Università degli Studi di Milano
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica
A. A. 2003/2004

Basi di Groebner e loro applicazioni

Elaborato finale di
Gabriele CATANIA (matr. 626442)

Relatore: Prof. Alberto ALZATI

Indice

Capitolo 1

Varietà affini

1.1 Funzioni polinomiali e spazi affini

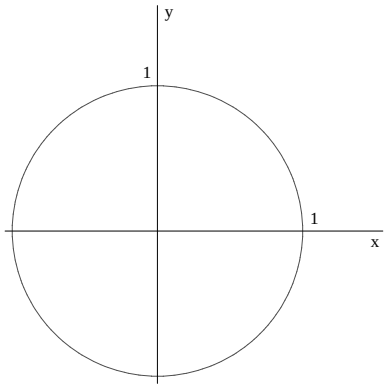
Definizione 1. *Sia* $\mathbb{K}$ *un campo, e siano* $f_1, \ldots, f_s$ *polinomi in* $\mathbb{K}[x_1, \ldots, x_n]$. *Allora definiamo*

$$\mathbf{V}(f_1, \ldots, f_s) = (a_1, \ldots, a_n) \in \mathbb{K}^n \,;\, f_i(a_1, \ldots, a_n) = 0 \quad \textit{per ogni} \, 1 \leq i \leq s$$

e chiamiamo $\mathbf{V}(f_1, \ldots, f_s)$ *la* ***varietà affine*** *definita da* $f_1, \ldots, f_s$.

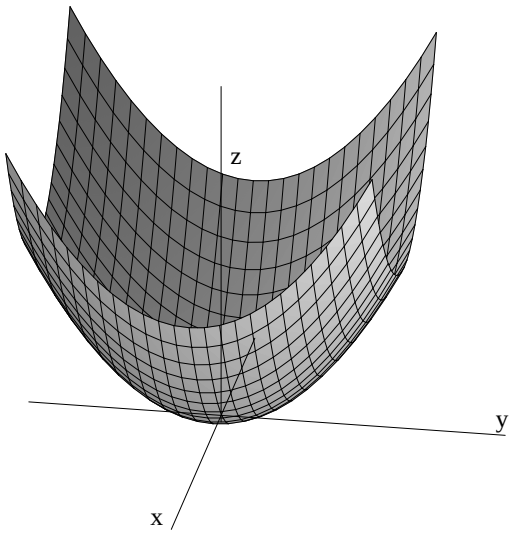
Quindi, una varietà affine $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{K}^n$ è l'insieme di tutte le soluzioni del sistema di equazioni $f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0$. Utilizzeremo le lettere *V, W*, ecc. per denotare varietà affini. Per chiarire meglio i termini del problema, poniamo $\mathbb{K} = \mathbb{R}$ e analizziamo quattro semplici esempi.

Esempio 1 : Nel piano $\mathbb{R}^2$, analizziamo la varietà $\mathbf{V}(x^2 + y^2 - 1)$. Si verifica facilmente che essa è il cerchio di raggio 1 centrato nell'origine:

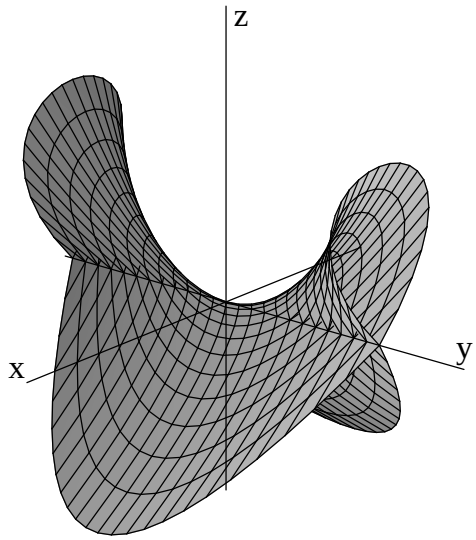


Esempio 2 : Passiamo ora allo spazio tridimensionale $\mathbb{R}^3$.

Una buona varietà affine è il paraboloide di rotazione $\mathbf{V}(z-x^2-y^2)$, ottenuto tramite rotazione della parabola $z=x^2$ attorno all'asse z. Otteniamo quindi il seguente grafico:

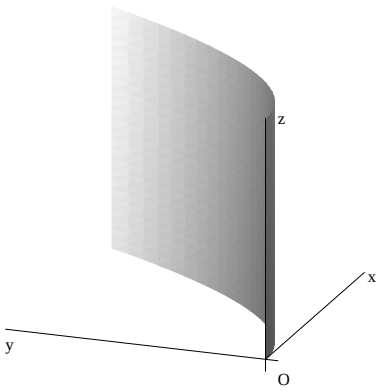


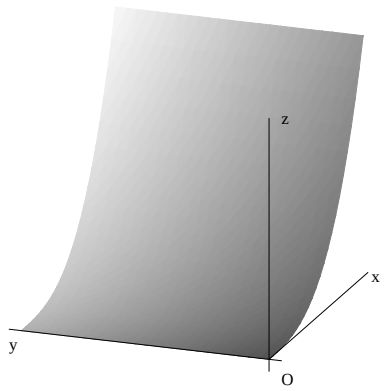
Esempio 3 : Una superficie molto più complicata è ottenuta da $\mathbf{V}(x^2-y^2z^2+z^3)$:



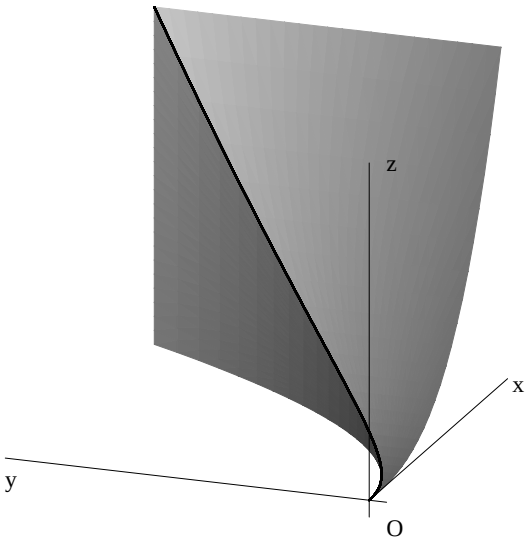
Nell'ultimo esempio, la superficie non è liscia ovunque: essa interseca sè stessa lungo tutto l'asse delle y. Questi sono esempi di *punti singolari*, di cui non ci occuperemo in questa tesi.

Esempio 4 : Vediamo ora una particolare curva di $\mathbb{R}^3$, detta *cubica gobba*. Essa è ottenuta dalla varietà $\mathbf{V}(y - x^2, z - x^3)$. Per semplicità, ci limiteremo alla porzione che giace sul primo ottante. Per cominciare, disegniamo le superfici $y = x^2$ e $z = x^3$ separatamente:





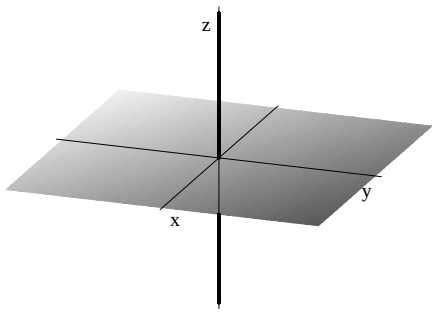
Quindi, la loro intersezione ci dà la cubica gobba:



Notiamo che quando avevamo una equazione in $\mathbb{R}^2$, abbiamo ottenuto una curva, ossia un oggetto 1-dimensionale. Una simile situazione accade in $\mathbb{R}^3$: una equazione in $\mathbb{R}^3$ dà solitamente origine ad una superfice, che ha dimensione 2. Di nuovo, la dimensione diminuisce di uno. Ma ora consideriamo la cubica gobba: qui, due equazioni in $\mathbb{R}^3$ danno una curva, quindi la dimensione diminuisce di due. Poiché ogni equazione impone un vincolo addizionale, l'intuito ci suggerisce che ogni equazione riduce la dimensione di uno. Così, se noi fossimo partiti da $\mathbb{R}^4$, ci saremmo aspettati che una varietà

affine definita da due equazioni fosse una superficie. Sfortunatamente, la nozione di dimensione è più sottile di quanto suggerito dai precedenti esempi. Per illustrare ciò, introduciamo un ulteriore esempio.

Esempio 5 : consideriamo la varietà $\mathbf{V}(xz, yz)$. Si verifica facilmente che le equazioni $xz = yz = 0$ definiscono l'unione del piano (x, y) con l'asse z:



Notiamo che questa varietà è formata da due componenti che hanno dimensioni differenti, una delle quali (il piano) ha dimensione "sbagliata" secondo la nostra precedente intuizione.

Diamo ora qualche esempio di varietà di dimensione maggiore. Un caso familiare è ottenuto dall'algebra lineare. Fissiamo infatti un campo $\mathbb{K}$ e consideriamo un sistema di m equazioni lineari in n incognite $x_1, \ldots, x_n$ con coefficienti in $\mathbb{K}$:

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1 \\ & \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m. \end{cases} \tag{1.1}$$

Le soluzioni di queste equazioni formano una varietà affine in $\mathbb{K}^n$, che chiameremo *varietà lineare*. Quindi, rette e piani sono varietà lineari, ed esistono esempi di dimensione arbitrariamente grande. Dall'algebra lineare conosciamo il metodo di riduzione matriciale (conosciuto anche come metodo di eliminazione di Gauss), che dà un algoritmo per trovare tutte le soluzioni di un tale sistema di equazioni. L'argomento di questa tesi è una generalizzazione di tale algoritmo, da applicare a sistemi di equazioni polinomiali.

Le varietà lineari sono in stretta relazione con la nostra discussione sulla dimensione. Infatti, se $V \subset \mathbb{K}^n$ è la varietà lineare definita da (1.1), allora V non ha necessariamente dimensione $n - m$ anche se V è definita da m equazioni. Infatti, se V non vuota, l'algebra lineare ci dice che V ha dimensione $n - r$, dove r è il rango della matrice (a_{ij}). Quindi, per varietà lineari la dimensione è determinata dal numero di equazioni *indipendenti*. Questa intuizione si applica a varietà affini più generali, salvo il fatto che la nozione di "indipendenza" è più sottile.

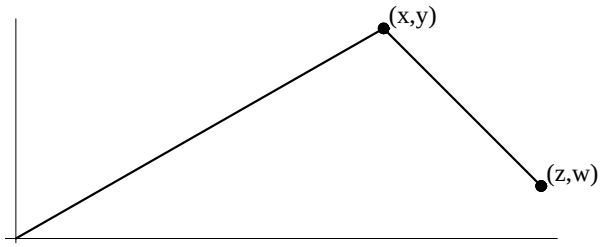
Esempio 6 : Possiamo considerare alcuni esempi complessi presi dall'analisi matematica. Supponiamo di voler trovare il massimo e minimo valore di $f(x, y, z) = x^3 + 2xyz - z^2$ soggetta al vincolo $g(x, y, z) = x^2 + y^2 + z^2 = 1$. Il metodo dei moltiplicatori di Lagrange afferma che $\nabla f = \lambda \nabla g$ per massimi e minimi locali[1]. Dobbiamo quindi risolvere il seguente sistema di quattro equazioni in quattro incognite, x, y, z, λ:

$$\begin{cases} 3x^2 + 2yz &= 2x\lambda, \\ 2xz &= 2y\lambda, \\ 2xy - 2z &= 2z\lambda, \\ x^2 + y^2 + z^2 &= 1. \end{cases} \tag{1.2}$$

Queste equazioni definiscono una varietà affine in $\mathbb{R}^4$, e la nostra intuizione riguardante la dimensione ci porta a sperare che consista di un insieme finito di punti (che ha dimensione 0) poiché è definita da quattro equazioni. Gli algoritmi che tratteremo in seguito ci forniranno uno strumento potente per risolvere problemi di questo tipo. In particolare, troveremo tutte le soluzioni delle precedenti equazioni.

Notiamo inoltre che le varietà affini possono essere l'insieme vuoto. Per esempio, quando $\mathbb{K} = R$, è ovvio che $\mathbf{V}(x^2 + y^2 + 1) = \emptyset$ poiché $x^2 + y^2 = -1$ non ha soluzioni reali (sebbene vi siano soluzioni per $\mathbb{K} = \mathbb{C}$). Un altro esempio è $\mathbf{V}(xy, xy - 1)$, che è l'insieme vuoto qualunque sia il campo, poiché x e y non possono soddisfare contemporaneamente $xy = 0$ e $xy = 1$. Esistono metodi (che non tratteremo in questa tesi) per determinare se una varietà affine su $\mathbb{C}$ è non vuota.

Esempio 7 : Per dare un'idea di alcune delle applicazioni delle varietà affini, consideriamo un semplice esempio dalla robotica. Supponiamo di avere, nel piano, un braccio meccanico formato da due rami collegati di lunghezza 1 e 2, con il ramo più lungo ancorato nell'origine:



Lo "stato" del braccio è completamente descritto dalle coordinate (x, y) e (z, w) indicate in figura. Quindi, lo stato può essere considerato come una 4-upla $(x, y, z, w) \in \mathbb{R}^4$. Però, non tutte le 4-uple sono stati del braccio. Infatti, è facile verificare che il sottoinsieme dei possibili stati è la varietà affine di $\mathbb{R}^4$ definita dalle equazioni

$$\begin{cases} x^2 + y^2 &= 4, \\ (x - z)^2 + (y - w)^2 &= 1. \end{cases}$$

[1]Ricordiamo che il gradiente di f è il vettore delle derivate parziali $\nabla f = (f_x, f_y, f_z)$

Notiamo come dimensioni maggiori possono essere facilmente introdotte: se avessimo considerato lo stesso braccio nello spazio 3-dimensionale, la varietà degli stati sarebbe stata definita da due equazioni in $\mathbb{R}^6$. Molte tecniche con importanti applicazioni nella teoria della robotica si basano sugli argomenti trattati in questo elaborato.

Finora, tutti i nostri disegni sono stati su $\mathbb{R}$. Più avanti nella trattazione, considereremo varietà su $\mathbb{C}$. Qui è più difficile (sebbene non impossibile) farsi un'idea "geometrica" dell'aspetto di tali varietà.

Infine, elenchiamo alcune proprietà elementari delle varietà affini.

Lemma 2. *Se $V, W \subset \mathbb{K}$ sono varietà affini, lo sono anche $V \cup W$ e $V \cap W$.*

Dimostrazione. Supponiamo che $V = \mathbf{V}(f_1, \ldots, f_s)$ e $W = \mathbf{V}(g_1, \ldots, g_t)$. Vogliamo ora affermare che

$$\begin{aligned} V \cap W &= \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t) \\ V \cup W &= \mathbf{V}(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t). \end{aligned}$$

La prima uguaglianza è banale: essere in $V \cap W$ significa imporre che le $f_1, \ldots, f_s$ e le $g_1, \ldots, g_t$ si annullino contemporaneamente, che equivale a imporre che $f_1, \ldots, f_s, g_1, \ldots, g_t$ si annullino.

La seconda uguaglianza richiede un po' più di lavoro. Se $(a_1, \ldots, a_n) \in V$, allora tutte le f_i si annullano in tale punto, e ciò implica l'annullarsi di tutte le $f_i g_j$ in $(a_1, \ldots, a_n)$. Da questo segue $V \subset \mathbf{V}(f_i g_j)$ e $W \subset \mathbf{V}(f_i g_j)$. Abbiamo dimostrato che $V \cup W \subset \mathbf{V}(f_i g_j)$. D'altra parte, scegliamo $(a_1, \ldots, a_n) \in \mathbf{V}(f_i g_j)$. Se questo sta in V abbiamo la tesi, altrimenti $f_{i_0}(a_1, \ldots, a_n) \neq 0$ per qualche i_0. Poiché $f_{i_0} g_j$ si annulla in $(a_1, \ldots, a_n)$ per ogni j, tutte le g_j devono ugualmente annullarsi in questo punto, e quindi $(a_1, \ldots, a_n) \in W$. Ciò implica $\mathbf{V}(f_i g_j) \subset V \cup W$. □

Una conseguenza di questo lemma è che intersezioni e unioni finite di varietà affini sono ancora varietà affini. Notiamo che abbiamo già visto esempi di unioni e intersezioni. Riguardo alle unioni, consideriamo l'unione del piano (x, y) con l'asse z nello spazio affine tridimensionale. Dalla formula precedente abbiamo

$$\mathbf{V}(z) \cup \mathbf{V}(x, y) = \mathbf{V}(zx, zy).$$

Questo, ovviamente, è uno degli esempi già discussi. Per quanto riguarda le intersezioni, ricordiamo che la cubica gobba è stata definita come intersezione di due superfici.

Gli esempi dati in questa sezione conducono ad alcune domande interessanti riguardanti le varietà affini. Supponiamo di avere $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Allora:

- (Consistenza) Possiamo determinare se $\mathbf{V}(f_1, \ldots, f_s) \neq 0$, ovvero, possiamo trovare una soluzione comune per le equazioni $f_1 = \cdots = f_s = 0$?
- (Finitezza) Possiamo determinare se $\mathbf{V}(f_1, \ldots, f_s)$ è finita, e se si possiamo trovare tutte le soluzioni in forma esplicita?
- (Dimensione) Possiamo determinare la "dimensione" di $\mathbf{V}(f_1, \ldots, f_s)$?

La risposta a queste domande è si, anche se dobbiamo prestare attenzione alla scelta del campo $\mathbb{K}$ su cui lavorare. Il problema più difficile riguarda la dimensione, poiché coinvolge concetti avanzati. Comunque, è possibile fornire soluzione completa a tutti e tre i problemi, sebbene ciò esuli dagli obiettivi di questa tesi.

1.2 Ideali

Definiamo ora l'oggetto algebrico di base della nostra trattazione.

Definizione 1. *Un sottoinsieme $I \subset \mathbb{K}[x_1, \ldots, x_n]$ è detto **ideale** se soddisfa:*

(i) $0 \in I$

(ii) *Se* $f, g \in I$, *allora* $f + g \in I$

(iii) *Se* $f \in I$ *e* $h \in \mathbb{K}[x_1, \ldots, x_n]$, *allora* $hf \in I$

Lo scopo di questa sezione è introdurre il lettore alla teoria degli ideali e mostrare come gli ideali sono in relazione con le varietà affini. La reale importanza degli ideali consiste nel fatto che essi ci danno un linguaggio per operare calcoli con le varietà affini.

Il primo esempio di ideale è quello generato da un numero finito di polinomi.

Definizione 2. *Siano $f_1, \ldots, f_s$ polinomi in $\mathbb{K}[x_1, \ldots, x_n]$. Allora poniamo*

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

Il fatto cruciale è che $\langle f_1, \ldots, f_s \rangle$ è un ideale.

Lemma 3. *Se $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, allora $\langle f_1, \ldots, f_s \rangle$ è un ideale di $\mathbb{K}[x_1, \ldots, x_n]$. Chiameremo $\langle f_1, \ldots, f_s \rangle$ l'**ideale generato da** $f_1, \ldots, f_s$.*

Dimostrazione. Prima di tutto, $0 \in \langle f_1, \ldots, f_s \rangle$ poiché $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Quindi, supponiamo $f = \sum_{i=1}^{s} p_i f_i$ e $g = \sum_{i=1}^{s} q_i f_i$, e sia $h \in \mathbb{K}[x_1, \ldots, x_n]$. Allora le equazioni

$$\begin{aligned} f + g &= \sum_{i=1}^{s} (p_i + q_i) f_i, \\ hf &= \sum_{i=1}^{s} (hp_i) f_i \end{aligned}$$

completano la dimostrazione che $\langle f_1, \ldots, f_s \rangle$ è un ideale. □

L'ideale $\langle f_1, \ldots, f_s \rangle$ ha una buona interpretazione in termini di equazioni polinomiali. Date $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, otteniamo il sistema di equazioni

$$\begin{cases} f_1 &= 0, \\ &\vdots \\ f_s &= 0. \end{cases}$$

Da queste equazioni possiamo ottenerne altre tramite passaggi algebrici. Per esempio, moltiplicando la prima equazione per $h_1 \in \mathbb{K}[x_1, \ldots, x_n]$, la seconda per $h_2 \in \mathbb{K}[x_1, \ldots, x_n]$, ecc., e sommando le equazioni risultanti, otteniamo

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0,$$

che è una conseguenza del nostro sistema originario. Notiamo che il primo membro dell'equazione è esattamente un elemento dell'ideale $\langle f_1, \ldots, f_s \rangle$. Quindi, possiamo pensare a $\langle f_1, \ldots, f_s \rangle$ come l'insieme di tutte le "conseguenze polinomiali" delle equazioni $f_1 = \cdots = f_s = 0$. Vediamo cosa ciò significhi in pratica introducendo un esempio.

