Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Specialistica in Matematica

La teoria dell'eliminazione e alcune sue applicazioni

Tesi di Laurea Specialistica in Algebra Computazionale

Relatore:
Chiar.mo Prof.
Mirella Manaresi

Presentata da:
Eugenio Laghi

II Sessione
Anno Accademico 2010/2011

Introduzione

La teoria dell'eliminazione è lo studio dei metodi che permettono di trasformare un sistema di equazioni polinomiali in più di variabili, in un sistema equivalente in cui interviene solo un sottoinsieme dell'insieme delle variabili di partenza.

Nel caso di un sistema lineare, se è risolubile, lo si può trasformare in un sistema di cui è facile determinare le soluzioni sfruttando il metodo di eliminazione di Gauss.

Ci sono testimonianze di utilizzo di questo metodo di eliminazione già nel III secolo da parte di matematici cinesi nel libro "Nove Capitoli sull'arte matematica" . L'ottavo dei nove capitoli parla di sistemi di equazioni lineari in un numero arbitrario di incognite e presenta 17 esempi di questo tipo, risolti tutti con lo stesso algoritmo proposto da Gauss nel 1826.

Se il sistema di equazioni polinomiali non è lineare, nel caso di due polinomi in una sola variabile possiamo sfruttare il determinante della matrice di Sylvester dei due polinomi, detto risultante, per trovare le soluzioni del sistema.

Un passaggio cruciale per lo sviluppo della teoria dell'eliminazione è stata l'introduzione delle basi di Groebner di un ideale dell'anello dei polinomi in un qualunque numero di indeterminate, rispetto ad un ordine monomiale fissato, secondo un'idea che risale a Gordan (1899). Tali basi per l'ideale generato dai polinomi che intervengono nelle equazioni del sistema costituiscono la più naturale generalizzazione del metodo di eliminazione di Gauss. Nel 1965 Bruno Buchberger ha dimostrato che una tale base esiste sempre

e ha elaborato un algoritmo per calcolare la base di Groebner di un ideale polinomiale rispetto ad un qualunque ordine monomiale. Attraverso tali basi si possono dare criteri per stabilire se un sistema è risolubile e se ne possono calcolare le soluzioni.

Un'applicazione naturale dell'eliminazione permette di determinare le equazioni cartesiane di una varietà algebrica definita mediante una parametrizzazione polinomiale o razionale, o più precisamente di determinare le equazioni della più piccola varietà algebrica affine che contiene l'insieme definito attraverso equazioni parametriche. Questo perché in generale la proiezione di una varietà affine può non essere una varietà affine. Nel caso di varietà proiettive, la proiezione è sempre una varietà proiettiva e la teoria dell'eliminazione proiettiva permette di determinarne le equazioni.

Attraverso l'eliminazione, e in particolare grazie all'uso del risultante, è possibile dare una dimostrazione del teorema di Bezout per le curve piane, che dice che la somma delle molteplicità di intersezione nei punti di intersezione di due curve senza componenti in comune è uguale al prodotto dei gradi dei polinomi che definiscono le due curve.

L'ultima applicazione dell'eliminazione che affronteremo in questa tesi è la *forma di Chow*: un polinomio che permette di individuare una varietà proiettiva equidimensionale di dimensione $k-1$ in $\mathbb{P}^{n-1}$ attraverso una ipersuperficie della grassmanniana $\mathbb{G}(n-k,n)$, di cui la forma di Chow fornisce l'equazione.

Indice

Introduzione **i**

1 Cenni preliminari **1**

1.1 Ideali radicali e Nullstellensatz 1

1.2 Basi di Groebner 3

1.2.1 Proprietà delle Basi di Groebner 4

1.3 Chiusura proiettiva di una varietà affine 6

2 Teoria dell'eliminazione affine **9**

2.1 Interpretazione dal punto di vista geometrico 11

2.2 Risultante 15

2.2.1 Risultante di polinomi in una variabile 16

2.2.2 Risultante di polinomi in più variabili 19

2.3 Implicitizzazione 26

3 Teoria dell'eliminazione proiettiva **31**

3.1 Chiusura proiettiva 37

3.2 Morfismi tra varietà proiettive 39

4 Teorema di Bezout **45**

4.1 Forma debole del Teorema di Bezout 45

4.2 Teorema di Bezout 47

4.2.1 Molteplicità di intersezione 48

4.2.2 Teorema di Bezout 55

4.3 Generalizzazione del teorema di Bezout a varietà di $\mathbb{P}^n(\mathbb{C})$ . . 59

5 Un'applicazione dell'eliminazione proiettiva: la forma di Chow 63

Bibliografia 69

Capitolo 1

Cenni preliminari

In questo capitolo sono presentate alcune nozioni basilari per gli argomenti dei capitoli successivi.

1.1 Ideali radicali e Nullstellensatz

Il primo dei risultati su cui si basa questa tesi è il teorema degli zeri di Hilbert, o Nullstellensatz, che ci garantisce una corrispondenza biunivoca tra ideali radicali e varietà affini, se consideriamo campi algebricamente chiusi. Per enunciarlo, abbiamo bisogno di definire gli ideali radicali e due funzioni per legare varietà ed ideali.

Definizione 1.1. Sia $I \subset \mathbb{K}[x_1, ..., x_n]$ un ideale. Il radicale di I denotato $\sqrt{I}$, è l'insieme

$$\sqrt{I} = \{f : f^m \in I \text{ per un qualche intero } m \geq 1\}.$$

Si verifica facilmente che $\sqrt{I}$ è un ideale di $\mathbb{K}[x_1, .., x_n]$ e che $I \subseteq \sqrt{I}$.

Definizione 1.2. Sia $I \subset \mathbb{K}[x_1, ..., x_n]$ un ideale. Denoteremo con $V(I)$ l'insieme

$$V(I) = \{(a_1, ..., a_n) \in \mathbb{K}^n : f(a_1, ..., a_n) = 0 \text{ per ogni } f \in I\}.$$

Definizione 1.3. Sia $V \subset \mathbb{K}^n$ una varietà. Allora chiameremo ideale di definizione di V, l'ideale

$$I(V) = \{f \in \mathbb{K}[x_1, ..., x_n] : f(a_1, ..., a_n) = 0 \text{ per ogni } (a_1, ..., a_n) \in V\}.$$

Teorema 1.1.1 (Nullstellensatz Affine)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso. Se I è un ideale in $\mathbb{K}[x_1, ..., x_n]$, allora*

$$I(V(I)) = \sqrt{I}.$$

Definizione 1.4. Se $f \in \mathbb{K}[x_1, ..., x_n]$ è un polinomio, definiamo la riduzione di f, denotata f_{red}, come il polinomio tale che $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$. Un polinomio è detto ridotto se $f = f_{red}$.

Anche nel caso della geometria proiettiva si può ottenere una corrispondenza biunivoca tra varietà proiettive diverse dal vuoto e ideali radicali omogenei contenenti propriamente $\langle x_0, ..., x_n \rangle$.

Definizione 1.5. Sia $I \subset \mathbb{K}[x_0, ..., x_n]$ un ideale omogeneo. Denoteremo con $V(I)$ la varietà proiettiva:

$$V(I) = \{[a_0, ..., a_n] \in \mathbb{P}^n : f(a_0, ..., a_n) = 0 \text{ per ogni } f \in I\}.$$

Teorema 1.1.2 (Nullstellensatz Proiettivo Debole)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso ed I un ideale omogeneo in $\mathbb{K}[x_0, ..., x_n]$. Allora le seguenti affermazioni sono equivalenti:*

1. *$V(I) \subset \mathbb{P}^n(\mathbb{K})$ è vuoto;*
2. *Sia G una base di Groebner ridotta per I (rispetto ad un certo ordinamento monomiale). Allora per ogni $0 \leq i \leq n$, esiste $g \in G$ tale che $LT(g)$ sia una potenza non negativa di x_i;*
3. *Per ogni $0 \leq i \leq n$, esiste un intero $m_I \geq 0$ tale che $x_i^{m_i} \in I$;*
4. *Esiste un $r \geq 1$ tale che $\langle x_0, ..., x_n \rangle^r \subset I$.*

Teorema 1.1.3 (Nullstellensatz Proiettivo)**.** *Sia* $\mathbb{K}$ *un campo algebricamente chiuso e sia* I *un ideale omogeneo in* $\mathbb{K}[x_0, ..., x_n]$*. Se* $V = V(I)$ *è una varietà proiettiva diversa dal vuoto in* $\mathbb{P}^n(\mathbb{K})$*, allora abbiamo*

$$I(V(I)) = \sqrt{I}.$$

Un'altra interessante corrispondenza biunivoca che si può citare in questo contesto è quella tra ideali primi e varietà irriducibili.

1.2 Basi di Groebner

Ogni volta che in questa tesi parleremo di base per un ideale, intenderemo un tipo particolare di insieme di generatori: una base di Groebner. Questo tipo di insieme è privilegiato, perché, oltre a generare l'ideale, permette anche di definire univocamente il resto della divisione di un polinomio per l'ideale. Il più grosso vantaggio dato dall'utilizzo di queste basi è la possibilità di vedere immediatamente se un elemento appartiene o meno ad un ideale di cui si conosce una base di Groebner: basta dividerlo per un polinomio qualsiasi della base e poi dividere il resto per un altro polinomio e così via finché non si ottiene resto 0, e quindi il polinomio appartiene all'ideale, oppure finiscono i polinomi della base, e il polinomio non appartiene.

Definizione 1.6 (Ordinamento monomiale)**.** Un **ordinamento monomiale** su $\mathbb{K}_{>}[x_1, ..., x_n]$ è una qualunque relazione $>$ su $\mathbb{Z}^n_{\geq 0}$, o equivalentemente $\forall$ relazione sull'insieme dei monomi x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$ che soddisfi:

1. $>$ è un ordinamento totale in $\mathbb{Z}^n_{\geq 0}$;
2. Se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0} \Rightarrow \alpha + \gamma > \beta + \gamma$;
3. $>$ è un buon ordinamento in $\mathbb{Z}^n_{\geq 0}$, cioé qualsiasi sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$ ha un elemento minimo per $>$.

Definizione 1.7. Sia $I \subset \mathbb{K}[x_1, ..., x_n]$ un ideale $\neq \{0\}$.

1. Denotiamo con $LT(I)$ l'insieme dei termini principali degli elementi di I. Cioé $LT(I) = \{cx^\alpha : \exists f \in I \text{ con } LT(f) = cx^\alpha\}$;

2. Denotiamo con $\langle LT(I)\rangle$ l'ideale generato dagli elementi di $LT(I)$.

Definizione 1.8 (Base di Groebner)**.** Fissiamo un ordine monomiale. Un sottoinsieme finito $G = \{g_1, ..., g_t\}$ di un ideale I è detta **base di Groebner** se $\langle LT(g_1), ..., LT(g_t)\rangle = \langle LT(I)\rangle$.

Si verifica facilmente che se G è una base di Groebner di I allora G è un sistema di generatori per l'ideale. Si veda [1] cor 6 pag. 77.

1.2.1 Proprietà delle Basi di Groebner

Proposizione 1.2.1. *Sia $G = \{g_1, ..., g_t\}$ una base di Groebner per un ideale $I \subset \mathbb{K}[x_1, ..., x_n]$ e sia $f \in \mathbb{K}[x_1, ..., x_n]$. Allora esiste ed è unico $r \in \mathbb{K}[x_1, ..., x_n]$ con le seguenti proprietà:*

1. *Nessun termine di r è divisibile per alcuno dei $LT(g_1), ..., LT(g_t)$;*

2. *$\exists g \in I$ tale che $f = g + r$*

In particolare, r è il resto della divisione di f per G, in qualunque ordine vengano considerati gli elementi di G utilizzando l'algoritmo di divisione.

Definizione 1.9. Scriveremo $\bar{f}^F$ per indicare il resto della divisione di f per la s-upla ordinata $F = (f_1, ..., f_s)$. Se F è una base di Groebner per $\langle f_1, ..., f_s\rangle$, allora possiamo considerare F come un insieme, grazie alla proposizione precedente.

Vediamo ora un algoritmo per ottenere una base di Groebner a partire da un qualunque insieme di generatori.

Definizione 1.10. Siano $f, g \in \mathbb{K}[x_1, ..., x_n]$ polinomi $\neq 0$.

1. Se $multideg(f) = \alpha$ e $multideg(g) = \beta$, allora sia $\gamma = (\gamma_1, ..., \gamma_n)$, dove $\gamma_i = max(\alpha_i, \beta_i) \forall i$. Chiamiamo x^γ il minimo comune multiplo di $LM(f)$ e $LM(g)$ scritto $x^\gamma = mcm(LM(f), LM(g))$;

2. L'**s-polinomio** di f e g è la combinazione lineare

$$S(f,g) = \frac{x^\gamma}{LT(f)}\dot{f} - \frac{x^\gamma}{LT(g)} \cdot g.$$

Teorema 1.2.2 (Algoritmo di Buchberger)**.** *Sia $I = \langle f_1, ..., f_s \rangle \neq 0$ un ideale polinomiale. Allora una base di Groebner per I può essere costruita in un numero finito di passi con l'algoritmo seguente:*
input: $F = (f_1, ..., f_s)$
output: base di Groebner $G = (g_1, ..., g_s)$

$G = F$
`Do` $G' = G$
`For` *ogni coppia* $\{p,q\}, p \neq q$ *in* G' `Do` $S = S(\bar{p}, q)^{G'}$
`If` $S \neq 0$ `Then` $G = G \cup \{S\}$
`Until` $G = G'$

Definiamo ora la base di Groebener ridotta, questo particolare tipo di base di Groebner ci risulta molto utile perché ogni ideale ne ha solo una e quindi possiamo identificarlo univocamente utilizzando questo nuovo strumento.

Definizione 1.11 (Base di Groebner Ridotta)**.** Una base di Groebner ridotta per un ideale polinomiale I è una base di Groebner G per I tale che:

1. $LC(p) = 1 \ \forall p \in G$;
2. $\forall p \in G$ nessun monomio di $p \in \langle LT(G - \{p\}) \rangle$

Proposizione 1.2.3. *Sia $I \neq \{0\}$ un ideale polinomiale. Allora per un dato ordinamento monomiale, I ha un'unica base di Groebner ridotta.*

Per trasformare una base di Groebner nella base ridotta, utilizziamo questo lemma:

Lemma 1.2.4. *Sia G una base di Groebner per l'ideale polinomiale I. SIa $p \in G$ un polinomio tale che $LT(p) \in \langle LT(G - \{p\}) \rangle$. Allora anche $G - \{p\}$ è una base di Groebner per I.*

Questo ci permette di eliminare i polinomi con termini principali non appropriati, poi basta semplicemente sostituire i polinomi che creano problemi combinandoli linearmente con polinomi di grado più basso per far sparire i monomi in $\langle LT(G - \{p\})\rangle$.

1.3 Chiusura proiettiva di una varietà affine

Sappiamo che ogni varietà affine può essere vista come una parte di una varietà proiettiva identificando $\mathbb{K}^n$ con un aperto affine

$$U_i := \{[x_0, ..., x_n] \in \mathbb{P}^n(\mathbb{K}) \mid x_i \neq 0\}.$$

A meno che non sia diversamente indicato, useremo sempre l'aperto U_0.

In questa sezione ricordiamo velocemente come ciò sia possibile e come si possa passare dalla varietà affine a quella proiettiva che la contiene.

Dato che le varietà proiettive sono definite da polinomi omogenei, dovremo omogeneizzare quelli che ci definiscono la varietà affine che vogliamo estendere aggiungendo una variabile, in questo caso x_0.

Definizione-Proposizione 1. Sia $g(x_1, ..., x_n) \in \mathbb{K}[x_1, ..., x_n]$ un polinomio di grado totale d.

1. Sia $g = \sum_{i=0}^{d} g_i$ l'espressione di g come somma delle sue componenti omogenee dove g_i ha grado totale i. Allora

$$\begin{aligned} g^h(x_0, ..., x_n) &= \sum_{i=0}^{d} g_i(x_1, ..., x_n)x_0^{d-i} \\ &= g_d(x_1, ..., x_n) + g_{d-1}(x_1, ..., x_n)x_0 \quad +... + g_0(x_1, ..., x_n)x_0^d \end{aligned}$$

   è un polinomio omogeneo di grado totale d in $\mathbb{K}[x_0, ..., x_n]$. Chiameremo g^h l'omogeneizzazione di g.

2. L'omogeneizzazione di g può essere calcolata con la formula $g^h = x_0^d \cdot g\left(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right)$.

3. Deomogeneizzare g^h restituisce g. Cioè, $g^h(1, x_1, ..., x_n) = g(x_1, ..., x_n)$.

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

Definizione 1.12. Sia I un ideale in $\mathbb{K}[x_1, ..., x_n]$. Definiamo l'omogeneizzazione di I come l'ideale $I^h = \langle f^h : f \in I \rangle \subset \mathbb{K}[x_0, ..., x_n]$, dove f^h è l'omogeneizzazione di f.

Proposizione 1.3.1. *Qualsiasi ideale $I \subset \mathbb{K}[x_1, ..., x_n]$, l'omogeneizzazione I^h è un ideale omogeneo in $\mathbb{K}[x_0, ..., x_n]$.*

Vediamo quindi che le basi di Groebner continuano ad essere basi di Groebner anche dopo l'omogeneizzazione.

Teorema 1.3.2. *Sia I un ideale in $\mathbb{K}[x_1, ..., x_n]$ e sia $G = \{g_1, ..., g_t\}$ una base di Groebner per I rispetto ad un ordine monomiale graduato in $\mathbb{K}[x_1, ..., x_n]$. Allora $G^h = \{g_1^h, ..., g_t^h\}$ è una base per $I^h \subset \mathbb{K}[x_0, ..., x_n]$.*

Lemma 1.3.3. *Se $f \in \mathbb{K}[x_1, ..., x_n]$ e $>$ è un ordine graduato su $\mathbb{K}[x_1, ..., x_n]$, allora $LM_> \left(f^h\right) = LM_> (f)$.*

Possiamo ora definire la chiusura proiettiva di una varietà affine ed enunciare le sue proprietà.

Definizione 1.13. Data una varietà affine $W \subset \mathbb{K}^n$, la **chiusura proiettiva** di W è la varietà proiettiva $\bar{W} = V\left(I_a (W)^h\right) \subset \mathbb{P}^n(\mathbb{K})$, dove $I_a\left(W^h\right) \subset \mathbb{K}[x_0, ..., x_n]$ è l'omogeneizzazione dell'ideale $I_a(W) \subset \mathbb{K}[x_1, ..., x_n]$.

Proposizione 1.3.4. *Sia $W \subset \mathbb{K}^n$ una varietà affine e sia $\bar{W} \subset \mathbb{P}^n(\mathbb{K})$ la sua chiusura proiettiva. Allora:*

1. *$\bar{W} \cap U_0 = \bar{W} \cap \mathbb{K}^n = W$;*
2. *$\bar{W}$ è la più piccola varietà proiettiva in $\mathbb{P}^n(\mathbb{K})$ che contiene W;*
3. *Se W è irriducibile, allora lo è anche $\bar{W}$;*

4. *Non ci sono componenti irriducibili di* $\bar{W}$ *sull'iperpiano all'infinito* $V(x_0) \subset \mathbb{P}^n(\mathbb{K})$.

Teorema 1.3.5. *Sia* $\mathbb{K}$ *un campo algebricamente chiuso e sia* $I \subset \mathbb{K}[x_1, ..., x_n]$ *un ideale. Allora* $V\left(I^h\right) \subset \mathbb{P}^n(\mathbb{K})$ *è la chiusura proiettiva di* $V_a(I) \subset \mathbb{K}^n$.

Capitolo 2

Teoria dell'eliminazione affine

La teoria dell'eliminazione è stata studiata per risolvere sistemi di equazioni polinomiali in molte variabili e ha portato ad un metodo diviso in tre fasi: prima si riduce il numero di variabili del sistema mediante l'eliminazione, poi si cercano gli zeri dei polinomi ottenuti e quindi si cerca di estendere le soluzioni.

In questo capitolo considereremo sempre un campo $\mathbb{K}$ algebricamente chiuso, ma molte delle dimostrazioni verranno fatte nel caso $\mathbb{K} = \mathbb{C}$.

