Indice

Introduzione

L'argomento della presente tesi è costituito dalle Basi di Groebner e da talune loro applicazioni; tra le quali la cosiddetta Teoria dell'eliminazione.

Le Basi di Groebner sono un utile strumento per risolvere alcuni problemi computazionali che si incontrano in ambito algebrico ed algebrico-geometrico.

Infatti, nell'anello dei polinomi in più di una variabile $k[x_1, \ldots, x_n]$, con k campo algebricamente chiuso, già il problema dell'appartenenza di un polinomio ad un ideale dato non è di soluzione immediata, il che è dovuto alla mancanza di un algoritmo di divisione efficiente come nel caso di una variabile.

Sempre attraverso le basi di Groebner è possibile risolvere computazionalmente problemi quali, ad esempio, la determinazione dell'intersezione di due ideali oppure la ricerca dei punti di una data varietà affine.

La definizione delle basi di Groebner risale all'austriaco Buchberger (1942). Esse sono dei particolari sistemi di generatori per un ideale $I \subset k[x_1, \ldots, x_n]$, con la proprietà che i loro leading monomials generano l'ideale iniziale di I. Questo fatto permette di generalizzare, opportunamente, l'algoritmo di divisione nel caso più generale di polinomi a più variabili.
Tali basi possono, inoltre, essere determinate algoritmicamente.

Nel corso della tesi, dopo avere definito le basi di Groebner e avere descritto l'algoritmo per determinarle, ci proporremo di affrontare i seguenti problemi:

- l'*appartenenza di un polinomio ad un ideale* I: dato $f \in k[x_1, \ldots, x_n]$ e dato l'ideale I, se f appartiene o meno ad I.

- la *risoluzione di sistemi di equazioni polinomiali*: è un problema strettamente connesso alla ricerca dei punti di una varietà affine, rappresentata, appunto, da un sistema di equazioni polinomiali; daremo una risoluzione di ciò all'interno del capitolo dedicato alla Teoria dell'Eliminazione, servendoci di due teoremi, il Teorema dell'Estensione e ed il Teorema dell'Eliminazione.

- l'*implicitazione*: è detto così il processo della costruzione di una rappresentazione implicita di una varietà, a partire da una rappresentazione parametrica; otterremo tale processo adoperando il Teorema di Eliminazione.

La tesi è suddivisa in tre capitoli.

Nel primo capitolo, introdurremo gli ordinamenti monomiali, descriveremo l'algoritmo di divisione in $k[x_1, \ldots, x_n]$ ed infine definiremo il concetto di ideale monomiale, una tipologia di ideale, per il quale il problema della descrizione, grazie al Lemma di Dickson, risulterà essere molto semplice da risolvere.

Nel capitolo successivo, daremo la definizione di base di Groebner, ne descriveremo le proprietà più importanti, daremo un criterio operativo per riconoscerle ed un algoritmo per costruirle.

L'ultima parte della tesi sarà dedicata alla Teoria dell'eliminazione, la quale ci permetterà di risovere il problema della determinazione dei punti di una qualsiasi varietà affine, tramite le basi di Groebner e i cosiddetti ideali di eliminazione. Introdurremo anche il concetto di risultante di due o più polinomi al fine di provare il Teorema dell'estensione, che ci consentirà di risolvere in un numero finito di passi un sistema di equazioni polinomiali.

1 Algoritmo di divisione in $k[x_1, \ldots, x_n]$

1.1 Ordinamenti sui monomi

In questa sezione, cercheremo di estendere l'algoritmo di divisione definito in $k[x]$ all'anello dei polinomi $k[x_1, \ldots, x_n]$.

È stato visto che uno dei requisiti più importanti di un algoritmo di divisione è che esso termini dopo un numero finito di passi: affinché ciò accada, nel caso ad una variabile, si sfrutta il fatto che due qualsiasi monomi sono confrontabili secondo l'ordinamento dato dal loro grado, e, difatti, in ogni passo di tale algoritmo, il grado diminuisce.

Ora, il nostro scopo è quello di ordinare i termini dei polinomi nell'anello $k[x_1, \ldots, x_n]$, in modo tale che gli ordinamenti così creati soddisfino ben determinate proprietà, che garantiscono la compatibilità con la struttura di anello di $k[x_1, \ldots, x_n]$.

Diamo alcune definizioni preliminari.

Definizione 1.1 *Un* ***monomio*** *in $x_1, \ldots, x_n$ è un prodotto della forma*

$$x_1^{\alpha(1)} \cdots x_n^{\alpha(n)},$$

dove tutti gli esponenti $\alpha(1), \ldots, \alpha(n)$ sono interi non negativi.

Definizione 1.2 *Sia $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$, se $a_\alpha \neq 0$, $a_\alpha x^\alpha$ è detto* ***termine*** *di f.*

Considerato un monomio $x^\alpha = x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$, ad esso possiamo associare una n-upla $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Si stabilisce, in tal modo, una corrispondenza biunivoca tra i monomi di $k[x_1, \ldots, x_n]$ e gli elementi di $\mathbb{N}^n$; questo implica che ogni ordinamento $\geq$ sullo spazio $\mathbb{N}^n$ ci restituisce un ordinamento sui monomi:

$$x^\alpha \geq x^\beta \iff \alpha \geq \beta.$$

Ci sono diversi modi di definire ordinamenti su $\mathbb{N}^n$, ma noi vogliamo che essi siano compatibili con la struttura algebrica degli anelli dei polinomi: innanzitutto, essendo i polinomi somme finite di monomi è necessario che questi ultimi si possano ordinare, in modo unico e non ambiguo, in modo crescente o decrescente. Per ottenere ciò, richiediamo che l'ordinamento sia

totale, cioè che per ogni coppia di monomi x^α e x^β, solo e soltanto una delle seguenti tre affermazioni sia vera:

$$x^\alpha < x^\beta, \qquad x^\alpha = x^\beta, \qquad x^\alpha > x^\beta.$$

Inoltre, nel prodotto tra due polinomi o, più semplicemente, nel prodotto di un monomio con un polinomio, vorremmo che si mantenga il termine massimo, ovvero che sia soddisfatta la seguente proprietà: se $x^\alpha \geq x^\beta$, allora anche $x^\alpha x^\gamma \geq x^\beta x^\gamma$; in termini di n-uple appartenenti a $\mathbb{N}^n$, tale proprietà si traduce nella seguente:

$$\alpha \geq \beta \Longrightarrow \quad \alpha + \gamma \geq \beta + \gamma, \ \forall\ \gamma \in \mathbb{N}^n.$$

Fatte queste considerazioni, diamo la seguente definizione:

Definizione 1.3 *Un* ***ordinamento monomiale*** $\geq$ *su* $k[x_1, \ldots, x_n]$ *è una qualsiasi relazione su* $\mathbb{N}^n$*, o, equivalentemente, una qualunque relazione sull'insieme dei monomi* x^α*, con* $\alpha \in \mathbb{N}^n$*, soddisfacente i seguenti tre requisiti:*

(i) La relazione $\geq$ *è un ordinamento totale su* $\mathbb{N}^n$*.*

(ii) Se $\alpha \geq \beta$ *e* γ *in* $\mathbb{N}^n$*, allora* $\alpha + \gamma \geq \beta + \gamma$*.*

(iii) La relazione $\geq$ *è un buon ordinamento su* $\mathbb{N}^n$*. Questo significa che ogni insieme non vuoto di* $\mathbb{N}^n$ *ha un elemento minimo secondo* $\geq$*.*

Il seguente lemma ci fornisce un'altra condizione di buon ordinamento:

Lemma 1.4 *Una relazione d'ordine totale* $\geq$ *su* $\mathbb{N}^n$ *è un buon ordinamento se e solo se ogni successione strettamente decrescente in* $\mathbb{N}^n$

$$\alpha(1) > \alpha(2) > \cdots$$

termina (ovvero esiste un i *tale che* $\alpha(i) = \alpha(j)$*, per ogni* $j \geq i$*).*

Dimostrazione
Dimostriamo l'enunciato equivalente: $\geq$ non è un buon ordinamento su $\mathbb{N}^n$ se e solo se esiste una successione strettamente decrescente in $\mathbb{N}^n$.
Se $\geq$ non è un buon ordinamento, allora esiste un sottoinsieme non vuoto S di $\mathbb{N}^n$, non dotato di minimo: sia $\alpha(1) \in S$, non essendo il minimo, possiamo trovare $\alpha(2) \in S$, tale che $\alpha(1) > \alpha(2)$ e, poichè neanche $\alpha(2)$ è il minimo per S, possiamo trovare un $\alpha(3) \in S$, tale che $\alpha(2) > \alpha(3)$. Iterando tale

procedimento, è possibile costruire una catena strettamente decrescente in $\mathbb{N}^n$.
Viceversa, data una successione infinita strettamente decrescente, l'insieme $\{\alpha(1), \alpha(2), \dots\}$ è un insieme non vuoto di $\mathbb{N}^n$ privo di minimo, quindi $\geq$ non è un buon ordinamento. □

Diamo, ora, alcuni esempi di ordinamenti monomiali.

Definizione 1.5 (Ordinamento Lessicografico) *Sia $\alpha = (\alpha_1, \dots, \alpha_n)$ e $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}^n$. Definiamo $\alpha >_{lex} \beta$, se nel vettore $\alpha - \beta \in \mathbb{Z}^n$, la componente non nulla più a sinistra è positiva. In tal caso, scriveremo $x^\alpha >_{lex} x^\beta$.*

Diamo qualche esempio:
a. $(2, 2, 0) >_{lex} (1, 2, 5)$ perchè $\alpha - \beta = (1, 0, -5)$;
b. $(1, 2, 5) >_{lex} (1, 2, 3)$ perchè $\alpha - \beta = (0, 0, 2)$;
c. le variabili $x_1, \dots, x_n$ sono ordinate nel seguente modo:

$$x_1 >_{lex} x_2 >_{lex} \cdots >_{lex} x_n;$$

infatti $(1, 0, \dots, 0) >_{lex} (0, 1, \dots, 0) >_{lex} \cdots >_{lex} (0, 0, \dots, 1)$.

Proviamo che l'ordinamento lessicografico è effettivamente un ordinamento monomiale:

Proposizione 1.6 *L'ordinamento lessicografico (chiamato più usualmente Lex order) su $\mathbb{N}^n$ è un ordinamento monomiale.*

Dimostrazione
(i) Il lex order è un ordinamento totale a causa del fatto che lo è l'usuale relazione di ordine in $\mathbb{N}$.
(ii) Se $\alpha >_{lex} \beta$, allora la componente non nulla più a sinistra di $\alpha - \beta$ è positiva; poiché, in $\mathbb{Z}^n$, $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, anche $\alpha + \gamma >_{lex} \beta + \gamma$.
(iii) Supponiamo per assurdo che $(\mathbb{N}^n, >_{lex})$ non sia un insieme ben ordinato; a causa del Lemma 1.4, esiste una successione infinita strettamente decrescente di elementi di $\mathbb{N}^n$

$$\alpha(1) > \alpha(2) > \cdots \quad .$$

Sia $\alpha_1(i)$ la prima componente della n-upla $\alpha(i)$; per definizione di ordinamento lessicografico, la successione $(\alpha_1(i))_{i \in \mathbb{N}}$ è non crescente ed è costituita

da interi non negativi; poiché l'usuale relazione di ordine su $\mathbb{N}$ è un buon ordinamento, tale successione dovrà stabilizzarsi, ovvero esiste k tale che $\alpha_1(k) = \alpha_1(i)$, per ogni $i \geq k$. In modo analogo, a partire da $\alpha(k)$, le seconde componenti $\alpha_2(i)$ formano una successione non crescente in $\mathbb{N}$, che dovrà stabilizzarsi. Continuando così, si arriverà ad un indice l, per cui $\alpha(l) = \alpha(l+1)$ e questo è un assurdo poiché la successione di vettori $\alpha(i)$ è strettamente decrescente. □

Osservazione 1.7 *È importante notare che vi sono tanti ordini lessicografici quanti sono i modi di ordinare le variabili $x_1, \ldots, x_n$, ovvero $n!$ modi.*

Osservazione 1.8 *Secondo l'ordinamento lessicografico, una variabile domina su ogni monomio in cui compaiono le variabili successive, indipendentemente dal grado dei due monomi a confronto.*

Definizione 1.9 (Graded Lex Order) *Siano α e β due n-uple di $\mathbb{N}^n$. Definiamo $\alpha >_{grlex} \beta$ se*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \quad \textit{oppure} \quad |\alpha| = |\beta| \quad e \quad \alpha >_{lex} \beta.$$

Anche in questo caso le variabili risultano ordinate nel seguente modo $x_1 >_{grlex} x_2 >_{grlex} \cdots >_{grlex} x_n$; inoltre si prova facilmente il seguente risultato:

Proposizione 1.10 *Il Graded Lex Order è un ordinamento monomiale.*

Diamo, infine, la definizione di un altro ordinamento monomiale:

Definizione 1.11 (Graded Reverse Lex Order) *Siano $\alpha, \beta \in \mathbb{N}^n$. Diciamo che $\alpha >_{grevlex} \beta$ se*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \quad \textit{oppure} \quad |\alpha| = |\beta|$$

e, in $\alpha - \beta \in \mathbb{N}^n$, la componente non nulla più a destra è negativa.

Osservazione 1.12 *Per evidenziare la differenza che vi è tra il grlex ed il grevlex, notiamo che entrambi usano il grado dei monomi nella stessa maniera, ma, in caso di uguaglianza tra gradi, il primo considera la variabile più grande e favorisce le potenze maggiori, il secondo, invece, considera la variabile più piccola e favorisce le potenze minori.*

Esempio 1.13 $x^5yz^3 >_{grlex} x^4y^3z^2$, *invece* $x^5yz^3 <_{grevlex} x^4y^3z^2$.

Una volta definito un ordinamento monomiale $\geq$, dato un polinomio $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x^n]$, possiamo ordinare i suoi monomi in modo non ambiguo rispetto a $\geq$: ovviamente, l'ordine dei monomi del nostro polinomio può essere diverso a secondo dell'ordinamento monomiale scelto.

Nel resto della tesi, useremo la seguente terminologia:

Definizione 1.14 *Sia* $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ *un polinomio non nullo e sia* $\geq$ *un ordinamento monomiale.*

(i) Il ***multigrado*** *di* f *è:*

$$multideg(f) = max\{\alpha \in \mathbb{N}^n \ : \ a_\alpha \neq 0\}$$

(il massimo è preso rispetto all'ordinamento monomiale scelto).

(ii) Il ***leading coefficient*** *di* f *è*

$$LC(f) = a_{multideg(f)} \in k.$$

(iii) Il ***leading monomial*** *di* f *è*

$$LM(f) = x^{multideg(f)}.$$

(iv) Il ***leading term*** *di* f *è*

$$LT(f) = LC(f) \cdot LM(f).$$

Lemma 1.15 *Siano* $f, g \in k[x_1, \ldots, x_n]$ *due polinomi non nulli. Allora:*

1. *multideg(fg)=multideg(f)+multideg(g).*
2. *Se* $f + g \neq 0$, *allora* $multideg(f + g) \leq max(multideg(f), multideg(f))$.

Inoltre, se $multideg(f) \neq multideg(g)$, *si ha che*

$$multideg(f + g) = max(multideg(f), multideg(f)).$$

1.2 Algoritmo di Divisione

Vogliamo, ora, generalizzare l'algoritmo di divisione, noto per i polinomi ad una variabile, al caso di più variabili. Il nostro obiettivo sarà quello di dividere $f \in k[x_1, \ldots, x_n]$ per $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Ciò significa esprimere f nella forma

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

dove i quozienti $a_1, \ldots, a_s$ ed il resto r stanno in $k[x_1, \ldots, x_n]$.