Esempio 1 : Consideriamo le equazioni

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

ed eliminiamo t, ottenendo

$$y = x^2 - 2x + 2.$$

Scriviamo ora l'equazione nella forma

$$\begin{aligned} x - 1 - t &= 0, \\ y - 1 - t^2 &= 0. \end{aligned} \tag{1.3}$$

Per eliminare la variabile t, moltiplichiamo la prima equazione per $x - 1 + t$ e la seconda per -1:

$$\begin{aligned} (x-1)^2 - t^2 &= 0, \\ -y + 1 + t^2 &= 0. \end{aligned}$$

e sommando otteniamo

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

Nei termini dell'ideale generato dalle equazioni (1.3), possiamo riscrivere tutto nella forma

$$x^2 - 2x + 2 - y = (x - 1 + t)(x - 1 - t) + (-1)(y - 1 - t^2) \in \langle x - 1 - t, y - 1 - t^2 \rangle.$$

Similmente, ogni altra "conseguenza polinomiale" di (1.3) conduce ad un elemento di questo ideale.

Diciamo che I è *finitamente generato* se esistono $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ tali che $I = \langle f_1, \ldots, f_s \rangle$, e diciamo che $f_1, \ldots, f_s$ costituiscono una *base* per I. In seguito, dimostreremo che *ogni* ideale di $\mathbb{K}[x_1, \ldots, x_n]$ è finitamente generato (questo fatto è conosciuto come Teorema della Base di Hilbert). Notiamo che un dato ideale può avere più basi differenti. Più avanti, mostreremo che si può scegliere un tipo di base particolarmente utile, detta base di Groebner.

Si può qui stabilire una analogia con l'algebra lineare. La definizione di ideale è simile a quella di sottospazio: entrambi devono essere chiusi rispetto all'addizione e alla moltiplicazione, tranne per il fatto che in un sottospazio moltiplichiamo per uno scalare, mentre in un ideale moltiplichiamo per un polinomio. Inoltre, notiamo che l'ideale generato dai polinomi $f_1, \ldots, f_s$ è simile allo span (sottospazio generato) di un numero finito di vettori $v_1, \ldots, v_s$. In tutti e due i casi consideriamo combinazioni lineari, utilizzando coefficienti in un campo per lo span e coefficienti polinomiali per l'ideale generato.

Un'altra indicazione del ruolo giocato dagli ideali è la seguente proposizione, che mostra come una varietà dipenda solo dall'*ideale* generato dalle equazioni che la definiscono.

Proposizione 4. *Se $f_1, \ldots, f_s$ e $g_1, \ldots, g_t$ sono basi di uno stesso ideale in $\mathbb{K}[x_1, \ldots, x_n]$, tale che $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, allora $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.*

Esempio 2 : Consideriamo la varietà $\mathbf{V}(2x^2+3y^2-11, x^2-y^2-3)$. Si mostra facilmente che $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$, in modo tale che

$$\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}$$

per la proposizione precedente. Quindi, cambiando la base dell'ideale abbiamo potuto più facilmente determinare la varietà.

La possibilità di cambiare base senza modificare la varietà è molto importante, dal momento che ci porta a osservare che le varietà affini sono

determinate da *ideali*, non da equazioni. Da un punto di vista più pratico, vedremo che la Proposizione 4, combinata con le basi di Groebner sopra menzionate, fornisce uno strumento potente per comprendere le varietà affini.

Discutiamo ora come le varietà affini diano origine ad una classe interessante di ideali. Supponiamo di avere una varietà affine $V = \mathbf{V}(f_1, \ldots, f_s) \subset \mathbb{K}^n$ definita da $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Sappiamo che $f_1, \ldots, f_s$ si annullano su V, ma possiamo affermare che non ne esistono altre?

Esempio 3 : Consideriamo la cubica gobba studiata in precedenza (si veda 1.1). Essa è definita dall'annullarsi di $y - x^2$ e $z - x^3$. Si verifica però facilmente che $z - xy$ e $y^2 - xz$ sono altri due polinomi che si annullano sulla cubica gobba. Ci sono altri polinomi come questi? Come possiamo trovarli tutti?

Per studiare queste domande, considereremo l'insieme di *tutti* i polinomi che si annullano su una varietà data.

Definizione 5. *Sia $V \subset \mathbb{K}^n$ una varietà affine. Allora poniamo*

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

L'osservazione cruciale è che $\mathbf{I}(V)$ è un ideale.

Lemma 6. *Se $V \subset \mathbb{K}^n$ è una varietà affine, allora $\mathbf{I}(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ è un ideale. Chiameremo $\mathbf{I}(V)$ l'**ideale di** V.*

Dimostrazione. Ovviamente $0 \in \mathbf{I}(V)$, poiché il polinomio nullo si annulla su tutto $\mathbb{K}^n$, e quindi in particolare anche in V. Supponiamo ora $f, g \in \mathbf{I}(V)$ e $h \in \mathbb{K}[x_1, \ldots, x_n]$. Sia $(a_1, \ldots, a_n)$ un punto arbitrario di V. Allora

$$\begin{aligned} f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) &= 0 + 0 = 0, \\ h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) &= h(a_1, \ldots, a_n) \cdot 0 = 0, \end{aligned}$$

da cui segue che $\mathbf{I}(V)$ è un ideale. □

Esempio 4 : Consideriamo la varietà $\{(0,0)\}$, costituita dall'origine in $\mathbb{K}^2$. Allora il suo ideale $\mathbf{I}(\{(0,0)\})$ è formato da tutti i polinomi che si annullano nell'origine, e affermiamo che

$$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle.$$

Un verso dell'uguaglianza è banale, poiché ogni polinomio della forma $A(x,y)x + B(x,y)y$ si annulla nell'origine. Percorrendo l'altro verso, supponiamo che $f = \sum_{i,j} a_{ij} x^i y^j$ si annulli nell'origine. Allora $a_{00} = f(0,0) = 0$ e, conseguentemente,

$$\begin{aligned} f &= a_{00} + \sum_{i,j \neq 0,0} a_{ij} x^i y^j \\ &= 0 + \left(\sum_{\substack{i,j \\ i>0}} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j} y^{j-1} \right) y \in \langle x, y \rangle. \end{aligned}$$

La nostra tesi è quindi dimostrata.

Esempio 5 : Consideriamo ora la cubica gobba $V = \mathbf{V}(y-x^2, z-x^3) \subset \mathbb{R}^3$. Affermiamo che

$$\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle.$$

Per provare ciò, prima di tutto mostreremo che dato un polinomio $f \in \mathbb{R}[x, y, z]$, possiamo scrivere f nella forma

$$f = h_1(y - x^2) + h_2(z - x^3) + r, \tag{1.4}$$

dove $h_1, h_2 \in \mathbb{R}[x, y, z]$ e r è un polinomio nella sola variabile x. Prima di tutto consideriamo il caso in cui f è un monomio $x^\alpha y^\beta z^\gamma$. Allora il teorema binomiale ci dice che

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (x^2 + (y - x^2))^\beta (x^3 + (z - x^3))^\gamma \\ &= x^\alpha (x^{2\beta} + \text{termini in } \ y - x^2)(x^{3\gamma} + \text{termini in } \ z - x^3), \end{aligned}$$

e svolgendo le moltiplicazioni otteniamo

$$x^\alpha y^\beta z^\gamma = h_1(y - x^2) + h_2(z - x^3) + x^{\alpha+2\beta+3\gamma}$$

per qualche polinomio $h_1, h_2 \in \mathbb{R}[x, y, z]$. Quindi, (1.4) è vera in questo caso. Poiché una arbitraria $f \in \mathbb{R}[x, y, z]$ è una combinazione $\mathbb{R}$-lineare di monomi, segue che (1.4) vale in generale.

Possiamo ora dimostrare che $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$. Innanzitutto, dalla definizione della cubica gobba V, abbiamo $y - x^2, z - x^3 \in \mathbf{I}(V)$, e poiché $\mathbf{I}(V)$ è un ideale, segue che $h_1(y - x^2) + h_2(z - x^3) \in \mathbf{I}(V)$. Ciò prova che $\langle y - x^2, z - x^3 \rangle \subset \mathbf{I}(V)$. Per dimostrare l'inclusione inversa, sia $f \in \mathbf{I}(V)$ e sia

$$f = h_1(y - x^2) + h_2(z - x^3) + r$$

la scomposizione data da (1.4). Per dimostrare che r è nullo, utilizzeremo la parametrizzazione (t, t^2, t^3) della cubica gobba. Poiché f si annulla su V, otteniamo

$$0 = f(t, t^2, t^3) = 0 + 0 + r(t)$$

(ricordiamo che r è un polinomio nella sola x). Poiché t può essere un qualsiasi numero reale, $r \in \mathbb{R}[x]$ deve essere il polinomio nullo. Ma $r = 0$ mostra che f ha la forma richiesta, e $\mathbf{I}(V) = \langle y - x^2, z - x^3 \rangle$ è dimostrata.

Ciò che abbiamo fatto in (1.4) è una reminiscenza della divisione di polinomi, tranne per il fatto che stiamo dividendo per due polinomi invece che per uno solo. In realtà, (1.4) è un caso particolare dell'algoritmo di divisione generalizzato che vedremo più avanti.

Un corollario di questo esempio è che dato un polinomio $f \in \mathbb{R}[x, y, z]$, abbiamo $f \in \langle y - x^2, z - x^3 \rangle$ se e solo se $f(t, t^2, t^3)$ è identicamente nulla. Questo ci dà un algoritmo per decidere se un polinomio giace nell'ideale. Tuttavia, questo metodo dipende dalla parametrizzazione (t, t^2, t^3). C'è un modo per decidere se $f \in \langle y - x^2, z - x^3 \rangle$ senza utilizzare la parametrizzazione? In seguito, risponderemo positivamente a queste domande utilizzando le basi di Groebner e l'algoritmo della divisione generalizzato.

L'esempio della cubica gobba è molto suggestivo. Abbiamo cominciato con i polinomi $y - x^2$ e $z - x^3$, li abbiamo usati per definire una varietà affine,

abbiamo considerato tutte le funzioni che si annullano su di essa, e abbiamo ottenuto l'ideale generato da due polinomi. É naturale chiedersi se ciò accade in generale. Consideriamo allora $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Questo ci dà

$$\begin{array}{ccccc} \text{polinomi} & & \text{varietà} & & \text{ideali} \\ f_1, \ldots, f_s & \to & \mathbf{V}(f_1, \ldots, f_s) & \to & \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) \end{array}$$

e ci chiediamo ora se $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$. La risposta, sfortunatamente, non è sempre sì. La migliore risposta che possiamo dare è il seguente lemma:

Lemma 7. *Se $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, allora*

$$\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)),$$

sebbene l'uguaglianza non sia vera in generale.

Dimostrazione. Sia $f \in \langle f_1, \ldots, f_s \rangle$: allora $f = \sum_{i=1}^{s} h_i f_i$ per qualche polinomio $h_1, \ldots, h_s \in \mathbb{K}[x_1, \ldots, x_n]$. Poiché gli $f_1, \ldots, f_s$ si annullano su $\mathbf{V}(f_1, \ldots, f_s)$, si annulla anche $\sum_{i=1}^{s} h_i f_i$. Quindi $f \equiv 0$ su $\mathbf{V}(f_1, \ldots, f_s)$, il che dimostra $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.

Per la seconda parte del lemma, abbiamo bisogno di un esempio in cui $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ contiene strettamente $\langle f_1, \ldots, f_s \rangle$. Mostreremo che l'inclusione

$$\langle x^2, y^2 \rangle \subset \mathbf{I}(\mathbf{V}(x^2, y^2))$$

non è un'uguaglianza. Calcoliamo innanzitutto $\mathbf{I}(\mathbf{V}(x^2, y^2))$. Le equazioni $x^2 = y^2 = 0$ implicano che $\mathbf{V}(x^2, y^2) = \{(0, 0)\}$. Un precedente esempio ci ha però mostrato che l'ideale di $\{(0, 0)\}$ è $\langle x, y \rangle$. Per mostrare che quest'ultimo contiene strettamente $\langle x^2, y^2 \rangle$, notiamo che $x \notin \langle x^2, y^2 \rangle$, poiché nei polinomi nella forma $h_1(x, y)x^2 + h_2(x, y)y^2$, ogni monomio ha grado totale almeno due. □

Per campi arbitrari, la relazione tra $\langle f_1, \ldots, f_s \rangle$ e $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ può essere molto sottile. Tuttavia, su un campo algebricamente chiuso come $\mathbb{C}$, c'è una relazione naturale tra questi ideali, ottenuta tramite il teorema di Nullstellensatz, che omettiamo per brevità.

Sebbene per un campo generico $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ possa essere diverso da $\langle f_1, \ldots, f_s \rangle$, l'ideale della varietà contiene sempre informazioni sufficienti per determinare univocamente la varietà.

Proposizione 8. *Siano V e W varietà affini in $\mathbb{K}^n$. Allora*

(i) $V \subset W$ se e solo se $\mathbf{I}(V) \supset \mathbf{I}(W)$

(ii) $V = W$ *se e solo se* $\mathbf{I}(V) = \mathbf{I}(W)$

Dimostrazione. Si mostra facilmente che (ii) è una diretta conseguenza di (i). Per provare (i), supponiamo $V \subset W$. Allora ogni polinomio che si annulla su W si annulla anche su V, il che implica $\mathbf{I}(W) \subset \mathbf{I}(V)$. Ora, supponiamo $\mathbf{I}(W) \subset \mathbf{I}(V)$. Sappiamo che W è la varietà definita da certi polinomi $g_1, \ldots, g_t \in \mathbb{K}[x_1, \ldots, x_n]$. Allora $g_1, \ldots, g_t \in \mathbf{I}(W) \subset \mathbf{I}(V)$, e di conseguenza le g_i si annullano su V. Poiché W è formato da tutti gli zeri comuni delle g_i, deve essere $V \subset W$. □

Ci sono molte relazioni tra ideali e varietà affini; il materiale presentato fino ad ora è solo la punta dell'iceberg. Infatti, molti teoremi riguardanti gli ideali hanno forti implicazioni geometriche. Ai fini della nostra trattazione, ci limiteremo però a porre le seguenti domande riguardanti gli ideali in $\mathbb{K}[x_1, \ldots, x_n]$:

- (Descrizione) Possiamo scrivere ogni ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ come $\langle f_1, \ldots, f_s \rangle$ per qualche $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$?
- (Appartenenza) Date $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, c'è un procedimento per decidere se una data $f \in \mathbb{K}[x_1, \ldots, x_n]$ è contenuta in $\langle f_1, \ldots, f_s \rangle$?
- (Nullstellensatz) Date $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, qual è la relazione tra $\langle f_1, \ldots, f_s \rangle$ e $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$?

In seguito risolveremo questi problemi (e spiegheremo la provenienza del nome "Nullstellensatz"), ma dovremo prestare attenzione al campo su cui lavorare.

1.3 Polinomi in una variabile

In questa sezione, tratteremo i polinomi di una variabile e studieremo l'*algoritmo euclideo della divisione*. Questo semplice algoritmo ha conseguenze sorprendentemente profonde: ad esempio, lo utilizzeremo per determinare la struttura degli ideali di $\mathbb{K}[x]$ e per esplorare l'dea di *massimo comun divisore*. La teoria sviluppata ci permetterà di risolvere, nel caso speciale di polinomi in $\mathbb{K}[x]$, gran parte dei problemi sollevati nelle sezioni precedenti. Incominceremo anche a comprendere il ruolo importante giocato dagli algoritmi.

Informalmente, un algoritmo è uno specifico insieme di istruzioni per manipolare dati simbolici o numerici. Ne sono esempi le formule di differenziazione nel calcolo e il metodo di riduzione diagonale dall'algebra lineare.

Un algoritmo avrà *input*, oggetti utilizzati dall'algoritmo, e *output*, ovvero i risultati. Ad ogni passaggio, l'algoritmo deve specificare esattamente quale sarà il passo successivo.

Per studiare un algoritmo, lo presenteremo solitamente in "pseudocodice", per rendere più facile la comprensione della struttura formale. Inoltre, esso dà una indicazione di come l'algoritmo possa essere implementato su un computer.

Cominciamo col discutere l'algoritmo della divisione per polinomi in $\mathbb{K}[x]$. Un elemento cruciale di questo algoritmo è la nozione di "termine direttivo" di un polinomio in una variabile. La definizione precisa è la seguente.

Definizione 1. *Dato un polinomio non nullo $f \in \mathbb{K}[x]$, sia*

$$f = a_0x^m + a_1x^{m-1} + \cdots + a_m,$$

dove $a_i \in \mathbb{K}$ e $a_0 \neq 0$ [quindi $m = \deg(f)$]. Allora diciamo che a_0x^m è il ***termine direttivo*** *di f, e lo indichiamo $\text{LT}(f) = a_0x^m$.*

Ad esempio, se $f = 2x^3 - 4x + 3$, allora $\text{LT}(f) = 2x^3$. Notiamo inoltre che se f e g sono polinomi non nulli, allora

$$\deg(f) \leq \deg(g) \Leftrightarrow \text{LT}(f) \text{ divide } \text{LT}(g). \tag{1.5}$$

Possiamo ora descrivere l'algoritmo.

Proposizione 2. *(Algoritmo della Divisione) Sia $\mathbb{K}$ un campo e g un polinomio non nullo in $\mathbb{K}[x]$. Allora ogni $f \in \mathbb{K}[x]$ può essere scritto come*

$$f = qg + r,$$

dove $q, r \in \mathbb{K}[x]$, e $r = 0$ oppure $\deg(r) < \deg(g)$. Inoltre, q e r sono unici e possono essere determinati con un algoritmo.

Dimostrazione. Presentiamo l'algoritmo per trovare q e r in pseudocodice.

`Input:` g, f
`Output:` q, r

$q := 0, r := f$
`WHILE` $r \neq 0$ `AND` $\text{LT}(g)$ `divide` $\text{LT}(f)$ `DO`
    $q := q + \text{LT}(r)/\text{LT}(g)$
    $r := r - (\text{LT}(r)/\text{LT}(g))$

Il costrutto `WHILE...DO` indica il ripetersi delle operazioni indentate fino a che l'espressione tra `WHILE` e `DO` diventa falsa. I costrutti $q := \cdots$ e $r := \cdots$

indicano l'assegnamento di valori per q e r. Sia q che r sono *variabili* in questo algoritmo. Dobbiamo mostrare che l'algoritmo termina e che i valori finali di q e r hanno le proprietà richieste.

Per vedere perché l'algoritmo funziona, prima di tutto notiamo che $f = qg + r$ è vera per i valori iniziali di q e r, e che ogni volta che ad essi vengono assegnati nuovi valori, l'uguaglianza rimane vera. Ciò accade grazie all'identità

$$f = qg + r = (q + \text{LT}(r)/\,\text{LT}(g))g + (r - (\text{LT}(r)/\,\text{LT}(g))g).$$

Ora, notiamo che il ciclo `WHILE...DO` termina quando "$r \neq 0$ `and` $\text{LT}(g)$ `divide` $\text{LT}(f)$" è falso, ovvero quando $r = 0$ oppure $\text{LT}(g)$ non divide $\text{LT}(r)$. Per (1.5), quest'ultima condizione è equivalente a $\deg(r) < \deg(g)$. Quindi, quando l'algoritmo termina produce q e r con le proprietà richieste.

Non abbiamo ancora finito; dobbiamo ancora mostrare che l'algoritmo termina, cioé che l'espressione tra `WHILE` e `DO` è definitivamente falsa (altrimenti, rimarremmo fermi in un ciclo infinito). L'osservazione chiave è che $r - (\text{LT}(r)/\,\text{LT}(g))$ è nullo o ha grado strettamente minore di r. Per dimostrarlo, supponiamo

$$\begin{aligned} r &= a_0x^m + \cdots + a_m, \quad \text{LT}(r) = a_0x^m, \\ g &= b_0x^k + \cdots + b_k, \quad \text{LT}(g) = b_0x^k, \end{aligned}$$

e supponiamo $m \geq k$. Allora

$$r - (\text{LT}(r)/\,\text{LT}(g))g = (a_0x^m + \cdots) - (a_0/b_0)x^{m-k}(b_0x^k + \cdots),$$

da cui segue che il grado di r deve diminuire (o che tutta l'espressione si annulla). Poiché il grado è finito, può diminuire al più un numero finito di volte, e quindi l'algoritmo termina.

