CAPITOLO VII. ELIMINANDO ED ESTENDENDO
PARTE 2. TEORIA DEL RISULTANTE

Si introduce qui la nozione di risultante di due polinomi in una o più indeterminate (e una generalizzazione di tale concetto): questa parte può essere omessa in prima lettura pur di tener conto dei risultati delle proposizioni 3.2, 4.2, 4.4 e 5.4.

3. TEORIA DEL RISULTANTE in $k[x]$

Abbiamo appena visto che l'ottica che ci permetterà di garantire l'estendibilità di soluzioni è quella di pensare ogni polinomio di $\mathbf{C}[x_1,\ldots,x_n]$ come un polinomio in x_1 a coefficienti in $\mathbf{C}[x_2,\ldots,x_n]$, cioè di utilizzare l'isomorfismo tra $\mathbf{C}[x_1,\ldots,x_n]$ e $\mathbf{C}[x_2,\ldots,x_n][x_1]$. Abbiamo anche visto che una volta sostituite le soluzioni $(c_2,\ldots,c_n)$ nelle equazioni contenenti x_1 si ha il sistema

$$g_1(x_1, c_2, \ldots, c_n) = 0, \ldots\ldots, g_r(x_1, c_2, \ldots, c_n) = 0,$$

le cui soluzioni sono le radici del massimo comun divisore e quindi è abbastanza logico che per dimostrare il teorema ci serva una teoria in grado di evidenziare fattori comuni di uno o più polinomi. L'algoritmo euclideo si mostra poco duttile proprio perché lavoriamo in astratto, cercando fattori comuni in $\mathbf{C}[x_2,\ldots,x_n][x_1]$.

Per individuare un nuovo strumento che permetta di stabilire se due polinomi hanno fattori comuni, cominciamo ad esaminare il caso in cui l'indeterminata è una sola.
Si sa che in $k[x]$ due polinomi f e g sono primi tra loro se e solo se esistono due polinomi a e b tali che $af+bg=1$. Anzi, applicando l'algoritmo euclideo si vede che si possono scegliere a e b in modo che il grado di a sia minore del grado di g e quello di b sia minore del grado di f (cfr. esercizio 3 negli Esercizi sul CAPITOLO VII). Questo suggerisce che due polinomi con un fattore comune possano essere legati da una proprietà simile. Possiamo in realtà essere molto precisi:

LEMMA 3.1 *Siano f e g polinomi di $k[x]$ di gradi rispettivamente l e m, entrambi >0. Essi hanno un fattore comune di grado >0 se e solo se esistono* A *e* B *in $k[x]$ tali che:*

i) A *e* B *non sono entrambi nulli*
ii) A *ha grado al più $m-1$ e* B *ha grado al più $l-1$*
iii) $Af+Bg=0$.

Le prime due richieste, che mimano quanto succede nel caso di polinomi primi tra loro, servono a evitare situazioni banali come $0f+0g=0$ oppure $gf+(-f)g=0$.

Dimostrazione Sia h un polinomio di grado >0 tale che $f=hf^*$ e $g=hg^*$: allora il grado di f^* è al più $l-1$ e il grado di g^* è al più $m-1$; d'altra parte $g^*f+(-f^*)g=0$.
Viceversa, se esistono A e B con le proprietà indicate e in particolare B non è nullo, i due polinomi non possono essere primi tra loro; infatti in caso contrario esisterebbero a e b tali che $af+bg=1$; moltiplicando per B e tenuto conto che $Bg = -Af$ si avrebbe: $Baf-Abf = (Ba-Ab)f = B$. Ma f non può dividere B, visto che il grado di B è minore e d'altra parte $Ba-Ab$ non può essere nullo, visto che moltiplicato per f dà B che per ipotesi è diverso da 0. C.V.D.

Questo lemma garantisce inoltre che se due polinomi f e g di $k[x]$ sono invece primi tra loro, i polinomi a e b rispettivamente di grado minore del grado di g e di quello di f tali che $af+bg=1$ sono univocamente determinati. Infatti da $cf+dg=1$ si ricava $(a-c)f+(b-d)g=0$ e, se anche c e d hanno rispettivamente grado minore del grado di g e di quello di f, la stessa cosa succede per le differenze $(a-c)$ e $(b-d)$ che devono quindi essere nulle, altrimenti i polinomi f e g non sarebbero primi tra loro.

Il problema, tanto nel caso in cui f e g sono primi tra loro che nell'altro, è quello di determinare i polinomi che soddisfano l'equazione

(*) $$Af+Bg = \delta$$

ove δ a seconda dei casi vale 1 o 0. Se

$$f = a_0x^l+\ldots+a_l, \qquad g = b_0x^m+\ldots+b_m,$$

ove per ipotesi $a_0\neq0$ e $b_0\neq0$ e $l>0$, $m>0$, indicati con

$$A = c_0x^{m-1}+\ldots+c_{m-1}, \quad B = d_0x^{l-1}+\ldots+d_{l-1}$$

i due polinomi incogniti (ove eventualmente possono essere nulli i primi coefficienti, poiché non è detto che il grado sia massimo), si vede che la (*) si traduce in un sistema lineare nelle $m+l$ incognite $c_0,\ldots,c_{m-1}$, $d_0,\ldots,d_{l-1}$, avente $l+m$ equazioni (corrispondenti al grado dei polinomi prodotto Af e Bg e quindi al numero di coefficienti da prendere in esame). Visto che la somma in entrambi i casi è una costante, le prime $l+m-1$ equazioni (corrispondenti ai coefficienti dei monomi di grado da $l+m-1$ a 1) sono omogenee, mentre l'ultima lo è o no in dipendenza dal caso:

$$\begin{aligned}
&a_0\,c_0+ && b_0\,d_0 && =0\\
&a_1\,c_0+a_0\,c_1+ && b_1\,d_0+b_0\,d_1 && =0\\
&\ldots\ldots\ldots\ldots\\
& && a_l\,c_{m-2}+a_{l-1}\,c_{m-1}+b_m\,d_{l-2}+b_{m-1}\,d_{l-1} && =0\\
& && a_l\,c_{m-1}+ && b_m\,d_{l-1} =\delta
\end{aligned}$$

La soluzione del sistema (quadrato di ordine $l+m$) è diversa nelle due situazioni, ma in entrambi i casi entra in gioco il determinante della matrice dei coefficienti, che (se ad es. $l>m$) ha la forma:

$$\left(\begin{array}{ccccc|ccccccc}
a_0 & 0 & 0 & \cdots & 0 & b_0 & 0 & 0 & \cdots & 0 & \cdots & 0\\
a_1 & a_0 & 0 & \cdots & 0 & b_1 & b_0 & 0 & \cdots & 0 & \cdots & 0\\
a_2 & a_1 & a_0 & \cdots & 0 & b_2 & b_1 & b_0 & \cdots & 0 & \cdots & 0\\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & & & \vdots\\
a_{m-1} & & & \cdots & a_0 & b_{m-1} & & & \cdots & b_0 & \cdots & 0\\
a_m & a_{m-1} & & \cdots & a_1 & b_m & b_{m-1} & & \cdots & b_1 & \cdots & 0\\
\hline
a_{m+1} & a_m & a_{m-1} & \cdots & a_2 & 0 & b_m & b_{m-1} & \cdots & b_2 & \cdots & 0\\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & & \vdots & & \vdots\\
a_l & a_{l-1} & a_{l-2} & \cdots & & 0 & 0 & 0 & \cdots & & & b_0\\
0 & a_l & a_{l-1} & \cdots & & 0 & 0 & 0 & \cdots & & & b_1\\
0 & 0 & a_l & \cdots & & 0 & 0 & 0 & \cdots & & & b_2\\
\vdots & \vdots & \vdots & \ddots & & \vdots & \vdots & \vdots & & & & \vdots\\
0 & 0 & 0 & \cdots & a_l & 0 & 0 & 0 & \cdots & 0 & \cdots & b_m
\end{array}\right) := \mathrm{Syl}(f,g,x)$$

