartimento di Matematica
Cagliari

SUMMARY. This paper is devoted to the study of the dual bialgebra $\mathcal{B}_n^\circ$ of the bialgebra $\mathcal{B}_n$ of polynomials in finitely many variables. The elements of $\mathcal{B}_n^\circ$ are described in various ways in order to obtain some useful formulae (e.g., a formula for the "remainder" modulo a cofinite ideal of $\mathcal{B}_n$). The subcoalgebra $C_{\mathbf{f}}$ generated by a given element $\mathbf{f} \in \mathcal{B}_n^\circ$ is studied and its structure constants with relation to different natural bases are given.

1. Generalità.

Sia K un campo e $X = \{x_1, \ldots, x_n\}$ un insieme di indeterminate. Consideriamo lo spazio $K[X] := K[x_1, \ldots, x_n]$ dei polinomi a coefficienti in K nelle indeterminate $x_1, \ldots, x_n$ e sia $K[X]^* \simeq K[[X]]$ il suo spazio duale. Facendo uso delle notazioni

$$\mathbf{i} := (i_1, \ldots, i_n) \in \mathbf{N}^n$$

e

$$\mathbf{x}^{\mathbf{i}} := x_1^{i_1} \ldots x_n^{i_n},$$

il generico elemento $\mathbf{f}$ di $K[X]^*$ verrà rappresentato nella forma

$$\mathbf{f} = \sum_{\mathbf{i} \in \mathbf{N}^n} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \tag{1}$$

dove $F_{\mathbf{i}} := \mathbf{f}(\mathbf{x}^{\mathbf{i}})$. L'usuale ordine su $\mathbf{N}$, come pure l'ordine parziale prodotto da esso indotto su $\mathbf{N}^n$, verrà denotato con $\leq$. La notazione $\preceq$ denoterà invece un arbitrario buon ordine su $\mathbf{N}^n$ compatibile con la sua struttura di monoide (equivalentemente, un ordine lineare compatibile per il quale l'elemento neutro sia il minimo).

Per ogni $j \in \{1, \ldots, n\}$, l'operatore "shift" E_j è l'operatore lineare definito da

$$\begin{aligned} E_j : K[x_j]^* &\longrightarrow K[x_j]^* \\ \sum_{i \in \mathbf{N}} F_i x_j^i &\longmapsto \sum_{i \in \mathbf{N}} F_{i+1} x_j^i . \end{aligned} \tag{2}$$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Identificato $K[X]$ con $K[x_1] \otimes \cdots \otimes K[x_n]$ tramite l'isomorfismo canonico

$$\begin{aligned} K[x_1] \otimes \cdots \otimes K[x_n] &\longrightarrow K[X] \\ x_1^{i_1} \otimes \cdots \otimes x_n^{i_n} &\longmapsto x_1^{i_1} \ldots x_n^{i_n} = \mathbf{x}^{\mathbf{i}} \quad , \end{aligned}$$

poniamo $\mathbf{E}^{\mathbf{i}} := E_1^{i_1} \otimes \cdots \otimes E_n^{i_n}$, per cui

$$\begin{aligned} \mathbf{E}^{\mathbf{i}} \colon K[X]^* &\longrightarrow K[X]^* \\ \sum_{\mathbf{j} \in \mathbf{N}^n} F_{\mathbf{j}} \mathbf{x}^{\mathbf{j}} &\longmapsto \sum_{\mathbf{j} \in \mathbf{N}^n} F_{\mathbf{j}+\mathbf{i}} \mathbf{x}^{\mathbf{j}} \quad . \end{aligned} \tag{3}$$

Conviene identificare E_j con $\mathbf{E}^{\varepsilon_j} = 1 \otimes \cdots \otimes E_j \otimes \cdots \otimes 1$ dove $\varepsilon_1 = (1, 0, \ldots, 0), \ldots, \varepsilon_n = (0, \ldots, 0, 1)$; inoltre, se $\gamma(x_1, \ldots, x_n) \in K[X]$, useremo la notazione $\gamma(\mathbf{E})$ come abbreviazione per $\gamma(E_1, \ldots, E_n)$.

Lo spazio $K[X]$ è dotato naturalmente di una struttura di bialgebra $\mathcal{B}_n := (K[X], m, u, \Delta, \varepsilon)$ (cfr. [3]). In particolare $\mathcal{A}_n := (K[X], m, u)$ è l'usuale algebra dei polinomi e $\mathcal{C}_n := (K[X], \Delta, \varepsilon)$ è la coalgebra per la quale la "diagonalizzazione" (o "comoltiplicazione") Δ e la "augmentation" (o "counit map") ε possono - via le identificazioni $x_1^0 \ldots x_i \ldots x_n^0 \otimes x_1^0 \ldots x_n^0 = x_i$ e $x_1^0 \ldots x_n^0 \otimes x_1^0 \ldots x_i \ldots x_n^0 = y_i$ - venir descritte in termini informali da:

$$\Delta \colon p(x_1, \ldots, x_n) \longmapsto p(x_1 + y_1, \ldots, x_n + y_n)$$

