Indice

0.1 Risultante. Eliminazione di una indeterminata

0.1.1 Polinomi simmetrici

Dato un campo $\mathbb{K}$, consideriamo l'insieme dei polinomi in n indeterminate $\mathbb{K}[X_1, \ldots, X_n]$, tra tutti gli elementi di tale insieme vi è una classe di polinomi notevoli detti *simmetrici*.

Definizione 0.1.1 *Un polinomio $f(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$ si dice simmetrico se è invariante rispetto ad ogni permutazione delle indeterminate.*

I seguenti polinomi simmetrici in n indeterminate $X_1, X_2, \ldots, X_n$

$$\begin{array}{rcl} \sigma_1(X_1, \ldots, X_n) & = & X_1 + X_2 + \cdots + X_n \\ \sigma_2(X_1, \ldots, X_n) & = & X_1X_2 + X_1X_3 + \cdots + X_n - 1X_n \\ \sigma_3(X_1, \ldots, X_n) & = & X_1X_2X_3 + X_1X_2X_4 + \cdots + X_n - 2X_n - 1X_n \\ & \vdots & \\ \sigma_n(X_1, \ldots, X_n) & = & X_1X_2 \cdot \cdots \cdot X_n \end{array}$$

prendono il nome di *polinomi simmetrici elementari* o *funzioni simmetriche elementari* in $\mathbb{K}[X_1, \ldots, X_n]$. Tali funzioni legano i coefficienti e le radici di un polinomio monico in una indeterminata. Sia $f(X) \in \mathbb{K}[X]$ monico

$$f(X) = X^n + a_1X^{n-1} + a_2X^{n-2} + \cdots + a_{n-1}X + a_n \tag{1}$$

e $x_1, x_2, \ldots, x_n$ le sue radici allora si può scrivere:

$$f(X) = (X - x_1) \cdot (X - x_2) \ldots (X - x_n). \tag{2}$$

Sviluppando e confrontando i coefficienti di 1 e 2 si ottengono le seguenti relazioni:

$$\begin{aligned} a_1 &= -(x_1 + x_2 + \cdots + x_n) \\ a_2 &= x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_1x_n \\ a_3 &= -(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n) \\ &\vdots \\ a_n &= (-1)^n(x_1x_2 \cdot \ldots \cdot x_n). \end{aligned}$$

Queste relazioni prendono il nome di *formule di Viète* ed esprimono i coefficienti di un polinomio monico in funzione delle sue radici.

In generale:

$$a_k = (-1)^k\sigma_k(x_1, x_2, \ldots, x_n)$$

cioè i coefficienti di ogni polinomio monico in una indeterminata a coefficienti in un campo sono, a meno del segno, le funzioni simmetriche elementari delle sue radici.

L'insieme S dei polinomi simmetrici in n variabili a coefficienti in $\mathbb{K}$ è un sottoanello di $\mathbb{K}[x_1, \ldots, x_n]$.

Ogni polinomio $f(\sigma_1, \ldots, \sigma_n)$ nelle funzioni simmetriche elementari è un polinomio simmetrico rispetto alle indeterminate $x_1, \ldots, x_n$. Si ha pertanto la seguente inclusione:

$$\mathbb{K}[\sigma_1, \ldots, \sigma_n] \subseteq S$$

Esempio 0.1.1 *Consideriamo i polinomi:*

$$2x_1 + 2x_2 + 2x_3 - 3x_1^2 - 3x_2^2 - 3x_3^2$$

$$x_1^2x_2^2x_3^2 + x_1x_2 + x_2x_3 + x_1x_3$$

essi sono simmetrici in $\mathbb{K}[x_1, x_2, x_3]$, mentre non lo sono i polinomi

$$x_1^2 - x_2^2 + x_3$$

$$x_1 + 2x_2 + 5x3$$

Esempio 0.1.2

$$\sigma_1\sigma_2 + 2\sigma_3 = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 + 5x_1x_2x_3$$

Il teorema che segue mostra che la precedente inclusione è una uguaglianza.

Teorema 0.1.1 (Teorema Fondamentale sui polinomi simmetrici)
Ogni polinomio simmetrico $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ *si può scrivere in modo unico come polinomio a coefficienti in* $\mathbb{K}$ *nei polinomi simmetrici elementari* $\sigma_1, \ldots, \sigma_n$.

Abbiamo quindi che $\mathbb{K}[\sigma_1, \ldots, \sigma_n] = S$.

Esempio 0.1.3 *Il seguente esempio illustra un'applicazione del teorema 0.1.1.*
Il polinomio simmetrico $x_1^3 + x_2^3 + x_3 3 - 3x_1x_2x_3$ *risulta essere uguale a:* $\sigma_1^3 - 3\sigma_1\sigma_2$ *essendo* σ_i *i polinomi simmetrici elementari.*

Veniamo ora a una generalizzazione della nozione di polinomio simmetrico.
Siano $x_1, \ldots, x_n$ e $y_1, \ldots, y_s$ due gruppi di indeterminate.

Definizione 0.1.2 *Dato* $f(x_1, \ldots, x_n, y_1, \ldots, y_s) \in \mathbb{K}[x_1, \ldots, y_s]$, *diremo che è simmetrico rispetto ai due gruppi di indeterminate se è invariante per ogni permutazione di* $x_1, \ldots, x_n$ *e per ogni permutazione di* $y_1, \ldots, y_s$. *Tale polinomio si dice semisimmetrico.*

Indicati con $\sigma_1, \ldots, \sigma_n$ e $\tau_1, \ldots, \tau_s$ i polinomi simmetrici elementari rispetto a $x_1, \ldots, x_n$ e $y_1, \ldots, y_s$ il Teorema Fondamentale si generalizza come segue: ogni polinomio $f(x_1, \ldots, x_n, y_1, \ldots, y_s)$ a coefficienti in $\mathbb{K}$ che sia simmetrico rispetto ai due gruppi

di indeterminate $x_1, \ldots, x_n$ e $y_1, \ldots, y_s$ si può scrivere, in modo unico, come polinomio a coefficienti in $\mathbb{K}$, nelle indeterminate $\sigma_1, \ldots, \sigma_n$ e $\tau_1, \ldots, \tau_s$.
Ossia

$$f(x_1, \ldots, x_n) = \phi(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_s).$$

Il seguente esempio mostra che esistono polinomi simmetrici per due gruppi di indeterminate ma che non sono polinomi simmetrici.

Esempio 0.1.4 *Il polinomio* $f(x_1, x_2, x_3, y_1, y_2) = x_1x_2x_3 - x_1x_2y_1 - x_1x_2y_2 - x_1x_3y_1 - x_1x_3y_2 - x_2x_3y_1 - x_2x_3y_2 + x_1y_1y_2 + x_2y_1y_2 + x_3y_1y_2$
è simmetrico rispetto alle x_i *e* y_j*, ma non lo è per l'insieme delle cinque indeterminate, come si vede scambiando* x_1 *con* y_1.
L'espressione di f *in funzione di* $\sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2$ *é data da:* $\sigma_3 - \sigma_2\tau_1 + \sigma_1\tau_2$.

Capitolo 1

Risultante, Teoria di Eliminazione e Molteplicità di Intersezione

1.1 Risultante alla Sylvester di due polinomi in una indeterminata

Il risultante alla Sylvester consente di decidere se due dati polinomi hanno una radice in comune.

Due polinomi $f(X)$ e $g(X)$ a coefficienti in un campo (non necessariamente algebricamente chiuso) $\mathbb{K}$ hanno una radice in comune in $\mathbb{K}$ o in un suo ampliamento $\overline{\mathbb{K}}$ se e solo se hanno un fattore in comune.

Consideriamo i due polinomi:

$$\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\ g(x) &= b_0x^s + b_1x^{s-1} + \cdots + n_{s-1}x + b_s. \end{aligned} \tag{1.1}$$

Siano $\alpha_1, \ldots, \alpha_n$ le radici di $f(x)$ e $\beta_1, \ldots, \beta_s$ le radici di $g(x)$ contenute in $\mathbb{K}$ o in $\overline{\mathbb{K}}$ se $\mathbb{K}$ non è algebricamente chiuso.

Definizione 1.1.1 *Il risultante alla Sylvester dei polinomi $f(x)$, e $g(x)$ è dato da*

$$R(f,g) = (a_0^s b_0^n) \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j).$$

Il risultante alla Sylvester per come è stato definito risulta essere un polinomio simmetrico nei due gruppi di indeterminate α_i , β_j.

Osservazione 1.1.1 $R(f,g) = 0$ *se e solo se esiste una radice comune ai polinomi* $f(x)$ $g(x)$.

Osserviamo che valgono le seguenti proprietà:

1. $R(f,g) = a_0^s \prod_{i=1}^n g(\alpha_i)$
2. $R(g,f) = b_0^n \prod_{j=1}^s f(\beta_j)$
3. $R(f,g) = (-1)^{ns} R(g,f)$
4. $R(f_1 f_2, g) = R(f_1, g) \cdot R(f_2, g)$.

Dimostriamo la prima proprietà.

Per definizione

$$R(f,g) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{n} (\alpha_i - \beta_j)$$

dove β_j sono le radici di $g(x)$ per $j = 1, \ldots, s$. Pertanto

$$g(x) = b_0(x - \beta_1) \cdot \ldots \cdot (x - \beta_s) = b_0 \prod_{j=1}^{s} (x - \beta_j).$$

Sostituendo al posto di x il valore α_i si ha:

$$g(\alpha_i) = b_0(\alpha_i - \beta_1) \cdot \ldots \cdot (\alpha_i - \beta_s) = \prod_{j=1}^{s} (\alpha_i - \beta_j).$$

Ora

$$\begin{aligned} \prod_{i=1}^{n} g(\alpha_i) &= b_0(\alpha_1 - \beta_1) \cdot \ldots \cdot (\alpha_1 - \beta_s) b_0(\alpha_2 - \beta_1) \cdot \ldots \cdot (\alpha_2 - \beta_s) \cdot \ldots \\ &\cdot \quad b_0(\alpha_n - \beta_1) \cdot \ldots \cdot (\alpha_n - \beta_s) \\ &= b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) \end{aligned}$$

Abbiamo ottenuto $\prod_{i=1}^{n} g(\alpha_i) = b_0 \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j)$. Moltiplicando entrambi i membri dell'espressione appena ricavata per a_0^n e avendo in mente la definizione 1.1.1 otteniamo: $R(f,g) = a_0^s \prod_{i=1}^{n} g(\alpha_i)$ $\square$

La dimostrazione della seconda proprietà è analoga alla precedente. La terza proprietà è ovvia. Dimostriamo l'ultima proprietà.

Sia $deg\ g = s$, $deg\ (f_1 f_2) = m + n$, con $m = deg\ f_1$ e $n = deg\ f_2$, il coefficiente direttore di $f_1 f_2$ è $f_{1,0} f_{2,0}$ essendo $f_{1,0}$ e $f_{2,0}$ i coefficienti direttori di f_1 e f_2 rispettivamente. Le radici di $f_1 f_2$ sono date da $x_1, \ldots, x_n$ e $y_1, \ldots, y_m$ che non sono altro che le radici di f_1 e f_2 rispettivamente; indichiamo tali radici con α_i per $i = 1, \ldots, m+n$.

$$\begin{aligned} R(f_1 f_2, g) &= (f_{1,0} f_{2,0})^s \prod_{i=1}^{m+n} g(\alpha_i) \\ &= f_{1,0}^s \prod_{i=1}^{n} g(\alpha_i) \cdot f_{2,0}^s \prod_{i=n+1}^{n+m} g(\alpha_i) \\ &= R(f_1, g) \cdot R(f_2, g). \end{aligned}$$

Per induzione su n si dimostra che:

$$R(\prod_{i=1}^{n} f_i, g) = \prod_{i=1}^{n} R(f_i, g).$$

Il risultante $R(f,g)$ può esprimersi come polinomio nelle indeterminate $a_0, \ldots, a_n, b_0 \ldots, b_s$. Per dimostrare quanto appena detto si usa la teoria dei polinomi simmetrici. Usando la definizione 1.1.1 si vede che:

$$R(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_s) = (a_0^s b_0^n)^{-1} R(f,g) = \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j)$$

è un polinomio simmetrico rispetto ai due gruppi $\{\alpha_1, \ldots, \alpha_n\}$ e $\{\beta_1, \ldots, \beta_s\}$.

Per il teorema 0.1.1 $R(\alpha_1, \ldots \beta_s)$ si può esprimere come polinomio nelle indeterminate $\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_s$ che sono rispettivamente i polinomi simmetrici elementari

nelle indeterminate $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_s$.

Ma $\sigma_1, \ldots, \sigma_n$ (risp. $\tau_1, \ldots, \tau_s$) sono, a meno del segno, (per le formule di Viète) i coefficienti dei polinomi $a_0^{-1} f(X)$ e $b_0^{-1} g(X)$.

Quindi $R(\alpha_1, \ldots, \beta_s)$ si può esprimere come polinomio nelle indeterminate $\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}, \frac{b_1}{b_0}, \ldots, \frac{b_s}{b_0}$. Il fattore $a_0^s b_0^n$ fa scomparire il denominatore in $R(\alpha_1, \ldots, \beta_s)$. Mostreremo che la definizione di $R(f, g)$ data dalla 1.1.1 è equivalente al seguente determinante di ordine $n + s$:

$$D = \left| \begin{array}{ccccccccc} a_0 & a_1 & & & & a_n & & & \\ & a_0 & a_1 & & & & a_n & & \\ & & & \cdots & & \cdots & & & \\ & & & a_0 & a_1 & & & a_n & \\ b_0 & b_1 & & & b_s & & & & \\ & b_0 & b_1 & & & b_s & & & \\ & & & \cdots & & \cdots & & & \\ & & & & b_0 & b_1 & & b_s & \end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} s \text{ righe} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \text{ righe} \end{array} \tag{1.2}$$

Dati

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

$$g(x) = b_0 x^s + b_1 x^{s-1} + \cdots + b_{s-1} x + b_s$$

con $a_i,\ b_j \in \mathbb{K}$ per $i = 0, \ldots, n$ $\quad j = 0, \ldots, s$; indichiamo con $\alpha_1, \ldots, \alpha_n$ e $\beta_1, \ldots, \beta_s$ le radici di $f(x)$ e $g(x)$ rispettivamente.

Consideriamo un nuovo determinante di ordine $n + s$

$$M = \left| \begin{array}{ccccccc} \beta_1^{n+s-1} & \beta_2^{n+s-1} & \cdots & \beta_s^{n+s-1} & \alpha_1^{n+s-1} & \cdots & \alpha_n^{n+s-1} \\ \beta_1^{n+s-2} & \beta_2^{n+s+-2} & \cdots & \beta_s^{n+s-2} & \alpha_1^{n+s-2} & \cdots & \alpha_n^{n+s-2} \\ \vdots & & & \vdots & & & \vdots \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_s^2 & \alpha_1^2 & \cdots & \alpha_n^2 \\ \beta_1 & \beta_2 & \cdots & \beta_s & \alpha_1 & \cdots & \alpha_n \\ 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \end{array} \right| \tag{1.3}$$

Calcoliamo il prodotto $(a_0^s b_0^n) DM$ in due modi diversi.

M è un determinante di Vandermonde il suo valore si calcola con la seguente formula:

$$M = \prod_{1\le i<j\le s}(\beta_i-\beta_j)\prod_{j=1}^{s}\prod_{i=1}^{n}(\beta_j-\alpha_i)\prod_{1\le i<j\le n}(\alpha_i-\alpha_j).$$

Ora

$$\begin{aligned} a_0^s b_0^n DM &= Da_0^s b_0^n \textstyle\prod_{j=1}^{s}\prod_{i=1}^{n}(\beta_j-\alpha_i)\cdot \prod_{1\le i<j\le s}(\beta_i-\beta_j)\prod_{1\le i<j\le n}(\alpha_i-\alpha_j) \\ &= D\cdot R(f,g)\prod_{1\le i<j\le s}(\beta_i-\beta_j)\prod_{1\le i<j\le n}(\alpha_i-\alpha_j). \end{aligned} \tag{1.4}$$

Il prodotto delle matrici associate ai determinanti D ed M è la matrice N:

$$\begin{pmatrix} \beta_1^{s-1}f(\beta_1) & \beta_2^{s-1}f(\beta_2) & \cdots & \beta_s^{s-1}f(\beta_s) & 0 & \cdots & 0 \\ \beta_1^{s-2}f(\beta_1) & \beta_2^{s-2}f(\beta_2) & \cdots & \beta_s^{s-2}f(beta_s) & 0 & \cdots & 0 \\ \vdots & & & \vdots & & & \vdots \\ f(\beta_1) & f(\beta_2) & \cdots & f(\beta_s) & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \alpha_{n-1}g(\alpha_1) & \cdots & \alpha_n^{n-1}g(\alpha_n) \\ \vdots & & \vdots & & & \vdots & \\ 0 & 0 & \cdots & 0 & g(\alpha_1) & \cdots & g(\alpha_n) \end{pmatrix}$$

Sviluppando il determinante $detN$ di N secondo il teorema di Laplace e mettendo a fattore i divisori comuni degli elementi di una stessa colonna e calcolando i corrispondenti determinanti di Vandermonde si ha:

$$(a_0^s b_0^n)\text{det N}= (a_0^s b_0^n)\prod_{j=1}^{s}f(\beta_j)\prod_{i=1}^{n}g(\alpha_i)\prod_{1\le k<l\le s}(\beta_k-\beta_l)\prod_{1\le r<t\le n}(\alpha_r-\alpha_t).$$

Ricordando che:

$$R(f,g)=a_0^s\prod_{i=1}^{n}g(\alpha_i)\ \text{ e }\ R(g,f)=b_0^n\prod_{j=1}^{s}f(\beta_j)$$

abbiamo:

$$(a_0^s b_0^n)detN = R(f,g)\cdot R(g,f)\prod_{1\le i<j\le s}(\beta_i-\beta_j)\prod_{1\le i<j\le n}(\alpha_i-\alpha_j). \tag{1.5}$$

Uguagliando le espressioni (1.4) e (1.5) e semplificando i termini comuni otteniamo:

$$R(f,g) = D.$$

Nella parte conclusiva della dimostrazione, abbiamo detto di semplificare i termini comuni (che sono $R(f,g)$ e $R(g,f)$). Potrebbe tuttavia capitare che un tale termine comune si annulli (per qualche f e g particolari); in questi casi la semplificazione non è ammissibile. Per mettere a posto la dimostrazione, conviene dare l'enunciato del teorema di Sylvester in termini polinomiali.

A tal fine, consideriamo due anelli di polinomi, $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s]$ e $\mathbb{K}[a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, \beta_s]$. Lo sviluppo del determinante (1.2) dà un polinomio di grado $n+s$ nelle indeterminate $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s$. Lo denoteremo con

$$D(a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s) \in \mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s].$$

Nello stesso spirito,

$$R(f,g) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) \in \mathbb{K}[a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, \beta_s].$$

Ora andiamo ad effettuare le seguenti sostituzioni in $D(a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s)$:

$$\begin{cases} a_1 = -(\alpha_1 + \ldots, \alpha_n)a_0, \\ a_2 = (\alpha_1 + \ldots, \alpha_n)a_0, \\ \cdots \cdots \\ a_i = (-1)^i(\alpha_1 \cdots \alpha_i + \ldots + \alpha_{n-(i-1)} \cdots \alpha_n)a_0 \\ \cdots \cdots \\ a_n = (-1)^n(\alpha_1 \cdots \alpha_n)a_0, \end{cases} \tag{1.6}$$

$$\begin{cases} b_1 = -(\beta_1 + \ldots, \beta_s)b_0, \\ b_2 = (\beta_1 + \ldots, \beta_s)b_0, \\ \cdots \cdots \\ b_j = (-1)^j(\beta_1 \cdots \beta_j + \ldots + \beta_{s-(j-1)} \cdots \beta_s)b_0 \\ \cdots \cdots \\ b_s = (-1)^s(\beta_1 \cdots \beta_s)b_0, \end{cases} \tag{1.7}$$

Otteniamo un polinomio $F(a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, b_s)$. Pertanto, è possibile confrontare questo polinomio F con il polinomio $R(f, g)$, dal momento che sia $R(f, g)$ che F appartengono ad un medesimo anello, cioè entrambi sono in $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s]$. Il teorema di Sylvester stabilise che questi due polinomi sono uguali.

Teorema 1.1.1 *Se tra* $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_n$ *e* $a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, \beta_s$ *intercedono le relazioni (1.6) e (1.7), allora* $D(a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s) = R(f, g)$.

Dimostrazione

Interpretiamo i calcoli precedentemente fatti in $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s]$ e $\mathbb{K}[a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1$
Possiamo riguardare $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ e $g(x) = b_0x^s + b_1x^{s-1} + \cdots + b_{s-1}x + b_s$ come polinomi nell'indeterminata x ed a coefficienti in $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s]$. Se questi coefficienti sono funzioni di $a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, \beta_s$ come nelle (1.6) e (1.7), allora $f(\alpha_1) = \ldots = f(\alpha_n) = 0$ e $g(\beta_1), \ldots, g(\beta_s) = 0$ (per le formule di Viete). Pertanto, i calcoli precedentemente fatti possono essere ripetuto i pari passo) per dimostrare che i determinanti (1.4) e (1.5), visti come polinomi in $\mathbb{K}[a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, \beta_s]$, sono uguali. Ora sono ammesse le semplificazioni con i termini comuni in quanto sono polinomi non nulli. (In un anello privo di divisori dello zero, come $\mathbb{K}[a_0, \alpha_1, \ldots, \alpha_n, b_0, \beta_1, \ldots, \beta_s]$, si può semplificare con qualunque elemento purché diverso dallo zero, cioè dal polinomio nullo). □

Chiaramente, se due polinomi $U(x_1, \ldots, x_r)$ e $V(x_1, \ldots, x_r$ sono uguali, (nel nostro caso D ed $R(f, g)$), allora $U(\xi_1, \ldots, \xi_r) = V(\xi_1, \ldots, \xi_r)$ per ogni r-pla $(\xi_1, \ldots, \xi_r)$ con $\xi_i \in \mathbb{K}$. In questo modo, possiamo dire che la semplificazione per un fattore comune non ha creato lacuna nelle argumentazioni.

Proposizione 1.1.1 *D è isobarico nelle indeterminate $a_0, \ldots, a_n, b_0, \ldots, b_s$ di peso $n \cdot s$. (Ossia ogni termine di D ha lo stesso peso.)*

Dimostrazione

Dato un termine generico di D :

$$ca_0^{i_0}a_1^{i_1}\cdot\ldots\cdot a_n^{i_n}b_0^{j_0}b_1^{j_1}\cdot\ldots\cdot b_s^{j_s}$$

definiamo peso di tale termine la seguente quantità: $\sum_{h=1}^{n} hi_h + \sum_{k=1}^{s} kj_k$.

Dimostreremo la proposizione usando la relazione $R(f,g) = D$.

Sia λ un elemento non nullo di $\mathbb{K}$, consideriamo, oltre ai polinomi $f(x)$ e $g(x)$ definiti all'inizio del paragrafo, due nuovi polinomi:

$$f_\lambda(x) = a_0x^n + a_1\lambda x^{n-1} + \cdots + a_{n-1}\lambda^{n-1}x + a_n\lambda^n$$

e

$$g_\lambda(x) = b_0x^s + b_1\lambda x^{s-1} + \cdots + b_{s-1}\lambda^{s-1}x + b_s\lambda^s.$$

Se α_i è radice di $f(x)$ allora $\lambda\alpha_i$ è radice di $f_\lambda(x)$ per ogni $i = 1,\ldots,n$ infatti:

$$\begin{aligned} f_\lambda(\lambda\alpha_i) &= a_0\lambda^n\alpha_i^n + a_1\lambda\lambda^{n-1}\alpha_i^{n-1} + \cdots + a_n\lambda^n \\ &= \lambda^n(a_0\alpha_i^n + \cdots + a_n) \\ &= \lambda^n f(\alpha_i) \\ &= 0 \end{aligned}$$

Analogamente se β_j è radice di $g(x)$ allora $\lambda\beta_j$ è radice di $g_\lambda(x)$ per ogni $j = 1,\ldots,s$.

Il risultante $R(f_\lambda, g_\lambda)$ dei polinomi appena definiti è uguale al determinante:

$$D_\lambda = \left|\begin{array}{ccccccccc} a_0 & \lambda a_1 & & & & \lambda^n a_n & & & \\ & a_0 & \lambda a_1 & & & & \lambda^n a_n & & \\ & & & \cdots & & \cdots & & & \\ & & & a_0 & \lambda a_1 & & & \lambda^n a_n & \\ b_0 & \lambda b_1 & & & \lambda^s b_s & & & & \\ & b_0 & \lambda b_1 & & & \lambda^s b_s & & & \\ & & & \cdots & & \cdots & & & \\ & & & & b_0 & \lambda b_1 & & \lambda^s b_s & \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} s \text{ righe} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \text{ righe} \end{array}$$

il cui generico termine è: $ca_0^{i_0}(\lambda a_1)^{i_1}(\lambda^2 a_2)^{i_2}\cdot\ldots\cdot(\lambda^n a_n)^{i_n}b_0^{j_0}(\lambda b_1)^{j_1}\cdot\ldots\cdot(\lambda^s b_s)^{j_s}$.
Mettendo λ in evidenza otteniamo:
$c\lambda^{i_1+2i_2+cdots+ni_n+j_1+2j_2+\cdots+sj_s}\cdot(a_0^{i_0}a_1^{i_1}\cdot\ldots\cdot a_n^{i_n}b_0^{j_0}b_1^{j_1}\cdot\ldots\cdot b_s^{j_s})$.
Ricordando la definizione 1.1.1 si ha: $R(f,g)=a_0^s b_0^n\prod_{i=1}^n\prod_{j=1}^s(\alpha_i-\beta_j)$ e
$R(f_\lambda,g_\lambda)=a_0^s b_0^n\prod_{i=1}^n\prod_{j=1}^s(\lambda\alpha_i-\lambda\beta_j)=a_0^s b_0^n\lambda^{ns}\prod_{i=1}^n\prod_{j=1}^s(\alpha_i-\beta_j)=\lambda^{ns}R(f,g)$.
Allora $D_\lambda=R(f_\lambda,g_\lambda)=\lambda^{ns}R(f,g)=\lambda^{ns}D$.
Da cui segue: $\lambda^{i_1+2i_2+\cdots+j_1+\cdots+sj_s}=\lambda^{ns}$, ottenendo quanto richiesto. □

Lo sviluppo del determinante (1.2) fornisce un polinomio omogeneo nelle $n+s+2$ indeterminate $a_0,\ldots,a_n,b_0,\ldots,b_s$, il cui generico termine ha grado $n+s$. Vediamo alcune proprietà del polinomio D e quindi di $R(f,g)$.