Tale matrice Syl(f,g,x) dipende unicamente dai coefficienti e dal grado di f e g ed è nota come **matrice di Sylvester di *f* e *g* rispetto a *x***. Per costruirla comodamente conviene osservare che essa si ottiene accostando - facendole scivolare ogni volta di 1 verso il basso - m colonne dei coefficienti di f e accostando loro l colonne dei coefficienti di g, anch'esse ogni volta spostate verso il basso, e riempiendo quel che rimane con 0.

Il determinante della matrice di Sylvester è noto come **risultante di *f* e *g* rispetto a *x***: Res(f,g,x). Per come si calcola, è un elemento di k e risulta essere un polinomio a coefficienti interi nei coefficienti dei due polinomi f e g.

Tornando al problema di determinare i polinomi A e B, osserviamo che il sistema omogeneo che nasce dall'equazione $Af+Bg=0$ ha soluzioni non banali (ma non uniche!) solo se Res(f,g,x)=0.

Invece il sistema non omogeneo che nasce dall'equazione $Af+Bg=1$ ha soluzione (unica per quanto osservato dopo il lemma 3.1) se e solo se Res(f,g,x)$\neq$0.

Inoltre la regola di Cramer per la soluzione di sistemi quadrati con determinante diverso da zero dice che ogni incognita $c_0,\ldots,c_{m-1}$, $d_0,\ldots,d_{l-1}$ (cioè ogni coefficiente di A e di B) è il rapporto tra il determinante della matrice che si ottiene sostituendo nella matrice di Sylvester la colonna corrispondente all'incognita con la colonna dei termini noti $((0,0,\ldots,0,1)^T)$ e il risultante e quindi è in ogni caso il rapporto tra un polinomio in $a_0,\ldots,a_l$, $b_0,\ldots,b_m$ e il risultante.
Moltiplicando per Res(f,g,x) si possono eliminare i denominatori [11]

$$[\mathrm{A}\cdot\mathrm{Res}(f,g,x)]f+[\mathrm{B}\cdot\mathrm{Res}(f,g,x)]g = \mathrm{Res}(f,g,x)$$

e rinominando [A·Res(f,g,x)]:=A e [B·Res(f,g,x)]:=B si mette in luce che tanto il caso in cui f e g hanno fattore comune quanto il caso in cui non l'hanno possono essere descritti da una stessa formula, che in sostanza dice che il risultante appartiene all'ideale generato da f e g. Di più, in entrambi i casi vale la seguente

PROPOSIZIONE 3.2 *Dati f, g in k*[x] *di grado* >0, *esistono due polinomi* A, B *in k*[x], *di grado rispettivamente minore del grado di g e di quello di f tali che*

$$\mathrm{A}f+\mathrm{B}g = \mathrm{Res}(f,g,x)$$

e i coefficienti di A *e di* B *sono polinomi a coefficienti interi nei coefficienti* $a_0,\ldots,a_l$, $b_0,\ldots,b_m$ *di f e g.*

Dimostrazione L'enunciato è appena stato provato nel caso in cui non ci sono fattori comuni. Se ci sono fattori comuni la matrice di Sylvester ha rango $r<l+m$: quindi il sistema si risolve mettendo in evidenza r righe e colonne indipendenti della matrice di Sylvester, scartando le rimanenti righe e considerando la somma delle rimanenti $l+m-r$ colonne moltiplicate per le corrispondenti incognite come colonna dei termini noti (a meno del segno). Quindi $l+m-r$ incognite funzionano come parametri $t_1,\ldots,t_{l+m-r}$ all'interno dei vettori soluzione, mentre le restanti componenti delle soluzioni si otterranno ancora applicando il metodo di Cramer a un sistema $r\times r$, in cui la colonna di termini noti, invece di essere $(0,0,\ldots,0,1)^T$ come nel caso precedente, sarà una combinazione lineare (mediante gli $l+m-r$ parametri) di colonne contenenti i coefficienti $a_0,\ldots,a_l,b_0,\ldots,b_m$: per la multi-linearità del determinante, il numeratore risulterà una combinazione lineare $p_1\cdot t_1+\ldots+p_{l+m-r}\cdot t_{l+m-r}$, tramite i parametri $t_1,\ldots,t_{l+m-r}$, di polinomi a coefficienti interi in $a_0,\ldots,a_l,b_0,\ldots,b_m$, mentre il denominatore (determinante della matrice quadrata di ordine r del sistema) sarà un polinomio p a coefficienti interi in $a_0,\ldots,a_l,b_0,\ldots,b_m$. Visto che ci interessa una soluzione (non tutte le possibili soluzioni), si può scegliere ad esempio di porre $t_1=p$, $t_2=\ldots=t_{l+m-r}=0$: con ciò si evidenzia che tutte le incognite possono essere rappresentate come polinomi a coefficienti interi in $a_0,\ldots,a_l$, $b_0,\ldots,b_m$. Si mostreranno i dettagli nell'esempio successivo. C.V.D.

ESEMPIO 3.3 Cerchiamo A e B nel caso dei due polinomi

$$f = 2x^3+10x^2+6x-18 \quad \text{e} \quad g = -x^3-8x^2-21x-18.$$

La matrice di Sylvester:

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} 2 & 0 & 0 & -1 & 0 & 0 \\ 10 & 2 & 0 & -8 & -1 & 0 \\ 6 & 10 & 2 & -21 & -8 & -1 \\ -18 & 6 & 10 & -18 & -21 & -8 \\ 0 & -18 & 6 & 0 & -18 & -21 \\ 0 & 0 & -18 & 0 & 0 & -18 \end{pmatrix}$$

ha rango ≥3, poiché la matrice formata con le prime 3 righe e colonne ha determinante 8, anzi ha rango 4, poiché (il metodo di Gauss-Jordan evidenzia una coppia di righe nulle … oppure poiché)

[11] L'importanza di eliminare i denominatori sarà evidente quando si passerà ad esaminare il caso $n>1$.