e rispettivamente

$$\varepsilon \colon p(x_1, \ldots, x_n) \longmapsto p(0, \ldots, 0).$$

La bialgebra $\mathcal{B}_n^\circ := (K[X]^\circ, \widetilde{\Delta}, \widetilde{\varepsilon}, \widetilde{m}, \widetilde{u})$ duale di $\mathcal{B}_n$ ha come sostegno l'insieme $K[X]^\circ$ formato da tutte le forme $\mathbf{f} \in K[X]^*$ il cui nucleo contiene un ideale cofinito J dell'algebra $K[X]$. La moltiplicazione $\widetilde{\Delta}$, la unità $\widetilde{\varepsilon}$, la comoltiplicazione $\widetilde{m}$ e la augmentation $\widetilde{u}$ di $\mathcal{B}_n$ sono le restrizioni a $K[X]^\circ$ delle applicazioni duali di Δ , ε , m e u rispettivamente. In particolare si ha

$$\widetilde{m}(\mathbf{f})(\mathbf{x}^{\mathbf{s}} \otimes \mathbf{x}^{\mathbf{t}}) = \mathbf{f}(\mathbf{x}^{\mathbf{s}+\mathbf{t}}), \qquad \widetilde{\Delta}(\mathbf{f} \otimes \mathbf{g})(\mathbf{x}^{\mathbf{s}}) = \sum_{\mathbf{t} \leq \mathbf{s}} \binom{\mathbf{s}}{\mathbf{t}} \mathbf{f}(\mathbf{x}^{\mathbf{t}}) \mathbf{g}(\mathbf{x}^{\mathbf{s}-\mathbf{t}}) \tag{4}$$

dove $\binom{\mathbf{s}}{\mathbf{t}} := \binom{s_1}{t_1} \ldots \binom{s_n}{t_n}$.

Ricordiamo che un ideale J di $K[X]$ si dice *cofinito* se l'algebra quoziente $K[X]/J$ è a dimensione finita:

$$codim(J) = dim(K[X]/J) < \infty.$$

Nel caso in cui il campo K sia algebricamente chiuso, consegue dal Nullstellensatz che un ideale $J \subseteq K[X]$ è cofinito se e solo se l'insieme algebrico

$$\mathcal{V}(J) := \{P \in K^n \mid p \in J \Rightarrow p(P) = 0\}$$

contiene un numero finito di punti. In tal caso si ha inoltre:

$$\#\mathcal{V}(J) \leq codim(J).$$

Nel seguito ogniqualvolta considereremo l'insieme algebrico $\mathcal{V}(J)$, assumeremo tacitamente che K sia algebricamente chiuso.

Nel caso $n = 1$ gli elementi della bialgebra $\mathcal{B}_1^\circ$ sono le successioni ricorrenti lineari. Un'analisi dettagliata di tale bialgebra – come pure una snella introduzione alle strutture qui considerate – può essere trovata in [3] (si veda anche [4]).

In forza della relazione

$$\mathcal{B}_n^\circ \simeq (\mathcal{B}_1 \otimes \cdots \otimes \mathcal{B}_1)^\circ \simeq \mathcal{B}_1^\circ \otimes \cdots \otimes \mathcal{B}_1^\circ ,$$

lo studio di $\mathcal{B}_n^\circ$ può essere parzialmente ricondotto a quello di $\mathcal{B}_1^\circ$. Tuttavia non è detto che una data sottostruttura (ad esempio sottocoalgebra) di $\mathcal{B}_n^\circ$ possa essere ottenuta come prodotto tensoriale di analoghe sottostrutture di $\mathcal{B}_1^\circ$. Scopo del presente lavoro è principalmente quello di analizzare alcune situazioni di questo tipo.

2. Forme ricorrenti n–lineari.

Per analogia con il caso in una sola indeterminata chiameremo forme ricorrenti n–lineari gli elementi di $K[X]^\circ$. Data una forma ricorrente n–lineare $\mathbf{f}$, chiameremo ideale caratteristico di $\mathbf{f}$ ogni ideale cofinito J contenuto in $Ker(\mathbf{f})$ e ideale massimale di $\mathbf{f}$ il suo più grande ideale caratteristico. Nel seguito, salvo indicazione contraria, con $\mathbf{f}$ indicheremo una forma ricorrente n–lineare e con J l'ideale massimale di $\mathbf{f}$. (Va osservato che nel caso $n = 1$ l'ideale massimale della successione ricorrente lineare $\mathbf{f}$ è quello generato dal suo polinomio minimale).

Date due forme ricorrenti n–lineari $\mathbf{f}$, $\mathbf{g}$ aventi J e I rispettivamente come ideale caratteristico, allora il meet $J \wedge I$ è un ideale caratteristico per la forma $\mathbf{f} + \mathbf{g}$.

Il cosiddetto teorema fondamentale della teoria delle coalgebre (cfr. [1], pag. 46) assicura che la più piccola sottocoalgebra di $\mathcal{B}_n^\circ$ contenente $\mathbf{f}$ – diciamola $C_\mathbf{f}$ – è a dimensione finita. $C_\mathbf{f}$ coincide con la sottocoalgebra C_J costituita da tutte le forme ricorrenti n–lineari aventi J per ideale caratteristico. Con riferimento alla sola struttura di spazio lineare si ha

$$C_J \simeq (K[X]/J)^*$$

(ciò consegue dall'universalità del quoziente) e quindi

$$dim(C_J) = dim(K[X]/J) = codim(J).$$

Va anche notato che $C_\mathbf{f} (= C_J)$ non costituisce una sottobialgebra di $\mathcal{B}_n^\circ$; in particolare – come discende facilmente dal Corollario alla Prop.5 – $C_\mathbf{f}$ non è chiuso rispetto alla moltiplicazione $\tilde{\Delta}$.