Definizione 2.1. Dato $I = \langle f_1, ..., f_s \rangle \subset \mathbb{K}[x_1, ..., x_n]$ l'**l-esimo ideale eliminazione** I_l è l'ideale di $\mathbb{K}[x_{l+1}, ..., x_n]$ definito da

$$I_l = I \cap \mathbb{K}[x_{l+1}, ..., x_n].$$

Per trovare gli elementi di I_l sfruttiamo il seguente teorema, che ci permette di trovare in modo semplice una base di Groebner per l'ideale eliminazione a partire da una base dell'ideale di partenza.

Teorema 2.0.6 (Teorema di eliminazione)**.** *Sia $I \subset \mathbb{K}[x_1, ..., x_n]$ un ideale e sia G una base di Groebner di I rispetto all'ordine lessicografico, dove $x_1 > \ldots > x_n$. Allora $\forall\ 0 \leq l \leq n$, l'insieme $G_l = G \cap \mathbb{K}[x_{l+1}, ..., x_n]$ è una base di Groebner per l'l-esimo ideale eliminazione I_l.*

Dimostrazione. Fissiamo l tra 0 ed n. Dato che $G_l \subset I_l$ per costruzione, è sufficiente mostrare che

$$\langle LT(I_l)\rangle = \langle LT(G_l)\rangle$$

utilizzando la definizione di base di Groebner. Una inclusione è ovvia, e per provare l'altra: $\langle LT(I_l)\rangle \subset \langle LT(G_l)\rangle$, abbiamo bisogno solo di mostrare che il termine principale $LT(f)$ per una qualsiasi $f \in I_l$ è divisibile per $LT(g)$ per un certo $g \in G_l$.
Per dimostrare questo, notiamo che f è in I, cioé $LT(f)$ è divisibile per $LT(g)$ per un certo $g \in G$ dato che G è una base di Groebner di I. Dato che $f \in I_l$, questo vuol dire che $LT(g)$ coinvolge solo le variabili $x_{l+1}, ..., x_n$. Quindi, dato che stiamo considerando un ordine lessicografico, dove $x_1 > ... > x_n$, qualunque monomio che contenga $x_1, ..., x_l$ è più grande di tutti i monomi in $\mathbb{K}[x_{l+1}, ..., x_n]$, così che $LT(g) \in \mathbb{K}[x_{l+1}, ..., x_n]$ implica che $g \in \mathbb{K}[x_{l+1}, ..., x_n]$. Questo mostra che $g \in G_l$ e il teorema è dimostrato. □

Consideriamo ora il caso in cui venga eliminata solo la prima variabile: una volta che abbiamo completato il passaggio dell'eliminazione e determinato le soluzioni parziali, il teorema di estensione ci dice quali di queste si estenderanno a soluzioni sullo spazio di partenza.

Teorema 2.0.7 (Teorema di estensione)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso. Sia $I = \langle f_1, ..., f_s\rangle \subset \mathbb{K}[x_1, ..., x_n]$ e sia I_1 il primo ideale eliminazione di I. $\forall\ 1 \leq i \leq s$, scriviamo f_i nella forma*

$$f_i = g_i(x_2, ..., x_n)x_1^{N_i} + \text{ termini in cui } x_1 \text{ ha grado minore di } N_i,$$

dove $N_i \geq 0$ e $g_i \in \mathbb{K}[x_2, ..., x_n]$ è $\neq 0$. Supponiamo di avere una soluzione parziale $(a_2, ..., a_n) \in V(I_1)$. Se $(a_2, ..., a_n) \notin V(g_1, ..., g_s)$ allora $\exists\ a_1 \in \mathbb{K}$ tale che $(a_1, a_2, ..., a_n) \in V(I)$.

Rimandiamo la dimostrazione di questo teorema a quando avremo definito il polinomio risultante.

Nel caso i coefficienti direttori delle f_i siano costanti, quindi diversi da zero su tutto $\mathbb{K}^{n-1}$, allora possiamo sfruttare questo corollario.

Corollario 2.0.8. *Sia $I = \langle f_1, ..., f_s \rangle \subset \mathbb{K}[x_1, ..., x_n]$ con $\mathbb{K}$ campo algebricamente chiuso, e poniamo che per un qualche i, f_i sia della forma $f_i = cx_i^N +$ termini in cui x_1 ha grado minore di N, dove $c \in \mathbb{K}$ e diverso da 0 ed $N > 0$. Se I_1 è il primo ideale eliminazione di I e $(a_2, ..., a_n) \in V(I_1)$ allora $\exists\, a_1 \in \mathbb{K}$ tale che $(a_1, a_2, ..., a_n) \in V(I)$.*

2.1 Interpretazione dal punto di vista geometrico

Notazione 1. Sia $\mathbb{K}$ un campo algebricamente chiuso. Denoteremo con π_l la mappa di proiezione sulle ultime $n - l$ coordinate

$$\begin{array}{rccc} \pi_l : & \mathbb{K}^n & \to & \mathbb{K}^{n-l} \\ & (a_1, ..., a_n) & \to & (a_{l+1}, ..., a_n) \end{array}$$

Geometricamente, il procedimento dell'eliminazione corrisponde alla proiezione di una varietà su uno spazio di dimensione minore mediante una mappa π_l. Gli zeri dell'ideale eliminazione però identificheranno una varietà che contiene la proiezione della varietà di partenza, dato che la proiezione di una varietà affine non è necessariamente una varietà affine. In particolare, il teorema di chiusura ci dirà che $V(I_l)$ è la più piccola varietà affine che contiene la proiezione mediante π_l della varietà iniziale.

Lemma 2.1.1. *Sia $I_l = \langle f_1, ..., f_s \rangle \cap \mathbb{K}[x_{l+1}, ..., x_n]$ l'l-esimo ideale eliminazione. Allora in $\mathbb{K}^{n-l}$ abbiamo*

$$\pi_l(V) \subset V(I_l).$$

Dimostrazione. Fissiamo un polinomio $f \in I_l$. Se $(a_1, ..., a_n) \in V$, allora f si annulla su $(a_1, ..., a_n)$ dato che $f \in \langle f_1, ..., f_s \rangle$. Ma f contiene solo le variabili $x_{l+1}, ..., x_n$, quindi possiamo scrivere

$$f(a_{l+1}, ..., a_n) = f(\pi_l(a_1, ..., a_n)) = 0$$

Questo mostra che f si annulla su tutti i punti di $\pi_l(V)$. □

Teorema 2.1.2. *Data $V = V(f_1, ..., f_s) \subset \mathbb{K}^n$ con $\mathbb{K}$ campo algebricamente chiuso, sia g_i come nel teorema di estensione. Se I_1 è il primo ideale eliminazione di $\langle f_1, ..., f_s \rangle$, allora abbiamo l'equivalenza in $\mathbb{K}^{n-1}$*

$$V(I_1) = \pi_1(V) \cup (V(\, g_1, .., g_s\,) \cap V\,(I_1))$$

dove $\pi_1 : \mathbb{K}^n \to \mathbb{K}^{n-1}$ è la mappa di proiezione sulle ultime $n-1$ coordinate.

Sappiamo quindi che i punti da eliminare da $V(I_l)$ per ottenere $\pi_l(V)$ sono da cercare all'interno di $V(g_1, ..., g_s)$.

Teorema 2.1.3 (Teorema di chiusura)**.** *Sia $V = V(f_1, ..., f_s) \subset \mathbb{K}^n$ con $\mathbb{K}$ campo algebricamente chiuso, e sia I_l l'$l-$esimo ideale eliminazione di $\langle f_1, ..., f_s \rangle$. Allora:*

1. *$V(I_l)$ è la più piccola varietà affine che contiene $\pi_l(V) \subset \mathbb{K}^{n-l}$;*
2. *Se V non è un punto, allora esiste una varietà affine $W \subsetneq V\,(I_l)$ tale che $V\,(I_l) \setminus W \subset \pi_l(V)$.*

Osservazione 1. Il primo punto del teorema di chiusura equivale a dire che

1. $\pi_l(V) \subset V(I_l)$;
2. se Z è una qualsiasi altra varietà affine di $\mathbb{K}^{n-1}$ che contiene $\pi_l(V)$, allora $V(I_l) \subset Z$.

Lo stesso concetto si può esprimere affermando che $V(I_l)$ è la chiusura di Zariski di $\pi_l(V)$, quindi ci basta dimostrare questo.

Dimostrazione.

1

Dobbiamo mostrare che $V(I_l) = V(I(\pi_l(V)))$. Sappiamo già che $\pi_l(V) \subset V(I_l)$. Dato che $V(I(\pi_l(V)))$ è la più piccola varietà che contiene $\pi_l(V)$, segue direttamente che $V(I(\pi_l(V))) \subset V(I_l)$.

Per ottenere l'inclusione inversa, supponiamo che $f \in I(\pi_l(V))$. Allora considerandola come un elemento di $\mathbb{K}[x_1, ..., x_n]$, avremo $f(a_1, ..., a_n) = 0$ per tutti gli $(a_1, ..., a_n) \in V$. Per il Nullstellensatz, $f^N \in \langle f_1, ..., f_s \rangle$ per un qualche intero N. Dato che f non contiene nessuno degli $x_1, ..., x_l$, non saranno presenti neanche in f^N, e avremo $f^N \in \langle f_1, ..., f_s \rangle \cap \mathbb{K}[x_{l+1}, ..., x_n] = I_l$. Cioé $f \in \sqrt{I_l}$, che implica $I(\pi_l(V)) \subset \sqrt{I_l}$. Segue che $V(I_l) = V(\sqrt{I_l}) \subset V(I(\pi_l(V)))$ e il primo punto del teorema è provato.

2

Dimostreremo la seconda parte solo per il caso $l = 1$, per la dimostrazione completa rimandiamo a [1].
Lo strumento principale che useremo è la scomposizione

$$V(I_1) = \pi_1(V) \cup (V(g_1, ..., g_s) \cap V(I_1))$$

dal teorema di estensione. Sia $W = V(g_1, ..., g_s) \cap V(I_1)$ e notiamo che W è una varietà affine. La scomposizione precedente implica che $V(I_1) - W \subset \pi_1(V)$, e quindi abbiamo raggiunto il risultato se $W \neq V(I_1)$. Però può succedere che W coincida con $V(I_1)$.
In questo caso dobbiamo modificare le equazioni che definiscono V in modo che W diventi più piccolo. L'osservazione chiave è che

$$\text{se } W = V(I_1), \text{ allora } V = V(f_1, ..., f_s, g_1, ..., g_s). \tag{2.1}$$

Questo viene dimostrato nel modo seguente. Prima di tutto, dato che stiamo aggiungendo nuove equazioni, è ovvio che $V(f_1, ..., f_s, g_1, ..., g_s) \subset V(f_1, ..., f_s) = V$. Per l'inclusione opposta, sia $(a_1, ..., a_n) \in V$. Di sicuro ogni f_i si annulla in questo punto, e dato che $(a_2, ..., a_n) \in \pi_1(V) \subset V(I_1) = W$, segue che i g_i si annullano quì. Quindi $(a_1, ..., a_n) \in V(f_1, ..., f_s, g_1, ..., g_s)$ e abbiamo provato 2.1.
Sia $I = \langle f_1, ..., f_s \rangle$ il nostro ideale iniziale e sia $\tilde{I}$ l'ideale $\langle (f_1, ..., f_s, g_1, ..., g_s) \rangle$. Notiamo che I e $\tilde{I}$ possono essere diversi, anche se definiscono la stessa varietà V. Quindi i corrispondenti ideali eliminazione I_1 ed $\tilde{I}_1$ possono essere

diversi. Comunque, dato che $V(I_1)$ e $V(\tilde{I}_1)$ sono entrambe la più piccola varietà che contiene $\pi_1(V)$ (come prova la prima parte del teorema), segue che $V(I_1) = V(\tilde{I}_1)$.
Il passaggio seguente consiste nel trovare una base migliore per $\tilde{I}$. Prima di tutto ricordiamo che i g_i sono definiti dalla scrittura:

$$f_i = g_i(x_2, ..., x_n)x_1^{N_i} + \text{ termini in cui } x_1 \text{ ha grado minore di } N_i,$$

dove $N_i \geq 0$ e $g_i \in \mathbb{K}[x_2, ..., x_n]$ è diverso da 0. Consideriamo ora

$$\tilde{f}_i = f_i - g_i x_1^{N_i}.$$

Per ogni i, notiamo che $\tilde{f}_i$ o è nulla o ha grado strettamente minore in x_1 di f_i. Avremo inoltre che

$$\tilde{I} = \left\langle \tilde{f}_1, ..., \tilde{f}_s, g_1, ..., g_s \right\rangle.$$

Ora applicando il teorema di estensione a $V = V(\tilde{f}_1, ..., \tilde{f}_s, g_1, ..., g_s)$. Notiamo che i coefficienti direttori dei generatori sono diversi, così otteniamo una diversa scomposizione

$$V(I_1) = V(\tilde{I}_1) = \pi_1(V) \cup \tilde{W}$$

dove $\tilde{W}$ è costituita da quelle soluzioni parziali sulle quali si annullano i coefficienti direttori di $\tilde{f}_1, ..., \tilde{f}_s, g_1, ..., g_s$. Mediante questo procedimento possiamo ottenere una $\tilde{W}$ che sia più piccola di $W = V(I_1)$, ma nel caso generale non c'è niente che ci garantisce questo risultato, quindi può ancora succedere che W coincida con $V(I_1)$. Se è questo il caso, si ripete il procedimento precedente e se in un passaggio successivo otteniamo qualcosa strettamente contenuto in $V(I_1)$ allora abbiamo concluso il procedimento.
Resta da considerare il caso in cui otteniamo sempre $V(I_1)$. Ogni volta che eseguiamo questo procedimento, i gradi in x_1 dei generatori diminuiscono (o restano 0), così che ad un certo punto tutti i generatori avranno grado 0 in x_1. Questo vuol dire che V può essere definito dall'annullarsi di polinomi in $\mathbb{K}[x_2, ..., x_n]$. Cioé se $(a_2, ..., a_n)$ è una soluzione parziale, segue che

$(a_1, ..., a_n) \in V$ per qualunque $a_1 \in \mathbb{C}$ dato che x_1 non appare nelle equazioni che definiscono la varietà. Quindi qualsiasi soluzione parziale si estende e questo prova che $\pi_1(V) = V(I_1)$. In questo caso, vediamo che la seconda parte del teorema è soddisfatta quando $W = \emptyset$ ($V \neq \emptyset$). E quindi il teorema è dimostrato. □

Corollario 2.1.4. *Sia $V = V(f_1, ..., f_s) \subset \mathbb{K}^n$ con $\mathbb{K}$ campo algebricamente chiuso, e assumiamo che per un qualche i, f_i sia della forma $f_i = cx_1^N +$ termini in cui x_1 ha grado minore di N, dove $c \in \mathbb{C} - \{0\}$ ed $N > 0$. Se I_1 è il primo ideale eliminazione, allora in $\mathbb{K}^{n-1}$: $\pi_1(V) = V(I_1)$, dove π_1 è la mappa di proiezione sulle ultime $n-1$ componenti.*

Questo succede perché i g_i non possono mai essere uguali a 0, dato che sono costanti. In questo modo abbiamo dato una versione geometrica del corollario del teorema di estensione.

2.2 Risultante

In questo paragrafo parleremo del polinomio risultante, che fornirà una condizione necessaria e sufficiente affinché due polinomi dati abbiamo fattori comuni.

In questa sezione, $\mathbb{K}$ denoterà sempre un campo

Lemma 2.2.1. *Siano $f, g \in \mathbb{K}[x]$ polinomi di gradi $l > 0$ ed $m > 0$ rispettivamente. Allora f e g hanno un fattore comune di grado positivo in $x]$ se e solo se esistono polinomi $A, B \in \mathbb{K}[x]$ tali che:*

- *A e B non sono entrambi nulli;*
- *il grado di A è al più $m-1$ e quello di B è al più $l-1$;*
- *$Af + Bg = 0$.*

2.2.1 Risultante di polinomi in una variabile

Definizione 2.2. Dati i polinomi $f, g \in \mathbb{K}[x]$ di grado positivo, scritti nella forma:
$f = a_0x^l + ... + a_l$ $\deg f = l,\ a_0 \neq 0$
$g = b_0x^m + ... + b_m$ $\deg g = m,\ b_0 \neq 0$
Allora il polinomio risultante di f e g rispetto a x, denotato $Res(f, g, x)$ è il determinante della matrice:

$$Res(f,g,x) = det \begin{pmatrix} a_0 & 0 & 0 & b_0 & 0 & 0 \\ \vdots & \ddots & 0 & \vdots & \ddots & 0 \\ a_l & & a_0 & b_m & & b_0 \\ 0 & \ddots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & a_l & 0 & 0 & b_m \end{pmatrix}$$

Vediamo che, mentre le colonne sono formate dai coefficienti dei due polinomi, le righe permettono di controllare velocemente quali coefficienti bisogna combinare linearmente per ottenere quelli di $Af + Bg$. Notiamo inoltre che questi sono $l + m$, quindi rientriamo ancora nelle condizioni date dal lemma. Quindi se riusciamo ad annullare tutti i coefficienti del polinomio $Af + Bg$, abbiamo trovato che f e g hanno un fattore in comune.

Proposizione 2.2.2. *Dati $f, g \in \mathbb{K}[x]$ di grado positivo, il polinomio risultante, $Res(f, g, x) \in \mathbb{K}$ è un polinomio intero nei coefficienti di f e g. Inoltre, f e g hanno un fattore comune in $\mathbb{K}[x]$ se e solo se $Res(f, g, x) = 0$.*

Dimostrazione. La formula standard per il determinante di una matrice $s \times s$ $A = (a_{ij})_{1 \leq i,j \leq s}$ è

$$\det(A) = \sum_{\sigma\ permutazione\ di\ [1,...,s]} \operatorname{sgn}(\sigma) a_{1\sigma 1} \cdot ... \cdot a_{s\sigma(s)},$$

dove $\operatorname{sgn}(\sigma)$ è $+1$ se σ scambia un numero pari di coppie di elementi di $\{1, ..., s\}$ e -1 se σ scambia un numero dispari di coppie. Questo mostra che il determinante è un polinomio intero (tutti i coefficienti sono ± 1) sui suoi

valori, e quind la prima affermazione segue immediatamente dalla definizione di risultante. La seconda affermazione viene provata invece in questo modo: il risultante è nullo $\Leftrightarrow$ la matrice del sistema di equazioni che si ottiene annullando tutti i coefficienti di $Af + Bg$ ha determinante nullo $\Leftrightarrow$ quel sistema di equazioni ha una soluzione non nulla. Abbiamo già visto che questo equivale all'esistenza di A e B come in 2.2.1, e quindi utilizziamo questo per completare la dimostrazione. □

Proposizione 2.2.3. *Dati $f, g \in \mathbb{K}[x]$ di grado positivo, esistono polinomi $A, B \in \mathbb{K}[x]$ tali che $Af + Bg = Res(f, g, x)$. Inoltre i coefficienti di A e B sono polinomi interi nei coefficienti di f e g.*

Dimostrazione. La definizione di risultante è stata basata sull'equazione $Af + Bg = 0$. In questa dimostrazione, applicheremo lo stesso metodo all'equazione

$$\tilde{A}f + \tilde{B}g = 1. \tag{2.2}$$

La proposizione è verificata in modo banale se $Res(f, g, x) = 0$, quindi possiamo imporre $Res(f, g, x) \neq 0$. Ora siano

$$f = a_0x^l + ...a_l, \quad a_0 \neq 0,$$

$$g = b_0x^m + ... + b_m, \quad b_0 \neq 0,$$

$$\tilde{A} = c_0x^{m-1} + ... + c_{m-1},$$

$$\tilde{B} = d_0x^{l-1} + ... + d_{l-1},$$

dove i coefficienti $c_0, ..., c_{m-1}, d_0, ..., d_{l-1}$ non sono noti. Se sostituiamo queste formule in 2.2 e confrontiamo i coefficienti delle potenze di x, otteniamo il seguente sistema di equazioni lineari con incognite c_i, d_i e coefficienti a_i, b_i in $\mathbb{K}$:

$$\begin{array}{ccccc}
a_0c_0 & + & b_0d_0 & = 0, \text{ coefficiente di } x^{l+m-1} \\
a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & = 0, \text{ coefficiente di } x^{l+m-2} \\
\vdots & & \vdots & \vdots \\
a_lc_{m-l} & + & b_md_{m-l} & = 1, \text{ coefficiente di } x^0.
\end{array}$$

La matrice dei coefficienti è la matrice di Sylvester di f e g, e quindi $Res(f,g,x) \neq 0$ ci garantisce che 2.2.1 avrà un'unica soluzione in $\mathbb{K}$. In questa situazione, possiamo usare la regola di Cramer per dare una formula per la soluzione unica. Troveremo l'i-esima incognita mediante una frazione dove il denominatore è il determinante della matrice dei coefficienti e il numeratore è il determinante della matrice in cui l'i-esima colonna della matrice dei coefficienti è stata sostituita dalla colonna dei termini noti. Per esempio la prima incognita c_0 è data da:

$$c_0 = \frac{1}{Res(f,g,x)} \det \begin{pmatrix} 0 & a_0 & 0 & 0 & b_0 & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots & \ddots & 0 \\ 0 & a_l & & a_0 & b_m & & b_0 \\ \vdots & 0 & \ddots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & a_l & 0 & 0 & b_m \\ 1 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$$

Dato che un determinante è un polinomio intero rispetto ai valori della matrice, segue che

$$c_0 = \frac{\text{polinomio intero nei coefficienti } a_i, b_i}{Res(f,g,x)}.$$

Ci sono formule simili per gli altri c_i e d_i. Dato che $\tilde{A} = c_0 x^{m-1} + ... + c_{m-1}$, possiamo eliminare il denominatore comune $Res(f,g,x)$ e scrivere $\tilde{A}$ nella forma

$$\tilde{A} = \frac{1}{Res(f,g,x)} A,$$

dove $A \in \mathbb{K}[x]$ e i coefficienti di A sono polinomi interi nelle a_i, b_i. Possiamo scrivere

$$\tilde{B} = \frac{1}{Res(f,g,x)} B,$$

dove $B \in \mathbb{K}[x]$ ha le stesse proprietà di A. Dato che $\tilde{A}$ e $\tilde{B}$ soddisfano l'equazione $\tilde{A}f + \tilde{B}g = 1$, possiamo moltiplicare a destra e sinistra per $Res(f,g,x)$ per ottenere

$$Af + Bg = Res(f,g,x).$$

Dato che A e B hanno i coefficienti richiesti, la proposizione è dimostrata. □

2.2.2 Risultante di polinomi in più variabili

La stesso ragionamento fatto per i polinomi in una sola variabile si può ripetere per $f, g \in \mathbb{K}[x_1, ..., x_n]$, $f = a_0 x_1^l + ... + a_l$, $g = b_0 x_1^m + ... + b_m$ con la sola differenza che i coefficienti $a_0, ..., a_l, b_0, ..., b_m$ saranno elementi di $\mathbb{K}[x_2, ..., x_n]$. Denoteremo il risultante ottenuto mettendo in evidenza la variabile raccolta come $Res(f, g, x_1)$.