$$\begin{vmatrix} 2 & 0 & 0 & 0 \\ 10 & 2 & 0 & 0 \\ 6 & 10 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 \\ 10 & 2 & 0 & 0 \\ 6 & 10 & 3 & -1 \\ 0 & 0 & 0 & -18 \end{vmatrix} = -6^3 \neq 0$$

mentre le 4 matrici quadrate di ordine 5 ottenute orlando questa sono nulle, come si vede - quando la colonna aggiunta è la quinta di Syl(*f*, *g*, *x*) - sommando alla quarta colonna metà della seconda e sottraendo la quinta colonna dalla terza:

$$\begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 10 & 2 & 0 & -1 & 0 \\ 6 & 10 & 2 & -8 & -1 \\ -18 & 6 & 10 & -21 & -8 \\ 0 & 0 & -18 & 0 & -18 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 10 & 2 & 0 & 0 & 0 \\ 6 & 10 & 3 & -3 & -1 \\ -18 & 6 & 18 & -18 & -8 \\ 0 & 0 & 0 & 0 & -18 \end{vmatrix} = 0, \quad \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 10 & 2 & 0 & -1 & 0 \\ 6 & 10 & 2 & -8 & -1 \\ 0 & -18 & 6 & -18 & -21 \\ 0 & 0 & -18 & 0 & -18 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 10 & 2 & 0 & 0 & 0 \\ 6 & 10 & 3 & -3 & -1 \\ 0 & -18 & 27 & -27 & -21 \\ 0 & 0 & 0 & 0 & -18 \end{vmatrix} = 0$$

e - quando la colonna aggiunta è la quarta di Syl(*f*, *g*, *x*) - sottraendo la quinta colonna dalla terza e sommando il risultato più metà della somma delle prime due alla quarta colonna:

$$\begin{vmatrix} 2 & 0 & 0 & -1 & 0 \\ 10 & 2 & 0 & -8 & 0 \\ 6 & 10 & 2 & -21 & -1 \\ -18 & 6 & 10 & -18 & -8 \\ 0 & 0 & -18 & 0 & -18 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 10 & 2 & 0 & -2 & 0 \\ 6 & 10 & 3 & -10 & -1 \\ -18 & 6 & 18 & -6 & -8 \\ 0 & 0 & 0 & 0 & -18 \end{vmatrix} = 0, \quad \begin{vmatrix} 2 & 0 & 0 & -1 & 0 \\ 10 & 2 & 0 & -8 & 0 \\ 6 & 10 & 2 & -21 & -1 \\ 0 & -18 & 6 & 0 & -21 \\ 0 & 0 & -18 & 0 & -18 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ 10 & 2 & 0 & -2 & 0 \\ 6 & 10 & 3 & -10 & -1 \\ 0 & -18 & 27 & 18 & -21 \\ 0 & 0 & 0 & 0 & -18 \end{vmatrix} = 0.$$

Si deve quindi risolvere il sistema

$$\begin{pmatrix} 2 & 0 & 0 & -1 & 0 & 0 \\ 10 & 2 & 0 & -8 & -1 & 0 \\ 6 & 10 & 2 & -21 & -8 & -1 \\ 0 & 0 & -18 & 0 & 0 & -18 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ d_0 \\ d_1 \\ d_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

pensando d_0 e d_1 come parametri, cioè risolvere

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 10 & 2 & 0 & 0 \\ 6 & 10 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ d_2 \end{pmatrix} = \begin{pmatrix} d_0 \\ 8d_0 + d_1 \\ 21d_0 + 8d_1 \\ 0 \end{pmatrix}$$

Si ha:

$$c_0 = \frac{\begin{vmatrix} d_0 & 0 & 0 & 0 \\ 8d_0 + d_1 & 2 & 0 & 0 \\ 21d_0 + 8d_1 & 10 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix}}{-6^3} = \frac{\begin{vmatrix} 1 & 0 & 0 & 0 \\ 8 & 2 & 0 & 0 \\ 21 & 10 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix} d_0 + \begin{vmatrix} 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 8 & 10 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix} d_1}{-6^3} = \frac{(2+1)2 \cdot 18}{6^3} d_0$$

$$c_1 = \frac{\begin{vmatrix} 2 & d_0 & 0 & 0 \\ 10 & 8d_0 + d_1 & 0 & 0 \\ 6 & 21d_0 + 8d_1 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix}}{-6^3} = \frac{\begin{vmatrix} 2 & 1 & 0 & 0 \\ 10 & 8 & 0 & 0 \\ 6 & 21 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix} d_0 + \begin{vmatrix} 2 & 0 & 0 & 0 \\ 10 & 1 & 0 & 0 \\ 6 & 8 & 2 & -1 \\ 0 & 0 & -18 & -18 \end{vmatrix} d_1}{-6^3} = \frac{2 \cdot 3^2 \cdot 18 d_0 + 2 \cdot 3 \cdot 18 d_1}{6^3}$$

$$c_2 = \frac{\begin{vmatrix} 2 & 0 & d_0 & 0 \\ 10 & 2 & 8d_0 + d_1 & 0 \\ 6 & 10 & 21d_0 + 8d_1 & -1 \\ 0 & 0 & 0 & -18 \end{vmatrix}}{-6^3} = \frac{\begin{vmatrix} 2 & 0 & 1 & 0 \\ 10 & 2 & 8 & 0 \\ 6 & 10 & 21 & -1 \\ 0 & 0 & 0 & -18 \end{vmatrix} d_0 + \begin{vmatrix} 2 & 0 & 0 & 0 \\ 10 & 2 & 1 & 0 \\ 6 & 10 & 8 & -1 \\ 0 & 0 & 0 & -18 \end{vmatrix} d_1}{-6^3} = \frac{2^2 \cdot 3 \cdot 18 d_0 + 2^2 \cdot 3 \cdot 18 d_1}{6^3}$$

$$d_2=\frac{\begin{vmatrix}2&0&0&d_0\\10&2&0&8d_0+d_1\\6&10&2&21d_0+8d_1\\0&0&-18&0\end{vmatrix}}{-6^3}=\frac{\begin{vmatrix}2&0&0&1\\10&2&0&8\\6&10&2&21\\0&0&-18&0\end{vmatrix}d_0+\begin{vmatrix}2&0&0&0\\10&2&0&1\\6&10&2&8\\0&0&-18&0\end{vmatrix}d_1}{-6^3}=-\frac{2^2\cdot3\cdot18d_0+2^2\cdot3\cdot18d_1}{6^3}$$

Allora ponendo ad esempio $d_0=0$ e $d_1=6^3$, si trova una possibile soluzione del problema ($c_0=0$, $c_1=2^23^3$, $c_2=2^33^3$, $d_2=-2^33^3$, e quindi

$$A=2^23^3(x+2), \qquad B=2^33^3(x-1)$$

o, più semplicemente

$$A=x+2, \qquad B=2(x-1).$$

Notare che, se $(x+2)f=2(1-x)g$, $(x+2)$ deve dividere g e $(x-1)$ deve dividere f (per il teorema di fattorizzazione unica) e gli altri fattori dei due polinomi f e g devono essere uguali: quindi si hanno indicazioni sulla fattorizzazione.