Per comprendere come funziona l'algoritmo di divisione facciamo dapprima due esempi:

Esempio 1.16 *Siano $f = xy^2 + 1$, $f_1 = xy + 1$, $f_2 = y + 1$; useremo il Lex Order, con $x > y$. Costruiamo il seguente schema:*

$$\begin{array}{rl} a_1: & \\ a_2: & \\ xy+1 & \sqrt{xy^2+1} \\ y+1 & \end{array}$$

I leading terms di f_1 e di f_2 dividono entrambi $LT(f) = xy^2$, ma prima divideremo f per f_1, per via dell'ordine in cui li abbiamo messi nella tabella; successivamente divideremo il resto ottenuto per f_2:

$$\begin{array}{rll} a_1: y & & \\ a_2: -1 & & \\ xy+1 & \sqrt{xy^2+1} & \\ y+1 & \underline{xy^2+y} & \\ & -y+1 & \\ & \underline{-y-1} & \\ & 2 & \end{array}$$

Quindi otteniamo:

$$xy^2 + 1 = y \cdot (xy + 1) - 1 \cdot (y + 1) + 2.$$

Esempio 1.17 *A volte capita che il leading term del resto parziale, che, d'ora in poi, chiameremo* dividendo intermedio*, non è diviso da nessun leading term dei polinomi divisori; in questo caso, è necessario, creare un'altra colonna, nella quale vanno posti tali leading terms. Questa colonna è detta colonna del resto. Vogliamo, ora, dividere* $f = x^2y + xy^2 + y^2$ *per* $f_1 = xy - 1$ *e* $f_2 = y^2 - 1$*; useremo, anche in questo caso, il Lex Order, con* $x > y$*.*

$$
\begin{array}{ll}
a_1 : x + y & \\
a_2 : & \\
xy - 1 \qquad & \sqrt{x^2y + xy^2 + y^2} \\
y^2 - 1 \qquad & \underline{x^2y - x} \\
& \qquad xy^2 + x + y^2 \\
& \qquad \underline{xy^2 - y} \\
& \qquad\quad x + y^2 + y
\end{array}
$$

Notiamo che nessuno dei leading terms dei divisori divide $LT(x+y^2+y) = x$*, sebbene* $x + y^2 + y$ *non sia il resto della divisione, dal momento che* $LT(f_2)$ *divide* y^2*. Occorre spostare* x *nella colonna del resto, come segue:*

$$
\begin{array}{lll}
a_1 : x + y & & \\
a_2 : & & \underline{r} \\
xy - 1 \qquad & \sqrt{x^2y + xy^2 + y^2} & \\
y^2 - 1 \qquad & \underline{x^2y - x} & \\
& \qquad xy^2 + x + y^2 & \\
& \qquad \underline{xy^2 - y} & \\
& \qquad\quad \underline{x + y^2 + y} & \\
& \qquad\quad\ y^2 + y \quad \rightarrow \quad x &
\end{array}
$$

Continuamo a dividere per $LT(f_1)$ *o per* $LT(f_2)$ *e, se non è possibile, spostiamo il leading term del dividendo intermedio nella colonna del resto. Infine,*

otteniamo:

$$
\begin{array}{lll}
a_1 : x+y & & \\
a_2 : & & \underline{\quad r \quad} \\
xy-1 \qquad & \sqrt{x^2y+xy^2+y^2} & \\
y^2-1 \qquad & \underline{x^2y-x\qquad\qquad} & \\
& \quad xy^2+x+y^2 & \\
& \quad \underline{xy^2-y\qquad\qquad} & \\
& \qquad x+y^2+y & \\
& \qquad \underline{y^2+y\qquad\qquad} & \to\ x \\
& \qquad\quad y^2-1 & \\
& \qquad\quad \underline{y+1} & \\
& \qquad\qquad \underline{1} & \to\ x+y \\
& \qquad\qquad 0 & \to\ x+y+1
\end{array}
$$

Dunque, abbiamo ottenuto che il resto della divisione è $x+y+1$.

Teorema 1.18 (Algoritmo di Divisione) *Fissato un ordinamento monomiale* $\geq$ *su* $\mathbb{N}^n$*, sia* $F = (f_1, \ldots, f_s)$ *una* s*-upla ordinata di polinomi in* $k[x_1, \ldots, x_n]$*. Allora ogni* $f \in k[x_1, \ldots, x_n]$ *può essere scritto come*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

dove $a_i,\ r \in k[x_1, \ldots, x_n]$*, ed* $r = 0$ *oppure* r *è una combinazione lineare, con coefficienti in* k*, di monomi, nessuno dei quali divisibile per qualche* $LT(f_1), \ldots, LT(f_s)$*. Chiameremo* r *il* ***resto*** *di* f *nella divisione per* F*. Inoltre, se* $a_i f_i \neq 0$*, abbiamo che*

$$multideg(f) \geq multideg(a_i f_i).$$

Dimostrazione
Proveremo l'esistenza dei quozienti a_i e di r dando l'algoritmo per la loro costruzione.

Input : $f_1, \ldots, f_s, f$
Output : $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots;\ a_s := 0;\ r := 0$
$p := f$
$WHILE\ p \neq 0\ DO$
$\quad i := 1$
$\quad divisionoccurred := false$
$\quad WHILE\ i \leq s\ AND\ divisionoccurred = false\ DO$
$\quad\quad IF\ \mathrm{LT}(f_i)\ divide\ \mathrm{LT}(p)\ THEN$
$\quad\quad\quad a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
$\quad\quad\quad p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
$\quad\quad\quad divisionoccurred := true$
$\quad\quad ELSE$
$\quad\quad\quad i := i + 1$
$\quad IF\ divisionoccurred = false\ THEN$
$\quad\quad r := r + \mathrm{LT}(p)$
$\quad\quad p := p - \mathrm{LT}(p)$

Nell'algoritmo la variabile p rappresenta il dividendo intermedio di cui abbiamo parlato nel precedente esempio, mentre la variabile r rappresenta la colonna dei resti. Infine , la variabile booleiana *divisionoccurred* ci dice quando qualcuno dei $\mathrm{LT}(f_i)$ divide il leading term del dividendo intermedio. Notiamo, inoltre, che all'interno del WHILE ...DO principale, si possono avere due diverse procedure:

- (Division step) Se qualcuno dei $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$, allora l'algoritmo procede come nel caso ad una variabile.
- (Remainder step) Se nessuno dei $\mathrm{LT}(f_i)$ divide $\mathrm{LT}(p)$, allora l'algoritmo aggiunge $\mathrm{LT}(p)$ al resto.

Una volta dato l'algoritmo, per provare che esso funziona, proviamo che

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{1}$$

si verifica ad ogni passo dell'algoritmo: al primo passo evidentemente la (1) è vera; supponiamo che tale equazione sia verificata ad un passo dell'algoritmo, allora al passo successivo abbiamo: se tale passo è un division step, esiste un indice i per cui $\mathrm{LT}(f_i)/\mathrm{LT}(p)$ e perciò si ha che

$$a_i f_i + p = \left(a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i + p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i = a_i f_i + p,$$

quindi $a_i f_i + p$ rimane invariato; poiché le altre variabili in tale division step non vengono toccate, la (1) rimane verificata; se invece tale passo è un remainder step, allora p ed r cambieranno, ma la loro somma rimarrà invariata, dato che $p - \mathrm{LT}(p) + r + \mathrm{LT}(p) = p + r$, quindi l'uguaglianza (1) rimane verificata.

Notiamo che l'algoritmo termina quando $p = 0$, ed in tal caso la (1) diviene:

$$f = a_1 f_1 + \cdots + a_s f_s + r \tag{2}$$

e, poiché vengono aggiunti in r solo i $\mathrm{LT}(p)$ che non sono divisibili per nessun $\mathrm{LT}(f_i)$, r risulta esser una combinazione lineare di monomi, nessuno dei quali divisibile per qualche $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$.

Dobbiamo verificare che effettivamente l'algoritmo termini dopo un numero finito di passi:
se si effettua un division step $p' = p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$ ha multigrado strettamente minore di p, essendo $\mathrm{LT}((\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i) = (\mathrm{LT}(p)/\mathrm{LT}(f_i))\mathrm{LT}(f_i) = \mathrm{LT}(p)$; se, per contro, si effettua un remainder step, $p' = p - \mathrm{LT}(p)$ e se $p' \neq 0$, il multigrado di p' è strettamente minore di quello di p.

In ogni caso, il multigrado decresce ad ogni passo: se per assurdo l'algoritmo non terminasse, avremmo una successione infinita strettamente decrescente di multigradi in $\mathbb{N}^n$, ma essendo $(\mathbb{N}^n, \geq)$ un insieme ben ordinato, ciò non può accadere. L'algoritmo, dunque, termina in un numero finito di passi. □

Osservazione 1.19 *Se nel caso dell'algoritmo di divisione in $k[x]$, il resto era univocamente determinato, in questo caso, la situazione è ben più complessa: difatti, il resto nella divisione di un polinomio $f \in k[x_1, \ldots, x_n]$ per*

un insieme non ordinato $F = \{f_1, \ldots, f_s\}$ può cambiare in funzione dell'ordine dei polinomi divisori. Fissato, però, tale ordine, il resto è univocamnete determinato.

Osservazione 1.20 *Ovviamente se $I = \langle f_1, \ldots, f_s \rangle$ è un ideale dell'anello $k[x_1, \ldots, x_n]$ ed $f = a_1 f_1 + \cdots + a_s f_s$, allora $f \in I$; esistono polinomi $f \in I$, tali che il resto r nella divisione di f per $(f_1, \ldots, f_s)$ sia non nullo; in questo caso si ha che anche $r \in I$. Questo problema non si verifica nel caso ad una variabile, in cui $f \in I = \langle g \rangle$ se e soltanto se $r = 0$, dove r è il resto della divisione di f per g. Quindi uno dei nostri scopi è ottenere un risultato simile anche nel caso a più variabili, per fare ciò avremo bisogno di un particolare insieme di generatori per I.*

Esempio 1.21 *Sia $f_1 = xy + 1$, $f_2 = y^2 - 1 \in k[x, y]$. Adoperando il Lex Order, con $x > y$, e dividendo $f = xy^2 - x$ per l'insieme ordinato $F = (f_1, f_2)$, otteniamo*

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y).$$

Tuttavia, dividendo per $F = (f_2, f_1)$, si ha

$$xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0.$$

Quindi, $f \in \langle f_1, f_2 \rangle$, sebbene nella prima divisione sia stato trovato un resto non nullo.

1.3 Ideali Monomiali e Lemma di Dickson

Definizione 1.22 *Un ideale $I \subseteq k[x_1, \ldots, x_n]$ si dice **ideale monomiale** se esiste $A \subset \mathbb{N}^n$ (possibilmente infinito), tale che I sia costituito da tutti e soli i polinomi che sono somme finite della forma $\sum_{\alpha \in A} h_\alpha x^\alpha$ dove gli $h_\alpha \in k[x_1, \ldots, x_n]$. In questo caso, scriviamo $I = \langle x^\alpha \ : \ \alpha \in A \rangle$. In altre parole, I può essere generato da un insieme (eventualmente infinito) di monomi.*

Diamo adesso una caratterizzazione di tutti i monomi che stanno in un dato ideale monomiale I.

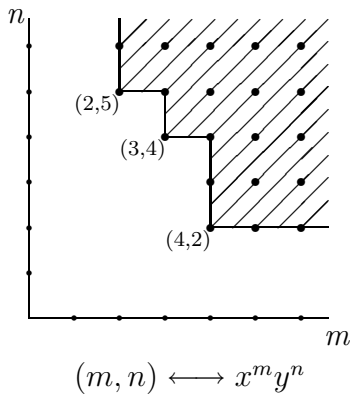
Lemma 1.23 *Sia $I = \langle x^\alpha \ : \ \alpha \in A \rangle$ un ideale monomiale, allora un monomio $x^\beta \in I$ se e solo se x^β è divisibile per qualche x^α, con $\alpha \in A$.*

Dimostrazione
Se x^β è divisibile per x^α, con $\alpha \in A$, per definizione di ideale, $x^\beta \in I$. Viceversa, se $x^\beta \in I$, allora $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ con $h_i \in k[x_1, \ldots, x_n]$ e $\alpha(i) \in A$; sviluppando i prodotti, dopo avere scritto gli h_i come combinazione lineare di monomi, si trova che nel secondo membro dell'equazione ogni termine è divisibile per qualche x^{α_i}. Poiché x^β coincide con uno degli addendi del secondo membro, anch'esso deve godere della stessa proprietà. □

Osservazione 1.24 *Notiamo che l'insieme di tutti i monomi divisibili per* x^α *è* $\{x^\beta |\ \beta \in \alpha + \mathbb{N}^n\} = \{x^\beta |\ \beta = \alpha + \gamma \text{ con } \gamma \in \mathbb{N}^n\}$. *Quindi, in virtù del Lemma 1.23 e di questa osservazione, possiamo rappresentare graficamente i monomi che giacciono in un dato ideale monomiale. Vediamo alcuni esempi: sia* $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$, *allora gli esponenti dei monomi di* I *formano l'insieme*

$$((4,2) + \mathbb{N}^2) \cup ((3,4) + \mathbb{N}^2) \cup ((2,5) + \mathbb{N}^2);$$

graficamente tale insieme è quello evidenziato nella seguente figura.



$$(m,n) \longleftrightarrow x^m y^n$$

Lemma 1.25 *Sia* I *un ideale monomiale e sia* $f \in k[x_1, \ldots, x_n]$*; le seguenti affermazioni sono equivalenti:*

1. $f \in I$.
2. *Ogni termine di* f *giace in* I.
3. f *è una combinazione lineare a coefficienti in* k *dei monomi di* I.

Dimostrazione
(1. $\Rightarrow$ 2.) Se $f \in I$, allora $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$ con $h_i \in k[x_1, \ldots, x_n]$ e $\alpha(i) \in A$. Scrivendo gli h_i come combinazioni lineari di monomi e sviluppando i prodotti, otteniamo una combinazione lineare di monomi, ognuno dei quali è divisibile per qualche $x^{\alpha(i)}$, e quindi, per il Lemma 1.23, sta in I. Le altre due implicazioni, (2. $\Rightarrow$ 3.) e (3. $\Rightarrow$ 1.), sono banali. $\square$

Come conseguenza di ciò, abbiamo il seguente risultato:

Corollario 1.26 *Due ideali monomiali sono uguali se e solo se contengono gli stessi monomi.*

Teorema 1.27 (Lemma di Dickson) *Un ideale monomiale dell'anello di polinomi $k[x_1, \ldots, x_n]$, $I = \langle x^\alpha \ : \ \alpha \in A \rangle$, è generato da un numero finito di monomi, ovvero può essere scritto come $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$ con $\alpha(1), \ldots, \alpha(s) \in A$. In particolare, I è finitamente generato.*

Dimostrazione
Proviamo il teorema per induzione sul numero n di variabili.
Se $n = 1$, allora I è generato dai monomi x_1^α, con $\alpha \in A \subset \mathbb{N}$. Sia β il più piccolo elemento di A; poiché $\beta \leq \alpha$, per ogni $\alpha \in A$, x_1^β divide ogni x_1^α e quindi $I = \langle x_1^\beta \rangle$.
Sia, ora, $n > 1$ e supponiamo il teorema vero per $n - 1$. In questo caso, per semplicità, scriveremo le variabili come $x_1, \ldots, x_{n-1}, y$, così i monomi di $k[x_1, \ldots, x_{n-1}, y]$ saranno scritti come $x^\alpha y^m$ con $\alpha \in \mathbb{N}^{n-1}$ e $m \in \mathbb{N}$.
Supponiamo che I sia un ideale monomiale di $k[x_1, \ldots, x_{n-1}, y]$; sia J l'ideale monomiale generato dai monomi x^α, tali che, per qualche m, $x^\alpha y^m \in I$: essendo J un ideale monomiale di $k[x_1, \ldots, x_{n-1}]$, possiamo applicare l'ipotesi induttiva ed ottenere che $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, con gli $\alpha(i)$ tali che, per ogni i, esiste $m_i \in \mathbb{N}$ con la proprietà $x^{\alpha(i)} y^{m_i} \in I$.
Fissati gli m_i, per ogni $i = 1, \ldots, n-1$, sia m il più grande di tali m_i e, per ogni $h = 0, \ldots, m-1$ consideriamo $J_h \in k[x_1, \ldots, x_{n-1}]$ generato dai monomi x^β tali che $x^\beta y^h \in I$: usando nuovamente l'ipotesi induttiva, si ottiene che $J_h = \langle x^{\alpha_h(1)}, \ldots, x^{\alpha_h(s_h)} \rangle$.
Il nostro scopo è quello di provare che I è generato dai monomi della seguente

lista:

$$\begin{aligned}
\text{da } J &: x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m \\
\text{da } J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)} \\
\text{da } J_1 &: x^{\alpha_1(1)}y, \ldots, x^{\alpha_1(s_1)}y \\
&\vdots \\
\text{da } J_{m-1} &: x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}.
\end{aligned}$$

In primo luogo, notiamo che ogni monomio $x^\alpha y^p$ di I è divisibile per uno di questa lista: se $p \geq m$, allora, a causa della costruzione di J, esiste $i \in \{1, \ldots, s\}$, tale che $x^\alpha y^p$ è diviso da $x^{\alpha(i)}y^m$; se invece $p \leq m-1$, per la costruzione di J_p, $x^\alpha y^p$ è diviso da $x^{\alpha_p(j)}y^p$. Usando, infine, il Lemma 1.23 ed il Corollario 1.26, si ha che i monomi della lista generano un ideale che ha gli stessi monomi di I e che perciò coincide con I.
Per completare la dimostrazione, occorre far vedere che da ogni sistema di generatori per I è possibile estrarre un sistema di generatori finito per tale ideale. Sia $I = \langle x^\alpha \ : \ \alpha \in A\rangle \subset k[x_1, \ldots, x_n]$; per quanto abbiamo appena detto $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)}\rangle$, per opportuni monomi $x^{\beta(i)}$ in $I = \langle x^\alpha \ : \ \alpha \in A\rangle$; dal Lemma 1.23 si ha che $x^{\beta(i)}$ è divisibile per qualche $x^{\alpha(i)}$ con $\alpha(i) \in A$, quindi $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)}\rangle$. □

Osservazione 1.28 *Esiste un unico sistema di generatori minimale.*
Infatti, per assurdo, siano $\langle x^{\alpha(1)}, \ldots, x^{\alpha(t)}\rangle$ e $\langle x^{\beta(1)}, \ldots, x^{\beta(s)}\rangle$ due sistemi minimali distinti di generatori per I; allora, per ogni $x^{\beta(i)}$, esiste $\alpha(j)$ tale che $x^{\alpha(j)}$ divide $x^{\beta(i)}$; inoltre, sempre per definizione di base, esiste $\beta(h)$ tale che $x^{\beta(h)}$ divide $x^{\alpha(j)}$, il che implica che $x^{\beta(i)}$ è un multiplo di $x^{\beta(h)}$, contro l'ipotesi di minimalità della base $\langle x^{\beta(1)}, \ldots, x^{\beta(s)}\rangle$.