Teorema 1.1.2 *Il polinomio $D(a_0,\ldots,a_n,b_0,\ldots,b_s)$ è omogeneo sia nelle indeterminate $a_0,\ldots,a_n$ che nelle indeterminate $b_0,\ldots,b_s$.*

Dimostrazione

Il termine generico del determinante D è:

$$a_0^{i_0}a_1^{i_1}\cdot\ldots\cdot a_n^{i_n}b_0^{j_0}b_1^{j_1}\cdot\ldots\cdot b_s^{j_s}$$

dove i fattori a_h, ciascuno contato con la molteplicità i_h, sono in numero di $\sum i_h = s$ in quanto essi sono tutti e soli i fattori che provengono dalle prime s righe di 1.2. Perciò $D(a_0,\ldots,b_s)$ visto come polinomio nelle sole indeterminate $a_0,\ldots,a_n$ è una somma di monomi tutti dello stesso grado pari ad s. Quindi tale polinomio è omogeneo in $a_0,\ldots,a_n$. In modo analogo si prova l'asserto per le indeterminate $b_0,\ldots,b_s$.
□

Teorema 1.1.3 *Il polinomio $D(a_0,\ldots,a_n,b_0,\ldots,b_s)$ risulta irriducibile sopra $\mathbb{K}$, e sopra una qualunque sua estensione.*

Dimostrazione

Nel dimostrare il teorema useremo la relazione esistente tra D e $R(f,g)$.

Supponiamo per assurdo che D sia riducibile, ossia esistono due polinomi $P(a_0,\ldots,a_n,b_0,\ldots,b_s)$ e $Q(a_0,\ldots,a_n,b_0,\ldots,b_s)$ non costanti tale che $D = P\cdot Q$, con P e Q omogenei[1].

Introduciamo nuove indeterminate $a_1^{'},a_2^{'},\ldots,a_n^{'},b_1^{'},b_2^{'},\ldots,b_s^{'}$ con $a_i^{'}=(-1)^i a_i/a_0$ e $b_j^{'}=(-1)^j b_j/b_0$ per $i=1,\ldots,n$ e $j=1,\ldots,s$.

Quindi $D(a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_s)=D(a_0,a_0a_1^{'},\ldots,a_0a_n^{'},b_0,b_0b_1^{'},\ldots,b_0b_s^{'})$.

Per l'omogeneità di D segue[2]:

$D(a_0,a_0a_1^{'},\ldots,a_0a_n^{'},b_0,b_0b_1^{'},\ldots,b_0b_s^{'})=a_0^s b_0^n D(1,a_1^{'},\ldots,a_n^{'},1,b_1^{'},\ldots,b_s^{'})$.

Poniamo $D(1,a_1^{'},\ldots,a_n^{'},1,b_1^{'},\ldots,b_s^{'})=D^{'}=(a_1^{'},\ldots,a_n^{'},b_1^{'},\ldots,b_s^{'})$; il polinomio $D^{'}$ non è costante, in quanto $a_0^s b_0^n$ non divide D. Da cui discende:

$D^{'}(a_1^{'},\ldots,a_n^{'},b_1^{'},\ldots,b_s^{'})=P^{'}(a_1^{'},\ldots,a_n^{'},b_1^{'},\ldots,b_s^{'})\cdot Q^{'}(a_1^{'},\ldots,a_n^{'},b_1^{'},\ldots,b_s^{'})$.

Consideriamo $R^{'}(f,g)=R(f,g)/(a_0^s b_0^n)=D/(a_0^s b_0^n)=D^{'}=P^{'}Q^{'}$; esprimendo le $a_i^{'}$ e $b_j^{'}$ come funzioni simmetriche elementari nelle α_i e β_j si ottiene: $P^{'}\cdot Q^{'}=\prod_{i=1}^{n}\prod_{j=1}^{s}(\alpha_i-\beta_j)$. Preso il fattore $(\alpha_i-\beta_j)$, esso divide $P^{'}\cdot Q^{'}$ essendo irriducibile deve dividere uno dei due polinomi. Supponiamo che $P^{'}$ contenga il suddetto fattore, perciò, quale polinomio simmetrico sia nelle α_i che nelle β_j li contiene tutti. Dunque $Q^{'}$ si riduce ad una costante, da cui segue l'irriducibilità di $D^{'}$ e quindi di D. □

Teorema 1.1.4 *Dati due polinomi $f(x),g(x)$ a coefficienti in $\mathbb{K}$, esistono due polinomi $A(x)$ e $B(x)$ di $grado\,A(x)<(s-1)$ e $grado\,B(x)<(n-1)$ tale che*

$$R(f,g)=A(x)f(x)+B(x)g(x).$$

[1] Se F è un polinomio omogeneo riducibile, allora i suoi fattori sono altresì omogenei. (prop 1.3.2)

[2] Vedere paragrafo 3 del seguente capitolo

Dimostrazione

Scriviamo

$$f(x) = a_0x^n + \cdots + a_{n-1}x + a_n$$

$$g(x) = b_0x^s + \cdots + b_{s-1}x + b_s$$

e consideriamo le seguenti identità:

$$\begin{aligned}
x^{s-1}f(x) &= a_0x^{n+s-1} + \cdots + a_{n-1}x^s + a_nx^{s-1} \\
x^{s-2}f(x) &= a_0x^{n+s-2} + \cdots + a_{n-1}x^{s-1} + a_nx^{s-2} \\
&\cdots\cdots \\
f(x) &= a_0x^n + \cdots + a_{n-1}x + a_n \\
x^{n-1}g(x) &= b_0x^{s+n-1} + \cdots + b_{s-1}x^n + b_sx^{n-1} \\
x^{n-2}g(x) &= b_0x^{s+n-2} + \cdots + b_{s-1}x^{n-1} + b_sx^{n-2} \\
&\cdots\cdots \\
g(x) &= b_0x^s + \cdots + b_{s-1}x + b_s.
\end{aligned}$$

Il determinante dei coefficienti a secondo membro, delle precedenti identità coincide con il determinante 1.2.

Siano A_i per $i = 1, \ldots, s-1$ e B_j per $j = 1, \ldots, n-1$ i cofattori del determinante 1.2 rispetto all'ultima colonna muniti di segno. Moltiplichiamo la i-ma delle prime s righe per A_i e, similmente, la i-ma delle rimanenti n righe per B_i. Sommando poi le righe otteniamo:

$$A(x)f(x) + B(x)g(x) = R(f, g)$$

con $A(x) = A_0x^{s-1} + \cdots + A_{s-1}$ e $B(x) = B_0x^{n-1} + \cdots + B_{n-1}$ $\square$

Teorema 1.1.5 (Teorema di Study) *Dato un campo $\mathbb{K}$ algebricamente chiuso, siano f e g polinomi nelle indeterminate $x_1, \ldots, x_r$ a coefficienti in $\mathbb{K}$, e sia f irriducibile sopra $\mathbb{K}$.*
Se ogni radice $(\xi_1, \ldots, \xi_r)$ di f è radice di g allora f divide g.

Dimostrazione Possiamo usare induzione sul numero r delle indeterminate, essendo l'asserto notoriamente vero per $r = 1$.

Scriviamo:

$$f(x_1, \ldots, x_r) = a_0(x_1, \ldots, x_{r-1})x_r^n + a_1(x_1, \ldots, x_{r-1})x_r^{n-1} + \cdots + a_n(x_1, \ldots, x_{r-1})$$

considerandolo come un polinomio nella sola variabile x_r. Due casi si trattano separatamente secondoché in l'indeterminata x_r è presente o meno in f.

Incominciamo con il secondo caso supponendo che in f manchi x_r, ossia $f(x_1, \ldots, x_r) = f(x_1, \ldots, x_{r-1})$. Prendiamo una qualunque radice $(\xi_1, \ldots, \xi_{r-1})$ of f, cioé $f(\xi_1, \ldots, \xi_{r-1}) = 0$. Per ogni $t \in \mathbb{K}$, abbiamo $f(\xi_1, \ldots, \xi_{r-1}, t) = f(\xi_1, \ldots, \xi_{r-1}) = 0$. Dall'ipotesi del teorema, $g(\xi_1, \ldots, \xi_{r-1}, t) = 0$. Scriviamo

$$g(x_1, \ldots, x_r) = b_0(x_1, \ldots, x_{r-1})x_r^m + b_1(x_1, \ldots, x_{r-1})x_r^{m-1} + \cdots + b_m(x_1, \ldots, x_{r-1}).$$

Qui $m \geq 1$, altrimenti $g(x_1, \ldots, x_r) = g(x_1, \ldots, x_{r-1})$ e l'asserto segue per induzione. Pertanto il polinomio $b_0(\xi_1, \ldots, \xi_{r-1})T_r^m + b_1(\xi_1, \ldots, \xi_{r-1})T_r^{n-1} + \cdots + b_m(\xi_1, \ldots, \xi_{r-1})$ ha grado positivo e ogni $t \in \mathbb{K}$ è una sua radice. Ma allora, tutti i suoi coefficienti, $b_i(\xi_1, \ldots, \xi_{r-1})$, $0 \leq i \leq m$, sono nulli. Poiché il teorema vale, grazie all'ipotesi induttiva, per $r - 1$, abbiamo che $f(x_1, \ldots, x_{r-1})$ deve dividere $b_i(x_1, \ldots, x_{r-1})$. Ne segue che esistono polinomi $u_i(x_1, \ldots, x_{r-1})$, con $0 \leq i \leq m$, tali che $b_i(x_1, \ldots, x_{r-1}) = u_i(x_1, \ldots, x_{r-1})f(x_1, \ldots, x_{r-1})$. Ma allora,

$$g(x_1, \ldots, x_r) = f(x_1, \ldots, x_{r-1})(u_0(x_1, \ldots, x_{r-1})x_r^m + \cdots + u_m(x_1, \ldots, x_{r-1})),$$

quindi segue la tesi del teorema.

Nel primo caso,

$$f(x_1,\ldots,x_r) = a_0(x_1,\ldots,x_{r-1})x_r^n + a_1(x_1,\ldots,x_{r-1})x_r^{n-1} + \cdots + a_n(x_1,\ldots,x_{r-1})$$

è un polinomio in x_r di grado positivo. I coefficienti $a_i(x_1,\ldots,x_{r-1})$ sono in $\mathbb{K}[x_1,\ldots,x_{r-1}]$, e possono essere considerati elementi del campo razionale $\mathbb{L} = \mathbb{K}(x_1,\ldots,x_{r-1})$ di $\mathbb{K}[x_1,\ldots,x_{r-1}]$, ossia $f(x_1,\ldots,x_r) \in \mathbb{L}[x_r]$. Allo stesso modo $g(x_1,\ldots,x_r)$ può essere visto come un polinomio in $\mathbb{L}[x_r]$. Sia $R(f,g)$ il risultante di f e g visti come polinomi in $\mathbb{L}[x_r]$. Per il teorema $R(f,g) = D(a_0,a_1,\ldots,a_n,b_0,b_1,\ldots,b_m)$ dove, attualmente, $a_i = a_i(x_1,\ldots,x_{r-1})$ per $0 \leq i \leq n$ e $b_i = b_i(x_1,\ldots,x_{r-1})$ per $0 \leq i \leq m$, abbiamo che $R(f,g)$ è un polinomio nelle indeterminate $x_1,\ldots,x_{r-1}$. Per un precedente teorema, $R(f,g) = A(x_r)f(x_1,\ldots,x_r) + B(x_r)g(x_1,\ldots,x_r)$ dove $A(x_r) \in \mathbb{L}(x_r)$ e $B(x_r) \in \mathbb{L}(x_r)$ e $\deg(A(x_r)) < m$ and $\deg(B(x_r)) < n$. Come abbiamo visto nella dimostrazione di quel teorema, i coefficienti di $A(x_r)$ sono cofattori di una matrice i cui elementi sono gli a_i ed i b_i. Pertanto i coefficienti di $A(x_r)$ sono polinomi in $K[x_1,\ldots,x_{r-1}]$, e quindi $A(x_r) \in K[x_1,\ldots,x_r]$. Lo stesso vale per $B(x_r)$. Ne segue che $R(f,g) = A(x_r)f(x_1,\ldots,x_r) + B(x_r)g(x_1,\ldots,x_r)$ è un'equazione polinomiale in $\mathbb{K}[x_1,\ldots,x_r]$. Sia $(\xi_1,\ldots,\xi_{r-1})$ una qualunque $(r-1)$-upla con $\xi_i \in \mathbb{K}$. Poiché non manca x_r in f, il polinomio $a_0(\xi_1,\ldots,\xi_{r-1})T_r^n + a_1(\xi_1,\ldots,\xi_{r-1})T_r^{n-1} + \cdots + a_n(\xi_1,\ldots,\xi_{r-1})$ ha grado positivo, quindi ha almento una radice che chiamiamo ξ_r. Pertanto $f(\xi_1,\ldots,\xi_{r-1},\xi_r) = 0$, e, per l'ipotesi, anche $g(\xi_1,\ldots,\xi_{r-1},\xi_r) = 0$. Ma allora, anche $R(f,g) = 0$ per $(\xi_1,\ldots,\xi_{r-1})$, perciò, $R(f,g)$ è identicamente nullo. Ne segue che

$$A(x_1,\ldots,x_r)f(x_1,\ldots,x_r) = -B(x_1,\ldots,x_r)g(x_1,\ldots,x_r)$$

quindi $f(x_1,\ldots,x_r)$ divide $-B(x_1,\ldots,x_r)g(x_1,\ldots,x_r)$ essendo per ipotesi f irriducibile deve dividere uno dei due polinomi, ma poiché $\deg(B) < \deg(f)$, allora f

divide g. $\square$

Proposizione 1.1.2 *Se $\mathbb{K}$ è un campo algebricamente chiuso ed $f(x, y)$ è un polinomio non costante a coefficienti in $\mathbb{K}$, allora l'equazione $f(x, y) = 0$ ha infinite soluzioni in $\mathbb{K}$.*

Dimostrazione

Possiamo supporre che $f(x, y)$ contenga qualche termine contenente x e qualche termine contenente y, altrimenti $f(x, y)$ è un polinomio in una sola indeterminata, diciamo $f(x, y) = h(x)$, e se ξ è una radice di $h(x)$ allora ogni (ξ, η) con $\eta \in \mathbb{K}$ è soluzione dell'equazione $f(x, y) = 0$.

Scriviamo $f(x, y) = a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y)$ con $n \geq 1$ (e $\deg(a_i(y)) \geq 1$ per qualche i). Gli elementi $\alpha \in \mathbb{K}$ che sono radici di $a_i(y)$ costituiscono un insieme Δ finito. Pertanto $\mathbb{K} \setminus \Delta$ è un insieme infinito. Per ogni $\eta \in \mathbb{K} \setminus \Delta$, il polinomio $h(x) = f(x, \eta) = a_0(\eta)x^n + a_1(\eta)x^{n-1} + \cdots + a_{n-1}(\eta)x + a_n(\eta)$ ha grado positivo, quindi ammette almeno una radice ξ in $\mathbb{K}$, dipendente da η. Per valori η distinti, si ottengono coppie (ξ, η) distinte. Pertanto la loro cardinalità, quindi il numero delle soluzioni $f(x, y) = 0$ è infinito. $\square$

Consideriamo i polinomi (1.1) se $a_0, b_0 \neq 0$ allora f e g hanno una radice in comune se e solo se $R(f, g) = 0$.

Se a_0 o b_0 o entrambi sono nulli l'espressione 1.1.1 per il risultante non è più utilizzabile, conviene sostituirla con D, tenendo conto che $D = R(f, g)$ se $a_0 \neq 0$ e $b_0 \neq 0$. Non si può affermare che l'esistenza di radici comuni a f e g sia equivalente all'annullarsi del risultante. Infatti se $a_0 = b_0 = 0$ risulta in ogni caso $R(f, g) = 0$, indipendentemente dall'esistenza di radici comuni, ma questo è l'unico caso in cui l'annullarsi del risultante non garantisce che vi siano radici comuni.

Proposizione 1.1.3 *Se i coefficienti direttori dei polinomi f e g dati da (*1.1*) non si annullano entrambi allora $R(f,g)=0$ se e solo se i due polinomi hanno una radice in comune.*

Dimostrazione

Supponiamo $a_0 \neq 0$, sia $b_0 = b_1 = \cdots = b_{k-1} = 0$, ma $b_k \neq 0$ poniamo

$$\overline{g}(x) = b_k x^{s-k} + b_{k+1} x^{s-(k+1)} + \cdots + b_{s-1}x + b_s$$

poiché i coefficienti direttori di f e $\overline{g}$ sono entrambi non nulli, allora l'annullarsi di $R(f,\overline{g})$ è, necessario e sufficiente affinché f e $\overline{g}$ abbiano una radice in comune.
Sostituendo in 1.2 gli elementi $b_0, b_1, \ldots, b_{k-1}$ con degli zeri e applicando il teorema di Laplace, otteniamo $R(f,g) = a_0^k R(f,\overline{g})$.
I polinomi $g(x)$ e $\overline{g}(x)$ hanno le stesse radici, quindi $R(f,g) = 0 \Leftrightarrow a_0^k R(f,\overline{g}) = 0$.

Proposizione 1.1.4 *Ogni polinomio omogeneo nelle indeterminate $a_0, \ldots, a_n, b_0, \ldots, b_s$ che si annulli ogni volta che le equazioni $f(X) = a_0X^n + \ldots + a_n = 0$ e $g(X) = b_0X^s + \ldots + + b_s = 0$ hanno una radice in comune, è divisibile per $D(a_0, \ldots, a_n, b_0, \ldots, b_s)$.*

Dimostrazione

Sia $S(a_0, \ldots, a_n, b_0, \ldots, b_s$ un polinomio tale che se i polinomi $f(X) = a_0X^n + \ldots + a_n = 0$ e $g(X) = b_0X^s + \ldots + + b_s = 0$ hanno una radice in comune, allora $S(a_0, \ldots, a_n, b_0, \ldots, b_s) = 0$. D'altro canto, se i polinomi $f(X) = a_0X^n + \ldots + a_n = 0$ e $g(X) = b_0X^s + \ldots + + b_s = 0$ hanno una radice in comune, allora $D(a_0, \ldots, a_n, b_0, \ldots, b_s) = 0$. Poiché il polinomio $D(a_0, \ldots, a_n, b_0, \ldots, b_s) = 0$ è irriducibile sopra ogni estensione di $\mathbb{K}$, l'asserto segue dal Teorema 1.1.5.

1.2 Eliminazione di una incognita in un sistema di due equazioni in due incognite

Siano f e g due polinomi nelle indeterminate x e y a coefficienti in $\mathbb{K}$.

Scriviamoli secondo le potenze decrescenti di x :

$$\begin{array}{c} f(x,y) = a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y) \\ g(x,y) = b_0(y)x^s + b_1(y)x^{s-1} + \cdots + b_{s-1}(y)x + b_s(y) \end{array} \tag{1.8}$$

in tal modo i coefficienti sono polinomi nell'anello $\mathbb{K}[y]$.

Sia $R_y(f,g)$ il risultante dei polinomi f e g considerati come polinomi in x. Per le proprietà del risultante, $R_y(f,g)$ è un polinomio $D(y)$ nella indeterminata y e a coefficienti in $\mathbb{K}$ dato dallo sviluppo del seguente determinante:

$$D(y) = \left| \begin{array}{ccccccccc} a_0(y) & a_1(y) & & & & a_n(y) & & & \\ & a_0(y) & a_1(y) & & & & a_n(y) & & \\ & & & \cdots & & \cdots & & & \\ & & & a_0(y) & a_1(y) & & & a_n(y) & \\ b_0(y) & b_1(y) & & & b_s(y) & & & & \\ & b_0(y) & b_1(y) & & & b_s(y) & & & \\ & & & \cdots & & \cdots & & & \\ & & & & b_0(y) & b_1(y) & & b_s(y) & \end{array} \right| \begin{array}{l} \left. \vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}} \right\} s \text{ righe} \\ \left. \vphantom{\begin{array}{c} a \\ a \\ a \\ a \end{array}} \right\} n \text{ righe} \end{array} \tag{1.9}$$

Invertendo i ruoli di x e y, il determinante $D(x)$ si introduce analogamente.

Se i due polinomi (1.8) hanno una radice in comune: $x = \alpha,\ y = \beta$, sostituendo in (1.8) a y il valore β otteniamo due polinomi nell'indeterminata x : $f(x,\beta)$ e $g(x,\beta)$. Questi polinomi hanno una radice in comune α, per cui il loro risultante deve annullarsi: β sarà radice di $R_y(f,g)$.

Viceversa se il risultante $R_y(f,g)$ dei polinomi (1.8) ammette una radice β, allora il risultante dei polinomi $f(x,\beta)$ e $g(x,\beta)$ si annulla, ossia:

o i polinomi $f(x,\beta)$ e $g(x,\beta)$ hanno una radice in comune, oppure i loro coefficienti direttori $a_0(\beta)$ e $b_0(\beta)$ sono entrambi nulli.

La determinazione delle radici comuni ai polinomi (1.8) è ricondotta alla determinazione delle radici del polinomio (1.9) nell'indeterminata y; ciò si esprime dicendo che l'indeterminata x è stata eliminata dal sistema formato dalle equazioni dei polinomi oppure che l'equazione $D(y) = 0$ è il risultato dell'eliminazione della x tra le (1.8). I seguenti esempi fanno vedere come il procedimento di eliminazione si effettui in casi concreti.

Esempio 1 Determinare le radici comuni ai polinomi $f(X,Y) = X^2Y + 3XY + 2Y + 3$ e $g(X,Y) = 2XY - 2X + 2Y + 3$. Con calcoli diretti si ottiene $R_y(f,g) = 2y^2 + 11y + 12$. Le radici del polinomio $2Y^2 + 11Y + 12$ sono $y_1 = -4, y_2 = -\frac{3}{2}$. Per questi due valori di y, i coefficienti direttori dei polinomi f e g non si annullano, quindi sia l'una che l'altra, assieme ad in opportuno valore x, fornisce una radice comune. I polinomi $f_4(X) = -4X^2 - 12X - 5,\ g_4(X) = -10X - 5$ hanno una radice in comune: $x_1 = -\frac{1}{2}$. Similmente, $x_2 = 0$ è una radice comune ad $f_{-\frac{3}{2}}(X) = -\frac{3}{2}X^2 - \frac{9}{2}X$ e $g_{\frac{3}{2}} = -5X$. Pertanto, la soluzione del problema è data da due coppie $(-\frac{1}{2}, -4)$ e $(0, -\frac{3}{2})$.

Nelle dimostrazioni dei due teoremi successivi risulterà utile la seguente osservazione. Si denoti con $\mathbb{L}$ il campo quoziente dell'anello $\mathbb{K}[y]$, e con $\mathbb{L}[x]$ l'anello dei polinomi a coefficienti in $\mathbb{L}$. Allora, $f(x,y) = a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y) \in \mathbb{L}[x]$ e $g(x,y) = b_0(y)x^s + b_1(y)x^{s-1} + \cdots + b_{s-1}(y)x + b_s(y) \in \mathbb{L}[x]$, e si può considerare il risultante di questi due polinomi, che sarà denotato con $R_y(f,g)$, Per il teorema fondamentale di Sylvester, si ha $R_y(f,g) = D(y)$. In forza del Teorema 1.1.4 applicato ad $f(x,y)$ e ad $g(x,y)$, visti come polinomi in $\mathbb{L}[x]$, si ha $R_y(f,g) = A_y(x)f(x,y) + B_y(x)g(x,y)$ dove $A_y(x), B_y(x) \in \mathbb{L}[x]$ e $\deg(A_y(x) < s$, $\deg(B_y(x)) < n$. Notiamo come $A_y(x) \in \mathbb{L}[x]$ vuol dire che esistono funzioni razionali $A_i(y) = a_i(y)/c_i(y)$ con $a_i(y), c_i(y) \in \mathbb{K}[y]$ tali che $A_y(x) = A_0(y)x^n + \ldots + A_n(y)$. Analogamente, $B_y(x) = B_0(y)x^s + \ldots + B_s(y)$.

In realtà, ripercorrendo la dimostrazione del Teorema 1.1.4, ponendovi $\mathbb{L}$ al posto di $\mathbb{K}$, si vede che le funzioni razionali $A_i(y)$ e $B_i(y)$ sono polinomi in y. Pertanto, $A_y(x) = A(x,y) \in \mathbb{K}[x,y]$ e $B_y(x) = B(x,y) \in \mathbb{K}[x,y]$ e, inoltre, $R_y(f,g) = A_y(x)f(x,y) + B_y(x)g(x,y)$ implica

$$D(y) = A(x,y)f(x,y) + B(x,y)g(x,y) \tag{1.10}$$

dove $\deg(A(x,y))$ in y è minore di s e $\deg(B(x,y))$ in y è minore di n.

Teorema 1.2.1 *Supponiamo che $\mathbb{K}$ sia algebricamente chiuso. Il sistema (1.8) ha infinite soluzioni se e soltanto se i polinomi $f(x,y)$ e $g(x,y)$ hanno un fattore non costante in comune.*

Dimostrazione Supponiamo che il sistema (1.8) abbia infinite soluzioni.

Se $D(y)$ è il polinomio identicamente nullo, da (1.10) segue $A(x,y)f(x,y) = -B(x,y)g(x,y)$, Notiamo che $f(x,y)$ non divide $B(x,y)$, essendo $\deg(B(x,y))$ in y minore di n (uguale a $\deg(f(x,y))$ in y). Perciò, qualche fattore non costante $h(x,y)$ di $f(x,y)$ dovrà dividere $g(x,y)$. Tale polinomio $h(x,y)$ è un fattore comune ad $f(x,y)$ e $g(x,y)$.

Se $D(y)$ non è identicamente nullo, $D(y)$ ha un numero finito di radici. Ne segue l'esistenza di almeno un elemento $\eta \in \mathbb{K}$ tale che entrambe le equazioni $f(x,\eta) = 0$ e $g(x,\eta) = 0$ hanno infinite soluzioni. Ma allora il polinomio $F(x) = f(x,\eta)$ ha infinite radici, quindi $F(x)$ è il polinomio nullo. Poiché $F(x) = f(x,\eta) = a_0(\eta)x^n + a_1(\eta)x^{n-1} + \cdots + a_{n-1}(\eta)x + a_n(\eta)$, ne segue $a_0(\eta) = \ldots = a_n(\eta) = 0$. Se $\mathbb{L}$ denota il campo quoziente di $\mathbb{K}[x]$ e si considera $U(y) = f(x,y)$ quale elemento di $\mathbb{L}[y]$, ciò implica $U(\eta) = 0$ quindi $(y-\eta) \mid U(y)$. Pertanto, $f(x,y) = (y-\eta)d(x,y)$ con $d(x,y) \in \mathbb{K}[x,y]$. Similmente si pone $V(y) = g(x,y)$ e si vede che esiste $e(x,y) \in \mathbb{K}[x,y]$ tale che $g(x,y) = (y-\eta)e(x,y)$. Da ciò discende che $y - \eta$ è un fattore non costante comune ad $f(x,y)$ e $g(x,y)$.