4. TEORIA DEL RISULTANTE in $k[x_1,\ldots,x_n]$

Dati due polinomi f e g in $k[x_1,\ldots,x_n]$ di grado ≥ 1 nell'indeterminata x_1, si può applicare la teoria vista nel precedente paragrafo pur di pensare i due polinomi come polinomi in x_1 a coefficienti in $k[x_2,\ldots,x_n]$

$$f=a_0x_1^{\,l}+\ldots+a_l, \qquad g=b_0x_1^{\,m}+\ldots+b_m,$$

ove $a_0\neq 0$ e $b_0\neq 0$ e $l>0$, $m>0$, e $a_0,\ldots,a_l$, $b_0,\ldots,b_m$ sono elementi di $k[x_2,\ldots,x_n]$. In realtà i risultati precedenti sono stati stabiliti per polinomi a coefficienti in un campo e non in un dominio; si può aggiustare quest'apparente pasticcio pensando $a_0,\ldots,a_l$, $b_0,\ldots,b_m$ addirittura come elementi del campo delle frazioni $k(x_2,\ldots,x_n)$ di $k[x_2,\ldots,x_n]$. In effetti le due cose sono equivalenti poiché vale il

LEMMA 4.1 *Se f e g sono polinomi di $k[x_1,\ldots,x_n]$ di grado >0 in x_1, f e g hanno un fattore comune di grado >0 in x_1 in $k[x_1,\ldots,x_n]$ se e solo se l'hanno in $k(x_2,\ldots,x_n)[x_1]$.*

Dimostrazione È chiaro che se h è un polinomio di $k[x_1,\ldots,x_n]$ esso lo è anche di $k(x_2,\ldots,x_n)[x_1]$ (coefficienti con denominatore 1) e quindi se f e g hanno un fattore comune di grado >0 in x_1 in $k[x_1,\ldots,x_n]$ allora l'hanno in $k(x_2,\ldots,x_n)[x_1]$.
Viceversa sia $f=HF^*$ e $g=HG^*$, con H, F^*, G^* in $k(x_2,\ldots,x_n)[x_1]$ e H di grado >0 in x_1. Riducendo eventualmente tutti i denominatori dei coefficienti del polinomio H ad uno stesso denominatore comune [12] si potrà scrivere $H=h(x_1,\ldots,x_n)/d(x_2,\ldots,x_n)$ ove $h(x_1,\ldots,x_n)$ contiene x_1 con grado >0. Analogamente $F^*=f^*(x_1,\ldots,x_n)/p(x_2,\ldots,x_n)$ e $G^*=g^*(x_1,\ldots,x_n)/q(x_2,\ldots,x_n)$, per cui la fattorizzazione scritta sopra si può ricondurre a
$d(x_2,\ldots,x_n)p(x_2,\ldots,x_n)f = h(x_1,\ldots,x_n)f^*(x_1,\ldots,x_n)$ $\quad$ $d(x_2,\ldots,x_n)q(x_2,\ldots,x_n)g = h(x_1,\ldots,x_n)g^*(x_1,\ldots,x_n)$.
Poiché $h(x_1,\ldots,x_n)$ contiene x_1 con grado >0, pure uno dei suoi fattori irriducibili contiene x_1 con grado >0; ora questo fattore deve dividere il prodotto $d(x_2,\ldots,x_n)p(x_2,\ldots,x_n)f$ ma non può dividere i due polinomi in cui manca l'indeterminata x_1 e quindi divide f; similmente divide g: ecco quindi un fattore comune di f e g di grado >0 in x_1! C.V.D.

Definiamo quindi $\mathrm{Res}(f,g,x_1)$ come nel precedente paragrafo (determinante della matrice di Sylvester).

[12] Non è necessario fare il minimo comune denominatore (cioè minimo comune multiplo dei denominatori) che risulta laborioso se n-1>1: basta infatti fare il prodotto di tutti i denominatori.

PROPOSIZIONE 4.2 *Se f e g sono polinomi di $k[x_1,\ldots,x_n]$ di grado >0 in x_1, allora*

(i) $\mathrm{Res}(f,g,x_1)$ *appartiene all'ideale* $\langle f, g\rangle \cap k[x_2,\ldots,x_n]$ [13]

(ii) $\mathrm{Res}(f,g,x_1) = 0$ *se e solo se f e g hanno un fattore comune in $k[x_1,\ldots,x_n]$ di grado >0 in x_1.*

Dimostrazione Come visto nella proposizione 3.2, $\mathrm{Res}(f,g,x_1)=Af+Bg$: quindi sicuramente $\mathrm{Res}(f,g,x_1)$ è un elemento di $\langle f,g\rangle$; inoltre per definizione $\mathrm{Res}(f,g,x_1)$ è un polinomio a coefficienti interi nelle "indeterminate" $a_0,\ldots,a_l, b_0,\ldots,b_m$ e quindi sta in $k[x_2,\ldots,x_n]$. Per le considerazioni svolte nel precedente paragrafo, $\mathrm{Res}(f,g,x_1)=0$ se e solo se f e g hanno un fattore comune in $k(x_2,\ldots,x_n)[x_1]$ di grado >0 in x_1: per il lemma ciò equivale ad averlo in $k[x_1,\ldots,x_n]$. C.V.D.

Per applicare questa proposizione alla teoria dell'eliminazione è importante sapere che cosa succede quando si sostituiscono parte delle indeterminate che compaiono nel risultante con elementi di k. Il problema nasce quando la sostituzione porta i polinomi f e g ad abbassarsi di grado rispetto a x_1.

ESEMPIO 4.3 Se $f=6x^2+y^2-4$ e $g=x^2y+3x-1$, $\mathrm{Res}(f,g,x)=\begin{vmatrix} 6 & 0 & y & 0 \\ 0 & 6 & 3 & y \\ y^2-4 & 0 & -1 & 3 \\ 0 & y^2-4 & 0 & -1 \end{vmatrix}$.

Ponendo nel risultante $y=0$, si ottiene

$$\begin{vmatrix} 6 & 0 & 0 & 0 \\ 0 & 6 & 3 & 0 \\ -4 & 0 & -1 & 3 \\ 0 & -4 & 0 & -1 \end{vmatrix} = 6\begin{vmatrix} 6 & 3 & 0 \\ 0 & -1 & 3 \\ -4 & 0 & -1 \end{vmatrix} = 6\cdot(-30),$$

mentre ponendo nei due polinomi $y=0$, si ottiene $f^*=6x^2-4$ e $g^*=3x-1$, $\mathrm{Res}(f^*,g^*,x)=\begin{vmatrix} 6 & 3 & 0 \\ 0 & -1 & 3 \\ -4 & 0 & -1 \end{vmatrix} = -30$.

Le cose vanno anche peggio partendo da un polinomio come $g=x^2y+3xy-1$ in cui la y compare come coefficiente anche del termine di primo grado in x. In tal caso ponendo nel risultante $y=0$, si ottiene

$$\begin{vmatrix} 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ -4 & 0 & -1 & 0 \\ 0 & -4 & 0 & -1 \end{vmatrix} = 6^2\begin{vmatrix} -1 & 0 \\ 0 & -1 \end{vmatrix} = 6^2,$$

mentre ponendo nei due polinomi $y=0$, si ottiene $f^*=6x^2-4$ e $g^*=-1$, $\mathrm{Res}(f^*,g^*,x)=\begin{vmatrix} -1 & 0 \\ 0 & -1 \end{vmatrix} = 1$.