2 Definizione e proprietà delle Basi di Groebner

2.1 Teorema della Base di Hilbert e Basi di Groebner

Nel seguito, daremo una risoluzione completa al problema della *descrizione degli ideali*. Questo ci porterà alla costruzione di basi che hanno buone proprietà rispetto all'algoritmo di divisione descritto nel precedente capitolo.

Definizione 2.1 *Sia $I \subset k[x_1, \ldots, x_n]$ un ideale non nullo.*

(i) Denotiamo con $LT(I)$, l'insieme di tutti i leading terms degli elementi di I. Dunque,

$$LT(I) = \{cx^\alpha \ : \ \exists \ f \in I \, con \ LT(f) = cx^\alpha\}.$$

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

Notiamo che dato un sistema finito di generatori per I, ovvero $I = \langle f_1, \ldots, f_s\rangle$, gli ideali $\langle \mathrm{LT}(I)\rangle$ e $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle$ possono essere differenti: difatti, $\langle \mathrm{LT}(I)\rangle \supseteq \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)\rangle$, ma non sempre vale il viceversa, come mostra il seguente esempio.

Esempio 2.2 *Sia $I = \langle f_1, f_2\rangle$, dove $f_1 = x^3 - 2xy$ ed $f_2 = x^2y - 2y^2 + x$; come ordinamento sui monomi di $k[x, y]$ scegliamo il grlex. Abbiamo*

$$x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2,$$

quindi $x^2 = LT(x^2) \in \langle LT(I)\rangle$, ma non appartiene a $\langle LT(f_1), LT(f_2)\rangle$, come si nota utilizzando il Lemma 1.23.

Proposizione 2.3 *Sia $I \subset k[x_1, \ldots, x_n]$ un ideale.*

1. *L'ideale $\langle LT(I)\rangle$ è monomiale.*
2. *Esistono $g_1, \ldots, g_s \in I$ tali che $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$.*

Dimostrazione
1. I leading monomials $\mathrm{LM}(g)$ con $g \in I \setminus \{0\}$, generano un ideale monomiale $\langle \mathrm{LM}(g) \ : \ g \in I \setminus \{0\} \rangle$. Dal momento che $\mathrm{LM}(g)$ e $\mathrm{LT}(g)$ differiscono per una costante non nulla, $\langle \mathrm{LM}(g) \ : \ g \in I - \{0\} \rangle = \langle \mathrm{LT}(I) \rangle$, quindi $\langle \mathrm{LT}(I) \rangle$ è un ideale monomiale.
2. Essendo $\langle \mathrm{LT}(I) \rangle$ generato dai monomi $\mathrm{LM}(g)$ con $g \in I \setminus \{0\}$, il Lemma di Dickson ci garantisce che $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t) \rangle$, per qualche $g_1, \ldots, g_t \in I$, ma poiché $\mathrm{LM}(g_i)$ differisce da $\mathrm{LT}(g_i)$ per una costante non nulla, si ha che $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. □

Possiamo ora usare l'algoritmo di divisione e la Proposizione 2.3 per provare l'esistenza di un sistema finito di generatori per *ogni* ideale.

Teorema 2.4 (Teorema della Base di Hilbert) *Sia I un ideale dell'anello $k[x_1, \ldots, x_n]$; allora I ha un sistema finito di generatori, ovvero esistono $g_1, \ldots, g_s \in I$ tali che $I = \langle g_1 \ldots, g_s \rangle$.*

Dimostrazione
Se $I = \{0\}$, il sistema di generatori che possiamo prendere è $\{0\}$, che è certamente finito. Se I è diverso dall'ideale nullo, possiamo costruire un sistema finito di generatori per I, $g_1, \ldots, g_s$ come segue. Per la Proposizione 2.3, esistono $g_1, \ldots, g_s \in I$ tali che $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, vogliamo provare che $I = \langle g_1, \ldots, g_s \rangle$.

Chiaramente $\langle g_1, \ldots, g_s \rangle \subseteq I$. Viceversa, sia $f \in I$, applichiamo l'algoritmo di divisione per dividere f per $\{g_1, \ldots, g_s\}$, allora otteniamo un'espressione della forma

$$f = a_1 g_1 + \cdots + a_t g_t + r,$$

in cui nessun termine di r è divisibile per $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Se per assurdo $r \neq 0$, essendo $r = f - (a_1 g_1 + \cdots + a_t g_t)$ un elemento di I, allora $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$, e quindi, per il Lemma 1.23, $\mathrm{LT}(r)$ deve essere divisibile per qualche $\mathrm{LT}(g_i)$. Questo contraddice la definizione di resto, dunque $r = 0$ ed $I \subseteq \langle g_1 \ldots, g_s \rangle$. □

Definizione 2.5 *Fissato un ordinamento monomiale, un sottoinsieme finito di un ideale I, $G = \{g_1, \ldots, g_s\}$, si dice* ***base di Groebner*** *(o* ***base standard****) se*

$$\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle.$$

Equivalentemente, un insieme $\{g_1, \ldots, g_s\} \subseteq I$ è una base di Groebner per I se e solo se il leading term di ogni elemento di I è divisibile per uno dei $\mathrm{LT}(g_i)$.

Corollario 2.6 *Fissato un ordinamento monomiale, ogni ideale $I \neq \{0\}$ di $k[x_1, \ldots, x_n]$ ha un base di Groebner. Inoltre, ogni base di Groebner per I è una base dell'ideale.*

Dimostrazione
La base $\{g_1, \ldots, g_s\}$ costruita nel Teorema 2.4 è una base di Groebner per costruzione, e, sempre per il Teorema 2.4, essa è anche una base per I. □

Il Teorema della base di Hilbert è equivalente al seguente:

Teorema 2.7 (Condizione sulle catene ascendenti) *Sia*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

una catena ascendente di ideali in $k[x_1, \ldots, x_n]$, allora esiste un $N \geq 1$ tale che

$$I_N = I_{N+1} = I_{N+2} = \cdots .$$

2.2 Proprietà delle Basi di Groebner

In precedenza, abbiamo visto che ogni ideale non nullo $I \subset k[x_1, \ldots, x_n]$ ha una base di Groebner. Ora scopriremo quali sono le proprietà di tali basi e come esse possono risultare utili all'interno dell'algoritmo di divisione.

Proposizione 2.8 *Sia $G = \{g_1, \ldots, g_s\}$ una base di Groebner per un ideale $I \subset k[x_1, \ldots, x_n]$ e sia $f \in k[x_1, \ldots, x_n]$. Allora esiste un unico $r \in k[x_1, \ldots, x_n]$ soddisfacente le seguenti due proprietà:*

1. *Nessun termine di r è divisibile per qualche $LT(g_i)$.*
2. *Esiste $g \in I$ tale che $f = g + r$.*

In particolare, il resto r della divisione di f per G non dipende dal modo in cui i polinomi $g_1, \ldots, g_s$ sono ordinati.

Dimostrazione
Dall'algoritmo di divisione si ottiene immediatamente l'uguaglianza $f = a_1g_1 + \cdots + a_sg_s + r$, con r soddisfacente la condizione 1.; d'altra parte, basta porre $g = a_1g_1 + \cdots + a_sg_s \in I$, per avere assicurata anche la condizione 2.
Resta da provare l'unicità del resto r: supponiamo, per assurdo, che esista $r' \neq r$ che soddisfi le condizioni 1. e 2., cioè che esista $g' \in I$ tale che $f = g' + r'$ e nessun termine di r' è divisibile per qualche $\mathrm{LT}(g_i)$. Allora $r - r' = g' - g \in I$, e, poiché $r - r' \neq 0$, ne segue $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle$. Dal Lemma 1.23 segue che $\mathrm{LT}(r - r')$ è divisibile per qualche $\mathrm{LT}(g_i)$, il che è impossibile dato che nessun termine di r e di r' è divisibile per qualcuno dei $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$. Quindi $r - r' = 0$ e l'unicità è provata. □

Il resto r è detto la *forma normale di* f e, sebbene esso sia unico, non sono tali i quozienti $a_1, \ldots, a_s$, i quali cambiano, dipendentemente da come ordiniamo nella divisione i generatori $g_1, \ldots, g_s$.

Osservazione 2.9 *Ci chiediamo adesso se il resto r, soddisfacente le condizioni 1. e 2. della precedente proposizione, cambia al variare della base di Groebner G scelta per l'ideale I. La risposta è negativa: difatti, siano date due basi di Groebner per I, $G_1 = \{g_1, \ldots, g_s\}$ e $G_2 = \{p_1, \ldots, p_t\}$, per ciascuna di esse esiste un resto soddisfacente le condizioni della Proposizione 2.8, siano essi r_1 ed r_2 e supponiamoli, per assurdo, distinti. Sappiamo che nessun termine di r_1 è divisibile per qualche $LT(g_i)$, in modo anologo, nessun termine di r_2 è divisibile per qualche $LT(p_j)$; inoltre, esistono h_1 ed h_2 appartenenti ad I tali che*

$$f = h_1 + r_1 \quad e \quad f = h_2 + r_2,$$

da cui $r_1 - r_2 = h_2 - h_1 \in I$, il che implica che $LT(r_1 - r_2) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$. Il resto r_1, per la condizione 1., è tale che nessuno dei suoi termini appartiene a quest'ultimo ideale ed inoltre nessuno dei termini di r_2 è divisibile per qualche $LT(g_i)$, perché, se così fosse, essendo $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(p_1), \ldots, LT(p_t) \rangle$, dovrebbe anche essere divisibile per qualche $LT(p_j)$, il che è un assurdo. Dunque, affinché $LT(r_1 - r_2)$ stia in $\langle LT(I) \rangle$, deve accadere che $r_1 = r_2$.

Come corollario otteniamo il seguente criterio di appartenenza di un polinomio ad un ideale:

Corollario 2.10 *Sia $G = \{g_1, \ldots, g_t\}$ una base di Groebner per un ideale $I \subset k[x_1, \ldots, x_n]$ e sia $f \in k[x_1, \ldots, x_n]$. Allora $f \in I$ se e solo se il resto nella divisione di f per G è nullo.*

Dimostrazione
Se il resto è nullo, allora abbiamo osservato che $f \in I$. Viceversa, se $f \in I$, $f = f + 0$ soddisfa le condizioni della Proposizione 2.8 e, a causa dell'unicità dei resti nella divisione per una base di Groebner, 0 è il resto nella divisione di f per G. □

Usando il precedente corollario, supposto di avere una base di Groebner per un ideale I, il *problema dell'appartenenza di un polinomio a tale ideale* è risolto.

Il nostro scopo è ora quello di trovare una base di Groebner per un dato ideale. Abbiamo bisogno di alcune definizioni.

Definizione 2.11 *Noi denoteremo con $\overline{f}^F$ il resto della divisione di f per la s-upla ordinata $F = (f_1, \ldots, f_s)$. Inoltre, se F è una base di Groebner per $\langle f_1, \ldots, f_s \rangle$, possiamo riguardare F come un insieme di elementi, senza un ordine particolare.*

Dato un ideale I, è stato osservato che il difetto principale che una sua qualsiasi base $F = \{f_1, \ldots, f_s\}$ ha, rispetto ad una base di Groebner, è che possono esistere combinazioni degli f_i tali che il loro leading terms non stiano in $\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$, pur stando in $\langle \mathrm{LT}(I) \rangle$: ad esempio può accadere che i leading terms di un'opportuna combinazione $ax^\alpha f_i - bx^\beta f_j$ si cancellino, lasciando solo i termini più piccoli.

Per studiare il fenomeno della cancellazione, introduciamo delle speciali combinazioni.

Definizione 2.12 *Siano $f, g \in K[x_1, \ldots, x_n]$ due polinomi non nulli.*

*(i) Se multideg$(f) = \alpha$ e multideg$(g) = \beta$, sia $\gamma = (\gamma_1, \ldots, \gamma_n)$, dove $\gamma_i = max(\alpha_i, \beta_i)$, per ogni i. Chiamiamo **minimo comune multiplo** (least common multiple) di $LT(f)$ e di $LT(g)$ il monomio x^γ, denotato con $LCM(LT(f), LT(g))$.*

*(ii) L'**S-polinomio** di f e g è la combinazione*

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

Un S-polinomio è un polinomio creato appositamente per dar luogo ad una cancellazione dei leading terms.
Anzi, con il prossimo lemma, vediamo che una qualsiasi cancellazione dei leading terms di due polinomi aventi lo stesso multigrado è riconducibile agli S-polinomi.

Lemma 2.13 *Supponiamo di avere una somma* $\sum_{i=1}^{s} c_i f_i$, *dove* $c_i \in k$ *e* $multideg(f_i) = \delta \in \mathbb{N}^n$, *per ogni* i. *Se* $multideg(\sum_{i=1}^{s} c_i f_i) < \delta$, *allora* $\sum_{i=1}^{s} c_i f_i$ *è una combinazione lineare a coefficienti in* k *degli* S*-polinomi* $S(f_j, f_h)$, *con* $1 \leq j, h \leq s$. *Inoltre, ogni* $S(f_j, f_h)$ *ha multigrado minore di* δ.

Dimostrazione
Sia $d_i = \mathrm{LC}(f_i)$ e quindi $c_i d_i = \mathrm{LC}(c_i f_i)$. Dal fatto che $\mathrm{multideg}(c_i f_i) = \delta$ e che $\mathrm{multideg}(\sum_{i=1}^{s} c_i f_i) < \delta$, segue che $\sum_{i=1}^{s} c_i d_i = 0$. Poniamo $p_i = f_i/d_i$; chiaramente p_i è monico. Consideriamo la somma telescopica:

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \\ &\quad (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s.\end{aligned}$$

Essendo $\mathrm{LT}(f_i) = d_i x^\delta$, $\mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_h)) = x^\delta$. Dunque

$$S(f_j, f_h) = \frac{x^\delta}{\mathrm{LT}(f_j)} \cdot f_j - \frac{x^\delta}{\mathrm{LT}(f_h)} \cdot f_h = \frac{x^\delta}{d_j x^\delta} \cdot f_j - \frac{x^\delta}{d_h x^\delta} \cdot f_h = p_j - p_h. \quad (3)$$

Usando questa equazione ed il fatto che $\sum_{i=1}^{s} c_i d_i = 0$, la precedente somma telescopica diventa:

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + \\ &\quad (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s),\end{aligned}$$

che è la combinazione lineare da noi desiderata. Infine, dal momento che p_j e p_h hanno lo stesso multigrado δ e sono monici, la differenza $p_j - p_h$ ha multigrado $< \delta$. A causa della (3), ciò vale anche per $S(f_j, f_h)$, ed il lemma è provato. □

Usando gli S-polinomi e il Lemma 2.13, possiamo provare il seguente criterio dovuto a Buchberger, per decretare quando una data base per un ideale è una base di Groebner.

Teorema 2.14 (Buchberger's S-pair criterion) *Sia I un ideale polinomiale. Una base $G = \{g_1, \ldots, g_t\}$ di I è una base di Groebner se e solo se, per ogni $i \neq j$, il resto nella divisione di $S(g_i, g_j)$ per G è zero.*

Dimostrazione
Se G è una base di Groebner per I, allora, essendo $S(g_i, g_j) \in I$, per il Corollario 2.10, il resto nella divisione per G deve essere nullo.

Viceversa, sia $f \in I$ un polinomio non nullo. Vogliamo provare che, se il resto nella divisione di $S(g_i, g_j)$ per G è zero, allora

$$\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle.$$

Il polinomio f sta in I, quindi

$$f = \sum_{i=1}^{t} h_i g_i. \tag{4}$$

Dal Lemma 1.15 segue che

$$\mathrm{multideg}(f) \leq \max(\mathrm{multideg}(h_i g_i)). \tag{5}$$

Sia $m(i) = \mathrm{multideg}(h_i g_i)$ e $\delta = \max(m(i), i = 1, \ldots, t)$; quindi

$$\mathrm{multideg}(f) \leq \delta.$$

Consideriamo tutti i modi di scrivere f nella forma (4); da ognuna di queste espressioni possiamo ottenere un diverso δ: noi scegliamo l'espressione (4) di f per cui si abbia il δ minimale; ciò può essere fatto in quanto l'ordinamento monomiale è un buon ordinamento. Proviamo che $\mathrm{multideg}(f) = \delta$: ciò completerebbe la prova, poiché, se $\mathrm{multideg}(f) = \max(\mathrm{multideg}(h_i g_i)) = \mathrm{multideg}(h_i g_i)$, per qualche i, allora $\mathrm{LT}(f) = c \cdot \mathrm{LT}(h_i) \cdot \mathrm{LT}(g_i)$ e quindi avremmo che $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$.