Sia $\mathcal{L}$ una base per il K–spazio lineare $K[X]/J$ tale che i suoi elementi siano classi di equivalenza della forma $[\mathbf{x}^\mathbf{i}]_J$ e sia $L \subseteq \mathbf{N}^n$ tale che $\mathcal{L} = \{[\mathbf{x}^\mathbf{i}]_J \mid \mathbf{i} \in L\}$. Per ogni $\mathbf{i} \in L$ consideriamo la forma ricorrente n–lineare

$$\mathbf{s}^\mathbf{i} = \sum_{\mathbf{j} \in \mathbf{N}^n} S_\mathbf{j}^\mathbf{i} \mathbf{x}^\mathbf{j} \in C_J \tag{5}$$

definita dalle condizioni iniziali

$$S_\mathbf{j}^\mathbf{i} = \delta_\mathbf{j}^\mathbf{i} := \delta_{j_1}^{i_1} \dots \delta_{j_n}^{i_n} \qquad \text{per } \mathbf{j} \in L. \tag{5'}$$

L'insieme $\{\mathbf{s}^{\mathbf{i}} \mid \mathbf{i} \in L\}$ forma una base per C_J. Per ogni $\mathbf{f} = \sum_{\mathbf{i}\in\mathbf{N}^n} F_{\mathbf{i}}\mathbf{x}^{\mathbf{i}} \in C_J$ si ha allora

$$\mathbf{f} = \sum_{\mathbf{i}\in L} F_{\mathbf{i}}\mathbf{s}^{\mathbf{i}} \tag{6}$$

da cui

$$F_{\mathbf{p}} = \mathbf{f}(\mathbf{x}^{\mathbf{p}}) = \sum_{\mathbf{i}\in L} F_{\mathbf{i}}S^{\mathbf{i}}_{\mathbf{p}}, \qquad \mathbf{p} \in \mathbf{N}^n. \tag{7}$$

Facendo uso delle forme $\mathbf{s}^{\mathbf{i}}$ si può agevolmente calcolare il "resto" modulo J di un qualunque polinomio in $K[X]$. Si ha infatti la

Proposizione 1. *Per ogni* $\mathbf{p} \in \mathbf{N}^n$ *si ha*

$$\mathbf{x}^{\mathbf{p}} \equiv \sum_{\mathbf{i}\in L} S^{\mathbf{i}}_{\mathbf{p}}\mathbf{x}^{\mathbf{i}} \qquad mod.J. \tag{8}$$

DIMOSTRAZIONE: Per ogni $\mathbf{p} \in L$ la (8) è ovvia. Per $\mathbf{p} \notin L$, sia

$$\mathbf{x}^{\mathbf{p}} - \sum_{\mathbf{i}\in L} T^{\mathbf{i}}_{\mathbf{p}}\mathbf{x}^{\mathbf{i}} \equiv 0 \quad mod.J\,.$$

Allora, per ogni $\mathbf{j} \in L$, si ha:

$$0 = \mathbf{s}^{\mathbf{j}}\Big(\mathbf{x}^{\mathbf{p}} - \sum_{\mathbf{i}\in L} T^{\mathbf{i}}_{\mathbf{p}}\mathbf{x}^{\mathbf{i}}\Big) = S^{\mathbf{j}}_{\mathbf{p}} - \sum_{\mathbf{i}\in L} T^{\mathbf{i}}_{\mathbf{p}}\delta^{\mathbf{j}}_{\mathbf{i}} = S^{\mathbf{j}}_{\mathbf{p}} - T^{\mathbf{j}}_{\mathbf{p}};$$

da cui

$$T^{\mathbf{j}}_{\mathbf{p}} = S^{\mathbf{j}}_{\mathbf{p}}. \quad \blacksquare$$

La formula (8) consente di ottenere una rappresentazione matriciale S della proiezione canonica (=applicazione lineare "resto *mod.J*") da $K[X]$ a $K[X]/J$. Infatti, ordiniamo linearmente sia gli elementi di $\mathbf{N}^n$ che, di conseguenza, quelli di L, ed assumiamo i primi come indici di colonna e i secondi come indici di riga; con riferimento a tale ordine S è la matrice di entrate $S^{\mathbf{i}}_{\mathbf{p}}$. Poichè, come mostreremo nel paragrafo seguente, i valori di $S^{\mathbf{i}}_{\mathbf{p}}$ possono venir calcolati mediante semplici ricorrenze, la formula (8) (o equivalentemente la matrice S) forniscono un algoritmo per il calcolo del resto *mod.J* più agevole - così almeno ci pare - di quanto non sia la riduzione tramite le basi di Groebner di J. Osserviamo inoltre che la Prop.1 continua a valere anche nel caso in cui l'ideale J non è cofinito.

3. Costanti di struttura della coalgebra C_J.

La proposizione seguente fornisce le <u>costanti di struttura</u> della comoltiplicazione $\tilde{m}$ in C_J rispetto alla base $\{\mathbf{s}^{\mathbf{i}} \mid \mathbf{i} \in L\}$ ora introdotta.

Proposizione 2.