Viceversa, si suppone che $f(x,y) = h(x,y)f^*(x,y), g(x,y) = h(x,y)g^*(x,y)$ per un polinomio non constante $h(x,y)$. Ovviamente, ogni soluzione dell'equazione $h(x,y)$ è altresì una soluzione del sistema (1.8). Basta pertanto far vedere che $h(x,y) = 0$ ha infinite soluzioni. Ma questo discende dalla Proposizione 1.1.2. □

Teorema 1.2.2 *Supponiamo che $\mathbb{K}$ sia algebricamente chiuso. Il sistema (1.8) ha infinite soluzioni se e soltanto se $R_y(f,g) = D(y)$ oppure $R_x(f,g) = D(x)$ (o entrambi) è identicamente nullo.*

Dimostrazione Ripercorrendo la dimostrazione del Teorema 1.2.1, vediamo che se il sistema (1.8) ha infinite soluzioni ma $D(y)$ non è identicamente nullo, allora $y - \eta$ è un fattore comune ai polinomi $U(y) = f(x,y)$ e $V(y) = g(x,y)$. Ma allora, il risultante $R_x(U,V)$ è uguale a 0. D'altro canto, $R_x(U,V) = D(x)$, e l'asserto segue.

Viceversa, supponiamo che $D(y)$ sia il polinomio nullo. Scegliamo $\eta \in \mathbb{K}$ in modo che $a_0(\eta) \neq 0$ e $b_0(\eta) \neq 0$. Allora il sistema $f_1(x) = f(x,\eta) = 0, g_1(x) = g(x,\eta) = 0$ ammette almeno una soluzione, essendo $R(f_1,g_1) = 0$ in forza della relazione $R(f_1,g_1) = D(\eta) = 0$. Presa una qualunque delle soluzioni $\xi \in \mathbb{K}$ abbiamo che $f_1(\xi) = 0, g_1(\xi) = 0$ quindi $f(\xi,\eta) = 0, g(\xi,\eta) = 0$. Ciò mostra che (ξ,η) è una soluzione del sistema $f(x,y) = 0, g(x,y) = 0$. Poiché $a_0(y)$ e $b_0(y)$ sono polinomi non nulli, entrambi hanno un numero finito di radici. Se omettiamo queste radici da $\mathbb{K}$, restano comunque infiniti valori η utili per il nostro ragionamento. Pertanto, il sistema ha infinite soluzioni. □

Esempio

$$\begin{array}{c} f(x,y) = (y-\eta)(x+y) \\ g(x,y) = (y-\eta)x^2 \end{array} \tag{1.11}$$

ha infinite soluzioni, essendo (ξ,η) per ogni $\xi \in \mathbb{K}$ è una soluzione. Il determinante $D(x)$ è identicamente nullo, ma non lo è $D(y)$. Infatti, $f(x,y) = y^2 + (x-\eta)y - \eta x$

e $g(x,y) = x^2y - \eta x^2$, quindi

$$D(x) = \begin{vmatrix} 1 & x-\eta & -\eta x \\ x^2 & -\eta x^2 & 0 \\ 0 & x^2 & -\eta x^2 \end{vmatrix} = 0,$$

D'altro canto, $f(x,y) = (y-\eta)x + y^2 - \eta y$ e $g(x,y) = x^2(y-\eta)$, quindi

$$D(y) = \begin{vmatrix} y-\eta & 0 & 0 \\ y-\eta & y^2-\eta y & 0 \\ 0 & y-\eta & y^2-\eta y \end{vmatrix} = (y-\eta)^3 y^2 \neq 0.$$

Teorema 1.2.3 *Se $R_y(f,g)$ non è identicamente nullo, il suo grado può essere al più $N \cdot S$, dove N indica il grado di $f(x,y)$ e S quello di $g(x,y)$ nelle indeterminate x e y.*

Dimostrazione

Riscriviamo $f(x,y)$ e $g(x,y)$ secondo le potenze decrescenti di x ossia:

$$f(x,y) = a_0(y)x^n + \cdots + a_n(y) \qquad g(x,y) = b_0(y)x^s + \cdots + b_s(y).$$

Si hanno allora le seguenti limitazioni:

$$\begin{array}{cc} grado\, a_0(y) \leq N-n & grado\, b_0(y) \leq S-s \\ grado\, a_1(y) \leq N-(n-1) & grado\, b_1(y) \leq S-(s-1) \\ \vdots & \vdots \\ grado\, a_h(y) \leq N-(n-h) & grado\, b_k(y) \leq S-(s-k) \\ \vdots & \vdots \\ grado\, a_n(y) \leq N & grado\, b_s(y) \leq S \end{array} \tag{1.12}$$

Il generico termine dello sviluppo del determinante 1.9 è:

$$ca_0(y)^{i_0} a_1(y)^{i_1} \cdot \ldots \cdot a_n(y)^{i_n} b_0(y)^{j_0} b_1(y)^{j_1} \cdot \ldots \cdot b_s(y)^{j_s}$$

il cui grado per le 1.12 è minore o uguale a:

$$(N-n)i_0 + \cdots + (N-(n-h))i_h + \cdots + Ni_n + (S-s)j_0 + \cdots + (S-(s-k))j_k + \cdots + Si_s$$

che può scriversi come $(N-n)\sum_{i=0}^{n} i_h + (S-s)\sum_{k=0}^{s} j_k + \sum_{h=1}^{n} hi_h + \sum_{k=1}^{s} kj_k$ ricordando che: $\sum_{i=0}^{n} i_h = s$, $\sum_{k=0}^{s} j_k = n$, $\sum_{h=1}^{n} hi_h + \sum_{k=1}^{s} kj_k = ns$, la precedente somma diventa: $(N-n)s + (S-s)n + ns$.
Poiché $n \leq N$ e $s \leq S$ il grado del termine generico del determinante $D(y)$ non supera $N \cdot S$. □

Il precedente teorema ha il seguente corollario:

Corollario 1.2.1 *Se $f(x,y)$ e $g(x,y)$ sono privi di fattori comuni non costanti, allora il numero delle soluzioni del sistema*
$\begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases}$ *è minore o uguale a $N \cdot S$,*
cioè $f(x,y)$ e $g(x,y)$ hanno al più $N \cdot S$ radici in comune.

Dimostrazione

Si denoti con Δ l'insieme (finito) delle soluzioni (ξ, η) del sistema (1.8). Nel piano cartesiano, si considerino le curve piane $\mathcal{F}$ di equazione $f(x,y) = 0$ e $\mathcal{G}$ di equazione $g(x,y) = 0$. I punti di intersezione delle curve $\mathcal{F}$ e $\mathcal{G}$ ci danno le soluzioni del sistema (1.8), nel senso che (ξ, η) è soluzione del sistema (1.8) se e soltanto se il punto $P(\xi, \eta)$ è un punto di intersezione di $\mathcal{F}$ e $\mathcal{G}$. Le rette che passano per almeno due dei punti di intersezione (cioè le corde comuni) sono di numero finito. Scegliamo due rette per l'origine, dette ℓ_x ed ℓ_y, che non siano corde comuni. Esse avranno equazioni: $\ell_x : y = cx$, $\ell_y : y = dx$. Andiamo a sostituire x, y in $f(x,y)$ e $g(x,y)$ mediante

$$x = \frac{dX - Y}{d - c}, \quad y = \frac{cX - Y}{c - d},$$

ottenendo i polinomi $F(X,Y)$ e $G(X,Y)$ rispettivamente. Ovviamente, valgono $\deg(f(x,y)) = \deg(F(X,Y))$ e $\deg(g(x,y)) = \deg(G(X,Y))$, Inoltre, il numero delle soluzioni del sistema (1.8) è uguale a quello delle soluzioni del sistema

$F(X,Y)=0$, $G(X,Y)=0$. Inoltre, per ogni $\eta \in \mathbb{K}$ esiste al più uno $\xi \in \mathbb{K}$ tale che (ξ,η) sia una soluzione del sistema $F(X,Y)=0$, $G(X,Y)=0$. Ora applicando il teorema precedente a quest'ultimo sistema si ottiene l'asserto.

Proposizione 1.2.1 *Se $f(x,y)$ e $g(x,y)$ sono due polinomi che non contengono termini di grado minore di u e v rispettivamente, allora $y=0$ è radice di $R_y(f,g)=D(y)$ con molteplicità almeno pari a uv.*

Dimostrazione

Vediamo dapprima il caso $u=2$ e $v=2$: siano $f(x,y)$ di grado 3 e $g(x,y)$ di grado 2.

$$f(x,y)=a_{2,0}x^2+a_{1,1}xy+a_{0,2}y^2+a_{3,0}x^3+a_{2,1}x^2y+a_{1,2}xy^2+a_{0,3}y^3$$

$$g(x,y)=b_{2,0}x^2+b_{1,1}xy+b_{0,2}y^2.$$

Dobbiamo provare che $R_y(f,g)=D(y)$ è divisibile per y^4 dove

$$D(y)=\begin{vmatrix} a_{3,0} & a_{2,1}y+a_{2,0} & a_{1,1}y+a_{1,2}y^2 & a_{0,2}y^2+a_{0,3}y^3 & 0 \\ 0 & a_{3,0} & a_{2,1}y+a_{2,0} & a_{1,1}y+a_{1,2}y^2 & a_{0,2}y^2+a_{0,3}y^3 \\ b_{2,0} & b_{1,1}y & b_{0,2}y^2 & 0 & 0 \\ 0 & b_{2,0} & b_{1,1}y & b_{0,2}y^2 & 0 \\ 0 & 0 & b_{2,0} & b_{1,1}y & b_{0,2}y^2 \end{vmatrix}.$$

Di ogni elemento del determinante ne consideriamo solo il termine di grado più basso tralasciando gli altri. Otteniamo un nuovo determinante $E(y)$:

$$E(y)=\begin{vmatrix} a_{3,0} & a_{2,0} & a_{1,1}y & a_{0,2}y^2 & 0 \\ 0 & a_{3,0} & a_{2,0} & a_{1,1}y & a_{0,2}y^2 \\ b_{2,0} & b_{1,1}y & b_{0,2}y^2 & 0 & 0 \\ 0 & b_{2,0} & b_{1,1}y & b_{0,2}y^2 & 0 \\ 0 & 0 & b_{2,0} & b_{1,1}y & b_{0,2}y^2 \end{vmatrix}.$$

y^4 divide $D(y)$ se e solo se y^4 divide $E(y)$. Eseguiamo alcune operazioni elementari su $E(y)$:

1. moltiplichiamo la prima riga per y;

2. moltiplichiamo la seconda riga per y^2;

3. moltiplichiamo la quarta riga per y;

4. moltiplichiamo la quinta riga per y^2.

Otteniamo cosìun nuovo determinante $F(y)$:

$$F(y) = \begin{vmatrix} a_{3,0}y & a_{2,0}y & a_{1,1}y^2 & a_{0,2}y^3 & 0 \\ 0 & a_{3,0}y^2 & a_{2,0}y^2 & a_{1,1}y^3 & a_{0,2}y^4 \\ b_{2,0} & b_{1,1}y & b_{0,2}y^2 & 0 & 0 \\ 0 & b_{2,0}y & b_{1,1}y^2 & b_{0,2}y^3 & 0 \\ 0 & 0 & b_{2,0}y^2 & b_{1,1}y^3 & b_{0,2}y^4 \end{vmatrix}$$

cioè $F(y) = y^{1+2+1+2}E(y) = y^6E(y)$.
Dobbiamo provare che $F(y)$ è divisibile per y^{10}.
In $F(y)$, nell'ultima colonna ogni elemento è divisibile per y^4, nella penultima per y^3, nella terzultima per y^2 e nella quartultima per y. Da cui segue che sviluppando $F(y)$ otteniamo un polinomio in y in cui il primo termine non nullo è y^{10}. Quindi y^{10} divide $F(y)$ e y^4 divide $E(y)$, da cui segue y^4 divide $D(y)$ come volevamo.
Consideriamo il caso generale. I due polinomi si scrivono nella forma:

$$\begin{aligned} f(x,y) &= a_{u,0}x^u + a_{u-1,1}x^{u-1}y + \cdots + a_{1,u-1}xy^{u-1} + a_{0,u}y^u + \cdots \\ g(x,y) &= b_{v,0}x^v + b_{v-1,1}x^{v-1}y + \cdots + b_{1,v-1}xy^{v-1} + b_{0,v}y^v + \cdots \end{aligned}$$

Indichiamo con $a(i)$ l'esponente più basso presente nel termine $a_i(y)$, e con $b(i)$ quello di $b_i(y)$, si ha allora :

$$f(x,y) = a_0(y)x^n + a_1(y)x^{n-1} + \cdots + a_{n-1}(y)x + a_n(y), \quad a(n-i) \geq u - i$$

$$g(x,y) = b_0(y)x^s + b_1(y)x^{s-1} + \cdots + b_{s-1}(y)x + b_s(y), \quad b(s-i) \geq v - i$$

Sappiamo che $R_y(f,g) = D(y)$. Come nell'esempio consideriamo un nuovo determinante $E(y)$ ottenuto da $D(y)$ conservando i termini di grado più basso in ogni riga. Indicando con A le prime s righe e con B le rimanenti n righe
effettuaiamo delle operazioni come segue:
moltiplichiamo la $(s-i+1)-ma$ riga delle A per y^{v-i+1} per ogni $1 \leq i \leq v$, e la $(n-j+1)-ma$ riga delle B per y^{u-j+1} per ogni $1 \leq j \leq u$.
Dopo queste operazioni si vede che ciascun elemento della $(n+s-k)-ma$ colonna, con $0 \leq k \leq u+v$, è divisibile per y^{u+v-k}. Ne segue che $R_y(f,g)$ è divisibile per la potenza y^t dove:

$$t = \sum_{k=1}^{u+v} k - \sum_{i=1}^{u} i - \sum_{j=1}^{v} j = \frac{1}{2}(u+v)(u+v+1) - \frac{1}{2}u(u+1) - \frac{1}{2}v(v+1).$$

Da cui otteniamo $t = uv$, e quindi l'asserto. □

Commento Nella precedente dimostrazione abbiamo asserito che era sufficiente far vedere che $E(y)$ è divisible per y^{uv}. Ci proponiamo di dimostrare un asserto più generale. Fissiamo un insieme finito di indeterminate u_i, e denotiamo con $\mathbb{L} = \mathbb{K}(u_1, u_2, \ldots, u_k)$ il campo quoziente dell'anello $\mathbb{K}[u_1, u_2, \ldots, u_k]$. Consideriamo il polinomio $U(y)$ che si ottiene sviluppando un determinante i cui elementi d_{ij} appartengono $\mathbb{L}[y]$ cioè sono polinomi in y a coefficienti in $\mathbb{L}$. Inoltre, introduciamo il polinomio $V(y)$ che si ottiene sviluppando del precedente determinante $\{d_{ij}\}$ dopo avere conservato, in ciascun elemento del determinante, soltanto il termine e_{ij} di grado più basso. L'asserto è che se r è il più grande intero positivo tale che y^r divide $V(y)$, allora y^r deve dividere anche $U(y)$. Tenendo presente come si sviluppa un determinante, vediamo che $U(y) = V(y) + W(y)$ dove $\text{sottogrado}(V(y)) < \text{sottogrado}(W(y))$ dove $\text{sottogrado}(F(y))$ di un polinomio in y indica il grado minimo s di y in $F(y)$; cioè $F(y) = h(u_1, \ldots, u_k)y^s + h_1(u_1, \ldots, u_k)y^{s_1} + h_2(u_1, \ldots, u_k)y^{s_2} + \ldots$ con $s < s_1 < s_2 \ldots$. Pertanto, $s = \text{sottogrado}(V(y)) < \text{sottogrado}(W(y)) = t$ im-

plica che $V(y) = h(u_1, \ldots, u_k)y^s + h_1(u_1, \ldots, u_k)y^{s_1} + h_2(u_1, \ldots, u_k)y^{s_2} + \ldots$ and $W(y) = p(u_1, \ldots, u_k)y^t + p_1(u_1, \ldots, u_k)y^{t_1} + p_2(u_1, \ldots, u_k)y^{t_2} + \ldots$, dove $s < t$. Applicando questo asserto al caso in questione, abbiamo che $s = uv$, quindi $uv \leq t$. Ovviamente, per certe scelte $(\xi_1, \ldots, \xi_k)$, con $\xi \in \mathbb{K}$, risulta $h(\xi_1, \ldots, \xi_k) = 0$. Allora, $\text{sottogrado}\, V((\xi_1, \ldots, \xi_k)(y)) = uv + j$ con $m > 0$, ed eventualmente, $\text{sottogrado}\, W((\xi_1, \ldots, \xi_k)(y)) = uv+n$, con $m > n$; ma in ogni caso, $\text{sottogrado}\, U((\xi_1, \ldots, \xi_k)(y)) \geq uv$.

1.3 Risultante di due polinomi omogenei

Definizione 1.3.1 *Un polinomio $F(x_0, \ldots, x_r) \in \mathbb{K}[x_0, \ldots, x_r]$ di grado N si dice omogeneo o forma se è somma di monomi che hanno tutti lo stesso grado.*

Esempio 1.3.1 *Il polinomio: $x_1^2 x_2 x_3 + x_1 x_3^3$ è omogeneo mentre non lo è $x_1^2 x_2 x_3 + x_1 x_3^2$.*

Osservazione 1.3.1 *Ogni polinomio $f(x_0, \ldots, x_r) \in \mathbb{K}[x_0, \ldots, x_r]$ di grado N può scriversi nella forma:*

$$f(x_0, \ldots, x_r) = \Phi_0 + \Phi_1(x_0, \ldots, x_r) + \cdots + \Phi_i(x_0, \ldots, x_r) + \cdots + \Phi_N(x_0, \ldots, x_r)$$

essendo $\Phi_j(x_0, \ldots, x_r)$ polinomio omogeneo di grado j per $j = 0, \ldots, N$.
(In ogni Φ_j vengono scritti tutti e soli i termini di $f(x_0, \ldots, x_r)$ di grado j.)

Teorema 1.3.1 *Affinché un polinomio non nullo $f(x_0, \ldots, x_r)$ di grado N sia omogeneo, occorre e basta che si abbia:*

$$f(tx_0, \ldots, tx_r) = t^N f(x_0, \ldots, x_r) \quad \textit{per ogni } \ t \in \mathbb{K}.$$

Dimostrazione

Supponiamo che $f(x_0, \ldots, x_r)$ sia omogeneo allora:
$f(x_0, \ldots, x_r) = \Phi_N(x_0, \ldots, x_r) = \sum a_{i_0,\ldots,i_r} x_0^{i_0} \cdot \ldots \cdot x_r^{i_r}$ con $i_0 + \cdots + i_r = N$.
Ora

$$\begin{aligned} f(tx_0, \ldots, tx_r) &= \Phi_N(tx_0, \ldots, tx_r) = \sum a_{i_0,\ldots,i_r} x_0^{i_0} \cdot \ldots \cdot x_r^{i_r}\, t^{i_0+\cdots+i_r} \\ &= t^N \sum a_{i_0,\ldots,i_r} x_0^{i_0} \cdot \ldots \cdot x_r^{i_r} \\ &= t^N \Phi_N(x_0, \ldots, x_r) \\ &= t^N f(x_0, \ldots, x_r). \end{aligned}$$

Viceversa supponiamo che valga $f(tx_0, \ldots, tx_r) = t^N f(x_0, \ldots, x_r)$.
Scriviamo $f(x_0, \ldots, x_r) = \Phi_0 + \cdots + \Phi_i(x_0, \ldots, x_r) + \cdots + \Phi_N(x_0, \ldots, x_r)$.
Sostituendo x_i con tx_i otteniamo:

$$f(tx_0, \ldots, tx_r) = \Phi_0 + \cdots + \Phi_i(tx_0, \ldots, tx_r) + \cdots + \Phi_N(tx_0, \ldots, tx_r).$$

Applicando l'ipotesi su f e sui Φ_i essendo omogenei segue:

$$t^N f(x_0, \ldots, x_r) = \Phi_0 + \cdots + t^i \Phi_i(x_0, \ldots, x_r) + \cdots + t^N \Phi_N(x_0, \ldots, x_r).$$

Riscrivendo tale espressione si ha:

$$t^N(\Phi_N(x_0, \ldots, x_r) - f(x_0, \ldots, x_r)) + \cdots + \Phi_i(x_0, \ldots, x_r) + \cdots + \Phi_0 = 0. \quad (1.13)$$

che possiamo vederla come un polinomio in t di grado N, che ha pertanto N radici. Presa una $(r+1)$-upla qualsiasi $(\xi_0, \ldots, \xi_r)$ con $\xi_i \in \mathbb{K}$ essa risulta radice del polinomio 1.13 per ogni $t \in \mathbb{K}$ con $t \neq 0$, quindi avendo infinite radici 1.13 è il polinomio nullo; ossia $\Phi_i = 0$ per $i = 1, \ldots, N-1$ e $\Phi_N = f$, cioè $f(x_0, \ldots, x_r)$ è omogeneo.
□

Per un polinomio $F(x_0, \ldots, x_r)$ omogeneo di grado n vale la seguente regola detta *Regola di Eulero*:

$$\sum_i \frac{\partial F}{\partial x_i} x_i = nF.$$

Infatti essendo F omogeneo vale:
$t^n F(x_0, \ldots, x_r) = F(tx_0, \ldots, tx_r)$ per ogni $x_0, \ldots, x_r$ e per ogni t.
Derivando l'espressione su vista rispetto a t si ha:
$nt^{n-1} F(x_0, \ldots, x_r) = x_0 \frac{\partial F}{\partial x_0} + \cdots + x_r \frac{\partial F}{\partial x_r}$
ponendo $t = 1$ otteniamo l'asserto.

Proposizione 1.3.1 *Il prodotto di due polinomi omogenei è ancora un polinomio omogeneo.*

Dimostrazione

Siano $G(x_0, \ldots, x_r)$ e $H(x_0, \ldots, x_r)$ due polinomi omogenei con $grado\, G = M$ e $grado\, H = N$.

$GH = \left(\sum a_{i_0,\ldots,i_r} x_0^{i_0} \cdots x_r^{i_r}\right) \cdot \left(\sum b_{j_0,\ldots,j_r} x_0^{j_0} \cdots x_r^{j_r}\right) = \left(\sum c x_0^{i_0+j_0} \cdots x_r^{i_r+j_r}\right)$ con $\sum_{h=0}^{r}(i_h + j_h) = M + N$.

Quindi $grado\, GH = M + N$ per ogni termine. □

Proposizione 1.3.2 *Ogni fattore di un polinomio omogeneo è ancora un polinomio omogeneo*

Dimostrazione

Dato un polinomio omogeneo $F(x_0, \ldots, x_r) \in \mathbb{K}[x_0. \ldots, x_r]$, supponiamo che esistono altri due polinomi $f(x_0, \ldots, x_r)$ e $g(x_0, \ldots, x_r)$ tale che $F = f \cdot g$.

Mostriamo che f e g sono anch'essi omogenei. Se f non è una forma allora se lo scriviamo in termini di polinomi omogenei ci sono almeno due termini; analogamente per g. Quindi $f(x_0, \ldots, x_r) = \Phi_i(x_0, \ldots, x_r) + \cdots + \Phi_k(x_0, \ldots, x_r)$ e $g(x_0, \ldots, x_r) = \Psi_u(x_0, \ldots, x_r) + \cdots + \Psi_v(x_0, \ldots, x_r)$. Allora si ha:

$$F = fg = \Phi_i(x_0, \ldots, x_r)\Psi_u(x_0, \ldots, x_r) + \cdots + \Phi_k(x_0, \ldots, x_r)\Psi_v(x_0, \ldots, x_r).$$

Per la proposizione 1.3.1 $\Phi_j \cdot \Psi_l$ per $j = i, \ldots, k$ e $l = u, \ldots, v$ è omogeneo di grado $j + l$. Poiché F è omogeneo, per ipotesi, allora tutti i termini del prodotto hanno lo stesso grado quindi $i + u = k + v$ da cui segue $i = k$ e $u = v$. □

Teorema 1.3.2 *Dati* $n + 1$ *polinomi* $A_j(x_0, \ldots, x_{r-1}) \in \mathbb{K}[x_0, \ldots, x_{r-1}]$ *per* $j = 0, \ldots, n$ *definiamo un nuovo polinomio nelle* $r + 1$ *indeterminate* $x_0, \ldots, x_r$:

$$f(x_0, \ldots, x_r) = A_0(x_0, \ldots, x_{r-1})x_r^n + A_1(x_0, \ldots, x_{r-1})x_r^{n-1} + \cdots + A_n(x_0, \ldots, x_{r-1}).$$

Se tale polinomio è omogeneo allora anche i polinomi $A_j(x_0, \ldots, x_{r-1})$ *lo sono.*

Dimostrazione

Scriviamo $A_j(x_0, \ldots, x_{r-1})$ come somma di polinomi omogenei:

$$A_j(x_0, \ldots, x_{r-1}) = \Phi_i(x_0, \ldots, x_{r-1}) + \cdots + \Phi_k(x_0, \ldots, x_{r-1}).$$

Il prodotto $A_j(x_0, \ldots, x_{r-1})x_r^{n-j}$ è somma di polinomi $\Phi_i(x_0, \ldots, x_{r-1})x_r^{n-j} + \cdots + \Phi_k(x_0, \ldots, x_{r-1})x_r^{n-j}$, di grado $i + (n-j), \ldots, k + (n-j)$.

Se $l \neq j$, nessun addendo di $A_l(x_0, \ldots, x_{r-1})x_r^{n-l}$ contiene un termine del tipo $\Phi_j(x_0, \ldots, x_{r-1})x_r^{n-j}$, dall'ipotesi che $f(x_0, \ldots, x_r)$ sia omogeneo segue che $i + (n-j) = \cdots = k + (n-j)$, ossia $i = k$.

Quindi $A_j(x_0, \ldots, x_{r-1}) = \Phi_i(x_0, \ldots, x_{r-1})$ è omogeneo. $\square$

Dato un polinomio $F(x_0, \ldots, x_r)$, ponendo in esso $x_0 = 1$ otteniamo il polinomio $F(1, x_1, \ldots, x_r)$ che, in generale, non è omogeneo.

Introduciamo la mappa

$$\varphi_0 = \begin{cases} \mathbb{K}[x_0, x_1, \ldots, x_r] \to \mathbb{K}[x_1, \ldots, x_{r-1}]; \\ F(x_0, x_1, \ldots, x_r) \to f(x_1, \ldots, x_r) = F(1, x_1, \ldots, x_r). \end{cases}$$

Chiaramente, φ_0 è una mappa additiva e moltiplicativa, cioè $\varphi_0(F_1 + F_2) = \varphi(F_1) + \varphi(F_2)$ e $\varphi_0(F_1F_2) = \varphi(F_1)\varphi(F_2)$. Ora restringiamo il dominio di φ_0 all'insieme Ω dei polinomi omogenei di $\mathbb{K}[x_0, x_1, \ldots, x_r]$. Notiamo che Ω è chiuso rispetto alla moltiplicazione (il prodotto di due polinomi omogenei è altresì omogeneo), ma non lo è più rispetto all'addizione (la somma di due polinomi omogonei è omogoneo se soltanto se hanno il medesimo grado). Notiamo inoltre che $\varphi_0 = \Omega \to \mathbb{K}[x_1, \ldots, x_{r-1}]$ non è iniettiva, ad esempio i polinomi $F_1 = x_0x_1 \cdots x_r$ e $F_2 = x_0^2x_1 \cdots x_r$ hanno la stessa imagine $\varphi_0(F_1) = \varphi_0(F_2) = x_1 \cdots x_r$. Proviamo a quest'ultimo riguardo la seguente proposizione.