Per provare i teoremi in più variabili abbiamo bisogno di ricordare qualche risultato sui polinomi in $\mathbb{K}[x_1, ..., x_n]$.

Teorema 2.2.4. *Sia $f \in \mathbb{K}[x_1, ..., x_n]$ irriducibile su $\mathbb{K}$ e supponiamo che f divida il prodotto $g \cdot h$, dove g, $h \in \mathbb{K}[x_1, ..., x_n]$. Allora f divide g oppure f divide h.*

Dimostrazione. Faremo questa dimostrazione per induzione sul numero delle variabili. Quando $n = 1$ possiamo usare il massimo comun divisore. Se $f | g \cdot h$, allora consideriamo $p =$MCD(f, g). Se p è non costante, allora f deve essere un multiplo costante di p dato che f è irriducibile, e segue che f divide g. Altrimenti, se p è costante, possiamo considerare $p = 1$, e poi possiamo trovare A, $B \in \mathbb{K}[x_1]$ tali che $Af + Bg = 1$. Se moltiplichiamo questo per h otteniamo

$$h = h(Af + Bg) = Ahf + Bgh.$$

Dato che f divide gh, f è un fattore di $Ahf + Bgh$, e quindi f divide h. Questo dimostra il caso in cui $n = 1$.

Ora consideriamo il teorema valido per $n - 1$. Vediamo prima il caso in cui il polinomio irriducibile non contiene x_1:

$$u \in \mathbb{K}[x_2, ..., x_n] \text{ è irriducibile }, u \text{ divide } g \cdot h \in \mathbb{K}[x_1, ..., x_n] \Rightarrow u \text{ divide } g \text{ o } h. \tag{2.3}$$

Per provare questo, scriviamo $g = \sum_{i=0}^{l} a_i x_1^i$ ed $h = \sum_{i=0}^{m} b_i x_1^i$, dove $a_i, b_i \in \mathbb{K}[x_2, ..., x_n]$. Se u divide ogni a_i, allora u divide g, e lo stesso vale per i b_i ed h. Quindi, se u non divide nessuno dei due, possiamo trovare $i, j \geq 0$ tali che u non divida né a_i né b_j. Prendiamo gli i e j più piccoli con questa proprietà. Quindi consideriamo

$$c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + ... + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + ... + a_{i+j} b_0).$$

Dato il modo in cui abbiamo scelto i, u divide ciascun termine nelle prime parentesi, e data la scelta di j, lo stesso vale per le ultime. Ma u non divide né a_i né b_j, e dato che u è irriducibile, la nostra ipotesi induttiva implica che u non divida $a_i b_j$. Dato che u divide tutti gli altri termini di c_{i+j}, non può dividere c_{i+j}. c_{i+j} è il coefficiente di x_1^{i+j} in gh, e quindi u non può dividere gh. Questa contraddizione dimostra 2.3.

Ora, dato 2.3, possiamo considerare il caso generale. Supponiamo che f divida gh. Se f non contiene x_1, allora 2.3 ci da il risultato, quindi consideriamo f di grado positivo in x_1. Useremo l'anello $\mathbb{K}(x_2, ..., x_n)[x_1]$, per poi passare all'anello più piccolo, $\mathbb{K}[x_1, ..., x_n]$.

Affermiamo che f è irriducibile anche come elemento di $\mathbb{K}(x_2, ..., x_n)[x_1]$. Per vedere perché, supponiamo di avere una fattorizzazione di f nell'anello più grande, $f = AB$. Qui, A e B sono polinomi in x_1 con coefficienti in $\mathbb{K}[x_2, ..., x_n]$. Per provare che f è irriducibile qui, dobbiamo mostrare che o A o B ha grado 0 in x_1. Sia $d \in \mathbb{K}[x_2, ..., x_n]$ il prodotto di tutti i denominatori in A e B. Allora $\tilde{A} = dA$ e $\tilde{B} = dB$ sono in $\mathbb{K}[x_1, ..., x_n]$, e

$$d^2 f = \tilde{A}\tilde{B} \tag{2.4}$$

in $\mathbb{K}[x_1, ..., x_n]$. Possiamo scrivere d^2 come prodotto di fattori irriducibili in $\mathbb{K}[x_2, ..., x_n]$ e per 2.3, ognuno di questi divide $\tilde{A}$ o $\tilde{B}$. Possiamo cancellare questo fattore da entrambi i membri di 2.4 e dopo averli cancellati, restiamo con

$$f = \tilde{A}_1 \tilde{B}_1 \tag{2.5}$$

in $\mathbb{K}[x_1, ..., x_n]$. Dato che f è irriducibile in $\mathbb{K}[x_1, ..., x_n]$, questo implica che o $\tilde{A}_1$ o $\tilde{B}_1$ sia costante. Ora, questi polinomi sono stati ottenuti dagli originali A, B moltiplicando e dividendo per vari elementi di $\mathbb{K}[x_2, ..., x_n]$. Questo mostra che né A né B contengono x_1. Ora che f è irriducibile in $\mathbb{K}(x_2, ..., x_n)[x_1]$, sappiamo dal caso $n = 1$ che f divide o g o h in $\mathbb{K}(x_2, ..., x_n)[x_1]$.

Consideriamo $g = Af$ per un certo $A \in \mathbb{K}(x_2, ..., x_n)[x_1]$. Se cancelliamo i denominatori, possiamo scrivere

$$dg = \tilde{A}f \tag{2.6}$$

in $\mathbb{K}[x_1, ..., x_n]$, dove $d \in \mathbb{K}[x_1, ..., x_n]$. Per 2.3, ogni fattore irriducibile di d divide $\tilde{A}$ o f. La seconda è impossibile dato che f è irriducibile e ha grado positivo in x_1. Ma ogni volta che un fattore irriducibile divide $\tilde{A}$, possiamo cancellarlo da entrambe le parti di 2.6. Quando abbiamo finito questo procedimento, vediamo che f divide g in $\mathbb{K}[x_1, ..., x_n]$. □

Il seguente corollario è l'analogo del lemma di Gauss[1]: entrambi ci assicurano che, se possiamo fattorizzare un polinomio su un campo che è campo dei quozienti del dominio su cui sono definiti i coefficienti del polinomio, allora lo possiamo fattorizzare anche sul dominio di partenza.

Corollario 2.2.5. *Supponiamo che $f, g \in \mathbb{K}[x_1, ..., x_n]$ abbiano grado positivo in x_1. Allora f e g hanno un fattore comune in $\mathbb{K}[x_1, ..., x_n]$ di grado positivo in x_1 se e solo se hanno un fattore comune in $\mathbb{K}(x_2, ..., x_n)[x_1]$.*

Dimostrazione. Se f e g hanno un fattore comune h in $\mathbb{K}[x_1, ..., x_n]$ di grado positivo in x_1, allora hanno certamente un fattore comune nell'anello $\mathbb{K}(x_2, ..., x_n)[x_1]$.

Per l'implicazione inversa, supponiamo che f e g abbiano un fattore comune $h \in \mathbb{K}(x_2, ..., x_n)[x_1]$. Allora

$$f = \tilde{h}\tilde{f}_1, \ \tilde{f}_1 \in \mathbb{K}(x_2, ..., x_n)[x_1].$$

$$g = \tilde{h}\tilde{g}_1, \ \tilde{g}_1 \in \mathbb{K}(x_2, ..., x_n)[x_1].$$

Ora, $\tilde{h}$, $\tilde{f}_1$ e $\tilde{g}_1$ possono avere denominatori che sono polinomi in $\mathbb{K}[x_2, ..., x_n]$. Chiamiamo $d \in \mathbb{K}[x_2, ..., x_n]$ il denominatore comune di questi polinomi, otteniamo $h = d\tilde{h}$, $f_1 = d\tilde{f}_1$ e $g_1 = d\tilde{g}_1$ in $\mathbb{K}[x_1, ..., x_n]$. Se moltiplichiamo ciascun membro delle equazioni precedenti per d^2, otteniamo

$$d^2 f = h f_1$$

[1] se un polinomio primitivo f si fattorizza su $\mathbb{Q}$, allora si fattorizza anche su $\mathbb{Z}$

$$d^2 g = h g_1$$

in $\mathbb{K}[x_1, ..., x_n]$. Ora sia h_1 un fattore irriducibile di h di grado positivo in x_1. Dato che $\tilde{h} = h/d$ ha grado positivo in x_1, un tale h_1 deve esistere. Allora h_1 divide $d^2 f$, cioé divide d^2 o f per il teorema precedente. La prima possibilità non può verificarsi perché $d^2 \in \mathbb{K}[x_2, ..., x_n]$, quindi h_1 deve dividere f in $\mathbb{K}[x_1, ..., x_n]$. Analogamente si vede che h_1 divide g, e quindi h_1 è il fattore comune ricercato, completando la dimostrazione del corollario. □

Teorema 2.2.6. *Ogni $f \in \mathbb{K}[x_1, ..., x_n]$ non costante può essere scritto come un prodotto $f = f_1 \cdot ... \cdot f_r$ di polinomi irriducibili in $\mathbb{K}$. Inoltre, se $f = g_1 \cdot ... \cdot g_s$ è un'altra fattorizzazione in irriducibili in $\mathbb{K}$, allora $r = s$ e i g_i possono essere permutati in modo che ciascun f_i sia un multiplo constante di g_i.*

Lemma 2.2.7. *Sia $f \in \mathbb{K}[x_1, ..., x_n]$ un polinomio irriducibile che divide il prodotto $h_1 \cdot ... \cdot h_s$, allora f divide h_i per un certo i.*

Dimostrazione. Dimostriamo questo lemma per induzione sul numero dei polinomi irriducibili:

Per $s = 1$, abbiamo che f divide h_1, quindi il primo passo è provato.

Se il lemma vale per $s = n-1$ allora consideriamo f che divide il prodotto $h_1 \cdot ... \cdot h_{n-1} \cdot h_n$, allora 2.2.4 mi dice che f dividerà o h_n o $h_1 \cdot ... \cdot h_{n-1}$. Nel primo caso il lemma è provato, nel secondo ritorniamo ad avere $s = n - 1$ concludendo la dimostrazione. □

Dimostrazione di 2.2.6. Sappiamo che esiste almeno una fattorizzazione, per provare l'unicità consideriamo

$$f = f_1 \cdot ... \cdot f_r = g_1 \cdot ... \cdot g_s$$

con f_i e g_j irriducibili. Abbiamo che f_1 divide il prodotto $g_1 \cdot ... \cdot g_s$, quindi grazie al lemma 2.2.7 sappiamo che per un certo j, f_1 divide g_j. Ma g_j è irriducibile, quindi sarà per forza $f_1 = a_j g_j$ con $a_j \in \mathbb{K}$ e possiamo dividere per f_1 entrambe le fattorizzazioni di f.

Procediamo ora per induzione sul grado di f:

Per $\deg(f) = 1$ abbiamo che $f = f_1 = g_1$ e quindi abbiamo provato il primo passo.

Se il teorema vale per $\deg(f) = d - 1$ allora consideriamo che dividendo $f_1 \cdot ... \cdot f_r$ e $g_1 \cdot ... \cdot g_s$ per f_1 avremo abbassato il grado almeno a $d-1$, ottenendo quindi una fattorizzazione unica in irriducibili a cui bisogna aggiungere f_1 o equivalentemente g_j per riottenere f. □

Proposizione 2.2.8. *Dati $f, g \in \mathbb{K}[x_1, ..., x_n]$ di grado positivo in x_1. Allora:*

- *$Res(f, g, x_1)$ è nel primo ideale eliminazione $\langle f, g\rangle \cap \mathbb{K}[x_2, ..., x_n]$;*
- *$Res(f, g, x_1) = 0$ se e solo se f e g hanno un fattore comune in $\mathbb{K}[x_1, ..., x_n]$ che abbia grado positivo in x_1.*

Dimostrazione. Come abbiamo già detto, se scriviamo f e g raccogliendo x_1, i coefficienti a_i, b_j sono in $\mathbb{K}[x_2, ..., x_n]$. Dato che il risultante è un polinomio intero in a_i, b_j (2.2.3), segue che $Res(f, g, x_1) \in \mathbb{K}[x_2, ..., x_n]$. Sappiamo anche che

$$Af + Bg = Res(f, g, x_1)$$

dove A e B sono polinomi in x_1 i cui coefficienti sono di nuovo polinomi interi in a_i, b_j per definizione. Quindi $A, B \in \mathbb{K}[x_2, ..., x_n][x_1] = \mathbb{K}[x_1, ..., x_n]$, e allora l'equazione precedente implica che $Res(f, g, x_1) \in \langle f, g\rangle$ e quindi la prima parte della proposizione è provata. Per provare la seconda parte, usiamo 2.2.2 per interpretare l'annullarsi del risultante in termini di fattori comuni. Per i polinomi in una sola variabile, abbiamo considerato i coefficienti in un campo, ora, dato che f e g sono polinomi in x_1 a coefficienti in $\mathbb{K}[x_2, ..., x_n]$, il più piccolo campo che lo contiene è $\mathbb{K}(x_2, ..., x_n)$. Allora possiamo applicare 2.2.2 ad f e $g \in \mathbb{K}(x_2, ..., x_n)[x_1]$ e ottenere che $Res(f, g, x_1) = 0$ se e solo se f e g hanno un fattore comune in $\mathbb{K}[x_2, ..., x_n][x_1] = \mathbb{K}[x_1, ..., x_n]$ di grado positivo in x_1, provando quindi la proposizione. □

Proposizione 2.2.9. *Sia $\mathbb{K}$ un campo algebricamente chiuso. Siano $f, g \in \mathbb{K}[x_1, ..., x_n]$ di grado l ed m rispettivamente e sia $c = (c_2, ..., c_n) \in \mathbb{K}^{n-1}$ tale che rispetti le seguenti condizioni:*

- $f(x_1, c) \in \mathbb{K}[x_1]$ *ha grado* l*;*

- $g(x_1, c) \in \mathbb{K}[x_1]$ *ha grado* $p \leq m$*.*

Allora il polinomio $h = Res(f, g, x_1) \in \mathbb{K}[x_2, ..., x_n]$ *soddisfa*

$$h(c) = a_0(c)^{m-p} Res\left(f(x_1, c), g(x_1, c), x_1\right)$$

dove $a_0 \neq 0$*.*

Dimostrazione. Se sostituiamo $c = (c_2, ..., c_n)$ ad $x_2, ..., x_n$ nella formula del determinante per $h = Res(f, g, x_1)$, otteniamo

$$h(c) = \det \begin{pmatrix} a_0(c) & 0 & 0 & b_0(c) & 0 & 0 \\ \vdots & \ddots & 0 & \vdots & \ddots & 0 \\ \vdots & & a_0(c) & \vdots & & b_0(c) \\ a_l(c) & & \vdots & b_m(c) & & \vdots \\ 0 & \ddots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & a_l(c) & 0 & 0 & b_m(c) \end{pmatrix}$$

Cominciamo supponendo che $g(x_1, c)$ abbia grado $p = m$. Allora

$$\begin{aligned} f(x_1, c) &= a_0(c)x_1^l + ... + a_l(c), \quad a_0(c) \neq 0, \\ g(x_1, c) &= b_0(c)x_1^m + ... + b_m(c), \quad b_0(c) \neq 0. \end{aligned}$$

Quindi il determinante quì sopra è il risultante di $f(x_1, c)$ e $g(x_1, c)$, cioé

$$h(c) = Res(f(x_1, c), g(x_1, c), x_1).$$

Questo prova la proposizione quando $p = m$.

Per provare il risultato anche per $p < m$, cominciamo prendendo $p = m - 1$, avremo:

$$h(c) = \det \begin{pmatrix} a_0(c) & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_1(c) & a_0(c) & 0 & 0 & b_1(c) & 0 & 0 & 0 \\ \vdots & a_1(c) & \ddots & 0 & \vdots & \ddots & 0 & 0 \\ \vdots & & \ddots & a_0(c) & \vdots & & \ddots & 0 \\ \vdots & & & a_1(c) & \vdots & & & b_1(c) \\ a_l(c) & & & \vdots & b_m(c) & & & \vdots \\ 0 & a_l(c) & & \vdots & 0 & b_m(c) & & \vdots \\ 0 & 0 & \ddots & \vdots & 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & a_l(c) & 0 & 0 & 0 & b_m(c) \end{pmatrix}$$

Basta calcolare il determinante rispetto alla prima riga e otteniamo che $h(c) = a_0(c) \cdot Res(f(x_1, c), g(x_1, c), x_1)$.

Per p ancora minore, basta ripetere il ragionamento con una matrice dove i coefficienti di b sono tutti uguali a zero fino a quello di indice $m - p - 1$, allora calcoleremo il determinante rispetto alle prime $m - p$ righe e avremo sempre a_0^{m-p} come fattore prima di $Res(f(x_1, c), g(x_1, c), c)$. □

Possiamo ora provare il teorema di estensione (2.0.7).