Si supponga per assurdo che $\mathrm{multideg}(f) < \delta$ e scriviamo f nella forma

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \tag{6}$$

$$= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \tag{7}$$

I monomi presenti nella seconda e nella terza sommatoria della (7) hanno tutti multigrado minore di δ. L'ipotesi di assurdo $\mathrm{multideg}(f) < \delta$ implica che anche la prima sommatoria deve avere multigrado minore di δ.

Sia $\mathrm{LT}(h_i) = c_i x^{\alpha(i)}$. Allora la prima sommatoria $\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ ha esattamente la forma descritta dal Lemma 2.13 con $f_i = x^{\alpha(i)} g_i$, quindi tale lemma implica che tale somma è una combinazione lineare degli S-polinomi $S(x^{\alpha(j)} g_j, x^{\alpha(h)} g_h)$. Tuttavia

$$\begin{aligned} S(x^{\alpha(j)} g_j, x^{\alpha(h)} g_h) &= \frac{x^\delta}{x^{\alpha(j)} \mathrm{LT}(g_j)} \cdot x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(h)} \mathrm{LT}(g_h)} \cdot x^{\alpha(h)} g_h \\ &= x^{\delta - \gamma_{jh}} S(g_j, g_h), \end{aligned}$$

dove $x^{\delta - \gamma_{jh}} = \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_h))$. Dunque esistono delle costanti $c_{jh} \in k$ tali che

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,h} c_{jh} x^{\delta - \gamma_{jh}} S(g_j, g_h). \tag{8}$$

Ora vogliamo usare l'ipotesi che il resto nella divisione di $S(g_j, g_h)$ per $g_1, \ldots, g_t$ è zero. Usando l'algoritmo di divisione, otteniamo

$$S(g_j, g_h) = \sum_{i=1}^{t} a_{ijh} g_i \qquad (\text{con} \quad a_{ijh} \in k[x_1, \ldots, x_n]) \tag{9}$$

$$\mathrm{multideg}(a_{ijh} g_i) \leq \mathrm{multideg}(S(g_j, g_h)) \qquad (\forall \ \ i, j, h). \tag{10}$$

Intuitivamente, questo ci dice che quando il resto è nullo, possimo trovare un'espressione per $S(g_j, g_h)$ in termini di G, dove i leading terms non si cancellano. Per capire meglio questo concetto, moltiplichiamo l'espressione di $S(g_j, g_h)$ per $x^{\delta - \gamma_{jh}}$, ottenendo

$$x^{\delta - \gamma_{jh}} S(g_j, g_h) = \sum_{i=1}^{t} b_{ijh} g_i$$

dove $b_{ijh} = x^{\delta-\gamma_{jh}} a_{ijh}$. Quindi, per la (10) e per il Lemma 2.13, si ha che

$$\text{multideg}(b_{ijh} g_i) \leq \text{multideg}(x^{\delta-\gamma_{jh}} S(g_j, g_h)) < \delta. \tag{11}$$

Infine sostituendo la precedente espressione ottenuta per $x^{\delta-\gamma_{jh}} S(g_j, g_h)$ nella (8), ricaviamo un'equazione

$$\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_{j,h} c_{jh} x^{\delta-\gamma_{jh}} S(g_j, g_h) = \sum_{j,h} c_{jh} \left(\sum_{i=1}^{t} b_{ijh} g_i \right) = \sum_i \widetilde{h}_i g_i$$

che per la (9) ha la proprietà che per ogni i,

$$\text{multideg}(\widetilde{h}_i g_i) < \delta.$$

Infine, sostituendo nella (7) $\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_i \widetilde{h}_i g_i$ otteniamo un'espressione per f come combinazione polinomiale dei g_i dove tutti i termini hanno multigrado minore di δ, il che è un assurdo, poiché contraddice la minimalità di δ. □

2.3 Algoritmo di Buchberger

È stato visto che ogni ideale non nullo $I \subset k[x_1, \ldots, x_n]$ ha una base di Groebner, ma non è stato fornito un metodo operativo per costruire una siffatta base per un ideale I dato. Forniremo adesso tale metodo.

Esempio 2.15 *Consideriamo $k[x, y]$ ed il grlex order, sia $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. L'insieme $\{f_1, f_2\}$ non è una base di Groebner perchè $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.*
Quindi un'idea intuitiva per produrre basi di Groebner è quella di estendere la base data fino ad ottenere una base di Groebner. Per decidere quali generatori aggiungere, possiamo fare riferimento al Teorema 2.14, e aggiungere dei polinomi tali che i resti, nelle divisioni degli $S(f_i, f_j)$ per il nuovo sistema di generatori, siano nulli.
Tornando al nostro esempio pratico, non essendo $-x^2 = S(f_1, f_2)$ divisibile né per $LT(f_1)$, né per $LT(f_2)$, il resto nella divisione di $S(f_1, f_2)$ per $F = (f_1, f_2)$ è proprio $-x^2$. Quindi, aggiungiamolo al nostro sistema, cioè sia

$f_3 = -x^2$ e sia $F = (f_1, f_2, f_3)$ il nuovo sistema di generatori. Per verificare se è una base di Groebner per il nostro ideale, riapplichiamo il Teorema 2.14, ed otteniamo che

$$\begin{aligned} S(f_1, f_2) &= f_3, \ \textit{quindi} \\ \overline{S(f_1, f_2)}^F &= 0, \\ S(f_1, f_3) &= (x^3 - 2xy) - (-x)(-x^2) = -2xy, \ \textit{ma} \\ \overline{S(f_1, f_3)}^F &= -2xy \neq 0. \end{aligned}$$

A questo punto, dobbiamo aggiungere ad F anche $f_4 = -2xy$, ma troviamo anche che $\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$. Infine, aggiungendo $f_5 = -2y^2 + x$ ad F, si calcola che:

$$\overline{S(f_i, f_j)}^F = 0 \quad \forall \ 1 \leq i \leq j \leq 5.$$

Quindi, abbiamo trovato una base di Groebner per il nostro ideale I.

Il precedente esempio ci suggerisce che in generale una base di Groebner si può ottenere a partire da una data base F, aggiungendo successivamente i resti non nulli $\overline{S(f_i, f_j)}^F$.

Teorema 2.16 (Algoritmo di Buchberger) *Sia $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideale polinomiale. Allora una base di Groebner per I può essere costruita in un numero finito di passi usando il seguente algoritmo:*

Imput: $F = (f_1, \ldots, f_s)$
Output: *una base di Groebner* $G = (g_i, \ldots, g_t)$ *per* I, *con* $F \subset G$
$G := F$
$REPEAT$
    $G' := G$
    FOR *ogni coppia* $\{p, q\}$, $p \neq q \in G'$ DO
        $S := \overline{S(p, q)}^{G'}$
        $IF \ S \neq 0 \ THEN \ G := G \cup \{S\}$
$UNTIL \ G = G'$

Dimostrazione
Denoteremo con $\langle G\rangle$ ed $\langle \mathrm{LT}(G)\rangle$ i seguenti ideali:

$$\begin{aligned}\langle G\rangle &= \langle g_1,\ldots,g_t\rangle\\ \langle \mathrm{LT}(G)\rangle &= \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle.\end{aligned}$$

Proviamo inizialmente che l'inclusione $G \subset I$ è verificata in ogni passo dell'algoritmo. Banalmente vale all'inizio, dato che $G := F$ e $I = \langle F\rangle$. Supponiamola vera in un passo intermedio, e proviamo l'inclusione per il successivo: se $p, q \in G' := G \subset I$, per ipotesi induttiva, anche $S(p,q) \in I$, quindi il resto $S := \overline{S(p,q)}^{G'}$ deve stare in I; dunque, $G = G' \cup \{S\} \subset I$. Inoltre, notiamo che $F \subset G$, quindi G genera l'ideale I.
L'algoritmo termina quando $G = G'$, ciò significa che $\overline{S(p,q)}^{G'} = 0$ per ogni $p, q \in G$, dunque, per il Teorema 2.14, G è una base di Groebner per I.
Rimane da provare che l'algoritmo termina in un numero finito di passi:
$G = G \cup \{S\} \supseteq G'$, con $S \neq 0$, quindi

$$\langle \mathrm{LT}(G')\rangle \subset \langle \mathrm{LT}(G)\rangle; \tag{12}$$

anzi, proviamo che se $G \neq G'$ allora $\langle \mathrm{LT}(G')\rangle \subsetneq \langle \mathrm{LT}(G)\rangle$. Per veder ciò, supponiamo che un resto non nullo r di un S-polinomio è stato aggiunto a G. Essendo r il resto nella divisione per G', $\mathrm{LT}(r)$ non è divisibile per nessuno dei leading terms degli elementi di G' e dunque $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G')\rangle$, ma $\mathrm{LT}(r) \in \langle \mathrm{LT}(G)\rangle$.

Per la (10), gli ideali $\langle \mathrm{LT}(G')\rangle$ formano, al procedere dell'algoritmo, una catena ascendente di ideali in $k[x_1,\ldots,x_n]$. Dunque, per il Teorema 2.7, tale catena deve stabilizzarsi, quindi dobbiamo ottenere, ad un certo passo dell'algoritmo, che $\langle \mathrm{LT}(G')\rangle = \langle \mathrm{LT}(G)\rangle$, il che implica che $G = G'$. Quindi, l'algoritmo finisce in un numero finito di passi. □

Osservazione 2.17 *Il precedente Algoritmo di Buchberger può essere ancora migliorato: difatti, se* $\overline{S(p,q)}^{G'} = 0$*, tale resto rimarrà nullo anche nei passi successivi dell'algoritmo, quindi possiamo non calcolarlo più.*

Le basi di Groebner calcolate usando il precedente algoritmo sono spesso troppo grandi. Possiamo, però, scartare dei generatori.

Lemma 2.18 *Sia G una base di Groebner per un ideale polinomiale I. Sia $p \in G$ un polinomio, tale che $LT(p) \in \langle LT(G \setminus \{p\})\rangle$. Allora, $G \setminus \{p\}$ è ancora una base di Groebner.*

Dimostrazione
Noi sappiamo che $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G)\rangle$; se $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\})\rangle$, allora $\langle \mathrm{LT}(G \setminus \{p\})\rangle = \langle \mathrm{LT}(G)\rangle$ e, per definizione, $G \setminus \{p\}$ è una base di Groebner per I. □

Moltiplicando per opportune costanti, affinché si ottengano polinomi monici e applicando quanto detto nel Lemma 2.18, possiamo ottenere particolari basi di Groebner.

Definizione 2.19 *Una **base di Groebner minimale** per un ideale polinomiale I è una base di Groebner G per I tale che:*

(i) $LC(p) = 1$, *per ogni* $p \in G$.

(ii) Per ogni $p \in G$, $LT(p) \notin \langle LT(G - \{p\})\rangle$.

Possiamo costruire una base di Groebner minimale usando l'algoritmo di Buchberger e poi eliminando i generatori superflui con l'aiuto del Lemma 2.18.

Esempio 2.20 *Sia I l'ideale studiato nell'esempio (2.15), usando il grlex order abbiamo trovato la base di Groebner:*

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2y - 2y^2 + x, \\ f_3 &= -x^2, \\ f_4 &= -2xy, \\ f_5 &= -2y^2 + x. \end{aligned}$$

La prima cosa che occorre fare per ottenere da questa una base di Groebner minimale è rendere tali polinomi monici; inoltre, in virtù del Lemma 2.18 si può fare a meno sia di f_1 che di f_2, essendo

$$\begin{aligned} &LT(f_1) = x^3 = -x \cdot LT(f_3) \\ &LT(f_2) = x^2y = -(1/2)x(-2xy) = -(1/2)x \cdot LT(f_4). \end{aligned}$$

Si ottiene dunque la base di Groebner minimale (moltiplicando per costanti opportune al fine di rendere i polinomi monici)

$$\tilde{f}_3 = x^2, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x.$$

Sfortunatamente, un dato ideale I non ha un'unica base di Groebner minimale: nel precedente esempio è mimimale la base di Groebner $G_a = \{x^2 + axy, xy, y^2 - (1/2)x\}$ per ogni $a \in k$, quindi se k ha infiniti elementi, I possiede infinite basi di Groebner minimali.

Definizione 2.21 *Una* ***base di Groebner ridotta*** *per $I \subset k[x_1, \ldots, x_n]$, è una base di Groebner G tale che:*

(i) $LC(p) = 1$ per ogni $p \in G$.

(ii) Per ogni $p \in G$, nessun monomio di p sta in $\langle LT(G \setminus \{p\})\rangle$.

In generale, una base di Groebner ridotta ha la seguente proprietà.

Proposizione 2.22 *Sia $I \neq \{0\}$ un ideale polinomiale. Allora, fissato un ordinamento monomiale, I ha un'unica base di Groebner ridotta.*

Dimostrazione
Sia G una base di Groebner minimale per I. Diremo che $g \in G$ è *ridotto* quando nessun monomio di g sta in $\langle \mathrm{LT}(G \setminus \{g\})\rangle$. Il nostro obiettivo è quello di modificare G sino a quando tutti i suoi elementi siano ridotti.

Premettiamo un'osservazione: se g è ridotto per G, allora è ridotto per ogni base di Groebner minimale per I contenente g e avente lo stesso insieme di leading terms, dato che la definizione di elemento ridotto coinvolge solo i leading terms.

Dato $g \in G$ e detto $g' = \overline{g}^{G \setminus \{g\}}$, proviamo che $G' = (G \setminus \{g\}) \cup \{g'\}$ è una base di Groebner minimale per I: innanzitutto, notiamo che $\mathrm{LT}(g) = \mathrm{LT}(g')$, in quanto, essendo G minimale per ipotesi, se dividiamo g per $G \setminus \{g\}$, $\mathrm{LT}(g)$ viene aggiunto al resto, non essendo divisibile per nessun elemento di $\mathrm{LT}(G \setminus \{g\})$. Questo implica che $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(G')\rangle$ e, poiché $G' \subset I$, G' risulta essere una base di Groebner minimale per I. Si noti, infine, che g' è ridotto per G' per costruzione. Ora, applicando tale processo a tutti gli elementi di G, otteniamo alla fine una base di Groebner ridotta.

Infine, per provare l'unicità di tale base, supponiamo che G e $\tilde{G}$ siano due basi di Groebner ridotte per I. In particolare esse sono minimali, da tale

fatto segue che $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$. Difatti, per ogni $p \in G$, $\mathrm{LT}(p) \in \langle \mathrm{LT}(\tilde{G}) \rangle$, e quindi esiste $q \in \tilde{G}$, tale che $\mathrm{LT}(q)$ divide $\mathrm{LT}(p)$; inoltre, $\mathrm{LT}(q) \in \langle \mathrm{LT}(G) \rangle$, quindi, esiste $p' \in G$, tale che $\mathrm{LT}(p')$ divide $\mathrm{LT}(q)$; dunque, se $p = p'$ abbiamo finito, essendo $\mathrm{LT}(p) = \mathrm{LT}(q)$, se invece $p \neq p'$, $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$, contro l'ipotesi di minimalità della base G. Quindi, $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$.

Dunque, dato $g \in G$, esiste $\tilde{g} \in \tilde{G}$, tale che $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$. Se dimostriamo che $g = \tilde{g}$, l'unicità è provata.

Consideriamo $g - \tilde{g} \in I$, e, poiché G è una base di Groebner, si ha che $\overline{g - \tilde{g}}^{G} = 0$. Ma $\mathrm{LT}(g) = \mathrm{LT}(\tilde{g})$, quindi questi termini si cancellano in $g - \tilde{g}$, rimanendo così i termini più piccoli, nessuno dei quali divisibile per qualche monomio di $\mathrm{LT}(G) = \mathrm{LT}(\tilde{G})$, essendo G e $\tilde{G}$ due basi di Groebner ridotte. Quindi, $\overline{g - \tilde{g}}^{G} = g - \tilde{g} = 0$, cioè $g = \tilde{g}$. Questo completa la prova. □

3 Teoria dell'eliminazione

Le basi di Groebner hanno diverse applicazioni in Algebra computazionale, una di esse è la Teoria dell'eliminazione ed in particolare la risoluzione del problema dell'implicitazione. In questa sezione, ci proponiamo di trattare questi due argomenti, almeno per sommi capi. Inizieremo con l'enunciare ed, in parte, con il dimostrare i teoremi che stanno alla base di tale teoria: il Teorema dell'estensione ed il Teorema dell'eliminazione; rimanderemo, però, la dimostrazione di quest'ultimo teorema alla fine del capitolo, dopo avere definito il risultante di due polinomi e dopo averne visto talune utili proprietà. In seguito, illustreremo il significato geometrico dei due teoremi e ne vedremo un'applicazione tangibile nella Teoria dell'implicitazione.