Vogliamo evidenziare la relazione (già intravista nell'esempio) tra ciò che si ottiene facendo una sostituzione nel risultante e il risultante dei polinomi in cui è stata operata la stessa sostituzione. Innanzi tutto quando sostituiamo in $(x_1,x_2,\ldots,x_i,x_{i+1},\ldots,x_n)$ le ultime $n-i$ coordinate ponendo $(x_{i+1},\ldots,x_n)=(c_{i+1},\ldots,c_n)=\mathbf{c}$, invece di $(x_1,x_2,\ldots,x_i,c_{i+1},\ldots,c_n)$ scriviamo con ovvia simbologia: $(x_1,\mathbf{y},\mathbf{c})$. Scritti i polinomi f e g di $k[x_1,\ldots,x_n]$, di grado >0 in x_1 come $f = a_0x_1^{\,l}+\ldots+a_l$, $g = b_0x_1^{\,m}+\ldots+b_m$ (con $a_0\neq0$ e $b_0\neq0$ e $l>0$, $m>0$, e $a_0,\ldots,a_l, b_0,\ldots,b_m \in k[x_2,\ldots,x_n]$) sostituendo nel risultante si ha

[13] Può peraltro succedere che $\mathrm{Res}(f,g,x_1)$ non generi tutto l'ideale $I_1=\langle f, g\rangle \cap k[x_2,\ldots,x_n]$, come mostra il caso in cui $f=x^2y+y^2-4$ e $g=xy-1$: allora $\mathrm{Res}(f,g,x)=y(y^3-4y+1)$, mentre la base di Gröbner ridotta rispetto a LEX di $I=\langle f, g\rangle$ è $\{x+y^2-4, y^3-4y+1\}$

$$h(\mathbf{y},\mathbf{c}) := \left[\mathrm{Res}\left(f,g,x_1\right)\right](\mathbf{y},\mathbf{c}) = \begin{vmatrix} a_0(\mathbf{y},\mathbf{c}) & \cdots & 0 & b_0(\mathbf{y},\mathbf{c}) & \cdots & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & & \vdots \\ \vdots & & a_0(\mathbf{y},\mathbf{c}) & \vdots & & \ddots & \vdots \\ \vdots & & \vdots & \vdots & & & b_0(\mathbf{y},\mathbf{c}) \\ \vdots & & \vdots & b_m(\mathbf{y},\mathbf{c}) & & & \vdots \\ a_l(\mathbf{y},\mathbf{c}) & & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & a_l(\mathbf{y},\mathbf{c}) & 0 & \cdots & \cdots & b_m(\mathbf{y},\mathbf{c}) \end{vmatrix}$$

Se $a_0(\mathbf{y},\mathbf{c})=0$ e $b_0(\mathbf{y},\mathbf{c})=0$, il determinante $h(\mathbf{y},\mathbf{c})$ si annulla e quindi non si riesce a stabilirne un legame significativo con $\mathrm{Res}(f(x_1,\mathbf{y},\mathbf{c}),g(x_1,\mathbf{y},\mathbf{c}), x_1)$.
Se $a_0(\mathbf{y},\mathbf{c})\neq 0$ e $b_0(\mathbf{y},\mathbf{c})\neq 0$, il determinante $h(\mathbf{y},\mathbf{c})$ coincide con $\mathrm{Res}(f(x_1,\mathbf{y},\mathbf{c}),g(x_1,\mathbf{y},\mathbf{c}), x_1)$, cioè con il risultante dei polinomi in cui si è operata la sostituzione; se $a_0(\mathbf{y},\mathbf{c})\neq 0$ ma $b_0(\mathbf{y},\mathbf{c})=0$ bisogna vedere qual è il primo r tale che $b_r(\mathbf{y},\mathbf{c})\neq 0$: ad esempio se $r=1$ il determinante $h(\mathbf{y},\mathbf{c})$ è il prodotto di $a_0(\mathbf{y},\mathbf{c})$ per il determinante della matrice che si ottiene dalla precedente togliendo la prima riga e la prima colonna

$$a_0(\mathbf{y},\mathbf{c})\begin{vmatrix} a_0(\mathbf{y},\mathbf{c}) & \cdots & 0 & b_1(\mathbf{y},\mathbf{c}) & \cdots & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & & \vdots \\ \vdots & & a_0(\mathbf{y},\mathbf{c}) & \vdots & & \ddots & \vdots \\ \vdots & & \vdots & \vdots & & & b_1(\mathbf{y},\mathbf{c}) \\ \vdots & & \vdots & b_m(\mathbf{y},\mathbf{c}) & & & \vdots \\ a_l(\mathbf{y},\mathbf{c}) & & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & \cdots & a_l(\mathbf{y},\mathbf{c}) & 0 & \cdots & \cdots & b_m(\mathbf{y},\mathbf{c}) \end{vmatrix} = a_0(\mathbf{y},\mathbf{c})\mathrm{Res}\left(f(x_1,\mathbf{y},\mathbf{c}),g(x_1,\mathbf{y},\mathbf{c}),x_1\right)$$

similmente se $r=2$ il determinante $h(\mathbf{y},\mathbf{c})$ è prodotto di $[a_0(\mathbf{y},\mathbf{c})]^2$ per il determinante della matrice che si ottiene dalla prima togliendo le prime due righe e colonne e che coincide con $\mathrm{Res}(f(x_1,\mathbf{y},\mathbf{c}),g(x_1,\mathbf{y},\mathbf{c}),x_1)$ ecc. Ovviamente considerazioni analoghe valgono se $b_0(\mathbf{y},\mathbf{c})\neq 0$ ma $a_0(\mathbf{y},\mathbf{c})=0$. In generale dunque vale la

PROPOSIZIONE 4.4 *Siano f e g polinomi di $k[x_1,\ldots,x_n]$ di grado >0 in x_1.*
Se $a_0(\mathbf{y},\mathbf{c})\neq 0$ e $b_r(\mathbf{y},\mathbf{c})\neq 0$ ma $b_j(\mathbf{y},\mathbf{c})=0$ per ogni $j<r$, in $k[\mathbf{y}]$ risulta

$$h(\mathbf{y},\mathbf{c}) = [a_0(\mathbf{y},\mathbf{c})]^r\,\mathrm{Res}(f(x_1,\mathbf{y},\mathbf{c}),g(x_1,\mathbf{y},\mathbf{c}),x_1);$$

un risultato simmetrico vale se $b_0(\mathbf{y},\mathbf{c})\neq 0$ e $a_r(\mathbf{y},\mathbf{c})\neq 0$ ma $a_j(\mathbf{y},\mathbf{c})=0$ per ogni $j<r$, mentre se $a_0(\mathbf{y},\mathbf{c})=0$ e $b_0(\mathbf{y},\mathbf{c})=0$ non si possono stabilire relazioni significative tra le due funzioni.