(9)
$$\tilde{m}(\mathbf{s^i}) = \sum_{\mathbf{p},\mathbf{q}\in L} S^{\mathbf{i}}_{\mathbf{p}+\mathbf{q}} \mathbf{s^p} \otimes \mathbf{s^q}.$$

DIMOSTRAZIONE: Applicando i due membri di (9) al generico elemento $\mathbf{x^u} \otimes \mathbf{x^v}$ di $K[X] \otimes K[X]$ si ha:

$$\tilde{m}(\mathbf{s^i})(\mathbf{x^u} \otimes \mathbf{x^v}) = \mathbf{s^i}(\mathbf{x^{u+v}}) = S^{\mathbf{i}}_{\mathbf{u}+\mathbf{v}}$$

e rispettivamente

$$\begin{aligned}
\Big(\sum_{\mathbf{p},\mathbf{q}\in L} S^{\mathbf{i}}_{\mathbf{p}+\mathbf{q}} \mathbf{s^p} \otimes \mathbf{s^q}\Big)(\mathbf{x^u} \otimes \mathbf{x^v}) &= \sum_{\mathbf{p},\mathbf{q}\in L} S^{\mathbf{i}}_{\mathbf{p}+\mathbf{q}} S^{\mathbf{p}}_{\mathbf{u}} S^{\mathbf{q}}_{\mathbf{v}} = \\
&= \sum_{\mathbf{p}\in L}\Big(\sum_{\mathbf{q}\in L}\big(\mathbf{E^p s^i}\big)_{\mathbf{q}} S^{\mathbf{q}}_{\mathbf{v}}\Big) S^{\mathbf{p}}_{\mathbf{u}} = \qquad \text{(per la (7))} \\
&= \sum_{\mathbf{p}\in L}\big(\mathbf{E^p s^i}\big)_{\mathbf{v}} S^{\mathbf{p}}_{\mathbf{u}} = \sum_{\mathbf{p}\in L}\big(\mathbf{E^v s^i}\big)_{\mathbf{p}} S^{\mathbf{p}}_{\mathbf{u}} = \qquad \text{(ancora per la (7))} \\
&= \big(\mathbf{E^v s^i}\big)_{\mathbf{u}} = S^{\mathbf{i}}_{\mathbf{u}+\mathbf{v}}.
\end{aligned}$$

Data l'arbitrarietà di $\mathbf{x^u} \otimes \mathbf{x^v}$, il confronto dei due calcoli precedenti dà la (9). ∎

Talvolta - nel considerare la sottocoalgebra $C_{\mathbf{f}} = C_J$ - l'attenzione viene focalizzata, piuttosto che su J, sulla forma $\mathbf{f}$ di ideale massimale J. In tal caso conviene far riferimento alla base di $C_{\mathbf{f}}$ definita come segue. Per ogni $\mathbf{p} \in L$, consideriamo la forma $\mathbf{E^p f}$, che ovviamente appartiene ancora a $C_{\mathbf{f}} = C_J$. Gli elementi dell'insieme $\{\mathbf{E^p f} \mid \mathbf{p} \in L\}$ sono linearmente indipendenti: in caso contrario infatti anche gli elementi di $\mathcal{L}$ dovrebbero soddisfare una relazione di ricorrenza lineare e non costituirebbero una base per $K[X]/J$. Da ciò e dal fatto che $\#L = dim(K[X]/J)$ si deduce che $\{\mathbf{E^p f} \mid \mathbf{p} \in L\}$ forma una base per $C_{\mathbf{f}}$. Vogliamo esprimere $\tilde{m}(\mathbf{f})$ - e più in generale calcolare le costanti di struttura della comoltiplicazione $\tilde{m}$ in $C_{\mathbf{f}}$ - anche rispetto a tale base.

Posto $\lambda = \#L$, associamo alla forma $\mathbf{f} = \sum_{\mathbf{i}\in\mathbf{N}^n} F_{\mathbf{i}}\mathbf{x^i} \in C_J$ la matrice Φ di tipo $\lambda \times \lambda$ così definita: sia le righe che le colonne di Φ sono indiciate su L e l'entrata $\Phi^{\mathbf{p}}_{\mathbf{q}}$ di posto $(\mathbf{p},\mathbf{q}) \in L \times L$ di Φ è data da

(10)
$$\Phi^{\mathbf{p}}_{\mathbf{q}} := F_{\mathbf{p}+\mathbf{q}} = (\mathbf{E^p f})_{\mathbf{q}} := (\mathbf{E^p f})(\mathbf{x^q}).$$

Poichè

$$(\mathbf{E^p f}) = \sum_{\mathbf{i}\in\mathbf{N}^n} F_{\mathbf{i}+\mathbf{p}}\mathbf{x^i} = \sum_{\mathbf{i}\in L} F_{\mathbf{i}+\mathbf{p}}\mathbf{s^i},$$

la matrice Φ rappresenta il cambiamento di base dalla base $\{\mathbf{s^i} \mid \mathbf{i} \in L\}$ alla base $\{\mathbf{E^p f} \mid \mathbf{p} \in L\}$ in $C_{\mathbf{f}}$. Denotiamo $\Psi = (\Psi^{\mathbf{p}}_{\mathbf{q}})$ $(\mathbf{p},\mathbf{q} \in L)$ la matrice inversa della Φ:

$$\sum_{\mathbf{q}\in L} \Psi^{\mathbf{p}}_{\mathbf{q}} F_{\mathbf{q}+\mathbf{t}} = \delta^{\mathbf{p}}_{\mathbf{t}} \quad ,$$

per cui

$$\mathbf{s}^{\mathbf{p}} = \sum_{\mathbf{i}\in L} \Psi^{\mathbf{p}}_{\mathbf{i}}(\mathbf{E}^{\mathbf{i}}\mathbf{f}). \tag{11}$$

La proposizione seguente dà un algoritmo per diagonalizzare una forma ricorrente n-lineare. Nel caso n=1, si ottiene un risultato di Peterson e Taft (cfr [3], p. 8)

Proposizione 3.