3.1 Il Teorema dell'Eliminazione e dell'Estensione

Il nostro scopo è ora quello di *eliminare* variabili da sistemi di equazioni polinomiali, per fare ciò ci serviremo delle basi di Groebner. Per introdurre il Teorema dell'eliminazione abbiamo bisogno della seguente definizione.

Definizione 3.1 *Dato un ideale $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$, diciamo* ***l-esimo ideale di eliminazione****, e lo denotiamo con il simbolo I_l, il seguente ideale:*

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

Per convenzione, poniamo $I_0 = I$.

L'ideale I_l è costituito dunque da quei polinomi appartenenti all'anello dei polinomi $k[x_{l+1}, \ldots, x_n]$ che si ottengono come combinazione dei generatori di I.

Diremo che stiamo eliminando le variabili $x_1, \ldots, x_l$ se siamo in grado di trovare un polinomio non nullo in I_l.

Teorema 3.2 (Teorema dell'eliminazione) *Sia $I \subset k[x_1, \ldots, x_n]$ un ideale e sia G una sua base di Groebner rispetto all'ordinamento lessicografico, con $x_1 > x_2 > \cdots > x_n$. Allora, per ogni $0 \leq l \leq n$, l'insieme $G_l = G \cap k[x_{l+1}, \ldots, x_n]$ è una base di Goebner per l'l-esimo ideale di eliminazione I_l.*

Dimostrazione
È sufficiente provare che $\langle LT(G_l)\rangle = \langle LT(I_l)\rangle$, essendo già verificata la condizione $G_l \subseteq I_l$.
È ovvio che $\langle LT(G_l)\rangle \subseteq \langle LT(I_l)\rangle$; viceversa, sia $f \in I_l$; dunque $f \in I$, quindi esiste $g \in G$, tale che $LT(g)$ divide $LT(f)$, ma essendo f un polinomio che coinvolge alcune delle variabili $x_{l+1}, \ldots, x_n$, anche $LT(g) \in k[x_{l+1}, \ldots, x_n]$; da ciò segue che $g \in k[x_{l+1}, \ldots, x_n]$, in quanto se, per assurdo, vi fosse in g un termine anche nelle variabili $x_1, \ldots, x_l$, tale monomio dovrebbe essere il leading term di g, poiché stiamo usando il lex order con $x_1 > x_2 > \cdots > x_n$ e ciò costituisce un assurdo. □

Per capire come utilizzare il teorema precedente, consideriamo il seguente esempio.

Esempio 3.3 *Sia dato il sistema di equazioni polinomiali*

$$\begin{cases} x^2 + y + z = & 1, \\ x + y^2 + z = & 1, \\ x + y + z^2 = & 1. \end{cases}$$

Sia $I = \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1\rangle \subset \mathbb{C}[x, y, z]$*; una base di Groebner per* I *è data da quattro polinomi*

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned}$$

I due sistemi di equazioni polinomiali hanno le stesse soluzioni, ma possiamo risolvere con una maggiore facilità l'equazione $g_4 = 0$*, essendo* g_4 *un polinomio nella sola variabile* z*; le possibili* z *sono* $0, 1, -1 \pm \sqrt{2}$*; sostituendo tali valori in* $g_2 = 0$ *ed in* $g_3 = 0$*, determinamo le possibili* y*, ed, infine, sostituendo in* $g_1 = 0$*, otteniamo esattamente le seguenti cinque soluzioni del sistema di partenza:*

$$\begin{aligned} &(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1), \\ &(-1 + \sqrt{2}, -1 + \sqrt{2}, -1 + \sqrt{2}),\ (-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}). \end{aligned}$$

Schematizzando, i passi che ci permettono di trovare le soluzioni di un sistema di equazioni polinomiali, come quello del precedente esempio, sono due:

- (Elimination Step) Dapprima, troviamo polinomi non nulli negli ideali di eliminazione, in particolare nell'ultimo ideale di eliminazione; risolviamo le equazioni date da tali polinomi, così da determinare delle soluzioni parziali: nel precedente esempio, è stato sfruttato il Teorema dell'eliminazione per fare ciò, in quanto per trovare un polinomio non nullo di $I_2 = I \cap \mathbb{C}[z]$, abbiamo calcolato una base di Groebner G per I e abbiamo trovato $g_4 \in G_2$ che genera tutti i polinomi di I che sono nella sola variabile z.
- (Extension Step) Attraverso sostituzioni nelle altre equazioni possiamo estendere le soluzioni parziali del sistema a soluzioni totali.

Abbiamo già parlato dell'Elimination Step, adesso trattiamo l'Extension Step.

Definizione 3.4 *Sia $I \subset k[x_1, \ldots, x_n]$ un ideale, si dice* ***varietà affine*** *il seguente insieme $\boldsymbol{V}(I) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0, \ \forall \ f \ \in I\}$.*

Definizione 3.5 *Sia $I \subset k[x_1, \ldots, x_n]$ un ideale e I_l il suo l-esimo ideale di eliminazione, diremo che $(a_{l+1}, \ldots, a_n) \in k^{n-l}$ è una* ***soluzione parziale*** *se $(a_{l+1}, \ldots, a_n) \in \boldsymbol{V}(I_l)$.*

Per trovare i punti della varietà $\boldsymbol{V}(I)$, vogliamo procedere *eliminando* una coordinata alla volta. Una volta ottenuta una soluzione parziale $(a_{l+1}, \ldots, a_n)$, si considera il successivo ideale di eliminazione,

$$I_{l-1} = \langle g_1, \ldots, g_r \rangle \subseteq k[x_l, x_{l+1}, \ldots, x_n],$$

e si cerca uno zero $a_l \in k$ comune ai polinomi

$$g_1(x_l, a_{l+1}, \ldots, a_n), \ldots, g_r(x_l, a_{l+1}, \ldots, a_n).$$

Non è detto a priori che ciò sia possibile.

Esempio 3.6 *Si consideri il sistema di equazioni* $xy - 1 = xz - 1 = 0$*, il primo ideale di eliminazione è* $I_1 = \langle y - z \rangle$*, quindi le coppie* (a, a)*, con* $a \in \mathbb{C}$*, sono tutte e sole le soluzioni parziali del nostro sistema, tra di esse, però, la soluzione* $(0, 0)$ *non può essere estesa ad una soluzione totale, dato che non soddisfa il nostro sistema. Si noti che* $(0, 0)$ *annulla i coefficienti, y e z, della massima potenza di x nelle equazioni del nostro sistema.*

Richiederemo che il campo k, entro il quale d'ora in poi lavoreremo, sia algebricamente chiuso.

Teorema 3.7 (Teorema dell'estensione) *Sia* $I = \langle f_1, \ldots, f_s \rangle$ *un ideale di* $k[x_1, \ldots, x_n]$ *ed* I_1 *il primo ideale di eliminazione di* I*. Per ogni* $1 \leq i \leq s$*, scriviamo* f_i *nella forma*

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

dove $N_i \geq 0$ *e* $g_i \in k[x_2, \ldots, x_n]$ *è un polinomio non nullo. Data una soluzione parziale* $(a_2, \ldots, a_n) \in \boldsymbol{V}(I_1)$*, se* $(a_2, \ldots, a_n) \notin \boldsymbol{V}(g_1, \ldots, g_s)$*, allora esiste* $a_1 \in k$ *tale che* $(a_1, a_2, \ldots, a_n) \in \boldsymbol{V}(I)$*.*

Proveremo tale teorema solo quando avremo dato alcune nozioni sui risultanti.

Osservazione 3.8 *Avendo scritto i generatori dell'ideale* I *nella forma*

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

è intuitivo che, se una soluzione parziale $(a_2, \ldots, a_n) \in \boldsymbol{V}(g_1, \ldots, g_s)$*, ovvero se* $g_1(a_2, \ldots, a_n) = \cdots = g_s(a_2, \ldots, a_n) = 0$*, si abbassa il grado dei polinomi* $f_1(x_1, a_2, \ldots, a_n), \ldots, f_s(x_1, a_2, \ldots, a_n)$*, dunque è come se avessimo minore possibilità di trovare uno zero,* a_1*, comune a tali polinomi.*
La questione è palese nel precedente esempio.

Osservazione 3.9 *Vediamo, con un esempio, che per* $k = \mathbb{R}$*, il Teorema dell'estensione non vale.*
Consideriamo il sistema di equazioni $x^2 - y = x^2 - z = 0$*, il primo ideale di eliminazione è generato dal polinomio* $y - z$*, perciò troviamo le infinite soluzioni parziali* (a, a)*, con* $a \in k$*; distinguiamo adesso due casi: se ci poniamo in* $\mathbb{C}$*, essendo* $g_1(y, z) = g_2(y, z) = 1 \neq 0$ *per ogni soluzione parziale* (a, a) *con* $a \in \mathbb{C}$*, tutte le soluzioni parziali sono, per il Teorema dell'Estensione, suscettibili ad essere estese al sistema di equazioni originario;*

se, invece, ci poniamo in $\mathbb{R}$*, solo le soluzioni parziali* (a, a) *con* $a \in \mathbb{R}_0^+$ *possono essere estese a soluzioni totali, anche se nessuna di esse appartiene a* $\boldsymbol{V}(g_1, g_2)$*.*

Osservazione 3.10 *La varietà* $\boldsymbol{V}(g_1, \ldots, g_s)$*, alla quale appartengono le soluzioni parziali* $(a_2, \ldots, a_n)$ *che non possono essere estese, dipende dai generatori* $f_1, \ldots, f_s$ *dell'ideale* I*, quindi cambiando tali generatori si può rendere tale varietà la più piccola possibile; addirittura, se lavoriamo in uno spazio proiettivo, quindi con polinomi omogenei, tutte le soluzioni parziali possono essere estese.*

Osservazione 3.11 *Il Teorema dell'estensione può essere usato per eliminare un numero qualsiasi di variabili. Infatti, basta osservare che l'ideale* $I_{l+1} \in k[x_{l+2}, \ldots, x_n]$ *è il primo ideale di eliminazione di* $I_l \in k[x_{l+1}, \ldots, x_n]$*: di certo* $I_{l+1} \subseteq I_l$*; inoltre*

$$(I_l)_1 = I_l \cap k[x_{l+2}, \ldots, x_n] = I \cap k[x_{l+1}, \ldots, x_n] \cap k[x_{l+2}, \ldots, x_n] = \\ = I \cap k[x_{l+2}, \ldots, x_n] = I_{l+1}.$$

Esempio 3.12 *Consideriamo il sistema di polinomi in* $\mathbb{C}[x, y, z]$*,*

$$\begin{cases} x^2 + y^2 + z^2 = 1 \\ xyz = 1 \end{cases}$$

Una base di Groebner per $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$ *è*

$$\begin{aligned} g_1 &= y^4z^2 + y^2z^4 - y^2z^2 + 1, \\ g_2 &= x + y^3z + yz^3 - yz. \end{aligned}$$

Sfruttando il teorema dell'eliminazione, troviamo che $I_1 = \langle g_1 \rangle$ *e* $I_2 = \{0\}$*, quindi ogni* $c \in \mathbb{C}$ *è una soluzione parziale; ma quali tra esse vengono estese ad una soluzione* $(a, b, c) \in \boldsymbol{V}(I)$*? Dal momento che* I_2 *è il primo ideale di eliminazione di* I_1*,* $c \in \mathbb{C}$ *può essere estesa a* $(b, c) \in \boldsymbol{V}(I_1)$ *se* $c \notin \boldsymbol{V}(z^2)$*, essendo* z^2 *il coefficiente in* $\mathbb{C}[z]$ *della* y *di grado massimo nel polinomio* g_1 *che genera* I_1 *e quindi se* $c \neq 0$*. Allo stesso modo,* $(b, c) \in \boldsymbol{V}(I_1)$ *può essere estesa ad una soluzione totale* $(a, b, c) \in \boldsymbol{V}(I) = \boldsymbol{V}(g_1, g_2)$ *se non appartiene a* $\boldsymbol{V}(1)$*, essendo* 1 *il coefficiente della* x *di grado massimo del polinomio* g_2*, e ciò è sempre verificato.*

Proviamo adesso il seguente corollario che costituisce un caso particolare del Teorema dell'estensione.

Corollario 3.13 *Sia $I = \langle f_1, \ldots, f_s \rangle$ un ideale di $k[x_1, \ldots, x_n]$ ed I_1 il primo ideale di eliminazione di I. Supponiamo che esista un indice i, $1 \leq i \leq s$, tale che f_i sia nella forma*

$$f_i = cx_1^N + \textit{termini in cui } x_1 \textit{ ha grado minore di } N,$$

dove $c \in k \setminus \{0\}$ ed $N > 0$. Se $(a_2, \ldots, a_n) \in \boldsymbol{V}(I_1)$, allora esiste $a_1 \in k$ tale che $(a_1, a_2, \ldots, a_n) \in \boldsymbol{V}(I)$.

Dimostrazione
Usando la notazione usata in precedenza, essendo $g_i = c \neq 0$, la varietà $\boldsymbol{V}(g_1, \ldots, g_s) = \emptyset$, ovvero ogni soluzione parziale può essere estesa. □

3.2 Geometria dell'Eliminazione

Diamo adesso un'interpretazione geometrica di quanto visto sino ad ora. L'eliminazione di alcune variabili può, in qualche misura, essere vista come una proiezione della varietà su certi sottospazi.

Definizione 3.14 *Sia data una varietà affine $V = \boldsymbol{V}(f_1, \ldots, f_s) \subset k^n$, l'applicazione*

$$\pi_l : k^n \longrightarrow k^{n-l}$$

*definita dalla legge $\pi_l(a_1, \ldots, a_n) = (a_{l+1}, \ldots, a_n)$ è detta **proiezione** di k^n su k^{n-l}. L'immagine tramite π_l di V, $\pi_l(V)$ è detta **proiezione** della varietà affine V sullo spazio affine k^{n-l}.*

Il seguente lemma instaura una relazione tra le proiezioni di $V = \boldsymbol{V}(f_1, \ldots, f_s)$ e le varietà degli ideali di eliminazione di $I = \langle f_1, \ldots, f_s \rangle$.

Lemma 3.15 *Sia $I = \langle f_1, \ldots, f_s \rangle$ un ideale di $k[x_1, \ldots, x_n]$ e sia I_l il suo l-esimo ideale di eliminazione. Allora in k^{n-l} sussiste la seguente relazione di inclusione*

$$\pi_l(V) \subseteq \boldsymbol{V}(I_l).$$

Dimostrazione
Si fissi un polinomio $f \in I_l$; sia $(a_1, \ldots, a_n) \in V$, $f(a_1, \ldots, a_n) = 0$, ma, essendo $f \in k[x_{l+1}, \ldots, x_n]$, si ha

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

Quindi ogni $(a_{l+1}, \ldots, a_n) = \pi_l(a_1, \ldots, a_n) \in \pi_l(V)$ appartiene a $\boldsymbol{V}(I_l)$, in quanto annulla tutti i polinomi $f \in I_l$. □

La varietà $\boldsymbol{V}(I_l) = \{(a_{l+1}, \ldots, a_n) |\ f(a_{l+1}, \ldots, a_n) = 0,\ \forall\ f \in I_l\}$ è costituita, per sua stessa definizione, da tutte le soluzioni parziali; invece, il suo sottoinsieme $\pi_l(V)$ è l'insieme di tutte le soluzioni parziali che possono essere estese a soluzioni totali.

Osservazione 3.16 *Nell'esempio (3.6), abbiamo trovato*

$$\begin{aligned} \pi_1(V) &= \{(a,a) |\ a \in \mathbb{C}^*\} \\ \boldsymbol{V}(I_1) &= \{(a,a) |\ a \in \mathbb{C}\}. \end{aligned}$$

In questo caso, è evidente che $\pi_1(V) \subset \boldsymbol{V}(I_1)$ e che $\pi_1(V)$ non è una varietà affine, essendo una retta privata di un punto.

Diamo adesso un altro enunciato del Teorema dell'estensione, dal quale si evince più chiaramente il significato geometrico di quest'ultimo.

Teorema 3.17 (Teorema geometrico dell'estensione) *Sia data una varietà affine $V = \boldsymbol{V}(f_1, \ldots, f_s) \in k^n$ e sia I_1 il primo ideale di eliminazione di I, scriviamo come al solito gli f_i nella forma*

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

dove $N_i \geq 0$ e $g_i \in k[x_2, \ldots, x_n]$ è un polinomio non nullo. Allora vale in k^{n-l} la seguente uguaglianza

$$\boldsymbol{V}(I_1) = \pi_1(V) \cup (\boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1)).$$

Dimostrazione
Occorre provare la doppia inclusione, supponendo dimostrato il Teorema dell'estensione. In virtù del Lemma 3.15, si ha che

$$\pi_1(V) \cup (\boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1)) \subseteq \boldsymbol{V}(I_1);$$

viceversa, sia $(a_2, \ldots, a_n) \in \boldsymbol{V}(I_1)$: se esiste $a_1 \in k$ tale che $(a_1, a_2, \ldots, a_n)$ sta in $\boldsymbol{V}(I)$, allora $(a_2, \ldots, a_n) \in \pi_1(V)$; se, per contro, non esiste $a_1 \in k$ tale che $(a_1, a_2, \ldots, a_n) \in \boldsymbol{V}(I)$, per il Teorema dell'estensione, si ha che la n-upla $(a_2, \ldots, a_n) \in \boldsymbol{V}(g_1, \ldots, g_s)$. □

Il seguente teorema precisa ancor meglio la relazione che intercorre tra $\boldsymbol{V}(I_l)$ e $\pi_l(V)$, ma prima di enunciarlo e di provarlo ricordiamo alcune nozioni preliminari, nelle quali supponiamo che k sia un campo algebricamente chiuso.

