UNIVERSITÀ
DEGLI STUDI
FIRENZE

**Scuola di
Scienze Matematiche
Fisiche e Naturali**

Corso di Laurea in
Matematica

La molteplicità di intersezione delle curve algebriche e il Teorema di Bezout

The intersection multiplicity of algebraic curves and Bezout's Theorem

Relatore
Prof. Giorgio Ottaviani

Candidato
Alessia Innocenti

Anno Accademico 2013/2014

Indice

1 Introduzione

L'obiettivo di questa relazione è lo studio dell'intersezione di due curve algebriche nel piano proiettivo, in particolare saranno trattati i problemi del numero di intersezioni e delle loro molteplicità. Inizialmente saranno introdotte le varietà proiettive e gli ideali omogenei, nozioni base nell'ambito della geometria algebrica, e alcuni risultati che servono alla formulazione del noto teorema di Bezout, che tratterò nel caso specifico del campo algebricamente chiuso $\mathbb{C}$. A partire da tale teorema, si giungerà al confonto tra le due definizioni di molteplicità che saranno definite.

2 Varietà proiettive e ideali omogenei

Lo spazio proiettivo n-dimensionale su un campo K, $\mathbb{P}^n(K)$, è definito come l'insieme $\mathbb{P}^n(K) = (K^{n+1}\backslash\{0\})/\sim$, dove la relazione di equivalenza è definita come segue: $(x'_0, \dots, x'_n) \sim (x_0, \dots, x_n)$ se $\exists\lambda \neq 0$ tale che $(x'_0, \dots, x'_n) = \lambda(x_0, \dots, x_n)$. In particolare ogni $(n+1)$-pla non nulla $(x_0, \dots, x_n) \in K^{n+1}$ definisce un punto p in $\mathbb{P}^n(K)$ e si dice che $(x_0, \dots, x_n)$ sono le coordinate omogenee di p. Geometricamente è possibile identificare $\mathbb{P}^n(K)$ con l'insieme delle rette che passano dall'origine in K^{n+1}.

Si osserva che il luogo degli zeri in $\mathbb{P}^n(K)$ non è ben definito per ogni polinomio, ma è necessario considerare i polinomi omogenei, ossia i polinomi i cui termini hanno tutti lo stesso grado. Infatti se f è omogeneo si ha $f(\lambda x_0, \dots, \lambda x_n) = \lambda^{\deg f} f(x_0, \dots, x_n)$, così che l'equazione $f(x_0, \dots, x_n) = 0$ non dipende dal rappresentante $(x_0, \dots, x_n)$ nella classe di equivalenza rispetto alla relazione $\sim$ sopra definita.

Definizione 2.1. *Sia K un campo e siano $f_1, \dots, f_t \in K[x_0, \dots, x_n]$ polinomi omogenei. L'insieme*

$$\boldsymbol{V}(f_1, \dots, f_t) = \{(a_0, \dots, a_n) \in \mathbb{P}^n(K) \mid f_i(a_0, \dots, a_n) = 0 \ \forall 1 \leq i \leq t\}$$

si chiama varietà proiettiva definita da $f_1, \dots, f_t$. In particolare, se f è un polinomio omogeneo, $\mathbf{V}(f)$ si dice una ipersuperficie.

Vediamo ora come le varietà affini in K^n definite da polinomi appartenenti a $K[x_1, \dots, x_n]$ possano essere ampliate a varietà proiettive rendendo i loro polinomi omogenei; tale procedimento è detto omogeneizzazione.

Proposizione 2.2. Sia $g(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ un polinomio di grado d.

(i) Sia $g = \sum_{i=0}^{d} g_i$ l'espansione di g nelle sue componenti omogenee, dove g_i ha grado i. Allora:

$$g^h(x_0, \dots, x_n) = \sum_{i=0}^{d} g_i(x_1, \dots, x_n) x_0^{d-i}$$

è un polinomio omogeneo di grado d in $K[x_0, \dots, x_n]$. g^h si dice omogeneizzazione di g.

(ii) L'omogeneizzazione di g si può ricavare dalla formula $g^h = x_0^d g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right)$.

(iii) La deomogeneizzazione di g^h riporta a g, ossia $g^h(1, x_1, \dots, x_n) = g(x_1, \dots, x_n)$.

(iv) Sia $F(x_0, \dots, x_n)$ polinomio omogeneo e sia x_0^e la potenza più grande di x_0 che divide F. Se $f(x_1, \dots, x_n) = F(1, x_1, \dots, x_n)$ è la deomogeneizzazione di F, allora $F(x_0, \dots, x_n) = x_0^e f^h(x_0, \dots, x_n)$.

La definizione di varietà proiettiva vista si può generalizzare, mettendo in luce la relazione che c'è tra varietà proiettive e ideali omogenei. Si nota che l'essere omogeneo non è una proprietà che conserva l'operazione di somma, infatti la somma di due polinomi omogenei di grado diverso non è uguale a un polinomio omogeneo. Per ovviare a tale problema è necessario considerare una particolare classe di ideali, detti ideali omogenei.