$$\tilde{m}(\mathbf{f}) = \sum_{\mathbf{p},\mathbf{q}\in L} \Psi^{\mathbf{p}}_{\mathbf{q}}(\mathbf{E}^{\mathbf{p}}\mathbf{f}) \otimes (\mathbf{E}^{\mathbf{q}}\mathbf{f}). \tag{12}$$

DIMOSTRAZIONE:

$$\begin{aligned}
\tilde{m}(\mathbf{f}) &= \tilde{m}\Big(\sum_{\mathbf{i}\in L} F_{\mathbf{i}}\mathbf{s}^{\mathbf{i}}\Big) = \quad \text{(per la Prop.2)}\\
&= \sum_{\mathbf{i}\in L} F_{\mathbf{i}}\Big(\sum_{\mathbf{d},\mathbf{p}\in L} S^{\mathbf{i}}_{\mathbf{d}+\mathbf{p}}\mathbf{s}^{\mathbf{d}} \otimes \mathbf{s}^{\mathbf{p}}\Big) = \sum_{\mathbf{d},\mathbf{p}\in L}\Big(\sum_{\mathbf{i}\in L} F_{\mathbf{i}} S^{\mathbf{i}}_{\mathbf{d}+\mathbf{p}}\Big)\mathbf{s}^{\mathbf{d}} \otimes \mathbf{s}^{\mathbf{p}} = \qquad \text{(per la (7))}\\
&= \sum_{\mathbf{d},\mathbf{p}\in L} F_{\mathbf{d}+\mathbf{p}}\mathbf{s}^{\mathbf{d}} \otimes \mathbf{s}^{\mathbf{p}} = \sum_{\mathbf{p}\in L}\Big(\sum_{\mathbf{d}\in L} F_{\mathbf{d}+\mathbf{p}}\mathbf{s}^{\mathbf{d}}\Big) \otimes \mathbf{s}^{\mathbf{p}} =\\
&= \sum_{\mathbf{p}\in L}(\mathbf{E}^{\mathbf{p}}\mathbf{f}) \otimes \mathbf{s}^{\mathbf{p}} = \sum_{\mathbf{p}\in L}(\mathbf{E}^{\mathbf{p}}\mathbf{f}) \otimes \Big(\sum_{\mathbf{q}\in L} \Psi^{\mathbf{p}}_{\mathbf{q}}(\mathbf{E}^{\mathbf{q}}\mathbf{f})\Big) =\\
&= \sum_{\mathbf{p},\mathbf{q}\in L} \Psi^{\mathbf{p}}_{\mathbf{q}}(\mathbf{E}^{\mathbf{p}}\mathbf{f}) \otimes (\mathbf{E}^{\mathbf{q}}\mathbf{f}). \ \blacksquare
\end{aligned}$$

Infine con un calcolo simile al precedente si trova l'uguaglianza

$$\tilde{m}(\mathbf{E}^{\mathbf{i}}\mathbf{f}) = \sum_{\mathbf{p},\mathbf{q}\in L}\Big(\sum_{\mathbf{c},\mathbf{d}\in L} F_{\mathbf{i}+\mathbf{c}+\mathbf{d}}\Psi^{\mathbf{c}}_{\mathbf{p}}\Psi^{\mathbf{d}}_{\mathbf{q}}\Big)(\mathbf{E}^{\mathbf{p}}\mathbf{f}) \otimes (\mathbf{E}^{\mathbf{q}}\mathbf{f}) \tag{13}$$

che si riduce alla (12) per $\mathbf{i} = (0,\ldots,0)$.

4. Base associata alla varietà $\mathcal{V}(J)$.

Assegnato, per ogni indeterminata $x_j \in K[X]$, un polinomio $\gamma_j(x_j)$ nella sola indeterminata x_j, consideriamo l'ideale $\Gamma = (\gamma_1,\ldots,\gamma_n) \subseteq K[X]$, generato da tali polinomi; nel seguito chiameremo ideale elementare ogni ideale di questa forma. Posto $h_j := deg(\gamma_j)$, le classi di equivalenza $mod.\Gamma$ dei monomi $\mathbf{x}^{\mathbf{i}}$ per $\mathbf{i} \leq (h_1,\ldots,h_n)$ costituiscono una base per l'algebra quoziente $K[X]/\Gamma$. Ne consegue che

$$h := h_1 \ldots h_n = codim(\Gamma).$$

Lemma. *Un ideale J di $K[X]$ è cofinito se e solo se contiene un ideale elementare $\Gamma = (\gamma_1, \dots, \gamma_n)$.*

DIMOSTRAZIONE: Se $\Gamma \subseteq J$ allora $K[X]/J$ si immerge canonicamente in $K[X]/\Gamma$ e quindi $codim(J) \leq codim(\Gamma) < \infty$.