Ne consegue, visto che $k[\mathbf{y}]$ è un dominio di integrità, che se $a_0(\mathbf{y},\mathbf{c})\neq 0$ e $h(\mathbf{y},\mathbf{c})=0$ (in particolare se $\mathrm{Res}(f,g,x_1)=0$) allora $\mathrm{Res}(f(x_1,\mathbf{y},\mathbf{c}),g(x_1,\mathbf{y},\mathbf{c}),x_1)=0$. Ciò si può interpretare così

COROLLARIO 4.5 *Siano f e g polinomi di $k[x_1,\ldots,x_n]$ di grado >0 in x_1. Se f e g hanno un fattore comune in $k[x_1,\ldots,x_n]$ di grado >0 in x_1 e $a_0(\mathbf{y},\mathbf{c})\neq 0$, allora anche $f(x_1,\mathbf{y},\mathbf{c})$ e $g(x_1,\mathbf{y},\mathbf{c})$ hanno un fattore comune in $k[x_1,\mathbf{y}]$ di grado >0 in x_1. Un risultato simmetrico vale se $b_0(\mathbf{y},\mathbf{c})\neq 0$.*

In sostanza, quindi, si hanno problemi a tradurre per sostituzione le scomposizioni ottenute in $k[x_1,\ldots,x_n]$ solo se entrambi i coefficienti dei termini di grado massimo di f e g si annullano quando si opera la sostituzione: per quanto sembri strano può davvero succedere che la traduzione sia falsa. Il verificarsi di tale spiacevole situazione è legato al fatto che la sostituzione abbassi a 0 il grado del fattore comune, come si vede nel prossimo esempio in cui $f = (xy-1)(x+1)$ e $g = (xy-1)(x+2)$.

ESEMPIO 4.6

$$\mathrm{Res}(x^2y+x(y-1)-1, x^2y+x(2y-1)-2, x)=\begin{vmatrix} y & 0 & y & 0 \\ y-1 & y & 2y-1 & y \\ -1 & y-1 & -2 & 2y-1 \\ 0 & -1 & 0 & -2 \end{vmatrix} = y\begin{vmatrix} 1 & 0 & 0 & 0 \\ y-1 & y & y & 0 \\ -1 & y-1 & -1 & y \\ 0 & -1 & 0 & -1 \end{vmatrix} = y^2\begin{vmatrix} 1 & 1 & 0 \\ y-1 & -1 & y \\ -1 & 0 & -1 \end{vmatrix} = 0,$$

il che conferma che i due polinomi in x a coefficienti in $k[y]$ hanno un fattore comune. Sostituendo $y=0$ nei due polinomi si ottengono i polinomi $-x-1$ e $-x-2$ che hanno grado inferiore a quello dei polinomi di partenza e che palesemente non hanno fattori comuni (si può anche verificarlo calcolando $\mathrm{Res}(-x-1, -x-2, x)=1$).

5. RISULTANTI GENERALIZZATI

Si vuole ora trovare l'equivalente del risultante di f e g rispetto ad x_1 per un insieme $\{f_1,\ldots,f_s\}$ di più di due polinomi. Si vogliono cioè costruire polinomi appartenenti all'ideale $\langle f_1,\ldots,f_s\rangle \cap k[x_2,\ldots,x_n]$, che si annullino se e solo se $f_1,\ldots,f_s$ hanno un fattore comune in $k[x_1,\ldots,x_n]$ di grado >0 in x_1.
Per farlo introduciamo delle indeterminate ausiliarie $u_1,\ldots,u_s$ e consideriamo i due polinomi f_i e $g_i = u_1f_1+\ldots+u_{i-1}f_{i-1}+u_{i+1}f_{i+1}+\ldots+u_sf_s$ appartenenti a $k[u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_s,x_1,\ldots,x_n]$ [14]. Nella matrice $\mathrm{Syl}(f_i, g_i, x_1)$ compariranno colonne - in numero pari al grado di f_i rispetto a x_1 - tutte contenenti combinazioni di termini appartenenti a $k[x_2,\ldots,x_n]$ mediante le indeterminate $u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_s$ e quindi, per la multilinearità del determinante, $\mathrm{Res}(f_i, g_i, x_1)$ sarà la combinazione mediante polinomi $h_{\boldsymbol{\alpha}}$ di $k[x_2,\ldots,x_n]$ di monomi in $u_1,\ldots,u_{i-1},u_{i+1},\ldots,u_s$ di grado totale pari al grado di f_i rispetto a x_1.

DEFINIZIONE 5.1 Se $\mathrm{Res}(f_i, g_i, x_1) = \Sigma\, h_{\boldsymbol{\alpha}}\mathbf{u}^{\boldsymbol{\alpha}}$ (ove $\mathbf{u}^{\boldsymbol{\alpha}}=u_1^{\alpha_1}\cdot\ldots\cdot u_{i-1}^{\alpha_{i-1}}\cdot u_{i+1}^{\alpha_{i+1}}\cdot\ldots\cdot u_s^{\alpha_s}$ e $|\boldsymbol{\alpha}|=$ grado di f_i rispetto a x_1) ogni polinomio $h_{\boldsymbol{\alpha}}$ è detto ***risultante generalizzato di*** $f_1,\ldots,f_s$ ***rispetto a*** x_1 ***e a*** f_i.

Come mostrano gli esempi successivi, la scelta di i condiziona la ricerca dei risultanti generalizzati: non solo possono essere diversi, ma possono essere in numero diverso e la matrice di Sylvester associata può avere ordine diverso.

ESEMPIO 5.2 Siano $f_1 = x^2+y+z-1$, $f_2 = x+y^2+z-1$, $f_3 = x+y+z^2-1$.
Scegliendo $i=1$ e $x_1=x$ si ha [15] $g_1= (u_2+u_3)x + u_2(f_2-x) + u_3(f_3-x)$ e quindi

$$\mathrm{Res}(f_1, g_1, x_1)=\begin{vmatrix} 1 & u_2+u_3 & 0 \\ 0 & u_2(f_2-x)+u_3(f_3-x) & u_2+u_3 \\ f_1-x^2 & 0 & u_2(f_2-x)+u_3(f_3-x) \end{vmatrix} =$$

$$\begin{vmatrix} 1 & 1 & 0 \\ 0 & f_2-x & 1 \\ f_1-x^2 & 0 & f_2-x \end{vmatrix}u_2^2 + \begin{vmatrix} 1 & 1 & 0 \\ 0 & f_3-x & 1 \\ f_1-x^2 & 0 & f_2-x \end{vmatrix}u_2u_3 + \begin{vmatrix} 1 & 1 & 0 \\ 0 & f_2-x & 1 \\ f_1-x^2 & 0 & f_3-x \end{vmatrix}u_2u_3 + \begin{vmatrix} 1 & 1 & 0 \\ 0 & f_3-x & 1 \\ f_1-x^2 & 0 & f_3-x \end{vmatrix}u_3^2.$$

Dunque si hanno i tre risultanti generalizzati (che denotiamo con un indice pari al multigrado del monomio in u_1, u_2, u_3, di cui sono coefficienti)

$$h_{020}=\begin{vmatrix} 1 & 1 & 0 \\ 0 & f_2-x & 1 \\ f_1-x^2 & 0 & f_2-x \end{vmatrix} = (f_2-x)^2+f_1-x^2$$