Definizione 2.3. *Un ideale I in $K[x_0, \dots, x_n]$ si dice omogeneo se per ogni $f \in I$, le sue componenti omogenee $f_i \in I$ $\forall i$.*

Segue che per ogni ideale omogeneo $I \subset K[x_0, \dots, x_n]$ si può definire la varietà proiettiva come $\mathbf{V}(I) = \{p \in \mathbb{P}^n(K) \mid f(p) = 0 \ \forall f \in I \text{ omogeneo}\}$. Inoltre se V è varietà proiettiva si può definire l'ideale omogeneo come $\mathbf{I}(V) = \{f \in K[x_0, \dots, x_n] \mid f(a_0, \dots, a_n) = 0 \quad \forall (a_0, \dots, a_n) \in V\}$.

3 Il Teorema di Bezout

Da questa sezione consideriamo solo il piano proiettivo sul campo dei complessi, ossia $\mathbb{P}^2(\mathbb{C})$, perciò le curve algebriche di cui trattiamo saranno varietà proiettive $\mathbf{V}(f)$ definite da $f \in \mathbb{C}[x, y, z]$ polinomio omogeneo non nullo. Prima di enunciare il teorema di Bezout, vediamo cosa si intende quando si parla di componenti irriducibili di una curva e di molteplicità di intersezione.

Proposizione 3.1. Sia $f \in \mathbb{C}[x,y,z]$ un polinomio omogeneo non nullo, allora i fattori irriducibili di f sono omogenei.

Dimostrazione. Suppongo che f omogeneo si fattorizzi come $f = gh$ per qualche polinomio $g, h \in \mathbb{C}[x,y,z]$. Allora si scrive $g = g_m + \cdots + g_0$, dove g_i è omogeneo di grado i e in modo analogo si scrive $h = h_n + \cdots + h_0$, dove h_j è omogeneo di grado j. Allora

$$f = gh = g_m h_n + \text{termini di grado minore}$$

Poichè f è omogeneo allora i termini di grado minore sono nulli. Segue $f = g_m h_n$, ossia $g = g_m$ e $h = h_n$, cioè g e h sono omogenei. □

Quindi se $C = \mathbf{V}(f)$ e f si fattorizza come $f = f_1^{\alpha_1} \cdots f_s^{\alpha_s}$, si dice che $f_1 \cdots f_s$ è l'equazione ridotta di C, unica a meno di costanti moltiplicative. La nostra prima ipotesi sarà quella di considerare due curve $C = \mathbf{V}(f)$ e $D = \mathbf{V}(g)$ senza componenti irriducibili in comune, ossia f e g non devono avere fattori in comune.

Definizione 3.2. *Siano $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{j=0}^{n} b_j x^j$ due polinomi in $\mathbb{C}[x]$. Il risultante è definito come il determinante della seguente matrice data dai coefficienti di f e g:*

$$Res(f,g,x) = \det \begin{pmatrix} a_0 & & & b_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_m & & a_0 & b_n & & b_0 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_m & & & b_n \end{pmatrix} \tag{1}$$

Lemma 3.3. Siano $f, g \in \mathbb{C}[x,y,z]$ polinomi omogenei di grado rispettivamente m, n. Se $f(0,0,1) \neq 0$ e $g(0,0,1) \neq 0$, allora il risultante $Res(f,g,z)$ è un polinomio omogeneo in x e y di grado mn.

Dimostrazione. Scrivo f e g come polinomi in z, ossia:

$$f = a_0 z^m + \cdots + a_m$$
$$g = b_0 z^n + \cdots + b_n$$

dove ogni $a_i, b_j \in \mathbb{C}[x,y]$ sono omogenei di grado rispettivamente i, j e $a_0 \neq 0$, $b_0 \neq 0$ poichè $f(0,0,1), g(0,0,1)$ sono non nulli. Il risultante $Res(f,g,z)$ è dato dal determinante della matrice $(m+n)\times(m+n)$ come in (1). Chiamo ora c_{ij} la componente (i,j) della matrice. Allora si ha:

$$c_{ij} = \begin{cases} a_{i-j} & \text{se } j \leq n \\ b_{n+i-j} & \text{se } j > n \end{cases}$$

c_{ij} è omogeneo di grado $i - j$ se $j \leq n$ oppure $n + i - j$ se $j > n$.
Il determinante è una somma i cui addendi sono del tipo $\pm \prod_{i=1}^{m+n} c_{i\sigma(i)}$, dove σ è una permutazione di $\{1, \ldots, m+n\}$. Poichè ogni fattore è non nullo allora si può scrivere il prodotto come:

$$\pm \prod_{\sigma(i) \leq n} c_{i\sigma(i)} \prod_{\sigma(i) > n} c_{i\sigma(i)}$$

Il prodotto è un polinomio omogeneo il cui grado è :

$$\underbrace{\sum_{\sigma(i)\leq n}(i-\sigma(i))}_{n \text{ addendi}} + \underbrace{\sum_{\sigma(i)>n}(n+i-\sigma(i))}_{m \text{ addendi}} = mn + \sum_{i=1}^{m+n} i - \sum_{i=1}^{m+n}\sigma(i) = mn$$