Per due polinomi omogenei $F_1 = F_1(x_0, x_1, \ldots, x_r)$ *e* $F_2 = F_2(x_0, x_1, \ldots, x_r)$ *si ha* $\varphi(F_1) = \varphi(F_2)$ *se e soltanto se* $F_1 = x_0^m F_2$ *oppure* $F_2 = x_0^m F_1$ *per un intero positivo* m. Se $F_1 = x_0^m F_2$, allora chiaramente $\varphi_0(F_1) = \varphi_0(F_2)$.

Per provare il viceversa, supponiamo che $\varphi(F_1) = \varphi(F_2)$. Senza ledere nella generalità, possiamo ammettere che $\deg(F_1) \geq \deg(F_2)$; poniamo $m = \deg(F_1) - \deg(F_2)$. Prendiamo un monomio $cx_1^{i_1} \cdots x_r^{i_r}$, con $c \in \mathbb{K} \setminus \{0\}$, e poniamo $n = i_1 + \ldots + i_r = \deg(cx_1^{i_1} \cdots x_r^{i_r})$. Allora $cx_0^{i_0} x_1^{i_1} \cdots x_r^{i_r}$ è un monomio G_1 di F_1 dove $i_0 = \deg(F_1) - n$. Similmente, $cx_0^{j_0} x_1^{i_1} \cdots x_r^{i_r}$ è un monomio G_2 di F_2 dove $j_0 = \deg(F_2) - n$. Ne segue che $i_0 - j_0 = \deg(F_1) - \deg(F_2) = m > 0$. Pertanto $x_0^m G_2 = G_1$, quindi $F_1 = x_0^m F_2$, come si voleva.

Si può osservare che la mappa di sopra può essere analogamente definita per ogni x_i ottenendo $r+1$ polinomi non omogenei associati ad F in r variabili $x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r$ per $0 \leq i \leq r$. Quindi dato un polinomio omogeneo ci sono tanti polinomi associati non omogenei quante sono le indeterminate in F.

Viceversa ad ogni polinomio $f(x_1, \ldots, x_r)$ possiamo associare un polinomio omogeneo $F(x_0, \ldots, x_r)$, nel seguente modo:

$$x_0^N \cdot f(\frac{x_1}{x_0}, \ldots, \frac{x_r}{x_0}) = F(x_0, x_1, \ldots, x_r) \tag{1.14}$$

essendo N il grado di $f(x_1, \ldots, x_r)$ nelle indeterminate $x_1, \ldots, x_r$. Osserviamo che $\varphi_0(F) = f$ e $\deg(F) = \deg(f)$. Poiché $\deg(f) \leq \deg(F)$, tra tutti i polinomi omegenei F tale che $\varphi_0(F) = f$, quello introdotto nella (1.14) ha il grado minimo. In virtù del precedente asserto (in corsivo), ogni polinomio omogeneo F tale che $\varphi_0(F) = f$ risulta essere multiplo della (1.14) per un fattore x_0^m con $m \geq 0$. Questo fatto giustifica il nome di *polinomio omogeneo associato di* f per indicare il polinomio omogeneo dato dalla nella (1.14).

Osserviamo che se $f(x_1,\ldots,x_r) = F_0 + F_1(x_1,\ldots,x_r) + \ldots + F_N(x_1,\ldots,x_r)$ essendo $F_i(x_1,\ldots,x_r)$ polinomio omogeneo di grado i per ogni $i = 0,1\ldots,N$, il polinomio omogeneo associato ad $f(x_1,\ldots,x_r)$ altro non è che $F(X_0,\ldots,X_r) = F_0x_0^N + F_1(x_1,\ldots,x_r)x_0^{N-1} + \ldots + F_N(x_1,\ldots,x_r)$.

Proposizione 1.3.3 *Dati due polinomi associati, $F(x_0,\ldots,x_r)$ e $f(x_1,\ldots,x_r)$, F è riducibile se e solo se f è riducibile.*

Dimostrazione

Supponiamo che $F(x_0,\ldots,x_r) = G(x_0,\ldots,x_r)\cdot H(x_0,\ldots,x_r)$ con G e H non costanti; ponendovi $x_0 = 1$ otteniamo: $F(1,\ldots,x_r) = G(1,\ldots,x_r)H(1,\ldots,x_r)$ cioè $f(x_1,\ldots,x_r) = g(x_1,\ldots,x_r)h(x_1,\ldots,x_r)$. Può essere g costante? Sì, ma nel solo caso in cui $G(x_0,\ldots,x_r)$ dipenda solamente da x_0. Ma allora, $G = G(x_0) \in \mathbb{K}[X_0]$ e $\deg(G_0) = d > 0$. Ora, $\deg(F) = \deg(G(x_0))\deg(H)$ implica $\deg(F) = d + \deg(H) > \deg(H) \geq \deg(h)$. D'altronde, $\deg(f) = \deg(g) + \deg(h) = \deg(h)$. Ne segue $\deg(F) > \deg(f)$ che contraddice la definizione di F associato di f. Pertanto g (e similmente h) non è costante, quindi f è altresì riducibile.

Viceversa supponiamo che $f(x_1,\ldots,x_r) = g(x_1,\ldots,x_r)\cdot h(x_1,\ldots,x_r)$ con $grado\, f = k,\ grado\, g = l,\ grado\, h = m$, ossia $k = l + m$.

Troviamo il polinomio omogeneo associato a f :

$$\begin{aligned} F(x_0,\ldots,x_r) &= x_0^k f(\frac{x_1}{x_0},\ldots,\frac{x_r}{x_0}) \\ &= x_0^k(g(\frac{x_1}{x_0},\ldots,\frac{x_r}{x_0})\cdot h(\frac{x_1}{x_0},\ldots,\frac{x_r}{x_0})) \\ &= x_0^l g(\frac{x_1}{x_0},\ldots,\frac{x_r}{x_0})\cdot x_0^m h(\frac{x_1}{x_0},\ldots,\frac{x_r}{x_0}) \\ &= G(x_0,\ldots,x_r)H(x_0,\ldots,x_r). \end{aligned}$$

Pertanto F è riducibile. □

Corollario 1.3.1 *Se F è un polinomio omogeneo in due variabili x_0, x_1 a coefficienti in un campo $\mathbb{K}$ algebricamente chiuso, allora si fattorizza come prodotto di fattori lineari ossia: Se* $\deg(F) = N$ *allora* $F(x_0, x_1) = a \cdot \prod_{i=1}^{N}(a_i x_0 + b_i x_1)$.

Dimostrazione

Se x_0 divide F, scriviamo $F(x_0, x_1) = x_0^m \bar{F}(x_0, x_1)$ dove x_0 non divide $\bar{F}(x_0, x_1)$.

Consideriamo il polinomio $\bar{f}(x_1)$ associato a $\bar{F}(x_0, x_1)$. $\bar{f}(x_1)$ è un polinomio di grado N, inoltre, essendo $\mathbb{K}$ algebricamente chiuso, esso ha esattamente N radici, $\alpha_1, \ldots, \alpha_N$, in $\mathbb{K}$. Ne segue:

$$\bar{f}(x_1) = a(x_1 - \alpha_1) \cdot \ldots \cdot (x_1 - \alpha_N).$$

Rendendo tale relazione omogenea otteniamo:

$$\begin{aligned} \bar{F}(x_0, x_1) = x_0^N \bar{f}(\frac{x_1}{x_0}) &= a x_0^N (\frac{x_1}{x_0} - \alpha_1) \cdot \ldots \cdot (\frac{x_1}{x_0} - \alpha_N) \\ &= a(x_1 - \alpha_1 x_0) \cdot \ldots \cdot (x_1 - \alpha_N x_0) \end{aligned}$$

Pertanto, $F(x_0, x_1) = a x_0^m (x_1 - \alpha_1 x_0) \cdot \ldots \cdot (x_1 - \alpha_N x_0)$ onde l'asserto.

Teorema 1.3.3 *Due polinomi omogenei*

$$F(x_0, x_1) = a_0 x_0^n + a_1 x_0^{n-1} x_1 + \cdots + a_n x_1^n$$

$$G(x_0, x_1) = b_0 x_0^s + b_1 x_0^{s-1} x_1 + \cdots + b_s x_1^s$$

hanno un fattore non costante in comune se e solo se il risultante dato dal determinante (1.2) è uguale a zero.

Dimostrazione

Consideriamo $F(x_0, x_1)$ e $G(x_0, x_1)$ come polinomi nella indeterminata x_0 ed a coef-

ficienti in $\mathbb{K}[x_1]$. Allora il risultante alla Sylvester $R(f,g,X_0)$ è uguale a

$$D^* = \left|\begin{array}{ccccccccc} a_0 & a_1x_1 & & & & a_nx_1^n & & & \\ & a_0 & a_1x_1 & & & & a_nx_1^n & & \\ & & & \cdots & & \cdots & & & \\ & & & a_0 & a_1x_1 & & & a_nx_1^n & \\ b_0 & b_1x_1 & & & b_sx_1^s & & & & \\ & b_0 & b_1x_1 & & & b_sx_1^s & & & \\ & & & \cdots & & \cdots & & & \\ & & & & b_0 & b_1x_1 & & b_sx_1^s & \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} s \text{ righe} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \text{ righe} \end{array} \tag{1.15}$$

Poiché $0i_0 + 1i_1 + \ldots ni_n + 0j_0 + 1j_1 + \ldots sj_s = ns$ per la proprietà isobarica, il generico elemento nello sviluppo del determinate D^* risulta essere

$$\pm a_0^{i_0}(a_1x_1)^{i_1}\cdots(a_nx_1)^{i_n}b_0^{j_0}(b1x_1)^{j_1}\cdots(b_sx_1)^{i_s} = \pm x_1^{ns}a_0^{i_0}a_1^{i_1}\cdots a_n^{i_n}b_0^{j_0}b_{j_1}\cdots b_d^{j_s}.$$

Ne segue che $D^* = x_1^{ns}D$ essendo D il determinante alla Sylvester (1.2). Chiaramente $(0,0)$ è una soluzione banale del sistema $F(x_0,x_1) = 0, G(x_0,x_1) = 0$. Se (ξ_0,ξ_1) è una soluzione non banale dello stesso sistema con $\xi_1 = 0$ allora $a_n\xi_0^n = 0$ e $b_s\xi_0^s = 0$ quindi $a_n = b_s = 0$ ed x_1 è un fattore comune ad $F(x_0,x_1)$ e $G(x_0,x_1)$. Altrimenti, $\xi_1 \neq 0$ e $D^* = 0$ se e solo se $D = 0$. □

Teorema 1.3.4 *Consideriamo due polinomi omogenei:*

$$f(x_0,\ldots,x_r) = A_n + A_{n-1}x_r + \cdots + A_0x_r^n$$

e

$$g(x_0,\ldots,x_r) = B_s + B_{s-1}x_r + \cdots + B_0x_r^s$$

dove A_i e B_i sono polinomi omogenei di grado i nelle $x_0,\ldots,x_{r-1}$ e con $A_0B_0 \neq 0$. Se $R(f,g)$ è il risultante alla Sylvester di f e g relativo alla indeterminata x_r, allora $R(f,g)$ è un polinomio omogeneo di grado ns se i due polinomi non hanno un fattore comune.

Dimostrazione

Il metodo adottato nella dimostrazione precedente può essere usato per provare l'asserto. Qui, facciamo vedere un'altra dimostrazione.

Poniamo $A_i(x_0, \ldots, x_{r-1}) = A_i$ per definizione si ha $R_{x_r}(f, g) = D(x)$:

$$\left|\begin{array}{ccccccccc} A_0 & A_1 & & & & A_n & & & \\ & A_0 & A_1 & & & & A_n & & \\ & & & \cdots & & \cdots & & & \\ & & & A_0 & A_1 & & & A_n & \\ B_0 & B_1 & & & B_s & & & & \\ & B_0 & B_1 & & & B_s & & & \\ & & & \cdots & & \cdots & & & \\ & & & & B_0 & B_1 & & B_s & \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} s \text{ righe} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \text{ righe} \end{array}$$

Sostituendo x con tx e ricordando che i polinomi A_i e B_j sono omogenei otteniamo $D(tx))$:

$$\left|\begin{array}{ccccccccc} A_0 & tA_1 & & & & t^nA_n & & & \\ & A_0 & tA_1 & & & & t^nA_n & & \\ & & & \cdots & & \cdots & & & \\ & & & A_0 & tA_1 & & & t^nA_n & \\ B_0 & tB_1 & & & t^sB_s & & & & \\ & B_0 & tB_1 & & & t^sB_s & & & \\ & & & \cdots & & \cdots & & & \\ & & & & B_0 & tB_1 & & & t^sB_s \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} s \text{ righe} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \text{ righe} \end{array}$$

Moltiplicando la i-ma riga della A per t^i con $1 \leq i \leq s$ e la j-ma riga delle B per t^j con $1 \leq j \leq n$ si ha $t^u D(tx)$:

$$\left|\begin{array}{ccccccccc} tA_0 & t^2A_1 & & & t^{n+1}A_n & & & & \\ & t^2A_0 & & & t^{n+1}A_{n-1} & t^{n+2}A_n & & & \\ & & & \cdots & & \cdots & & & \\ & & & & t^sA_0 & & & t^{n+s}A_n & \\ tB_0 & t^2B_1 & & & t^{s+1}B_s & & & & \\ & t^2B_0 & & & t^{s+1}B_{s-1} & t^{s+2}B_s & & & \\ & & & \cdots & & \cdots & & & \\ & & & & t^nB_0 & & & t^{s+n}B_s & \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} s \text{ righe} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} n \text{ righe} \end{array}$$

essendo $u = s(s+1)/2 + n(n+1)/2$.

Ma tale determinante è uguale a $t^v D(x)$ con $v = (s+n)(s+n+1)/2$. Ne segue $t^u D(tx) = t^v D(x)$ ossia $D(tx) = t^{v-u} D(x)$ da cui $R(tx_1, \ldots, tx_{r-1}) = t^{ns} R(x_1, \ldots, x_{r-1})$ quindi per il teorema 1.3.1 otteniamo l'asserto. □

Terminiamo lo studio del risultante alla Sylvester con il seguente teorema.

Teorema 1.3.5 *Siano $F(X), G(X)$ ed $H(X)$ sono tre qualsiasi polinomi in $\mathbb{K}[X]$. Se $n = \deg(F(X)), s = \deg(G(X)), m = \deg(H(X))$ e c è il coefficiente principale di $F(X)$, allora*

$$R(F,G) = \begin{cases} R(F, G+FH) \text{ per } n+m < s; \\ R(F, G+FH) \text{ per } n+m = s; \\ c^{n+m-s} R(F, G+FH) \text{ per } n+m > s. \end{cases}$$

Dimostrazione Poniamo $H(X) = \delta_0 X^m + \ldots + \delta_m$ con $\delta_0, \ldots, \delta_m \in \mathbb{K}$. Consideriamo l'anello dei polinomi $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_s]$.

Chiaramente, il determinante alla Sylvester (1.2), riguardato quale polinomio $D(a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s)$ nelle $n+s+2$ indeterminate $a_0, \ldots, a_n$, $b_0, \ldots, b_s$, è un elemento di $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_s]$. Inoltre, $F(X) = a_0 X^n + \cdots + a_n$ e $G(X) = b_0 X^s + \ldots b_s$ sono due polinomi in X a coefficienti in $\in \mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_s]$. Poiché i coefficienti di $H(X)$ sono elementi in $\mathbb{K}$, l'espressione $U(X) = G(X) + H(X)F(X)$ è altresì un polinomio in X i cui coefficienti sono in $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_s]$.

Ci proponiamo di provare l'asserto servendoci del teorema di Study. A tal fine ricordiamo, come è già stato dimostrato, che D è un polinomio irreducibile di $\mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_s]$. Scriviamo $G(X) + H(X)F(X)$ in forma canonica: $G(X) + H(X)F(X) = e_0 X^t + \ldots + e_t$ con $e_0, \ldots, e_t \in \mathbb{K}[a_0, a_1, \ldots, a_n, b_0, b_1, \ldots b_s]$.

Allora il determinante alla Sylvester dei polinomi $F(X)$ e $G(X)+H(X)F(X)$ è

$$D^*=\left|\begin{array}{ccccccccc}
a_0 & a_1 & & & & a_n & & & \\
 & a_0 & a_1 & & & & a_n & & \\
 & & & \cdots & & \cdots & & & \\
 & & & a_0 & a_1 & & & a_n & \\
e_0 & e_1 & & & e_t & & & & \\
 & e_0 & e_1 & & & e_t & & & \\
 & & & \cdots & & \cdots & & & \\
 & & & & e_0 & e_1 & & e_t &
\end{array}\right|\begin{array}{l}\left.\begin{array}{l}\\\\\\\\\end{array}\right\} t \text{ righe}\\ \left.\begin{array}{l}\\\\\\\\\end{array}\right\} n \text{ righe}\end{array} \tag{1.16}$$

Notiamo che $t=\deg(G(X)+h(X)F(X))\geq\deg(F(X))=n$. Inoltre,

$$d_0=\begin{cases}b_0 \text{ se } s>m+n \text{ i.e. } t=s;\\ b_0+\delta_0 a_0 \text{ se } s=m+n \text{ i.e. } t=s=m+n;\\ \delta_0 a_0 \text{ se } s<m+n \text{ i.e. } t=m+n.\end{cases} \tag{1.17}$$

Osserviamo che un termine nello sviluppo di D^* è $\pm d_0^n a_n^t$.

Supponiamo che D e D^* differiscano soltanto per una costante $\kappa\in\mathbb{K}$ allora $t=s$. Inoltre,

(i) se $s>m+n$, allora $d_0=b_0$. Poiché un termine di sviluppo di D è $\pm b_0^n a_n^s$, ne segue che $\kappa=1$;

(ii) se $t=s=m+n$, abbiamo

$$e_0=b_0+a_0\delta_0,\ e_1=b_1+a_0\delta_1+a_1\delta_0, e_2=b_2+a_0\delta_2+a_1\delta_1+a_2\delta_0,\ldots,e_s=b_s+a_0\delta_s+\ldots+a_s\delta_0,$$

dove $a_i=0$ per $n<i\leq s$.

Ora D^* verrà trasformato in un determinante D' come segue. Le prime s righe di D' sono le stesse di D^* (cioè del determinante di Sylvester D, blocco A). La prima riga successiva di D' si ottiene dalla prima riga del blocco E di D^* sottraendone l'ultima (s-ma) riga del blocco A moltiplicata per δ_0 poi la penultima ($s-1$-ma) riga del blocco A moltiplicata per δ_1 andando avanti così fino a sottrare l'ultima ($s-(n+1)$-ma) riga del blocco A moltiplicata per δ_0. Questa modifica fa sì che l'elemento e_s

nella prima riga del blocco E in D^* diventa b_s. Ripetiamo il processo passando alla seconda riga del blocco E in $D*$ otteniamo che e_s nella seconda riga del blocco E in D^* diventa b_s. Andando avanti in questa maniera otteniamo un determinante D' ha lo stesso diagonale di D. Intanto $D^* = D'$. Poiché $D^* = \kappa D$, risulta che $a_0^s e_s^n = a_0^s b_0^n$.

sottraendo la i-esima riga del blocco A, molteplicata per δ_0, dalla i-esima riga del blocco D, per $i = 1, \ldots, n$. Un termine nello sviluppo di D' è $\pm b_0^n a_n^s$. Il confronto con D mostra che $\kappa = 1$ e $D = D^*$.

Sia $P = (\xi_0, \xi_1, \ldots, \xi_n, \eta_0, \eta_1, \ldots \eta_s)$ con $\xi_i, \eta_j \in \mathbb{K}$. Se $\xi_0 = \eta_0 = 0$ allora $D(P) = 0$, in quanto nella prima colonna di D tutti gli elementi sono nulli, e lo stesso vale per D^* (cioè $D^*(P) = 0$) in forza della (1.17). Supponiamo ora invece che almeno una delle ξ_0 e η_0 non sia zero. Consideriamo i polinomi $u(X) = \xi_0 X^n + \ldots + \xi_n$ e $v(X) = \eta_0 X^s + \ldots + \eta_s$, entrambi elementi di $\mathbb{K}[X]$. Per il teorema di Sylvester, i due polinomi $u(X)$ e $v(X)$ hanno una radice in comune se e solo se $D(P) = D(\xi_0, \xi_1, \ldots, \xi_n, \eta_0, \eta_1, \ldots \eta_s)$ è uguale a zero. Inoltre, se $u(X)$ e $v(X)$ hanno una radice in comune, diciamo θ, allora θ è anche una radice comune ai polinomi $u(X)$ e $w(X) = v(X) + h(X)u(X)$ (ma il viceversa non vale). Ne segue che $D(P) = 0$ implica $D^*(P) = 0$. In virtù del teorema di Study, il polinomio $D(a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s)$ divide il polinomio $D^*(a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_s)$. Nel caso in cui $\deg(D^*) \leq \deg(D)$ (ossia $s \geq m + n$), ne segue che $\deg(D) = \deg(D^*)$, quindi D e D^* differiscono soltanto per una costante. Altrimenti, $\deg(D^*) - \deg(D) = m + n - s$. Proviamo per questo caso che a_0^{m+n-s} divide D^*. A tal fine, come nella dimostrazione del Teorema 1.1.3, effettuiamo le sostituzioni $a_0 = a_1' a_0, \ldots, a_n = a_n' a_0$. Risulta $D(a_0, a_1, \ldots, a_n, b_0 b_1, \ldots, b_s) = a_0^s D'(a_1', \ldots, a_n', b_0, b_1 \ldots, b_s)$. Con le stesse sostituzioni in D^*, $D^*(a_0, a_1, \ldots, a_n, b_0 b_1, \ldots, b_s) = a_0^{m+n} D^{*\prime}(a_1', \ldots, a_n', b_0, b_1 \ldots, b_s)$ in quanto $\deg(g(X) + h(X)f(X)) = m + n$. Poiché $D | D^*$ implica $D' | D^{*\prime}$ vediamo

che $a_0^{m+n-s}D$ divide D^*. Ne segue che D^* e $a_0^{m+n-s}D$ differiscono per una costante κ essendo $\deg(D) = n+s, \deg(D') = n+(n+m)$, e $\deg(a_0^{m+n-s}D) = m+n-s+n+s = n+(m+n)$. Confrontiamo, come prima, due termini corrispondenti in D^* e D. Nella diagonale principale di D^* troviamo a_0 $(m+n)$-volte e d_{m+n} per n volte. Poiché $d_{m+n} = b_s + \delta_m a_n$, nello sviluppo di D^* abbiamo $d_{m+s}^n = b_s^n + (n-1)b_{s-1}\delta_m a_n + \ldots$. Pertanto, lo sviluppo di D^* contiene il monomio $a_0^{m+n}b_s^n$. Poiché $D^* = \kappa a_0^{m+n}D$ ne segue che $a_0^{m+n}b_s^n = \kappa a_0^s b_s^n$ da cui $\kappa = a_0^{m+n-s}$.
□

1.4 Molteplicità d'intersezione

Date due curve algebriche d'equazione minima $F = 0$ e $G = 0$ rispettivamente, introduciamo la *molteplicità di intersezione* $I(F, G; P)$ *nel punto* $P(a, b)$ mediante i seguenti postulati:

P0) $I(F, G; P)$ è un intero non negativo purché F e G siano prive di componenti comuni per P;

P1) $I(F, G; P) = \infty$ se F e G hanno una componente in comune per P;

P2) $I(F, G; P) = 0$ se P non è un punto comune ad F e G;

P3) $I(F, G; P) = 1$ se F e G sono due rette distinte per P;

P4) $I(F, G; P) = I(G, F; P)$;

P5) $I(F, G + HF; P) = I(F, G; P)$ per ogni curva algebrica H;

P6) $I(F, GH; P) = I(F, G; P) + I(F, H; P)$ per ogni curva algebrica H.

Incominciamo lo studio col dimostrare il seguente teorema.

Teorema 1.4.1 $I(F, G; P)$ *dipende dall'ideale* (F, G) *generato da* F *e* G*, nel senso che se* F' *e* G' *sono curve algebriche tali che* $(F, G) = (F', G')$ *allora*

$$I(F, G; P) = I(F', G'; P) \tag{1.18}$$

Dimostrazione

Se $(F, G) = (F', G')$, allora

$$F' = AF + BG; \tag{1.19}$$

$$G' = CF + DG \tag{1.20}$$

con $A, B, C, D \in \mathbb{K}[X, Y]$. Per la (1.18), esistono $H, L, M, I \in \mathbb{K}[X, Y]$ tali che

$$F = HF' + IG'; \tag{1.21}$$

$$G = LF' + MG' \tag{1.22}$$

Se U è un divisore comune ad F e G, lo è anche ad F' e G', e viceversa. Per **P2)**, ciò dice che se $I(F, G; P) = \infty$, allora $I(F', G'; P) = \infty$. Possiamo pertanto supporre che F' e G' siano privi di fattori comuni. Posto $\Delta = AD - BC$ con $\Delta \in \mathbb{K}[X, Y]$, proviamo dapprima che se P è un punto comune alle curve F e G, allora $\Delta(P) \neq 0$. Con calcoli diretti, dalle (1.19),(1.20),(1.21) e (1.22) si ricavano:

$$F'(1 - (AH + BL)) = (AI + BM)G',$$

$$G'(1 - (CI + DM)) = (CH + DL)F'.$$

Supponiamo dapprima che $AI+BM$, e quindi anche $(1-(AH+BL)$, sia diverso dal polinomio nullo. Allora F' e G' dividono $AI+BM$ e $1-(AH+BL)$, rispettivamente. Poiché $F(P) = G(P) = 0$ implica $F'(P) = G'(P) = 0$, ne segue che

$$A(P)I(P) + B(P)M(P) = 0,\ A(P)H(P) + B(P)L(P) = 1. \tag{1.23}$$

Similmente,

$$C(P)H(P) + D(P)L(P) = 0,\ C(P)I(P) + D(P)M(P) = 1. \tag{1.24}$$

purché $CH + DL$, quindi $1 - (CI + DM)$, non sia il polinomio nullo.
È di verifica immediata che (1.23) e (1.24)) restano valide se $AI+BM$ e $CH+DL$ sono polinomi nulli. Pertanto, $(A(P)H(P)+B(P)L(P))(C(P)I(P)+D(P)M(P))-$

$((A(P)I(P)+B(P)M(P))(C(P)H(P)+D(P)L(P))=1$. D'altro canto, $(AH+BL)(CI+DM)-(AI+BM)(CH+DL)=(AD-BC)(HM-IL)$. Ne consegue che $\Delta(P)=A(P)D(P)-B(P)C(P)\neq 0$, come si voleva. Tenuto conto di **P2)**, se ne deduce

$$I((AD-BC,F;P)=0. \tag{1.25}$$

Ciò premesso, proviamo l'asserto tenendo conto di **P4),P5),P6)** e della (1.24): $I(F',G';P)=I(AF+BG,CF+DG;P)=I(AFD+BGD,CF+DG;P)-I(D,CF-DG;P)=I(AFD-BCF+BCF+BGD,CF+DG;P)-I(D,CF;P)$
$=I((AD-BC)F+B(CF+DG),CF+DG;P)-I(D,CF;P)=I((AD-BC)F,CF+DG;P)-I(D,CF;P)=I(AD-BC,CF+DG;P)+I(F,CF+DG;P)-I(D,CF;P)=I(F,DG;P)-I(D,CF;P)=I(F,D;P)+I(F,G;P)-I(D,C;P)-I(D,F;P)=I(F,G;P)-I(C,D;P)$.