Il passo finale della dimostrazione consiste nel mostrare che q e r sono univocamente determinati. Supponiamo $f = qg + r = q'g + r'$ dove sia r che r' hanno grado minore di g, o almeno uno di essi è nullo. Se $r \neq r'$, allora $\deg(r - r') < \deg(g)$. D'altra parte, poiché

$$(q - q')g = r' - r, \tag{1.6}$$

avremmo $q - q' \neq 0$, e di conseguenza

$$\deg(r - r') = \deg((q - q')g) = \deg(q - q') + \deg(g) \geq \deg(g).$$

Questa contraddizione impone $r = r'$, e quindi (1.6) implica $q = q'$. Questo completa la dimostrazione. □

Gran parte dei sistemi informatici di algebra implementa l'algoritmo sopra citato per dividere polinomi.

Un utile corollario dell'algoritmo della divisione riguarda il numero di radici di un polinomio in una variabile.

Corollario 3. *Se $\mathbb{K}$ è un campo e $f \in \mathbb{K}[x]$ è un polinomio non nullo, allora f ha al più* $\deg(f)$ *radici in $\mathbb{K}$.*

Dimostrazione. Faremo induzione su $m = \deg(f)$. Per $m = 0$, f è una costante non nulla, e il corollario è banalmente vero. Supponiamolo vero per ogni polinomio di grado $m-1$ e sia f di grado m. Se f non ha radici in $\mathbb{K}$, abbiamo la tesi. Supponiamo allora a radice in $\mathbb{K}$ di f. Se dividiamo f per $x-a$, la Proposizione 2 ci dice che $f = q(x-a)+r$, dove $r \in \mathbb{K}$ poiché $x-a$ ha grado uno. Per determinare r, valutiamo entrambi i membri per $x = a$ ottenendo $0 = f(a) = q(a)(a-a)+r = r$ da cui segue che $f = q(x-a)$. Notiamo inoltre che q ha grado $m-1$.

Vogliamo dimostrare che ogni radice di f diversa da a è anche una radice di q. Sia $b \neq a$ una radice di f: allora $0 = f(b) = q(b)(b-a)$ implica $q(b) = 0$ poiché $\mathbb{K}$ è un campo. Dal momento che q ha al massimo $m-1$ radici per ipotesi di induzione, f ha al massimo m radici in $\mathbb{K}$. □

Il corollario 3 può essere utilizzato per dimostrare che $\mathbf{I}(\mathbb{K}^n) = \{0\}$ per ogni $\mathbb{K}$ infinito. Questo è un esempio di come un fatto geometrico possa essere conseguenza di un algoritmo.

Possiamo utilizzare la Proposizione 2 per determinare la struttura di tutti gli ideali di $\mathbb{K}[x]$.

Corollario 4. *Se $\mathbb{K}$ è un campo, ogni ideale di $\mathbb{K}[x]$ può essere scritto nella forma $\langle f \rangle$ per qualche $f \in \mathbb{K}[x]$. Inoltre, f è unico a meno di moltiplicazioni per elementi non nulli di $\mathbb{K}$.*

Dimostrazione. Consideriamo in un ideale $I \subset \mathbb{K}[x]$. Se $I = \{0\}$ abbiamo la tesi, infatti $I = \langle 0 \rangle$. Altrimenti, sia f un polinomio non nullo di grado minimo contenuto in I. Vogliamo dimostrare che $\langle f \rangle = I$. L'inclusione $\langle f \rangle \subset I$ è ovvia dal momento che I è un ideale. Percorrendo l'altro verso, prendiamo $g \in I$. Per l'algoritmo della divisione (Proposizione 2), abbiamo $g = qf + r$, dove $r = 0$ oppure $\deg(r) < \deg(f)$. Poiché I è un ideale, $qf \in I$ e, di conseguenza, $r = g - qf \in I$. Se r non fosse zero, allora avremmo $\deg(r) < \deg(f)$, che sarebbe in contraddizione con la nostra scelta di f. Quindi abbiamo $r = 0$, che implica $g = qf \in \langle f \rangle$. Ciò dimostra che $I = \langle f \rangle$.

Per studiare l'unicità, supponiamo $\langle f \rangle = \langle g \rangle$. Allora $f \in \langle g \rangle$ implica $f = hg$ per qualche polinomio h. Allora

$$\deg(f) = \deg(h) + \deg(g), \tag{1.7}$$

e quindi $\deg(f) \geq \deg(g)$. Lo stesso ragionamento scambiando f e g mostra che $\deg(g) \geq \deg(f)$, da cui segue $\deg(f) = \deg(g)$. Allora (1.7) implica che $\deg(h) = 0$, quindi h è una costante non nulla. □

In generale, un ideale generato da un solo elemento è detto *ideale principale*. Grazie al Corollario 4 possiamo affermare che $\mathbb{K}[x]$ è un *dominio a ideali principali*, abbreviato PID[2].

La dimostrazione del Corollario 4 ci dice che il generatore di un ideale è il polinomio non nullo di grado minimo contenuto nell'ideale. Questa descrizione non è utile in pratica, perché ci obbliga a controllare il grado di tutti i polinomi (infiniti in generale) nell'ideale. C'è un modo migliore di trovare il generatore? Ad esempio, come possiamo trovare il generatore dell'ideale

$$\langle x^4 - 1, x^6 - 1 \rangle \subset \mathbb{K}[x]?$$

Lo strumento necessario per risolvere questo problema è il massimo comun divisore.

Definizione 5. *Il* ***massimo comun divisore*** *di due polinomi $f, g \in \mathbb{K}[x]$ è un polinomio h tale che:*

(i) h divide f e g

(ii) Se p divide f e g, allora p divide h.

Indichiamo allora $h = \text{MCD}(f, g)$.

Ecco le principali proprietà dell'MCD.

Proposizione 6. *Siano $f, g \in \mathbb{K}[x]$. Allora:*

(i) $\text{MCD}(f, g)$ esiste ed è unico a meno di moltiplicazioni per costanti non nulle di $\mathbb{K}$.

(ii) $\text{MCD}(f, g)$ è un generatore dell'ideale $\langle f, g \rangle$.

(iii) Esiste un algoritmo per trovare $\text{MCD}(f, g)$.

Dimostrazione. Consideriamo l'ideale $\langle f, g \rangle$. Poiché ogni ideale di $\mathbb{K}[x]$ è principale (Corollario 4), esiste $h \in \mathbb{K}[x]$ tale che $\langle f, g \rangle = \langle h \rangle$. Vogliamo dimostrare che h è l'MCD tra f e g. Per fare ciò, prima di tutto notiamo che h divide f e g dal momento che $f, g \in \langle h \rangle$. Quindi, la prima parte della definizione è soddisfatta. Ora, supponiamo che $p \in \mathbb{K}[x]$ divida f e g. Questo

[2]Dall'inglese "*Principal Ideal Domain*".

significa che $f = Cp$ e $g = Dp$ per qualche $C, D \in \mathbb{K}[x]$. Poiché $h \in \langle f, g \rangle$, esistono A, B tali che $Af + Bg = h$. Sostituendo, otteniamo

$$h = Af + Bg = ACp + BDp = (AC + BD)p,$$

da cui p divide h. Quindi, $h = \text{MCD}(f, g)$.

Questo prova l'esistenza dell'MCD. Per provare l'unicità, supponiamo che h' sia un altro MCD di f e g. Allora, per la seconda parte della definizione, h e h' si dividerebbero a vicenda. Questo implica che h è multiplo di h'. Quindi, la parte (i) è dimostrata, e la parte (ii) segue dal modo in cui abbiamo trovato h nel paragrafo precedente.

La dimostrazione di esistenza appena fornita non è utile nella pratica, in quanto dipende dalla capacità di trovare un generatore per $\langle f, g \rangle$. Come abbiamo osservato nella discussione successiva al Corollario 4, questo richiede il controllo del grado per infiniti polinomi. Fortunatamente, c'è un algoritmo classico, conosciuto con il nome di *algoritmo euclideo delle divisioni successive*, che calcola l'MCD di due polinomi in $\mathbb{K}[x]$. Questo è ciò di cui tratta la parte (iii).

Avremo bisogno della seguente notazione: siano $f, g \in \mathbb{K}[x]$, con $g \neq 0$, e scriviamo $f = qg + r$, dove q e r sono dati dalla Proposizione 2. Indicheremo allora $r = \texttt{resto}(f, g)$. Possiamo ora enunciare l'algoritmo euclideo per trovare $\text{MCD}(f, g)$.

```
Input:  f, g
Output: h

h := f
s := g
WHILE s ≠ 0 DO
      re =resto(h, s)
      h := s
      s := re
```

Per vedere perché questo algoritmo calcoli l'MCD, scriviamo $f = qg + r$ come nella Proposizione 2. Vogliamo dimostrare che

$$\text{MCD}(f, g) = \text{MCD}(f - qg, g) = \text{MCD}(r, g). \tag{1.8}$$

Per dimostrare ciò, dalla parte (ii) della proposizione, è sufficiente dimostrare che gli ideali $\langle f, g \rangle$ e $\langle f - qg, g \rangle$ sono uguali (omettiamo questa dimostrazione per brevità).

Possiamo scrivere 1.8 nella forma

$$\text{MCD}(f, g) = \text{MCD}(g, r).$$

Notiamo che $\deg(g) > \deg(r)$ oppure $r = 0$. Se $r \neq 0$, possiamo ridurre il problema iterando il procedimento. Infatti, scriviamo $g = q'r + r'$ come nella Proposizione 2, e argomentando come sopra, otteniamo

$$\text{MCD}(g, r) = \text{MCD}(r, r'),$$

dove $\deg(r) > \deg(r')$ oppure $r' = 0$. Continuando nello stesso modo, abbiamo

$$\text{MCD}(f, g) = \text{MCD}(g, r) = \text{MCD}(r, r') = \text{MCD}(r', r'') = \cdots , \qquad (1.9)$$

dove il grado diminuisce

$$\deg(g) > \deg(r) > \deg(r') > \deg(r'') > \cdots ,$$

oppure il processo termina quando uno degli $r, r', r'', \ldots$ si annulla.

Possiamo ora spiegare come funziona l'algoritmo euclideo. Esso ha come variabili h e s, come possiamo vedere nell'equazione (1.9): i valori di h sono i primi polinomi in ogni MCD, e i valori di s sono i secondi. Si verifica facilmente che in (1.9) il passaggio da un MCD al successivo è esattamente ciò che viene fatto nel ciclo `WHILE...DO` dell'algoritmo. Quindi, ad ogni passaggio $\text{MCD}(h, s) = \text{MCD}(f, g)$.

L'algoritmo deve necessariamente terminare dal momento che il grado di s decresce ad ogni passaggio, quindi ad un certo punto avremo $s = 0$. Quando ciò accade, abbiamo $\text{MCD}(h, 0) = \text{MCD}(f, g)$, e poiché $\langle h, 0 \rangle$ è evidentemente uguale a $\langle h \rangle$, abbiamo $\text{MCD}(h, 0) = h$. Combinando queste ultime due equazioni otteniamo $h = \text{MCD}(f, g)$ per $s = 0$. Questo dimostra che h è l'MCD di f e g quando l'algoritmo termina, e la dimostrazione è quindi completa. □

Esempio 1 : Per mostrare il funzionamento dell'algoritmo euclideo, calcoliamo l'MCD tra $x^4 - 1$ e $x^6 - 1$. Prima di tutto utilizziamo l'algoritmo della divisione:

$$\begin{aligned} x^4 - 1 &= 0(x^6 - 1) + x^4 - 1, \\ x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1, \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0. \end{aligned}$$

Quindi, dall'equazione (1.9) abbiamo

$$\begin{aligned} \text{MCD}(x^4 - 1, x^6 - 1) &= \text{MCD}(x^6 - 1, x^4 - 1) \\ &= \text{MCD}(x^4 - 1, x^2 - 1) = \text{MCD}(x^2 - 1, 0) = x^2 - 1. \end{aligned}$$

Notiamo che questo calcolo dell'MCD risponde alle nostre precedenti esigenze di trovare un generatore per l'ideale $\langle x^4 - 1, x^6 - 1 \rangle$. Precisamente, la Proposizione 6 e $\text{MCD}(x^4 - 1, x^6 - 1) = x^2 - 1$ implicano

$$\langle x^4 - 1, x^6 - 1 \rangle = \langle x^2 - 1 \rangle.$$

A questo punto, è naturale chiedersi cosa accada per un ideale generato da tre o più polinomi.

Definizione 7. *Il* ***massimo comun divisore*** *di polinomi $f_1, \ldots, f_s \in \mathbb{K}[x]$ è un polinomio h tale che*

(i) h divide $f_1, \ldots, f_s$.

(ii) Se p è un altro polinomio che divide $f_1, \ldots, f_s$, allora p divide h.

Quando h ha queste proprietà, scriviamo $h = \text{MCD}(f_1, \ldots, f_s)$.

Ecco le principali proprietà di questi MCD.

Proposizione 8. *Siano $f_1, \ldots, f_s \in \mathbb{K}[x]$, dove $s \geq 2$. Allora*

(i) $\text{MCD}(f_1, \ldots, f_s)$ esiste ed è unico a meno di moltiplicazioni per costanti non nulle di $\mathbb{K}$.

(ii) $\text{MCD}(f_1, \ldots, f_s)$ è un generatore dell'ideale $\langle f_1, \ldots, f_s \rangle$.

(iii) Se $s \geq 3$, allora $\text{MCD}(f_1, \ldots, f_s) = \text{MCD}(f_1, \text{MCD}(f_2, \ldots, f_s))$.

(iv) Esiste un algoritmo per trovare $\text{MCD}(f_1, \ldots, f_s)$.

Dimostrazione. La dimostrazione dei punti (i) e (ii) è simile a quella data nella Proposizione 6 e sarà omessa. Per dimostrare il punto (iii), sia $h = \text{MCD}(f_2, \ldots, f_s)$. Si mostra facilmente che

$$\langle f_1, h \rangle = \langle f_1, f_2, \ldots, f_s \rangle.$$

Per il punto (ii) di questa proposizione, notiamo che

$$\langle \text{MCD}(f_1, h) \rangle = \langle \text{MCD}(f_1, \ldots, f_s) \rangle.$$

Allora $\text{MCD}(f_1, h) = \text{MCD}(f_1, \ldots, f_s)$ segue dall'unicità del generatore di un ideale (Corollario 4), il che dimostra ciò che ci interessa.

Resta da dimostrare che esiste un algoritmo per trovare $\text{MCD}(f_1, \ldots, f_s)$. L'idea di base è combinare il punto (iii) con l'algoritmo euclideo. Per esempio, supponiamo di voler calcolare l'MCD di quattro polinomi f_1, f_2, f_3, f_4. Utilizzando due volte il punto (iii) della proposizione, otteniamo

$$\begin{aligned} \text{MCD}(f_1, f_2, f_3, f_4) &= \text{MCD}(f_1, \text{MCD}(f_2, f_3, f_4)) \\ &= \text{MCD}(f_1, \text{MCD}(f_2, \text{MCD}(f_3, f_4))). \end{aligned} \tag{1.10}$$

Iterando quindi l'algoritmo euclideo una volta per ogni MCD nella seconda riga di (1.10), otteniamo l'MCD tra f_1, f_2, f_3, f_4. Per brevità, non enunciamo qui il listato in pseudocodice dell'algoritmo. □

Esempio 2 : Il comando MCD implementato nella maggioranza dei programmi di computazione algebrica gestisce solo due polinomi alla volta. Quindi, per lavorare con più di due polinomi avremo bisogno di utilizzare il metodo descritto nella dimostrazione della Proposizione 8. Per esempio, consideriamo l'ideale

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1\rangle \subset \mathbb{K}[x].$$

Sappiamo che $\text{MCD}(x^3 - 3x + 2, x^4 - 1, x^6 - 1)$ è un generatore. Inoltre, si può mostrare che

$$\begin{aligned} \text{MCD}(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \text{MCD}(x^3 - 3x + 2, \text{MCD}(x^4 - 1, x^6 - 1)) \\ &= \text{MCD}(x^3 - 3x + 2, x^2 - 1) = x - 1. \end{aligned}$$

Ne segue che

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1\rangle = \langle x - 1\rangle.$$

Più in generale, dati $f_1, \ldots, f_s \in \mathbb{K}[x]$, è chiaro che ora conosciamo un algoritmo per trovare un generatore di $\langle f_1, \ldots, f_s\rangle$.

Per un'altra applicazione degli algoritmi qui sviluppati, consideriamo il *problema di appartenenza all'ideale* visto nella Sezione 1.2: dati $f_1, \ldots, f_s \in \mathbb{K}[x]$, esiste un algoritmo per decidere se un polinomio dato $f \in \mathbb{K}[x]$ giace nell'ideale $\langle f_1, \ldots, f_s\rangle$? La risposta è sì, e l'algoritmo è semplice da descrivere. Il primo passo consiste nell'utilizzare gli MCD per trovare un generatore h di $\langle f_1, \ldots, f_s\rangle$. Poi, dal momento che $f \in \langle f_1, \ldots, f_s\rangle$ è equivalente a $f \in \langle h\rangle$, dobbiamo semplicemente utilizzare l'algoritmo della divisione per scrivere $f = qh + r$, dove $\deg(r) < \deg(h)$. Ne segue che f appartiene all'ideale se e solo se $r = 0$.

Esempio 3 : Supponiamo di voler sapere se

$$x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1\rangle.$$

Abbiamo visto nell'esempio precedente che $x - 1$ è un generatore per questo ideale, quindi possiamo riformulare la nostra domanda:

$$x^3 + 4x^2 + 3x - 7 \in \langle x - 1\rangle?$$

Dividendo, otteniamo

$$x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$$

e di conseguenza $x^3 + 4x^2 + 3x - 7$ *non* appartiene all'ideale $\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1\rangle$.

Nel prossimo capitolo, risolveremo il problema di appartenenza all'ideale per polinomi in $\mathbb{K}[x_1, \ldots, x_n]$ utilizzando una strategia simile: troveremo una base particolare dell'ideale (detta base di Groebner) e quindi utilizzeremo un algoritmo della divisione generalizzato per determinare se il polinomio appartiene all'ideale o no.

Capitolo 2

Basi di Groebner

2.1 Introduzione

Nel Capitolo 1, abbiamo visto come l'algebra degli anelli di polinomi in $\mathbb{K}[x_1, \ldots, x_n]$ sia strettamente connessa con la geometria delle varietà affini. In questo capitolo, studieremo il metodo delle basi di Groebner, che ci permetterà di risolvere problemi riguardanti anelli di polinomi in maniera algoritmica o computazionale. Il metodo delle basi di Groebner è utilizzato anche in molti programmi informatici di algebra per studiare particolari ideali polinomiali che si incontrano nelle applicazioni. Ora approfondiremo i problemi che abbiamo posto nel capitolo precedente riguardanti l'algebra degli ideali di polinomi e la geometria delle varietà affini.

Problemi

(i) Descrizione dell'ideale: possiamo trovare un insieme finito di generatori per ogni ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$? In altre parole, possiamo scrivere $I = \langle f_1, \ldots, f_s \rangle$ per qualche $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$?

(ii) Appartenenza all'ideale: dati $f \in \mathbb{K}[x_1, \ldots, x_n]$ e un ideale I con $I = \langle f_1, \ldots, f_s \rangle$, vogliamo determinare se $f \in I$. Geometricamente, ciò è strettamente legato al problema di determinare se $\mathbf{V}(f_1, \ldots, f_s)$ giace sulla varietà $\mathbf{V}(f)$.

(iii) Risolvere equazioni polinomiali: vogliamo trovare tutte le soluzioni comuni di

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0.$$

Ovviamente, questo problema corrisponde alla ricerca i punti della varietà affine $\mathbf{V}(f_1, \ldots, f_s)$.

(iv) Forma Implicita: sia V un sottoinsieme di $\mathbb{K}^n$ dato tramite la seguente parametrizzazione:

$$\begin{cases} x_1 &= g_1(t_1, \ldots, t_m), \\ & \vdots \\ x_n &= g_n(t_1, \ldots, t_m) \end{cases}$$

Se le g_i sono polinomi (o funzioni razionali) nelle variabili t_j, allora V sarà una varietà affine o il sottoinsieme di una varietà affine. Vogliamo trovare un sistema di equazioni polinomiali (nelle x_i) che definiscano la varietà.

Alcuni commenti sono necessari. Il problema (i) chiede se ogni ideale di polinomi possa essere descritto tramite un numero finito di generatori. Molti degli ideali che abbiamo visto finora possono in effetti essere descritti nel modo richiesto: infatti, abbiamo scelto gli esempi in modo da trovare un insieme finito di generatori. Tuttavia, vi sono altri modi di costruire ideali, che non conducono direttamente a questo tipo di descrizione: l'esempio principale che abbiamo visto è l'ideale di una varietà, $\mathbf{I}(V)$. Sarà utile sapere che anche questi ideali sono finitamente generati. D'altra parte, si può osservare che permettendo un numero *infinito* di variabili per i polinomi, la risposta ad (i) è no.