Questo prova che $Res(f, g, z)$ è una somma di polinomi omogenei nelle coordinate x e y di grado mn. □

Lemma 3.4. Sia $h \in \mathbb{C}[x, y]$ un polinomio omogeneo non nullo. Allora si può scrivere nella forma:

$$h = c(s_1x - r_1y)^{m_1} \dots (s_kx - r_ky)^{m_k}$$

dove $c \neq 0$ in $\mathbb{C}$ e $(r_1, s_1), \dots, (r_k, s_k)$ sono punti distinti di $\mathbb{P}^1(\mathbb{C})$. In particolare , $\mathbf{V}(h) = \{(r_1, s_1), \dots, (r_k, s_k)\} \subset \mathbb{P}^1(\mathbb{C})$.

Dai due lemmi appena dimostrati segue un importante teorema che mostra che il numero di punti di intersezione di due curve è finito e, in particolare, non è maggiore del prodotto dei gradi delle equazioni ridotte che le definiscono.

Teorema 3.5 (**Forma debole del Teorema di Bezout**)**.** Siano C e D curve in $\mathbb{P}^2(\mathbb{C})$ senza fattori comuni. Se i gradi delle equazioni ridotte di C e D sono rispettivamente m e n, allora l'intersezione $C \cap D$ è finita ed ha al massimo mn punti.

Dimostrazione. Suppongo per assurdo che $C \cap D$ abbia più di mn punti. Prendo i punti $p_1, \dots, p_{mn+1}$ e considero, per $1 \leq i < j \leq mn + 1$, le rette L_{ij} che passano da p_i e da p_j. Fisso ora un punto $q \in \mathbb{P}^2(\mathbb{C})$ tale che

$$q \notin C \cup D \cup \bigcup_{i<j} L_{ij} \tag{2}$$

Ora è facile trovare un'applicazione lineare $A : \mathbb{P}^2(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C})$ tale che $A(q) = (0, 0, 1)$. Perciò considero q nelle nuove coordinate in modo tale che la condizione (2) valga per il punto $q = (0, 0, 1)$.

Suppongo $C = \mathbf{V}(f)$ e $D = \mathbf{V}(g)$ con f e g equazioni ridotte di gradi rispettivamente m e n. Allora per (2) si ha che $(0, 0, 1) \notin C$, che implica $f(0, 0, 1) \neq 0$, e analogamente $g(0, 0, 1) \neq 0$. Inoltre per il lemma 3.3 $Res(f, g, z)$ è un polinomio omogeneo di grado mn in x e y e, poichè f e g hanno grado positivo in z e non hanno fattori in comune in $\mathbb{C}[x, y, z]$, allora $Res(f, g, z) \neq 0$.

Chiamo $p_i = (u_i, v_i, w_i)$ e, da $Res(f, g, z) \in (f, g) \cap \mathbb{C}[x, y]$ (vedi [1], p. 163), segue

$$Res(f, g, z)(u_i, v_i) = 0 \tag{3}$$

Si nota ora che se considero la retta passante per $q = (0, 0, 1)$ e p_i, questa interseca la retta $z = 0$. Quindi, per (3), $Res(f, g, z)$ si annulla sui punti che si ottengono proiettando $p_i \in C \cap D$ da $(0, 0, 1)$ sulla retta $z = 0$. Ma da (2), $(0, 0, 1)$ non giace su nessuna delle rette L_{ij}, quindi i punti $(u_i, v_i, 0)$ sono tutti distinti per $i = 1, \dots, mn + 1$.

Se si prendono i punti distinti $(u_i, v_i) \in \mathbb{P}^1(\mathbb{C})$ per $i = 1, \ldots, mn + 1$, allora il polinomio omogeneo $Res(f, g, z)$ si annulla su tutti gli $mn + 1$ punti considerati. Ma questo è assurdo poichè per il lemma precedente, $Res(f, g, z)$ è non nullo di grado mn. □

Definizione 3.6. *Siano C e D curve in $\mathbb{P}^2(\mathbb{C})$ senza fattori comuni e definite dalle equazioni ridotte $f = 0$ e $g = 0$. Scelte le coordinate per $\mathbb{P}^2(\mathbb{C})$ così che sia soddisfatta*

$$(0, 0, 1) \notin C \cup D \cup \bigcup_{p \neq q \in C \cap D} L_{pq} \tag{4}$$

Allora, preso $p = (u, v, w) \in C \cap D$, la molteplicità di p, $I_p(C, D)$, è definita dall'esponente di $vx - uy$ nella fattorizzazione di $Res(f, g, z)$.

Osserviamo che prese le curve $C = \mathbf{V}(f)$ e $D = \mathbf{V}(g)$ senza componenti irriducibili in comune, se $p = (u, v, w) \in C \cap D$ e vale (4), allora, come visto nella dimostrazione del teorema precedente, $Res(f, g, z)(u, v) = 0$. Quindi effettivamente $(vx - uy)$ è un fattore del risultante.