Resta da far vedere che $I(C,D;P)=0$. Se così non fosse, si avrebbe $C(P)=D(P)=0$, onde $A(P)D(P)-B(P)C(P)=0$ in contraddizione con quanto stabilito precedentemente.

Per curve riducibili riesce spesso utile la seguente formula che discende da **PO6)** e **PO4)**.

Teorema 1.4.2 *$I(F,G;P)$ dipende dalle componenti di F e G. Più precisamente, se $F=\prod_i F_i^{r_i}$ e $G=\prod_j G_j^{s_j}$, allora $I(F,G;P)=\sum_{i,j} r_i s_j I(F,G;P)$.*

Proviamo ora alcune proposizioni che saranno utili per il seguito.

Proposizione 1.4.1 *Per ogni $F\in \mathbb{K}[X,Y]$ non avente, come componente, Y, se $f(X):=F(X,0)=X^r(X-a_1)^{r_1}\dots(X-a_m)^{r_m}$, allora $I(F,Y;O)=r$, essendo $O=(0,0)$ l'origine.*

Dimostrazione.

Poiché $F(X,Y)=f(X)+Y(\dots)$, da **P6)** discende $I(F,Y;O)=I(f(X),Y;O)$,

quindi, per il Teorema 1.4.2, $I(F,Y;O) = rI(X,Y;O) + r_1 I(X-a_1,Y;O) + \ldots + r_m I(X-a_m,Y;O)$. In virtù di **P2** e **P3)**, ne segue l'asserto. □

Per il prossimo risultato, introduciamo l'omomorfismo

$$\Phi = \begin{cases} \mathbb{K}[X,Y] \to \mathbb{K}[X], \\ H(X,Y) \to h(X) = H(X,0). \end{cases} \tag{1.26}$$

Dati due polinomi $F, G \in \mathbb{K}[X,Y]$ non nulli, siano $f = \Phi(F), g = \Phi(G)$, e sia $d \in \mathbb{K}[X]$ il massimo comun divisore di f e g. Si sa dall'Algebra che esistono allora polinomi $a, b, c, e \in \mathbb{K}[X]$ tali che $d = af + bg, f = cd, g = ed.$. Pertanto,

$$ac + be = 1 \tag{1.27}$$

Poniamo ora $D = aF + bG$ e $H = -eF + cG$, e calcoliamo $I(D,H;O)$ essendo O l'origine del riferimento. Poiché $\Phi(D) = d$ e $\Phi(H) = 0$, ne segue $H = YH'$ con $H' \in \mathbb{K}[X,Y]$. Per quanto sopra, gli ideali (F,G) e (D,H) coincidono. Tenuto conto di **PO6)** dal Teorema 1.4.1 discende ora che se O è l'origine, allora

$$I(F,G;O) = I(D,H,O) = I(D,Y;O) + I(D,H';O). \tag{1.28}$$

Proposizione 1.4.2 *Se $\bar{I}(F,G;P)$ una funzione soddisfacente* **P0),...,P6)***, allora per ogni coppia (F,G) con $F, G \in \mathbb{K}[X,Y]$ vale*

$$\bar{I}(F,G;O) = I(F,G,O). \tag{1.29}$$

Dimostrazione.

Posto $i = I(F,G;O)$, se $i = 0$ (risp. $i = \infty$), la proposizione discende da **P2)** (risp. da **P1)**). Procederemo per induzione su i supponendo che $I(U,V;O) = \bar{I}(U,V;O)$ ogni volta che $U, V \in \mathbb{K}[X,Y]$ e $I(U,V;O) < i$.

Con le notazioni precedenti, dalla (1.28) discende che $I(D, Y; O) \leq i$. Per **P1)**, Y non può dividere D. Verifichiamo ora che

$$I(D, Y; O) = \bar{I}(D, Y; O). \tag{1.30}$$

A tal fine scriviamo $D = d(X) + YR$ con $d(X) \neq 0$ ed $R \in \mathbb{K}[X, Y]]$. Per **P5)**, $I(D, Y; O) = I(d(X), Y; O)$. Posto $d(X) = X^k(s + s(X))$ con $s \neq 0$ and $s(X) \in \mathbb{K}[X]$, risulta, per **P5)** e **P6)**, $I(d(X), Y; O) = I(X^k, Y; O) = k$. Similmente, $\bar{I}(D, Y; O) = k$, onde l'asserto. Inoltre, $I(D, Y; 0) \geq 1$. Infatti, essendo $F(0, 0) = G(0, 0) = 0$ anche $D(0, 0) = 0$, e per **P2)**, segue l'asserto. Avuto riguardo alla (1.28), si ottiene $I(D, H'; O) < i$; e, per l'ipotesi induttiva, risulta $I(D, H'; O) = \bar{I}(D, H'; O)$. Tenuto conto della (1.30), ne segue

$$I(F, G; O) = I(D, Y; O) + I(D, H'; O) = \bar{I}(D, Y; O) + \bar{I}(D, H'; O) =$$

$$\bar{I}(D, H; O) = \bar{I}(F, G; O),$$

che completa la dimostrazione del Proposizione 1.4.2.

Nella proposizione successiva useremo la nozione di tangente ad una curva $F = 0$ nell'origine.

A tal fine scriviamo $F(X, Y) = F_m(X, Y) + F_{m+1}(X, Y) + \ldots + F_N(X, Y)$ dove $F_j(X, Y)$ è un polinomio omogeneo di grado j e $F_m X, Y \neq 0$. Poiché $F_m(X, Y)$ è un polinomio omogeneo (non nullo) esso si fattorizza nel prodotto di polinomi omogenei lineari, come abbiamo mostrato prima; vedi Corollario 1.3.1:

$$F_m(X, Y) = (\alpha_1 X + \beta_1 Y)^{u_1}(\alpha_2 X + \beta_2 Y)^{u_2} \cdots (\alpha_k X + \beta_k Y)^{u_k}; \quad u_1 + u_2 + \ldots u_k = m.$$

Al fattore $\alpha_j X + \beta_j Y$, $1 \leq j \leq k$, può essere associata la retta ℓ_j di equazione $\alpha_j X + \beta_j Y = 0$ (passante per l'origine O). Vedremo in seguito che, da un punto di

vista geometrico, è giustificato considerare la retta ℓ_j come tangente alla curva $F = 0$. In tutto, abbiamo k rette siffatte, e ciascuna è chiamata retta tangente (principale).

Data anche un'altra curve $G = 0$, scriviamo $G(X, Y) = G_n(X, Y)+G_{n+1}(X, Y)+ \ldots + G_S(X, Y)$ dove $G_j(X, Y)$ è un polinomio omogeneo di grado j e $G_nX, Y \neq 0$. Inoltre,

$$G_n(X, Y) = (\gamma_1 X+\delta_1 Y)^{v_1}(\gamma_2 X+\delta_2 Y)^{v_2} \cdots (\gamma_k X+\delta_k Y)^{v_k}; \quad v_1+u_2+\ldots v_k = n.$$

Si può notare che $F = 0$ e $G = 0$ hanno una tangente (principale) nell'origine O se qualche fattore $\alpha_j X + \beta_j Y$ di F_m è anche fattore di G_n (a meno di un fattore costante).

Inoltre, denoteremo con $m_O(F)$ il sottogrado di F, che è uguale ad r con le notazioni appena introdotte. In geometria, $m_O(F)$ è detta la molteplicità del punto O (l'origine) per la curva $F = 0$, oppure si dice che O un punto della curva $F = 0$ di molteplicità $m_O(F)$,

Proposizione 1.4.3 *Se $D \in \mathbb{K}[X, Y]$, allora $I(D, Y; O) \geq m_0(D)$ avendosi l'uguaglianza se e solo se Y non è tangente (principale) a D in O.*

Dimostrazione.
In virtù di **P0)** possiamo supporre che Y non è componente di D. Scriviamo

$$D(X, Y) = d(X) + Y D'(X, Y) \tag{1.31}$$

essendo

$$d(X) = X^m(\lambda_m + \lambda_{m+1}X + \ldots), \lambda_m \neq 0. \tag{1.32}$$

Posto $m_0(D) = n$, si ha

$$D(X, Y) = D_n(X, Y) + D_{n+1}(X, Y) + \ldots, \tag{1.33}$$

essendo $D_i(X,Y)$ un polinomio omogeneo di grado i. Da (1.31),(1.32) e (1.33) ne seguono $m \geq n$ e $D_n(X,Y) = a\lambda_m X^m + YP'_{n-1}(X,Y)$ dove:

$$a = \begin{cases} 0 & se \quad m > n \\ 1 & se \quad m = n \end{cases}$$

per $m > n$ e P'_{n-1} è un polinomio omogeneo di grado $n-1$. Perciò, $n = m$ se e solo se Y non divide $D_n(X,Y)$, ossia se Y non è tangente a D in O. Da **PO4)**, (1.31), **PO5)**, (1.32), **PO6), PO2)** e **PO3)**, si ottiene

$$I(D,Y;O) = I(Y,d+YD';O) = I(Y,d;O) = I(Y,X^m(\lambda_m + \lambda_{m+1}X + \ldots;O) =$$

$$I(X,X^m;O) + I(Y,\lambda_m + \lambda_{m+1}X + \ldots;O) = mI(Y,X;O) + 0 = m \cdot 1 = m.$$

Proseguiamo il nostro studio dimostrando un primo risultato significativo.

Proposizione 1.4.4 $I(F,G;O) \geq m_O(F) \cdot m_O(G)$*, avendosi l'uguaglianza se e solo se le tangenti (principali) ad* F *sono diverse da quelle a* G*.*

Dimostrazione

In forza di **PO2)**, la proposizione è vera se $I(F,G;O) = 0$. Ragionando per induzione supponiamo che la proposizione sia dimostrata per ogni $U, V \in \mathbb{K}[X,Y]$ tale che $I(U,V;O) < i$ e ci proponiamo di dimostrarla per $I(F,G;O) = i$. Con le notazioni precedentemente introdotte, dalla Proposizione 1.4.3 segue che $I(D,Y;O) > 0$. Ora, per la (1.28), $I(D,H';O) < i$. Grazie all'ipotesi induttiva, $I(D,H',O) \geq m_O(D) \cdot m_O(H')$, avendosi l'uguaglianza se e solo se D e H' non hanno la stessa tangente in O. Ad ogni modo, la Proposizione 1.4.3 insieme alla (1.28) implicano

$$I(F,G;O) = I(D,Y;O) + I(D,H';O) \geq m_O(D) + m_O(D)m_O(H') = m_O(D)m_O(H), \tag{1.34}$$

avendosi l'uguaglianza se e solo se D non ha tangenti comuni né con Y né con H' il che val quanto a dire con H.

Ci proponiamo ora di trovare una relazione tra $m_O(D)m_O(H)$ e $m_O(F)m_O(G)$.

Supponiamo che Y non divida né $F_m(X,Y)$ né $G_n(X,Y)$ ove

$$F(X,Y) = F_m(X,Y) + F_{m+1}(X,Y) + \ldots,$$

$$G(X,Y) = G_n(X,Y) + G_{n+1}(X,Y) + \ldots,$$

con $F_i(X,Y)$ e $G_i(X,Y)$ polinomi omogenei di grado i.

Moltiplicando F e G per opportuni scalari (appartenenti a $\mathbb{K}$), possiamo far sì che si abbiano $F_m(X,Y) = X^m + Y \cdot F'_{m-1}(X,Y)$ e $G_n(X,Y) = X^n + Y \cdot G'_{n-1}(X,Y)$, ove F'_{m-1} e G'_{n-1} sono polinomi omogenei di grado $m-1$ e $n-1$ rispettivamente. Con le notazioni precedenti: $f(X) = X^m + \ldots$ e $g(X) = X^n + \ldots$. Non lede la generalità aver supposto $m \leq n$. Allora $d = m.c.d.[f,g]$ è divisibile per X^m ma non per X^{m+1}. Pertanto,

$$d = X^m + \ldots, \tag{1.35}$$

onde $c = 1 + \ldots, e = X^{n-m} + \ldots$. Posto, $a = \alpha_r X^r + \ldots, b = \beta_s X^s + \ldots$, otteniamo

$$1 = (\alpha_r X^r + \ldots)(1 + \ldots) + (\beta X^s + \ldots)(X^{n-m} + \ldots) = (\alpha X^r + \ldots) + (\beta_s X^{n-m+s} + \ldots),$$

abbiamo

$$\begin{cases} r = 0,\ \alpha_0 = 1 & \textit{se } n + s > m, \\ \beta_0 = 1 & \textit{se } n = m, s = 0, r > 0, \\ \alpha_0 + \beta_0 = 1,\ \alpha_0\beta_0 \neq 0 & \textit{se } n = m, r = s = 0. \end{cases} \tag{1.36}$$

Poiché $D = aF + bG$ e $H = -eF + cG$,

$$D = (a_r X^r + \ldots)(F_m + \ldots) + (\beta_s X^s + \ldots)(G_n + \ldots) = (a_r X^r F_m + \ldots) + (\beta_s X^s G_n + \ldots), \tag{1.37}$$

$$H = -(X^{n-m} + \ldots)(F_m + \ldots) + (1 + \ldots)(G_n + \ldots) = \ (-X^{n-m}F_m + G_n) + \ldots . \tag{1.38}$$

Ne segue che $m_O(H) \geq n$ e $m_O(D) \geq m$. D'altro canto, da (1.31) e (1.35) segue $D = d + YD' = (X^m + \ldots) + YD'$. Pertanto, $m_O(D) \leq m$. Risulta $m_O(D) = m$. Scriviamo ora $D = D_m + \ldots$ con D_m polinomio omogeneo di grado m. Da (1.37) e (1.36)

$$D_m = \begin{cases} F_m & \textit{se } n + s > m, \\ G_m & \textit{se } n = m, s = 0, r > 0, \\ \alpha_0 F_m + \beta_0 G_m & \textit{se } n = m, r = s = 0. \end{cases} \tag{1.39}$$

Siamo ormai in grado di completare la dimostrazione. Distinguiamo due casi a seconda che $m_O(H) > n$ oppure $m_O(H) = n$. Supposto $m_O(H) > n$, (1.38) implica $G_n = X^{n-m}F_m$ sicché ciascuna tangente (principale) a F in O è altresì tangente a G in O. Per la (1.34), $I(F, G; O) \geq m_O(D) \cdot m_O(H) > mn$, e l'asserto è dimostrato. Supposto $m_O(H) = n$, si ha $I(F, G; O) = I(D, H; O) \geq mn$. Abbiamo già visto prima che vale l'uguaglianza se e solo se D ed H hanno una tangente in comune. Notiamo inoltre che

$$H_n = -X^{n-m}F_m + G_n \neq 0. \tag{1.40}$$

Occorre ancora verificare che F e G hanno tangenti in comune se e solo se D e H l'hanno; in altre parole H_n e D_m hanno un divisore non costante se e solo se F_m e G_n l'hanno. Ma questo segue immediatamente dal fatto che H_n e D_m sono combinazioni lineari di F_m e G_n a coefficienti in $K[X]$ e viceversa; vedi (1.40), (1.39) e (1.36). Resta così dimostrato l'asserto anche per $m_O(H) = n$.

Osservazione 1.4.1 *Nel corso della dimostrazione abbiamo supposto che Y non divida né F_m né G_m. In realtà, si può recuperare tale caso con il seguente ragionamento. Dati $a, b, c, d \in \mathbb{K}$ con $ad - bc \neq 0$, introduciamo una nuova funzione col porre*

$$\bar{I}(\bar{F}, \bar{G}; \bar{P}) := I(F, G; P),$$

ove $\bar{F}(X, Y) := F(aX + bY, cX + dY)$,$\bar{G} = G(aX + bY, cX + dY)$ e $\bar{P} = (\bar{u}, \bar{v})$ con $u = a\bar{u} + b\bar{v}$ e $v = c\bar{u} + d\bar{v}$. Osserviamo che $F(u, v) = F(a\bar{u} + b\bar{v}, c\bar{u} + d\bar{v}) = \bar{F}(\bar{u}, \bar{v})$ e $G(u, v) = G(a\bar{u} + b\bar{v}, c\bar{u} + d\bar{v}) = \bar{G}(\bar{u}, \bar{v})$. In particolare, $F(u, v) = 0$ se e solo se $\bar{F}(\bar{u}, \bar{v}) = 0$, e lo stesso vale per G.

È di verifica immediata che anche $\bar{I}(\bar{F}, \bar{G}; \bar{P})$ soddisfa i postulati **P0),...,P6)**. *Scelti ora $a, b, c, d \in \mathbb{K}$ in modo che nelle decomposizioni in somma di polinomi omogenei*

$$\bar{F}(X, Y) = \bar{F}_m(X, Y) + \bar{F}_{m+1} \ldots,$$

$$\bar{G}(X, Y) = \bar{G}_n(X, Y) + \bar{G}_{n+1} \ldots$$

i termini $\bar{F}_m$ e $\bar{G}_n$ non siano divisibili per Y. Tuttavia $\bar{F}_m$ e $\bar{G}_n$ hanno un divisore comune dato da $cX + dY$. Notiamo inoltre che $\bar{O} = O$. Per il precedente risultato applicato a $\bar{I}$, abbiamo che $\bar{I}(\bar{F}, \bar{G}; O) \geq m_O(\bar{F}) m_O(\bar{G})$. Poiché $m_O(\bar{F}) = m_O(F), m_O(\bar{G}) = m_O(G)$, ne segue $I(F, G; O) \geq m_O(F) m_O(G)$, avendosi uguaglianza solo nel caso già considerato, come si voleva.

I risultati finora ottenuti riguardano $I(F, G; O)$, essendo O l'origine del riferimento. Ora li estendiamo al caso in cui il punto P non cada nell'origine. Posto $P = P(x_0, y_0)$, la traslazione $\sigma : (X, Y) \mapsto (X - x_0, Y - y_0)$ manda il punto P nell'origine. La stessa σ manda le curve F e G nelle curve F' e G' tali che $F'(X, Y) = F(X + x_0, Y + y_0)$ e $G'(X, Y) = G(X + x_0, Y + y_0)$. Introduciamo la funzione $\bar{I}(F, G; P)$ ponendo $\bar{I}(F, G; P) = I(F', G'; O)$. È di verifica immediata che $\bar{I}(F, G; P)$ soddisfa tutti i postulati **PO),. . . P6).** E viceversa, supposto che una funzione $I(F, G; P)$ soddisfi ai suddetti postulati per un determinato punto P, allora anche la funzione $\bar{I}(F', G'; O) = I(F, G; P)$ gode della stessa proprietà rispetto all'origine. Dalle Proposizioni 1.4.2 e 1.4.4 otteniamo finalmente i seguenti teoremi principali:

Teorema 1.4.3 *$I(F, G; P) \geq m_P(F) \cdot m_P(G)$, avendosi l'uguaglianza se e solo se le tangenti (principali) ad F sono diverse da quelle a G.*

Teorema 1.4.4 *Teorema di unicità: Esiste al più una funzione $I(F, G; P)$ che soddisfi tutti e sette i postulati* **PO),. . . ,P6)**.

Proveremo infine il seguente teorema.

Teorema 1.4.5 *Teorema di esistenza: Esiste una funzione $J(F, G; P)$ che soddisfi tutti e sette i postulati* **PO),. . . ,P6)**.

Dimostrazione. Nella letteratura si trovano due dimostrazioni, una si poggia su strumenti e risultati di Algebra Commutativa, l'altra si basa sulla nozione di ramo di una curva piana. Qui faremo vedere un approccio elementare che ci fornirà anche un metodo per il calcolo della molteplicità d'intersezione.

Dati due polinomi $F = F(X, Y), G = G(X, Y)$, introduciamo una funzione $J(F, G; P)$ che associa ad ogni punto $P = P(a, b)$ un intero non-negativo oppure ∞

e discutiamo il problema se essa soddisfa i postulati **P0)...P6)**. Nel caso in cui F e G abbiano un fattore comune non costante, denotiamo con $d = d(X, Y)$ il massimo comun divisore di F e G, e scriviamo $F(X, Y) = d(X, Y)F_1(X, Y)$ e $G(X, Y) = d(X, Y)G_1(X, Y)$. Se $d(P) = 0$, poniamo $J(F, G; P) = \infty$. Altrimenti, definiamo $J(F, G; P) = J(F_1, G_1, P)$.

Così facendo, ci siamo ricondotti al caso in cui

$$F \text{ e } G \text{ sono privi di fattori comuni non-costanti.} \tag{1.41}$$

Se (a, b) non è soluzione al sistema $f = 0, g = 0$, poniamo $J(f, g; P) = 0$. Riguardiamo f e g come polinomi nelle indeterminate X:

$$f(X, Y) = a_0(Y)X^n + \ldots + a_{n-1}(Y)X + a_n(Y),$$

$$g(X, Y) = b_0(Y)X^s + \ldots + b_{s-1}(Y)X + b_s(Y).$$

In forza dei teoremi 1.2.1 e 1.2.2, l'ipotesi (1.41) implica che né il determinante $D(X)$ né il determinante D(Y) sia identicamente nullo.

Può capitare che $a_0(Y)$ e $b_0(Y)$ abbiano una radice in comune. Per come andiamo a definire $J(F, G; P)$ conviene al momento escludere che ciò accada. Per tale scopo, poniamo la seguente ipotesi:

$$a_0(Y) \text{ è non-zero costante.} \tag{1.42}$$

Ammettiamo pure che $b_0(Y) = 0$. Siano $\beta_1, \ldots, \beta_m$ le radici di $D(Y)$. Allora $D(Y) = c\prod(Y - \beta_i)^{r_i}$ e $\sum r_i = \deg(D(Y))$, ed ogni soluzione (ξ, η) del sistema $F = 0, G = 0$ è tale che η coincide con una delle radici β_i. Può capitare il caso eccezionale che per qualche $\eta = \beta_i$ esistano più soluzioni, diciamo (ξ, η) e (ζ, η) con $\xi \neq \zeta$ cioè la retta orizzontale $Y - \eta = 0$ passa per almeno due punti comuni alle curve $\mathcal{F}$ e $\mathcal{G}$ di equazione $F = 0$ e $G = 0$ rispettivamente. Come vedremo, anche

questa situazione ci potrebbe causare difficoltà. Al momento la scartiamo ponendo la seguente ipotesi aggiuntiva:

$$\begin{array}{l}\text{Per ogni radice } \beta_i \text{ di } D(Y), \text{ esiste un'unica } \alpha_i \\ \text{tale che } (\alpha_i, \beta_i) \text{ è soluzione del sistema } f = 0, g = 0.\end{array} \tag{1.43}$$

Sotto le ipotesi (1.42) e (1.43), definiamo $J(F.G; P)$ come la molteplicità della radice $b = \beta_i$ nella fattorizzazione di $D(Y)$. In altre parole, se $F(a, b) = G(a, b) = 0$ e $D(b) = 0$, poniamo

$$I(f, g; P) = r_i \text{ se } b = \beta_i. \tag{1.44}$$

Ci proponiamo di provare che $I(F, G; P)$ soddisfa i postulati **PO),...,P6)**. I primi tre, **PO),P1),P2)** sono banalmente veri. Inoltre, **P4)** discende dal fatto che $D(Y)$ calcolato dalla coppia (F, G) è uguale a quello calcolato dalla coppia (G, F) a meno dell'ordine delle righe. Pertanto, i due determinanti differiscono tutt'al più per il segno; in ogni caso lo sviluppo dà gli stessi fattori lineari e con le stesse molteplicità. Ne segue che $J(F, G; P) = J(G, F; P)$.

Per la verifica di **P3)**, sia $F = A_1(X - a) + B_1(Y - b)$ e $G = A_2(X - a) + B_2(Y - b)$. Allora, $D(Y) = (A_1B_2 - A_2B_1)(Y - b)$. Poiché $A_1B_2 - A_2B_1 \neq 0$, altrimenti avremmo $F = G$, si ha $J(F, G; P) = 1$.

Prendiamo un ulteriore $H \in \mathbb{K}[X, Y]$. Lo scriviamo come polinomio nella indeterminata X: $H(X, Y) = d_0(Y)X^m + \ldots + d_m(Y)$.

Per la verifica di **P5)**, Denotiamo con $D^*(Y)$ il determinante alla Sylvester associato alla coppia $F(X, Y)$, $G(X, Y) + F(X, Y)H(X, Y)$. Dal teorema 1.3.5, vale, a meno di un fattore di proporzionalità, $D(Y) = D^*(Y)$ per $n + n - s \leq 0$, e $a_0(Y)^{n+m-s}D(Y) = D^*(Y)$ per $n + m - s > 0$. Per l'ipotesi (1.42) $a_0(Y)$ è costante, quindi $D(Y)$ e $D^*(Y)$ differiscono al più per una costante non nulla. Ne segue che $J(F, G; P) = J(F, G + FH; P)$.

Per la verifica di **P6)**, siano $D(Y), D_1(Y)$ e $D_2(Y)$ i determinanti associati ai sistemi $F = 0, GH = 0$, $F = 0, G = 0$ e $F = 0, H = 0$ rispettivamente. Dalla formula $R(F, GH) = R(F, G)R(F, H)$ otteniamo $D(Y) = D_1(Y)D_2(Y)$. Siano $P_1 = (\alpha_1, \beta)$ una soluzione del sistema $F = 0, G = 0$, e $P_2(\alpha_2, \beta)$ una soluzione di $F = 0, H = 0$. Scriviamo $D_1(Y) = (Y - \beta)^{r_1}U(Y)$ con $(Y - \beta) \nmid U(Y)$ e $D_2(Y) = (y - \beta)^{r_2}V(Y)$ con $(Y - \beta) \nmid V(Y)$. Allora $D(Y) = (Y - \beta)^{r_1+r_2}U(Y)V(Y)$. Supponiamo che entrambe le coppie (F, G) ed (F, H) soddisfino l'ipotesi (1.43). Allora, per definizione, $I(F, G; P_1) = r_1$ ed $J(F, H; P_2) = r_2$, quindi $I(F, G; P_1) + I(F, H; P_2) = r_1 + r_2$. Tuttavia, se $P_1 \neq P_2$, $I(F, G; P_2) = I(F, H; P_1) = 0$, abbiamo $I(F, G; P_1) + I(F, H; P_1) = r_1$ e $I(F, G; P_2) + I(F, H; P_2) = r_2$. D'altronde, se applicassimo la definizione alla coppia (F, GH) avremmo $I(F, GH; P_1) = I(F, GH, P_2) = r_1 + r_2$ ottenendo che $I(F, G; P_1) + I(F, H; P_1) < I(F, GH; P_1)$ e $I(F, G; P_2) + I(F, H; P_2) < I(F, GH; P_1)$. Se anche la coppia (F, GH) soddisfa l'ipotesi (1.43), questa situazione non si verifica, e si ha $I(F, G; P) + I(F, H; P) = I(F, GH; P)$.