Viceversa se J è cofinito allora, per ogni $j \in \{1, \dots, n\}$, le classi di equivalenza, modulo J, dei monomi $1, x_j, x_j^2, \dots$ non sono linearmente indipendenti in $K[X]/J$; se indichiamo con $\gamma_j(x_j)$ il generatore dell'ideale principale $J \cap K[x_j] \neq \{0\}$, allora l'ideale elementare $\Gamma := (\gamma_1, \dots, \gamma_n)$ è contenuto in J. ∎

Dato un ideale cofinito J e indicata con $\Gamma = (\gamma_1, \dots, \gamma_n)$ l'ideale elementare massimale contenuto in J, i punti di $\mathcal{V}(J)$ vanno ricercati tra i punti $P = (a_1, \dots, a_n)$ per cui $\gamma_j(a_j) = 0$, $j = 1, \dots, n$. Viceversa se, per qualche j, $\gamma_j(a) = 0$ allora esiste almeno un punto di $\mathcal{V}(J)$ avente il valore a per j–esima coordinata. Si ha inoltre

$$\#(\mathcal{V}(J)) \leq codim(J) \leq codim(\Gamma) = h.$$

Va notato che, dato un sistema di generatori per l'ideale J di $K[X]$, la teoria delle basi di Groebner (cfr. [5]) fornisce algoritmi per decidere se J è cofinito e, se ciò si verifica, per determinare i generatori $\gamma_1, \dots, \gamma_n$ dell'ideale elementare massimale contenuto in J. In effetti, sia $\mathcal{G}_{\preceq} = (g_1, \dots, g_s)$ ($g_i \in K[X]$) una base di Groebner (ridotta) per J con riferimento ad un qualunque buon ordine $\preceq$ su $\mathbf{N}^n$, compatibile con l'usuale struttura di monoide di $\mathbf{N}^n$. Posto $M := \{\mathbf{x}^{\mathbf{i}} \mid \mathbf{i} \in \mathbf{N}^n\}$ e indicata con $\mathbf{m}_r \in M$ la parte letterale del "monomio direttore" (rispetto a $\preceq$) di $g_r \in \mathcal{G}_{\preceq}$, l'insieme:

$$\mathcal{L} := \{[\mathbf{x}^{\mathbf{i}}]_J \mid \mathbf{x}^{\mathbf{i}} \in M - \cup_{r=1}^{s} \mathbf{m}_r M\} \subseteq K[X]/J$$

costituisce una base per $K[X]/J$. Ne consegue che J è cofinito se e solo se – per ogni $j = 1, \dots, n$ – uno degli $\mathbf{m}_r$ è una potenza di x_j. Inoltre, per ogni fissato $j = 1, \dots, n$, sia $\preceq_j$ l'ordine lessicografico su M (o equivalentemente su $\mathbf{N}^n$) per il quale $x_j \preceq_j x_i$ per ogni $i \neq j$; allora uno dei generatori della base di Groebner $\mathcal{G}_{\preceq_j}$ di J è il polinomio $\gamma_j(x_j)$ dell'ideale elementare $\Gamma \subseteq J$.

Dal Lemma precedente consegue immediatamente la

Proposizione 4. *Un elemento $\mathbf{f} \in K[X]^*$ è una forma ricorrente n–lineare se e solo se il suo nucleo contiene un ideale elementare $\Gamma := (\gamma_1, \dots, \gamma_n)$ di $K[X]$, cioè, posto $\gamma_j(x_j) = x_j^{h_j} - a_{h_j-1,j} x_j^{h_j-1} - \dots - a_{1,j} x_j - a_{0,j}$ e $\varphi_{j,m} = E_j^m \gamma_j(\mathbf{E})$, se e solo se $\mathbf{f}$ soddisfa alle n relazioni di ricorrenza lineare:*

$$\varphi_{j,m}(\mathbf{f})(\mathbf{x}^{\mathbf{i}}) = \mathbf{f}(\mathbf{x}^{\mathbf{i}} x_j^m \gamma_j) = \mathbf{f}(x_j^{m+h_j} \mathbf{x}^{\mathbf{i}}) - a_{h_j-1,j} \mathbf{f}(x_j^{m+h_j-1} \mathbf{x}^{\mathbf{i}}) - \dots - a_{1j} \mathbf{f}(x_j^{m+1} \mathbf{x}^{\mathbf{i}}) - a_{0,j} \mathbf{f}(x_j^m \mathbf{x}^{\mathbf{i}}) = 0$$

per ogni $j = 1, \dots, n$ e qualunque siano $m \in \mathbf{N}$ e $\mathbf{i} \in \mathbf{N}^n$. ∎

Assunto come ideale elementare Γ l'ideale elementare massimale contenuto nel nucleo di una data forma $\mathbf{f} \in K[X]$, osserviamo esplicitamente che – in virtù della loro linearità – le relazioni di ricorrenza precedenti consentono un agevole calcolo della $\mathbf{f}$, una volta noti i valori assunti da essa negli $h := h_1 \dots h_n$ monomi $\mathbf{x}^{\mathbf{i}}$ per $\mathbf{i} \leq (h_1, \dots, h_n)$; va anche sottolineato tuttavia che in generale tali valori iniziali non possono essere scelti ad arbitrio, ma – se l'ideale massimale J di $\mathbf{f}$ contiene propriamente Γ – devono soddisfare ulteriori relazioni.

Per una coalgebra $C_\Gamma \subseteq \mathcal{B}_n^\circ$ relativa ad un ideale elementare $\Gamma = (\gamma_1, \ldots, \gamma_n)$ possiamo introdurre una ulteriore base, analoga alla cosiddetta "base delle radici" (cfr. [4] p.76, b)) del caso in una indeterminata. Se $P = (\rho_1, \ldots, \rho_n) \in \mathcal{V}(\Gamma)$, sia m_j la molteplicità della radice ρ_j di γ_j e poniamo

$$\mathbf{m}(P) := (m_1 - 1, \ldots, m_n - 1).$$

Per ogni $P \in \mathcal{V}(\Gamma)$ e ogni $\mathbf{i} \leq \mathbf{m}(P)$ sia

$$\begin{aligned} v_{P,\mathbf{i}} : K[X] &\longrightarrow K \\ q &\longmapsto v_{P,\mathbf{i}}(q) := (\mathbf{D}^{\mathbf{i}} q)(P) \end{aligned}$$

dove

$$\mathbf{D}^{\mathbf{i}} = \frac{\partial^{i_1 + \cdots + i_n}}{\partial^{i_1} x_1 \ldots \partial^{i_n} x_n}, \qquad \mathbf{i} = (i_1, \ldots, i_n)$$

(in altri termini: $v_{P,\mathbf{i}}$ è la composizione dell'applicazione lineare $\mathbf{D}^{\mathbf{i}}$ con la valutazione in P).