Abbiamo ora tutte le ipotesi per poter enunciare il teorema di Bezout.

Teorema 3.7 (di Bezout). Siano C e D due curve in $\mathbb{P}^2(\mathbb{C})$ senza fattori in comune, e siano m e n i gradi rispettivi delle equazioni ridotte che definiscono le curve. Allora

$$\sum_{p \in C \cap D} I_p(C, D) = mn$$

dove $I_p(C, D)$ indica la molteplicità di intersezione di p, come definita nella Definizione 3.6.

Dimostrazione. Siano f e g le equazioni ridotte di C e D e suppongo che le coordinate siano scelte in modo che soddisfino (4). Scrivo i punti di $C \cap D$ come $p = (u_p, v_p, w_p)$. Allora per i lemmi 3.3 e 3.4:

$$Res(f, g, z) = c \prod_{p \in C \cap D} (v_p x - u_p y)^{I_p(C,D)} \tag{5}$$

dove c è una costante non nulla. Dalla definizione di molteplicità, $\forall p$, è chiaro che $(v_p x - u_p y)^{I_p(C,D)}$ è l'esatta potenza che divide il risultante.

Proviamo ora che vale per tutte le radici. Se $(u, v) \in \mathbb{P}^1(\mathbb{C})$ soddisfa $Res(f, g, z)(u, v) = 0$, allora $\exists w \in \mathbb{C}$ tale che f e g si annulla in (u, v, w). Infatti se f e g sono scritte come nel Lemma 3.3, a_0 e b_0 sono costanti non nulle per (4). Allora $(u, v, w) \in C \cap D$.

Sappiamo inoltre che $Res(f, g, z)$ è un polinomio omogeneo non nullo di grado mn. Allora il teorema segue facilmente confrontando il grado del risultante e della produttoria. □

4 Decomposizione primaria

Sia $I = (f_1, \ldots, f_t)$ un ideale zero dimensionale di $\mathbb{C}[x_1, \ldots, x_n]$, ossia il sistema costituito dalle f_i ha un numero finito di soluzioni uguale a k, e considero il quoziente $\mathbb{C}[x_1, \ldots, x_n]/I$, la cui dimensione è pari a k. Prendiamo come base di tale quoziente $\{[x^a] \mid x^a \notin LT(I)\}$,

costituita dalle classi di monomi modulo I non contenuti in $LT(I)$ (vedi [1], §5.3). Consideriamo ora l'applicazione lineare rispetto alla base data dalle classi $[x^a]$ indotta dalla moltiplicazione per x_i:

$$M_{x_i} : \mathbb{C}[x_1, \ldots, x_n]/I \to \mathbb{C}[x_1, \ldots, x_n]/I$$
$$[g] \mapsto [gx_i]$$

Tali matrici sono dette matrici compagne di I. Similmente si definisce la matrice compagna rispetto alla moltiplicazione per $h(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ come $M_{h(x_1,\ldots,x_n)} = h(M_{x_1}, \ldots, M_{x_n})$. Inoltre, per ogni $h, k \in \mathbb{C}[x_1, \ldots, x_n]$ e $a \in \mathbb{C}$, sono soddisfatte le proprietà di linearità rispetto alla somma e al prodotto di M_h e M_k, e al prodotto di M_h per uno scalare a.

Teorema 4.1 (**Decomposizione primaria**)**.** (Per la dimostrazione vedi [4])

Sia $\mathbf{V}(I) = \{p_1, \ldots, p_k\}$. Sia $h(x) \in \mathbb{C}[x_1, \ldots, x_n]$ tale che $h(p_i)$ siano distinti. Considero per $i = 1, \ldots, k$ le applicazioni lineari

$$M_{h(x)-h(p_i)} : \mathbb{C}[x_1, \ldots, x_n]/I \to \mathbb{C}[x_1, \ldots, x_n]/I$$

(i) Posto $A_i = Ker(M_{(h(x)-h(p_i))})^\infty$, ossia gli autospazi generalizzati di $M_{h(x)}$, sottoalgebre e ideali di $\mathbb{C}[x_1, \ldots, x_n]$, abbiamo la decomposizione diretta di sottoalgebre

$$\mathbb{C}[x_1, \ldots, x_n]/I = \oplus_{i=1}^{k} A_i \tag{6}$$

(ii) Posto $J_i = \oplus_{j \neq i} A_j$, ideale di $\mathbb{C}[x_1, \ldots, x_n]/I$, la sua retroimmagine $\tilde{J}_i \subset \mathbb{C}[x_1, \ldots, x_n]$ è un ideale primario, tale che $\sqrt{\tilde{J}_i} = M_i$, dove M_i è l'ideale massimale dato dai polinomi che si annullano in p_i, e $A_i = \mathbb{C}[x_1, \ldots, x_n]/(\tilde{J}_i)$,

$$\cap_{i=1}^{n} \tilde{J}_i = I$$

Tale intersezione si dice decomposizione primaria di I.