Notiamo inoltre che i problemi (iii) e (iv) sono, per così dire, problemi tra loro inversi. In (iii), vogliamo conoscere l'insieme delle soluzioni di un dato sistema di equazioni polinomiali. In (iv), invece, ci vengono fornite le soluzioni, e il problema è trovare un sistema di equazioni che abbia tali soluzioni.

Per cominciare il nostro studio delle basi di Groebner, consideriamo alcuni casi speciali in cui si impiegano tecniche algoritmiche per risolvere i problemi introdotti sopra.

Esempio 1 : Per $n = 1$, abbiamo risolto il problema di descrizione dell'ideale nella Sezione 1.3. Infatti, dato un ideale $I \subset \mathbb{K}[x]$, abbiamo mostrato che $I = \langle g \rangle$ per qualche $g \in \mathbb{K}[x]$. Gli ideali possono quindi essere descritti in maniera particolarmente semplice in questo caso.

Abbiamo anche visto che la soluzione del problema di appartenenza all'ideale è una semplice conseguenza dell'algoritmo della divisione: dato $f \in \mathbb{K}[x]$, per verificare se $f \in I = \langle g \rangle$, dividiamo f per g:

$$f = q \cdot g + r,$$

dove $q, r \in \mathbb{K}[x]$ e $r = 0$ o $\deg(r) < \deg(g)$. Abbiamo anche dimostrato che $f \in I$ se e solo se $r = 0$. In questo modo, abbiamo un test algoritmico per l'appartenenza all'ideale nel caso $n = 1$.

Esempio 2 : Ora, sia n (il numero delle variabili) arbitrario, e consideriamo il problema della risoluzione di un sistema di equazioni polinomiali:

$$\left\{\begin{array}{rcl} a_{11}x_1 + \cdots + a_{1n}x_n & = & b_1, \\ & \vdots & \\ a_{m1}x_1 + \cdots + a_{mn}x_n & = & b_m, \end{array}\right. \tag{2.1}$$

dove ogni polinomio è lineare (grado complessivo 1).

Ad esempio, consideriamo il sistema

$$\left\{\begin{array}{rcl} 2x_1 + 3x_2 - x_3 & = & 0, \\ x_1 + x_2 - 1 & = & 0, \\ x_1 + x_3 - 3 & = & 0. \end{array}\right. \tag{2.2}$$

Riduciamo la matrice in forma triangolare superiore unipotente:

$$\begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

La forma di questa matrice mostra che x_3 è una variabile indipendente, e ponendo $x_3 = t$ abbiamo

$$\begin{array}{rcl} x_1 & = & -t + 3, \\ x_2 & = & t - 2, \\ x_3 & = & t. \end{array}$$

Queste sono le equazioni parametriche di una retta L in $\mathbb{K}^3$. Il sistema di equazioni originario (2.2) ci presenta sotto forma di varietà affine.

Nel caso generale, si cerca di ridurre la matrice di (2.1)

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & -b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & -b_m \end{pmatrix}$$

in *forma triangolare superiore ridotta*. Dopodichè possiamo trovare tutte le soluzioni del problema originario (2.2) sostituendo valori alle *variabili indipendenti* nel sistema di equazioni in forma triangolare. In generale potrebbe esserci una sola o addirittura nessuna soluzione. Quest'ultimo caso accadrebbe, ad esempio, se la matrice triangolare superiore contenesse una riga $(0 \cdots 0\, 1)$ corrispondente all'equazione inconsistente $0 = 1$

Esempio 3 : Di nuovo, sia n arbitrario, e consideriamo il sottoinsieme V dello spazio $\mathbb{K}^n$ parametrizzato da

$$\left\{\begin{array}{rcl} x_1 & = & a_{11}t_1 + \cdots + a_{1m}t_m + b_1, \\ & \vdots & \\ x_n & = & a_{n1}t_1 + \cdots + a_{nm}t_m + b_n. \end{array}\right. \tag{2.3}$$

Notiamo che V è un sottospazio lineare affine di $\mathbb{K}^n$ poiché è l'immagine della mappa $F : \mathbb{K}^m \to \mathbb{K}^n$ definita da

$$F(t_1, \ldots, t_m) = (a_{11}t_1 + \cdots + a_{1m}t_m + b_1, \ldots, a_{n1}t_1 + \cdots + a_{nm}t_m + b_n).$$

Questa è una mappa lineare, seguita da una traslazione. Supponiamo di voler trovare la forma implicita in questo caso: in altre parole, cerchiamo un sistema di equazioni lineari la cui soluzione siano i punti di V.

Ad esempio, consideriamo il sottospazio lineare affine $V \subset \mathbb{K}^4$ definito da

$$\begin{aligned} x_1 &= t_1 + t_2 + 1, \\ x_2 &= t_1 - t_2 + 3, \\ x_3 &= 2t_1 - 2, \\ x_4 &= t_1 + 2t_2 - 3. \end{aligned}$$

Riscriviamo le equazioni sottraendo i termini x_i da ambo i lati e applichiamo l'algoritmo di riduzione triangolare alla matrice corrispondente:

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{pmatrix}$$

dove i coefficienti delle x_i sono stati messi dopo i coefficienti delle t_j in ogni riga. Otteniamo la forma triangolare superiore unipotente

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{pmatrix}.$$

Poiché i valori nelle prime due colonne delle righe 3 e 4 sono zero, le ultime due righe di questa matrice corrispondono alle due seguenti equazioni senza termini t_j:

$$\begin{aligned} x_1 - (1/4)x_3 - (1/2)x_4 - 3 &= 0, \\ x_2 - (3/4)x_3 + (1/2)x_4 - 3 &= 0. \end{aligned}$$

(Notiamo che anche questo sistema è in forma triangolare superiore unipotente.) Queste due equazioni definiscono V in $\mathbb{K}^4$.

Lo stesso metodo può essere utilizzato per trovare equazioni implicite per qualsiasi sottospazio lineare affine V dato in forma parametrica come in (2.3): si calcola la forma triangolare superiore unipotente della matrice, e le righe che coinvolgono solo $x_1, \ldots, x_n$ danno le equazioni di V. Abbiamo quindi una soluzione algoritmica per il problema di forma implicita in questo caso.

Il nostro scopo in questo capitolo sarà lo sviluppo di estensioni dei metodi utilizzati in questi esempi per sistemi di equazioni polinomiali di qualsiasi grado in un numero qualsiasi di variabili. Ciò che vedremo è che una sorta di "combinazione" di riduzione in forma triangolare e divisione di polinomi (il metodo delle basi di Groebner menzionato all'inizio) ci permette di gestire tutti questi problemi.

2.2 Ordinamenti monomiali in $\mathbb{K}[x_1, \ldots, x_n]$

Se esaminiamo in dettaglio l'algoritmo della divisione in $\mathbb{K}[x]$ e l'algoritmo di riduzione triangolare (eliminazione di Gauss) per sistemi di equazioni lineari (o matrici), notiamo che la nozione di *ordinamento dei termini* nei polinomi è un elemento chiave di entrambi. Per l'algoritmo della divisione per polinomi di una variabile, infatti, lavoriamo con l'ordinamento secondo il grado per monomi in una variabile:

$$\cdots > x^{m+1} > x^m > \cdots > x > 1. \tag{2.4}$$

Il successo dell'algoritmo dipende dalla scelta sistematica dei termini direttivi di f e g, senza togliere termini "a caso" da f utilizzando termini arbitrari di g.

Similmente, nell'algoritmo di riduzione triangolare per le matrici, in ogni singola riga lavoriamo prima con i valori a sinistra. A livello di equazioni lineari, ciò è espresso tramite ordinamento delle variabili $x_1, \ldots, x_n$ come segue:

$$x_1 > x_2 > \cdots > x_n. \tag{2.5}$$

Scriviamo i termini nelle nostre equazioni in ordine decrescente. Inoltre, in un sistema in forma triangolare, le equazioni sono elencate con i rispettivi termini direttivi in ordine decrescente.

Dalle osservazioni precedenti, potremmo ipotizzare che un ordinamento dei termini dei polinomi di $\mathbb{K}[x_1, \ldots, x_n]$ sarà una componente fondamentale di qualsiasi estensione di divisioni e riduzioni matriciali ad arbitrari polinomi in più di una variabile. In questa sezione, discuteremo le proprietà che un tale ordinamento dovrebbe avere, e costruiremo diversi esempi che soddisfino le nostre richieste. Ciascuno di questi ordinamenti sarà utile in un differente contesto.

Per prima cosa, osserviamo che possiamo ricostruire il monomio $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ dalle n-uple di esponenti $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Questo fatto stabilisce una corrispondenza biunivoca tra i monomi di $\mathbb{K}[x_1, \ldots, x_n]$ e $\mathbb{Z}^n_{\geq 0}$. Inoltre, ogni relazione d'ordine $>$ che stabiliremo sullo spazio $\mathbb{Z}^n_{\geq 0}$ ci fornirà un ordinamento per i monomi: se $\alpha > \beta$ secondo questa relazione d'ordine, diremo anche che $x^\alpha > x^\beta$.

Ci sono molti modi differenti per definire relazioni d'ordine in $\mathbb{Z}^n_{\geq 0}$. Per i nostri scopi, tuttavia, gran parte di queste relazioni non sarà utile, poiché cercheremo ordinamenti "compatibili" con la struttura algebrica degli anelli di polinomi.

Per cominciare, poiché un polinomio è somma di monomi, vorremmo poter riordinare i termini in un polinomio in modo non ambiguo in ordine

discendente (o ascendente). Per fare ciò, dobbiamo essere in grado di confrontare ogni coppia di monomi per stabilire le rispettive posizioni corrette. Quindi, richiederemo che le nostre relazioni d'ordine siano *totali*, cioé che per ogni coppia di monomi x^α e x^β una e una sola tra

$$x^\alpha > x^\beta, \quad x^\alpha = x^\beta, \quad x^\alpha < x^\beta$$

sia vera.

Poi, dobbiamo prendere in considerazione l'effetto delle operazioni di somma e prodotto di polinomi. Quando sommiamo polinomi, dopo aver raccolto i termini simili, possiamo semplicemente riordinare i termini secondo l'ordine appropriato: la somma non comporta quindi difficoltà. Il prodotto, tuttavia, è più sottile. Poiché la moltiplicazione in un anello è distributiva rispetto all'addizione, basta analizzare ciò che accade quando moltiplichiamo un monomio per un polinomio. Se questa operazione alterasse l'ordine relativo dei termini, potrebbero sorgere problemi significativi in ogni processo simile all'algoritmo della divisione in $\mathbb{K}[x]$, in cui dovessimo identificare i termini "direttivi" dei polinomi. La ragione sta nel fatto che il termine direttivo del prodotto potrebbe essere diverso dal prodotto tra monomio e termine direttivo del polinomio originario.

Perciò, richiederemo che tutte le relazioni d'ordine tra termini abbiano anche la seguente proprietà: se $x^\alpha > x^\beta$ e x^γ è un monomio qualunque, deve valere $x^\alpha x^\gamma > x^\beta x^\gamma$. In termini dei vettori esponente, questa proprietà si traduce nell'imporre che se $\alpha > \beta$ nel nostro ordinamento di $\mathbb{Z}^n_{\geq 0}$, allora $\alpha + \gamma > \beta + \gamma$ per ogni $\gamma \in \mathbb{Z}^n_{\geq 0}$.

Tenendo presente queste osservazioni, enunciamo la seguente definizione.

Definizione 1. *Un* ***ordinamento monomiale*** *su* $\mathbb{K}[x_1, \ldots, x_n]$ *è una qualsiasi relazione* $>$ *su* $\mathbb{Z}^n_{\geq 0}$*, o equivalentemente, una qualsiasi relazione sull'insieme dei monomi* $x^\alpha, \alpha \in \mathbb{Z}^n_{\geq 0}$*, che soddisfi:*

(i) $>$ *è una relazione d'ordine totale su* $\mathbb{Z}^n_{\geq 0}$*.*

(ii) Se $\alpha > \beta$ *e* $\gamma \in \mathbb{Z}^n_{\geq 0}$*, allora* $\alpha + \gamma > \beta + \gamma$*.*

(iii) $>$ *è una buona relazione d'ordine su* $\mathbb{Z}^n_{\geq 0}$*, ovvero ogni sottoinsieme non vuoto di* $\mathbb{Z}^n_{\geq 0}$ *ha elemento minimo rispetto a* $>$*.*

Il seguente lemma ci aiuterà a capire il significato della richiesta di un buon ordinamento.

Lemma 2. *Una relazione d'ordine* $>$ *su* $\mathbb{Z}^n_{\geq 0}$ *è una buona relazione d'ordine se e solo se ogni sequenza strettamente decrescente in* $\mathbb{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

è finita.

Dimostrazione. Dimostreremo il lemma mostrando che $>$ non è una buona relazione d'ordine se e solo se esiste in $\mathbb{Z}^n_{\geq 0}$ una sequenza strettamente decrescente infinita.

Se $>$ non è un buona relazione d'ordine, allora esiste un sottoinsieme non vuoto $S \subset \mathbb{Z}^n_{\geq 0}$ senza elemento minimo. Sia $\alpha(1) \in S$; poiché $\alpha(1)$ non è l'elemento minimo, esiste $\alpha(2) < \alpha(1)$. Ma nemmeno $\alpha(2)$ è minimo, quindi esiste $\alpha(3) < \alpha(2)$. Continuando in questo modo, abbiamo costruito una sequenza strettamente decrescente infinita

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots .$$

Inversamente, data una tale sequenza infinita, allora $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ è un sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$ senza elemento minimo, e quindi $>$ non è una buona relazione d'ordine. □

L'importanza di questo lemma sarà evidente nelle sezioni a seguire: sarà infatti utilizzato per mostrare che diversi algoritmi devono terminare perché alcuni termini sono strettamente decrescenti (rispetto ad un fissato ordinamento monomiale) ad ogni passo dell'algoritmo.

Nella Sezione 2.4 vedremo che date (i) e (ii) come nella Definizione 1, la condizione di buona relazione d'ordine nella parte (iii) è equivalente a $\alpha \geq 0$ per ogni $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Esempio 1 : Per un semplice esempio di ordinamento monomiale, osserviamo che l'ordinamento numerico usuale

$$\cdots > m+1 > m > \cdots > 3 > 2 > 1 > 0$$

sugli elementi di $\mathbb{Z}^n_{\geq 0}$ soddisfa le tre condizioni della Definizione 1. Quindi, l'ordinamento secondo il grado (2.4) sui monomi di $\mathbb{K}[x]$ è un ordinamento monomiale.

Il nostro primo esempio di ordinamento su n-uple sarà l'ordine lessicografico, in breve **lex**.

Definizione 3. *(Ordine Lessicografico) Presi due vettori $\alpha = (\alpha_1, \ldots, \alpha_n)$, e $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, diremo che $\alpha >_{\text{lex}} \beta$ se, nel vettore differenza $\alpha - \beta \in \mathbb{Z}^n$, il primo valore non nullo da sinistra è positivo, e indicheremo $x^\alpha >_{\text{lex}} x^\beta$ se $\alpha >_{\text{lex}} \beta$.*

Esempio 2 : Presentiamo alcuni esempi:

a. $(1,2,0) >_{\text{lex}} (0,3,4)$ poiché $\alpha - \beta = (1,-1,-4)$.

b. $(3,2,4) >_{\text{lex}} (3,2,1)$ poiché $\alpha - \beta = (0,0,3)$.

c. Le variabili $x_1, \ldots, x_n$ vengono ordinate nella maniera usuale (vedere (2.5)) dall'ordinamento lex:

$$(1, 0, \ldots, 0) >_{\text{lex}} (0, 1, 0, \ldots, 0) >_{\text{lex}} \cdots >_{\text{lex}} (0, \ldots, 0, 1),$$

quindi $x_1 >_{\text{lex}} x_2 >_{\text{lex}} \cdots >_{\text{lex}} x_n$.

In pratica, quando lavoriamo con polinomi in due o tre variabili, chiameremo le variabili x, y, z piuttosto che x_1, x_2, x_3. Supporremo inoltre che l'ordine alfabetico $x > y > z$ sulle variabili sia utilizzato per definire l'ordine lessicografico a meno che non sia esplicitamente indicato altrimenti.

L'ordine lex è analogo all'ordine delle parole utilizzato nei dizionari (da cui il nome). Possiamo vedere i valori di una n-upla $\alpha \in \mathbb{Z}^n_{\geq 0}$ analogamente alle lettere di una parola. Le lettere sono in ordine alfabetico:

$$a > b > \cdots > y > z.$$

Quindi, ad esempio,

$$\text{farro} >_{\text{lex}} \text{farsa}$$

poiché la quarta lettera di "farro" viene prima della quarta lettera di "farsa" in ordine alfabetico, sebbene le prime tre lettere siano le stesse in ambedue. Poiché tutti gli elementi $\alpha \in \mathbb{Z}^n_{\geq 0}$ hanno lunghezza n, questa analogia si applica solo a parole con un numero fissato di lettere.

Per completezza, dobbiamo verificare che l'ordine lessicografico soddisfi le tre condizioni della Definizione 1.

Proposizione 4. *L'ordinamento lex su $\mathbb{Z}^n_{\geq 0}$ è un ordinamento monomiale.*

Dimostrazione. (i) Il fatto che $>_{\text{lex}}$ sia un ordinamento totale segue direttamente dalla definizione e dal fatto che l'ordine numerico usuale su $\mathbb{Z}_{\geq 0}$ sia un ordinamento totale.

(ii) Se $\alpha >_{\text{lex}} \beta$, allora il primo valore non nullo da sinistra in $\alpha - \beta$, poniamo $\alpha_k - \beta_k$, è positivo. Ma $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ e $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Allora, il primo valore non nullo da sinistra in $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$ è ancora $\alpha_k - \beta_k > 0$.

(iii) Supponiamo che $>_{\text{lex}}$ non sia un buon ordinamento. Allora, per il Lemma 2, esisterebbe una sequenza infinita strettamente decrescente

$$\alpha(1) >_{\text{lex}} \alpha(2) >_{\text{lex}} \alpha(3) >_{\text{lex}} \cdots$$

di elementi di $\mathbb{Z}^n_{\geq 0}$. Vogliamo mostrare che questo porta ad una contraddizione.

Consideriamo i primi valori dei vettori $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$. Per la definizione dell'ordine lex, questi primi valori formano una sequenza non crescente di interi non negativi. Poiché $\mathbb{Z}_{\geq 0}$ è ben ordinato, i primi valori degli $\alpha(i)$ devono definitivamente "stabilizzarsi". Ovvero, esiste un k tale che tutte le componenti degli $\alpha(i)$ con $i \geq k$ siano uguali.

Cominciando da $\alpha(k)$, i secondi valori e seguenti entrano in gioco per determinare l'ordine lex. I secondi valori di $\alpha(k), \alpha(k+1), \ldots$ formano una sequenza non crescente e, per lo stesso ragionamento di prima, si devono anch'essi "stabilizzare" definitivamente. Continuando nello stesso modo, osserviamo che, per qualche l, gli $\alpha(l), \alpha(l+1), \ldots$ sono tutti uguali, il che contraddice $\alpha(l) > \alpha(l+1)$. □

É importante rendersi conto che esistono diversi ordini lex, corrispondenti al modo in cui vengono ordinate le variabili. Finora abbiamo utilizzato l'ordine lex con $x_1 > x_2 > \cdots, x_n$, ma dato un *qualsiasi* ordine per le variabili $x_1, \ldots, x_n$ esiste un ordine lex corrispondente. Per esempio, se le variabili sono x e y, possiamo costruire un ordine lex con $x > y$ ed un altro con $y > x$. Nel caso generale di n variabili, esistono $n!$ ordini lex; nel seguito, l'espressione "ordine lex" si riferirà a quello in cui $x_1 > \cdots > x_n$ a meno che non venga specificato altrimenti.

Nell'ordine lex, notiamo che una variabile domina *qualsiasi* monomio composto esclusivamente da variabili minori, indipendentemente dal proprio grado totale. Quindi, per l'ordine lex in cui $x > y > z$, abbiamo $x > y^3 z^5$. Per diversi scopi, potremmo avere necessità di considerare il grado complessivo dei monomi e considerare maggiori quelli di grado più alto: un modo per fare ciò è l'ordine lessicografico per gradi, detto ordine **grlex**[1].

Definizione 5. *(Ordine Lessicografico per Gradi) Siano $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Diremo che $\alpha >_{\text{grlex}} \beta$ se*

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

Notiamo che grlex ordina prima secondo il grado complessivo, dopodichè "risolve i pareggi" utilizzando l'ordine lex.