Per rimuovere le ipotesi (1.42) e (1.43), l'artifizio introdotto nell'osservazione (1.4.1) può essere usato come segue. Presi $u_1, u_2, v_1, v_2 \in \mathbb{K}$ con $u_1v_2 - u_2v_1 \neq 0$, introduciamo $F(X, Y) = f(u_1X + u_2Y, v_1X + v_2Y)$, $G(X, Y) = g(u_1X + u_2Y, v_1X + v_2Y)$ e definiamo a_1, b_1 in modo che si abbiano $a = u_1a_1 + u_2b_1$ e $b = v_1a + v_2b$. Chiaramente, le soluzioni del sistema $F = 0, G = 0$ sono le coppie (ξ_1, η_1) per cui (ξ, η) con $\xi = u_1\xi_1 + u_2\eta_1$ e $\eta = v_1\xi_1 + v_2\eta_1$. Ora, scelti opportunamente u_1, u_2, v_1, v_2, possiamo far sì che nessuna retta orizzantale nel piano (X, Y) contenga più di un punto comune alle curve $F = 0$ e $G = 0$. Allora, porremo $J(f, g; P) = J(F, G, P_1)$ dove $P_1 = (a_1, b_1)$. In altre parole, sostituiamo f, g con F, G dove per la coppia (F, G) non si presenta il caso eccezionale. Si può provare che $J(F, G; P)$ rimane invariata

purché u_1, v_1, u_2, v_2 si prendano in modo come descritto evitando scelte in contrasto con le ipotesi (1.42) e (1.43). Con questo accorgimento, il teorema di esistenza resta provato. □

I seguenti esempi mostrano i ragionamenti di sopra.

Esempio 1. Sia $f(X,Y) = X^2 - Y^3$, $g(X,Y) = X^3 - Y^2$. Utilizziamo i postulati per calcolare $I(f,g;O)$:

$$I(X^2-Y^3, X^3-Y^2; O) = I(X^2-Y^3, X^3-Y^2-X(X^2-Y^3); O) =$$
$$I(X^2-Y^3, XY^3-Y^2; O) = I(X^2-Y^3, (XY-1)Y^2; O) =$$
$$I(X^2-Y^3, XY-1; O) + I(X^2-Y^3, Y^2; O) = 0 + I(X^2-Y^3, Y^2; O) =$$
$$2I(X^2-Y^3, Y; O) = 2I(Y, X^2-Y^3; O) = 2I(Y, 2X^2; O) = 4I(Y, X; O) = 4.$$

Pertanto, $I(f,g;O) = 4$ Inoltre, $f(X,Y) = a_0(Y)X^2 + a_1(Y)X + a_2(Y)$ con $a_Y(0) = 1, a_2(Y) = 0, a_3(Y) = -Y^3$ e $g(X,Y) = b_0(Y)X^3 + b_1(Y)X^2 + b_2(Y)X + b_3(Y)$ con $b_0(Y) = 1, b_1(Y) = 0 = b_2(Y), b_3(Y) = -Y^2$. Quindi,

$$D(Y) = \begin{vmatrix} 1 & 0 & -Y^3 & 0 & 0 \\ 0 & 1 & 0 & -Y^3 & 0 \\ 0 & 0 & 1 & 0 & -Y^3 \\ 1 & 0 & 0 & -Y^2 & 0 \\ 0 & 1 & 0 & 0 & -Y^2 \end{vmatrix} = Y^4(1-Y^5).$$

Quindi, $I(f,g;O) = 4$, in accordo con quanto visto prima.

Esempio 2. Sia $f(X,Y) = X^2 - Y$, $g(X,Y) = X^2 + Y - 8$, e $P = P(2,4)$. Utilizzando i postulati

$$I(X^2-Y, X^2+Y-8; P) = I(X^2-Y, X^2+Y-8-(X^2-Y); P) =$$
$$I(X^2-Y, 2(Y-4); P) = I(X^2-Y, Y-4; P) = I(Y-4, X^2-Y; P) =$$
$$I(Y-4, X^2-Y+(Y-4); P) = I(Y-4, X^2-4; P) = \quad ;$$
$$I(Y-4, (X+2)(X-2); P) = I(Y-4, X+2; P) + I(Y-4, X-2; P) =$$
$$0 + 1 = 1.$$

quindi $I(f,g;P) = 1$.

Inoltre, $f(X,Y) = a_0(Y)X^2 + a_1(Y)X + a_2(Y)$ con $a_Y(0) = 1, a_2(Y) = 0, a_3(Y) = -Y$ e $g(X,Y) = b_0(Y)X^2 + b_1(Y)X + b_2(Y)$ con $b_0(Y) = 1, b_1(Y) = 0, b_2(Y) = Y - 8$. Quindi,

$$D(Y) = \begin{vmatrix} 1 & 0 & -Y & 0 \\ 0 & 1 & 0 & -Y \\ 1 & 0 & Y-8 & 0 \\ 0 & 1 & 0 & Y-8 \end{vmatrix} = (Y-4)^2.$$

Poiché, come abbiamo visto, $I(f,g;P) = 1$, non è corretto dire che la molteplicità della radice $Y = 4$, che è uguale a 2, fornisca il valore di $I(f,g;P)$. Ciò mostra che l'ipotesi (ii) non può essere lasciata cadere, la retta orizzontale di equazione $Y-4 = 0$ contiene due punti di intersezione: $P(2,4)$ e $P(-2,4)$. Il valore giusto da attribuire è 1. D'altro canto, $f(X,Y) = a_0(X)Y + a_1(Y)$ con $a_0(Y) = 1, a_1(Y) = -X^2$ e $g(X,Y) = b_0(X)Y + b_1(Y)$ con $b_0(Y) = 1, b_1(Y) = Y - 8$. Quindi,

$$D(X) = \begin{vmatrix} 1 & -X^2 \\ 1 & X^2+8 \end{vmatrix} = (X+2)(X-2).$$

Quindi, la molteplicità della radice $X = 2$, che è uguale a 1, fornisce il valore corretto di $I(f,g;P)$.

Esempio 3. Sia $f(X,Y) = X^2 - Y^3$, $g(X,Y) = X + Y^2 + X^3 - 8$, e $P = P(0,0)$. Utilizzando i postulati

$$I(X^2 - Y^3, X + Y^2 + X^3; P) = \dots ;$$

Capitolo 2

Geometria proiettiva

2.1 Coordinate Omogenee e Principio di Covarianza

Il piano proiettivo $PG(2, \mathbb{K})$ coordinatizzato con il campo $\mathbb{K}$ ha come punti le terne ordinate omogenee non banali $(x_1 : x_2 : x_3)$, determinate a meno di un fattore di proporzionalità non nullo, e, similmente, come rette le terne ordinate omogenee non banali $[u_1 : u_2 : u_3]$, determinate a meno di un fattore di proporzionalità non nullo, l'incidenza punto-retta essendo definita come segue: Il punto $P = (x_1 : x_2 : x_3)$ e la retta $r = [u_1 : u_2 : u_3]$ sono incidenti se il loro prodotto scalare, $u_1x_1 + u_2x_2 + u_3x_3$ è uguale a 0. Un riferimento proiettivo di $PG(2, \mathbb{K})$ è dato dal triangolo dei punti fondamentali $X_\infty = (1 : 0 : 0)$, $Y_\infty = (0 : 1 : 0)$ e $O = (0 : 0 : 1)$ e il punto unità $(1 : 1 : 1)$. Le rette fondamentali sono $\ell_1 = [1 : 0 : 0], \ell_2 : [0 : 1 : 0]$ ed $\ell_\infty = [0 : 0 : 1]$.

Ricordiamo che da $PG(2, \mathbb{K})$ possiamo passare al piano affine $AG(2, \mathbb{K})$ pensando la retta ℓ_∞ quale "retta orizzonte". Più precisamente, i punti $P = (x_1 : x_2 : x_3)$ con $x_3 \neq 0$ sono i punti di $AG(2, \mathbb{K})$, quindi $P = (x, y)$ con $x = x_1x_3^{-1}$ e $y = x_2x_3^{-1}$. I punti $P = (x_1 : x_2 : 0)$ sono i punti all'infinito (cioè all'orizzonte); se $x_1 \neq 0$, allora $P = (1 : m : 0)$ mentre per $x_1 = 0$, abbiamo $P = (0 : 1 : 0)$. Le ret-

te $\ell = [u_1 : u_2 : u_3]$ con $(u_1, u_2) \neq (0, 0)$ sono le rette di $AG(2, \mathbb{K})$ di equazine $u_1x + u_2y + u_3 = 0$, mentre quella con $(u_1, u_2) = 0$ è la retta ℓ_∞ all'infinito. Si può anche osservare che il punto $P_m = (1 : m : 0)$ è incidente tutte le rette parallele con pendenza m (di equazione $y = mx + b$) e, anche incidente, la retta all'infinito. Il punto $P_\infty = (0 : 1 : 0)$ è incidente tutte le rette verticali (di equazione $x - c = 0$ con $c \in \mathbb{K}$), ed è incidente la retta all'infinito.

Un cambiamento di riferimento di $PG(2, \mathbb{K})$ è dato da una matrice (a_{ij}) non-singolare di ordine 3, ad elementi in $\mathbb{K}$. Se $(\bar{x}_1 : \bar{x}_2 : \bar{x}_3)$ sono le coordinate del punto $P = (x_1 : x_2 : x_3)$ rispetto al nuovo sistema di riferimento, allora abbiamo le seguenti relazioni:

$$\begin{aligned} x_1 &= a_{11}\bar{x}_1 + a_{12}\bar{x}_2 + a_{13}\bar{x}_3 \\ x_2 &= a_{21}\bar{x}_1 + a_{22}\bar{x}_2 + a_{23}\bar{x}_3 \\ x_3 &= a_{31}\bar{x}_1 + a_{32}\bar{x}_2 + a_{33}\bar{x}_3. \end{aligned}$$

Sia $\mathcal{C}$ una curva piana. Sia $F(x_1, x_2, x_3) = 0$ un'equazione di $\mathcal{C}$ nel vecchio riferimento. La stessa curva ha equazione $\bar{F}(\bar{x}_1, \bar{x}_2, \bar{x}_3) = 0$ nel nuovo riferimento, dove $\bar{F}$ si ottiene da F nel modo seguente:

$$\begin{aligned} &F(x_1, x_2, x_3) = \\ &F(a_{11}\bar{x}_1 + a_{12}\bar{x}_2 + a_{13}\bar{x}_3, a_{21}\bar{x}_1 + a_{22}\bar{x}_2 + a_{23}\bar{x}_3, a_{31}\bar{x}_1 + a_{32}\bar{x}_2 + a_{33}\bar{x}_3) = \\ &\bar{F}(\bar{x}_1 : \bar{x}_2 : \bar{x}_3). \end{aligned}$$

In particolare, $\deg(F) = \deg(\bar{F})$.

Un punto $P = (\xi_1, \xi_2, \xi_3)$ appartiene alla curva $\mathcal{C}$ di equazione $F(x_1, x_2, x_3) = 0$ se e solo se, nel nuovo riferimento, lo stesso punto ha coordinate $(\bar{\xi}_1 : \bar{\xi}_2 : \bar{\xi}_3)$ che soddisfano l'equazione $\bar{F}(\bar{x}_1 : \bar{x}_2 : \bar{x}_3)$ della stessa curva $\mathcal{C}$. Possiamo dire che la nozione di curva è covariante (cioè, in qualunque riferimento, il luogo dei punti di $\mathcal{C}$ è una curva algebrica essendo data dagli zeri di un polinomio omogeneo).

Si scelga un triangolo $U_1U_2U_3$ ed un ulteriore punto E non situato sui lati del triangolo. Verifichiamo l'esistenza di un nuovo riferimento in cui $U_1U_2U_3$ sia il triangolo fondamentale e E sia il punto unità. Analogamente a come si procede in Algebra

lineare, s'introduce la matrice (b_{ij}) le cui colonne sono date dalle coordinate dai punti U_1, U_2 ed U_3. Allora, l'inversa (a_{ij}) della matrice (b_{ij}) definisce un cambimaneto di riferimento tale che i punti U_1, U_2, U_3 avranno coordinate $U_1 = (1:0:0), U_2 = (0:1:0), U_3 = (0:0:1)$. Inoltre, scegliendo opportunamente le coordinate omogenee dei punti U_1, U_2, U_3 nel vecchio riferimento (sfruttando il fatto che esse sono determinate a meno di fattore di proporzionalità), si può ottenere che la somma vettoriale $U_1 + U_2 + U_3$ sia la terna $(1, 1, 1)$. Allora, E avrà coordinate $(1:1:1)$, quindi sarà il punto unità del nuovo riferimento.

Come conseguenza, abbiamo anche il seguente fatto. Per una qualunque retta ℓ nel piano, data da due suoi punti U_1 e U_2, esiste un riferimento in cui ℓ è la retta per il punto $U_1 = (1:0:0)$ e $U_2 = (0:1:0)$, cioè la retta all'infinito $[0:0:1]$. Questo fatto viene utilizzato nella dimostrazione (vedi 2.2 pg. 8-9, Vaccaro). Inoltre, l'asserto al termine "L'ordine di una curva algebrica ha signifcato proiettivo" vuol dire che la nozione di ordine di una curva algebrica piana è covariante.

Commenti pg.10 Vaccaro Siano dati cinque punti $P_1, P_2, \ldots, P_5$ nel piano proiettivo $PG(2, \mathbb{K})$. Scegliamo una retta ℓ disgiunta dai punti P_i e fissiamo un riferimento proiettivo $PG(2, \mathbb{K})$ in modo che ℓ sia la retta all'infinito. Allora P_i sono punti nel piano affine $AG(2, \mathbb{K})$, quindi $P_i = (a_i, b_i)$ con $i = 1, 2, \ldots, 5$. (Se vogliamo usare coordinate omogenee, allora $P_i = (a_i : b_i : 1)$.) Ci proponiamo di verificare l'esistenza di almeno una conica passante per questi cinque punti. Per conica intendiamo una curva piana di grado 2; cioè una conica di $PG(2, \mathbb{K})$ è una curva di equazione

$$F(x_1, x_2, x_3) = c_{11}x_1^2 + c_{12}x_1x_2 + c_{22}x_2^2 + c_{13}x_1x_3 + c_{23}x_2x_3 + c_{33}x_3^2 = 0, \quad (2.1)$$

equivalentemente in $AG(2, \mathbb{K})$, di equazione

$$f(x, y) = c_{11}x^2 + c_{12}xy + c_{22}y^2 + c_{13}x + c_{23}y + c_{33} = 0. \quad (2.2)$$

Occorre far vedere che i sei coefficienti $c_{11}, \ldots, c_{33}$ possono essere scelti in modo che $f(a_i, b_i) = 0$ per $i = 1, \ldots, 5$. Chiaramente, si tratta di verificare che il sistema lineare omogeneo nelle sei incognite $X_{11}, \ldots, X_{33}$

$$\begin{cases} a_1^2 X_{11} + a_1 b_1 X_{12} + b_1^2 X_{22} + a_1 X_{13} x + b_1 X_{23} y + X_{33} = 0, \\ a_2^2 X_{11} + a_2 b_2 X_{12} + b_2^2 X_{22} + a_2 X_{13} x + b_2 X_{23} y + X_{33} = 0, \\ \ldots \\ a_5^2 X_{11} + a_5 b_5 X_{12} + b_5^2 X_{22} + a_5 X_{13} x + b_5 X_{23} y + X_{33} = 0, \end{cases}$$

ammetta almeno una soluzione non banale $(c_{11}, c_{12}, \ldots, c_{33})$. Ma questo lo sappiamo dall'Algebra lineare, poiché il numero delle equazioni è minore del numero delle incognite. In base al rango della matrice del sistema, si può anche stabilire quante sono le coniche passanti per i punti P_i, tenendo conto del fatto che due soluzioni definiscono una stessa conica se e solo se differiscono per un fattore non nullo di proporzionalità. Ad esempio, se i punti P_i sono a tre a tre non-allineati, allora vi è una sola conica siffatta; ma non vale il viceversa. Diremo che i punti $P_1, P_2, \ldots, P_5$ sono in posizione generica (rispetto alle coniche del piano) se determinano univocamente la conica passante per gli stessi punti.

Analogamente, si può dimostrare il seguente teorema. Siano dati k punti nel piano, $P_1, P_2, \ldots, P_k$. Scegliamo un intero positivo n tale che $k \leq n(n+3)/2$. Allora esiste una curva di ordine n passante per i punti P_i. Come spiegato nella sezione 2.4 (pg. 10) di Vaccaro, il numero dei coefficienti di un polinomio $f(x, y)$ è uguale ad $(n+1)/(n+2)/2$. Il ragionamento fatto precedentemente per $k = 5, n = 2$ dà luogo ora ad un sistema lineare omogeneo in $n(n+3)/2$ incognite e con k equazione. Pertanto, se $k < (n+1)(n+2)/2$, cioè $k \leq (n+1)(n+2) - 1 = n(n+3)/2$, esiste almeno una tale curva di ordine n. Per avere una unica curva di ordine n passante per i punti P_i occorre (ma non basta) che $k = n(n+3)/2$.

2.2 Esempi di curve con punti singolari

Sia $\mathcal{C}$ la curva piana di equazione $f(x, y) = y - x^2 + x^3 = 0$. Nel piano proiettivo l'equazione di $\mathcal{C}$ è $F(x_1, x_2, x_3) = x_2x_3^2 - x_1^2x_3 + x_1^3 = 0$. Ci proponiamo di determinare gli eventuali punti singolari di $\mathcal{C}$ illustrando i due possibili approcci.

2.2.1 Metodo Proiettivo

Le derivate parziali di $F(x_1, x_2, x_3)$ sono

$$\frac{\partial F}{\partial x_1} = -2x_1x_3 + 3x_1^2, \quad \frac{\partial F}{\partial x_2} = x_3^2, \quad \frac{\partial F}{\partial x_3} = 2x_2x_3 - x_1^2.$$

Un punto $P = (\xi_1 : \xi_2 : \xi_3)$ è un punto singolare di $\mathcal{C}$ se è soltanto se tutte e tre le derivate parziali di $F(x_1, x_2, x_3)$ si annullano in (ξ_1, ξ_2, ξ_3). Pertanto, occorre risolvere il sistema

$$\begin{cases} -2x_1x_3 + 3x_1^2 = 0, \\ x_3^2 = 0, \\ 2x_2x_3 - x_1^2 = 0. \end{cases}$$

E' subito visto che $\xi_1 = 0, \xi_2 = 1, \xi_30$ l'unica soluzione non banale del sistema, a meno di un fattore di proporzionalità. Ciò ci dice che $P_\infty = (0 : 1 : 0)$ è l'unico punto singolare di $\mathcal{C}$. Proviamo che P_∞ è un punto doppio. Le derviate parziali seconde di $F(x_1, x_2, x_3)$ non sono tutte nulle in $(0, 1, 0)$, ad esempio

$$\frac{\partial^2 F(x_1, x_2, x_3)}{\partial x_3 \partial x_3} = 2x_2,$$

e $2x_2$ valutato in $(0, 1, 0)$ è uguale a 2, cioè diverso da zero. Vogliamo far vedere che P_∞ è una cuspide la cui (unica) tangente principale è la retta all'infinito $[0 : 0 : 1]$ (di equazione $x_3 = 0$). A tal fine cambiamo il riferimento proiettivo in modo che P_∞ diventi l'origine. E' chiaro che la sostituzione

$$\begin{aligned} x_1 &= \bar{x}_1 \\ x_2 &= \bar{x}_3 \\ x_3 &= \bar{x}_2. \end{aligned}$$

va bene. Nel nuovo riferimento $(\bar{x}_1, \bar{x}_2, \bar{x}_3)$, l'equazione di $\mathcal{C}$ è $\bar{F}(\bar{x}_1, \bar{x}_2, \bar{x}_3) = \bar{x}_2^2\bar{x}_3 - \bar{x}_1^2\bar{x}_2 + \bar{x}_1^3 = 0$. Poiché P_∞ è l'origine $(0 : 0 : 1)$ del nuovo riferimento, ci siamo ricondotti allo studio del comportamento dell'origine rispetto alla curva di equazione $\bar{x}_2^2\bar{x}_3 - \bar{x}_1^2\bar{x}_2 + \bar{x}_1^3 = 0$, quindi possiamo usare coordinate cartesiane (cioè lavorare sul piano affine). A tale scopo introduciamo le coordinate affine $\bar{x} = \bar{x}_1\bar{x}_3^{-1}$ e $\bar{y} = \bar{x}_2\bar{x}_3^{-1}$. Ora l'equazione della curva è $\bar{f}(\bar{x}, \bar{y}) = \bar{y}^2 - \bar{x}^2\bar{y} + \bar{x}^3 = 0$. Poiché mancano il termine noto e quelli di primo grado, ma vi è un termine non nullo di grado 2, l'origine è un punto doppio (conformemente a quanto detto sopra). Inoltre, la decomposizione di $\bar{f}$, nella somma di polinomi omogenei, ha un solo addendo di grado minimo, $\Phi_2(\bar{x}, \bar{y}) = \bar{y}^2$. Inoltre, $\Phi_2(\bar{x}, \bar{y}) = \bar{y}\bar{y}$ è una fattorizzazione di $\Phi_2(\bar{x}, \bar{y})$ in polinomi lineari. Possiamo concludere che la retta $\bar{y} = 0$ è tangente (doppia), cioè l'origine è punto cuspidale. Tornando al riferimento originale, la retta di equazione $\bar{y} = 0$, ovvero di equazione omogenea $\bar{x}_2 = 0$, diventa la retta di equazione omogenea $x_3 = 0$, come si voleva.

2.2.2 Metodo Cartesiano

Usiamo soltanto l'equazione affine (detta anche cartesiana) della curva $\mathcal{C}$: $f(x, y) = y - x^2 + x^3 = 0$. Proviamo innanzitutto che $\mathcal{C}$ non ha punti singolari sul piano affine. Infatti, $f_y = 1$, quindi il sistema formato dalle equazioni $f = 0, f_x =, f_y = 0$ non può avere soluzioni (ξ, η). Consideriamo una retta ℓ_c verticale di equazione $x = c$. E' subito visto che il sistema $f(x, y) = 0$, $x - c = 0$ ha sempre un'unica soluzione (ξ, η) dove $\xi = c$ ed $\eta = \xi^2 - \xi^3$. Poiché la curva ha ordine 3, il punto all'infinito delle verticali, cioè $Y_\infty = (0 : 1 : 0)$, deve essere un punto doppio di $\mathcal{C}$ dovendo assorbire esattamente due delle tre intersezioni tra $\mathcal{C}$ e ℓ_c. Inoltre, ℓ_c non può essere una tangente principale a $\mathcal{C}$ in Y_∞. Pertanto, l'unica retta ulteriore per Y_∞, cioè la retta all'infinito ℓ_∞ è l'unica tangente principale a $\mathcal{C}$ in Y_∞. Pertanto, P_∞ è una cuspide di

$\mathcal{C}$.

2.3 Il teorema di Bézout

Incominciamo col dimostrare una versione debole del teorema di Bézout, detto *piccolo teorema di Bézout*.

Lemma 2.3.1 *Se due curve proiettive piane $\mathcal{F}$ and $\mathcal{G}$, di grado m ed n rispettivamente, sono prive di componenti comuni, allora hanno al piú mn punti in comune.*

Dimostrazione. Supponiamo per assurdo che le due curve abbiano più di mn punti in comune, e ne scegliamo $mn + 1$ a piacere. Le corde determinate dai punti scelti sono di numero finito, sicché esiste una retta t da esse distinta. Inoltre, esiste un punto $P \in \ell$ che non giaccia su tali corde.

Fissiamo un riferimento nel piano tale che $t = \ell_\infty$ sia la retta all'infinito e che P sia il punto all'infinito dell'asse X. In altri termini, se (X_0, X_1, X_2) sono le coordinate di un punto del piano, allora ℓ_∞ ha equazione $X_0 = 0$ e $P = X_\infty = (0, 1, 0)$. Come al solito, useremo anche coordinate (X, Y) nel piano affine associato ad ℓ, ponendo $X = X_1/X_0$ e $Y = X_2/X_0$.

Chiaramente, ciascuno degli $mn + 1$ punti scelti ha un'ordinata diversa. Denotiamo con $f(X, Y)$ e $g(X, Y)$ i polinomi associati alle curve $\mathcal{F}$ e $\mathcal{G}$, rispettivamente. Vediamo che il sistema di equazioni

$$\begin{array}{rcl} f(X,Y) & = & a_0(Y)X^m + a_1(Y)X^{m-1} + \cdots + a_{m-1}(Y)X + a_m(Y), \\ g(X,Y) & = & b_0(Y)X^n + b_1(Y)X^{n-1} + \cdots + b_{n-1}X + b_n(Y) \end{array} \tag{2.3}$$

ammette almeno $mn + 1$ soluzioni (x, y), mai due di esse con la medesima ordinata y. L'eliminazione di X dal sistema produce un polinomio $D(Y) = R_X(f, g)$, detto polinomio di Sylvester, che ha almeno $mn+1$ radici. D'altro canto, $\deg\ D(Y) \leq mn$.

Pertanto, $D(Y)$ is identicamente nullo. Ma quando ció accade, $\mathcal{F}$ e $\mathcal{G}$ devono avere un fattore non-costante in comune, a contradizione.

Ora siamo in grado di dimostrare il teorem di Bézout.

Teorema 2.3.1 *Se due curve proiettive piane $\mathcal{F}$ and $\mathcal{G}$ di grado rispettivamente m and n, sono prive di fattori comuni, allora*

$$\sum I(P, \mathcal{F} \cap \mathcal{G}) = mn.$$

Dimostrazione. Per il piccolo teorema di Bézout, $\mathcal{F}$ e $\mathcal{G}$ hanno al piú nm punti in comune, diciamo h. Allora, tali punti comuni sono

$$P_i = (x_0^{(i)}, x_1^{(i)}, x_2^{(i)})$$

con $i = 1, \ldots, h$.