Dimostrazione del Teorema di estensione. Come prima, consideriamo $c = (c_2, ..., c_n)$. Poi consideriamo l'omomorfismo di anelli

$$\begin{array}{rcl} \mathbb{K}[x_1, ..., x_n] & \to & \mathbb{K}[x_1] \\ f(x_1, ..., x_n) & \mapsto & f(x_1, c). \end{array}$$

L'immagine di un ideale I mediante questo omomorfismo è un ideale di $\mathbb{K}[x_1]$. Dato che $\mathbb{K}[x_1]$ è un dominio a ideali principali, l'immagine di I è generata da un solo polinomio $u(x_1)$. In altri termini:

$$\{f(x_1, c) : f \in I\} = \langle u(x_1) \rangle .$$

Se $u(x_1)$ non è una costante, allora esiste $c_1 \in \mathbb{K}$ tale che $u(c_1) = 0$ per il teorema fondamentale dell'algebra. Ne segue che $f(c_1, c) = 0$ per ogni

$f \in I$, così che $(c_1, c) = (c_1, c_2, ..., c_n) \in V(I)$. Notiamo che questo argomento funziona anche se $u(x_1) = 0$. Resta da considerare il caso in cui $u(x_1)$ sia un polinomio costante non nullo u_0. Per l'uguaglianza precedente, esiste $f \in I$ tale che $f(x_1, c) = u_0$. Dobbiamo mostrare che questo caso non può presentarsi. Per ipotesi, la nostra soluzione parziale soddisfa $c \notin V(g_1, ..., g_s)$. Quindi $g_i(c) \neq 0$ per un qualche i. Quindi consideriamo

$$h = Res(f_i, f, x_1) \in \mathbb{K}[x_2, ..., x_n].$$

Applichiamo 2.2.9 ad f_i ed f, e otteniamo

$$h(c) = g_0(c)^{\deg(f)} Res(f_i(x_1, c), u_0, x_1)$$

dato che $f(x_1, c) = u_0$. Abbiamo anche che $Res(f_i(x_1, c), u_0, x_1) = u_0^{N_i}$. Quindi

$$h(c) = g_0(c)^{\deg(f)} u_0^{N_i} \neq 0.$$

Però $f_i, f \in I$ e 2.2.8 implicano che $h \in I_1$, così che $h(c) = 0$ dato che $c \in V(I_1)$. Questa contraddizione completa la dimostrazione del teorema di estensione. □

2.3 Implicitizzazione

Vediamo ora un'applicazione dell'eliminazione: vogliamo determinare le equazioni cartesiane di una varietà definita mediante una parametrizzazione.

Teorema 2.3.1 (Implicitizzazione polinomiale)**.** *Sia $\mathbb{K}$ è un campo infinito di caratteristica zero, sia $F : \mathbb{K}^m \to \mathbb{K}^n$ la funzione determinata dalla parametrizzazione polinomiale*

$$\begin{cases} x_1 = f_1(t_1, ..., t_m) \\ \quad \cdots \\ x_n = f_n(t_1, ..., t_m) \end{cases}$$

Sia I l'ideale $I = \langle x_1 - f_1, ..., x_n - f_n \rangle \subset \mathbb{K}[t_1, ..., t_m, x_1, ..., x_n]$ e sia $I_m = I \cap \mathbb{K}[x_1, ..., x_n]$ l'm-esimo ideale eliminazione. Allora $V(I_m)$ è la più piccola varietà in $\mathbb{K}^n$ che contiene $F(\mathbb{K}^m)$.

Dimostrazione. Sia $V = V(I) \subset \mathbb{K}^{n+m}$. Si vede che V è il grafico di $F : \mathbb{K}^m \to \mathbb{K}^n$.

Ora pensiamo $\mathbb{K} = \mathbb{C}$. Consideriamo inoltre

$$\begin{array}{rccc} i: & \mathbb{K}^m & \to & \mathbb{K}^{n+m} \\ & (t_1, ..., t_m) & \to & (t_1, ..., t_m, f_1(t_1, ..., t_m), ..., f_n(t_1, ..., t_m)). \end{array} \tag{2.7}$$

Questo ci dirà che $F(\mathbb{K}^m) = \pi_m(i(\mathbb{K}^m)) = \pi_m(V)$ e quindi $F(\mathbb{C}^m) = \pi_m(V)$. Questo prova il teorema quando $\mathbb{K} = \mathbb{C}$. Ora supponiamo che $\mathbb{K}$ sia un sottocampo di $\mathbb{C}$. Questo significa che $\mathbb{K} \subset \mathbb{C}$ e $\mathbb{K}$ ha le operazioni indotte da $\mathbb{C}$. Un tale campo contiene sempre gli interi $\mathbb{Z}$ (infatti contiene $\mathbb{Q}$) e quindi è infinito. Dato che $\mathbb{K}$ può essere più piccolo di $\mathbb{C}$, non possiamo usare direttamente il teorema di chiusura. Da qui in poi passeremo da $\mathbb{K}$ a $\mathbb{C}$ e viceversa: indicheremo il campo che stiamo considerando con dei pedici opportuni. Quindi $V_{\mathbb{K}}(I_m)$ è la varietà che otteniamo in $\mathbb{K}^n$, mentre $V_{\mathbb{C}}(I_m)$ è l'insieme di soluzioni in $\mathbb{C}^n$. (Notiamo che passare al campo più grande non cambia l'ideale eliminazione I_m, perché l'algoritmo usato per calcolare l'ideale eliminazione non subisce modifiche passando da $\mathbb{K}$ a $\mathbb{C}$.) Dobbiamo dimostrare che $V_{\mathbb{K}}(I_m)$ è la più piccola varietà di $\mathbb{K}^n$ che contiene $F(\mathbb{K}^m)$. 2.1.1 e $F(\mathbb{K}^m) = \pi_m(i(\mathbb{K}^m)) = \pi_m(V)$ ci dicono che $F(\mathbb{K}^m) = \pi_m(V_{\mathbb{K}}) \subset V_{\mathbb{K}}(I_m)$. Ora sia $Z_{\mathbb{K}} = V_{\mathbb{K}}(g_1, ..., g_s) \subset \mathbb{K}^n$ una qualunque varietà di $\mathbb{K}^n$ tale che $F(\mathbb{K}^m) \subset Z_{\mathbb{K}}$. Dobbiamo mostrare che $V_{\mathbb{K}}(I_m) \subset Z_k$. Cominciamo notando che $g_i = 0$ su $Z_{\mathbb{K}}$ e quindi $g_i = 0$ sull'insieme più piccolo $F(\mathbb{K}^m)$. Questo mostra che ogni $g_i \circ F$ si annulla su tutto $\mathbb{K}^m$. Ma i g_i sono polinomi in $\mathbb{K}[x_1, ..., x_n]$, ed $F = (f_1, ..., f_n)$ è fatto di polinomi in $\mathbb{K}[t_1, ..., t_m]$. Segue che $g_i \circ F \in \mathbb{K}[t_1, ..., t_m]$. Quindi, i $g_i \circ F$ sono polinomi che si annullano su $\mathbb{K}^m$. Dato che $\mathbb{K}$ è infinito, ogni $g_i \circ F$ è il polinomio nullo. In particolare, questo significa anche che $g_i \circ F$ si annulla su $\mathbb{C}^m$, e quindi che i g_i si annullano su $F(\mathbb{C}^m)$. Quindi $Z_{\mathbb{C}} = V_{\mathbb{C}}(g_1, ..., g_s)$ è una varietà di $\mathbb{C}^n$ che contiene $F(\mathbb{C}^m)$. Dato che il teorema è verificato per $\mathbb{C}$, segue che $V_{\mathbb{C}}(I_m) \subset Z_{\mathbb{C}}$ in $\mathbb{C}^n$. Se guardiamo le soluzioni che sono in $\mathbb{K}^n$, segue immediatamente che $V_{\mathbb{K}}(I_m) \subset Z_{\mathbb{K}}$. Questo prova che $V_{\mathbb{K}}(I_m)$ è la più piccola varietà di $\mathbb{K}^n$ che contiene $F(\mathbb{K}^m)$.

Infine, se $\mathbb{K}$ è un campo non contenuto in $\mathbb{C}$, si può lavorare sulla chiusura algebrica di $\mathbb{K}$, $\mathbb{K}'$. Abbiamo visto che il teorema di chiusura vale per un qualunque campo algebricamente chiuso, quindi questo teorema si può ridimostrare sostituendo $\mathbb{K}'$ a $\mathbb{C}$ in questa dimostrazione. □

Vediamo ora che un risultato analogo vale anche per funzioni definite con una parametrizzazione razionale:

Teorema 2.3.2 (Implicitizzazione razionale)**.** *Se $\mathbb{K}$ è un campo infinito, sia $F : \mathbb{K}^m \setminus W \to \mathbb{K}^n$ la funzione determinata dalla parametrizzazione razionale:*

$$\begin{cases} x_1 = \frac{f_1(t_1,...,t_m)}{g_1(t_1,...,t_m)} \\ \quad \cdots \\ x_n = \frac{f_n(t_1,...,t_m)}{g_n(t_1,...,t_m)} \end{cases}$$

e $W = V(g_1 \cdots g_n) \subset \mathbb{K}^n$. Sia $J = \langle g_1 x_1 - f_1, ..., g_n x_n - f_n, 1 - gy \rangle \subset \mathbb{K}[y, t_1, ..., t_m, x_1, ..., x_n]$, dove $g = g_1 \cdots g_n$, e sia $J_{m+1} = J \cap \mathbb{K}[x_1, ..., x_n]$ l'$(m+1)$-esimo ideale eliminazione di J. Allora $V(J_{m+1})$ è la più piccola varietà di $\mathbb{K}^n$ che contiene $F(\mathbb{K}^m \setminus W)$.

Per la dimostrazione abbiamo bisogno di provare questo lemma:

Lemma 2.3.3. *Sia $\mathbb{K}$ un campo infinito e siano $f, g \in \mathbb{K}[t_1, ..., t_m]$. Prendiamo $g \neq 0$ ed f che si annulla su $\mathbb{K}^m \setminus V(g)$. Allora f è il polinomio nullo.*

Dimostrazione. Consideriamo il prodotto $f(t) \cdot g(t)$ per $t \in \mathbb{K}^m$. Se $t \in V(g)$ allora $g(t) = 0$ e il prodotto si annulla. Se $t \in \mathbb{K}^m \setminus V(g)$ allora $f(t) = 0$. Quindi $\forall t \in \mathbb{K}^m$, $f(t) \cdot g(t) = 0$, ma g non è il polinomio nullo e quindi avremo $f(t) = 0 \ \forall t \in \mathbb{K}^m$. □

Dimostrazione. Questa dimostrazione è costruita sul modello del caso precedente, dove invece di 2.7 usiamo:

$$\begin{array}{rccc} j : & \mathbb{K}^m & \to & \mathbb{K}^{n+m+1} \\ & (t_1, ..., t_m) & \to & (\frac{1}{g(t_1,...,t_m)}, t_1, ..., t_m, \frac{f_1(t_1,...,t_m)}{g_1(t_1,...,t_m)}, ..., \frac{f_n(t_1,...,t_m)}{g_n(t_1,...,t_m)}). \end{array} \tag{2.8}$$

E di conseguenza, analogamente a prima avremo $F(\mathbb{K}^m \setminus W) = \pi_{m+1}(j(\mathbb{K}^m \setminus W)) = \pi_{m+1}(V(J))$.

L'unico problema restante viene risolto dal lemma, che ci assicura che un polinomio che si annulla su $\mathbb{K}^m \setminus W$ deve essere il polinomio nullo. □

Per vedere come funziona questo teorema, possiamo provare con l'esempio di un'iperbole piana.

Esempio 2.1. Consideriamo l'iperbole definita dall'equazione $t \cdot x = 1$. Per sfruttare la notazione utilizzata nel teorema scriveremo $x = \frac{f(t)}{g(t)} = \frac{1}{t}$.

Abbiamo $g = 0$ per $t = 0$ e quindi $W = V(g)$ è formata dal solo punto 0, $F(\mathbb{C} \setminus \{0\})$ sarà $\mathbb{C} \setminus \{0\}$. Possiamo trovare anche $J \subset \mathbb{C}[y, t, x]$, $J = \langle t \cdot x - 1, 1 - t \cdot y \rangle$.

Per calcolare l'ideale eliminazione utilizziamo il programma CoCoA. Riportiamo di seguito le quattro righe di codice necessarie per calcolare il secondo ideale eliminazione di J:

```
Use R::=QQ[y,t,x];

J:=Ideal(t*x-1,1-t*y);

GBasis(J);
[t*x -1, -y +x]

Elim(y..t,J);
ideal()
```

Otteniamo quindi che $J_2 = \{0\}$ e quindi $V(J_2) = \mathbb{C}$, che è la più piccola varietà che contiene (strettamente) $\mathbb{C} \setminus \{0\}$.

Questo esempio ci serve per evidenziare il fatto negli spazi affini, anche considerando campi algebricamente chiusi, l'immagine di una funzione

[2] in questo caso l'ideale non cambia se consideriamo $\mathbb{Q}$ o $\mathbb{C}$

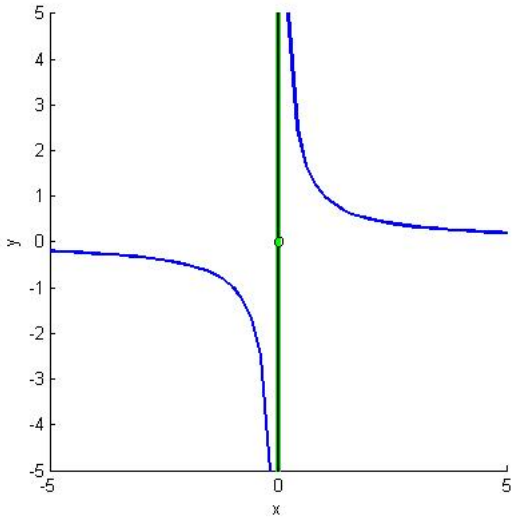

Figura 2.1: Iperbole in $\mathbb{K}^2$ e proiezione sull'asse y a confronto con la varietà data dall'ideale eliminazione: notiamo che il punto $(0,0)$ non è nella prima, ma solo nella seconda

razionale può essere contenuta strettamente nella proiezione ottenuta mediante l'eliminazione delle variabili del dominio.

Negli spazi proiettivi invece, vedremo che queste due coincideranno sempre.

Capitolo 3

Teoria dell'eliminazione proiettiva

Nel capitolo precedente abbiamo considerato il procedimento dell'eliminazione per polinomi generici, che definiscono varietà affini. In questo ci concentreremo su quelli omogenei, che definiscono varietà proiettive, oppure omogenei solo su un certo numero di variabili, che invece definiscono varietà in spazi prodotto tra uno spazio proiettivo e uno affine.

Cominciamo definendo questo nuovo insieme di polinomi:

Definizione 3.1. Sia $\mathbb{K}$ un campo

1. Un polinomio $F \in \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$ è $(x_0, ..., x_n)$-omogeneo se esiste un intero $l \geq 0$ tale che $F = \sum_{|\alpha|=l} h_\alpha (y_1, .., y_m) x^\alpha$ dove x^α è un monomio in $x_0, ..., x_n$ di multigrado α e $h_\alpha \in \mathbb{K}[y_1, ..., y_m]$;

2. La varietà $V(F_1, ..., F_s) \subset \mathbb{P}^n \times \mathbb{K}^m$ definita da polinomi $(x_0, ..., x_n)$-omogenei $F_1, ..., F_s \in \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$ è l'insieme

   $$\{(a_0, ..., a_n, b_1, ..., b_m) \in \mathbb{P}^n \times \mathbb{K}^m : F_i (a_0, ..., a_n, b_1, ..., b_m) = 0 \text{ per } 1 \leq i \leq s\}$$

   .

Analogamente al caso dell'eliminazione affine, possiamo definire l'ideale eliminazione proiettiva:

Definizione 3.2. Dato un ideale $I \subset \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$ generato da polinomi $(x_0, ..., x_n)$-omogenei, l' **ideale di eliminazione proiettiva** di I è l'insieme $\hat{I} = \{f \in \mathbb{K}[y_1, ..., y_m] : \ \forall\, 0 \leq i \leq n \ \exists\ e_i \geq 0 \text{ tc } x_i^{e_i} f \in I\}$.

Vediamo che in un campo generico (non necessariamente algebricamente chiuso) l'ideale eliminazione proiettiva definisce una varietà $V(\hat{I})$ più grande della semplice proiezione della varietà V di partenza sulla parte affine dello spazio.

Proposizione 3.0.4. *Sia $V = V(F_1, ..., F_s) \subset \mathbb{P}^n \times \mathbb{K}^m$ una varietà definita da polinomi $(x_0, ..., x_n)$-omogenei e sia $\pi : \mathbb{P}^n \times \mathbb{K}^m \to \mathbb{K}^m$ la mappa di proiezione. Allora in $\mathbb{K}^m$ abbiamo $\pi(V) \subset V(\hat{I})$ dove $\hat{I}$ è l'ideale di eliminazione proiettiva di $I = \langle F_1, ..., F_s \rangle$.*

Dimostrazione. Supponiamo di avere $(a_0, ..., a_n, b_1, ..., b_m) \in V$ ed $f \in \hat{I}$. Allora $x_i^{e_i} f(y_1, ..., y_m) \in I$ implica che questo polinomio si annulla su V, e quindi,

$$a_i^{e_i} f(b_1, ..., b_m) = 0$$

per qualsiasi i. Dato che $(a_0, ..., a_n)$ sono coordinate omogenee, almeno un $a_i \neq 0$ e, quindi, $f(b_1, ..., b_m) = 0$. Questo prova che f si annulla su $\pi(V)$ e la proposizione è provata. □

Invece se ci poniamo in un campo algebricamente chiuso, otteniamo che la proiezione della varietà V sullo spazio affine coincide con la varietà $V(\hat{I})$ definita dall'ideale eliminazione proiettiva e abbiamo il teorema di estensione proiettiva.