Da questo teorema deriva la seguente definizione di molteplicità, che nella prossima sezione faremo vedere essere equivalente a quella già definita in precedenza:

Definizione 4.2. $\dim A_i$ *si dice molteplicità di* p_i *in* I

Osservazione 4.3. La decomposizione diretta di sottoalgebre del Teorema 4.1 non dipende dalla scelta di $h(x)$. Supponiamo di avere un secondo polinomio $k(x) \in \mathbb{C}[x_1, \ldots, x_n]$ che assume valori distinti sui punti p_i e vediamo che $A_i = Ker(M_{h(x)-h(p_i)})^\infty = Ker(M_{k(x)-k(p_i)})^\infty = A_i'$.

Ora, A_i è $k(x)$-invariante, infatti $A_i = Ker(M_{h(x)-h(p_i)})^N$ per N sufficientemente grande e preso $v \in A_i$ si ha che $(M_{h(x)-h(p_i)})^N \cdot (M_{k(x)}v) = M_{k(x)} \cdot (M_{h(x)-h(p_i)})^N v = 0$, perchè $(M_{h(x)-h(p_i)})^N v = 0$, ossia $M_{k(x)}v \in A_i$. Dal Teorema 4.1 si sa inoltre che $A_i = \mathbb{C}[x_1, \ldots, c_n]/(\tilde{J}_i)$ e $\mathbf{V}(\tilde{J}_i) = \{p_i\}$, allora l'unico autovalore di $M_{k(x)}$ su A_i è $k(p_i)$ (vedi [4], p. 17). Segue che $A_i = Ker(M_{h(x)-h(p_i)})^\infty \subseteq Ker(M_{k(x)-k(p_i)})^\infty = A_i'$. Inoltre, la somma dei A_i e quella dei A_i' sono dirette, quindi vale l'uguaglianza: $A_i = A_i'$.

Dall'osservazione segue che la Definizione 4.2 è ben definita e non dipende dalla scelta del polinomio $h(x)$, così come le sottoalgebre A_i del Teorema che dipendono solo da I.

5 Molteplicità di intersezione di curve algebriche

Abbiamo visto due definizioni diverse di molteplicità dei punti di intersezione di due curve e si vuole ora dimostrare che tali definizioni sono equivalenti. Da qui in avanti useremo la notazione m_{CLO} e m_{GAC} per indicare la molteplicità rispettivamente secondo la definizione 3.6 e 4.2 e supporremmo che, date le curve C e D, i punti appartenenti a $C \cap D$ soddisfino la condizione (4).

Lemma 5.1. Siano $C = \mathbf{V}(f)$ e $D = \mathbf{V}(g)$ due curve in $\mathbb{P}^2(\mathbb{C})$ senza fattori in comune e siano $p_i = (\alpha_i, \beta_i, 1)$, per $i = 1, \ldots, k$, i punti distinti di $C \cap D$ che soddisfano le seguenti condizioni :

1. Nessun punto p_i giace sulla retta all'∞, ossia $z = 0$.
2. Ogni polinomio $a_s(x, y) = \beta_s x - \alpha_s y$ assume valori distinti sui punti (α_i, β_i), per ogni $i = 1, \ldots, k$.

Se $\mathcal{R} = \mathbb{C}[x, y]/(f(x, y, 1), g(x, y, 1))$ e $\mathcal{R}_i = Ker(M_{\beta_i x - \alpha_i y})^\infty$ per $i = 1, \ldots, k$, allora

$$\mathcal{R} = \oplus_{i=1}^{k} \mathcal{R}_i$$

Dimostrazione. Fissato s, il polinomio $a_s(x, y) = \beta_s x - \alpha_s y$ per ipotesi assume valori distinti sui punti $p_i = (\alpha_i, \beta_i)$ $\forall i$ e in particolare:

$$\beta_s \alpha_i - \alpha_s \beta_i = \begin{cases} = 0, & \text{se } i = s \\ \neq 0, & \text{se } i \neq s \end{cases}$$

Chiamo $A_i^{(s)} = Ker(M_{a_s(x,y) - a_s(\alpha_i, \beta_i)})^\infty$ e osserviamo che $A_s^{(s)} = Ker(M_{a_s(x,y) - a_s(\alpha_s, \beta_s)})^\infty = Ker(M_{\beta_s x - \alpha_s y})^\infty = \mathcal{R}_s$. Per il Teorema di Decomposizione Primaria, $\mathcal{R} = \oplus_{i=1}^{k} A_i^{(s)}$, ma la decomposizione in somma diretta non dipende dalla scelta del polinomio $a_s(x, y)$ per ogni s, per l'osservazione 4.3. In particolare per il punto p_i si osserva che $\forall s$:

$$\mathcal{R}_i = A_i^{(i)} = Ker(M_{a_i(x,y) - a_i(\alpha_i, \beta_i)})^\infty = Ker(M_{a_s(x,y) - a_s(\alpha_i, \beta_i)})^\infty = A_i^{(s)}$$

Segue che $\mathcal{R} = \oplus_{i=1}^{k} A_i^{(s)} = \oplus_{i=1}^{k} \mathcal{R}_i$. □

Osservazione 5.2. Segue dalla dimostrazione del lemma precedente che $\dim \mathcal{R}_i = m_{GAC,i}$.