[14] Non è importante quale indice i si scelga, come si vedrà. Per comodità si può scrivere $i=1$: tanto a questo caso ci si può sempre ricondurre pur di riordinare i polinomi in gioco.
[15] Adottiamo questa rappresentazione invece della più ovvia $g_1=(u_2+u_3)x+u_2(y^2+z-1)+u_3(y+z^2-1)$ perché semplifica i conti successivi e permette di evidenziare le relazioni tra gli ideali generalizzati ottenuti con differenti scelte di i.

$$h_{011}=\begin{vmatrix} 1 & 1 & 0 \\ 0 & f_3-x & 1 \\ f_1-x^2 & 0 & f_2-x \end{vmatrix}+\begin{vmatrix} 1 & 1 & 0 \\ 0 & f_2-x & 1 \\ f_1-x^2 & 0 & f_3-x \end{vmatrix}=2\left[(f_2-x)(f_3-x)+f_1-x^2\right]$$

$$h_{002}=\begin{vmatrix} 1 & 1 & 0 \\ 0 & f_3-x & 1 \\ f_1-x^2 & 0 & f_3-x \end{vmatrix}=(f_3-x)^2+f_1-x^2\,.$$

Invece scegliendo i=2 e x_1=x si ha $g_2 = u_1x^2 + u_3x + u_1(f_1–x^2) + u_3(f_3–x)$ e quindi

$$\mathrm{Res}(f_2, g_2, x_1)=\begin{vmatrix} 1 & 0 & u_1 \\ f_2-x & 1 & u_3 \\ 0 & f_2-x & u_1(f_1-x^2)+u_3(f_3-x) \end{vmatrix}=\begin{vmatrix} 1 & 0 & 1 \\ f_2-x & 1 & 0 \\ 0 & f_2-x & f_1-x^2 \end{vmatrix}u_1+\begin{vmatrix} 1 & 0 & 0 \\ f_2-x & 1 & 1 \\ 0 & f_2-x & f_3-x \end{vmatrix}u_3\,.$$

Dunque si hanno i due risultanti generalizzati

$$h_{100}=\begin{vmatrix} 1 & 0 & 1 \\ f_2-x & 1 & 0 \\ 0 & f_2-x & f_1-x^2 \end{vmatrix}=(f_2-x)^2+f_1-x^2=h_{020}$$

$$h_{001}=\begin{vmatrix} 1 & 0 & 0 \\ f_2-x & 1 & 1 \\ 0 & f_2-x & f_3-x \end{vmatrix}=(f_3-x)-(f_2-x)=f_3-f_2\,.$$

Il secondo è un fattore della differenza $h_{002} – h_{020}$; inoltre $h_{020} – h_{011} + h_{002} = (f_2–f_3)^2 = {h_{001}}^2$. Dunque si vede che:
$h_{020} = h_{100}$, $h_{002} = h_{100} + h_{001}(f_2+f_3–2x)$, $h_{011} = h_{020} + h_{002} – {h_{001}}^2 = 2h_{100} + h_{001}(f_2+f_3–2x) – {h_{001}}^2$, cioè i primi 3 risultanti generalizzati appartengono all'ideale generato dagli ultimi due.

ESEMPIO 5.3 Siano $f_1 = x^3+y, f_2 = x^2+y, f_3 = x+y$.
Scegliendo i=1 e x_1=x si ha $g_1 = u_2x^2 + u_3x + (u_2+u_3)y$ e quindi

$$\mathrm{Res}(f_1, g_1, x_1)=\begin{vmatrix} 1 & 0 & u_2 & 0 & 0 \\ 0 & 1 & u_3 & u_2 & 0 \\ 0 & 0 & (u_2+u_3)y & u_3 & u_2 \\ y & 0 & 0 & (u_2+u_3)y & u_3 \\ 0 & y & 0 & 0 & (u_2+u_3)y \end{vmatrix}=\begin{vmatrix} 1 & 0 & u_2 & 0 & 0 \\ 0 & 1 & u_3 & u_2 & 0 \\ 0 & 0 & (u_2+u_3)y & u_3 & u_2 \\ 0 & 0 & -u_2y & (u_2+u_3)y & u_3 \\ 0 & 0 & -u_3y & -u_2y & (u_2+u_3)y \end{vmatrix}=$$

$$=\begin{vmatrix} (u_2+u_3) & u_3 & u_2 \\ -u_2 & (u_2+u_3)y & u_3 \\ -u_3 & u_2 & (u_2+u_3)y \end{vmatrix}y=(u_2+u_3)^3y^3+{u_2}^3y^2-{u_3}^3y+3(u_2+u_3)u_2u_3y^2=$$

$$={u_2}^3(y^3+y^2)+3{u_2}^2u_3(y^3+y^2)+3u_2{u_3}^2(y^3+y^2)+(y^3-y){u_3}^3\,.$$

Dunque si hanno formalmente 4 risultanti generalizzati; i primi tre coincidono, a meno del prodotto per 3: quindi gli unici utili sono $h_{030} = y^3+y^2$ e $h_{003} = y^3–y$.
Ma si può arrivare ad un risultato analogo più semplicemente fissando i=3 e quindi $f_3 = x+y$ e $g_3 = u_1x^3 + u_2x^2 + (u_1+u_2)y$: in questo modo la matrice di Sylvester ha ordine 4 e

$$\mathrm{Res}(f_3, g_3, x)=\begin{vmatrix} 1 & 0 & 0 & u_1 \\ y & 1 & 0 & u_2 \\ 0 & y & 1 & 0 \\ 0 & 0 & y & (u_1+u_2)y \end{vmatrix}=-u_1y^3+u_2y^2+(u_1+u_2)y=u_1(y-y^3)+u_2(y^2+y),$$

che evidenzia i risultanti generalizzati $h_{100} = y^2 + y$ e $h_{010} = y – y^3$, che dividono quelli trovati in precedenza.

Si vede che, se è vero (come dimostreremo subito dopo) che non importa quale indice si sceglie, conviene isolare come f_i il polinomio in cui x_1 compare con il grado minimo, visto che g_i avrà comunque grado in x_1 pari al massimo dei gradi in x_1 dei polinomi f_j con $j\neq i$.

PROPOSIZIONE 5.4 *Siano* $\{f_1,\dots,f_s\}$ *polinomi di* $k[x_1,\dots,x_n]$ *di grado* >0 *in* x_1 *e sia* $g_1 = u_2f_2+\dots+u_sf_s$. *Si ha* [16]:

(i) *ogni risultante generalizzato sta in* $<f_1,\dots,f_s>\cap k[x_2,\dots,x_n]$;

(ii) *Sono equivalenti le seguenti condizioni*:

a) *ogni risultante generalizzato rispetto a* x_1 *si annulla*

b) $\mathrm{Res}(f_1, g_1, x_1) = 0$

c) $f_1,\dots,f_s$ *hanno in* $k[x_1,\dots,x_n]$ *un fattore comune* F *di grado* >0 *in* x_1.