Definizione 3.18 *Dato un insieme $X \subset k^n$, si definisce **vanishing ideal** di X, o, semplicemente, **ideale** di X, il seguente ideale*

$$\boldsymbol{I}(X) = \{f \in k[x_1, \ldots, x_n] |\ f(a_1, \ldots, a_n) = 0,\ \forall\ (a_1, \ldots, a_n) \in X\}.$$

Teorema 3.19 (Teorema degli zeri di Hilbert) *Sia k un campo algebricamente chiuso, l'assegnazione $V \mapsto \boldsymbol{I}(V)$ definisce una biiezione tra l'insieme di tutte le varietà affini di k^n e l'insieme di tutti gli ideali I dell'anello $k[x_1, \ldots, x_n]$ tali che*

$$I = \sqrt{I} = \{f \in k[x_1, \ldots, x_n] |\ f^n \in I \text{ per qualche } n \in \mathbb{N}\}.$$

Teorema 3.20 (Teorema della chiusura) *Sia $V = \boldsymbol{V}(f_1, \ldots, f_s)$ una varietà affine di k^n e sia I_l l'l-esimo ideale di eliminazione di $I = \langle f_1, \ldots, f_s \rangle$, allora:*

1. *la più piccola varietà contenente $\pi_l(V)$ è $\boldsymbol{V}(I_l)$;*
2. *se $V \neq \emptyset$, esiste una varietà affine $W \subsetneq \boldsymbol{V}(I_l)$ tale che*

$$\boldsymbol{V}(I_l) \backslash W \subset \pi_l(V).$$

<u>*Dimostrazione*</u>

1. Dire che $\boldsymbol{V}(I_l)$ è la più piccola varietà affine contenente $\pi_l(V)$ equivale a dire che:
   a) $\pi_l(V) \subseteq \boldsymbol{V}(I_l)$ e ciò è già stato provato nel Lemma 3.15;
   b) se W è una varietà affine contenente $\pi_l(V)$, allora $\boldsymbol{V}(I_l) \subseteq W$.

Proviamo innanzitutto che, se $I = \sqrt{I}$, $\boldsymbol{I}(\pi_l(V)) = I_l$, altrimenti, se si ha $I \subsetneq \sqrt{I}$, $I_l \subset \boldsymbol{I}(\pi_l(V))$:
difatti, in entrambi i casi vale l'inclusione $I_l \subset \boldsymbol{I}(\pi_l(V))$, dato che se $f \in I_l$, allora $f(x_1, \ldots, x_n) = 0$, per ogni $(x_1, \ldots, x_n) \in V$; ma $f(x_1, \ldots, x_n) = f(x_{l+1}, \ldots, x_n) = f(\pi_l(x_1, \ldots, x_n)) = 0$, quindi $f \in \boldsymbol{I}(\pi_l(V))$; l'inclusione inversa vale di certo se I è radicale, in quanto se $f \in \boldsymbol{I}(\pi_l(V))$, $f \in k[x_{l+1}, \ldots, x_n]$ ed inoltre $f \in \boldsymbol{I}(V)$, essendo $f(\pi_l(Q)) = f(Q) = 0$ per ogni $Q \in V$; per il Teorema 3.19 si ottiene $\boldsymbol{I}(V) = \boldsymbol{I}(\boldsymbol{V}(I)) = \sqrt{I} = I$ (nell'ipotesi che I sia radicale), quindi $f \in I_l = I \cap k[x_{l+1}, \ldots, x_n]$.

Sia adesso $W = \boldsymbol{V}(J)$ con J ideale di $k[x_{l+1}, \ldots, x_n]$ una varietà contenente $\pi_l(V)$. Se I è un ideale radicale, si ha che $\boldsymbol{I}(W) \subset \boldsymbol{I}(\pi_l(V)) = I_l$, dunque, passando alle varietà, $\boldsymbol{V}(I_l) \subset \boldsymbol{V}(\boldsymbol{I}(W)) = W$, essendo W una varietà affine; se, invece, $I \subsetneq \sqrt{I}$, occorre provare che

$$W \supset \boldsymbol{V}(\sqrt{I_l}) = \boldsymbol{V}(I_l).$$

Per dimostrare ciò, sapendo che $W \supset \pi_l(V)$ e, dunque, che $\boldsymbol{I}(W) \subset \boldsymbol{I}(\pi_l(V))$, basta far vedere che $\boldsymbol{I}(\pi_l(V)) \supset \sqrt{I_l}$. Questa inclusione segue da $\boldsymbol{V}(\sqrt{I_l}) \subset \pi_l(V)$. Quest'ultima inclusione vale poiché $\boldsymbol{I}(\pi_l(V)) \subset \boldsymbol{I}(\boldsymbol{V}(\sqrt{I_l})) = \sqrt{I_l}$; infatti, per come abbiamo visto, $\boldsymbol{I}(\pi_l(V)) \subset \sqrt{I} \cap k[x_{l+1}, \ldots, x_n]$, e vale l'inclusione $\sqrt{I} \cap k[x_{l+1}, \ldots, x_n] \subset \sqrt{I_l}$, dato che, se $f \in \sqrt{I} \cap k[x_{l+1}, \ldots, x_n]$, esiste un $m \in \mathbb{N}$ tale che $f^m \in I$ ed f^m è nelle sole variabili $x_{l+1}, \ldots, x_n$, dunque $f^m \in I \cap k[x_{l+1}, \ldots, x_n] = I_l$.

2. Proviamo solo il caso in cui $l = 1$.
Dal Teorema 3.17, sappiamo che

$$\boldsymbol{V}(I_1) = \pi_1(V) \cup (\boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1)).$$

Se $\boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1) \neq \boldsymbol{V}(I_1)$, questa è la varietà W da noi cercata. Se invece $\boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1) = \boldsymbol{V}(I_1)$, vogliamo determinare una sottovarietà non banale di $\boldsymbol{V}(I_1)$ che soddisfi la condizione 2.. Poniamo anche in questo caso $W = \boldsymbol{V}(g_1, \ldots, g_s) \cap \boldsymbol{V}(I_1)$ e proviamo che

$$W = \boldsymbol{V}(I_1) \Longrightarrow V = \boldsymbol{V}(f_1, \ldots, f_s, g_1, \ldots, g_s).$$

Ovviamente $\boldsymbol{V}(f_1, \ldots, f_s, g_1, \ldots, g_s) \subseteq V$; viceversa, sia $(a_1, a_2, \ldots, a_n) \in V$; di certo, per ogni $i = 1, \ldots s$, $f_i(a_1, a_2, \ldots, a_n) = 0$, ma, d'altra

parte, $(a_2, \ldots, a_n) \in \pi_1(V) \subseteq \boldsymbol{V}(I_1) = W$, quindi $g_i(a_1, a_2, \ldots, a_n) = g_i(a_2, \ldots, a_n) = 0$, per ogni i. Si ha dunque

$$V = \boldsymbol{V}(f_1, \ldots, f_s, g_1, \ldots, g_s). \tag{13}$$

Consideriamo adesso gli ideali

$$I = \langle f_1, \ldots, f_s \rangle \text{ e } \tilde{I} = \langle f_1, \ldots, f_s, g_1, \ldots, g_s \rangle;$$

essi possono essere diversi, ma, per la (13), $\boldsymbol{V}(I) = \boldsymbol{V}(\tilde{I})$ e $\pi_1(\boldsymbol{V}(I)) = \pi_1(\boldsymbol{V}(\tilde{I}))$, dunque, per la parte 1., essendo $\boldsymbol{V}(I_1)$ e $\boldsymbol{V}(\tilde{I}_1)$ rispettivamente la più piccola varietà contenente $\pi_1(\boldsymbol{V}(I))$ e $\pi_1(\boldsymbol{V}(\tilde{I}))$, si ha che

$$\boldsymbol{V}(I_1) = \boldsymbol{V}(\tilde{I}_1); \tag{14}$$

Troviamo, ora, una base migliore per $\tilde{I}$: per ogni $i = 1, \ldots, s$, poniamo

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

di certo tale polinomio, per come è stato definito g_i, ha grado in x_1 strettamente minore di f_i. Si prova facilmente che

$$\tilde{I} = \langle \tilde{f}_1, \ldots, \tilde{f}_s, g_1, \ldots, g_s \rangle. \tag{15}$$

Applicando il Teorema 3.17 a tale ideale, otteniamo

$$\boldsymbol{V}(I_1) = \boldsymbol{V}(\tilde{I}_1) = \pi_1(V) \cap \tilde{W},$$

dove $\tilde{W}$ è costituito dalle soluzioni parziali che annullano i coefficienti della x_1 di grado massimo, $\tilde{g}_1, \ldots, \tilde{g}_s$, nei polinomi $\tilde{f}_i$. Se $\tilde{W} \neq \boldsymbol{V}(I_1)$, essa è la varietà cercata, altrimenti reiteriamo il procedimento fino a quando non troviamo una varietà siffatta. Se non riuscissimo a trovarla, poiché ad ogni passo abbassiamo il grado in x_1 dei generatori (notiamo che i g_i hanno già grado 0 in x_1), arriveremmo ad un punto in cui $V = \boldsymbol{V}(\overline{f}_1, \ldots, \overline{f}_s, g_1, \ldots, g_s)$, dove $\overline{f}_1, \ldots, \overline{f}_s \in k[x_2, \ldots, x_n]$; se fosse così la varietà da noi cercata sarebbe $W = \emptyset$, dal momento che ogni soluzione parziale potrebbe essere estesa.

□

Notiamo che il precedente teorema vale quando k è un campo algebricamente chiuso qualsiasi: tale ipotesi è necessaria poiché richiesta nel Teorema degli zeri di Hilbert e nel Teorema 3.17.

Corollario 3.21 *Sia $I = \langle f_1, \ldots, f_s \rangle$ un ideale di $k[x_1, \ldots, x_n]$, I_1 il primo ideale di eliminazione di I ed $V = \boldsymbol{V}(f_1, \ldots, f_s)$ la sua varietà affine. Supponiamo che esista un indice i, $1 \leq i \leq s$, tale che f_i sia nella forma*

$$f_i = cx_1^N + \textit{termini in cui } x_1 \textit{ ha grado minore di } N,$$

dove $c \in k \setminus \{0\}$ ed $N > 0$. Allora $\pi_1(V) = \boldsymbol{V}(I_1)$.

Osservazione 3.22 *Il nome dato al Teorema 3.20 proviene dal fatto che, nella topologia di Zariski (topologia sullo spazio affine k^n costruita a partire dalla famiglia di chiusi, che sono le varietà affini), $\boldsymbol{V}(I_l)$ rappresenta la chiusura di $\pi_l(V)$. In particolare, se $\boldsymbol{V}(I_l)$ è un chiuso irriducibile, $\pi_l(V)$ è denso in esso.*

Osservazione 3.23 *Il Teorema della chiusura non ci dà una descrizione completa di $\pi_l(V)$, ci dice solo che esiste una varietà W strettamente contenuta in $\boldsymbol{V}(I_l)$ che contiene quei punti di $\boldsymbol{V}(I_l)$ che mancano a $\pi_l(V)$, ma, purtroppo, in W potrebbero stare anche punti di $\pi_l(V)$.*

3.3 Implicitazione

Il problema dell'implicitazione consiste, sostanzialmente, nel trovare le equazioni implicite che definiscono una varietà V a partire dalle sue equazioni parametriche.
In generale, però, l'insieme dei punti descritti dalla parametrizzazione non è uguale all'insieme dei punti della varietà V; per cui il problema dell'implicitazione si traduce nel trovare la più piccola varietà affine che contenga i punti descritti da un data parametrizzazione; nel risolvere questo problema adopereremo quanto introdotto nelle due precedenti sezioni.
Facciamo un esempio per capire meglio come la parametrizzazione in generale non riempie tutta la varietà.

Esempio 3.24 *Si consideri nello spazio affine $\mathbb{C}^2$, la circonferenza unitaria di centro l'origine del riferimento affine canonico, una delle sue parametrizzazioni è la seguente*

$$\begin{cases} x = & \dfrac{1-t^2}{1+t^2} \\ y = & \dfrac{2t}{1+t^2} \end{cases}$$

il punto $(-1, 0)$ *non corrisponde, nella parametrizzazione, ad alcun valore del parametro* t*, eppure esso è un punto della circonferenza unitaria con centro nell'origine.*

Iniziamo con il trattare il caso più semplice di *parametrizzazione polinomiale*.

Sia dato il sistema parametrico

$$\begin{cases} x_1 &= f_1(t_1, t_2, \ldots, t_m) \\ x_2 &= f_2(t_1, t_2, \ldots, t_m) \\ \vdots & \\ x_n &= f_n(t_1, t_2, \ldots, t_m) \end{cases} \tag{16}$$

dove $f_1, f_2, \ldots, f_n \in k[t_1, \ldots, t_m]$.
Introduciamo un'applicazione $F : k^m \to k^n$, così definita

$$F(t_1, t_2, \ldots, t_m) = (f_1(t_1, t_2, \ldots, t_m), f_2(t_1, t_2, \ldots, t_m), \ldots, f_n(t_1, t_2, \ldots, t_m)).$$

L'immagine secondo F di k^m, $F(k^m) \subseteq k^n$ è il sottoinsieme parametrizzato di k^n; poiché non è detto che quest'ultimo costituisca una varietà affine di k^n, diremo di aver risolto il problema dell'implicitazione, in questo caso di parametrizzazione polinomiale, solo quando avremo trovato la più piccola varietà affine di k^n contenente $F(k^m)$.

Sia $V = \boldsymbol{V}(x_1 - f_1(t_1, \ldots, t_m), \ldots, x_n - f_n(t_1, \ldots, t_m)) \subseteq k^{n+m}$, essendo $V = \{(t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m))$ dove $(t_1, \ldots, t_m) \in k^m\}$ essa può essere considerata il *grafico* della nostra funzione F. Si considerino, adesso, le applicazioni $i : k^m \to k^{n+m}$ e $\pi_m : k^{n+m} \to k^n$ definite nel modo seguente:

$$\begin{aligned} &i(t_1, \ldots, t_m) = (t_1, \ldots, t_m, f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)); \\ &\pi_m(x_1, \ldots, x_m, x_{m+1}, \ldots, x_n) = (x_{m+1}, \ldots, x_n). \end{aligned}$$

Otteniamo, quindi, il seguente diagramma di applicazioni:

$$\begin{array}{ccccc} & & k^{n+m} & & \\ & \overset{i}{\nearrow} & & \overset{\pi_m}{\searrow} & \\ k^m & & \xrightarrow{F} & & k^n \end{array} \tag{17}$$

Notiamo che $F = \pi_m \circ i$ e che $F(k^m) = \pi_m(i(k^m)) = \pi_m(V)$, quindi l'immagine della parametrizzazione è la proiezione del suo grafico

$$F(k^m) = \pi_m(V) \tag{18}$$

Teorema 3.25 (Implicitazione Polinomiale) *Sia k un campo infinito ed $F : k^m \to k^n$ la funzione determinata dalla parametrizzazione (16). Sia $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subseteq k[t_1, \ldots, t_m, x_1, \ldots, x_n]$ e sia $I_m = I \cap k[x_1, \ldots, x_n]$ l'm-esimo ideale di eliminazione di I. Allora $\boldsymbol{V}(I_m)$ è la più piccola varietà di k^n contenente $F(k^m)$.*

Dimostrazione

Poniamoci, dapprima, nel caso in cui k sia algebricamente chiuso.
Sia $V = \boldsymbol{V}(I) \subseteq k^{n+m}$ il grafico di F; per la (18) e per il Teorema 3.20, $\boldsymbol{V}(I_m)$ è la più piccola varietà di k^n contenente $\pi_m(V)$. Quindi il teorema è subito provato per k algebricamente chiuso.

Sia adesso k un campo infinito e $\overline{k}$ una sua chiusura algebrica.