Prima di enunciare il Teorema, definiamo la funzione di Hilbert che ci servirà per la dimostrazione.

Definizione 5.3. *Sia I ideale omogeneo di $\mathbb{C}[x_0, \ldots, x_n]$. La funzione di Hilbert proiettiva è definita per ogni naturale s da*

$$F_I(s) = \dim \frac{\mathbb{C}[x_0, \ldots, x_n]_s}{I_s}$$

dove $I_s = I \cap \mathbb{C}[x_0, \ldots, x_n]_s$ e $\mathbb{C}[x_0, \ldots, x_n]_s = \{p \in \mathbb{C}[x_0, \ldots, x_n] \mid \deg p = s\}$.

Teorema 5.4. Siano C e D due curve in $\mathbb{P}^2(\mathbb{C})$ senza fattori in comune e siano m e n i gradi rispettivi delle equazioni ridotte f e g che definiscono le curve. Allora le Definizioni 3.6 e 4.2 di molteplicità sono equivalenti.

Dimostrazione. Siano $f(x,y,z)$ e $g(x,y,z)$ i polinomi omogenei che definiscono rispettivamente le curve C e D. Deomogeneizzando i due polinomi rispetto a z, si trova $F(x,y) = f(x,y,1)$ e $G(x,y) = g(x,y,1)$, entrambi non nulli per la condizione (4).

Chiamo $\mathcal{R} = \mathbb{C}[x,y]/(F(x,y),G(x,y))$ e sia $h(x,y) = Res(f,g,z)$ polinomio omogeneo in x e y. I punti $p_i = (\alpha_i,\beta_i)$ per $i = 1,\dots,k$ sono i punti distinti di $C \cap D$ in $\mathbb{C}^2 \subset \mathbb{P}^2(\mathbb{C})$, infatti si può assumere che nessuno dei punti p_i stia su $z = 0$, se necessario si può operare un cambio di coordinate. Allora si può scrivere il risultante come:

$$h(x,y) = c\prod_{i=1}^{k}(\beta_i x - \alpha_i y)^{m_{CLO,i}} \tag{7}$$

dove $m_{CLO,i} = I_{p_i}(C,D)$ e $c \neq 0$ costante.

Se inoltre consideriamo il polinomio $a_j(x,y) = \beta_j x - \alpha_j y$, possiamo supporre che il polinomio a_j assuma valori distinti su ogni punto (α_i,β_i) $\forall i = 1,\dots,k$; infatti questo è vero per una scelta strategica di $(0,0,1)$ e si può sempre trovare tale punto con un opportuno cambio di coordinate.

La dimostrazione si può ora suddividere in due parti. Nella prima parte vedremo che $m_{GAC,i} \leq m_{CLO,i}$, mentre nella seconda proveremo che $\dim \mathcal{R} = mn$.

I) Dal lemma 5.1, $\mathcal{R} = \oplus_{i=1}^{k}\mathcal{R}_i$ e per il punto (ii) del Teorema 4.1 si ha che, per ogni i, $\mathcal{R}_i = \mathbb{C}[x,y]/(\tilde{J}_i)$, con $\tilde{J}_i$ ideale tale che $\sqrt{\tilde{J}_i} = (x-\alpha_i, y-\beta_i)$. Per come è definito $\sqrt{\tilde{J}_i}$, $\exists N_i$ tale che $(x-\alpha_i)^{N_i} \equiv 0 \bmod (\tilde{J}_i)$ e $(y-\beta_i)^{N_i} \equiv 0 \bmod (\tilde{J}_i)$.

Pongo $N = \max(N_1,\dots,N_k)$ e $t = \frac{y}{x}$ e definisco l'applicazione lineare e suriettiva:

$$\begin{aligned}\phi: \qquad \mathbb{C}[t]/(h(t)) &\longrightarrow \mathcal{R}\\ p(t) \bmod (h(t)) &\longmapsto x^{2N}p\left(\frac{y}{x}\right) \bmod (F,G)\end{aligned}$$

- ϕ è suriettiva. Per dimostrarlo vediamo che ogni classe $[q] \in \mathcal{R}$ ha un rappresentante della forma $q(x,y) = x^{2N}p(\frac{y}{x})$ con $\deg p < 2N$. In particolare, poichè $\mathcal{R}$ è somma diretta di $\mathcal{R}_i$, è sufficiente provare la tesi per un $[q] \in \mathcal{R}_i$.
  Considero lo sviluppo di Taylor in (α_i,β_i) di $q(x,y)$, ossia $q(x,y) = q(\alpha_i,\beta_i) + (x-\alpha_i)\frac{\partial q}{\partial x}(\alpha_i,\beta_i) + (y-\beta_i)\frac{\partial q}{\partial y}(\alpha_i,\beta_i) + \cdots = \sum_{i,j} c_{ij}(x-\alpha_i)^i(y-\beta_i)^j$ per opportune costanti c_{ij}. Per $q(x,y) \bmod (\tilde{J}_i)$ si può osservare che non ci sono addendi di grado totale $\geq 2N$, quindi ogni $[q] \in \mathcal{R}_i$ ha un rappresentante di grado totale $\leq 2N$.