Siano $R = (\xi_0, \xi_1, \xi_2) \notin \mathcal{F}$ e $Q = (\eta_0, \eta_1, \eta_2)$ due punti distinti, e denotiamo con ℓ la retta per R e Q. Un punto P sta su ℓ se e solo se esiste $\lambda, \mu \in K$ tale che

$$P = (\lambda\xi_0 + \mu\eta_0, \lambda\xi_1 + \mu\eta_1, \lambda\xi_2 + \mu\eta_2). \tag{2.4}$$

Condizione necessaria e sufficiente affinché P stia su $\mathcal{F}$ è che

$$F(\lambda\xi_0 + \mu\eta_0, \lambda\xi_1 + \mu\eta_1, \lambda\xi_2 + \mu\eta_2) = 0.$$

$F(\lambda\xi_0 + \mu\eta_0, \lambda\xi_1 + \mu\eta_1, \lambda\xi_2 + \mu\eta_2)$ può essere visto come polinomio omogeneo $F'(\lambda, \mu)$ nelle indeterminate λ e μ; poniamo

$$F'(\lambda, \mu) = a_0\lambda^m + a_1\lambda^{m-1}\mu + \mathcal{D}ots + a_{m-1}\lambda\mu^{m-1} + a_m\mu^m. \tag{2.5}$$

Per calcolare esplicitamente a_s, scriviamo

$$F(X_0, X_1, X_2) = \sum_{i+j+k=m} a_{ijk} X_0^i X_1^j X_2^k.$$

Per il binomio di Newton,

$$a_s = \sum_{u+v+w=m-s} \sum_{i+j+k=m} \binom{i}{u}\binom{j}{v}\binom{k}{w} a_{ijk}(\xi_0^u \xi_1^v \xi_2^w)(\eta_0^{i-u}\eta_1^{j-v}\eta_2^{k-w}).$$

Osserviamo che a_s è un polinomio omogeneo di grado m nelle indeterminate $\xi_0, \xi_1, \xi_2, \eta_0, \eta_1, \eta_2$. Se η_0, η_1, η_2 sono considerate costanti, allora a_s è un polinomio omogeneo di grado $m - s$ nelle indeterminate ξ_0, ξ_1, ξ_2. Similmente, se ξ_0, ξ_1, ξ_2 sono costanti, allora a_s è un polinomio omogeneo di grado s nelle indeterminate η_0, η_1, η_2. Le radici non banali di $F'(\lambda, \mu)$ corrispondono ai punti comuni della curva $\mathcal{F}$ con la retta ℓ. Inoltre, $a_0 \neq 0$ essendo $F(\xi_0, \xi_1, \xi_2) \neq 0$.

Un risultato simile vale per la curva $\mathcal{G}$. La retta ℓ per R e Q incontra $\mathcal{G}$ nei punti P per i quali (λ, μ) è una radice non banale del polinomio omogeneo

$$G'(\lambda, \mu) = b_0\lambda^n + b_1\lambda^{n-1}\mu + \mathcal{D}ots + b_{n-1}\lambda\mu^{n-1} + b_n\mu^n. \tag{2.6}$$

essendo

$$b_s = \sum_{u+v+w=n-s} \sum_{i+j+k=n} \binom{i}{u}\binom{j}{v}\binom{k}{w} b_{ijk}(\xi_0^u \xi_1^v \xi_2^w)(\eta_0^{i-u}\eta_1^{j-v}\eta_2^{k-w}).$$

Ne segue il seguente risultato: F' e G' hanno una radice non banale in comune, equivalentemente il risultante alla Sylvester $D = (F'(\lambda, \mu), G'(\lambda, \mu)) = 0$, cioè

$$D = \left| \begin{array}{ccccccccccc} a_0 & a_1 & \dots & a_m & 0 & 0 & & & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_m & 0 & & & \dots & 0 \\ \vdots & & \vdots & & & & & & \vdots & \\ 0 & 0 & \dots & 0 & a_0 & a_1 & & & \dots & a_m \\ b_0 & b_1 & & \dots & & b_n & 0 & & \dots & 0 \\ 0 & b_0 & b_1 & & \dots & & b_n & 0 & \dots & 0 \\ \vdots & & & & & \vdots & & & \vdots & \\ 0 & \dots & 0 & b_0 & b_1 & & & & \dots & b_n \end{array} \right| \left.\begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right\} n \text{ rows} \left.\begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right\} m \text{ rows} = 0, \tag{2.7}$$

se e soltanto se $\mathcal{F}$ e $\mathcal{G}$ hanno un punto in comune

$$P_i = (x_0^{(i)}, x_1^{(i)}, x_2^{(i)})$$

sopra la retta per R e Q. Pertanto, $R(F'(\lambda,\mu), G'(\lambda,\mu)) = 0$ se e soltanto se uno dei determinanti

$$D(\xi,\eta,x^{(i)}) = \begin{vmatrix} \xi_0 & \xi_1 & \xi_2 \\ \eta_0 & \eta_1 & \eta_2 \\ x_0^{(i)} & x_1^{(i)} & x_2^{(i)} \end{vmatrix} \tag{2.8}$$

è uguale a zero.

Ora, fissiamo il punto R e consideriamo Q come punto variabile; cioè, teniamo la terna omogenea (ξ_0,ξ_1,ξ_2) fissa e consideriamo η_0,η_1,η_2 come indeterminate. Notiamo che lo sviluppo del determinante $D(\xi,\eta,x^{(i)})$ in (2.8) fornisce un polinomio lineare omogeneo nelle indeterminate η_0,η_1,η_2, mentre il risultante alla Sylvester $D = R(F'(\lambda,\mu), G'(\lambda,\mu))$ è un polinomio omogeneo, nelle indeterminate η_0,η_1,η_2, di grado mn.

Ogni radice $(\eta_0^*,\eta_1^*,\eta_2^*)$ di $D(\xi,\eta,x^{(i)}))$ è anche una radice di

$$D = R(F'(\lambda,\mu), G'(\lambda,\mu)).$$

In termini geometrici, ciò vuol dire che ogni punto della retta ℓ_i di equazione $D(\xi,\eta,x^{(i)})) = 0$ è anche punto della curva piana $\mathcal{D}$ di equazione $D = R(F'(\lambda,\mu),\, G'(\lambda,\mu)) = 0$. Ma allora tale retta ℓ_i è una componente di $\mathcal{D}$, diciamo di molteplicità (massima) r_i. Pertanto, esiste un polinomio $H(\eta_0,\eta_1,\eta_2)$, possibilmente costante, ma non contenente come componente alcune delle suddette rette ℓ_i, tale che

$$R(F'(\lambda,\mu), G'(\lambda,\mu)) = c\prod_{i=1}^{k} D(\xi,\eta,x^{(i)})^{r_i} H(\eta_0,\eta_1,\eta_2), \tag{2.9}$$

dove $c \neq 0$ è una costante e $k \leq h$.

In realtà, $H(\eta_0,\eta_1,\eta_2)$ non può essere che costante. Questo discende dal fatto che anche ogni punto di $\mathcal{D}$ sta sopra una delle rette ℓ_i. Infatti, ogni punti della curva $\mathcal{H}$ di equazione $H(\eta_0,\eta_1,\eta_2) = 0$ è un punto di $\mathcal{D}$, pertanto, come osservato prima, deve stare sopra una delle rette ℓ_i. Poiché $\mathcal{H}$ ha infiniti punti, mentre abbiamo soltanto

un numero finito di rette ℓ_i, almeno una di tali rette, diciamo ℓ, contiene un numero infinito di punti di $\mathcal{H}$. Ma allora ℓ è una componente di $\mathcal{H}$, contraddizione.

$$R(F'(\lambda,\mu),G'(\lambda,\mu)) = c\prod_{i=1}^{k} D(\xi,\eta,x^{(i)})^{r_i}. \tag{2.10}$$

Ne segue che

$$nm = \sum_{i=1}^{k} r_i. \tag{2.11}$$

Come conseguenza immediata, $k \geq 1$ e perciò $h \geq 1$.

Ci proponiamo di dimostrare che r_i è covariante.

Se $(\bar{X}_0,\bar{X}_1,\bar{X}_2)$ è un nuovo sistema di coordinate omogenee, la relazione tra il vecchio e il nuovo sistema è data dalle sostituzioni lineari $X_i = \sum_{j=0}^{2} a_{ij}\bar{X}_j$, $i = 0,1,2$, dove la matrice di passaggio (a_{ij}) è non-singolare. Per effetto di questo cambiamento, l'equazione di $\mathcal{F}$ nel nuovo sistema di riferimento è

$$\bar{F}(\bar{X}_0,\bar{X}_1,\bar{X}_2) = F(\sum_{j=0}^{2} a_{0j}\bar{X}_j,\ \sum_{j=0}^{2} a_{1j}\bar{X}_j,\ \sum_{j=0}^{2} a_{2j}\bar{X}_j),$$

mentre un punto $U = (x_0,x_1,x_2)$ rispetto al nuovo sistema di riferimento è $U = (\bar{x}_0,\bar{x}_1,\bar{x}_2)$ dove

$$x_0 = \sum_{j=0}^{2} a_{0j}\bar{x}_j,\ \sum_{j=0}^{2} a_{1j}\bar{x}_j,\ \sum_{j=0}^{2} a_{2j}\bar{x}_j.$$

In particolare, i punti Q, R sono, rispetto al vecchio riferimento,

$$Q(\xi_0,\xi_1,\xi_2) = (\sum_{j=0}^{2} a_{0j}\bar{\xi}_j,\ \sum_{j=0}^{2} a_{1j}\bar{\xi}_j,\ \sum_{j=0}^{2} a_{2j}\bar{\xi}_j),$$

e

$$R = (\eta_0,\eta_1,\eta_2) = (\sum_{j=0}^{2} a_{0j}\bar{\eta}_j,\ \sum_{j=0}^{2} a_{1j}\bar{\eta}_j,\ \sum_{j=0}^{2} a_{2j}\bar{\eta}_j).$$

Pertanto,

$$(\lambda\xi_0+\mu\eta_0, \lambda\xi_1+\mu\eta_1, \lambda\xi_2+\mu\eta_2) = (\lambda(\sum_{j=0}^{2} a_{0j}\bar{\xi}_j) + \mu(\sum_{j=0}^{2} a_{0j}\bar{\eta}_j),$$
$$\lambda(\sum_{j=0}^{2} a_{1j}\bar{\xi}_j) + \mu(\sum_{j=0}^{2} a_{1j}\bar{\eta}_j), \lambda(\sum_{j=0}^{2} a_{2j}\bar{\xi}_j) + \mu(\sum_{j=0}^{2} a_{2j}\bar{\eta}_j)) =$$
$$(\sum_{j=0}^{2}(a_{0j}(\lambda\bar{\xi}_j + \mu\bar{\eta}_j)), \sum_{j=0}^{2}(a_{1j}(\lambda\bar{\xi}_j + \mu\bar{\eta}_j)), \sum_{j=0}^{2}(a_{2j}(\lambda\bar{\xi}_j + \mu\bar{\eta}_j))) =$$
$$(\lambda\sum_{j=0}^{2} a_{0j}\bar{\xi}_j + \mu\sum_{j=0}^{2} a_{0j}\bar{\eta}_j, \lambda\sum_{j=0}^{2} a_{1j}\bar{\xi}_j + \mu\sum_{j=0}^{2} a_{1j}\bar{\eta}_j, \lambda\sum_{j=0}^{2} a_{2j}\bar{\xi}_j + \mu\sum_{j=0}^{2} a_{2j}\bar{\eta}_j) \tag{2.12}$$

Ne segue che il punto $P = (\lambda\xi_0+\mu\eta_0, \lambda\xi_1+\mu\eta_1, \lambda\xi_2+\mu\eta_2)$ ha, nel nuovo riferimento, coordinate $(\lambda\bar{\xi}_0 + \mu\bar{\eta}_0, \lambda\bar{\xi}_1 + \mu\bar{\eta}_1, \lambda\bar{\xi}_2 + \mu\bar{\eta}_2)$. Siano

$$\bar{F}'(\lambda,\mu) = \bar{a}_0\lambda^m + \bar{a}_1\lambda^{m-1}\mu + \cdots + \bar{a}_{m-1}\lambda\mu^{m-1} + \bar{a}_m\mu^m,$$

e

$$\bar{G}'(\lambda,\mu) = \bar{b}_0\lambda^n + \bar{b}_1\lambda^{n-1}\mu + \ldots + \bar{b}_{n-1}\lambda\mu^{n-1} + \bar{b}_n\mu^n,$$

i polinomi che derivano, rispetto al nuovo sistema di riferimento, da Q, R e P allo stesso modo come (2.5) e (2.6) sono stati ottenuti rispetto al vecchio riferimento.

La relazione (2.12) mostra che (λ^*, μ^*) è una radice di $F'(\lambda,\mu)$ se e solo se la medesima coppia (λ^*, μ^*) è una radice di $\bar{F}(\lambda,\mu)$. Ne segue che $F'(\lambda,\mu) = c\bar{F}'(\lambda,\mu)$ per una costante $c \neq 0$. Pertanto, $a_s = c\,\bar{a}_s$ per $s = 0, 1, \ldots m$. Lo stesso vale quando F viene sostituito con G, quindi $G'(\lambda,\mu) = d\bar{G}'(\lambda,\mu)$ per una costante $d \neq 0$. Pertanto, $b_s = d\,\bar{b}_s$ per $s = 0, 1, \ldots n$. Tenuto conto della (2.7), ne consegue che

$$R(F'(\lambda,\mu), G'(\lambda,\mu)) = c^n d^m\, R(\bar{F}(\lambda,\mu), \bar{G}(\lambda,\mu)).$$

Ciò dimostra la covarianza di $R(F'(\lambda,\mu), G'(\lambda,\mu))$, visto, in particolare, come polinomio nelle indeterminate η_0, η_1, η_2.

Intanto, $D(\xi, \eta, x^{(i)})$ è, rispetto al nuovo riferimento,

$$\begin{vmatrix} \sum_{j=0}^{2} a_{0j}\bar{\xi}_j & \sum_{j=0}^{2} a_{1j}\bar{\xi}_j & \sum_{j=0}^{2} a_{2j}\bar{\xi}_j \\ \sum_{j=0}^{2} a_{0j}\bar{\eta}_j & \sum_{j=0}^{2} a_{1j}\bar{\eta}_j & \sum_{j=0}^{2} a_{2j}\eta_j \\ \sum_{j=0}^{2} a_{0j}\bar{x}_j^{(i)} & \sum_{j=0}^{2} a_{1j}\bar{x}_j^{(i)} & \sum_{j=0}^{2} a_{2j}\bar{x}_j^{(i)} \end{vmatrix} = \det(a_{ij}) \begin{vmatrix} \bar{\xi}_0 & \bar{\xi}_1 & \bar{\xi}_2 \\ \bar{\eta}_0 & \bar{\eta}_1 & \bar{\eta}_2 \\ \bar{x}_0^{(i)} & \bar{x}_1^{(i)} & \bar{x}_2^{(i)} \end{vmatrix}, \tag{2.13}$$

e ciò mostra la covarianza di $D(\xi, \eta, x^{(i)})$ visto, in particolare, come polinomio omogeneo nelle indeterminate η_0, η_1, η_2. Da quanto sopra discende che gli interi $r_1, \ldots, r_h$ sono anche essi covarianti, ossia indipendenti dalla scelta del sistema di riferimento.

Pertanto, possiamo supporre che $\mathcal{F}$ e $\mathcal{G}$ non abbiano punti comuni sopra la retta ℓ_∞ di equazione $X_0 = 0$. Allora, tali punti comuni si trovano sul piano affine di coordinate (X, Y) dove, come di consueto, $X = X_1/X_0$ e $Y = X_2/X_0$. Consideriamo le curve $\mathcal{F}$ and $\mathcal{G}$, come curve affini e scriviamo le loro equazioni $f(X, Y) = 0$ e $g(X, Y) = 0$. Possiamo anche supporre che mai due dei punti comuni alle due curve siano situati su una medesima retta orizzontale. Ora, poniamo R nel punto X_∞ all'infinito dell'asse X e facciamo variare $Q = (w, \eta)$ nel piano affine. Qui, $(\xi_0, \xi_1, \xi_2) = (0, 1, 0)$ e $(\eta_0, \eta_1, \eta_2) = (1, w, \eta)$. Inoltre $P_i = (x_0^{(i)}, x_1^{(i)}, x_2^{(i)}) = (1, x^{(i)}, y^{(i)})$.

Con queste notazioni,

$$D(\xi, \eta, x^{(i)}) = \eta - y^{(i)},$$

quindi, per la (2.10),

$$R(F'(\lambda, \mu), G'(\lambda, \mu)) = c \prod_{i=1}^{k} (Y - y^{(i)})^{\nu_i}. \tag{2.14}$$

Ora, calcoliamo $F'(\lambda, \mu)$. Poiché $(\xi_0, \xi_1, \xi_2) = (0, 1, 0)$ e $(\eta_0, \eta_1, \eta_2) = (1, w, \eta)$, abbiamo che il punto P nella (2.4) è $P = (\mu, \lambda + \mu w, \mu\eta)$; in coordinate affini, $P = ((\lambda/\mu) + w, \eta)$. Sostituendo $(\lambda/\mu) + w$ con Λ, abbiamo $P = (\Lambda, \eta)$. Pertanto $F'(\lambda, \mu) = f(\Lambda, \eta)$. Similmente, $G'(\lambda, \mu) = g(\Lambda, \eta)$ dove $f(x, y) = F(1, x, y)$ e

$g(x,y) = G(1,x,y)$. Ne segue che $R(F'(\lambda,\mu), G'(\lambda,\mu))$ è il risultante $R_Y(X)$ di $f(X,Y)$ e $g(X,Y)$ mediante l'eliminazione di X. Ne segue che

$$\prod_{i=1}^{k} (Y - y^{(i)})^{r_i} = c \prod_{i=1}^{k} (Y - y^{(i)})^{\nu_i}.$$

Poiché

$$r_i = I(\mathcal{F} \cap \mathcal{G}, P_i) \tag{2.15}$$

segue l'asserto.

Esempio With $K = \mathbb{C}$ and (X,Y,Z) homogeneous coordinates, let

$$\begin{aligned} F &= Y^5 - X(Y^2 - XZ)^2, \\ G &= Y^4 - X^2Z^2 + Y^3Z. \end{aligned}$$

Then

$$\begin{aligned} ZF - Y^2G &= -XZ(Y^2 - XZ)^2 - Y^2(Y^2 - XZ)(Y^2 + XZ) \\ &= (Y^2 - XZ)(-Y^2XZ + X^2Z^2 - Y^4 - Y^2XZ) \\ &= (Y^2 - XZ)(X^2Z^2 - 2Y^2XZ - Y^4). \end{aligned}$$

If $\mathcal{F}$ e $\mathcal{G}$ are the curves of equation $F = 0$ and $G = 0$ respectively, and $P = (x,y,z) \in$

$\mathcal{F} \cap \mathcal{G}$, then

$$y^2 - xz = 0 \Rightarrow y = 0 \Rightarrow P = P_1 \text{ or } P_2$$

with $P_1 = (1, 0, 0)$, $P_2 = (0, 0, 1)$;

$$y^4 - x^2z^2 = -2y^2xz \Rightarrow -2y^2xz + y^3z = 0$$

$$\Rightarrow y = 2x \Rightarrow 16x^4 - x^2z^2 + 8x^3z = 0$$

$$\Rightarrow 16x^2 + 8xz - z^2 = 0$$

$$\Rightarrow P = P_3 \text{ or } P_4$$

with $P_3 = (-1 + \sqrt{2}, -2 + 2\sqrt{2}, 4)$, $P_4 = (-1 - \sqrt{2}, -2 - 2\sqrt{2}, 4)$.

The points P_3 and P_4 are simple on both the curves $\mathcal{F}$ and $\mathcal{G}$, which intersect transversally at both points, whence

$$I(P_3, F \cap G) = I(P_3, F \cap G) = 1.$$

For $P_2 = (0, 0, 1)$, put $f(X, Y) = F(X, Y, 1), \quad g(X, Y) = G(X, Y, 1)$. Then

$$\begin{aligned} f &= Y^5 - X(Y^2 - X)^2 = -X^3 + 2X^2Y^2 - XY^4 + Y^5, \\ g &= Y^4 - X^2 + Y^3 = -X^2 + Y^3 + Y^4, \\ h &= f - Xg = 2X^2Y^2 - XY^3 - 2XY^4 + Y^5 \\ &\qquad = Y^2(2X - Y)(X - Y^2); \end{aligned}$$

$$\begin{aligned} I(P_2, F \cap G) &= I(P_2, G \cap F) = I(P_2, g \cap f) = I(P_2, g \cap h) \\ &= I(P_2, g \cap Y^2) + I(P_2, g \cap (2X - Y)) + I(P_2, g \cap (X - Y^2)) \\ &= 4 + 2 + I(P_2, (X - Y^2) \cap Y^3) \\ &= 4 + 2 + 3 = 9. \end{aligned}$$

For $P_1 = (1, 0, 0)$, put

$$f(Y, Z) = F(1, Y, Z), \quad g(Y, Z) = G(1, Y, Z).$$

Then

$$\begin{aligned} f &= -Z^2 + 2Y^2Z - Y^4 + Y^5, \\ g &= -Z^2 + Y^3Z + Y^4, \\ h &= g - f = -2Y^2Z + Y^3Z + 2Y^4 - Y^5 \\ &\qquad = -Y^2(2-Y)(Z-Y^2); \end{aligned}$$

$$\begin{aligned} I(P_1, F \cap G) &= I(P_1, f \cap g) = I(P_1, f \cap h) \\ &= I(P_1, f \cap Y^2) + I(P_1, f \cap (2-Y)) + I(P_1, f \cap (Z-Y^2)) \\ &= 4 + 0 + I(P_1, (Z-Y^2) \cap f) \\ &= 4 + I(P_1, (Z-Y^2) \cap (f + (Z-Y^2)^2)) \\ &= 4 + I(P_1, (Z-Y^2) \cap Y^5) \\ &= 4 + 5 = 9. \end{aligned}$$

Hence

$$\sum_{i=1}^{4} I(P_i, F \cap G) = 1 + 1 + 9 + 9 = 20 = \deg \mathcal{F} \cdot \deg \mathcal{G}.$$

2.4 Unicità del ramo lineare

Per rendere completa la dimostrazione nella sezione 12 (Ramo lineare) del libro di Vaccaro, il seguente lemma è utile. Con le stesse notazioni del libro, siano $f(x,y) = a_{10}x + a_{01}y + \varphi_2(x,y) + \ldots + \varphi_n(x,y)$ e $y = a_1x + a_2x^2 + \ldots + a_ix^i + \ldots + a_hx^h$, dove $\varphi_i(x,y) = a_{i,0}x^i + a_{i-1,1}x^{i-1}y + \ldots + a_{1,i-1}xy^{i-1} + a_{0,i}y^i$ è il polinomio omogeneo ottenuto sommando tutti i monomi di grado i in $f(x,y)$. Si suppone che $a_{01} \neq 0$, ovvero $O = (0,0)$ sia un punto semplice di $\mathcal{C}$ la cui tangente in O sia diversa dalla retta verticale (cioè dall'asse y). Si introduce il polinomio $g(x) = f(x, a_1x + a_2x^2 + \ldots + a_ix^i + \ldots + a_hx^h)$ e si scrive $g(x) = b_1x + b_2x^2 + \ldots + b_jx^j + \ldots b_mx^m$. Allora, b_j è un

polinomio nelle indeterminate $a_1, \ldots,$ ed $a_{10}, a_{01}, \ldots, a_{i,0}, a_{i-1,1}, \ldots, a_{1,i-1}, a_{0,i}, \ldots$. Proviamo che $b_j = a_{01}a_j + c_j$ dove c_j è un polinomio nelle indeterminate a_k con $k = 1, \ldots, j-1$ e a_{uv} con $u + v \leq j$. Per $j = 1$, l'asserto vale essendo $b_1 = a_{10} + a_{01}a_1$, e anche per $j = 2$ in quanto $b_2 = a_{01}a_2 + a_{20} + a_{11}a_1 + a_{02}a_1^2$. Nel il caso generale, i coefficienti di b_j provengono da $\varphi_k(x, a_1x + a_2x^2 + \ldots a_hx^h)$ per $k = 1, 2 \ldots$. Conviene notare che $\varphi_k(x, a_1x + a_2x^2 + \ldots a_hx^h)$ è divisibile per x^k, quindi $\varphi_k(x, a_1x + a_2x^2 + \ldots a_hx^h) = x^k\psi$ per un polinomio ψ nelle indeterminate $a_1, \ldots, a_{10}, a_{01}, \ldots$. In particolare, b_k non contiene $a_{k+1}, \ldots$. Inoltre, $\psi = a_ka_{01} + \theta$ dove il polinomio θ contiene $a_1, \ldots, a_{k-1}$ ma non a_r con $r \geq k$ da cui segue l'asserto.

Nel libro si afferma inoltre che "*con procedimento del tutto analogo si vede che in relazione ad ogni tangente semplice risulta determinato un ramo lineare della curva*". Ora forniamo qualche dettaglio al riguardo per il caso in cui il punto sia un nodo. Senza ledere in generalità, si suppone che le due tangenti principali siano gli assi del sistema di riferimento. Allora

$$f(x, y) = xy + \Phi_3(x, y) + \ldots + \Phi_i(x, y) + \ldots + \Phi_n(x, y).$$

Ci proponiamo di provare l'esistenza (e l'unicità) di una parabola generalizzata $\mathcal{P}_h$ di ordine $h > 1$ (di equazione $y = a_1x + a_2x^2 + \ldots + a_hx^h$) tale che $I(O, \mathcal{C} \cap \mathcal{P}_h) > h$. A tal fine osserviamo anzittutto che $I(O, \mathcal{C} \cap \mathcal{P}_h) > 1$ se solo se $a_1 = 0$. Pertanto, cerchiamo coefficienti $a_2, \ldots, a_h \in \mathbb{K}$ tali che $I(O, \mathcal{C} \cap \mathcal{P}_h) > h$ con $y = a_2x^2 + \ldots + a_hx^h$. Osserviamo inoltre che

$$g(x) = f(x, a_2x^2 + \ldots + a_hx^h) = x^3(a_2 + \ldots a_hx^{h-2}) + x^4\Phi_3(1, a_2 + a_3x + \ldots) + \ldots + x^i\Phi_{i-1}(1, a_2 + a_3x + \ldots) + x^{i+1}\Phi_i(1, a_2 + a_3x + \ldots) + \ldots.$$

Vediamo che il coefficiente di x^i in $g(X)$ è una somma, uno degli addendi è a_i tutti gli altri provengono dai $\Phi_k(x, a_2x^2 + \ldots + a_hx^h)$. Poichè $\Phi_k(x, y)$ è un polinomio

omogeneo di grado k, si ha

$$\Phi_k(x,y) = \sum_{u=0}^{k} \binom{k}{u} x^{u-k}(a_2x^2 + \ldots + a_hX^h)^u. \tag{2.16}$$

Chiaramente, se un addendo proviene da (2.16), allora esso per forza proviene da $\sum_{u=0}^{k} \binom{k}{u} x^{u-k}(a_2x^2 + \ldots + a_{i-1}X^{i-1})^u$. Ne segue che tale addendo sarà un'espressione polinomiale dipendente da $a_2, \ldots, a_{i-1}$ e dai coefficienti di $f(x,y)$. Quindi, anche la somma di tutti questi addendi sarà della forma $a_1 + \varphi$ dove φ risulta essere un'espressione polinomiale dipendente da $a_2, \ldots, a_{i-1}$ e dai coefficienti di $f(x,y)$, ma non da $a_i, a_{i+1}, \ldots$. Pertanto, $I(O, \mathcal{C} \cap \mathcal{P}) > i$ vale se e solo se $a_i + \varphi = 0$. Ciò mostra come la (unica) scelta giusta sia $a_i = \varphi$. In particolare, i coefficienti $a_2, a_3, \ldots, a_h$ esistono e sono univocamente determinati (con un procedimento induttivo) affinchè $I(O, \mathcal{C} \cap \mathcal{P}_h) > h$. Ne discende l'esistenza di un unico ramo lineare γ di equazione $y = a_2x^2 + \ldots + a_hx^h + \ldots$. La tangente a γ in O è l'asse x (essendo $dy/dx = 2a_2x + \ldots na_nx^{n-1} + \ldots$). Invertendo i ruoli di x e y, otteniamo esattamente un altro ramo lineare δ di equazione $x = a_2y^2 + \ldots + a_hy^h + \ldots$. La tangente a δ in O è l'asse y. Si può concludere la presente discussione osservando che ciascuna delle due tangenti principali di un nodo genera un ramo lineare ad esso tangente. Questa proprietà non vale per i punti doppi cuspidali, in quanto ci possono essere due rami lineari, ma anche nessuno. Quest'ultimo caso si verifica sempre se $a_{3,0} \neq 0$.