Teorema 3.0.5 (Teorema di estensione proiettiva)**.** *Sia $\mathbb{K}$ un campo algebricamente chiuso e $V = V(F_1, ..., F_s) \in \mathbb{P}^n \times \mathbb{K}^m$ la varietà definita da polinomi $(x_0, ..., x_n)$-omogenei in $\mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$. Sia $I = \langle F_1, ..., F_s \rangle$ e sia $\hat{I} \subset \mathbb{K}[y_1, ..., y_m]$ l'ideale di eliminazione proiettiva di I. Se $\pi : \mathbb{P}^n \times \mathbb{K}^m \to \mathbb{K}^m$ è la proiezione sulle ultime m coordinate, allora $\pi(V) = V(\hat{I})$.*

Dimostrazione. L'inclusione $\pi(V) \in V\left(\hat{I}\right)$ segue da 3.0.4. Per l'inclusione inversa, sia $c = (c_1, ..., c_m) \in V\left(\hat{I}\right)$ e $F_i(x_0, ..., x_n, c) = F_i(x_0, ..., x_n, c_1, ..., c_m)$. Questo è un polinomio omogeneo nelle variabili $x_0, ..., x_n$ di grado totale d_i (uguale al grado totale di $F_i(x_0, ...x_n, y_1, ...y_m)$ nelle $x_0, ..., x_n$).
Se $c \notin \pi(V)$, allora segue che le equazioni

$$F_1(x_0, ..., x_n, c) = \ldots = F_s(x_0, ..., x_n, c) = 0$$

definiscono la varietà vuota in $\mathbb{P}^n$. Dato che il campo $\mathbb{K}$ è algebricamente chiuso, il teorema di Nullstellensatz Proiettivo Debole (1.1.2) implica che esiste $r \geq 1$ tale che

$$\langle x_0, ..., x_n \rangle^r \subset \langle F_1(x_0, ..., x_n, c), \ldots, F_s(x_0, ..., x_n, c) \rangle .$$

Questo significa che i monomi del tipo x^α, con $|\alpha| = r$, possono essere scritti come combinazione polinomiale lineare degli $F_i(x_0, ..., x_n n, c)$, cioé:

$$x^\alpha = \sum_{i=1}^{s} H_i(x_0, ..., x_n) F_i(x_0, ..., x_n, c).$$

Prendendo le componenti omogenee, possiamo richiedere che ogni H_i sia omogeneo di grado totale $r - d_i$ (dato che d_i è il grado totale della $F_i(x_0, ..., x_n, c)$). Allora, se scriviamo ogni H_i come combinazione lineare dei monomi x^{β_i} con $|\beta_i| = r - d_i$, vediamo che i polinomi

$$x^{\beta_i} F_i(x_0, ..., x_n, c), i = 0, ..., s, |\beta_i| = r - d_i$$

riempiono lo spazio vettoriale di tutti i polinomi omogenei di grado totale r nelle variabili $x_0, ..., x_n$. Se la dimensione dello spazio è denotata come N_r, allora possiamo trovare N_r di questi polinomi che formino una base per questo spazio. Denoteremo questa base come

$$G_j(x_0, ..., x_n, c), j = 1, ..., N_r.$$

Per vedere perché questo porta ad una contraddizione, useremo l'algebra lineare e le proprietà dei determinanti per creare un elemento interessante

dell'ideale eliminazione $\hat{I}$. Il polinomio $G_j(x_0, ..., x_n, c)$ viene da un polinomio $G_j = G_j(x_0, ..., x_n, y_1, ..., y_m) \in \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$. Ogni G_j è della forma $x^{\beta_i} F_i$, per qualche i e β_i, ed è omogeneo in $x_0, ..., x_n$ di grado totale r. Quindi possiamo scrivere

$$G_j = \sum_{|\alpha|=r} a_{j\alpha}(y_1, ..., y_m) x^\alpha.$$

Dato che gli x^α con $|\alpha| = r$ formano una base per tutti i polinomi omogenei di grado totale r, esistono N_r monomi di questo tipo. Cioé otteniamo una matrice quadrata di polinomi $a_{j_\alpha}(y_1, ..., y_m)$. Sia

$$D(y_1, ..., y_m) = det(a_{j\alpha}(y_1, ..., y_m) : 1 \leq j \leq N_r, |\alpha| = r)$$

il determinante corrispondente. Se sostituiamo c nell'espressione di G_j otteniamo

$$G_j(x_0, ..., x_n, c) = \sum_{|\alpha|=r} a_{j\alpha}(c) x^\alpha$$

e dato che i $G_j(x_0, ..., x_n, c)$ e gli x^α sono basi dello stesso spazio vettoriale, vediamo che

$$D(c) \neq 0.$$

In particolare, questo mostra che $D(y_1, ..., y_m) \neq 0$ in $\mathbb{K}[y_1, ..., y_m]$.
Lavorando sullo spazio di funzioni $\mathbb{K}(y_1, ..., y_m)$, possiamo considerare l'espressione di G_j come un sistema di equazioni lineari in $\mathbb{K}(y_1, ..., y_m)$ con le x^α come variabili. Applicando la regola di Cramer, concludiamo che

$$x^\alpha = \frac{det\,(M_\alpha)}{D(y_1, ..., y_m)},$$

dove M_α è la matrice ottenuta da $(a_{j\alpha})$ rimpiazzando la colonna α-esima con $G_1, ..., G_{N_r}$. Se moltiplichiamo entrambi i membri per $D(y_1, ..., y_m)$ ed espandiamo $det\,(M_\alpha)$ lungo questa colonna otteniamo un'equazione della forma

$$x^\alpha D(y_1, ..., y_m) = \sum_{j=1}^{N_r} H_{j\alpha}(y_1, ..., y_m) G_j(x_0, ..., x_n, y_1, ..., y_m).$$

Comunque, ogni G_j è della forma $x^{\beta_i}F_i$, e se operiamo questa sostituzione e scriviamo la somma in termini degli F_i, otteniamo

$$x^{\alpha}D(y_1, ..., y_m) \in \langle F_1, ..., F_s \rangle = I.$$

Ciò mostra che $D(y_1, ..., y_m)$ è nell'ideale eliminazione proiettiva $\hat{I}$, e dato che $c \in V\left(\hat{I}\right)$, concludiamo che $D(c) = 0$. Questo contraddice quanto avevamo trovato prima e quindi prova che $c \in \pi(V)$, come volevamo. □

Il risultato ottenuto differisce dal caso dell'eliminazione affine, perché abbiamo un modo per trovare $\pi(V)$ esattamente mediante l'eliminazione di variabili, senza aggiungere sottovarietà.

Esempio 3.1. Per riprendere l'esempio precedente dell'iperbole nel piano, consideriamo l'iperbole in $\mathbb{P}^1 \times \mathbb{K}^1$:

$$x_1 \cdot y_1 = x_0.$$

Questa è definita da un polinomio (x_0, x_1)-omogeneo: $x_1 \cdot y_1 - x_0$.

Ripetendo il procedimento dell'implicitizzazione per polinomi razionali, si ottiene che $\pi(V)$ è tutto l'asse y_1, perchè aggiungiamo il punto all'infinito, e anche $V(\hat{I})$, dato che nuovamente l'ideale eliminazione è composto solo dal polinomio nullo.

Questa situazione è rappresentata graficamente in 3.1, dove le due varietà coincidono, in accordo con quanto provato nel teorema 3.0.5, diversamente da quanto succede nel caso affine, in cui utilizziamo polinomi non omogenei.

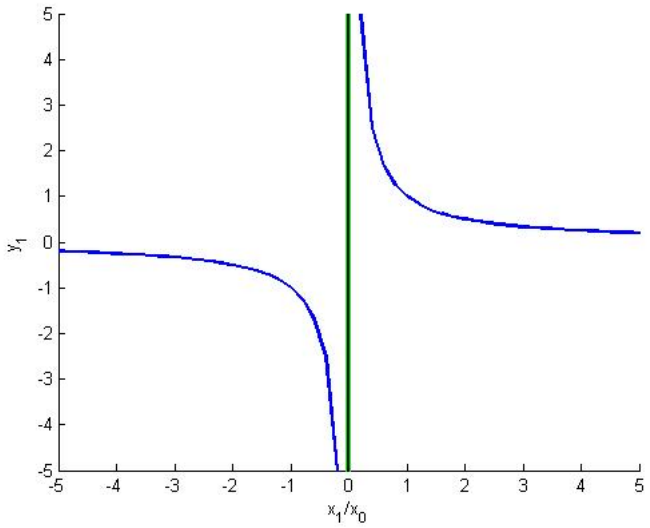

Figura 3.1: Iperbole in $\mathbb{K}^1 \times \mathbb{P}^1$ e proiezione sull'asse y a confronto con la varietà data dall'ideale eliminazione: entrambe ricoprono tutto l'asse y.

Vediamo ora un metodo costruttivo per ottenere l'ideale eliminazione proiettiva.

Proposizione 3.0.6. *Sia* $I \subset \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$ *un ideale generato da polinomi* $(x_0, ..., x_n)$*-omogenei. Allora* $\hat{I} = I_n^{(0)} \cap I_n^{(1)} \cap ... \cap I_n^{(n)}$.
Dove $F^{(i)} = F(x_0, ..., x_{i-1}, 1, x_{i+1}, ..., x_n, y_1, ..., y_m)$, $I^{(i)} = \left\{F^{(i)} : F \in I\right\}$, $I = \langle F_1, ..., F_s \rangle \Rightarrow I^{(i)} = \left\langle F_1^{(i)}, ..., F_s^{(i)} \right\rangle$, $I_n^{(i)} = I^{(i)} \cap \mathbb{K}[y_1, ..., y_m]$.

In questa dimostrazione abbiamo polinomi omogeneizzati usando x_i per un i qualsiasi, non solo per x_0. Il procedimento è identico, l'unica differenza è quale U_i si identifica con $\mathbb{K}^n$.

Dimostrazione. Basta mostrare che

$$\hat{I} = I^{(0)} \cap ... \cap I^{(n)} \cap \mathbb{K}[y_1, ..., y_m].$$

Prima di tutto supponiamo che $f \in \hat{I}$. Poi $x_i^{e_i} f(y_1, ..., y_m) \in I$, così che quando poniamo $x_i = 1$, otteniamo $f(y_1, ..., y_m) \in I^{(i)}$. Questo prova $f \in I^{(0)} \cap ... \cap I^{(n)} \cap \mathbb{K}[y_1, ..., y_m]$. Per l'inclusione inversa, studiamo prima la

relazione tra I e $I^{(i)}$. Un elemento $f \in I^{(i)}$ è ottenuto da un qualche $F \in I$ ponendo $x_i = 1$. Affermiamo che F può essere presa come $(x_0, ..., x_n)$-omogenea. Per provarlo, notiamo che F può essere scritta come una somma $F = \sum_{j=0}^{d} F_j$, dove F_j è $(x_0, ..., x_n)$-omogeneo di grado totale j nelle $x_0, ..., x_n$. Dato che I è generato da polinomi $(x_0, ..., x_n)$-omogenei, segue facilmente che $F_j \in I \ \forall j$. Questo implica che

$$\sum_{j=0}^{d} x_i^{d-j} F_j$$

sia un polinomio $(x_0, ..., x_n)$-omogeneo in I che deomogeneizzato diventa f quando $x_i = 1$. Quindi possiamo considerare $F \in I$ come $(x_0, ..., x_n)$-omogeneo. Possiamo ora definire un operatore di omogeneizzazione che prenda un polinomio $f \in \mathbb{K}[x_0, ..., \hat{x}_i, ..., x_n, y_1, ..., y_m]$ e usi la variabile extra x_i per produrre un polinomio $(x_0, ..., x_n)$-omogeneo $f^h \in \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$. Notiamo che se un polinomio $(x_0, ..., x_n)$-omogeneo F deomogeneizzato utilizzando $x_i = 1$, diventa f, allora

$$f = x_i^e f^h$$

per un qualche intero $e \geq 0$. Ora supponiamo $f \in I^{(i)} \cap \mathbb{K}[y_1, ..., y_m]$. Come abbiamo visto prima, f deriva da $F \in I$, che è $(x_0, ..., x_n)$-omogenea. Dato che f non riguarda $x_0, ..., x_n$, abbiamo $f = f^h$, e allora per l'uguaglianza precedente $x_i^e f \in I$. Segue immediatamente che $I^{(0)} \cap ... \cap I^{(n)} \cap \mathbb{K}[y_1, ..., y_m] \subset \hat{I}$, e la proposizione è provata. □

3.1 Chiusura proiettiva

In questa sezione vediamo che cosa si ottiene omogeneizzando un ideale solo per alcune variabili, cioé passeremo da varietà in spazi affini a varietà in spazi ottenuti dal prodotto tra uno spazio affine ed uno proiettivo.

Come primo risultato troviamo un'equivalenza fra eliminazione proiettiva ed eliminazione affine considerando gli ideali, poi vediamo come ottenere la più piccola varietà proiettiva che ne contiene una affine.

Proposizione 3.1.1. *Dato un ideale $I \subset \mathbb{K}[x_1, ..., x_n, y_1, ..., y_m]$, sia I^h la sua $(x_0, ..., x_n)$-omogeneizzazione. Allora:*

1. *L'ideale di eliminazione proiettiva di I^h equivale all'n-esimo ideale eliminazione di I. Cioé $\hat{I}^h = I_n \subset \mathbb{K}[y_1, ..., y_m]$;*

2. *Se $\mathbb{K}$ è algebricamente chiuso, allora la varietà $\bar{V} = V(I^h)$ è la più piccola varietà in $\mathbb{P}^n \times \mathbb{K}^m$ che contiene la varietà affine $V = V_a(I) \subset \mathbb{K}^n \times \mathbb{K}^m$. Chiamiamo $\bar{V}$ la **chiusura proiettiva** di V in $\mathbb{P}^n \times \mathbb{K}^m$.*

Dimostrazione. 1. Risulta direttamente che la deomogeneizzazione di I^h rispetto ad x_0 ci restituisce $\left(I^h\right)^{(0)} = I$. Allora 3.0.6 ci dice che $\hat{I^h} \subset I_n$. Per provare l'impocazione inversa, bisogna considerare $f \in I_n$. Dato che $f \in \mathbb{K}[y_1, ..., y_m]$, allora è già $(x_0, ..., x_n)-$omogenea. Quindi $f = f^h \in I^h$ e segue che $x_i^0 f \in I^h$ per qualsiasi i. Questo mostra che $f \in \hat{I^h}$, e il primo punto è provato.

2. Vogliamo provare che se W è una varietà in $\mathbb{P}^n \times \mathbb{K}^m$ che contiene $V = V_a(I)$, allora $\bar{V} = V\left(I^h\right) \subset W$. Supponiamo che $W = V(F_1, ..., F_s)$. Allora le F_i si annullano su W e le loro $(x_0, ..., x_n)-$deomogeneizzazioni $f_i = F_i(1, x_1, ..., x_n, y_1, ..., y_m)$ si annullano su $V_a(I)$. Cioé $f_i \in I$ e quindi la sua $(x_0, ..., x_n)-$omogeneizzazione $f_i^h \in I^h$. Questo mostra che le f_i^h si annullano su $\bar{V} = V\left(I^h\right)$, ma sappiamo che $\forall i\ \exists e_i \in \mathbb{N}$ tale che $F_i = x_0^{e_i} f_i^h$.
   Quindi le F_i si annullano su $\bar{V}$ e dato che questo succede per tutti gli i, segue che $\bar{W} \subset V$.

□

Usando questa proposizione insieme al Teorema di estensione proiettiva, otteniamo il risultato seguente.

Corollario 3.1.2. *Sia $\mathbb{K}$ algebricamente chiuso e $V = V_a(I) \subset \mathbb{K}^n \times \mathbb{K}^m$, dove $I \subset \mathbb{K}[x_1, ..., x_n, y_1, ..., y_m]$ è un ideale. Allora:*

$$V(I_n) = \pi(\bar{V})$$

dove $\bar{V} \subset \mathbb{P}^n \times \mathbb{K}^m$ è la chiusura proiettiva di V e $\pi : \mathbb{P}^n \times \mathbb{K}^m \to \mathbb{K}^m$ è la proiezione sulle ultime m coordinate.

Dimostrazione. Dato che 3.1.1 ci dice che $\bar{V} = V\left(I^h\right)$ e $\hat{I^h} = I_n$, allora segue direttamente la dimostrazione del corollario dal Teorea di Estensione Proiettiva (3.0.5). □

3.2 Morfismi tra varietà proiettive

Cominciamo questa sezione definendo i morfismi di varietà proiettive e osservando che hanno sempre immagine chiusa.

Definizione 3.3. Siano $V \subset \mathbb{P}^n(\mathbb{K})$ e $W \subset \mathbb{P}^m(\mathbb{K})$ due varietà proiettive. Un morfismo $\phi : V \to W$ è definito come un morfismo

$$\begin{array}{rccc} \phi : & V & \longrightarrow & \mathbb{P}^m(\mathbb{K}) \\ & (x_0, ..., x_n) & \mapsto & (\phi_0(x_0, ..., x_n), ..., \phi_m(x_0, ..., x_n)) \end{array}$$

con $\phi(V) \subset W$ e $\phi_0, ..., \phi_m$ polinomi omogenei nelle indeterminate $x_0, ..., x_n$.

Teorema 3.2.1. *Sia $\mathbb{K}$ algebricamente chiuso. Sia $V \subset \mathbb{P}^n(\mathbb{K})$ una varietà proiettiva, W una varietà qualsiasi, $\phi : V \to W$ un morfismo. Allora $\phi(V)$ è chiuso.*

Dimostrazione. Denotiamo il grafico di ϕ come

$$\Gamma_\phi \subset X \times Y \subset \mathbb{P}^n(\mathbb{K}) \times Y.$$

Vogliamo provare che questo è chiuso. Consideriamo il morfismo indotto

$$(\phi, Id) : X \times Y \to Y \times Y,$$

con l'identita a secondo termine. Abbiamo

$$\Gamma_\phi = \{(x, y) \in X \times Y : (f, Id)(x, y) = (y, y)\} = (\phi, Id)^{-1}(\Delta_Y)$$

dove Δ_Y è la diagonale. Dato che Δ_Y è chiusa in $Y \times Y$, anche Γ_ϕ è chiuso. Scegliamo un ricoprimento affine $\{V_j\}$ per Y; costruiamo $V_j \subset \mathbb{K}^m$ come un insieme chiuso. Anche l'intersezione

$$\Gamma_\phi \cap \pi_2^{-1}(V_j) \subset \mathbb{P}^n(\mathbb{K}) \times \mathbb{K}^m$$

è chiusa, e il teorema di estensione (3.0.5) ci dice che anche $\pi_2(\Gamma_\phi \cap \pi_2^{-1}(V_j))$ è chiuso, e questo equivale a $\pi_2(\Gamma_p hi) \cap V_j = \phi(X) \cap V_j$. Quindi l'intersezione di $\phi(X)$ con ogni aperto affine è chiusa in quell'aperto, e $\phi(X)$ è chiuso in Y. □

Vogliamo ora vedere cosa succede applicando una funzione polinomiale, definita da polinomi omogenei, ad uno spazio proiettivo.

Per fare questo abbiamo bisogno di dimostrare che, con un buon ordinamento monomiale, l'omogeneizzazione non cambia la base di Groebner di un ideale.

Proposizione 3.2.2. *Sia $>$ un ordinamento monomiale fissato sull'anello $\mathbb{K}[x_1, ..., x_n, y_1, ..., y_m]$ tale che per tutti i monomi $x^\alpha y^\gamma$, $x^\beta y^\delta$ nelle variabili $x_1, ..., x_n, y_1, ..., y_m$, abbiamo*

$$|\alpha| > |\beta| \Rightarrow x^\alpha y^\gamma > x^\beta y^\delta.$$

Se $G = \{g_1, ..., g_s\}$ è una base di Groebner per $I \subset \mathbb{K}[x_1, ..., x_n, y_1, ..., y_m]$ rispetto a $>$, allora $G^h = \{g_1^h, ..., g_s^h\}$ è una base per $I^h \subset \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$

Per provare questa proposizione abbiamo bisogno del seguente lemma:

Lemma 3.2.3. *Se $f \in \mathbb{K}[x_1, ..., x_n]$ e $>$ è un ordine graduato su $\mathbb{K}[x_1, ..., x_n]$, allora*

$$LM_{>h}(f^h) = LM_>(f).$$

Dimostrazione. Dato che $>$ è un ordine graduato, per qualsiasi $f \in \mathbb{K}[x_1, ..., x_n]$, $LM_>(f)$ è uno dei monomi x^α che appare nella componente omogenea di f di grado totale massimo. Quando omogeneizziamo, questo termine non viene modificato. Se $x^\beta x_0^e$ è un qualsiasi altro monomio che appare in f^h, allora

$\alpha > \beta$. Per definizione di $>_h$, segue che $x^\alpha >_h x^\beta x_0^e$. Quindi, $x^\alpha = LM_{>h}(f^h)$, e il lemma è provato. □

Ora possiamo dimostrare la proposizione

Dimostrazione. Grazie al lemma appena dimostrato, sappiamo che i monomi principali di tutti gli elementi di I non verranno modificati dall'omogeneizzazione parziale, quindi neanche i termini principali, che sono quelli che determinano se una base è di Groebner o meno. Otteniamo quindi $\langle LT(I^h)\rangle = \langle LT(I)\rangle = \langle LT(g_1), ..., LT(g_s)\rangle = \langle LT(g_1^h), ..., LT(g_s^h)\rangle$. E la proposizione è provata. □

Arriviamo quindi al teorema finale di questo capitolo, che estende il risultato ottenuto precedentemente per le sole proiezioni a tutte le funzioni definite da polinomi omogenei: potremo trovare l'immagine di un tale morfismo sfruttando il procedimento dell'eliminazione sull'ideale che definisce il grafico della funzione.

Per fare questo dobbiamo considerare varietà nel prodotto $\mathbb{P}^n \times \mathbb{P}^m$, definite da polinomi biomogenei.

Definizione 3.4. Un polinomio $h \in \mathbb{K}[x_0, ..., x_n, y_0, ..., y_m]$ è detto *biomogeneo* se può essere scritto come

$$h = \sum_{|\alpha|=k, |\beta|=l} a_{\alpha\beta} x^\alpha y^\beta.$$

Osservazione 2. Se $h_1, ..., h_s$ sono biomogenei, otteniamo un insieme ben definito

$$V(h_1, ..., h_s) \subset \mathbb{P}^n \times \mathbb{P}^m$$

che è una varietà definita da $h_1, ..., h_s$.