Esempio 3 :

a. $(1,2,3) >_{\text{grlex}} (3,2,0)$ poiché $|(1,2,3)| = 6 > |(3,2,0)| = 5$.

b. $(1,2,4) >_{\text{grlex}} (1,1,5)$ poiché $|(1,2,4)| = |(1,1,5)|$ e $(1,2,4) >_{\text{lex}} (1,1,5)$.

c. Le variabili vengono ordinate secondo l'ordine lex, cioè $x_1 >_{\text{grlex}} \cdots >_{\text{grlex}} x_n$.

[1]Dall'inglese *Graded Lexicographic Order*.

La dimostrazione che l'ordinamento grlex soddisfa le tre condizioni della Definizione 1 è molto simile a quella già esposta per l'ordinamento lex, e sarà quindi omessa. Come nel caso dell'ordine lex, esistono $n!$ ordini grlex su n variabili, a seconda del modo in cui esse sono ordinate.

Un altro ordine, meno intuitivo, sui monomi è l'ordine lessicografico per gradi inverso, o **grevlex**[2]. Anche se questo ordinamento non è dei più intuitivi, è stato recentemente mostrato che, per alcune operazioni, è il più efficiente dal punto di vista del calcolo.

Definizione 6. *(Ordine Lessicografico per Gradi Inverso) Siano* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *Diremo che* $\alpha >_{\text{grevlex}} \beta$ *se*

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

e, in $\alpha - \beta \in \mathbb{Z}^n$, *il primo valore non nullo da destra è negativo.*

Come grlex, grevlex ordina secondo il grado complessivo, ma "risolve i pareggi" in maniera differente.

Esempio 4 :

a. $(4,7,1) >_{\text{grevlex}} (4,2,3)$ poiché $|(4,7,1)| = 12 > |(4,2,3)| = 9$.

b. $(1,5,2) >_{\text{grevlex}} (4,1,3)$ poiché $|(1,5,2)| = |(4,1,3)|$ e $\alpha - \beta = (-3,4,-1)$.

c. Osserviamo che grevlex e lex inducono lo stesso ordinamento sulle variabili, infatti

$$(1,0,\ldots,0) >_{\text{grevlex}} (0,1,0,\ldots,0) >_{\text{grevlex}} \cdots >_{\text{grevlex}} (0,\ldots,0,1),$$

ovvero

$$x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \cdots >_{\text{grevlex}} x_n.$$

Quindi, grevlex è in realtà differente dall'ordine grlex con le variabili permutate (al contrario di quanto saremmo portati a pensare dal nome).

Per spiegare la relazione tra grlex e grevlex, notiamo che entrambi utilizzano il grado complessivo nello stesso modo. Per "risolvere un pareggio", grlex utilizza l'ordine lex, cioè controlla la variabile più a sinistra (la maggiore) e favorisce la potenza maggiore. Per contro, quando grevlex incontra due monomi con lo stesso grado totale, controlla la variabile più a destra (la minore) e favorisce la potenza *minore*, portando ad una "doppia inversione" dell'ordine lex. Ad esempio,

$$x^5yz >_{\text{grlex}} x^4yz^2,$$

[2]Dall'inglese *Graded Reverse Lexicographic Order*.

poiché entrambi i monomi hanno grado totale 7 e $x^5yz >_{\text{lex}} x^4yz^2$. In questo caso, abbiamo anche

$$x^5yz >_{\text{grevlex}} x^4yz^2,$$

ma per un motivo differente: x^5yz è maggiore perché la variabile minore z compare con una potenza minore.

Come per lex e grlex, esistono $n!$ ordinamenti corrispondenti al modo in cui vengono ordinate le n variabili.

Esistono molti altri ordinamenti monomiali oltre a quelli trattati qui; gran parte dei sistemi algebrici per computer implementano l'ordine lex, ed alcuni (come Macaulay e REDUCE) permettono anche altri ordini, come grlex e grevlex. Una volta che un tale ordine è stato scelto, questi sistemi permettono all'utente di specificare uno qualsiasi degli $n!$ ordinamenti delle variabili, la qual cosa è molto utile nelle applicazioni.

Termineremo questa sezione con una discussione su come un ordinamento monomiale possa essere applicato ai polinomi. Se $f = \sum_\alpha a_\alpha x^\alpha$ è un polinomio in $\mathbb{K}[x_1, \ldots, x_n]$ e abbiamo scelto un ordinamento monomiale $>$, possiamo ordinare i monomi di f in maniera univoca rispetto a $>$.

Esempio 5 : Sia $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{K}[x, y, z]$. Allora:

a. Rispetto all'ordine lex, riordineremo i termini di f in ordine decrescente come

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

b. Rispetto all'ordine grlex, avremo

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z.$$

c. Rispetto all'ordine grevlex, avremo

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z.$$

Utilizzeremo la seguente notazione.

Definizione 7. *Sia $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio non nullo in $\mathbb{K}[x_1, \ldots, x_n]$ e sia $>$ un ordinamento monomiale.*

(i) Il ***multigrado*** *di f è*

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} \,:\, a_\alpha \neq 0)$$

(il massimo è valutato rispetto a $>$).

(ii) Il ***coefficiente direttivo*** *di f è*

$$\text{LC}(f) = a_{\text{multideg}(f)} \in \mathbb{K}.$$

(iii) Il ***monomio direttivo*** *di* f *è*

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

(con coefficiente 1*).*

(iv) Il ***termine direttivo*** *di* f *è*

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

Esempio 6 : Sia $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ come prima e denotiamo con $>$ l'ordine lex. Allora

$$\begin{aligned} \text{multideg}(f) &= (3,0,0), \\ \text{LC}(f) &= -5, \\ \text{LM}(f) &= x^3, \\ \text{LT}(f) &= -5x^3. \end{aligned}$$

Enunciamo, senza dimostrarle, le seguenti proprietà.

Lemma 8. *Siano* $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ *polinomi non nulli. Allora:*

(i) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.

(ii) Se $f + g \neq 0$*, allora* $\text{multideg}(f+g) \leq \max(\text{multideg}(f), \text{multideg}(g))$.

Se inoltre $\text{multideg}(f) \neq \text{multideg}(g)$*, vale l'uguaglianza.*

D'ora in poi, daremo per scontato che sia stato scelto un particolare ordine monomiale, e che i termini direttivi, ecc., saranno calcolati esclusivamente in relazione a quest'ordine.

2.3 Un algoritmo della divisione in $\mathbb{K}[x_1, \ldots, x_n]$

Nella Sezione 2.1, abbiamo visto come l'algoritmo della divisione possa essere utilizzato per risolvere il problema di appartenenza all'ideale per polinomi di una variabile. Per studiare questo problema in presenza di più variabili, formuleremo un algoritmo della divisione per polinomi in $\mathbb{K}[x_1, \ldots, x_n]$ che estende l'algoritmo per $\mathbb{K}[x]$. Nel caso generale, l'obiettivo è dividere $f \in$

$\mathbb{K}[x_1, \ldots, x_n]$ per $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. Come vedremo, questo significa esprimere f nella forma

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r,$$

dove i "quozienti" $a_1, \ldots, a_s$ ed il resto r giacciono in $\mathbb{K}[x_1, \ldots, x_n]$. Sarà necessario prestare attenzione nel decidere come caratterizzare il resto, ed è a questo punto che entreranno in gioco gli ordinamenti monomiali introdotti nella Sezione 2.2. Allora vedremo come l'algoritmo della divisione si applica al problema di appartenenza all'ideale.

L'idea che sta alla base dell'algoritmo è la stessa del caso ad una variabile: vogliamo elidere il termine direttivo di f (rispetto ad un ordine monomiale fissato) moltiplicando qualche f_i per un appropriato monomio e sottraendo: allora, questo monomio diventa un termine nel corrispondente a_i. Piuttosto che enunciare l'algoritmo in generale, incominciamo prima a lavorare su qualche esempio per vedere cosa ci sia in gioco.

Esempio 1 : Incominceremo col dividere $f = xy^2 + 1$ per $f_1 = xy + 1$ e $f_2 = y + 1$, utilizzando l'ordine lex con $x > y$. Vogliamo utilizzare la stessa traccia vista per la divisione di polinomi di una variabile, con la differenza che ora ci sono diversi divisori e quozienti. Elencando i divisori f_1, f_2 ed i quozienti a_1, a_2 *in verticale*, abbiamo la seguente disposizione:

$$\begin{array}{rl} a_1 & : \\ a_2 & : \end{array}$$

$$\begin{array}{r|l} xy+1 & xy^2+1 \\ y+1 & \\ \end{array}$$

Entrambi i termini direttivi $\text{LT}(f_1) = xy$ e $\text{LT}(f_2) = y$ dividono il termine direttivo $\text{LT}(f) = xy^2$. Useremo f_1 poiché è elencato per primo: dividiamo xy^2 per xy ottenendo y, dopodichè sottraiamo $y \cdot f_1$ a f:

$$\begin{array}{rl} a_1 & : \; y \\ a_2 & : \end{array}$$

$$\begin{array}{r|l} xy+1 & xy^2 \;\; +1 \\ y+1 & xy^2 \;\; +y \\ & \hline \\ & \quad -y+1 \end{array}$$

Ripetiamo ora lo stesso procedimento su $-y + 1$. Questa volta dobbiamo utilizzare f_2 poiché $\text{LT}(f_1) = xy$ non divide $\text{LT}(-y + 1) = -y$. Otteniamo

$$\begin{array}{rl} a_1 & : \; y \\ a_2 & : \; -1 \end{array}$$

$$\begin{array}{r|l} xy+1 & xy^2 \;\; +1 \\ y+1 & xy^2 \;\; +y \\ & \hline \\ & \quad -y \;\; +1 \\ & \quad -y \;\; -1 \\ & \hline \\ & \qquad\quad 2 \end{array}$$

Poiché $\text{LT}(f)$ e $\text{LT}(f_2)$ non dividono 2, il resto è $r = 2$ ed il procedimento è finito. Quindi, abbiamo scritto $f = xy^2$ nella forma

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

Esempio 2 : Incontreremo ora una sottigliezza inaspettata che può accadere trattando polinomi di più variabili. Dividiamo $f = x^2y + xy^2 + y^2$ per $f_1 = xy$ e $f_2 = y^2 - 1$. Come nel precedente esempio, utilizzeremo l'ordine lex con $x > y$. I primi due passaggi dell'algoritmo si svolgono come al solito, fornendoci la divisione parzialmente completa (ricordiamo che nel caso in cui tutti e due i termini dividano f, utilizziamo f_1):

$$\begin{array}{rl} a_1 & : \; x + y \\ a_2 & : \end{array}$$

$$\begin{array}{r|l} xy - 1 & x^2y \;\; +xy^2 \;\; +y^2 \\ y^2 - 1 & x^2y \;\; -x \\ \hline & \quad xy^2 \;\; +x + y^2 \\ & \quad xy^2 \;\; -y \\ \hline & \quad x + y^2 + y \end{array}$$

Notiamo che né $\text{LT}(f_1)$ né $\text{LT}(f_2)$ dividono $\text{LT}(x + y^2 + y) = x$. Tuttavia, $x + y^2 + y$ *non* è il resto dal momento che $\text{LT}(f_2)$ divide y^2. Quindi, se portiamo x al resto, possiamo continuare a dividere. (Questo non accade mai nel caso ad una variabile: una volta che il termine direttivo del divisore non divide più il termine direttivo di ciò che resta da dividere, l'algoritmo termina.)

Per rendere questa idea, creiamo una colonna dei resti r a destra della tabella, dove metteremo i termini appartenenti al resto. Inoltre, durante le fasi intermedie, chiameremo *dividendo intermedio* il polinomio da dividere. Ecco il passo successivo, dove portiamo x alla colonna del resto (come indicato dalla freccia):

$$\begin{array}{rl} a_1 & : \; x + y \\ a_2 & : \quad 1 \end{array}$$

$$\begin{array}{r|l|c|l} & & & r \\ xy - 1 & x^2y \;\; +xy^2 \;\; +y^2 & & \\ y^2 - 1 & x^2y \;\; -x & & \\ \hline & \quad xy^2 \;\; +x \;\; +y^2 & & \\ & \quad xy^2 \;\; -y & & \\ \hline & \quad x \;\; +y^2 \;\; +y & & \\ \hline & \quad y^2 \;\; +y & \longrightarrow & x \end{array}$$

Ora continuiamo a dividere. Se possiamo dividere per $\text{LT}(f_1)$ o $\text{LT}(f_2)$ procediamo come al solito, altrimenti spostiamo il termine direttivo del dividendo intermedio alla colonna

del resto. Ecco l'ultima parte della divisione:

$$
\begin{array}{rcl}
a_1 & : & x+y \\
a_2 & : & 1
\end{array}
$$

$$
\begin{array}{r|l|l}
 & & r \\
xy-1 & x^2y \quad +xy^2 \quad +y^2 & \\
y^2-1 & x^2y \quad -x & \\
\hline
 & \quad xy^2 \quad +x \quad +y^2 & \\
 & \quad xy^2 \quad -y & \\
\hline
 & \qquad x \quad +y^2 \quad +y & \\
\hline
 & \qquad\quad y^2 \quad +y & \longrightarrow \quad x \\
 & \qquad\quad y^2 \quad -1 & \\
\hline
 & \qquad\qquad y \quad +1 & \\
\hline
 & \qquad\qquad\quad 1 & \longrightarrow \quad x+y \\
\hline
 & \qquad\qquad\quad 0 & \longrightarrow \quad x+y+1
\end{array}
$$

Quindi, il resto è $x + y + 1$, e otteniamo

$$x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1. \tag{2.6}$$

Osserviamo che il resto è una somma di monomi, nessuno dei quali è divisibile per i termini direttivi di f_1 o f_2.

L'esempio precedente illustra con sufficiente completezza il modo in cui l'algoritmo della divisione agisce. Mostra inoltre quale proprietà deve avere il resto: nessuno dei suoi termini deve essere divisibile per i termini direttivi dei polinomi per cui stiamo dividendo. Possiamo ora enunciare la forma generale dell'algoritmo della divisione.

Teorema 1. *(Algoritmo della Divisione in $\mathbb{K}[x_1, \ldots, x_n]$) Sia $>$ un ordine monomiale su $\mathbb{Z}^n_{\geq 0}$ fissato, e sia $F = (f_1, \ldots, f_s)$ una s-upla ordinata di polinomi in $\mathbb{K}[x_1, \ldots, x_n]$. Allora ogni $f \in \mathbb{K}[x_1, \ldots, x_n]$ può essere scritto come*

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

*dove $a_i, r \in \mathbb{K}[x_1, \ldots, x_n]$, e $r = 0$ oppure r è una combinazione $\mathbb{K}$-lineare di monomi, nessuno dei quali è divisibile per i $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Diremo che r è un **resto** di f diviso F. Inoltre, se $a_i f_i \neq 0$, vale*

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i f_i).$$

Dimostrazione. Dimostreremo l'esistenza di $a_1, \ldots, a_s$ e r fornendo un algoritmo per la loro costruzione e mostrando che esso opera correttamente per ogni dato in ingresso. Ricordiamo che tale algoritmo è una generalizzazione di quanto visto nella Proposizione 2 nella Sezione 1.3.

`Input:` $f_1, \ldots, f_s$

```
Output:  a_1, ..., a_s, r

a_1 := 0; ... a_s := 0; r := 0
p := f
WHILE p ≠ 0 DO
     i := 1
     divisione := falso
     WHILE i ≤ s AND divisione = falso DO
          IF LT(f_i) divide LT(p) THEN
               a_i := a_i + LT(p)/ LT(f_i)
               p := p − (LT(p)/ LT(f_i))f_i
               divisione := vero
          ELSE                    i = i + 1
     IF divisione = falso THEN
          r := r + LT(p)
          p = p − LT(p)
```

Possiamo confrontare questo algoritmo con l'esempio precedente osservando che la variabile p rappresenta il dividendo intermedio ad ogni passaggio, la variabile r rappresenta la colonna sulla destra, e le variabili $a_1, \ldots, a_s$ sono i quozienti elencati sopra la divisione. Infine, la variabile booleana `divisione` ci dice quando qualcuno dei $\text{LT}(f_i)$ divide il termine direttivo del dividendo intermedio. Ogni volta che il ciclo `WHILE...DO` principale viene eseguito, accade una ed una sola tra queste due possibilità:

- (Passo di Divisione) Se qualcuno dei $\text{LT}(f_i)$ divide $\text{LT}(p)$, allora l'algoritmo procede come nel caso ad una variabile.
- (Passo di Resto) Se nessuno dei $\text{LT}(f_i)$ divide $\text{LT}(p)$, allora l'algoritmo aggiunge $\text{LT}(p)$ al resto.

Questi passaggi corrispondono esattamente a ciò che abbiamo fatto nell'esempio.

Per dimostrare che l'algoritmo è corretto, mostreremo prima di tutto che

$$f = a_1 f_1 + \cdots + a_s f_s + p + r \tag{2.7}$$

è vera ad ogni passaggio. Ciò è evidente per i valori iniziali di $a_1, \ldots, a_s, p, r$. Ora supponiamo che (2.7) sia vera ad un generico passaggio dell'algoritmo: se il passaggio successivo è un Passo di Divisione, allora qualcuno dei $\text{LT}(f_i)$ divide $\text{LT}(p)$, e l'uguaglianza

$$a_i f_i = (a_i + \text{LT}(p)/\,\text{LT}(f_i))f_i + (p - (\text{LT}(p)/\,\text{LT}(f_i))f_i)$$

mostra che $a_i f_i + p$ non è cambiato. Poiché nessuna delle altre variabili viene modificata, (2.7) rimane vera in questo caso. Se invece il passo successivo è un Passo di Resto, allora p e r vengono modificati, ma la somma $p+r$ rimane uguale, infatti

$$p + r = (p - \text{LT}(p)) + (r + \text{LT}(p)).$$

Come prima, l'uguaglianza (2.7) è preservata.

Poi, notiamo che l'algoritmo termina quando $p = 0$, ed in questa situazione (2.7) diventa

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

Poiché vengono aggiunti termini a r solo quando non sono divisibili per nessuno dei $\text{LT}(f_i)$, ne consegue che $a_1, \ldots, a_s$ e r hanno le proprietà richieste nel momento in cui l'algoritmo termina.

Infine, dobbiamo mostrare che l'algoritmo termina. L'osservazione fondamentale è che ogni volta che ridefiniamo la variabile p, il suo multigrado diminuisce o si annulla. Per vedere questo, supponiamo che durante un Passo di Divisione p sia ridefinito secondo

$$p' = p - \frac{\text{LT}(p)}{\text{LT}(f_i)} f_i.$$

Per il Lemma 8 abbiamo

$$\text{LT}\left(\frac{\text{LT}(p)}{\text{LT}(f_i)} f_i\right) = \frac{\text{LT}(p)}{\text{LT}(f_i)} \text{LT}(f_i) = \text{LT}(p),$$

e quindi p e $(\text{LT}(p)/\text{LT}(f_i))f_i$ hanno lo stesso termine direttivo. Allora, la loro differenza p', se non nulla, deve avere multigrado strettamente minore. Ora, supponiamo che durante un Passo di Resto p sia ridefinito secondo

$$p' = p - \text{LT}(p).$$

In questo caso, è ovvio che $\text{multideg}(p') < \text{multideg}(p)$ per $p' \neq 0$. Quindi, in ogni caso, il multigrado deve diminuire. Se l'algoritmo non terminasse, otterremmo una sequenza infinita di multigradi, la qual cosa è in contrasto con la proprietà di buon ordinamento di $>$, come enunciato nel Lemma 8. Quindi deve essere definitivamente $p = 0$, e l'algoritmo termina in un numero finito di passi.

Resta da studiare la relazione tra $\text{multideg}(f)$ e $\text{multideg}(a_i f_i)$. Ogni termine nelle a_i è nella forma $\text{LT}(p)/\text{LT}(f_i)$ per certi valori della variabile p. L'algoritmo comincia con $p = f$, ed abbiamo appena finito di dimostrare che il multigrado di p decresce. Questo mostra che $\text{LT}(p) \leq \text{LT}(f)$, ed utilizzando la definizione di ordinamento monomiale troviamo facilmente che $\text{multideg}(a_i f_i) \leq \text{multideg}(f)$ per $a_i f_i \neq 0$, e con questo la dimostrazione è completa. □

L'algebra che sta dietro l'algoritmo della divisione è molto semplice, il che sorprende dal momento che questa forma dell'algoritmo è stata isolata e sfruttata per la prima volta negli ultimi 30 anni.

Concludiamo questa sezione chiedendoci se l'algoritmo della divisione abbia le stesse proprietà del caso ad una variabile. Sfortunatamente, la risposta non è delle migliori: i prossimi esempi mostreranno che l'algoritmo è lontano dalla perfezione. Infatti, si possono sfruttare appieno le sue potenzialità solo accoppiandolo con le basi di Groebner, che studieremo nelle Sezioni 2.5 e 2.6.