2.5 Curve di genere 0

Teorema 2.5.1 *Ogni curva algebrica irriducibile di genere zero è razionale.*

Dimostrazione

Sia $\mathcal{C}^n$ una curva algebrica irriducibile dotata di sole singolarità ordinarie e di genere

zero, cioè

$$\frac{1}{2}(n-1)(n-2) = \frac{1}{2}\sum_{i=1}^{k} r_i(r_i-1)$$

ove la somma a secondo membro è estesa ai punti singolari $P_1, \ldots, P_k$ di $\mathcal{C}^n$ che hanno molteplicità $r_1, \ldots, r_k$ rispettivamente. Ricordiamo che un punto r-plo ($r \geq 2$) è detto ordinario se le r tangenti principali alla curve nel punto sono due a due distinte (in particolare, un punto doppio è ordinario se esso è un nodo).

Scelti su $\mathcal{C}^n$ *n* - 3 punti *non singolari*, diciamo $Q_1, \ldots, Q_{n-3}$, verificheremo l'esistenza di una curva $\mathcal{C}^{n-2}$ di ordine *n*-2, che passi per i punti Q_i (con *i*= 1, . . . , *n*-3), per i punti $P_1, \ldots, P_k$ con molteplicità pari a $r_i - 1$ (con $i = 1, \ldots, k$) e per un qualunque punto ulteriore A (detto punto *variabile*), scelto su $\mathcal{C}^n$.

Se Φ denota una curva piana di ordine *n* - 2, nel polinomio (omogeneo) ad essa associato appaiono $(n-2)(n+1)/2 + 1$ coefficienti, ma è lecito supporre che uno dei coefficienti sia uguale a 1, per cui il numero delle incognite nel sistema che impone il passaggio di $\mathcal{C}^{n-2}$ per i punti P_i e Q_i è $(n-2)(n+1)/2$. Il passaggio per i *k* punti singolari si traduce in un massimo di

$$\frac{1}{2}\sum_{i=1}^{k} r_i(r_i-1)$$

condizioni lineari per i coefficienti, ad esse ne vanno aggiunte altre *n* - 3 (dovute al passaggio della curva per i punti $Q_1, \ldots, Q_{n-3}$) inoltre, si aggiunge un'altra condizione lineare dovuta al passaggio di $\mathcal{C}^{n-2}$ per il punto variabile A scelto su $\mathcal{C}^n$.

In tutto il numero delle condizioni richieste ammonta al più ad

$$(n-3) + \frac{1}{2}\sum_{i=1}^{k} r_i(r_i-1) + 1$$

e tale numero non supera $\frac{1}{2}(n-2)(n+1)$, per cui ne segue l'esistenza di una curva $\mathcal{C}^{n-2}$ che soddisfa tutte le richieste di passaggio.

Viene determinato un fascio di curve di ordine *n*- 2, che può essere individuato mediante due "posizioni" del punto variabile A. Una qualunque curva di questo fascio interseca $\mathcal{C}^n$ in *n*(*n* - 2) punti (essendo $\mathcal{C}^n$ irriducibile), di cui (*n* - 1)(*n* - 2) vengono assorbiti nei punti singolari di $\mathcal{C}^n$ e altri (*n* - 3) dai punti $Q_1, \ldots, Q_{n-3}$. Pertanto fuori di essi, la curva $\mathcal{C}^{n-2}$ incontra $\mathcal{C}^n$ nel solo punto variabile A.

Vogliamo provare che le coordinate del punto A risultano funzioni razionali di una variabile λ. A tal fine, denoteremo con $f(X,Y) = 0$ l'equazione di $\mathcal{C}^n$ e con $u(X,Y) + \lambda v(X,Y) = 0$ l'equazione della generica curva $\mathcal{C}_\lambda$ del fascio. Le coordinate y_i (supposte a due a due distinte), dei $k + (n-3) + 1$ punti comuni a $\mathcal{C}^n$ e $\mathcal{C}_\lambda$, sono radici del polinomio $D(Y)$, che si ottiene sviluppando il determinante associato al risultante alla Sylvester dopo aver scritto $f(X,Y)$ e $u(X,Y) + \lambda v(X,Y)$ come polinomi nella indeterminata X, cioè :

$$f(X,Y) = a_0(Y)X^h + \ldots + a_h(Y) \;\; e \;\; u(X,Y) + \lambda v(X,Y) = b_0(Y)X^s + \ldots + b_s(Y)$$

ove $b_i(Y) = u_i(Y) + \lambda v_i(Y)$.

Sia

$$D(Y) = \begin{vmatrix} a_0(Y) & a_1(Y) & & & a_h(Y) & & \\ & a_0(Y) & & & & a_h(Y) & \\ & \ldots\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & a_0(Y) & & & & a_h(Y) \\ b_0(Y) & b_1(Y) & & b_s(Y) & & & \\ & b_0(Y) & & & b_s(Y) & & \\ & \ldots\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & b_0(Y) & & & b_s(Y) \end{vmatrix}$$

Ovviamente $D(Y) = d_0(\lambda)Y^r + \ldots + d_r(\lambda)$, ed ha $r = k + (n-3) + 1$ radici, che denoteremo con $y_1, \ldots, y_r$ (tutte sopra $\mathbb{K}$, essendo $\mathbb{K}$ algebricamente chiuso). Si può pertanto scrivere

$$D(Y) = c(Y - y_1) \cdot \ldots \cdot (Y - y_r)$$

ovviamente $y_1, \ldots, y_{r-1}$ non dipendono da λ, essendo le ordinate dei punti fissi.
Il confronto delle due espressioni di $D(Y)$ mostra che $c = d_0(\lambda)$ e quindi, $d_0(\lambda)(y_1 + \ldots + y_r) = d_1(\lambda)$. Ne segue che

$$y_r = y_r(\lambda) = [d_1(\lambda) - (y_1 + \ldots + y_{r-1})d_0(\lambda)]/d_0(\lambda)$$

e ciò mostra che l'ordinata del punto variabile A è funzione razionale di λ. Procedendo in modo analogo si perviene alla conclusione che anche l'ascissa del punto variabile A è funzione razionale di λ. Quindi esistono funzioni razionali $a(\lambda)$ e $b(\lambda)$, in modo che l'equazione parametrica della traiettoria del punto variabile A sia $x = a(\lambda)$, $y = b(\lambda)$. Posto $a(\lambda) = f(\lambda)/g(\lambda)$, $b(\lambda) = h(\lambda)/q(\lambda)$ con $f(\lambda)$, $g(\lambda)$, $h(\lambda)$, $q(\lambda) \in \mathbb{K}[\lambda]$, risulta che ogni coppia (x, y) tale che $A(x, y)$ è un punto variabile, il sistema

$$\begin{cases} f(\lambda) - g(\lambda)x = 0 \\ h(\lambda) - q(\lambda)y = 0 \end{cases} \tag{2.17}$$

ammette almeno una soluzione in λ. Indicato con $D(x, y)$ il polinomio ottenuto mediante lo sviluppo del determinante associato al risultante di Sylvester del sistema (2.17), si vede che se $A(x, y)$ è un punto variabile, allora $D(x, y) = 0$. Poiché vi sono infiniti punti variabili siffatti, $\mathcal{C}^n$ e la curva D di equazione $D(X, Y) = 0$ hanno infiniti punti in comune. Essendo $\mathcal{C}^n$ irriducibile, ne segue che $\mathcal{C}^n$ è componente di D, in altri termini ciò significa che ogni punto di $\mathcal{C}^n$, fisso o variabile, è anche un punto di D, perciò se un tal punto è $B(x_0, y_0)$, risulta $D(x_0, y_0) = 0$, onde il sistema (2.17) ammette una soluzione λ_0, da cui segue che $x_0 = a(\lambda_0)$ e $y_0 = b(\lambda_0)$ come si voleva. □

2.6 Il teorema di Bertini

Il teorema di Bertini riguarda gli eventuali punti singolari di curve appartenenti ad uno stesso fascio. La dimostrazione che riportiamo di seguito è valida sul campo

reale $\mathbb{R}$; quella proposta nel libro non ha tutti i requisiti di rigore matematico.

Teorema 2.6.1 *Sia $\mathcal{F}$ un fascio. Supponiamo che esista una curva Γ irriducibile tale che ogni suo punto (a prescindere da un numero finito di essi) sia singolare per qualche curva del fascio $\mathcal{F}$. Allora, Γ è componente di in una medesima curva del fascio $\mathcal{F}$.*

Per la dimostrazione, prendiamo due curve $\mathcal{C}$ e $\mathcal{D}$ del fascio $\mathcal{F}$ di equazioni $\varphi(X,Y) = 0$ e $\psi(X,Y) = 0$ rispettivamente dove $f(X,Y), g(X,Y) \in \mathbb{R}[X,Y]$. Possiamo considerarle come generatrici di $\mathcal{F}$. Se la curva $\mathcal{E} \in \mathcal{F}$ di equazione

$$\varphi(X,Y) + \lambda_0\psi(X,Y) = 0 \tag{2.18}$$

ha $P_0 = (x_0, y_0)$ come punto singolare, allora

$$\varphi_X(x_0,y_0) + \lambda_0\psi_X(x_0,y_0) = 0; \quad \varphi_Y(x_0,y_0) + \lambda_0\psi_Y(x_0,y_0) = 0. \tag{2.19}$$

Supponiamo che P_0 non sia un punto base del fascio $\mathcal{F}$. Allora $\varphi(x_0,y_0)$ oppure $\psi(x_0,y_0)$ è diverso da zero, e senza ledere in generalità possiamo ammettere che $\psi(x_0,y_0) \neq 0$. Dalla (2.18), $\lambda_0 = -\varphi(x_0,y_0)/\psi(x_0,y_0)$. Sostituendo λ_0 nelle equazioni in (2.19), otteniamo

$$\begin{aligned}\psi(x_0,y_0)\varphi_X(x_0,y_0) - \psi_X(x_0,y_0)\varphi(x_0,y_0) = 0,\\ \psi(x_0,y_0)\varphi_Y(x_0,y_0) - \psi_Y(x_0,y_0)\varphi(x_0,y_0) = 0.\end{aligned}$$

Ciò mostra che entrambe le derivate parziali

$$\frac{\partial}{\partial X}\Big(\frac{\varphi(X,Y)}{\psi(X,Y)}\Big) = 0; \quad \frac{\partial}{\partial Y}\Big(\frac{\varphi(X,Y)}{\psi(X,Y)}\Big) = 0$$

si annullano in (x_0,y_0). Pertanto, ogni punto di Γ (a prescindere da un numero finito di essi) annulla tali derivate parziali. Scegliamo un punto $Q = (\xi,\eta)$ di Γ che

sia semplice (e anche diverso dai punti esclusi) tale che la tangente a Γ nel punto Q non sia la retta verticale per Q. Per il teorema di Dini (riguardante le funzioni implicite reali), esiste una funzione $f(X)$ (non necessariamente polinomiale, è un ramo lineare) ed un intorno $(\xi - \delta, \xi + \delta)$ tale che i punti $(x, f(x))$ appartengono a Γ purché $\xi - \delta < x < \xi + \delta$ cioè x sia in quell'intorno. Posto $g(X) = \varphi(X, f(X))$ e $h(X) = \psi(X, f(X))$, dall'annullamento delle suddette derivate parziali nei punti di Γ segue che la derivata della funzione $g(X)/(h(X)$ si annulla per ogni $x \in (\xi - \delta, \xi + \delta)$. Ma allora, $g(X)/h(X)$ è costante, diciamo c. Ne segue che $\varphi(X, f(X)) - c\psi(X, f(X)) = 0$ per ogni $x \in (\xi - \delta, \xi + \delta)$. Poiché quest'intorno contiene infiniti punti, abbiamo che Γ e la curva $\mathcal{U}$ del fascio di equazione $\varphi(X, Y) + \lambda\psi(X, Y) = 0$ con $\lambda = -c$ hanno infiniti punti in comune. Essendo Γ irriducibile, ne segue che Γ è componente di $\mathcal{U}$.

2.7 Le formule di Plücker per le cubiche piane

Come nel libro di Vaccaro, indichiamo, rispettivamente, con $n, m, \delta, \kappa, \iota, \tau, p$, le caratteristiche di $C - n$,(cioè il grado (ordine), la classe, il numero dei nodi, il numero delle cuspidi, il numero dei flessi, il numero delle bitangenti e il genere) di una curva piana C_n irriducibile di ordine n dotate di soli punti singolari doppi (nodi, cuspidi). Le formule di Plücker sono

- $m = n(n-1) - 2\delta - 3\kappa$,
- $n = m(m-1) - 2\tau - 3\iota$,
- $\iota = 3n(n-3) - 6\delta - 8\kappa$.

Benché tali formule siano valide per una scelta generica di C_n (e non per ciascuna C_n), esse valgono per tutte le cubiche piane irriducibili. D'ora in avanti ci limitiamo

a quest'ultimo caso, e calcoliamo le suddette caratteristiche. Per questo, la seguente osservazione è utile: una C_3 irriducibile non può avere bitangenti, poiché , per una retta ℓ non passante per i punti singulari di C_n, abbiamo che $n = \sum_{P \in C_n \cap \ell} I(P; C_n \cap \ell$ dove $I(P; C_n \cap \ell) \geq 2$ se ℓ è la tangente a C_n in P. Ne segue $\tau = 0$. Inoltre, C_3 può avere al più un punto doppio. Petanto, $\delta \leq 1$ e $\kappa \leq 1$ e $\delta + \kappa \leq 1$. Poiché $n = 3$, dalle formule di Plücker, abbiamo i seguenti tre casi:

(i) $n = 3, m = 4, \delta = 1, \kappa = 0, \tau = 0, \iota = 3, g = 0$; un esempio è la C_3 di equazione $f(x, y) = xy + x^3 + y^3$.

(ii) $n = 3, m = 3, \delta = 0, \kappa = 1, \tau = 0, \iota = 1, g = 0$; un esempio è la C_3 di equazione $f(x, y) = x^2 - y^3$.

(iii) $n = 3, m = 6, \delta = 0, \kappa = 0, \tau = 0, \iota = 9, g = 1$; un esempio è la C_3 di equazione omogenea $x_1^3 + x_2^3 + x_3^3 = 0$.

Si può dimostrare che se una retta passa per due flessi di una C_3 irriducibile, allora passa anche per un terzo punto di flesso della stessa C_3. Qui proviamo quest'asserto per la C_3 che appare, come esempio, nel caso (iii). Poiché la curva hessiana H_3 di C_3 ha equazione $x_1 x_2 x_3 = 0$, i flessi di C_3 sono i punti di C_3 situati sui lati fondamentali del riferimento. Prendiamo il lato ℓ di equazione $x_2 = 0$ (cioè l'asse x); allora $C_3 \cap \ell = \{P_{21}, P_{22}, P_{23}\}$ dove $P_{21} = (-1 : 0 : 1)$, $P_{22} = (\varepsilon_1 : 0 : 1)$ e $P_{23} = (\varepsilon_2 : 0 : 1)$ essendo $\varepsilon_{1,2} = \frac{1}{2}(1 \pm i\sqrt{3})$. Analogamente per i lati di equazione, rispettivamente, di $x_1 = 0$ e $x_3 = 0$ si determinano i punti di intersezione con C_3: Essi sono $P_{11} = (0 : -1 : 1)$, $P_{22} = (0 : \varepsilon_1 : 1), P_{23} = (0 : \varepsilon_2 : 1)$ e $P_{31} = (-1 : 1 : 0)$, $P_{32} = (\varepsilon_1 : 1 : 0)$ e $P_{33} = (\varepsilon_2 : 1 : 0)$. Ora, l'asserto si prova con calcoli diretti.

2.8 Curva polare di un punto situato sulla stessa curva

Sia C_3 una cubica non-singolare data nella sua forma di Weierstrass, cioè C_3 ha equazione cartesiana $y^2 = x(x-1)(x-c)$ essendo $c \in K$, $c \neq 0, 1$. Calcoliamo l'equazione della polare dell'origine $O = (0,0)$. In coordinate omogenee, C_3 ha equazione $F(x_1, x_2, x_3) = x_2^2 x_3 - x_1(x_1 - x_3)(x_1 - cx_3)$. Pertanto, la polare C_2 di O rispetto alla C_3 ha equazione $G(x_1, x_2, x_3) = \partial F/\partial x_3 = (c+1)x_1^2 - 2cx_1x_3 + x_2^2 = 0$. In coordinate non-omogenee, $g(x,y) = G(x,y,1) = -2cx + (c+1)x^2 + y^2$. Ne segue che anche C_2 passa per O. Più precisamente, O è un punto semplice di C_2 e la tangente in quel punto è l'asse y. Perciò, C_2 e C_3 hanno la stessa tangente in O, quindi $I(C_3 \cap C_2; O) \geq 2$, e si può dimostrare che vale l'uguaglianza. Ne discende che delle sei intersezion di C_3 con C_3 quattro non cadono nell'origine. Pertanto, si possono condurre quattro tangenti a C_3 da O, i cui punti di contatto sono distinti da O. Per trovare le equazioni di queste quattro tangenti, occorre risolvere il sistema

$$\begin{cases} y^2 - x(x-1)(x-c) = 0, \\ -2cx + (c+1)x^2 + y^2 = 0. \end{cases}$$

Eliminando y, si ottiene $2cx - (c+1)x^2 = x(x-1)(x-c)$. Quest'ultima equazione ha tre soluzioni: $\xi_1 = 0$, $\xi_2 = \sqrt{c}$ e $\xi_3 = -\sqrt{c}$. Ne segue che le soluzioni non-banali del sistema sono quattro ossia $(\sqrt{c}, \pm\eta_1)$ e $(-\sqrt{c}, \pm\eta_2)$ con

$$\eta_1 = \sqrt{\sqrt{c}(\sqrt{c}-1)(\sqrt{c}-c)}, \quad \eta_2 = -\sqrt{-\sqrt{c}(-\sqrt{c}-1)(-\sqrt{c}-c)}.$$

Le curve ellittiche (cioè curve piane di grado 3 prive di punti singolari) sopra un campo arbitrario $\mathbb{K}$ sono molto importanti nella teoria dei numeri e ne costituiscono uno dei maggiori campi di ricerca attuale. Per esempio furono utilizzate da Andrew Wiles per la risoluzione dell'ultimo teorema di Fermat. Queste curve inoltre hanno molteplici applicazioni in crittografia.

Una curva ellittica definita su un campo arbitrario $\mathbb{K}$ è rappresentabile mediante l'equazione di Weierstrass generalizzata, che è della forma:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

con $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$ e tali che la varietà algebrica da essa definita sia non singolare. In questo caso il punto O è solitamente il punto all'infinito sull'asse y.

Se la caratteristica di $\mathbb{K}$ non è 2, allora ogni curva ellittica, attraverso opportunio cambio di riferimento può essere scritta nella forma:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

dove b_2, b_4, b_6 sono elementi di $\mathbb{K}$ tali che il polinomio al secondo membro abbia radici distinte (la notazione è stata scelta in base a ragioni storiche).

Se la caratteristica di $\mathbb{K}$ non è 2 né 3 allora ogni curva ellittica, attraverso ulteriorie cambio di riferimento, può essere scritta nella forma:

$$y^2 = x^3 + ax + b,$$

dove $a, b \in \mathbb{K}$ tali che il polinomio al secondo membro non abbia radici multiple.

2.9 Operazione sui punti di una curva ellittica

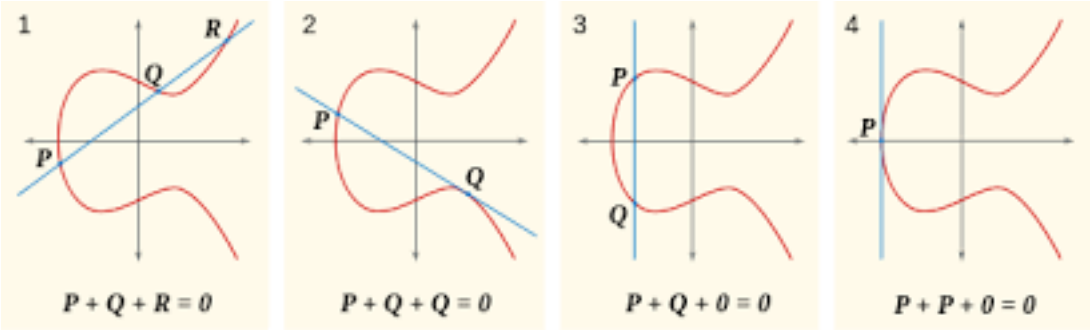
Siano A e B due punti su di una curva ellittica C e sia r la retta per A e B. Il terzo punto è l'ulteriore intersezione della retta r con C e si indica con $[PQ]$. Osserviamo che il punto P è un punto di flesso se e solo se $[PP] = P$. Fissiamo ora su C il punto O che chiameremo origine e definiamo una legge di composizione interna. Siano P, Q due punti di C, allora $P + Q := [O, [PQ]]$, cioè $P + Q$ è il terzo punto di $C \cap r$ dove r è la retta generata da O e da $[PQ]$.

Lemma 2.9.1 *Con le notazioni precedenti si hanno:*

(i) (proprietà commutativa) Per ogni due punti $P, Q \in C$ (non necessariamente distinti) $P + Q = Q + P$.

(ii) (esistenza dell'elemento neutro) Per ogni punto $P \in C$, $P + O = O + P = P$.

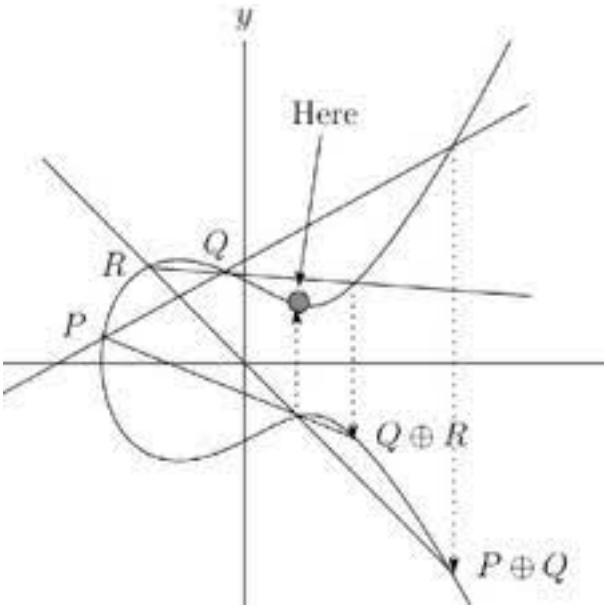
(iii) (esistenza dell'elemento opposto) Per ogni $P \in C$, esiste $Q \in C$ tale che $P + Q = Q + P = O$.



Proposizione 2.9.1 *$(C, +)$ è un gruppo commutativo (detto anche abeliano).*

In virtù del Lemma 2.9.1, resta da dimostrare la proprietà associativa, cioè $P + (Q + R) = (P + Q) + R$ per tre qualsiansi punti $P, Q, R \in C$. La proprietà associativa è un corollario di un teorema classico sulle curve cubica, detto il teorema dei 9 punti che stabilisce come tutte le cubiche piane che passano per 8 punti passano per un nono punto. Per la costruzione di $(P + Q) + R)$ sono necessarie le rette: $r_1 = (P, Q)$ $r_2 = (O, [PQ])$ ed $r_3 = (R, (P + Q))$. Per la costruzione di $P + (Q + R)$ vengono utilizzate le rette: $q_1 = (Q, R)$, $q_2 = (O, [QR]$ e $q_3 = (P, (Q + R))$. Si considerino ora due cubiche piane, $\mathcal{D}_1$ e $\mathcal{D}_2$ dove $\mathcal{D}_1$ ha come componenti le rette r_1, q_2, r_3 e $\mathcal{D}_2$ ha come componenti le rette q_1, r_2, q_3.

$$C \cap \mathcal{D}_1 = \{P, Q, [PQ], O, [QR], Q + R, (P + Q), R, [((P + Q)R]\}$$



$$C \cap \mathcal{D}_2 = \{R, Q, [QR]), O, [PQ], P+Q, P, Q+R, [P(Q+R)]\}$$

Ora, basta applicare il teorema dei 9 punti agli otto punti $P, Q, R, O, [PQ], P + Q, [QR], Q + R$ comuni alle cubiche $C, \mathcal{D}_1, \mathcal{D}_2$.

2.9.1 Le formule

Se $\mathbb{K}$ ha caratteristica diversa da $2, 3$, la cubica ellittica C ha equazione (in forma canonica) $y^2 = x^3 + ax + b$ con $a, b \in \mathbb{K}$. Scegliamo per O il punto Y_∞ dell'asse y. Siano $P = (x_1, y_1)$, $Q(x_2, y_2)$ ed $R = (x_3, y_3)$ con $R = P + Q$. Allor, per $x_1 \neq x_2$, si hanno le seguenti formule:

$$x_3 = \frac{y_2 - y_1)^2}{(x_2 - x_1)^2} - (x_1 + x_2),$$

$$y_3 = \frac{y_2 - y_1)}{(x_2 - x_1)}(x_3 - x_1) - y_1.$$

Inoltre, $-P = (x_1, -y_1)$.

Se $\mathbb{K}$ ha caratteristica 2, la cubica ellittica C ha equazione (in forma canonica) $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ con $a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}$. In caratteristica 3, una forma canonica è $y^2 = x^3 + b_2x^2 + 2b_4 + b_6$ con $b_2, b_4, b_6 \in \mathbb{K}$. In entrambi i casi, le formule sono più complicate anche se simili a quelle precedenti.