Ora per il Teorema cinese dei resti, $\mathbb{C}[t]/(h(t)) = \oplus_{i=1}^{k}\mathbb{C}[t]/((\beta_i - \alpha_i t)^{m_{CLO,i}})$, mentre $\mathcal{R} = \oplus_{i=1}^{k}\mathcal{R}_i$, vogliamo allora dimostrare che l'applicazione definita rispetta gli addendi.

- ϕ rispetta gli addendi.
  Sia $h_i(t) = \frac{h(t)}{(\beta_i - \alpha_i t)^{m_{CLO,i}}}$ per $i = 1, \ldots, k$. Si osserva che $MCD(h_1, \ldots, h_k) = 1$, allora $\exists b_1, \ldots, b_k$ tali che $\sum_{i=1}^{k} b_i h_i = 1$. Preso $\bar{f} \in \mathbb{C}[t]/(h(t))$, $\bar{f} = \sum_{i=1}^{k} b_i h_i \bar{f}$, e in particolare $b_i h_i \bar{f} \in \mathbb{C}[t]/(\beta_i - \alpha_i t)^{m_{CLO,i}}$, per ogni i.

  $$(b_i h_i \bar{f})(\beta_i x - \alpha_i y)^{m_{CLO,i}} \equiv 0 (mod(F, G))$$

  quindi $(b_i h_i \bar{f})$ è autovettore di $(M_{\beta_i x - \alpha_i y})^{m_{CLO,i}}$ con autovalore nullo.
  $\mathcal{R}_s$ è autospazio generalizzato per $(M_{\beta_i x - \alpha_i y})^{m_{CLO,i}}$ con autovalore $a_i(\alpha_s, \beta_s)$ che è $= 0$ se $i = s$ ed è $\neq 0$ se $i \neq s$. Perciò

  $$b_i h_i \bar{f} = \begin{cases} \in \mathcal{R}_i \\ \notin \mathcal{R}_s \quad \text{se } s \neq i \end{cases}$$

  $\mathcal{R}_i$ sono sottoalgebre (e ideali) perciò sono chiuse per la moltiplicazione per potenze di x, segue che $\phi(b_i h_i \bar{f}) = x^{2N}(b_i h_i \bar{f})\left(\frac{y}{x}\right) \in \mathcal{R}_i$.

Allora:

$$m_{GAC} = \sum_{i=1}^{k} m_{GAC,i} = \sum_{i=1}^{k} \dim \mathcal{R}_i = \dim \mathcal{R} \leq \dim \frac{\mathbb{C}[t]}{(h(t))} =$$
$$= \sum_{i=1}^{k} \dim \frac{\mathbb{C}[t]}{((\beta_i - \alpha_i t)^{m_{CLO,i}})} = \sum_{i=1}^{k} m_{CLO,i} = mn = m_{CLO} \quad (8)$$

Ma in particolare poichè l'applicazione rispetta gli addendi si ha che $m_{GAC,i} \leq m_{CLO,i}$.

II) Sia $I = (f, g)$ e provo che la funzione di Hilbert $F_I(d) = \dim \frac{\mathbb{C}[x,y,z]_d}{I_d} = mn \ \forall d \geq m + n$.
Infatti sia $S = \mathbb{C}[x, y, z]$, allora $I_d \to S_d \to S_d/I_d$. Considero ora:

$$\mathbb{C}_{d-m} \oplus \mathbb{C}_{d-n} \to I_d \to 0$$
$$(h_1, h_2) \mapsto h_1 f + h_2 g$$

Il cui nucleo è

$$\mathbb{C}_{d-m-n} \hookrightarrow \mathbb{C}_{d-m} \oplus \mathbb{C}_{d-n}$$
$$k \mapsto (kg, -kf)$$

Infatti $(kg)f + (-kf)g = 0$. Si può quindi concludere che

$$F_I(d) = \dim(S_d/I_d) =$$
$$= \binom{d+2}{2} - \left(\binom{d-m+2}{2} + \binom{d-n+2}{2}\right) + \binom{d-m-n+2}{2} =$$
$$= \frac{(d+2)(d+1)}{2} - \left(\frac{(d-m+2)(d-m+1)}{2} + \frac{(d-n+2)(d-n+1)}{2}\right) +$$
$$+ \frac{(d-m-n+2)(d-m-n+1)}{2} = \frac{1}{2}\{d[3 - (-2m + 3 - 2n + 3)$$
$$- 2m - 2n + 3] + [-(m^2 - 3m + n^2 - 3n) + m^2 + 2mn - 3m + n^2 - 3n]\}$$
$$= \frac{2mn}{2} = mn$$