Teorema 3.2.4. *Sia $\mathbb{K}$ un campo algebricamente chiuso e sia $F : \mathbb{P}^n \to \mathbb{P}^m$ definita da polinomi omogenei $f_0, ..., f_m \in \mathbb{K}[x_0, ..., x_n]$ che hanno lo stesso grado totale > 0 e nessuno zero comune su $\mathbb{P}^n$. In $\mathbb{K}[x_0, ..., x_n, y_0, ..., y_m]$ sia I l'ideale $\langle y_0 - f_0, ..., y_m - f_m\rangle$ e sia $I_{n+1} = I \cap \mathbb{K}[y_0, ..., y_m]$. Allora I_{n+1} è un ideale omogeneo in $\mathbb{K}[y_0, ..., y_m]$ e $F(\mathbb{P}^n) = V(I_{n+1})$.*

Dimostrazione. Per prima cosa mostriamo che I_{n+1} è un ideale omogeneo. Supponiamo che gli f_i abbiano grado totale d. Dato che i generatori $y_i - f_i$ di I non sono omogenei (a meno che $d = 1$), introdurremo dei pesi sulle variabili $x_0, ..., x_n, y_1, ..., y_m$. Diciamo che ogni x_i ha peso 1 e ogni y_i ha peso d. Allora un monomio $x^\alpha y^\beta$ ha peso $|\alpha| + d\,|\beta|$, e un polinomio $f \in \mathbb{K}[x_0, ..., x_n, y_1, ..., y_m]$ è omogeneo pesato se ogni monomio in f ha lo stesso peso.
I generatori $y_i - f_i$ di I hanno tutti peso d, così che I è un ideale omogeneo pesato. Se calcoliamo una base di Groebner ridotta G per I rispetto ad un qualunque ordine monomiale, un argomento simile alla dimostrazione del Teorema di eliminazione (2.0.6) mostra che G consiste di polinomi omogenei pesati. Per un ordine lessicografico appropriato, il Teorema di eliminazione ci dice che $G \cap \mathbb{K}[y_0, ..., y_m]$ è una base di $I_{n+1} = I \cap \mathbb{K}[y_0, ..., y_m]$. Quindi I_{n+1} ha una base omogenea pesata. Dato che gli y_i hanno tutti lo stesso peso, un polinomio in $\mathbb{K}[y_0, ..., y_m]$ è omogeneo pesato se e solo se è omogeneo nel senso usuale. Questo prova che I_{n+1} è un ideale omogeneo.

Se $J \subset \mathbb{K}[x_0, ..., x_n, y_0, ..., y_m]$ è generato da polinomi biomogenei, l'osservazione 2 ci dice che otterremo una varietà $V(J) \subset \mathbb{P}^n \times \mathbb{P}^m$. La teoria dell'eliminazione si applica facilmente a questa situazione. L'ideale di eliminazione proiettiva $\hat{J} \subset \mathbb{K}[y_0, ..., y_m]$ è un ideale omogeneo. Allora, usando la proiezione $\pi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$, risulta come corollario del Teorema di estensione proiettiva (3.0.5) che

$$\pi(V(J)) = V(\hat{J})$$

in $\mathbb{P}^m$.
Non possiamo applicare questo risultato ad I perché non è generato da polinomi biomogenei. Quindi lavoreremo con l'ideale biomogeneo $J = \langle y_i f_j - y_j f_i \rangle$. Mostriamo prima che $V(J) \subset \mathbb{P}^n \times \mathbb{P}^m$ è il grafico di $F : \mathbb{P}^n \to \mathbb{P}^m$. Dato $p \in \mathbb{P}^n$, abbiamo $(p, F(p)) \in V(J)$ dato che $y_i = f_i(p)$ per ogni i.

Viceversa, supponiamo che $(p, q) \in V(J)$. Allora $q_i f_j(p) = q_j f_i(p)$ per ogni i, j, dove q_i è l'i-esima coordinata omogenea di q. Possiamo trovare j

con $q_j \neq 0$, e per la nostra imposizione su $f_0, ..., f_m$ esiste i con $f_i(p) \neq 0$. Allora $q_i f_j(p) = q_j f_i(p) \neq 0$ mostra che $q_i \neq 0$. Ora sia $\lambda = q_i/f_i(p)$, che è un elemento diverso da zero di $\mathbb{K}$. Dalle equazioni che definiscono $V(J)$, segue che $q = \lambda F(p)$, che mostra che (p,q) è nel grafico di F in $\mathbb{P}^n \times \mathbb{P}^m$.
Come ci mostra la parte introduttiva sull'implicitizzazione (2.3.1), la proiezione del grafico è l'immagine della funzione. Quindi mediante $\pi : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$, abbiamo $\pi(V(J)) = F(\mathbb{P}^n)$. Se combiniamo questo con il risultato appena ottenuto, otteniamo $F(\mathbb{P}^n) = V(\hat{J})$, dato che $\mathbb{K}$ è algebricamente chiuso. Questo prova che l'immagine di F è una varietà in $\mathbb{P}^m$.
Dato che conosciamo un algoritmo per calcolare $\hat{J}$, potremmo fermarci qui. Il problema è che $\hat{J}$ è complicato da calcolare. Risulta molto più semplice lavorare con $I_{n+1} = I \cap \mathbb{K}[y_0, ..., y_m]$, quindi l'ultimo passaggio della dimostrazione è provare che $V(\hat{J}) = V(I_{n+1})$ in $\mathbb{P}^m$.
Basta lavorare nello spazio affine $\mathbb{K}^{m+1}$ e provare che $V_a(\hat{J}) = V_a(I_{n+1})$. Osserviamo che la varietà $V_a(I) \subset \mathbb{K}^{n+1} \times \mathbb{K}^{m+1}$ è il grafico della mappa $\mathbb{K}^{n+1} \to \mathbb{K}^{m+1}$ definita da $(f_0, ..., f_m)$. Mediante la proiezione $\pi : \mathbb{K}^{n+1} \times \mathbb{K}^{m+1} \to \mathbb{K}^{m+1}$, diciamo che $\pi(V_a(I)) = V_a(\hat{J})$. Sappiamo che $V(\hat{J})$ è l'immagine di F in $\mathbb{P}^m$. Una volta che escludiamo l'origine, questo significa che $q \in V_a(\hat{J})$ se e solo se esiste un $p \in \mathbb{K}^{n+1}$ tale che q sia uguale a $F(p)$ in $\mathbb{P}^m$. Quindi, $q = \lambda F(p)$ in $\mathbb{K}^{m+1}$ per qualche $\lambda \neq 0$. Se poniamo $\lambda' = \sqrt[d]{\lambda}$, allora $q = F(\lambda' p)$, che è equivalente a $q \in \pi(V_a(I))$. L'enunciato ora segue facilmente.
Per il Teorema di Chiusura (2.1.3), $V_a(I_{n+1})$ è la più piccola varietà che contiene $\pi(V_a(I))$. Dato che questa proiezione è la varietà $V_a(\hat{J})$, segue che $V_a(I_{n+1}) = V_a(\hat{J})$. Questo completa la dimostrazione del teorema. □

Lo stesso risultato si può infine estendere a funzioni definite su varietà proiettive invece che su tutto lo spazio.

Corollario 3.2.5. *Sia $V \subset \mathbb{P}^n(\mathbb{K})$ e $F : V \to \mathbb{P}^m(\mathbb{K})$ un morfismo di varietà proiettive. Allora il grafico $\Gamma_F \subset \mathbb{P}^n \times \mathbb{P}^m$ è dato dalle equazioni biomogenee*

$$I(\Gamma_F) = \langle y_i f_j - y_j f_i \rangle .$$

Quindi su un campo algebricamente chiuso, le equazioni dell'immagine $F(V)$ *sono date dall'*$(n+1)$*-esimo ideale eliminazione proiettiva di* $I(\Gamma_F)$.

Dimostrazione. Sia $U_i \subset X$ l'aperto affine dove $f_i \neq 0$ e $V_i \subset \mathbb{P}^m$ l'aperto affine dove $y_i \neq 0$, così che $f_i(U_i) \subset V_i$. Su $U_i \times V_i$, $J(\Gamma_f)$ si deomogenizza in

$$y_j = f_j/f_i$$

l'equazione del grafico di F. □

Capitolo 4

Teorema di Bezout

Vediamo ora un'applicazione dell'eliminazione e in particolare del risultante: il teorema di Bezout, che riguarda il numero dei punti di intersezione tra due curve in $\mathbb{P}^2(\mathbb{C})$ e contati con molteplicità.

4.1 Forma debole del Teorema di Bezout

Proposizione 4.1.1. *Sia $f \in \mathbb{C}[x,y,z]$ un polinomio omogeneo non nullo. Allora anche i fattori irriducibili di f sono omogenei e se fattorizziamo f in irriducibili: $f = f_1^{a_1} \cdot ... \cdot f_s^{a_s}$ dove f_i non è un multiplo di f_j per $i \neq j$, allora $V(f) = V(f_1) \cup ... \cup V(f_s)$ è la scomposizione minimale di $V(f)$ in componenti irriducibili in $\mathbb{P}^2(\mathbb{C})$.*
Inoltre $I(V(f)) = \sqrt{\langle f \rangle} = \langle f_1, ..., f_s \rangle$.

Dimostrazione. Per prima cosa supponiamo che f si fattorizzi come $f = gh$ per due polinomi $g, h \in \mathbb{C}[x,y,z]$. Mostriamo che g ed h debbono essere omogenei, dato che f lo è. Per provare questo, scriviamo $g = g_m + ... + g_0$, dove g_i è omogeneo di grado totale i e $g_m \neq 0$. In modo simile avremo $h = h_n + ... + h_0$. Allora

$f = gh = (g_m + ... + g_0)(h_n + ... + h_0) = g_m h_n +$ termini di grado più basso.

Dato che f è omogeneo, dobbiamo avere $f = g_m h_n$, e quindi possiamo concludere che $g = g_m$ e $h = h_n$. Quindi g ed h sono omogenei. Da qui

segue facilmente che anche i fattori irriducibili di f sono omogenei. Ora supponiamo che f si fattorizzi come sopra. Allora $V(f) = V(f_1) \cup ... \cup V(f_s)$ segue immediatamente, e questa è la scomposizione minimale in componenti irriducibili. Dato che $V(f) \neq \emptyset$, l'affermazione su $I(V(f))$ segue dal Nullstellensatz proiettivo. □

Osservazione 3. Nel seguito del capitolo, ogni curva $C \subset \mathbb{P}^2(\mathbb{C})$ sarà $C = V(f)$ con $I(C) = \langle f_1 \cdot ... \cdot f_s \rangle$ con f_i fattori irriducibili $\Rightarrow f_1 \cdot ... \cdot f_s = 0$ è l'equazione che definisce C.

Lemma 4.1.2. *Siano $f, g \in \mathbb{C}[x, y, z]$ polinomi omogenei di grado m ed n rispettivamente. Se $f(0, 0, 1)$ e $g(0, 0, 1)$ sono $\neq 0$ allora il risultante $Res(f, g, z)$ è omogeneo in x e y di grado totale mn.*

Lemma 4.1.3. *Sia $h \in \mathbb{C}[x, y]$ un polinomio omogeneo $\neq 0$. Allora h può essere scritto nella forma $h = c(s_1x - r_1y)^{m_1} \cdots (s_tx - r_ty)^{m_t}$ dove $c \neq 0$ in $\mathbb{C}$ e $(r_1, s_1), ..., (r_t, s_t)$ sono punti distinti di $\mathbb{P}^1$.*
Inoltre $V(h) = \{(r_1, s_1), ..., (r_t, s_t)\} \subset \mathbb{P}^1$.

Dimostrazione. Questo lemma si prova facilmente pensando che se fra i fattori vi fosse un elemento del tipo $(s_ix - r_i)$ (oppure equivalentemente $(s_i - r_iy)$) non potremmo ottenere un polinomio omogeneo. □

Teorema 4.1.4 (Forma debole del teorema di Bezout)**.** *Siano C e D curve proiettive in $\mathbb{P}^2(\mathbb{C})$ senza componenti irriducibili in comune. Se i gradi delle equazioni ridotte per C e D sono m ed n rispettivamente, allora $C \cap D$ è finito e ha al più mn punti.*

Dimostrazione. Supponiamo che $C \cap D$ abbia più di mn punti. Scegliamone $mn + 1$, che chiamiamo $p_1, ..., p_{mn+1}$, e per $1 \leq i < j \leq mn + 1$, sia L_{ij} la retta passante per p_i e p_j. Quindi prendiamo un punto $q \in \mathbb{P}^2$ tale che

$$q \notin C \cup D \cup \bigcup_{i<j} L_{ij}. \tag{4.1}$$

Scegliamo un cambiamento di coordinate per $\mathbb{P}^2$ in modo che il punto q abbia coordinate $(0, 0, 1)$ nel nuovo sistema. Possiamo quindi considerare

$q = (0, 0, 1)$ che soddisfa la condizione 4.1.
Ora supponiamo che $C = V(f)$ e $D = V(g)$, dove f e g sono ridotti di gradi m ed n rispettivamente. Allora 4.1 implica che $f(0, 0, 1) \neq 0$ dato che $(0, 0, 1) \notin C$, e $g(0, 0, 1) \neq 0$ perché $(0, 0, 1) \notin D$. Quindi per il lemma 4.1.2, il risultante $Res(f, g, z)$ è un polinomio omogeneo di grado mn in x, y. Dato che f e g hanno grado positivo nella z e non hanno fattori comuni in $\mathbb{C}[x, y, z]$, la proposizione 2.2.8 ci mostra che $Res(f, g, z)$ non è nulla.
Se poniamo $p_i = (u_i, v_i, w_i)$, allora dato che il risultante è nell'ideale generato da f e g, abbiamo

$$Res(f, g, z)(u_i, v_i) = 0. \tag{4.2}$$

Bisogna notare che la retta passante per per $q = (0, 0, 1)$ e $p_i = (u_i, v_i, w_i)$ interseca $z = 0$ nel punto $(u_i, v_i, 0)$ (si vede facilmente facendo i conti). Abbiamo quindi una proiezione da q sulla retta $z = 0$. Un punto $(u, v, w) \in \mathbb{P}^2 \setminus \{(0, 0, 1)\}$ viene mandato in $(u, v, 0)$. Quindi 4.2 ci dice che $Res(f, g, z)$ si annulla sui punti ottenuti proiettando i $p_i \in C \cap D$ da $(0, 0, 1)$ sulla retta $z = 0$.
Per 4.1, $(0, 0, 1)$ non è in nessuna delle rette che passano per i p_i e i p_j e quindi i punti $(u_i, v_i, 0)$ sono distinti per $i = 1, ..., mn + 1$. Se consideriamo $z = 0$ come una copia di $\mathbb{P}^1$ con coordinate omogenee x, y, allora otteniamo punti distinti $(u_i, v_i) \in \mathbb{P}^1$, e i polinomi omogenei $Res(f, g, z)$ si annullano su tutti gli $mn + 1$ punti. Per il lemma 4.1.3, questo è impossibile, dato che $Res(f, g, z)$ è un polinomio non nullo di grado mn e quindi il teorema è provato. □

4.2 Teorema di Bezout

L'ultimo teorema dimostrato ci assicura che se C e D non hanno componenti irriducibili in comune, $C \cap D$ sarà sempre costituito da un numero finito di punti. Definendo la molteplicità di intersezione tra due curve in un punto comune possiamo ulteriormente rendere più preciso il risultato.

4.2.1 Molteplicità di intersezione

Diamo la definizione di molteplicità di intersezione attraverso le proprietà che la caratterizzano.

Definizione-Proposizione 2 (Proprietà della molteplicità dell'intersezione di due curve)**.** Esiste una e una sola molteplicità di intersezione $I_p(C, D)$ definita per ogni coppia di curve proiettive C e D in $\mathbb{P}^2$ in un loro punto comune p. Questa soddisfa le seguenti proprietà:

1. $I_p(C, D) = I_p(D, C)$;
2. $I_p(C, D) = \infty$ se p giace su una componente comune di C e D. Altrimenti $I_p(C, D)$ è un intero non negativo;
3. $I_p(C, D) = 0$ se e solo se $p \notin C \cap D$;
4. Due rette distinte si incontrano con molteplicità di intersezione uno nel loro unico punto in comune;
5. Se C_1 e C_2 sono definite da polinomi omogenei $f_1(x, y, z)$ e $f_2(x, y, z)$ e C è definita da $f(x, y, z) = f_1(x, y, z)f_2(x, y, z)$ allora $I_p(C, D) = I_p(C_1, D) + I_p(C_2, D)$
6. Se C e D sono definite da polinomi omogenei $f(x, y, z)$ e $g(x, y, z)$ di gradi n ed m ed E è definita da $f \cdot h + g$ dove $h(x, y, z)$ è omogeneo di grado $m - n$ allora $I_p(C, D) = I_p(C, E)$

Inoltre se C e D non hanno componenti comuni e scegliamo coordinate proiettive in modo che siano soddisfatte le condizioni

(a) $(0, 0, 1) \notin C \cup D$

(b) $(0, 0, 1) \notin$ a nessuna retta congiungente due punti distinti di $C \cap D$

(c) $(0, 0, 1) \notin$ a nessuna retta tangente a C o a D in nessun punto di $C \cap D$

allora la molteplicità dell'intersezione $I_p(C, D)$ di C e D in qualsiasi $p = (a, b, c) \in C \cap D$ è il più grande intero k tale che $(ax - by)^k$ divida il risultante $Res(f, g, z)$.

Dimostrazione. Consideriamo le curve C e D definite rispettivamente da $f(x, y, z)$ e $g(x, y, z)$. Prima di tutto mostriamo che la molteplicità di intersezione può essere calcolata usando solo queste sei condizioni, dato che queste determinano $I_p(C, D)$ completamente. Dato che le condizioni sono indipendenti dalla scelta delle coordinate, possiamo assumere $p = [0, 0, 1]$. Inoltre possiamo prendere f, g irriducibili per 1 e 6, che $I_p(C, D)$ sia finito per 2 e che $I_p(C, D) = k > 0$ per 3. Infine, per induzione su k possiamo assumere che qualsiasi molteplicità di intersezione strettamente minore di k possa essere calcolata usando solo queste sei condizioni. Consideriamo i polinomi $f(x, 0, 1)$ e $g(x, 0, 1)$ in x; poniamo che abbiano grado r ed s rispettivamente. Per 1 possiamo assumere $r \leq s$. Ci sono due casi da considerare. *Caso 1:* $r = 0$. In questo caso $f(x, 0, 1)$ è costante e quindi zero, perché $f(0, 0, 1) = 0$. Dato che $f(x, y, z)$ è un polinomio omogeneo, segue che $f(x, 0, z)$ è identicamente zero, e quindi che

$$f(x, y, z) = y \cdot h(x, y, z)$$

per un qualche polinomio omogeneo $h(x, y, z)$. Inoltre possiamo scrivere

$$g(x, y, z) = g(x, 0, z) + y \cdot s(x, y, z) = x^e \cdot t(x, z) + y \cdot s(x, y, z)$$

per due polinomi omogenei $t(x, z)$ e $s(x, y, z)$ tali che $t(0, 1)$ sia diverso da zero, e un intero e, che è positivo dato che $g(0, 0, 1) = 0$. Notiamo che la condizione $t(0, 1) \neq 0$ significa che il punto $p = [0, 0, 1]$ non è sulla curva definita da $t(x, z) = 0$, e quindi, per 3, che

$$I_p(y, t(x, z)) = 0,$$

quando abbiamo, da 4,

$$I_p(y, x) = 1.$$

Mettendo insieme queste informazioni, 5 ci dice che

$$I_p(f, g) = I_p(h, g) + I_p(y, h),$$

da 6 abbiamo

$$I_p(y, g) = I_p(y, x^q \cdot t(x, z))$$

e da un uso ripetuto di 5 e 3

$$I_p(y, x^q \cdot t(x, z)) = qI_p(y, x) + I_p(y, t(x, z)) = q.$$

Quindi

$$I_p(f, g) = I_p(h, g) + q,$$

e dato che $q > 0$ la nostra ipotesi induttiva ci dice che $I_p(h, g)$ può essere calcolata usando solo le sei condizioni.

Caso 2: $r > 0$. In questo caso possiamo moltiplicare $f(x, y, z)$ e $g(x, y, z)$ per delle costanti per rendere monici i polinomi in x $f(x, 0, 1)$ e $g(x, 0, 1)$. Se n ed m sono i gradi di $f(x, y, z)$ e $g(x, y, z)$, consideriamo il polinomio

$$h(x, y, z) = z^{n+s-r} \cdot g(x, y, z) - x^{s-r} \cdot z^m \cdot f(x, y, z).$$

Questo è costruito come un polinomio omogeneo in x, y, z tale che il polinomio

$$h(x, 0, 1) = g(x, 0, 1) - x^{s-r} \cdot f(x, 0, 1)$$

in x abbia grado $t < s$. Notiamo che $h(x, y, z)$ non è identicamente nullo dato che $f(x, y, z)$ e $g(x, y, z)$ sono irriducibili e distinti. Inoltre per 1, 5 e 6

$$I_p(f, h) = I_p(f, z^{n+s-r} \cdot g) = I_p(f, g).$$

Ora rimpiazziamo f e g con f ed h (o con h ed f se $t < r$). Dopo aver ripetuto questo procedimento un numero finito di volte, raggiungiamo la situazione del caso 1.