Una prima, importante proprietà dell'algoritmo della divisione in $\mathbb{K}[x]$ è che il resto è univocamente determinato. Per vedere come questo possa non accadere in presenza di più variabili, consideriamo il seguente esempio.

Esempio 3 : Dividiamo $f = x^2y + xy^2 + y^2$ per $f_1 = y^2 - 1$ e $f_2 = xy - 1$. Utilizzeremo l'ordine lex con $x > y$, come nell'esempio precedente, salvo per il fatto che abbiamo cambiato l'ordine dei divisori. Facendo la divisione,

$$
\begin{array}{rcl}
a_1 & : & x+y \\
a_2 & : & 1
\end{array}
$$

$$
\begin{array}{r|l|c|l}
 & & & r \\
y^2-1 & x^2y \;+xy^2\; +y^2 & & \\
xy-1 & x^2y \;\;\; -x & & \\
\cline{2-2}
 & \;\;\; xy^2 \;\; +x \;\; +y^2 & & \\
 & \;\;\; xy^2 \;\; -x & & \\
\cline{2-2}
 & \;\;\;\;\;\; 2x \;\; +y^2 & & \\
\cline{2-2}
 & \;\;\;\;\;\;\;\;\; y^2 & \longrightarrow & 2x \\
 & \;\;\;\;\;\;\;\;\; y^2 \;\; -1 & & \\
\cline{2-2}
 & \;\;\;\;\;\;\;\;\;\;\;\; y \;\; +1 & & \\
\cline{2-2}
 & \;\;\;\;\;\;\;\;\;\;\;\;\;\; 1 & & \\
\cline{2-2}
 & \;\;\;\;\;\;\;\;\;\;\;\;\;\; 0 & \longrightarrow & 2x+1
\end{array}
$$

Questo mostra che

$$x^2y + xy^2 + y^2 = (x+1)\cdot(y^2-1) + x\cdot(xy-1) + 2x + 1. \tag{2.8}$$

Confrontando con l'equazione (2.6), notiamo che il resto è differente da quanto avevamo ottenuto in precedenza.

Siamo giunti alla conclusione che il resto r non è univocamente determinato dalla condizione che nessuno dei suoi termini sia divisibile per i termini $\text{LT}(f_1), \ldots, \text{LT}(f_s)$. La situazione non è completamente caotica: se seguiamo l'algoritmo esattamente nel modo in cui è stato enunciato, soprattutto verificando la divisibilità di $\text{LT}(p)$ per $\text{LT}(f_1), \text{LT}(f_2), \ldots$ in quest'ordine, allora $a_1, \ldots, a_s, r$ sono univocamente determinati. Tuttavia, abbiamo appena mostrato come l'*ordinamento* delle s-uple di polinomi $(f_1, \ldots, f_s)$ sia fondamentale sia per il numero di passi che l'algoritmo impiega, sia nel risultato.

Gli a_i e r possono cambiare semplicemente riordinando gli f_i (gli a_i e r possono cambiare anche al variare dell'ordinamento monomiale, ma questo è un altro tipo di problema).

Una buona caratteristica dell'algoritmo della divisione in $\mathbb{K}[x]$ è il modo in cui risolve il problema di appartenenza all'ideale (Vedere gli esempi della Sezione 2.1). Otteniamo qualcosa di simile per più variabili? Una implicazione segue facilmente dal Teorema 1: se dopo aver diviso f per $F = (f_1, \ldots, f_s)$ otteniamo resto nullo, allora

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

e di conseguenza $f \in \langle f_1, \ldots, f_s \rangle$. Quindi $r = 0$ è una condizione *sufficiente* per l'appartenenza all'ideale. Tuttavia, come vedremo nel prossimo esempio, tale condizione non è *necessaria*.

Esempio 4 : Sia $f_1 = xy + 1, f_2 = y^2 - 1 \in \mathbb{K}[x, y]$ con l'ordine lex. Dividendo $f = xy^2 - x$ per $F = (f_1, f_2)$ il risultato è

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

Ponendo tuttavia $F = (f_2, f_1)$, otteniamo

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

Il secondo procedimento implica $f \in \langle f_1, f_2 \rangle$, e di conseguenza dal primo procedimento deduciamo che, nonostante ciò, possiamo ottenere resto non nullo dividendo per $F = (f_1, f_2)$.

Dobbiamo concludere che l'algoritmo della divisione enunciato nel Teorema 1 è una generalizzazione imperfetta della sua controparte in una variabile. Per rimediare a questa situazione, ritorniamo su un argomento visto nel Capitolo 1. Infatti, avendo a che fare con un insieme di polinomi $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, è spesso comodo passare all'ideale generato I. Questo permette di trovare un insieme finito di generatori diverso da $f_1, \ldots, f_s$, e possiamo dunque chiederci se esista un "buon" insieme di generatori per I. Per tale insieme, vogliamo che il resto r della divisione per i "buoni" generatori sia univocamente determinato e che la condizione $r = 0$ sia *equivalente* all'appartenenza all'ideale. Nella Sezione 2.6, vedremo che le basi di Groebner hanno esattamente queste "buone" proprietà.

2.4 Ideali monomiali e lemma di Dickson

In questa sezione, considereremo il problema di descrizione dell'ideale della Sezione 2.1 nel caso speciale di ideali monomiali. Questo richiederà uno

studio attento delle proprietà di questi ideali e i nostri risultati avranno anche inaspettate applicazioni per gli ordinamenti monomiali.

Per cominciare, definiamo gli ideali monomiali in $\mathbb{K}[x_1, \ldots, x_n]$.

Definizione 1. *Un ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ è un **ideale monomiale** se esiste un sottoinsieme $A \subset \mathbb{Z}^n_{\geq 0}$ (eventualmente infinito) tale che I sia formato da tutti i polinomi che sono somme finite nella forma $\sum_{\alpha \in A} h_\alpha x^\alpha$. dove $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. In questo caso, scriviamo $I = \langle x^\alpha : \alpha \in A \rangle$.*

Un esempio di ideale monomiale è dato da $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subset \mathbb{K}[x, y]$. Esempi più interessanti verranno forniti nella Sezione 2.5.

Prima di tutto dobbiamo caratterizzare *tutti* i monomi che appartengono ad un dato ideale monomiale.

Lemma 2. *Sia $I = \langle x^\alpha : \alpha \in A \rangle$ un ideale monomiale. Allora un monomio x^β appartiene a I se e solo se x^β è divisibile per x^α per qualche $\alpha \in A$.*

Dimostrazione. Se x^β è un multiplo di x^α per qualche $\alpha \in A$, allora $x^\beta \in I$ per definizione di ideale. Inversamente, se $x^\beta \in I$, allora $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, dove $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ e $\alpha(i) \in A$. Se riscriviamo ogni h_i come combinazione lineare di monomi, notiamo che ogni termine al secondo membro dell'equazione è divisibile per $x^{\alpha(\tilde{i})}$, dove $\alpha(\tilde{i})$ il minimo degli $\alpha(i)$ (che esiste in quanto essi sono un numero finito) e, quindi, il primo membro deve anch'esso avere tale proprietà. □

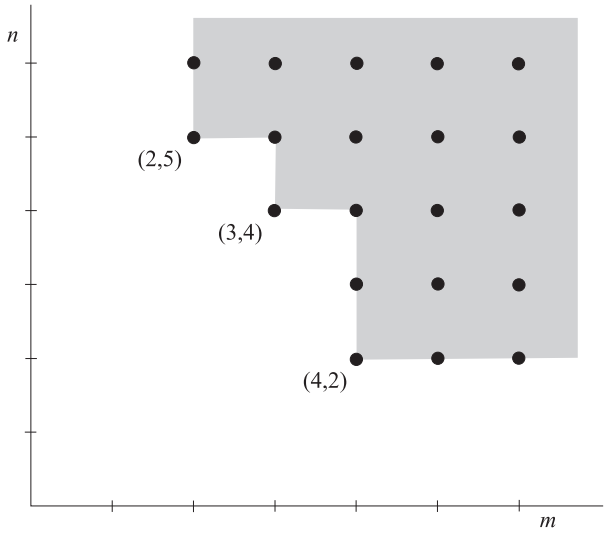
Notiamo che x^β è divisibile per x^α esattamente quando $x^\beta = x^\alpha \cdot x^\gamma$ per qualche $\gamma \in \mathbb{Z}^n_{\geq 0}$. Questo è equivalente a $\beta = \alpha + \gamma$. Allora, l'insieme

$$\alpha + \mathbb{Z}^n_{\geq 0} = \left\{\alpha + \gamma : \gamma \in \mathbb{Z}^n_{\geq 0}\right\}$$

è formato dagli esponenti di tutti i monomi divisibili per x^α. Questa osservazione, assieme al Lemma 2, ci permette di tracciare grafici dei monomi in un dato ideale monomiale. Per esempio, se $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$, allora gli esponenti dei monomi in I formano l'insieme

$$((4, 2) + \mathbb{Z}^2_{\geq 0}) \cap ((3, 4) + \mathbb{Z}^2_{\geq 0}) \cap ((2, 5) + \mathbb{Z}^2_{\geq 0}).$$

Possiamo visualizzare questo insieme come l'unione dei punti interi in tre copie traslate del primo quadrante del piano, con la biiezione $(m, n) \leftrightarrow x^m y^n$.



Ora, mostriamo che si può determinare se un dato polinomio f giace su un ideale monomiale analizzando i monomi di f.

Lemma 3. *Sia I un ideale monomiale, e sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. I seguenti sono fatti equivalenti:*

(i) $f \in I$.

(ii) Ogni termine di f appartiene a I.

(iii) f è una combinazione $\mathbb{K}$-lineare di monomi di I.

Corollario 4. *Due ideali monomiali coincidono se e solo se contengono gli stessi monomi.*

Il risultato principale di questa sezione è che tutti gli ideali monomiali di $\mathbb{K}[x_1, \ldots, x_n]$ sono finitamente generati.

Teorema 5. *(Lemma di Dickson) Un ideale monomiale $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1 \ldots, x_n]$ può essere scritto nella forma $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, dove $\alpha(1), \ldots, \alpha(s) \in A$. In particolare, I ha una base finita.*

Dimostrazione. (Per induzione sul numero delle variabili n.) Se $n = 1$, allora I è generato dai monomi x^α, dove $\alpha \in \mathbb{Z}_{\geq 0}$. Sia β il più piccolo elemento di $A \subset \mathbb{Z}_{\geq 0}$; allora x^β divide tutti gli altri generatori, e quindi $I = \langle x^\beta \rangle$.

Ora supponiamo $n > 1$ e che il teorema sia vero per $n - 1$. Scriveremo le variabili come $x_1, \ldots, x_{n-1}, y$ in modo tale da poter scrivere i polinomi di $\mathbb{K}[x_1, \ldots, x_{n-1}, y]$ nella forma $x^\alpha y^m$, dove $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ e $m \in \mathbb{Z}_{\geq 0}$.

Supponiamo che $I \subset \mathbb{K}[x_1, \ldots, x_{n-1}, y]$ sia un ideale monomiale. Per trovare generatori per I, sia J l'ideale in $\mathbb{K}[x_1, \ldots, x_{n-1}]$ generato dai monomi x^α per cui $x^\alpha y^m \in I$ per qualche $m \geq 0$. Poiché J è un ideale monomiale in $\mathbb{K}[x_1, \ldots, x_{n-1}]$, l'ipotesi di induzione implica che un numero finito di x^α generi J, poniamo $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. L'ideale J può essere visto come la "proiezione" di I su $\mathbb{K}[x_1, \ldots, x_{n-1}]$.

Per ogni i tra 1 e s, la definizione di J ci dice che $x^{\alpha(i)} y^{m_i} \in I$ per qualche $m_i \geq 0$. Sia m il massimo degli m_i, allora per ogni k tra 0 e $m-1$ consideriamo l'ideale $J_k \subset \mathbb{K}[x_1, \ldots, x_{n-1}]$ generato dai monomi x^β tali che $x^\beta y^k \in I$. Possiamo pensare a J_k come alla "fetta" di I generata dai monomi contenenti y esattamente alla k-esima potenza. Utilizzando nuovamente l'ipotesi di induzione, J_k ha un insieme finito di generatori, poniamo $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle$.

Vogliamo dimostrare che I è generato dai monomi del seguente elenco:

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

Prima di tutto osserviamo che ogni monomio in I è divisibile per un elemento dell'elenco. Per vedere perché, sia $x^\alpha y^p \in I$. Se $p \geq m$, allora $x^\alpha y^p$ è divisibile per qualche $x^{\alpha(i)} y^m$ per costruzione di J. Al contrario, se $p \leq m-1$, allora $x^\alpha y^p$ è divisibile per qualche $x^{\alpha_p(j)} y^p$ per costruzione di J_p. Per il Lemma 2, questi monomi generano un ideale avente gli stessi monomi di I. Per il Corollario 4, questo implica che gli ideali coincidono, e abbiamo dimostrato la nostra affermazione.

Per completare la dimostrazione del teorema, dobbiamo mostrare che l'insieme finito dei generatori può essere scelto da un dato insieme di generatori per l'ideale. Tornando a indicare le variabili con $x_1, \ldots, x_n$, il nostro ideale monomiale è $I = \langle x^\alpha : \alpha \in A \rangle \subset \mathbb{K}[x_1 \ldots, x_n]$. Dobbiamo dimostrare che I è generato da un numero finito di x^α, dove $\alpha \in A$. Per il paragrafo precedente, sappiamo che $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ per certi monomi $x^{\beta(i)}$ in I. Poiché $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A \rangle$, il Lemma 2 ci dice che per ogni $\beta(i)$ esiste almeno un $\alpha(i) \in A$ tale che $x^{\beta(i)}$ sia divisibile per $x^{\alpha(i)}$. Si mostra ora facilmente che $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, e la dimostrazione è conclusa. □

Per comprendere meglio come funzioni la dimostrazione del Teorema 5, applichiamola all'ideale $I = \langle x^4 y^2, x^3 y^4, x^2 y^5 \rangle$ già incontrato in questa sezione. Dal grafico degli esponenti, possiamo vedere che la "proiezione" è

$J = \langle x^2 \rangle \subset \mathbb{K}[x]$. Poiché $x^2y^5 \in I$, abbiamo $m = 5$, e otteniamo le "fette" $J_k, 0 \leq k \leq 4 = m - 1$, generate dai monomi contenenti y^k:

$$\begin{aligned} J_0 = J_1 &= \{0\}, \\ J_2 = J_3 &= \langle x^4 \rangle, \\ J_4 &= \langle x^3 \rangle. \end{aligned}$$

Queste "fette" sono facili da vedere utilizzando il grafico degli esponenti. Allora la dimostrazione del Teorema 5 dà $I = \langle x^2y^5, x^4y^2, x^4y^3, x^3y^4 \rangle$.

Il Teorema 5 risolve il problema di descrizione per ideali monomiali, poiché ci dice che tali ideali hanno base finita. Questo, inoltre, ci permette di risolvere il problema di appartenenza ad un ideale per ideali monomiali. Infatti, se $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, allora possiamo mostrare facilmente che un dato polinomio f appartiene a I se e solo se il resto di f diviso $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ è zero.

Possiamo anche utilizzare il lemma di Dickson per dimostrare il seguente fatto importante a proposito di ordinamenti monomiali in $\mathbb{K}[x_1 \ldots, x_n]$.

Corollario 6. *Sia $>$ una relazione su $\mathbb{Z}^n_{\geq 0}$ che soddisfi:*

(i) $>$ è una relazione d'ordine totale su $\mathbb{Z}^n_{\geq 0}$.

(ii) se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, allora $\alpha + \gamma > \beta + \gamma$.

Allora $>$ è una buona relazione d'ordine se e solo se $\alpha \geq 0$ per ogni $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Dimostrazione. $\Rightarrow$: Assumendo che $>$ sia una buona relazione d'ordine, sia α_0 il più piccolo elemento di $\mathbb{Z}^n_{\geq 0}$. Supponiamo che $0 > \alpha_0$. Aggiungendo $n\alpha_0$ da entrambe le parti, l'ipotesi (ii) implica che $n\alpha_0 > (n+1)\alpha_0$. Quindi

$$0 > \alpha_0 > 2\alpha_0 > \cdots > n\alpha_0 > (n+1)\alpha_0 > \cdots .$$

Questa sequenza decrescente infinita contraddice l'assunto che $>$ fosse una buona relazione d'ordine.

$\Leftarrow$: Assumendo che valga $\alpha \geq 0$ per ogni $\alpha \in \mathbb{Z}^n_{\geq 0}$, sia $A \subset \mathbb{Z}^n_{\geq 0}$ non vuoto. Dobbiamo mostrare che A ammette minimo. Poiché $I = \langle x^\alpha : \alpha \in A \rangle$ è un ideale monomiale, il Lemma di Dickson ci dice che esistono $\alpha(1), \ldots, \alpha(s) \in A$ tali che $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Rinominandoli se necessario, possiamo supporre $\alpha(1) < \alpha(2) < \cdots < \alpha(s)$, e affermiamo che $\alpha(1)$ è il minimo di A. Per dimostrare ciò prendiamo $\alpha \in A$: allora $x^\alpha \in I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Quindi, per il Lemma 2, x^α è divisibile per qualche $x^{\alpha(i)}$. Questo implica $\alpha = \alpha(i) + \gamma$ per qualche $\gamma \in \mathbb{Z}^n_{\geq 0}$. Allora $\gamma \geq 0$ e l'ipotesi (ii) implica che

$$\alpha = \alpha(i) + \gamma \geq \alpha(i) + 0 = \alpha(i) \geq \alpha(1).$$

E di conseguenza $\alpha(1)$ è l'elemento minimo di A. $\square$

Grazie a questo corollario, la definizione di ordinamento monomiale data in (1) può essere semplificata. Le condizioni (i) e (ii) rimangono invariate, ma si può sostituire a (iii) la più semplice condizione che $\alpha \geq 0$ per ogni $\alpha \in \mathbb{Z}^n_{\geq 0}$. Questo rende *molto* più facile verificare se una data relazione d'ordine sia effettivamente un ordinamento monomiale.

2.5 Teorema della base di Hilbert e basi di Groebner

In questa sezione daremo una completa soluzione del *problema di descrizione dell'ideale* visto nella Sezione 2.1, e la nostra trattazione condurrà anche a basi di ideali con "buone" proprietà relative all'algoritmo della divisione introdotto nella Sezione 2.3. L'idea fondamentale che useremo è il fatto che una volta scelto l'ordinamento monomiale, ogni $f \in \mathbb{K}[x_1, \ldots, x_n]$ ha un unico termine direttivo $\text{LT}(f)$. Allora, per ogni ideale I possiamo definire il suo *ideale iniziale* come segue.

Definizione 1. *Sia $I \subset \mathbb{K}[x_1 \ldots, x_n]$ un ideale diverso da $\{0\}$.*

(i) Denotiamo con $\text{LT}(I)$ l'insieme dei termini direttivi degli elementi di I, ovvero

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

(ii) Denotiamo con $\text{in}(I)$ l'ideale generato dagli elementi di $\text{LT}(I)$.

Abbiamo già visto che i termini direttivi hanno un ruolo importante nell'algoritmo della divisione. Questo conduce ad un aspetto importante riguardante $\text{in}(I)$: infatti, se abbiamo un insieme finito di generatori per I, diciamo $I = \langle f_1, \ldots, f_s \rangle$, allora $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$ e $\text{in}(I)$ possono essere ideali *differenti*. É vero che $\text{LT}(f_i) \in \text{LT}(I) \subset \text{in}(I)$ per definizione, il che implica $\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle \subset \text{in}(I)$. Tuttavia, $\text{in}(I)$ può essere strettamente più grande. Per vedere ciò, consideriamo il seguente esempio.

Esempio 1 : Sia $I = \langle f_1, f_2 \rangle$, dove $f_1 = x^3 - 2xy$ e $f_2 = x^2y - 2y^2$, e utilizziamo l'ordine grlex sui monomi di $\mathbb{K}[x, y]$. Allora

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

e quindi $x^2 \in I$. Allora, $x^2 = \text{LT}(x^2) \in \text{in}(I)$. Tuttavia, x^2 non è divisibile per $\text{LT}(f_1) = x^3$ o per $\text{LT}(f_2) = x^2y$, e quindi $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$ per il Lemma 2.

Mostreremo ora che $\text{in}(I)$ è un ideale monomiale, il che ci permetterà di applicare i risultati della Sezione 2.4. In particolare, avremo che $\text{in}(I)$ è generato da un numero finito di termini direttivi.

Proposizione 2. *Sia $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideale.*

(i) $\text{in}(I)$ *è un ideale monomiale.*

(ii) Esistono $g_1, \ldots, g_t \in I$ *tali che* $\text{in}(I) = \big\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \big\rangle$.