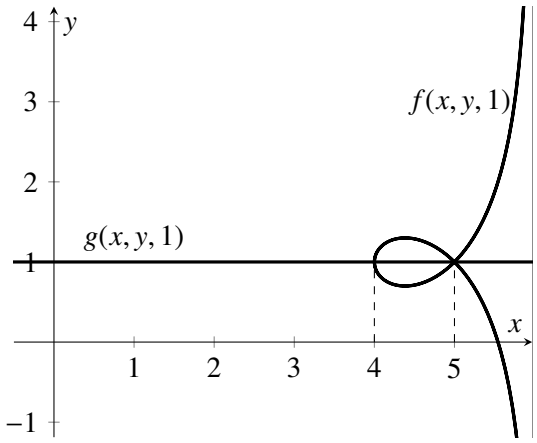
Ora, $\dim \mathcal{R} = \dim \frac{\mathbb{C}[x,y,z]_d}{I_d}$ per $d \gg 0$. Questo termina la dimostrazione poichè si ha che le disuguaglianze della prima parte diventano uguaglianze per ogni i, ossia $m_{GAC,i} = m_{CLO,i}$.

□

6 Esempio

Prendiamo le due curve algebriche $C = \mathbf{V}(-x^3 + 14x^2z + y^2z - 65xz^2 - 2yz^2 + 101z^3)$ e $D = \mathbf{V}((y-z)^3)$. Osserviamo che C e D non hanno componenti irriducibili in comune e che $f(0,0,1) = 101 \neq 0$ e $g(0,0,1) = -1 \neq 0$, perciò è soddisfatta la condizione (4). Usiamo il software Macaulay2 per vedere che le molteplicità m_{GAC} e m_{CLO} coincidono. Calcoliamo il risultante $Res(f,g,z)$ con il seguente codice:

```
R=QQ[x,y,z]
f=-x^3+14*x^2*z+y^2*z-65*x*z^2-2*y*z^2+101*z^3
g=(y-z)^3
factor resultant(f,g,z)
```



Tale codice ci rende la fattorizzazione del risultante uguale a $Res(f,g,z) = (x-5y)^6(x-4y)^3$. I punti di intersezione in $\mathbb{C}^2$ e le relative molteplicità sono: $p_1 = (5,1)$ con $I_{p_1}(C,D) = 6$ e $p_2 = (4,1)$ con $I_{p_2}(C,D) = 3$. Inoltre si può osservare dal grafico di $f(x,y,1)$ e $g(x,y,1)$ che i due punti di intersezione non intersecano la retta $z = 0$, quindi anche l'ideale zero dimensionale $I = (-x^3 + 14x^2 + y^2 - 65x - 2y + 101, (y-1)^3)$ ha esattamente 9 soluzioni e $\mathbf{V}(I) = \{p_1, p_2\} \subset \mathbb{C}^2$.

Vediamo ora che prese le matrici compagne relative ai polinomi ottenuti dalla fattorizzazione di $Res(f,g,z)$ cosa otteniamo.

```
J=ideal(sub(f,z=>1),sub(g,z=>1))
S=QQ[x,y]
I=sub(J,S)
bb=sub(basis(S/I),S)
```

```
h=x-5*y
comph=sub(contract(transpose bb,(bb_(0,0))*h%I),{x=>0,y=>0})
for i from 1 to 8 do
comph=comph|sub(contract(transpose bb,(bb_(0,i))*h%I),{x=>0,y=>0})
for i from 1 to 6 do print(i,rank comph^i)
--si puo' ripetere il procedimento con h=x-4*y
```

Nel codice, preso l'ideale zero dimensionale I, abbiamo costruito la matrice compagna M_h con $h = x - 5y$ relativa all'autovalore $h(p_1) = h(5, 1) = 0$. Abbiamo stampato il rango di $(M_{x-5y})^i$ per $i = 1, \ldots, 6$, ottenendo i seguenti valori:
$(1, 7); (2, 5); (3, 4); (4, 3); (5, 3); (6, 3)$

dove il primo elemento è relativo alla potenza della matrice compagna e il secondo è relativo al rango.

Si osserva che il rango dalla quarta potenza si stabilizza a 3, quindi $m_{GAC,1} = \dim Ker(M_{x-5y})^\infty = 9 - 3 = 6$. Questo prova che la molteplicità del punto p_1 secondo le due definizioni viste è uguale a 6. Analogamente si può vedere che $m_{GAC,2} = 3$.

Riferimenti bibliografici

[1] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties and Algorithms*, third edition, Springer, New York, 2007.

[2] W. Fulton, *Algebraic Curves, An introduction to algebraic geometry*, Benjamin, New York, 1969

[3] F. Kirwan, *Complex Algebraic Curves*, London Mathematical Society Student Texts 23, Cambridge University Press, Cambridge, 1992

[4] G. Ottaviani, *Soluzioni di equazioni polinomiali zero dimensionali*, note reperibili online

[5] G. Ottaviani, *Introduzione alle varietà algebriche, un punto di vista costruttivo*, note reperibili online