Dimostrazione (i) Scriviamo $\mathrm{Res}(f_1, g_1, x_1)$ come $\Sigma h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)\mathbf{u}^{\boldsymbol{\alpha}}$ (ove $\mathbf{u}^{\boldsymbol{\alpha}} = u_1^{\,0}\cdot u_2^{\,\alpha_2}\cdot\dots\cdot u_s^{\,\alpha_s}$ e $|\boldsymbol{\alpha}|$ = grado di f_1 rispetto a x_1); per costruzione $h_{\boldsymbol{\alpha}}$ sta in $k[x_2,\dots,x_n]$: resta da provare che sta in $<f_1,\dots,f_s>$.
Pensando $\mathrm{Res}(f_1, g_1, x_1)$ come risultante di due polinomi di $k(u_2,\dots,u_s,x_2,\dots,x_n)[x_1]$ si ha che esistono due polinomi (a coefficienti interi nei coefficienti di f_1 e g_1 rispetto a x_1) A e B tali che

(*) $$\mathrm{Res}(f_1, g_1, x_1) = \mathrm{A}\,f_1+\mathrm{B}g_1.$$

Sviluppiamo A e B secondo potenze di $u_2,\dots,u_s$: $\mathrm{A} = \Sigma \mathrm{A}_{\boldsymbol{\lambda}}(x_1,\dots,x_n)\mathbf{u}^{\boldsymbol{\lambda}}$, $\mathrm{B} = \Sigma \mathrm{B}_{\boldsymbol{\mu}}(x_1,\dots,x_n)\mathbf{u}^{\boldsymbol{\mu}}$ ove i coefficienti, come evidenziato, sono in generale polinomi di $k[x_1,\dots,x_n]$ e confrontiamo i coefficienti dei monomi in $u_2,\dots,u_s$ che compaiono in (*):

$$\Sigma h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)\mathbf{u}^{\boldsymbol{\alpha}} = (\Sigma \mathrm{A}_{\boldsymbol{\lambda}}(x_1,\dots,x_n)\mathbf{u}^{\boldsymbol{\lambda}})\,f_1 + (\Sigma \mathrm{B}_{\boldsymbol{\mu}}(x_1,\dots,x_n)\mathbf{u}^{\boldsymbol{\mu}})(u_2f_2+\dots+u_sf_s).$$

Distribuendo il prodotto nel secondo addendo e tenendo conto che ogni u_i si può riscrivere come $\mathbf{u}^{\mathbf{e}(j)}$ ove $\mathbf{e}(j)$ è la s-pla che ha 1 in posizione j e 0 altrove, si trova:

$$\Sigma h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)\mathbf{u}^{\boldsymbol{\alpha}} = (\Sigma \mathrm{A}_{\boldsymbol{\lambda}}(x_1,\dots,x_n)\,f_1\mathbf{u}^{\boldsymbol{\lambda}}) + (\Sigma \mathrm{B}_{\boldsymbol{\mu}}(x_1,\dots,x_n)\,f_2\,\mathbf{u}^{\boldsymbol{\mu}+\mathbf{e}(2)}) +\dots+ (\Sigma \mathrm{B}_{\boldsymbol{\mu}}(x_1,\dots,x_n)\,f_s\,\mathbf{u}^{\boldsymbol{\mu}+\mathbf{e}(s)}).$$

A costruire il coefficiente $h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)$ di $\mathbf{u}^{\boldsymbol{\alpha}}$ contribuiranno allora $\mathrm{A}_{\boldsymbol{\alpha}}(x_1,\dots,x_n)\,f_1$ e tutti i coefficienti $\mathrm{B}_{\boldsymbol{\mu}}(x_1,\dots,x_n)\,f_j$ (con $j=2,\dots,s$) tali che $\boldsymbol{\mu}+\mathbf{e}(j)=\boldsymbol{\alpha}$, cioè

$$h_{\boldsymbol{\alpha}}(x_2,\dots,x_n) = \mathrm{A}_{\boldsymbol{\alpha}}(x_1,\dots,x_n)\,f_1 + \mathrm{B}_{\boldsymbol{\alpha}-\mathbf{e}(2)}(x_1,\dots,x_n)\,f_2+\dots+\mathrm{B}_{\boldsymbol{\alpha}-\mathbf{e}(s)}(x_1,\dots,x_n)\,f_s.$$

Questo finalmente garantisce che il risultante generalizzato $h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)$ sta in $<f_1,\dots,f_s>$.
Notiamo per finire che questo risultato è stato dimostrato per comodità a partire da f_1, g_1, ma nulla sarebbe cambiato, se non gli indici, partendo da un'altra coppia f_i, g_i.
(ii) L'equivalenza tra (a) e (b) è ovvia, poiché $\mathrm{Res}(f_1, g_1, x_1) = \Sigma h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)\mathbf{u}^{\boldsymbol{\alpha}}$ è il polinomio nullo in $k(x_2,\dots,x_n)[u_2,\dots,u_s]$ se e solo se i suoi coefficienti $h_{\boldsymbol{\alpha}}(x_2,\dots,x_n)$ sono nulli.
Inoltre, se $f_1,\dots,f_s$ hanno in $k[x_1,\dots,x_n]$ un fattore comune F di grado >0 in x_1, anche f_1 e g_1 hanno in $k[u_2,\dots,u_s,x_1,\dots,x_n]$ un fattore comune F di grado >0 in x_1 e quindi, per la prop. 4.2, $\mathrm{Res}(f_1, g_1, x_1)=0$: ciò prova che (c) implica (b).
Viceversa, ancora per la prop. 4.2, se $\mathrm{Res}(f_1, g_1, x_1)=0$, allora f_1 e g_1 hanno in $k[u_2,\dots,u_s,x_1,\dots,x_n]$ un fattore comune F di grado >0 in x_1. Esso appartiene a $k[x_1,\dots,x_n]$, poiché divide f_1 e quindi non può contenere indeterminate diverse da quelle di f_1. Inoltre visto che le indeterminate ausiliarie sono tutte diverse, gli addendi che compaiono in g_1 non possono compensarsi: quindi se F divide g_1 deve necessariamente dividere $u_2f_2,\dots,u_sf_s$ e non contenendo indeterminate ausiliarie deve dividere $f_2,\dots$, f_s: ciò prova che (b) implica (c). C.V.D.

Osserviamo per finire che, in realtà noi abbiamo provato che i risultanti generalizzati di $f_1,\dots,f_s$ rispetto a x_1 e a f_1 sono nulli se e solo se $f_1,\dots,f_s$ hanno in $k[x_1,\dots,x_n]$ un fattore comune F di grado >0 in x_1. Visto che quest'ultima condizione è intrinseca (cioè indipendente dalla scelta dell'indice i) è chiaro che se si annullano quei particolari risultanti generalizzati si annullano anche tutti quelli che si ottengono per differente scelta dell'indice i. A livello pratico questo significa che se si deve verificare se ci sono fattori comuni si può scegliere un indice i qualunque: ovviamente la scelta cadrà su quello che permette di fare i conti più semplici.

[16] I due risultati generalizzano quelli visti nella proposizione 4.2