Dimostrazione. (i) I monomi direttivi $\text{LM}(g)$ degli elementi $g \in I \setminus \{0\}$ generano l'ideale monomiale $\big\langle \text{LM}(g) : g \in I \setminus \{0\} \big\rangle$. Poiché $\text{LM}(g)$ e $\text{LT}(g)$ differiscono per una costante non nulla, questo ideale è uguale a $\big\langle \text{LT}(g) : g \in I \setminus \{0\} \big\rangle$. Allora, $\text{in}(I)$ è un ideale monomiale.

(ii) Poiché $\text{in}(I)$ è generato dai monomi $\text{LM}(g)$ per $g \in I \setminus \{0\}$, il Lemma di Dickson ci dice che $\text{in}(I) = \big\langle \text{LM}(g_1), \ldots, \text{LM}(g_t) \big\rangle$ per un numero finito di $g_1, \ldots, g_t \in I$. Poiché $\text{LM}(g_i)$ differisce da $\text{LT}(g_i)$ per una costante non nulla, ne segue che $\text{in}(I) = \big\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \big\rangle$, e con questo la dimostrazione è quindi conclusa. □

Possiamo ora usare la Proposizione 2 e l'algoritmo della divisione per dimostrare l'esistenza di un insieme finito di generatori per *ogni* ideale di polinomi, dando quindi risposta affermativa al problema di descrizione dell'ideale della Sezione 2.1. Sia $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un generico ideale e consideriamo l'ideale associato $\text{in}(I)$ come nella Definizione 1. Come sempre, abbiamo scelto un particolare ordine monomiale da utilizzare nell'algoritmo e nel calcolo dei termini direttivi.

Teorema 3. *(Teorema della Base di Hilbert) Ogni ideale* $\mathbf{I} \subset \mathbb{K}[x_1, \ldots, x_n]$ *ha un insieme finito di generatori, ovvero* $I = \big\langle g_1, \ldots, g_t \big\rangle$ *per certi* $g_1, \ldots, g_t \in I$.

Dimostrazione. Se $I = \{0\}$, prendiamo come insieme di generatori $\{0\}$, che è finito. Se I contiene polinomi non nulli, allora possiamo costruire un insieme di generatori $g_1, \ldots, g_t$ per I nel modo seguente. Per la Proposizione 2, esistono $g_1, \ldots, g_t \in I$ tali che $\text{in}(I) = \big\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \big\rangle$, e affermiamo che $I = \big\langle g_1, \ldots, g_t \big\rangle$.

É chiaro che $\big\langle g_1, \ldots, g_t \big\rangle \subset I$ poiché ogni $g_i \in I$. D'altra parte, sia $f \in I$ un generico polinomio. Se applichiamo l'algoritmo della divisione della Sezione 2.3 e dividiamo f per $g_1, \ldots, g_t$, allora otteniamo un'espressione nella forma

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

dove nessun termine di r è divisibile per i $\text{LT}(g_1), \ldots, \text{LT}(g_t)$. Affermiamo che $r = 0$, e per mostrare ciò notiamo che

$$r = f - a_1 g_1 - \cdots a_t g_t \in I.$$

Se $r \neq 0$, allora $\text{LT}(r) \in \text{in}(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, e per il Lemma 2 segue che $\text{LT}(r)$ deve essere divisibile per qualche $\text{LT}(g_i)$. Questo contraddice il fatto che r sia un resto, e quindi deve essere $= 0$. Quindi,

$$f = a_1 g_1 + \cdots a_t g_t + 0 \in \langle g_1, \ldots, g_t \rangle,$$

che mostra il fatto che $I \subset \langle g_1, \ldots, g_t \rangle$, e la dimostrazione è completa. □

Oltre a rispondere alla domanda sulla descrizione dell'ideale, la base $\{g_i\}$ utilizzata nella dimostrazione del Teorema 3 ha la particolare proprietà che $\text{in}(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Come abbiamo visto negli esempi, non tutte le basi di un ideale si comportano in questo modo. Daremo a queste speciali basi il seguente nome.

Definizione 4. *Fissato un ordine monomiale, un sottoinsieme finito $G = \{g_1, \ldots, g_t\}$ di un ideale I è detto* ***base di Groebner*** *(o* ***base standard****) se*

$$\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle = \text{in}(I).$$

Equivalentemente, anche se in modo meno formale, un insieme $\{g_1, \ldots, g_t\} \subset I$ è una base di Groebner per I se e solo se il termine direttivo di ogni elemento di I è divisibile per uno dei $\text{LT}(g_i)$ (questo fatto è una diretta conseguenza del Lemma 2). La dimostrazione del Teorema 3 stabilisce anche il seguente risultato.

Corollario 5. *Fissato un ordine monomiale, ogni ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ diverso da $\{0\}$ ammette una base di Groebner. Inoltre, ogni base di Groebner di un ideale I è una base di I.*

Dimostrazione. Dato un ideale non nullo, l'insieme $G = \{g_1, \ldots, g_t\}$ costruito nella dimostrazione del Teorema 3 è una base di Groebner per definizione. Per quanto riguarda la seconda affermazione, notiamo che se $\text{in}(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, allora il procedimento mostrato nel Teorema 3 ci porta a dire che $I = \langle g_1, \ldots, g_t \rangle$, quindi G è una base per I. □

Nella Sezione 2.6 studieremo le proprietà delle basi di Groebner più in dettaglio, ed in particolare vedremo come esse danno una soluzione del problema di appartenenza all'ideale. Le basi di Groebner sono i "buoni" insiemi di generatori che cercavamo alla fine della Sezione 2.3.

Esempio 2 : Consideriamo innanzitutto l'ideale I, già visto in precedenza, che ha per base $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$. Allora, $\{f_1, f_2\}$ *non* è una base di Groebner per I rispetto all'ordine grlex, dal momento che abbiamo visto che $x^2 \in \text{in}(I)$, ma $x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$. Nella Sezione 2.7, impareremo a trovare una base di Groebner per I.

Esempio 3 : Consideriamo ora l'ideale $J = \langle g_1, g_2 \rangle = \langle x + z, y - z \rangle$. La nostra tesi è che g_1 e g_2 costituiscono una base di Groebner secondo l'ordine lex in $\mathbb{R}[x, y, z]$. Quindi, dobbiamo mostrare che il termine direttivo di ogni elemento non nullo di J giace nell'ideale $\langle \text{LT}(g_1), \text{LT}(g_2) \rangle = \langle x, y \rangle$. Per il Lemma 2, ciò equivale a mostrare che la forma iniziale di *ogni* elemento non nullo di J sia divisibile per x o y.

Per dimostrare questo, consideriamo un generico $f = Ag_1 + Bg_2 \in J$. Supponiamo per assurdo che f sia non nullo e che $\text{LT}(f)$ non sia divisibile né per x né per y: allora, per la definizione di ordine lex, f deve essere un polinomio nella sola z. Tuttavia, f si annulla sul sottospazio lineare $L = \mathbf{V}(x + z, y - z) \subset \mathbb{R}^3$ poiché $f \in J$. Si verifica facilmente che $(x, y, z) = (-t, t, t) \in L$ per ogni valore reale di t. L'unico polinomio nella sola z che si annulla in tutti questi punti è il polinomio nullo, e siamo giunti ad un assurdo. Ne segue che $\{g_1, g_2\}$ è una base di Groebner per J. Nella Sezione 2.6 vedremo un metodo più sistematico per determinare quando una base sia di Groebner.

Osserviamo tra l'altro che i generatori dell'ideale J vengono da una matrice in forma triangolare superiore:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$$

Questo non accade per caso; per ideali generati da polinomi lineari, una base di Groebner per l'ordine lex è determinata dalla forma triangolare superiore della matrice costruita a partire dai coefficienti dei generatori.

Le basi di Groebner sono state introdotte per la prima volta nella prima metà del 1960 da H. Hironaka (che le chiamò "basi standard") e, indipendentemente, poco più tardi da B. Buchberger nella sua tesi di dottorato. Il nome "basi di Groebner" fu coniato da Buchberger in onore del suo relatore W. Gröbner (1899 - 1980). Utilizziamo la dicitura "basi di Groebner", derivante dall'inglese, dal momento che questo è il nome del comando in gran parte dei sistemi informatici di algebra che le implementano.

Concludiamo questa sezione con due applicazioni del Teorema della base di Hilbert. La prima è un fatto algebrico riguardante gli ideali dello spazio $\mathbb{K}[x_1, \ldots, x_n]$: una **catena ascendente** di ideali è una sequenza crescente

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

Ad esempio, la sequenza

$$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, \ldots, x_n \rangle \tag{2.9}$$

formano una catena ascendente (finita) di ideali. Se tentiamo di *estendere* questa catena includendo un ideale con ulteriori generatori, si verifica uno tra i due seguenti casi. Consideriamo l'ideale $\langle x_1, \ldots, x_n, f \rangle$, dove $f \in \mathbb{K}[x_1, \ldots, x_n]$. Se $f \in \langle x_1, \ldots, x_n \rangle$, allora otteniamo $\langle x_1, \ldots, x_n \rangle$ e nulla è cambiato. Se tuttavia valesse $f \notin \langle x_1, \ldots, x_n \rangle$, allora affermiamo che $\langle x_1, \ldots, x_n, f \rangle = \mathbb{K}[x_1, \ldots, x_n]$. Omettiamo la dimostrazione di questo fatto, ma osserviamo che di conseguenza la catena ascendente (2.9) può essere

continuata solo in due versi, o ripetendo l'ultimo ideale all'infinito, oppure aggiungendo $\mathbb{K}[x_1, \ldots, x_n]$ e quindi ripetendo all'infinito quest'ultimo. In ogni caso, la catena ascendente si sarà "stabilizzata" dopo un numero finito di passi, nel senso che tutti gli ideali oltre quel punto nella catena saranno uguali. Il nostro prossimo risultato mostra che lo stesso fenomeno si verifica in *ogni* catena ascendente di ideali in $\mathbb{K}[x_1, \ldots, x_n]$.

Teorema 6. *(Condizione della Catena Ascendente) Sia*

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

una catena ascendente di ideali in $\mathbb{K}[x_1, \ldots, x_n]$. *Allora esiste un* $N \geq 1$ *tale che*

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

Dimostrazione. Data la catena ascendente $I_1 \subset I_2 \subset I_3 \subset \cdots$, consideriamo l'insieme $\bigcup_{i=1}^{\infty} I_i$. Cominciamo col mostrare che I è anch'esso un ideale in $\mathbb{K}[x_1, \ldots, x_n]$: prima di tutto, $0 \in I$ poiché $0 \in I_i$ per ogni i. Poi, se $f, g \in I$, allora per definizione $f \in I_i$ e $g \in I_j$ per certi i, j (eventualmente diversi). Tuttavia, poiché gli ideali I_i formano una catena ascendente, se riordiniamo gli indici in modo tale che $i \leq j$, f e g saranno contenuti in I_j. Poiché I_j è un ideale, la somma $f + g \in I_j$, e quindi $\in I$. Analogamente, se $f \in I$ e $r \in \mathbb{K}[x_1, \ldots, x_n]$, allora $f \in I_i$ per qualche i, e $r \cdot f \in I_i \subset I$. Quindi, I è un ideale.

Per il Teorema della base di Hilbert, l'ideale I deve avere un insieme finito di generatori: $I = \langle f_1, \ldots, f_s \rangle$. ma ciascun generatore è contenuto in qualcuno dei I_j, supponiamo $f_i \in I_{j_i}$ per certi $j_i, i = 1, \ldots, s$. Sia N il massimo degli j_i: per la definizione di catena ascendente $f_i \in I_N$ per ogni i. Quindi abbiamo

$$I = \langle f_1, \ldots, f_s \rangle \subset I_N \subset I_{N+1} \subset \cdots \subset I,$$

e risulta che la catena ascendente si stabilizza con I_N, e tutti gli ideali successivi nella catena sono uguali. □

Il fatto che ogni catena ascendente di ideali in un anello (nel nostro caso $\mathbb{K}[x_1, \ldots, x_n]$) si stabilizzi è spesso detto **condizione della catena ascendente**, in breve CCA; l'anello prende inoltre il nome di **anello Noetheriano**. Si può dimostrare che, se vale la CCA, ogni ideale è finitamente generato; la condizione è quindi equivalente alla conclusione del Teorema della base di Hilbert. Utilizzeremo la CCA in un passaggio fondamentale nella Sezione 2.7, quando analizzeremo l'algoritmo di Buchberger per costruire basi di Groebner.

La seconda conseguenza del Teorema della base di Hilbert che trattiamo sarà di tipo geometrico. Fino ad ora, abbiamo considerato le varietà affini come insiemi di soluzioni di specifici insiemi finiti di equazioni polinomiali:

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f_i(a_1, \ldots, a_n) = 0 \quad \forall\, i\}.$$

Il Teorema della base di Hilbert mostra che, in realtà, ha ugualmente senso parlare della varietà affine definita da un *ideale* $I \subset \mathbb{K}[x_1, \ldots, x_n]$.

Definizione 7. *Sia* $I \subset \mathbb{K}[x_1, \ldots, x_n]$ *un ideale. Indicheremo con* $\mathbf{V}(I)$ *l'insieme*

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0 \quad \forall\, f \in I\}.$$

Sebbene un ideale non nullo I contenga sempre infiniti polinomi distinti, l'insieme $\mathbf{V}(I)$ può comunque essere definito da un insieme finito di equazioni polinomiali.

Proposizione 8. $\mathbf{V}(I)$ *è una varietà affine. In più, se* $I = \langle f_1, \ldots, f_s \rangle$, *allora* $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

Dimostrazione. Per il Teorema della base di Hilbert, $I = \langle f_1, \ldots, f_s \rangle$ per qualche insieme finito di generatori. Vogliamo mostrare che $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$. Prima di tutto, poiché le $f_i \in I$, se $f(a_1, \ldots, a_n) = 0$ per ogni $f \in I$, allora $f_i(a_1, \ldots, a_n) = 0$, e quindi $\mathbf{V}(I) \subset \mathbf{V}(f_1, \ldots, f_s)$. Supponiamo invece $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$ e sia $f \in I$. Poiché $I = \langle f_1, \ldots, f_s \rangle$, possiamo scrivere

$$f = \sum_{i=1}^{s} h_i f_i$$

per certi $h_i \in \mathbb{K}[x_1, \ldots, x_n]$. Ma allora

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0. \end{aligned}$$

Quindi, $\mathbf{V}(f_1, \ldots, f_s) \subset \mathbf{V}(I)$, e la doppia inclusione è dimostrata. □

La conseguenza più importante di questa proposizione è che *le varietà sono determinate dagli ideali*. Ad esempio, nel Capitolo 1 abbiamo dimostrato che $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$ quando $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. (cfr. Capitolo 1, Proposizione 4). Questo fatto è un immediato corollario della Proposizione 8.

2.6 Proprietà delle basi di Groebner

Come visto nella Sezione 2.5, ogni ideale non nullo $I \subset \mathbb{K}[x_1, \ldots, x_n]$ ammette una base di Groebner. In questa sezione, studieremo le proprietà delle basi di Groebner e forniremo un metodo per capire se una data base sia di Groebner. Cominciamo col mostrare che il comportamento indesiderato dell'algoritmo della divisione in $\mathbb{K}[x_1, \ldots, x_n]$ (di cui ci siamo occupati nella Sezione 2.3) non si verifica quando dividiamo per gli elementi di una base di Groebner.

Il nostro primo passo è dimostrare che il resto è univocamente determinato quando dividiamo per una base di Groebner.

Proposizione 1. *Sia $G = \{g_1, \ldots, g_t\}$ una base di Groebner per un ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ e sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Allora esiste un unico $r \in \mathbb{K}[x_1, \ldots, x_n]$ con le seguenti proprietà:*

(i) Nessun termine di r è divisibile per alcuno dei $\text{LT}(g_1), \ldots, \text{LT}(g_t)$.

(ii) Esiste $g \in I$ tale che $f = g + r$.

In particolare, r è il resto della divisione di f per G indipendentemente dall'ordine in cui gli elementi di G vengono considerati nell'esecuzione dell'algoritmo della divisione.

Dimostrazione. L'algoritmo della divisione produce $f = a_1 g_1 + \cdots + a_t g_t + r$, con r che soddisfa (i). Possiamo anche soddisfare (ii) ponendo $g = a_1 g_1 + \cdots + a_t g_t \in I$. Questo prova l'esistenza di r.

Per dimostrare l'unicità, supponiamo che $f = g_1 + r_1 = g_2 + r_2$ soddisfino (i) e (ii). Allora $r_2 - r_1 = g_2 - g_1 \in I$, e quindi se $r_2 \neq r_1$, allora $\text{LT}(r_2 - r_1) \in \text{in}(I) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Per il Lemma 2, segue che $\text{LT}(r_2 - r_1)$ è divisibile per qualche $\text{LT}(g_i)$. Questo è impossibile dal momento che nessun termine di r_1, r_2 è divisibile peri $\text{LT}(g_1), \ldots, \text{LT}(g_t)$. Allora deve essere $r_2 - r_1 = 0$, e l'unicità è dimostrata.

La parte finale della proposizione segue dall'unicità di r. □

Sebbene il resto r sia unico, anche per una base di Groebner i "quozienti" a_i prodotti dall'algoritmo della divisione $f = a_1 g_1 + \cdots + a_t g_t + r$ possono variare se elenchiamo i generatori in un ordine differente.

Come corollario, forniamo il seguente criterio per determinare se un polinomio giace in un ideale.

Corollario 2. *Sia $G = \{g_1, \ldots, g_t\}$ una base di Groebner per un ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ e sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Allora $f \in I$ se e solo se il resto di f diviso G è zero.*

Dimostrazione. Se il resto è zero, abbiamo già osservato che $f \in I$. Altrimenti, data $f \in I$ abbiamo che $f = f + 0$ soddisfa le due condizioni della Proposizione 1. Ne segue che 0 è il resto di f diviso G. □

La proprietà enunciata nel Corollario 2 è a volte considerata come definizione di base di Groebner dal momento che è equivalente alla condizione

$$\left\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \right\rangle = \text{in}(I).$$

Utilizzando il Corollario 2, otteniamo un algoritmo per risolvere il problema di appartenenza all'ideale della Sezione 2.1 *ammesso che* conosciamo una base di Groebner G dell'ideale in questione: dobbiamo semplicemente calcolare il resto rispetto a G per determinare se $f \in I$. Nella Sezione 2.7, esamineremo un metodo per trovare le basi di Groebner, e daremo una completa soluzione del problema di appartenenza all'ideale nella Sezione 2.8.

Utilizzeremo la seguente notazione per il resto.

Definizione 3. *Indicheremo con* $\overline{f}^F$ *il resto della divisione di* f *per la* s*-upla ordinata* $F = (f_1, \ldots, f_s)$*. Se* F *è una base di Groebner per* $\left\langle f_1, \ldots, f_s \right\rangle$*, possiamo considerare* F *come un insieme (senza un ordine particolare) per la Proposizione 1.*

Esempio 1 : Considerando $F = (x^2y - y^2, x^4y^2 - y^2) \subset \mathbb{K}[x, y]$, utilizziamo l'ordine lex e otteniamo

$$\overline{x^5y}^F = xy^3$$

poiché l'algoritmo della divisione produce

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Discuteremo ora su come stabilire se un dato insieme di generatori di un ideale sia una base di Groebner. Come abbiamo indicato, l'"ostacolo" al fatto che $\{f_1, \ldots, f_s\}$ sia una base di Groebner è la possibile esistenza di combinazioni polinomiali delle f_i i cui termini direttivi non appartengano all'ideale generato dai $\text{LT}(f_i)$. Un modo in cui questo si può verificare è se i termini direttivi in una apposita combinazione

$$ax^\alpha f_i - bx^\beta f_j$$

si elidono, e rimangono solo termini più piccoli. D'altra parte, $ax^\alpha f_i - bx^\beta f_j \in I$, quindi il suo termine direttivo è in $\text{in}(I)$. Per studiare questo fenomeno di cancellazione, introduciamo le seguenti combinazioni speciali.

Definizione 4. *Siano* $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ *polinomi non nulli.*

(i) *Se* $\text{multideg}(f) = \alpha$ *e* $\text{multideg}(g) = \beta$*, allora sia* $\gamma = (\gamma_1, \ldots, \gamma_n)$*, dove* $\gamma_i = \max(\alpha_i, \beta_i)$ *al variare di* i*. Chiamiamo* x^γ *il* ***minimo comune multiplo*** *di* $\text{LM}(f)$ *e* $\text{LM}(g)$*, e indichiamo* $x^\gamma = \text{mcm}(\text{LM}(f), \text{LM}(g))$*.*

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

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

(Osserviamo che stiamo invertendo i coefficienti direttivi anche qui.)