Questo completa la parte della dimostrazione relativa all'unicità. Per provare l'esistenza, dobbiamo definire la molteplicità di intersezione $I_p(C, D)$ in questo modo:

- Se p è in una componente comune di C e D, allora $I_p(C, D) = \infty$;

- Se p non appartiene a $C \cap D$, allora $I_p(C, D) = 0$;
- Se $p \in C \cap D$ ma non è in una componente comune di C e D, prima di tutto rimuoviamo tutte le componenti comuni tra C e D e scegliamo delle coordinate in modo che (a), (b) e (c) siano soddisfatte. Se $p = [a, b, c]$ in queste coordinate, allora $I_p(C, D)$ è il più grande intero k tale che $(bz - cy)^k$ divida il risultante $Res(f, g, x)$ di f e g rispetto alla x.

Resta da mostrare che le sei condizioni vengono soddisfatte in questo modo.

1. è una conseguenza diretta del fatto che scambiando due righe di una matrice, cambia il segno del determinante, e quindi
$$Res(f, g, x) = \pm Res(g, f, x).$$
2. segue dalla definizione e dal secondo punto di 2.2.8.
3. risulta perché se $p = [a, b, c] \in C \cap D$, allora i polinomi $f(x, b, c)$ e $g(x, b, c)$ hanno una radice comune a, così per 2.2.8, il polinomio omogeneo $Res(f, g, x)$ si annulla quando $y = b$ e $z = c$. Quindi è divisibile per $bz - cy$ e $I_p(C, D) > 0$.
4. è un risultato immediato del calcolo con determinanti 2×2.
5. segue immediatamente da 2.2.9.
6. è vera perché un determinante non è modificato dalla combinazione lineare di due righe. Il risultante di f e $f \cdot h + g$ è il determinante di una matrice (s_{ij}) ottenuta da quella (r_{ij}) che definisce $Res(f, g, x)$ aggiungendo multipli scalari delle prime n righe alle ultime m. Più precisamente, se
$$h(x, y, z) = \rho_0(y, z) + \rho_1(y, z)x + ... + \rho_{n-m}(y, z)x^{n-m}$$
allora
$$s_{ij} = \begin{cases} r_{ij} & \text{se } i \leq m \\ r_{ij} + \sum_{k=i-m}^{i-n} \rho_{i-n-k} r_{kj} & \text{se } i > m \end{cases}$$

così che

$$Res(f, f \cdot h + g, x) = \det(s_{ij}) = \det(r_{ij}) = Res(f, g, x).$$

Questo completa la dimostrazione e la definizione della molteplicità di intersezione $I_p(C, D)$.

□

Osservazione 4. I punti 3 e 4 del precedente teorema ci dicono che $I_p(C, D)$ dipende solo dalle componenti di C e D che contengono p.

Possiamo definire anche la molteplicità di un punto in una curva. Conoscere la molteplicità dell'interserzione ci dà un metodo per trovare le tangenti ad una curva in un punto di cui conosciamo la molteplicità.

Definizione 4.1. Sia C una curva algebrica in $\mathbb{P}^2(\mathbb{C})$ e sia p un punto di C. Siano (x, y, z) le coordinate tali che p abbia coordinate (a, b, c) e C l'equazione $f(x, y, z) = 0$. La molteplicità $m_p(C)$ di C in p è il grado del più piccolo intero m per cui $\frac{\partial^m f}{\partial x^i y^j z^k}(a, b, c) \neq 0$, dove $m = i + j + k$;

Osservazione 5. Questa definizione porta immediatamente a due osservazioni:

- Le tangenti a C in p sono le rette t passanti per p che intersecano C con molteplicità dell'intersezione $I_p(C, t) > m_p(C)$. Contando la molteplicità, C ha esattamente $m_p(C)$ tangenti in p;

- p è un punto non-singolare di C quando $m_p(C) = 1$, p è un punto singolare di C quando $m_p(C) > 1$.

Proposizione 4.2.1. *Siano C e D curve proiettive in $\mathbb{P}^2$ e sia p un punto di $\mathbb{P}^2$. Allora $I_p(C, D) = 1$ se e solo se p è un punto non singolare di C e di D e le rette tangenti a C e D in p sono distinte.*

Lemma 4.2.2. *Se $p \in C \cap D$ è un punto singolare di C o $D \Rightarrow I_p(C, D) > 1$.*

Dimostrazione. Possiamo considerare C e D senza componenenti comuni, per poter scegliere coordinate tali che $p = [0, 0, 1]$ e valgano le condizioni $(a) - (c)$ di 2. Vogliamo mostrare che y^2 divide il risultante $Res(f, g, x)$ dei polinomi $f(x, y, z)$ e $g(x, y, z)$ che definiscono C e D. Dato che p è singolare per C, abbiamo

$$\frac{\partial f}{\partial x}(0, 0, 1) = \frac{\partial f}{\partial y}(0, 0, 1) = f(0, 0, 1) = 0.$$

$f(x, y, z)$ è una somma di monomi, tutti di grado almeno 2 nella x e nella y;

$$f(x, y, z) = a_0(y, z) + a_1(y, z) + \ldots + a_n(y, z)x^n$$

dove y^2 divide $a_0(y, z)$ e y divide $a_1(y, z)$. Inoltre, $g(0, 0, 1) = 0$ quindi

$$g(x, y, z) = b_0(y, z) + b_1(y, z)x + \ldots + b_m(y, z)x^m$$

dove y divide $b_0(y, z)$. Possiamo quindi scrivere

$$b_0(y, z) = b_{01}yz^{m-1} + y^2c_0(y, z),$$

e

$$b_1(y, z) = b_{10}z^{m-1} + yc_1(y, z)$$

per dei polinomi omogenei $c_0(y, z)$ e $c_1(y, z)$. Se $b_{01} = 0$ allora la prima colonna della matrice che determina $Res(f, g, x)$ è divisibile per y^2 e quindi y^2 divider $Res(f, g, x)$ come richiesto. Se $b_{01} \neq 0$ allora la prima colonna è divisibile per y; se estraiamo questo fattore e sottraiamo $\frac{b_{10}}{b_{01}}$ volte la prima colonna dalla seconda, allora la seconda diventa divisibile per y e quindi di nuovo y^2 divide $Res(f, g, x)$. □

Nella dimostrazione useremo anche questo lemma sul risultante

Lemma 4.2.3. *Se* $f, g \in \mathbb{C}[x]$

$$f(x) = (x - \lambda_1) \cdot \ldots \cdot (x - \lambda_n),\ g(x) = (x - \mu_1) \cdot \ldots \cdot (x - \mu_m)$$

dove $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_m$ *sono numeri complessi, allora*

$$Res(f, g, x) = \prod_{1 \leq i \leq n, 1 \leq j \leq m} (\mu_j - \lambda_i).$$

In particolare

$$Res(f, g \cdot h, x) = Res(f, g, x) \cdot Res(f, h, x)$$

dove f, g ed h sono polinomi nella x. Il risultato corrispondente è vero anche se f, g ed h sono polinomi nelle x, y e z.

Dimostrazione della Proposizione 4.2.1. Possiamo considerare C e D senza componenenti comuni, per poter scegliere coordinate tali che $p = [0, 0, 1]$ e valgano le condizioni $(a) - (c)$ di 2. Possiamo prendere p come punto non singolare di C e D. Siano $f(x, y, z)$ e $g(x, y, z)$ i polinomi che definiscono C e D. vogliamo mostrare che le rette tangenti a C e D in p coincidono se e solo se y^2 divide il risultante $Res(f, g, x)$ o equivalentemente se e solo se

$$\frac{\partial Res(f, g, x)}{\partial y}(0, 1) = 0$$

dato che $Res(f, g, x)$ è omogeneo e divisibile per y.

Per il punto (c) di 2, il punto $[1, 0, 0]$ non appartiene alla retta tangente a C in $p = [0, 0, 1]$

$$x\frac{\partial f}{\partial x}(0, 0, 1) + y\frac{\partial f}{\partial y}(0, 0, 1) + z\frac{\partial f}{\partial z}(0, 0, 1) = 0$$

quindi

$$\frac{\partial f}{\partial x}(0, 0, 1) \neq 0. \tag{4.3}$$

Per il teorema della funzione implicita applicato al polinomio $f(x, y, 1)$ in x ed y, esiste una funzione olomorfa $\lambda_1 : U \to V$ dove U e V sono intorni aperti di 0 in C tali che $\lambda_1(0) = 0$ e se $x \in V$ e $y \in U$ allora

$$f(x, y, 1) = 0 \text{ se e solo se } x = \lambda_1(y).$$

Più precisamente, $f(x, y, 1) = (x - \lambda_1(y))l(x, y)$ dove $l(x, y)$ è un polinomio in x i cui coefficienti sono funzioni olomorfe della y. Se assumiamo che il coefficiente $f(1, 0, 0)$ di x^n in $f(x, y, z)$ sia 1, allora

$$l(x, y) = \prod_{i=2}^{n}(x - \lambda_i(y))$$

dove $\lambda_1(y), ..., \lambda_n(y)$ sono le radici di $f(x, y, 1)$ considerate come polinomi in x con y fissata. Allora stesso modo, se U e V sono scelte sufficientemente piccole, c'è una funzione olomorfa $\mu_1 : U \to V$ tale che $\mu_1(0) = 0$ e possiamo scrivere

$$g(x, y, 1) = (x - \mu_1(y))m(x, y)$$

dove $m(x, y) = \prod_{i=2}^{m}(x - \mu_i(y))$ è un polinomio in x i cui coefficienti sono funzioni olomorfe della y. Allora le rette tangenti a C e D in $p = [0, 0, 1]$ sono definite dalle equazioni

$$x = \lambda_1'(0)y \text{ e } x = \mu_1'(0).$$

Se $y \in U$ allora per il lemma 4.2.3

$$Res(f, g, x)(y, 1) = (\mu_1(y) - \lambda_1(y))S(y) \tag{4.4}$$

dove $S(y) = \prod_{(i,j)\neq(1,1)}(\mu_i(y) - \lambda_j(y))$.

Notiamo che $S(y)$ è il prodotto del risultante delle coppie di polinomi $l(x, y)$ e $m(x, y)$, $l(x, y)$ e $x - \mu_1(y)$, e $m(x, y)$ e $x - \lambda_1(y)$. Quindi $S(y)$ è una funzione olomorfa di $y \in U$. Dato che $\lambda_1(0) = 0 = \mu_1(0)$, derivando l'equazione 4.4 otteniamo

$$\frac{\partial Res(f, g, x)}{\partial y}(0, 1) = (\mu_1'(0) - \lambda_1'(0))S(0).$$

Segue dalla disuguaglianza 4.3 che il polinomio $f(x, 0, 1)$ non ha radici multiple in 0, quindi se $i > 1$, allora $\lambda_i(0) \neq 0 = \mu_1(0)$ e similmente $\mu_i \neq 0 = \lambda_1(0)$. Inoltre se $\lambda_i(0) = \mu_j(0)$ per qualche $i, j > 1$ allora $[0, 0, 1]$ e $[\lambda_i(0), 0, 1] = [\mu_j(0), 0, 1]$ sono punti distinti di $C \cap D$ ed entrambi appartengono alla retta $y = 0$, e ciò contraddice il punto (b) di 2.

Quindi $S(0) \neq 0$ e $\frac{\partial Res(f,g,x)}{\partial y}(0, 1) = 0$ se e solo se $\lambda_1'(0) = \mu_1'(0)$. Cioè $I_p(C, D) > 1$ se e solo se le tangenti a C e D in p coincidono. □

4.2.2 Teorema di Bezout

Siamo ora pronti a enunciare e dimostrare una versione più completa del teorema di Bezout.

Teorema 4.2.4 (di Bezout)**.** *Siano C, D curve in $\mathbb{P}^2(\mathbb{C})$ senza componenti irriducibili in comune, e siano m ed n i gradi delle equazioni ridotte che le definiscono. Allora $\sum_{p \in C \cap D} I_p(C, D) = mn$ dove $I_p(C, D)$ è la molteplicità di intersezione di C e D in p.*

Dimostrazione. Siano $f = 0$ e $g = 0$ le equazioni ridotte di C e D, e poniamo che le coordinate siano state scelte in modo che valga:

$$(0, 0, 1) \notin C \cup D \cup \bigcup_{p \neq q \text{ in } C \cap D} L_{pq}. \tag{4.5}$$

Scriviamo $p \in C \cap D$ come $p = (u_p, v_p, w_p)$.
Affermiamo quindi che

$$Res(f, g, z) = c \prod_{p \in C \cap D} (v_p x - u_p y)^{I_p(C,D)} \tag{4.6}$$

dove c è una costante diversa da zero. Per ogni p, è chiaro che $(v_p x - u_p y)^{I_p(C,D)}$ è l'esatta potenza di $v_p x - u_p y$ che divide il risultante, questo segue dalla definizione di $I_p(C, D)$.
Abbiamo ancora bisogno di controllare che questo valga per tutte le radici della risultante. Ma se $(u, v) \in \mathbb{P}^1$ soddisfa $Res(f, g, z)(u, v) = 0$, allora 2.2.9 implica che esiste un qualche $w \in \mathbb{C}$ tale che f e g si annullano in (u, v, w). Questo accade perché se scriviamo f e g come polinomi nella z:

$$f = a_0 z^m + \ldots + a_m$$

$$g = b_0 z^n + \ldots + b_n$$

a_0 e b_0 sono costanti diverse da zero per 4.5. Quindi $(u, v, w) \in C \cap D$ e l'affermazione è provata.
Per il lemma 4.1.2, $Res(f, g, z)$ è un polinomio omogeneo non nullo di grado mn. Quindi il Teorema di Bezout risulta dimostrato confrontando i gradi dei membri dell'equazione 4.6. □

Lemma 4.2.5. *La molteplicità di intersezione di due curve in un punto $I_p(C, D)$ non dipende dalla scelta del sistema di coordinate proiettive.*

Dimostrazione. Sia (x_0, x_1, x_2) un sistema di coordinate omogenee che soddisfi le condizioni per la definizione di molteplicità, cioé che $(0,0,1) \notin C \cup D \cup \bigcup_{p,q} L_{p,q}$, dove $L_{p,q}$ è la retta che unisce i punti di intersezione p e q di C e D. Otteniamo un qualsiasi altro sistema di coordinate accettabile (x'_0, x'_1, x'_2) con una trasformazione lineare $x_i = \sum a_{ij} x'_j$, dove $A = (a_{ij})$ è una matrice di $GL(3, \mathbb{C})$. Le matrici che trasformano in sistemi di coordinate accettabili, sono precisamente quelle per cui il punto con coordinate x' $(0,0,1)$ continua a non appartenere a $C \cup D \cup \bigcup_{p,q} L_{p,q}$.

Nel sistema x, questo punto è (a_{02}, a_{12}, a_{22}). Se $h(x_0, x_1, x_2) = 0$ è l'equazione di $C \cup D \cup \bigcup_{p,q} L_{p,q}$ nel sistema x, allora l'insieme X di tutte le matrici A che portano in un sistema di coodinate accettabile, è descritto da

$$X = \{A \in GL(3, \mathbb{C}) | h(a_{02}, a_{12}, a_{22}) \neq 0\}.$$

Si può descrivere questo insieme nel modo seguente: sia $M(3 \times 3, \mathbb{C})$ l'insieme di tutte le matrici 3×3, $A = (a_{ij})$, con $a_{ij} \in \mathbb{C}$. Questo è un $\mathbb{C}^9$ con coordinate a_{ij}. Il determinante è un polinomio omogeneo $d(a_{ij})$ di grado 3 nelle a_{ij}.

Sia $p(a_{ij}) = d(a_{ij}) \cdot h(a_{02}, a_{12}, a_{22})$. Allora:

$$X = \{(a_{ij}) \in M(3 \times 3, \mathbb{C}) | p(a_{ij}) \neq 0\}.$$

Cioè X è in complementare di una ipersuperficie affine nello spazio di dimensione 9, $M(3 \times 3, \mathbb{C}) = \mathbb{C}^9$. X è uno spazio topologico connesso come sottospazio di $\mathbb{C}^9$.

Ora possiamo provare che la molteplicità d'intersezione è indipendente dalle coordinate scelte. Sia $x = Ax'$. Per la connessione di X, possiamo trovare una curva continua A_t, $0 < t < 1$ in X con $A_0 = 1$, $A_1 = A$. Un sistema di coordinate accettabile $x_t = (x_{t,0}, x_{t,1}, x_{t,2})$ è definito per ciascun t da $A_t x_t$. Se sostituiamo questo nelle equazioni $f(x) = 0$ e $g(x) = 0$ di C e D rispettivamente, allora otteniamo le equazioni $f_t(x_t) = 0$ e $g_t(x_t) = 0$ di C e D relativamente alle coordinate x_t.

Consideriamo il risultante $Res(f_t, g_t, x_{t,2})$. Per costruzione, $Res_t(x_2) = Res(f_t, g_t, x_2)$ è una famiglia di polinomi omogenei di grado $m \cdot n$ in una sola

variabile, con la seguente proprietà: il numero degli zeri distinti $c_i(t)$ di R_t (senza contare la molteplicità) è costante (uguale cioé al numero di punti di intersezione distinti p_i di C e D, a cui corrispondono mediante proiezione). Da questo segue che anche la molteplicità degli zeri $c_i(t)$ di R_t, che dipende in modo continuo da t, è costante. Ciò è immediato, per la seguente proposizione si polinomi in una variabile:

Sia $f \in \mathbb{C}[x]$ un polinomio di grado d e sia $c \in \mathbb{C}$ uno zero di f di molteplicità ν. Sia $c > 0$ così piccolo che tutti gli altri zeri abbiano distanza maggiore di ϵ da x. Allora esiste un $\delta > 0$ per ϵ tale che qualunque polinomio i cui coefficienti differiscano da quelli di f per meno di δ, abbia esattamente ν zeri nel disco di raggio ϵ attorno a c, contando le molteplicità.

Questo prova che la molteplicità degli zeri $c_i(t)$, e con questa la molteplicità di intersezione di C e D in p_i rispetto al sistema di coordinate x_t, è indipendente da t. Quindi la molteplicità di intersezione di due curve è indipendente dal sistema di coordinate scelto. □

Osservazione 6. Usare il risultante, che è una caratteristica globale della curva, per determinare la molteplicità di un punto di intersezione, che invece è solo locale, non è molto elegante, ma è il metodo più semplice.

Osservazione 7. La dimostrazione di 4.2.1 può essere estesa per mostrare che in generale $I_p(C, D) \geq m_p(C)m_p(D)$ dove $m_p(C)$ ed $m_p(D)$ sono le molteplicità di C e D in p. L'uguaglianza vale se e solo se C e D non hanno rette tangenti in comune.

Corollario 4.2.6. *Siano C e D curve proiettive in $\mathbb{P}^2$ di grado n ed m. Supponiamo che ogni $p \in C \cap D$ sia un punto non singolare di C e D e che le rette tangenti di C e D in p siano distinte. Allora l'intersezione $C \cap D$ consiste di esattamente nm punti.*

Dimostrazione. Risulta immediatamente considerando 4.2.4 e 4.2.1. □

Proposizione 4.2.7. *Se consideriamo due curve C e D composte da più componenti irriducibili C_i e D_j con molteplicità (grado del polinomio cor-*

rispondente nella scomposizione) n_i *ed* m_j *avremo che*

$$I_p(C, D) = \sum n_i m_j I_p(C_i, D_j).$$

Dimostrazione. Consideriamo una curva come somma delle sue componenti connesse moltiplicate per le rispettive molteplicità $C = n_1C_1 + ... + n_rC_r$. Scriviamo $F_i = 0$ come equazione di C_i e quindi avremo che l'equazione di C è $F_1^{n_1} \cdot ... \cdot F_r^{n_r} = 0$.