È facile verificare che l'insieme

$$\{v_{P,\mathbf{i}} \mid P \in \mathcal{V}(\Gamma), \mathbf{i} \leq \mathbf{m}(P)\}$$

forma una base per C_Γ.

Per ogni $\mathbf{f}, \mathbf{g} \in \mathcal{B}_n^\circ$ indichiamo con $\mathcal{V}_\mathbf{f}$ la varietà dell'ideale massimale di $\mathbf{f}$ e scriviamo $\mathbf{f} * \mathbf{g}$ in luogo di $\widetilde{\Delta}(\mathbf{f} \otimes \mathbf{g})$. Inoltre dati due punti $P = (\rho_1, \ldots, \rho_n)$ e $Q = (\sigma_1, \ldots, \sigma_n)$ di K^n indichiamo con $P + Q$ il punto $(\rho_1 + \sigma_1, \ldots, \rho_n + \sigma_n)$ e poniamo $A + B := \{P + Q \mid P \in A \, \mathrm{e} \, Q \in B\}$ per due sottoinsiemi arbitrari A e B di K^n. Ciò premesso proviamo la

Proposizione 5.

$$v_{P,\mathbf{i}} * v_{Q,\mathbf{j}} = v_{P+Q,\mathbf{i}+\mathbf{j}}.$$

DIMOSTRAZIONE: Posto $[s]_i := s(s-1)\ldots(s-i+1)$, un calcolo diretto dà:

$$\begin{aligned}
&(v_{P,\mathbf{i}} * v_{Q,\mathbf{j}})(\mathbf{x}^{\mathbf{s}}) = \quad \text{(per la seconda delle (4))} \\
&= \sum_{\mathbf{t} \leq \mathbf{s}} \binom{\mathbf{s}}{\mathbf{t}} v_{P,\mathbf{i}}(\mathbf{x}^{\mathbf{t}}) \, v_{Q,\mathbf{j}}(\mathbf{x}^{\mathbf{s}-\mathbf{t}}) = \\
&= \prod_{\alpha=1}^{n} \sum_{t_\alpha=0}^{s_\alpha} \binom{s_\alpha}{t_\alpha} [t_\alpha]_{i_\alpha} [s_\alpha - t_\alpha]_{j_\alpha} \rho_\alpha^{t_\alpha - i_\alpha} \sigma_\alpha^{s_\alpha - t_\alpha - j_\alpha} = \\
&= \prod_{\alpha=1}^{n} \sum_{t_\alpha = i_\alpha}^{s_\alpha - j_\alpha} \frac{s_\alpha!}{(t_\alpha - i_\alpha)!(s_\alpha - j_\alpha - t_\alpha)!} \rho_\alpha^{t_\alpha - i_\alpha} \sigma_\alpha^{s_\alpha - t_\alpha - j_\alpha} = \\
&\text{(ponendo } u_\alpha := t_\alpha - i_\alpha) \\
&= \prod_{\alpha=1}^{n} [s_\alpha]_{i_\alpha + j_\alpha} \sum_{u_\alpha=0}^{s_\alpha - i_\alpha - j_\alpha} \binom{s_\alpha - i_\alpha - j_\alpha}{u_\alpha} \rho_\alpha^{u_\alpha} \sigma_\alpha^{s_\alpha - i_\alpha - j_\alpha - u_\alpha} = \\
&= \prod_{\alpha=1}^{n} [s_\alpha]_{i_\alpha + j_\alpha} (\rho_\alpha + \sigma_\alpha)^{s_\alpha - i_\alpha - j_\alpha} = \\
&= v_{P+Q,\mathbf{i}+\mathbf{j}}(\mathbf{x}^{\mathbf{s}}). \quad \blacksquare
\end{aligned}$$

Corollario. *Siano* $\mathbf{f}, \mathbf{g} \in \mathcal{B}_n^\circ$; *allora*

$$\mathcal{V}_{\mathbf{f}*\mathbf{g}} = \mathcal{V}_{\mathbf{f}} + \mathcal{V}_{\mathbf{g}}. \quad \blacksquare$$

5. Funzioni generatrici.

Vogliamo ora descrivere la "funzione generatrice" di una forma ricorrente n–lineare. A tale scopo indichiamo con $\widetilde{q}(x_1, \ldots, x_n)$ il polinomio "reciproco" del polinomio $q(x_1, \ldots, x_n)$, cioè il polinomio $\widetilde{q} = x_1^{d_1} \ldots x_n^{d_n} q(x_1^{-1}, \ldots, x_n^{-1})$, dove si è indicato con d_i il grado di q rispetto a x_i. Ricordiamo che nel caso $n = 1$ le funzioni generatrici sono le funzioni razionali. Più precisamente se $f = (F_i)_{i \in \mathbf{N}}$ è una successione ricorrente lineare avente per polinomio minimale $\gamma(x)$ (cioè, per ideale massimale l'ideale $(\gamma) \subseteq K[x]$) allora si ha

$$f = \sum_{i \in \mathbf{N}} F_i x^i = \frac{a_0 + \cdots + a_{h-1} x^{h-1}}{\widetilde{\gamma}(x)} \qquad h := deg(\gamma) \tag{14}$$

dove il polinomio a numeratore è univocamente determinato dalla f. Viceversa ogni frazione della forma in (14) determina univocamente un elemento f di $C_{(\gamma)}$. Nel caso in più variabili la situazione è un po' più complessa. In generale si può intanto osservare che ogni funzione razionale

$$\frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} \qquad \text{con } q(0, \ldots, 0) \neq 0$$