Notiamo che l'ideale I_m è invariante al passaggio dal campo k ad un campo più grande, qual'è $\overline{k}$; quindi consideriamo gli insiemi

$$\begin{aligned} \boldsymbol{V}_k(I_m) &= \{(a_1, \ldots a_n) \in k^n |\ f(a_1, \ldots a_n) = 0,\ \forall\ f \in I_m\}, \\ \boldsymbol{V}_{\overline{k}}(I_m) &= \{(a_1, \ldots a_n) \in \overline{k}^n |\ f(a_1, \ldots a_n) = 0,\ \forall\ f \in I_m\}; \end{aligned}$$

di certo, si ha $\boldsymbol{V}_k(I_m) \subset \boldsymbol{V}_{\overline{k}}(I_m)$. Proviamo che $\boldsymbol{V}_k(I_m)$ è la più piccola varietà contenente $F(k^m)$. Si ha innanzitutto, in virtù del Lemma 3.15, che $F(k^m) = \pi_m(V) \subseteq \boldsymbol{V}_k(I_m)$. Sia, ora, Z_k una varietà affine di k^n contenente $F(k^m)$, $Z_k = \boldsymbol{V}_k(g_1, \ldots, g_s)$, dove $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ e ognuno di tali polinomi si annulla in ogni punto di $F(k^m)$. Abbiamo ottenuto quindi che, per ogni $1 \leq i \leq s$, $g_i \circ F : k^m \to k$ si annulla su tutto k^m; in virtù del fatto che k è infinito, questo implica che $g_i \circ F$ è la funzione identicamente nulla, dunque i g_i si annullano su tutto $F(\overline{k}^m)$ e $Z_{\overline{k}} = \boldsymbol{V}_{\overline{k}}(g_1, \ldots, g_s)$ è una varietà di $\overline{k}^n$ contenente $F(\overline{k}^m)$, questo, per la prima parte del teorema, implica che $\boldsymbol{V}_{\overline{k}}(I_m) \subset Z_{\overline{k}}$. Tale inclusione si conserva anche se ci limitiamo a considerare le due varietà nel campo k:

$$\boldsymbol{V}_k(I_m) \subset Z_k.$$

Questo prova che $\boldsymbol{V}_k(I_m)$ è la più piccola varietà contenente $F(k^m)$. □

Il problema dell'implicitazione, in caso di parametrizzazione polinomiale, è stato così completamente risolto: data una parametrizzazione polinomiale come la (16), occorre considerare l'ideale $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ e calcolare una sua base di Groebner usando il lex order con $t_1 > \cdots > t_m > x_1 > \cdots > x_n$; quindi, utilizzando il teorema dell'eliminazione, posso determinare l'ideale I_m e ottenere $\boldsymbol{V}_k(I_m)$, che, come visto nel precedente teorema, è la più piccola verietà affine contenente la parametrizzazione.

Passiamo adesso a trattare il caso di una *parametrizzazione razionale*. Sia data la parametrizzazione

$$\begin{cases} x_1 &= \dfrac{f_1(t_1, t_2, \ldots, t_m)}{g_1(t_1, t_2, \ldots, t_m)} \\ x_2 &= \dfrac{f_2(t_1, t_2, \ldots, t_m)}{g_2(t_1, t_2, \ldots, t_m)} \\ \vdots & \\ x_n &= \dfrac{f_n(t_1, t_2, \ldots, t_m)}{g_n(t_1, t_2, \ldots, t_m)} \end{cases} \tag{19}$$

dove $f_1, \ldots, f_n, g_1, \ldots, g_n \in k[t_1, \ldots, t_m]$. In questo caso, non possiamo definire, come prima, l'applicazione F su tutto k^m, ma occorre restringere il dominio di F a $k^m \backslash W$, con $W = \boldsymbol{V}(g_1 g_2 \cdots g_n)$. Avremo, perciò, un'applicazione $F : k^m \backslash W \to k^n$, definita nel modo seguente:

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, t_2, \ldots, t_m)}{g_1(t_1, t_2, \ldots, t_m)}, \ldots, \frac{f_n(t_1, t_2, \ldots, t_m)}{g_n(t_1, t_2, \ldots, t_m)} \right).$$

Il nostro scopo, in questo caso, è determinare la più piccola varietà affine di k^n contenente $F(k^m \backslash W)$.
Adattando il diagramma (17) alla presente situazione, otteniamo

$$\begin{array}{ccccc} & & k^{n+m} & & \\ & \overset{i}{\nearrow} & & \overset{\pi_m}{\searrow} & \\ k^m \backslash W & & \xrightarrow{F} & & k^n \end{array}$$

ma purtroppo, detto I l'ideale $\langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n \rangle$, ottenuto eliminando i denominatori, $\boldsymbol{V}(I)$ non è la più piccola varietà di k^{n+m} contenente $i(k^m \backslash W)$.

Occorre, per ovviare a tale inconveniente, ricorrere ad un espediente. Poniamoci nell'anello dei polinomi $k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$ e consideriamo in esso l'ideale

$$J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle,$$

dove $g = g_1 g_2 \cdots g_n$. Notiamo che i polinomi $g_1, \ldots, g_n$ non si annullano mai nei punti di $\boldsymbol{V}(J)$, in virtù dell'equazione $1 - gy = 0$. Quindi, considerate le applicazioni $j : k^m \backslash W \to k^{n+m+1}$ e $\pi_{m+1} : k^{n+m+1} \to k^n$, definite da

$$\begin{aligned} j(t_1, \ldots, t_m) &= \left(\frac{1}{g(t_1, \ldots, t_m)}, t_1, \ldots, t_m, \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right) \\ & \pi_{m+1}(y, t_1, \ldots, t_m, x_1, \ldots, x_n) = (x_1, \ldots, x_n), \end{aligned}$$

otteniamo il diagramma

$$\begin{array}{ccccc} & & k^{n+m+1} & & \\ & \overset{j}{\nearrow} & & \overset{\pi_{m+1}}{\searrow} & \\ k^m \backslash W & & \xrightarrow{F} & & k^n \end{array}$$

Come prima, si ha che $F = \pi_{m+1} \circ j$ ed inoltre $j(k^m \backslash W) = \boldsymbol{V}(J)$: difatti, $j(k^m \backslash W) \subseteq \boldsymbol{V}(J)$, a causa della definizione di J che abbiamo dato; viceversa, se $(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in \boldsymbol{V}(J)$, essendo $g(t_1, \ldots, t_m)y = 1$, nessuno dei g_i si annulla in $(t_1, \ldots, t_m)$ e perciò, da $g_i(t_1, \ldots, t_m)x_i = f_i(t_1, \ldots, t_m)$, possiamo dedurre che

$$x_i = \frac{f_i(t_1, \ldots, t_m)}{g_i(t_1, \ldots, t_m)}, \quad \forall\ 1 \leq i \leq n, \quad \text{e che} \quad y = \frac{1}{g(t_1, \ldots, t_m)},$$

ovvero che il punto sta in $j(k^m \backslash W)$. Abbiamo, in tal modo, ottenuto che

$$F(k^m \backslash W) = \pi_{m+1}(j(k^m \backslash W)) = \pi_{m+1}(\boldsymbol{V}(J)), \tag{20}$$

in questo caso, quindi, l'immagine della parametrizzazione è la proiezione della varietà $\boldsymbol{V}(J)$.

Teorema 3.26 *Sia k un campo infinito e sia $F : k^m \backslash W \to k^n$ l'applicazione definita dalla parametrizzazione (19). Sia dato $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle$, dove $g = g_1 g_2 \cdots g_n$, e sia $J_{m+1} = J \cap k[x_1, \ldots, x_n]$, l'$(m+1)$-esimo ideale di eliminazione di J. Allora $\boldsymbol{V}(J_{m+1})$ è la più piccola varietà di k^n contenente l'immagine della parametrizzazione $F(k^m \backslash W)$.*

Dimostrazione
La prova di tale teorema è del tutto analoga a quella del Teorema dell'implicitazione polinomiale, eccetto che per un particolare. Dati due polinomi $f, g \in k[t_1, \ldots, t_m]$, con $g \neq 0$, se f si annulla su tutto $k^m \setminus \boldsymbol{V}(g)$, allora f è il polinomio nullo.
Infatti, il polinomio $f \cdot g$ si annulla su tutto k^m, poiché $g(P) = 0$, per ogni $P \in \boldsymbol{V}(g)$, e $f(Q) = 0$, per ogni $Q \in k^m \setminus \boldsymbol{V}(g)$, per ipotesi; ma, essendo k un campo infinito, si ha che $f \cdot g = 0$, dunque $f = 0$. □

Possiamo dire di avere risolto il problema dell'implicitazione anche nel caso di parametrizzazione razionale. Data la parametrizzazione (17), consideriamo l'ideale J, definito nel solito modo; quindi, calcoliamo una sua base di Groebner e, adoperando il lex order con $y > t_1 > \cdots > t_m > x_1 > \cdots > x_n$, determiniamo una base per J_{m+1}; la verietà da esso determinata è la varietà cercata.

Osservazione 3.27 *Nel caso di parametrizzazione polinomiale, abbiamo visto che l'immagine della parametrizzazione è $\pi_m(V) = F(k^m)$ e che $\boldsymbol{V}(I_m)$ è la più piccola varietà la contiene. Questo concorda con quanto detto a pagina 38: difatti, $\boldsymbol{V}(I_m)$ è l'insieme di k^n costituito da tutte le soluzioni parziali del sistema polinomiale di equazioni*

$$\begin{cases} x_1 &= f_1(t_1, t_2, \ldots, t_m) \\ \vdots & \\ x_n &= f_n(t_1, t_2, \ldots, t_m) \end{cases}$$

Invece, in $\pi_m(V)$ vi sono le soluzioni parziali che possono essere completate a soluzioni totali del sistema, ovvero, se $(x_1, \ldots, x_n) \in \pi_m(V)$, esiste almeno una m-upla $(t_1, \ldots, t_m) \in k^m$ tale che $x_i = f_i(t_1, \ldots, t_m)$ per ogni $1 \leq i \leq n$, cioè è un punto che sta nell'immagine della parametrizzazione. È evidente che in generale, poiché non tutte le soluzioni parziali possono essere estese, vi sono punti nella varietà $\boldsymbol{V}(I_m)$ che non sono descritti dalla parametrizzazione.

3.4 Risultante di due polinomi

Lemma 3.28 *Siano $f, g \in k[x]$ due polinomi di grado, rispettivamente, $l > 0$ e $m > 0$. Essi hanno un fattore in comune se e solo se esistono due polinomi $A, B \in k[x]$ tali che:*

1. *I polinomi A e B sono entrambi non nulli.*
2. *Il polinomio A ha al più grado $m-1$, B ha al più grado $l-1$.*
3. *Vale l'uguaglianza $Af + Bg = 0$.*

Dimostrazione
($\Rightarrow$) Sia $h \in k[x]$ il fattore in comune di f e g; dunque esistono due polinomi f_1 e g_1 aventi, rispettivamente, grado al più $l-1$ ed $m-1$, tali che

$$f = hf_1 \ e \ g = hg_1,$$

per i quali si ha $g_1 f + (-f_1)g = 0$, quindi ponendo $A = g_1$ e $B = -f_1$ si ha la tesi.
($\Leftarrow$) Supponiamo che esistano due polinomi A e B, che godono delle proprietà prima elencate; sia inoltre $B \neq 0$. Supponiamo, per assurdo, che tali due polinomi non abbiano fattori in comune, allora per l'identità di Bezout, abbiamo che

$$\exists \widetilde{A} \text{ e } \widetilde{B} \text{ tali che } \ \widetilde{A}f + \widetilde{B}g = 1;$$

da ciò segue, essendo $Af + Bg = 0$,

$$B = Bg\widetilde{B} + Bf\widetilde{A} = (-Af)\widetilde{B} + B\widetilde{A}f = (\widetilde{A}B - A\widetilde{B})f;$$

quindi, dovendo essere $B \neq 0$, B ha almeno il grado di f, e ciò contraddice la condizione 3. . □

Per determinare i polinomi A e B, possiamo ricondurre il problema ad un sistema lineare omogeneo di $l + m$ equazioni in $l + m$ incognite.
Scriviamo A e B nella seguente forma:

$$\begin{aligned} A &= c_o x^{m-1} + c_1 x^{m-2} + \cdots + c_{m-1}; \\ B &= d_o x^{l-1} + d_1 x^{l-2} + \cdots + d_{l-1}. \end{aligned}$$

Il sistema si ottiene imponendo che valga

$$Af + Bg = 0 \tag{21}$$

(dove le incognite sono $c_0, \ldots, c_{m-1}, d_0, \ldots, d_{l-1}$).
Per ottenere il sistema in forma esplicita, scriviamo

$$\begin{aligned} f &= a_o x^l + a_1 x^{l-1} + \cdots + a_l, \text{ con } a_0 \neq 0 \\ g &= b_o x^m + b_1 x^{m-1} + \cdots + b_m, \text{ con } b_0 \neq 0. \end{aligned}$$

Andando a sostituire nella (21), si ha

$$\begin{array}{rcrcll} a_0 c_0 & + & b_0 d_0 & = 0 & \text{coefficiente di } x^{l+m-1} \\ a_1 c_0 + a_0 c_1 & + & b_1 d_0 + b_0 d_1 & = 0 & \text{coefficiente di } x^{l+m-2} \\ \ddots & & \ddots & \vdots & \\ & & a_l c_{m-1} \; + \; b_m d_{l-1} & = 0 & \text{coefficiente di } x^0 \end{array} \tag{22}$$

Tale sistema ammette una soluzione non nulla se e solo se la sua matrice dei coefficienti ha determinante nullo.

Definizione 3.29 *Siano $f, g \in k[x]$ due polinomi di grado positivo della forma seguente*

$$\begin{aligned} f &= a_o x^l + a_1 x^{l-1} + \cdots + a_l, \text{ con } a_0 \neq 0 \\ g &= b_o x^m + b_1 x^{m-1} + \cdots + b_m, \text{ con } b_0 \neq 0. \end{aligned}$$

Allora la ***matrice di Sylvester*** *di f e g rispetto ad x, denotata con* $\mathrm{Syl}(f, g, x)$, *è la matrice dei coefficienti del sistema (22). Quindi*

$$Syl(f,g,x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix},$$

dove gli spazi vuoti sono riempiti da zeri. Definiamo ***risultante*** *di f e g rispetto ad x, e lo denotiamo con* $\mathrm{Res}(f, g, x)$, *il determinante della matrice di Sylvester*

$$\mathrm{Res}(f, g, x) = \det(\mathrm{Syl}(f, g, x)).$$

Dalla definizione, segue immediatamente la seguente proposizione.

Proposizione 3.30 *Dati i polinomi $f, g \in k[x]$ di grado positivo , il risultante* $\mathrm{Res}(f, g, x)$ *è un polinomio intero (ovvero, a coefficienti in $\mathbb{Z}$) nei coefficienti di f e di g . Inoltre, f e g hanno un fattore comune in $k[x]$ se e solo se* $\mathrm{Res}(f, g, x) = 0$.

Dimostrazione
La tesi segue immediatamente dalla definizione di determinante di una matrice e dal modo in cui abbiamo costruito il risultante. □

Proposizione 3.31 *Dati due polinomi $f, g \in k[x]$ di gradi positivi l ed m, rispettivamente, esistono due polinomi $A, B \in k[x]$, tali che*

$$Af + Bg = \mathrm{Res}(f, g, x).$$

Inoltre, i coefficienti di A e di B sono polinomi interi nei coefficienti di f e di g.

Dimostrazione
Se $\mathrm{Res}(f, g, x) = 0$, basterà scegliere $A = B = 0$ per ottenere la tesi.
Supponiamo, dunque, che $\mathrm{Res}(f, g, x) \neq 0$, ovvero f, g non abbiano un fattore in comune. Dunque esistono $\widetilde{A}, \widetilde{B} \in k[x]$, di grado al più $m - 1$ ed $l - 1$, rispettivamente, tali che

$$\widetilde{A}f + \widetilde{B}g = 1. \tag{23}$$

Scriviamo ora

$$\begin{aligned} f &= a_o x^l + \cdots + a_l, \text{ con } a_0 \neq 0, \\ g &= b_o x^m + \cdots + b_m, \text{ con } b_0 \neq 0, \\ \widetilde{A} &= c_0 x^{m-1} + \cdots + c_{m-1} \\ \widetilde{B} &= d_0 x^{l-1} + \cdots + d_{l-1}. \end{aligned}$$

Andando a sostituire in (23), otteniamo il sistema

$$\begin{array}{rcrcll} a_0c_0 & + & b_0d_0 & = 0 & \text{coefficiente di } x^{l+m-1} \\ a_1c_0 + a_0c_1 & + & b_1d_0 + b_0d_1 & = 0 & \text{coefficiente di } x^{l+m-2} \\ \ddots & & \ddots & \vdots & \\ & & a_lc_{m-1} & + \; b_md_{l-1} = 1 & \text{coefficiente di } x^0 \end{array} \tag{24}$$

Questo sistema differisce dal (22) solo per la colonna dei termini noti, essendoci 1 al posto di 0 nel secondo membro dell'ultima equazione; la matrice dei coefficienti è la matrice di Sylvester per entrambi i sistemi, per cui, essendo

$$\det(\mathrm{Syl}(f,g,x)) = \mathrm{Res}(f,g,x) \neq 0,$$

esiste un'unica soluzione per il sistema (24), che è lineare non omogeneo; essa può essere determinata mediante la regola di Cramer; così, ad esempio, c_0 è data da

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

Dal momento che un determinante di una matrice è un polinomio intero nei suoi coefficienti, segue che

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

Tramite un procedimento analogo, otteniamo formule simili per gli altri c_i e d_i. Essendo $\widetilde{A} = c_0 x^{m-1} + \cdots + c_{m-1}$, possiamo scrivere $\widetilde{A}$ nella forma

$$\widetilde{A} = \frac{A}{\mathrm{Res}(f,g,x)}$$

dove $A \in k[x]$ e i suoi coefficienti sono polinomi interi negli a_i, b_i. In modo simile, scriviamo

$$\widetilde{B} = \frac{B}{\mathrm{Res}(f,g,x)}$$

con $B \in k[x]$ e i suoi coefficienti sono polinomi interi negli a_i, b_i. Infine, essendo valida la (23), moltiplicandola per $\mathrm{Res}(f,g,x)$, otteniamo

$$Af + Bg = \mathrm{Res}(f,g,x)$$

con A, B aventi i coefficienti richiesti dalla tesi. □

3.5 Risultanti e Teorema dell'Estensione

Per vedere che ruolo hanno i risultanti nel procedimento dell'estensione di soluzioni parziali a soluzioni totali, bisogna riformulare quanto ottenuto nella precedente sezione nel caso di polinomi a più variabili.