Se prendiamo due curve $C = \sum n_iC_i$ e $D = \sum m_jD_j$ senza componenti comuni, per trovare $I_p(C, D)$, basterà sommare le molteplicità di intersezione delle componenti C_i e D_j in p, perché ogni componente irriducibile può essere considerata come una curva a se che non modifica la molteplicità di intersezione delle altre. □

4.3 Generalizzazione del teorema di Bezout a varietà di $\mathbb{P}^n(\mathbb{C})$

Possiamo generalizzare il Teorema di Bezout a varietà che si intersecano in spazi proiettivi di dimensione maggiore di 2. Nel caso l'intersezione delle varietà sia composta da soli punti, l'espressione resta sostanzialmente la stessa.

Per poter fare questo, abbiamo bisogno di determinare la molteplicità di intersezione di più superfici in uno stesso punto mediante la seguente definizione.

Definizione 4.2. Chiamiamo localizzazione in un punto $p \in \mathbb{P}^n(\mathbb{K})$ dell'insieme dei polinomi omogenei in $\mathbb{K}[x_0, ..., x_n]$ l'insieme degli elementi del tipo $\frac{a}{s}$, dove $a \in \mathbb{K}[x_0, ..., x_n]$ omogeneo ed s polinomio omogeneo in $\mathbb{K}[x_0, ..., x_n]\backslash\mathfrak{p}$ (dove $\mathfrak{p}$ è l'ideale omogeneo di $\mathbb{K}[x_0, ..., x_n]$ costituito dai polinomi che si annullano in p) con $\deg s = \deg a$.

Denoteremo questo insieme come $\mathcal{O}_{\mathbb{P}^n(\mathbb{K}),p}$.

Teorema 4.3.1. *Siano $f_1, ..., f_n$ dei polinomi omogenei in $n+1$ variabili, che definiscono le ipersuperfici $V_1 = V(f_1), ..., V_n = V(f_n)$ in $\mathbb{P}^n(\mathbb{C})$; se $V_1 \cap ... \cap V_n = K$ è un numero finito di punti, abbiamo:*

$$deg(f_1) \cdot ... \cdot deg(f_n) = \sum_{p \in K} I_p(V_1, ..., V_n).$$

dove $I_p(V_1, ..., V_n)$ è definita come $\dim_{\mathbb{C}} \frac{\mathcal{O}_{\mathbb{P}^n(\mathbb{C}),p}}{(f_1,...,f_n)_p}$.

Per la dimostrazione rimandiamo a [6] teor 2 pag 6.

Questo teorema generalizza il Teorema di Bezout ad ipersuperfici in $\mathbb{P}^n(\mathbb{C})$, la cui intersezione sia formata solo da punti isolati, ma possiamo generalizzare anche alle coppie di sottovarietà di dimensione minore rispetto alle ipersuperfici, mediante una generalizzazione della nozione di grado.

Definizione 4.3. A qualunque sottovarietà $X \subset \mathbb{P}^n(\mathbb{C})$ di dimensione r si può associare un intero $d(X)$, il suo grado, tale che per tutti i sottospazi lineari L di dimensione $n-r$ che soddisfino:

1. $L \cap X = \{M_1, ..., M_k\}$ è un insieme finito di punti;
2. $\forall i = 1, ..., k$ M_i è un punto liscio di X e lo spazio tangenti T_{X,M_i} ed L si intersecano trasversalmente, cioé il generato dalla loro somma è tutto $\mathbb{P}^n(\mathbb{C})$;

si abbia $k = d(X)$.

Ora possiamo dare una versione del Teorema di Bezout per sottovarietà irriducibili di $\mathbb{P}^n(\mathbb{C})$ la cui intersezione sia formata da k componenti irriducibili.

Teorema 4.3.2 (Teorema di Bezout)**.** *Siano X ed Y due sottovarietà di $\mathbb{P}^n(\mathbb{C})$ di dimensioni r ed s, sia $X \cap Y = W_1 \cup ... \cup W_k$ la scomposizione in componenti irriducibili dell'intersezione. Supponiamo:*

- *$\forall i = 1, ..., k$ W_i è di dimensione $r + s - n$;*

- $\forall i = 1, ..., k$ *esiste* $M_i \in W_i$*, punto non singolare per* X *ed* Y *e tale che* $\dim\left(T_{X,M_I} \cap T_{Y,M_i}\right) = r + s - n$.

Allora $deg(X)\dot{deg}(Y) = \sum_{i=1}^{k} deg(W_i)$.

Questo teorema può essere ulteriormente generalizzato definendo la molteplicità di intersezione $I_{W_i}(X, Y)$ di X ed Y lungo W_i.

Per la dimostrazione rimandiamo a [5] pag 80.

Capitolo 5

Un'applicazione dell'eliminazione proiettiva: la forma di Chow

Mostriamo ora un'altra applicazione della teoria dell'eliminazione proiet¡3tiva: il calcolo della forma e della varietà di Chow di una varietà in $\mathbb{P}^n$.

Cominciamo ricordando la definizione Grassmanniana.

Definizione 5.1. Dati $k, n \in \mathbb{N}$, $k > n$, denotiamo con $\mathbb{G}(k, n)$ l'insieme di tutti i sottospazi di dimensione k di $\mathbb{P}^n$ e lo chiameremo Grassmanniana dei sottospazi k-dimensionali di $\mathbb{P}^n$.

Osservazione 8. La Grassmanniana $\mathbb{G}(k, n)$ contiene $\mathbb{K}^{k(n-k)}$ come sottoinsieme aperto e quindi ha dimensione $k(n-k)$. Vedi [12] pag. 138.

Definizione 5.2. Sia X una varietà proiettiva irriducibile k-dimensionale in $\mathbb{P}^n$. La varietà di Chow di X è:

$$Z_X = \{L \in \mathbb{G}(n-k-1, n) \text{ dove } L \cap X \neq \emptyset\}.$$

Vediamo ora che la varietà di Chow è un'ipersuperficie di $\mathbb{G}(n-k-1, n)$:

Proposizione 5.0.3. *Data una varietà X di $\mathbb{P}^{n-1}$ di grado d e dimensione $n-k-1$, la sua varietà di Chow Z_X è un'ipersuperficie irriducibile di grado d in $\mathbb{G}(n-k,n)$.*

Dimostrazione. La varietà Z_X è inclusa nel diagramma:

$$Z_X \xleftarrow{q} B(X) \xrightarrow{p} X$$

dove $B(X)$ è la varietà delle coppie (x, L) tali che $x \in X$, $L \in \mathbb{G}(n-k,n)$ ed $x \in L$ e siano q e p le proiezioni canoniche. Risulta $Z_X = q(B(X))$. Date le rispettive dimensioni, un generico sottospazio proiettivo $(n-k-1)$dimensionale che interseca X, lo incontra in un solo punto. Quindi q è un isomorfismo birazionale. La controimmagine mediante p di $x \in X$ è isomorfa alla Grassmanniana $\mathbb{G}(n-k-1, n-1)$. Quindi se X è irriducibile, allora lo sono anche $B(X)$ e Z_X. Inoltre abbiamo

$$\dim Z_X = \dim B(X) = (n-k-1)k + (k-1) = k(n-k) - 1 =$$

$$\dim \mathbb{G}(n-k,n) - 1$$

Per trovare il grado di $Z_X \subset \mathbb{G}(n-k,n)$, dovremmo scegliere una generica catena crescente di sottospazi proiettivi $N \subset M \subset \mathbb{P}^{n-1}$, tali che $\dim N = n-k-2$, $\dim M = n-k$, e contare il numero dei sottospazi $(n-k-1)$dimensionali $L \in Z_X$ che soddisfano $N \subset L \subset M$. Ma dato che $\deg X = d$, l'intersezione $M \cap X$ sarà costituita di d punti, $x_1, ..., x_d$. I sottospazi $L \in Z_X$ che contengono N e contenuti in M saranno i sottospazi proiettivi generati da N e dagli x_i presi uno alla volta. Quindi il loro numero sarà uguale a d come richiesto. Questo prova la proposizione. □

Quindi Z_X è una ipersuperficie in $\mathbb{G}(n-k-1,n)$ definita da un solo polinomio di grado d, R_X, detto Forma di Chow.

Sia $\mathcal{B} = \bigoplus \mathcal{B}_m$ l'anello delle coordinate della Grassmanniana $\mathbb{G}(n-k,n)$. Scegliendo una base in $\mathcal{B}_d$, possiamo associare X all'insieme di coordinate di R_X in questa base. Queste coordinate sono dette coordinate di Chow di X.

Proposizione 5.0.4. *Una sottovarietà irriducibile di dimensione* $(k-1)$*,* $X \subset \mathbb{P}^{n-1}$ *è univocamente determinata dalla sua varietà di Chow* Z_X*. Più precisamente, un punto* $p \in \mathbb{P}^{n-1}$ *è in* X *se e solo se qualunque sottospazio di dimensione* $(n-k-1)$ *contenente* p*, appartiene a* Z_X*.*

Dimostrazione. La dimostrazione è ovvia, date la definizione di Z_X e la proposizione precedente. □

Vediamo ora alcuni esempi di forme di Chow di varietà

Esempio 5.1 (Ipersuperfici)**.** Sia $X \subset \mathbb{P}^n$ un'ipersuperficie definita dal polinomio f. Allora $k = n-1$, e quindi $Z_X \subset \mathbb{G}(0,n)$ è costituita da punti di $\mathbb{P}^n$, perché $\mathbb{G}(0,n) = \mathbb{P}^n$. L'insieme di punti che intersecano X è solo X stesso. Quindi per un'ipersuperficie X,

$$Z_X = X$$

e la forma di Chow è f stessa.

Esempio 5.2 (Un punto in $\mathbb{P}^n$)**.** Sia $p = (a_0, ..., a_n) \in \mathbb{P}^n$. Allora Z_p è l'insieme di iperpiani di $\mathbb{P}^n$ che passano per p. Ogni iperpiano L è definito dall'annullarsi di una singola equazione

$$L(x) = b_0x_0 + ... + b_nx_n.$$

Quindi possiamo usare $(b_0, ..., b_n)$ come coordinate di L in $\mathbb{G}(n-1,n)$. Se L contiene p dobbiamo avere che $L(p) = 0$, cioé $a_0b_0 + ... + a_nb_n = 0$. Quindi Z_X è l'iperpiano in $\mathbb{G}(n-1,n)$ definito dall'annullarsi della forma di Chow

$$R_p = a_0b_0 + ... + a_nb_n.$$

Esempio 5.3 (m punti in $\mathbb{P}^n$)**.** Sia $X = \{p_1, ..., p_m\}$ un insieme di m punti di $\mathbb{P}^n$. Allora Z_X è l'insieme di iperpiani che contengono almeno uno dei p_i. Quindi Z_X sarà l'unione dei vari Z_{p_i}, e la forma di Chow è il polinomio di grado m dato dai prodotti delle forme di Chow: $R_X = R_{p_1} \cdot ... \cdot R_{p_n}$.

Esempio 5.4. Andiamo ora a calcolare la varietà di Chow della retta proiettiva in $\mathbb{P}^3$. In pratica questo consiste nell'individuare quali rette di $\mathbb{P}^3$ intersechino la retta data.

Nel caso che stiamo per considerare, la varietà di Chow sarà all'interno di $\mathbb{G}(1,3)$: l'insieme delle rette proiettive in $\mathbb{P}^3$. Definiamo le coordinate di Plücker per questo caso:

Definizione 5.3. Fissiamo una retta L in $\mathbb{P}^3$ mediante la scelta di due punti, $x = [a_{00}, a_{01}, a_{02}, a_{03}]$ e $y = [a_{10}, a_{11}, a_{12}, a_{13}]$. Formiamo la matrice $M = \begin{bmatrix} a_{00} & a_{10} \\ a_{01} & a_{11} \\ a_{02} & a_{12} \\ a_{03} & a_{13} \end{bmatrix}$ e i minori $p_{ij} = \begin{vmatrix} a_{0i} & a_{1i} \\ a_{0j} & a_{1j} \end{vmatrix} = a_{0i}a_{1j} - a_{0j}a_{1i}$. Diremo che le coordinate omogenee $[p_{01}, p_{02}, p_{12}, p_{03}, p_{13}, p_{23}]$ sono le coordinate di Plücker di L in $\mathbb{G}(1,3)$. In questo modo $\mathbb{G}(1,3)$ viene considerato come un sottoinsieme di $\mathbb{P}^5$.

Possiamo definire anche l'immersione di Plücker

$$\begin{array}{rccc} \alpha: & \mathbb{G}(1,3) & \to & \mathbb{P}^5 \\ & L & \mapsto & L^\alpha \end{array}$$

dove $L^\alpha = [p_{01}, p_{02}, p_{12}, p_{03}, p_{13}, p_{23}]$.

Queste coordinate ci danno un metodo per controllare che due rette in $\mathbb{P}^3$ si intersechino:

Osservazione 9. Due rette in $\mathbb{P}^3$ sono o sghembe o complanari, e nel secondo caso o coincidono o hanno un solo punto in comune. Se p_{ij} e p'_{ij} sono le coordinate di Plücker delle due rette, allora queste sono complanari quando

$$\begin{vmatrix} a_{00} & a_{10} & b_{00} & b_{10} \\ a_{01} & a_{11} & b_{01} & b_{11} \\ a_{02} & a_{12} & b_{02} & b_{12} \\ a_{03} & a_{13} & b_{03} & b_{13} \end{vmatrix} = p_{01}p'_{23} - p_{02}p'_{13} + p_{03}p'_{12} + p_{23}p'_{01} - p_{13}p'_{02} + p_{12}p'_{03} = 0$$

Possiamo quindi determinare la forma di Chow di una retta di $\mathbb{P}^3$:

Sia $\mathbb{K}$ un campo algebricamente chiuso, sia $\mathbb{P}^3$ lo spazio proiettivo tridimensionale su $\mathbb{K}$. Fissiamo una retta L in $\mathbb{P}^3$. La retta generica di $\mathbb{P}^3$ non interseca L. Così le rette di $\mathbb{P}^3$ che intersecano L formano un sottoinsieme proprio $C(L)$ della grassmaniana delle rette in $\mathbb{P}^3$.

Proviamo ora a descrivere questo sottoinsieme. Siano $\sum_{i=0}^{3} a_{0i}x_i$ e $\sum_{i=0}^{3} a_{1i}x_i$ i due polinomi che generano $I(L)$, l'ideale di L. Sia L' una retta di $\mathbb{P}^3$ definita dai due polinomi $\sum_{i=0}^{3} b_{0i}x_i$ e $\sum_{i=0}^{3} b_{1i}x_i$. Allora L ed L' si intersecano se e solo se si annulla il determinante della matrice

$$\Lambda = \begin{bmatrix} a_{00} & a_{10} & b_{00} & b_{10} \\ a_{01} & a_{11} & b_{01} & b_{11} \\ a_{02} & a_{12} & b_{02} & b_{12} \\ a_{03} & a_{13} & b_{03} & b_{13} \end{bmatrix}.$$

Per $0 \leq i < j \leq 3$, siano

$$p_{ij} = a_{0i}a_{1j} - a_{1i}a_{0j} \text{ e } p'_{ij} = b_{0i}b_{1j} - b_{1i}b_{0j}$$

sappiamo che $\det(\Lambda) = 0$ se e solo se

$$F = p_{01}p'_{23} - p_{02}p'_{13} + p_{03}p'_{12} + p_{12}p'_{03} - p_{13}p'_{02} + p_{23}p'_{01} = 0$$

Ricordiamo che l'immersione di Plucker da $\mathbb{G}(1,3)$ a $\mathbb{P}^5$ è definita come

$$L' \mapsto [p'_{01}, p'_{02}, p'_{12}, p'_{03}, p'_{13}, p'_{23}] = [X_0, ..., X_5].$$

Consideriamo l'anello $\mathbb{K}[b_{00}, ..., b_{13}, X_0, ..., X_5]$ e l'ideale

$$I = \langle X_0 - p'_{01}, X_1 - p'_{02}, X_2 - p'_{12}, X_3 - p'_{03}, X_4 - p'_{13}, X_5 - p'_{23}, F \rangle$$

Sia $J = I \cap \mathbb{K}[X_0, ..., X_5] = I_8$, l'ottavo ideale eliminazione. Allora $J = \langle Q, F' \rangle$, dove

$$Q = X_0X_5 - X_1X_4 + X_2X_3$$

$$F' = p_{01}X_5 - p_{02}X_4 + p_{03}X_3 + p_{12}X_2 - p_{13}X_1 + p_{23}X_0$$

Notiamo che Q è l'equazione che definisce $\mathbb{G}(1,3)$ (basta effettuare le sostituzioni), così $C(L)$ può essere vista come un'ipersuperficie in $\mathbb{G}(1,3)$.

Questa ipersuperficie è chiamata varietà di Chow di L, e il polinomio lineare F' è la forma di Chow di L.

Esempio 5.5. Conoscere la forma di Chow di una retta di $\mathbb{P}^3$ porta altri risultati, per esempio, ci assicura che, date L_1, L_2, L_3 ed L_4 rette sghembe a due a due, esisteranno due sole rette che le intersecano tutte e 4. Dimostriamo prima l'esistenza e poi controlliamo il numero di queste rette:

Supponiamo che esista una retta L che interseca tutte le L_i. Allora L può essere considerata come un punto in $\mathbb{G}(1,3)$. Dato che L interseca L_1, L_2, L_3 ed L_4, il punto corrispondente in $\mathbb{G}(1,3)$ è contenuto nella varietà di Chow di ognuna delle rette. Denotiamo con F_i la forma di Chow di L_i, con $i = 1,2,3,4$. Allora l'intersezione delle varietà di Chow è definita dall'ideale $I = (Q, F_1, F_2, F_3, F_4)$, dove Q è l'equazione che definisce $\mathbb{G}(1,3)$ in $\mathbb{P}^5$. Dato che l'ideale è generato da 5 polinomi, la varietà corrispondente $V(I)$ non può essere vuota. Dalla scelta generica delle rette sghembe, possiamo aspettarci che $\{Q, F_1, F_2, F_3, F_4\}$ sia un insieme generatore minimale per I. In questo caso, $(\dim(V(I))) = 0$, cioé $V(I)$ è un insieme finito di punti.

Per determinare in numero delle rette L, notiamo che $\deg(\mathbb{G}(1,3)) = 2$ perché è definito da $Q = X_0X_5 - X_1X_4 + X_2X_3$, polinomio di grado 2. Le forme di Chow F_1, F_2, F_3 ed F_4 definiscono una retta in $\mathbb{P}^5$ e questa retta incontra $V(Q)$ esattamente in due punti, perché altrimenti sarebbe contenuta in $V(Q)$ e ci sarebbe una quantità infinita di rette che intersecano le 4 rette e ciò contraddirrebbe l'osservazione precedente. Quindi il numero di punti in $V(I)$ sarà 2.

Bibliografia

[1] Cox, David; Little, John; O'Shea, Donal Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra. Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2007.

[2] Fulton, W. (2008) Algebraic Curves,
www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf .

[3] Kirwan, Frances Complex algebraic curves. London Mathematical Society Student Texts, 23. Cambridge University Press, Cambridge, 1992.

[4] Brieskorn, Egbert; Knörrer, Horst Plane algebraic curves. Translated from the German by John Stillwell. Birkhäuser Verlag, Basel, 1986.

[5] Mumford, David Algebraic geometry. I. Complex projective varieties. Reprint of the 1976 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1995.

[6] Dieudonne J.A. (1985) Le théorème de Bezout, Nice, Prepublication mathématiques.

[7] Hassett, Brendan. Introduction to algebraic geometry. Cambridge University Press, Cambridge, 2007.

[8] Gelfand, I. M.; Kapranov, M. M.; Zelevinsky, A. V. Discriminants, resultants, and multidimensional determinants. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 1994.

[9] Lien, T. Notes on Chow Forms,
http://www.math.wisc.edu/ lien/research/chowforms.pdf

[10] Peterson, C. & Abo, H. Chow Forms
http://www.webpages.uidaho.edu/∼abo/research/smi/sample-solution8.pdf

[11] Atiyah, M. F.; Macdonald, I. G. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969

[12] Harris, Joe Algebraic geometry. A first course. Graduate Texts in Mathematics, 133. Springer-Verlag, New York, 1992.