(sotto opportune condizioni per il numeratore sulle quali è inutile soffermarsi) genera una forma $f = (F_{\mathbf{i}})_{\mathbf{i} \in \mathbf{N}^n}$:

$$\frac{p}{q} = \sum_{\mathbf{i} \in \mathbf{N}^n} F_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}$$

il cui nucleo $Ker(\mathbf{f})$ contiene l'ideale principale $(\widetilde{q})$ –ma in generale $Ker(f)$ <u>non</u> conterrà <u>anche</u> un ideale cofinito. La seguente Proposizione 6 assicura che, perchè ciò avvenga, <u>occorre</u> (e basta) richiedere che il denominatore q possa decomporsi in un prodotto della forma $q = q_1(x_1) \ldots q_n(x_n)$ e che, posto $k_i = deg(q_i) - 1$ e $\mathbf{k} = (k_1, \ldots, k_n)$, il numeratore sia della forma

$$p(x_1, \ldots, x_n) = \sum_{\mathbf{i} \leq \mathbf{k}} p_{\mathbf{i}} x^{\mathbf{i}} \qquad p_{\mathbf{i}} \in K.$$

In corrispondenza ad un fissato ideale $\Gamma = (\gamma_1, \ldots, \gamma_n)$, indichiamo con S_Γ lo spazio di tutte le funzioni razionali della forma

$$\frac{\sum_{\mathbf{i} \leq \mathbf{m}(\Gamma)} a_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}}{\widetilde{\gamma}_1(x_1) \ldots \widetilde{\gamma}_n(x_n)} \tag{15}$$

dove $\mathbf{m}(\Gamma) := (h_1 - 1, \ldots, h_n - 1)$ e $a_{\mathbf{i}} \in K$. Si ha allora la

Proposizione 6. *L'usuale sviluppo in serie di potenze determina un isomorfismo di spazi vettoriali da S_Γ a C_Γ.*

DIMOSTRAZIONE: Poichè $dim_K(S_\Gamma) = h_1 \dots h_n = dim_K(C_\Gamma)$ è sufficiente provare che ogni elemento $\mathbf{f} = \sum_{\mathbf{i}\in\mathbf{N}^n} F_\mathbf{i}\mathbf{x}^\mathbf{i}$ può essere scritto in uno ed un solo modo nella forma (15). Si è già osservato che si ha:

$$C_\Gamma = C_{(\gamma_1)} \otimes \dots \otimes C_{(\gamma_n)}, \qquad C_{(\gamma_i)} \subseteq K[x_i]$$

e che ogni elemento f_i di $C_{(\gamma_i)}$ è della forma

$$f_i = \frac{p_i(x_i)}{\tilde{\gamma}_i(x_i))}$$

con $deg(p_i) < h_i$.

Indicata con $\{r^{ij} \mid j = 0, \dots, h_i - 1\}$ una base per $C_{(\gamma_i)}$, $(i = 1, \dots, n)$, e con

$$\frac{p_{ij}(x_j)}{\tilde{\gamma}_j(x_j)}$$

la funzione generatrice di r^{ij}, si ha, per opportuni coefficienti $A_{j_1,\dots,j_n}$,

$$\begin{aligned}\mathbf{f} &= \sum_{(j_1,\dots,j_n)\leq \mathbf{m}(\Gamma)} A_{j_1,\dots,j_n} r^{1j_1} \otimes \dots \otimes r^{nj_n} = \\ &= \sum_{(j_1,\dots,j_n)\leq \mathbf{m}(\Gamma)} A_{j_1,\dots,j_n} \frac{p_{1j_1} \cdots p_{nj_n}}{\tilde{\gamma}_1 \cdots \tilde{\gamma}_n}\end{aligned}$$

che è proprio della forma (15). ∎

Per quanto concerne gli elementi $\mathbf{f}$ di C_J, va osservato che anche questi ammettono una funzione generatrice della forma (15), in relazione al più grande ideale elementare Γ contenuto in J. Ciò è una conseguenza immediata della Prop.6 e del fatto che $C_J \subseteq C_\Gamma$. Va solo aggiunto che in tal caso i coefficienti del numeratore in (15) non sono più completamente arbitrari ma dovranno soddisfare a $h - codim(J)$ equazioni lineari indipendenti.

BIBLIOGRAFIA

[1] M. F. Sweedler, "Hopf Algebras," Benjamin, New York, 1969.

[2] E. Abe, "Hopf Algebras," Cambridge University Press, Cambridge, 1980.

[3] B. Peterson, E. J. Taft, *The Hopf algebra of linearly recursive sequences*, Aeq. Math. 20 (1980), 1–17.

[4] L. Cerlienco, M. Mignotte, F. Piras, *Suites récurrentes linéaires. Propriétés algébriques et arithmétiques*, L'Enseignement Math 33 (1987), 67–108.

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