Definizione 3.32 *Siano $f, g \in k[x_1, \ldots, x_n]$ due polinomi di grado positivo in x_1; scriviamoli nella forma*

$$\begin{aligned} f = &\quad a_o x_1^l + \cdots + a_l, \ \textit{con } a_0 \neq 0, \\ g = &\quad b_o x_1^m + \cdots + b_m, \ \textit{con } b_0 \neq 0, \end{aligned} \tag{25}$$

dove gli $a_i, b_i \in k[x_2, \ldots, x_n]$. Definiamo ***risultante*** *di f e di g rispetto ad x_1 il seguente determinante*

$$\mathrm{Res}(f, g, x_1) = \ det \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}$$

dove gli spazi vuoti sono riempiti con zeri.

Per i risultanti di due polinomi a più variabili, otteniamo le seguenti proposizioni.

Proposizione 3.33 *Siano $f, g \in k[x_1, \ldots, x_n]$ due polinomi di grado positivo in x_1. Allora:*

1. *il risultante $\mathrm{Res}(f, g, x_1)$ appartiene al primo ideale di eliminazione $\langle f, g \rangle \cap k[x_2, \ldots, x_n]$;*
2. *il risultante $\mathrm{Res}(f, g, x_1) = 0$ se e solo se f e g hanno un fattore comune in $k[x_1, \ldots, x_n]$, avente grado positivo in x_1.*

Dimostrazione
1. Scriviamo nel solito modo f, g in termini di x_1. Per la Proposizione 3.30, applicata a $k(x_2, \ldots, x_n)[x_1]$, $\mathrm{Res}(f, g, x_1)$ è un polinomio intero nei coefficienti, rispetto ad x_1, di f e di g, quindi, in questo caso, esso appartiene a $k[x_2, \ldots, x_n]$. Inoltre, per la Proposizione 3.31, applicata a $k(x_2, \ldots, x_n)[x_1]$, esistono due polinomi in x_1, A e B tali che

$$\mathrm{Res}(f, g, x_1) = Af + Bg, \tag{26}$$

i coefficienti dei quali sono polinomi interi negli a_i, b_i; dunque, A e B appartengono all'anello $k[x_1, \ldots, x_n]$ ed, in virtù della (26), si ha

$$\mathrm{Res}(f, g, x_1) \in \langle f, g \rangle \cap k[x_2, \ldots, x_n].$$

2. Possiamo vedere i polinomi $f, g \in k[x_1, \ldots, x_n]$ come elementi dell'anello $k(x_2, \ldots, x_n)[x_1]$, dove $k(x_2, \ldots, x_n)$ è il campo delle frazioni di $k[x_2, \ldots, x_n]$. Per quanto visto per i polinomi in una variabile, $\mathrm{Res}(f, g, x_1) = 0$ se e solo se f e g hanno un fattore in comune in $k(x_2, \ldots, x_n)[x_1]$ di grado positivo in x_1, ma, essendo $k[x_1, \ldots, x_n]$ un UFD, ciò è equivalente ad avere un fattore comune di grado positivo in x_1 in $k[x_1, \ldots, x_n]$. □

Poniamoci, adesso, nel caso specifico, in cui k sia un campo algebricamente chiuso, ovvero $k = \overline{k}$; si ha subito il risultato seguente.

Corollario 3.34 *Se $f, g \in k[x]$, $\mathrm{Res}(f, g, x_1) = 0$ se e solo se f e g hanno una radice in comune.*

Proviamo la proposizione seguente, essenziale per la dimostrazione del Teorema dell'estensione.

Proposizione 3.35 *Dati $f, g \in k[x_1, \ldots, x_n]$, siano a_0, b_0 rispettivamente i coefficienti non nulli del termine di grado massimo in x_1 dei polinomi f, g. Se $\mathrm{Res}(f, g, x_1)$ si annulla in $(c_2, \ldots, c_n) \in k^{n-1}$, allora almeno uno tra a_0 e b_0 si annulla in $(c_2, \ldots, c_n)$, oppure esiste $c_1 \in k$ tale che i polinomi f e g si annullano in $(c_1, c_2, \ldots, c_n) \in k^n$.*

Dimostrazione
Denotiamo con $\boldsymbol{c}$ la $(n-1)$-upla $(c_2, \ldots, c_n)$. Per ottenere la tesi è sufficiente provare che $f(x_1, \boldsymbol{c})$ ed $g(x_1, \boldsymbol{c})$ hanno una radice in comune, quando $a_0(\boldsymbol{c})$ e

$b_0(\boldsymbol{c})$ sono entrambi diversi da zero.
Per ipotesi, $h = \mathrm{Res}(f, g, x_1)(\boldsymbol{c}) = 0$, ovvero

$$0 = h(\boldsymbol{c}) = \det \begin{pmatrix} a_0(\boldsymbol{c}) & & & b_0(\boldsymbol{c}) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0(\boldsymbol{c}) & \vdots & & b_0(\boldsymbol{c}) \\ a_l(\boldsymbol{c}) & & \vdots & b_m(\boldsymbol{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(\boldsymbol{c}) & & & b_m(\boldsymbol{c}) \end{pmatrix}. \tag{27}$$

Ma il determinante (27) è esattamente uguale a $\mathrm{Res}(f(x_1, \boldsymbol{c}), g(x_1, \boldsymbol{c}), x_1)$, ovvero quest'ultimo è nullo; quindi, per il Corollario 3.34, i due polinomi $f(x_1, \boldsymbol{c})$ e $g(x_1, \boldsymbol{c})$ hanno una radice in comune. □

Proveremo il Teorema dell'estensione in due passi: dapprima, proveremo tale teorema nel caso di ideali generati da due soli polinomi; successivamente, estenderemo la dimostrazione al caso generale.

Teorema 3.36 *Sia $I = \langle f, g\rangle \subset k[x_1, \ldots, x_n]$ ed I_1 il suo primo ideale di eliminazione. Siano $a_0, b_0 \in k[x_2, \ldots, x_n]$ i coefficienti del termine di grado massimo in x_1. Sia $(c_2, \ldots, c_n) \in \boldsymbol{V}(I_1)$, una soluzione parziale. Se $(c_2, \ldots, c_n) \notin \boldsymbol{V}(a_0, b_0)$, esiste $c_1 \in k$, tale che $(c_1, c_2, \ldots, c_n) \in \boldsymbol{V}(I)$.*

Dimostrazione
Denotiamo con $\boldsymbol{c}$ la $(n-1)$-upla $(c_2, \ldots, c_n)$. Abbiamo già visto nella Proposizione 3.33 che $\mathrm{Res}(f, g, x_1) \in I_1$, quindi si annulla nella soluzione parziale $\boldsymbol{c}$. Se nessuno tra a_0 e b_0 si annulla in $\boldsymbol{c}$, per la Proposizione 3.35, esiste $c_1 \in k$, tale che $(c_1, \boldsymbol{c}) \in \boldsymbol{V}(I)$. Ma, dall'ipotesi $\boldsymbol{c} \notin \boldsymbol{V}(a_0, b_0)$, possiamo dedurre solamente che almeno uno tra a_0 e b_0 non si annulla in $\boldsymbol{c}$. Supponiamo, ad esempio, che si abbia

$$a_0(\boldsymbol{c}) \neq 0 \quad e \quad b_0(\boldsymbol{c}) = 0.$$

In tal caso, occorre scegliere un'altra base per I. Sia $N \in \mathbb{N}$ grande abbastanza perché $x_1^N f$ abbia grado maggiore, nella variabile x_1, di g. Di certo, sussiste la seguente uguaglianza

$$\langle f, g\rangle = \langle f, g + x_1^N f\rangle.$$

In questo modo, ci siamo assicurati che il leading coefficient di $g + x_1^N f$ in x_1 sia a_0, che sappiamo non annullarsi in $\boldsymbol{c}$. Possiamo, ora, applicare la Proposizione 3.35 alla nuova base di I ed ottenere la tesi. □

Per ottenere la prova del Teorema dell'estensione, nel caso di un ideale arbitrario $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$, bisogna anzitutto dare la definizione di risultante di più di due polinomi.
Introduciamo, a tal fine, le $s-1$ nuove variabili $u_2, \ldots, u_s$ e sia

$$u_2 f_2 + \cdots + u_s f_s \in k[u_2, \ldots, u_s, x_1, \ldots, x_n].$$

Guardando f_1 come polinomio dello stesso anello, si consideri

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) \in k[u_2, \ldots, u_s, x_2, \ldots, x_n];$$

per definizione, esso è il **risultante** dei polinomi $f_1, \ldots, f_s$.
Inoltre, ponendo $u^\alpha = u_1^{\alpha_1} \cdot \cdots \cdot u_s^{\alpha_s}$, possiamo scrivere il risultante nel modo che segue

$$\mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) u^\alpha, \tag{28}$$

dove i polinomi $h_\alpha(x_2, \ldots, x_n) \in k[x_2, \ldots, x_n]$ sono detti *risultanti generalizzati* di $f_1, \ldots, f_s$.

Teorema 3.37 (Teorema dell'estensione) *Sia $I = \langle f_1, \ldots, f_s \rangle$ un ideale di $k[x_1, \ldots, x_n]$ ed I_1 il primo ideale di eliminazione di I. Per ogni $1 \leq i \leq s$, scriviamo f_i nella forma*

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

dove $N_i \geq 0$ e $g_i \in k[x_2, \ldots, x_n]$ è un polinomio non nullo. Data una soluzione parziale $(c_2, \ldots, c_n) \in \boldsymbol{V}(I_1)$, se $(c_2, \ldots, c_n) \notin \boldsymbol{V}(g_1, \ldots, g_s)$, allora esiste $c_1 \in k$ tale che $(c_1, c_2, \ldots, c_n) \in \boldsymbol{V}(I)$.

Dimostrazione
Poniamo $\boldsymbol{c} = (c_2, \ldots, c_n)$ e supponiamo che $s \geq 3$, avendo già provato il teorema nel caso in cui $s = 1, 2$.

Essendo, per ipotesi $\boldsymbol{c} \notin \boldsymbol{V}(g_1, \ldots, g_s)$, possiamo, senza perdita di generalità, supporre che g_1 non si annulli in $\boldsymbol{c}$. Scriviamo il risultante dei polinomi $f_1, \ldots, f_s$ nella forma (28) e siano $h_\alpha \in k[x_2, \ldots, x_n]$ i risultanti generalizzati. Proviamo che $h_\alpha \in I_1$. Sappiamo che esistono due polinomi $A, B \in k[u_2, \ldots, u_s, x_1, \ldots, x_n]$, tali che

$$Af_1 + B(u_2 f_2 + \cdots + u_s f_s) = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1). \tag{29}$$

Scriviamo $A = \sum_\alpha A_\alpha u^\alpha$ e $B = \sum_\alpha B_\alpha u^\alpha$, con $A_\alpha, B_\alpha \in k[x_1, \ldots, x_n]$, e $u_2 f_2 + \cdots + u_s f_s = \sum_{i \geq 2} u^{e_i} f_i$, dove gli e_i sono gli elementi della base canonica dello spazio vettoriale k^s. Fatto ciò, l'equazione (29) diviene

$$\begin{aligned}
\sum_\alpha h_\alpha u^\alpha &= \left(\sum_\alpha A_\alpha u^\alpha\right) f_1 + \left(\sum_\beta B_\beta u^\beta\right)\left(\sum_{i \geq 2} u^{e_i} f_i\right) \\
&= \sum_\alpha (A_\alpha f_1) u^\alpha + \sum_{i \geq 2, \beta} B_\beta f_i u^{\beta + e_i} \\
&= \sum_\alpha (A_\alpha f_1) u^\alpha + \sum_\alpha \left(\sum_{i \geq 2,\ \beta,\ \beta + e_i = \alpha} B_\beta f_i\right) u^\alpha \\
&= \sum_\alpha \left(A_\alpha f_1 + \sum_{i \geq 2,\ \beta,\ \beta + e_i = \alpha} B_\beta f_i\right) u^\alpha.
\end{aligned}$$

Otteniamo, dunque, che

$$h_\alpha = A_\alpha f_1 + \sum_{i \geq 2,\ \beta,\ \beta + e_i = \alpha} B_\beta f_i,$$

il che prova che $h_\alpha \in I \cap kx_2, \ldots, x_n] = I_1$, per ogni α.
Essendo $\boldsymbol{c} \in \boldsymbol{V}(I_1)$, si ha che $h_\alpha(\boldsymbol{c}) = 0$ per ogni α, e ciò, in virtù della (28), implica che il risultante $h = \mathrm{Res}(f_1, u_2 f_2 + \cdots + u_s f_s, x_1)$ si annulla identicamente se valutato in $\boldsymbol{c}$, ovvero si ha

$$h(\boldsymbol{c}, u_2, \ldots, u_s) = 0. \tag{30}$$

Supponiamo adesso che

$$g_2(\boldsymbol{c}) \neq 0 \text{ e che } f_2 \text{ abbia grado in } x_1 \text{ maggiore di } f_3, \ldots, f_s. \tag{31}$$

Da ciò segue che

$$h(\boldsymbol{c}, u_2, \ldots, u_s) = \mathrm{Res}(f_1(x_1, \boldsymbol{c}), u_2 f_2(x_1, \boldsymbol{c}) + \cdots + u_s f_s(x_1, \boldsymbol{c}), x_1).$$

Difatti, supposto che i leading coefficients di f_1 e di $u_2f_2+\cdots+u_sf_s$ non siano nulli in $\boldsymbol{c}$, il che è garantito dalla (31), valutando h in $\boldsymbol{c}$, ottengo proprio il determinante risultante di $f_1(x_1, \boldsymbol{c})$ e di $u_2f_2(x_1, \boldsymbol{c})+\cdots+u_sf_s(x_1, \boldsymbol{c})$. Dunque abbiamo ottenuto che

$$\mathrm{Res}(f_1(x_1, \boldsymbol{c}), u_2f_2(x_1, \boldsymbol{c}) + \cdots + u_sf_s(x_1, \boldsymbol{c}), x_1) = 0,$$

ovvero che $f_1(x_1, \boldsymbol{c})$ e $u_2f_2(x_1, \boldsymbol{c}) + \cdots + u_sf_s(x_1, \boldsymbol{c})$ hanno un fattore F in comune di grado positivo in x_1 nell'anello $k[x_1, u_2, \ldots, u_s]$. Poiché F divide $f_1(x_1, \boldsymbol{c})$, esso deve appartenere a $k[x_1]$, e, quindi, perché esso possa dividere $u_2f_2(x_1, \boldsymbol{c}) + \cdots + u_sf_s(x_1, \boldsymbol{c})$, tutti gli $f_i(x_1, \boldsymbol{c})$ devono essere suoi multipli. In conclusione, avendo noi trovato un fattore comune $F \in k[x_1]$ agli $f_i(x_1, \boldsymbol{c})$, di grado positivo in x_1, esiste $c_1 \in k$, radice di F, tale che $(c_1, \boldsymbol{c}) \in \boldsymbol{V}(I)$.

Se per la base $\{f_1, f_2, \ldots, f_s\}$ non è vera la (31), basta sostituire ad f_2 il polinomio $f_2 + x_1^N f_1$ con $N \in \mathbb{N}$ grande abbastanza perché il leading coefficient di $f_2 + x_1^N f_1$ sia g_1, che non si annulla in $\boldsymbol{c}$, e perché $f_2 + x_1^N f_1$ abbia grado in x_1 maggiore di $f_3, \ldots, f_s$; ripetendo la dimostrazione per questa nuova base, abbiamo la tesi. □

Riferimenti bibliografici

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1961, pp. 17-37.

[2] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, Springer, 2007, pp. 47-164.

[3] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser Boston, 1985, pp. 1-29.