Esempio 2 : Sia $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ in $\mathbb{R}[x,y]$ con l'ordine grlex. Allora $\gamma = (4,2)$ e

$$\begin{aligned} S(f,g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - (1/3) \cdot y \cdot g \\ &= -x^3y^3 + x^2 - (1/3)y^3. \end{aligned}$$

Un S-polinomio è "progettato" per produrre la cancellazione dei termini direttivi. Infatti, la seguente proposizione mostra che ogni cancellazione di termini direttivi tra polinomi aventi lo stesso multigrado è un risultato di questo tipo di cancellazione.

Lemma 5. *Supponiamo di avere una somma nella forma* $\sum_{i=1}^t c_i x^{\alpha(i)} g_i$*, dove* $c_1, \ldots, c_t$ *sono costanti e* $\alpha(i) + \text{multideg}(g_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ *per ogni* $c_i \neq 0$*. Se la somma ha multigrado strettamente minore, ovvero* $\text{multideg}(\sum_{i=1}^t c_i x^{\alpha(i)} g_i) < \delta$*, allora esistono costanti* c_{jk} *tali che*

$$\sum_{i=1}^t c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k),$$

dove $x^{\gamma_{jk}} = \text{mcm}(\text{LM}(g_j), \text{LM}(g_k))$*. Inoltre, ogni* $x^{\delta-\gamma_{jk}} S(g_j, g_k)$ *ha multigrado* $< \delta$*.*

Dimostrazione. Poniamo $d_i = \text{LC}(g_i)$, in modo tale che $c_i d_i$ sia il coefficiente direttivo di $c_i x^{\alpha(i)} g_i$. Poiché i $c_i x^{\alpha(i)} g_i$ hanno multigrado δ e la loro somma ha multigrado strettamente minore, ne consegue che $\sum_{i=1}^t c_i d_i = 0$.

Definiamo $p_i = x^{\alpha(i)} g_i / d_i$ e osserviamo che p_i ha coefficiente direttivo 1. Consideriamo la somma telescopica

$$\begin{aligned} \sum_{i=1}^t c_i x^{\alpha(i)} g_i = \sum_{i=1}^t c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &\quad + (c_1 d_1 + \cdots + c_{t-1} d_{t_1})(p_{t-1} - p_t) + \\ &\quad + (c_1 d_1 + \cdots + c_t d_t) p_t. \end{aligned}$$

Ora, sia $\text{LT}(g_i) = d_i x^{\beta(i)}$. Per ipotesi, abbiamo $\alpha(i) + \beta(i) = \delta$ per ogni i. Allora $\text{LM}(g_i) = x^{\beta(i)}$ divide x^δ, e di conseguenza anche $x^{\gamma_{jk}} = \text{mcm}(\text{LM}(g_j), \text{LM}(g_k))$ divide x^δ. Allora, $x^{\delta-\gamma_{jk}}$ è un monomio, e abbiamo

$$\begin{aligned} x^{\delta-\gamma_{jk}} S(g_j, g_k) = & \quad x^{\delta-\gamma_{jk}} \left(\frac{x^{\gamma_{jk}}}{\text{LT}(g_j)} g_j - \frac{x^{\gamma_{jk}}}{\text{LT}(g_k)} g_k \right) \\ = & \quad \frac{x^\delta}{d_j x^{\beta(j)}} g_j - \frac{x^\delta}{d_k x^{\beta(k)}} g_k \\ = & \quad \frac{x^{\alpha(j)} g_j}{d_j} - \frac{x^{\alpha(k)} g_k}{d_k} = p_j - p_k. \end{aligned} \tag{2.10}$$

Utilizzando questa equazione e $\sum_{i=1}^t c_i d_i = 0$, la precedente somma telescopica può essere scritta nella forma

$$\begin{aligned} \sum_{i=1}^t c_i x^{\alpha(i)} g_i \quad = \quad & c_1 d_1 x^{\delta-\gamma_{12}} S(g_1, g_2) + (c_1 d_1 + c_2 d_2) x^{\delta-\gamma_{23}} S(g_2, g_3) + \cdots \\ & + (c_1 d_1 + \cdots + c_{t-1} d_{t_1})(x^{\delta-\gamma_{t-1,t}}) S(g_{t-1}, g_t), \end{aligned}$$

che è una somma nella forma desiderata.

Poiché p_j e p_k hanno multigrado δ e termine direttivo 1, la differenza $p_j - p_k$ ha multigrado $< \delta$. Per l'equazione (2.10), lo stesso vale per $x^{\delta-\gamma_{jk}} S(g_j, g_k)$, ed il lemma è dimostrato. □

Per comprendere l'equazione

$$\sum_{i=1}^t c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k),$$

nel Lemma 5, osserviamo quando avviene la cancellazione. Nella somma al primo membro, ogni addendo $c_i x^{\alpha(i)} g_i$ ha multigrado δ, quindi la cancellazione avviene solo dopo averli sommati. Tuttavia, nella somma al secondo membro, ogni addendo $c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k)$ ha multigrado $< \delta$, quindi la cancellazione è già avvenuta. Intuitivamente, questo significa che tutte le cancellazioni vanno attribuite agli S-polinomi.

Utilizzando gli S-polinomi ed il Lemma 5, possiamo ora dimostrare il seguente criterio per determinare quando una base sia una base di Groebner.

Teorema 6. *Sia I un ideale di polinomi. Allora una base $G = \{g_1, \ldots, g_t\}$ per I è base di Groebner per I se e solo se per ogni coppia $i \neq j$, il resto di $S(g_i, g_j)$ diviso G (elencata in un qualsiasi ordine) è zero.*

Dimostrazione. $\Rightarrow$: Se G è una base di Groebner, allora dal momento che $S(g_i, g_j) \in I$ il resto della divisione per G è zero per il Corollario 2.

$\Leftarrow$: Sia $f \in I$ un polinomio non nullo. Dobbiamo mostrare che se gli S-polinomi divisi per G danno tutti resto nullo, allora $\text{LT}(f)$ appartiene a $\langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$ e quindi G è base di Groebner. Prima di scendere nel dettaglio, diamo un'idea del procedimento.

Data $f \in I = \langle g_1, \ldots, g_t \rangle$, esistono polinomi $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ tali che

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.11}$$

Dal Lemma 2 del Capitolo 1, Sezione 1.1, ne segue che

$$\text{multideg}(f) \leq \max_i(\text{multideg}(h_i g_i)). \tag{2.12}$$

Se non vale l'uguaglianza, allora devono avvenire cancellazioni tra i termini direttivi di (2.11). Il Lemma 5 ci permetterà di riscrivere questo in termini degli S-polinomi, e la nostra ipotesi che gli S-polinomi hanno resto nullo ci permetterà di sostituirli con espressioni che implicano meno cancellazioni. Quindi, otterremo una espressione per f che avrà meno cancellazioni di termini direttivi. Continuando in questo modo, ad un certo punto troveremo un'espressione (2.11) per f tale che valga l'uguaglianza in (2.12). Allora $\text{multideg}(f) = \text{multideg}(h_i g_i)$ per certi i, e ne seguirà che $\text{LT}(f)$ è divisibile per $\text{LT}(g_i)$. Questo implicherà $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, che è la nostra tesi.

Forniamo ora i dettagli della dimostrazione. Data un'espressione (2.11) per f, sia $m(i) = \text{multideg}(h_i g_i)$ e definiamo $\delta = \max(m(1), \ldots, m(s))$. Allora la disequazione (2.12) diventa

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

Ora consideriamo *tutti* i possibili modi in cui f può essere scritta nella forma (2.11). Per ognuna di queste espressioni, otteniamo un δ eventualmente differente. Poiché un ordinamento monomiale è un buon ordinamento, possiamo scegliere una espressione (2.11) per f tale che δ sia *minimo*.

Dimostreremo che, scelto il minimo δ, abbiamo $\text{multideg}(f) = \delta$. Allora varrà l'uguaglianza in (2.12), e come abbiamo osservato, ne seguirà che $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, e ciò basterà a dimostrare il teorema.

Resta da mostrare che $\text{multideg}(f) = \delta$. Per assurdo, sia $\text{multideg}(f) < \delta$;

per isolare i termini di multigrado δ, scriviamo f nella seguente forma:

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \text{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \text{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{2.13}$$

I monomi che compaiono nella seconda e terza somma della seconda riga hanno tutti multigrado $< \delta$. Quindi, l'ipotesi multideg$(f) < \delta$ significa che la prima somma ha anch'essa multigrado $< \delta$.

Sia $\text{LT}(h_i) = c_i x^{\alpha(i)}$. Allora la prima somma

$$\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$$

ha esattamente la forma descritta nel Lemma 5 dal momento che i $c_i x^{\alpha(i)} g_i$ hanno multigrado δ e la loro somma ha multigrado strettamente minore. Allora, il Lemma 5 implica

$$\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k), \tag{2.14}$$

dove $c_{jk} \in \mathbb{K}$ e $x^{\gamma_{jk}} = \text{mcm}(\text{LM}(g_j), \text{LM}(g_k))$.

Il prossimo passo è utilizzare la nostra ipotesi che il resto di $S(g_j, g_k)$ diviso $g_1, \ldots, g_t$ sia zero. Utilizzando l'algoritmo della divisione, questo significa che ciascun S-polinomio può essere scritto nella forma

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i, \tag{2.15}$$

dove $a_{ijk} \in \mathbb{K}[x_1, \ldots, x_n]$. L'algoritmo della divisione ci dice anche che

$$\text{multideg}(a_{ijk} g_i) \leq \text{multideg}(S(g_j, g_k)) \tag{2.16}$$

per ogni i, j, k (vedere il Teorema 1), Sezione 2.3. Intuitivamente, questo ci dice che, quando il resto è zero, possiamo trovare un'espressione per $S(g_j, g_k)$ in termini di G dove non tutti i termini direttivi si annullano.

Per sfruttare questo, moltiplichiamo l'espressione di $S(g_j, g_k)$ per $x^{\delta - \gamma_{jk}}$ per ottenere

$$x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

dove $b_{ijk} = x^{\delta-\gamma_{jk}} a_{ijk}$. Allora (2.16) ed il Lemma 5 implicano

$$\text{multideg}(b_{ijk} g_i) \leq \text{multideg}(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta. \tag{2.17}$$

Se sostituiamo la precedente espressione per $x^{\delta-\gamma_{jk}} S(g_j, g_k)$ nell'equazione (2.14), otteniamo

$$\begin{aligned} \sum_{m(i)=\delta} \text{LT}(h_i) g_i &= \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k) \\ &= \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i \left(\sum_{j,k} c_{jk} b_{ijk} \right) g_i. \end{aligned}$$

Scrivendo l'ultima somma come $\sum_i \tilde{h}_i g_i$, dall'equazione (2.17) segue che

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

dal momento che i c_{jk} sono costanti.

Per il passo finale della dimostrazione, sostituiamo $\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_i \tilde{h}_i g_i$ nell'equazione (2.13) per ottenere

$$f = \sum_i \tilde{h}_i g_i + \sum_{m(i)=\delta} (h_i - \text{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i.$$

Abbiamo quindi scritto f come combinazione polinomiale dei g_i dove *tutti* i termini hanno multigrado $< \delta$. Questo contraddice il fatto che δ è minimo e completa la dimostrazione del teorema. □

Il criterio fornito dal Teorema 6 è estremamente utile dal momento che fornisce un algoritmo per controllare se una base sia di Groebner.

Esempio 3 : Consideriamo l'ideale $I = \langle y - x^2, z - x^3 \rangle$ della cubica gobba in $\mathbb{R}^3$. Vogliamo dimostrare che $G = \{y - x^2, z - x^3\}$ è una base di Groebner per l'ordine lex con $y > z > x$. Per provare ciò, utilizziamo il Teorema 6. Il solo S-polinomio che dobbiamo controllare è

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3.$$

Utilizzando l'algoritmo della divisione, giungiamo facilmente a

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0,$$

e di conseguenza $\overline{S(y - x^2, z - x^3)}^G = 0$. Quindi, G è una base di Groebner per I. Inoltre, si può dimostrare che G *non* è una base di Groebner quando utilizziamo l'ordine lex con $x > y > z$.

2.7 Algoritmo di Buchberger

Nel Corollario 5 della Sezione 2.5, abbiamo visto che ogni ideale dello spazio vettoriale $\mathbb{K}[x_1, \ldots, x_n]$ diverso da $\{0\}$ ammette (almeno) una base di Groebner. Sfortunatamente, la dimostrazione fornita non era costruttiva, cioè non ci forniva un metodo per costruire una base di Groebner. Occupiamoci allora del problema: dato un ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$, come possiamo costruire una base di Groebner per I? Per vedere le idee principali alla base del metodo che useremo, torniamo all'ideale visto negli esempi della Sezione 2.5 e procediamo come segue.

Esempio 1 : Consideriamo $\mathbb{K}[x, y]$ con l'ordine grlex, e sia $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Ricordiamo che $\{f_i, f_2\}$ non è una base di Groebner per I dal momento che $\text{LT}(S(f_1, f_2)) = -x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$.

Per produrre una base di Groebner, un'idea naturale è cercare di estendere l'insieme di generatori originario ad una base di Groebner aggiungendo altri polinomi di I. In un certo senso, questo procedimento non aggiunge nulla di nuovo, anzi introduce una certa ridondanza. Tuttavia, le informazioni addizionali che possiamo ottenere da una base di Groebner valgono la nostra fatica.

Che nuovi generatori dovremmo aggiungere? Da quello che abbiamo detto a proposito degli S-polinomi nella Sezione 2.6, ciò che segue non dovrebbe sorprendere. Abbiamo $S(f_1, f_2) = -x^2 \in I$, ed il resto della sua divisione per $F = (f_1, f_2)$ è $-x^2$, che è non nullo. Quindi, dovremmo includere tale resto nel nostro insieme di generatori, come nuovo generatore $f_3 = -x^2$. Se poniamo $F = (f_1, f_2, f_3)$, possiamo utilizzare il Teorema 6 della Sezione 2.6 per verificare se questo nuovo insieme sia una base di Groebner per I. Calcoliamo:

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

Quindi, dobbiamo aggiungere $f_4 = -2xy$ al nostro insieme di generatori. Se poniamo $F = (f_1, f_2, f_3, f_4)$, allora

$$\begin{aligned} \overline{S(f_1, f_2)}^F &= \overline{S(f_1, f_3)}^F = 0, \\ S(f_1, f_4) &= y(x^3 - 2xy) - (1/2)x^2(-2xy) = -2xy^2 = yf_4, \text{ quindi} \\ \overline{S(f_1, f_4)}^F &= 0, \\ S(f_2, f_3) &= (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \text{ ma} \\ \overline{S(f_2, f_3)}^F &= -2y^2 + x \neq 0. \end{aligned}$$

Quindi, dobbiamo aggiungere anche $f_5 = -2y^2 + x$ al nostro insieme di generatori. Ponendo $F = \{f_1, f_2, f_3, f_4, f_5\}$, si verifica che

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

Per il Teorema 6 della Sezione 2.6, una base di Groebner per I è allora data da

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

La procedura che abbiamo usato nell'esempio, consistente nell'aggiungere $\overline{S(f_i, f_j)}^F$ a F se è non nullo può essere tradotta in un algoritmo per produrre basi di Groebner. La versione che presenteremo è molto rudimentale: questo algoritmo di Buchberger è la pietra miliare della geometria computazionale algebrica. Negli anni '70 e '80, Buchberger ed i suoi collaboratori hanno introdotto diversi miglioramenti per aumentare l'efficienza dell'algoritmo.

Teorema 1. *Sia $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ un ideale di polinomi. Allora, una base di Groebner per I può essere costruita in un numero finito di passi tramite il seguente algoritmo.*

```
Input:  F = (f_1, ..., f_s)
Output: una base di Groebner G = (g_1, ..., g_t) per I, con F ⊂ G

G := F
DO
    G' := G
    FOR ogni coppia {p, q}, p ≠ q in G DO
        S := S(p, q)^G'
        IF S ≠ 0 THEN G := G ∪ {S}
WHILE G ≠ G'
```

Dimostrazione. Mostriamo innanzitutto che $G \subset I$ è vera ad ogni passo dell'algoritmo. Ciò è vero all'inizio, ed ogni volta che espandiamo G, lo facciamo aggiungendo il resto $S = \overline{S(p,q)}^{G'}$ per $p, q \in G$. Quindi, se $G \subset I$, allora p, q e conseguentemente anche $S(p, q)$ appartengono a I, e dal momento che stiamo dividendo per $G' \subset I$, otteniamo $G \cup \{S\} \subset I$. Notiamo anche che G contiene la base iniziale F di I, quindi G è effettivamente una base di I.

L'algoritmo termina quando $G = G'$, che significa $\overline{S(p,q)}^G = 0$ per ogni $p, q \in G$. Quindi G è una base di Groebner per $\langle G \rangle = I$ per il Teorema 6 della Sezione 2.6.

Resta da dimostrare che l'algoritmo termina. Dobbiamo considerare ciò che accade dopo ogni passo nel ciclo principale. L'insieme G consiste di G' (la precedente G) unita ai resti non nulli degli S-polinomi di elementi di G'. Allora

$$\text{in}(G') \subset \text{in}(G) \tag{2.18}$$

dal momento che $G' \subset G$. Inoltre, se $G' \neq G$, affermiamo che $\text{in}(G')$ è strettamente contenuto in $\text{in}(G)$. Per vedere ciò, supponiamo che un resto non nullo r di un S-polinomio sia stato aggiunto a G'. Poiché r è il resto di una divisione per G', $\text{LT}(r)$ non è divisibile per i termini direttivi degli elementi di G', e quindi $\text{LT}(r) \notin \text{in}(G')$. Tuttavia, $\text{LT}(r) \in \text{in}(G)$, e la nostra affermazione è provata.

Per (2.18), gli ideali $\text{in}(G')$ ottenuti dalle successive iterazioni del ciclo formano una catena ascendente di ideali in $\mathbb{K}[x_1, \ldots, x_n]$. Quindi la CCA (Sezione 2.4, Teorema 6) implica che dopo un numero finito di iterazioni la catena si stabilizzi, e quindi vale definitivamente $\text{in}(G') = \text{in}(G)$. Per il paragrafo precedente, questo implica $G' = G$, ovvero l'algoritmo deve terminare dopo un numero finito di passi. □

Prima di continuare, dovremmo precisare che l'algoritmo utilizzato nel teorema è stato scelto per una maggiore chiarezza espositiva, ma non è un metodo pratico per eseguire i calcoli. Osserviamo che, come prima ottimizzazione, una volta che un resto $\overline{S(p,q)}^{G'} = 0$, tale resto rimarrà zero anche se aggiungiamo ulteriori elementi alla fine dell'insieme ordinato di generatori G'. Quindi, non c'è ragione di ricalcolare tali resti nei passaggi successivi del ciclo principale: in effetti, aggiungendo i nostri nuovi generatori f_j uno per volta, gli unici resti che dobbiamo verificare saranno $\overline{S(f_i, f_j)}^{G'}$, dove $i \leq j - 1$. Altre ottimizzazioni di natura più elaborata possono essere implementate, ma per brevità ometteremo una trattazione dettagliata di questo argomento.

Le basi di Groebner calcolate dall'algoritmo del Teorema 1 sono spesso più grandi del necessario, e possiamo eliminare i generatori non necessari utilizzando il seguente fatto.

Lemma 2. *Sia G una base di Groebner per l'ideale di polinomi I. Sia $p \in G$ un polinomio tale che $\text{LT}(p) \in \text{in}(G \setminus \{p\})$. Allora $G \setminus \{p\}$ è ancora una base di Groebner per I.*

Dimostrazione. Sappiamo che $\text{in}(G) = \text{in}(I)$. Se $\text{LT}(p) \in \text{in}(G - \{p\})$, allora $\text{in}(G \setminus \{p\}) = \text{in}(G)$. Per definizione, segue che $G \setminus \{p\}$ è anch'essa una base di Groebner per I. □

Introducendo costanti per rendere monici (ovvero con coefficiente direttivo unitario) tutti i polinomi di G e togliendone ogni p tale che $\text{LT}(p) \in \text{in}(G \setminus \{p\})$, giungiamo a quella che chiameremo base di Groebner **minimale**.

Definizione 3. *Una **base di Groebner minimale** per un ideale polinomiale I è una base di Groebner G per I tale che:*

(i) $\text{LC}(p) = 1$ *per ogni* $p \in G$, *e*

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

Possiamo costruire una base di Groebner minimale per un dato ideale non nullo applicando l'algoritmo del Teorema 1 e successivamente utilizzando il Lemma 2 per eliminare ogni generatore superfluo.

Esempio 2 : Per illustrare la procedura di generazione di una base di Groebner minimale, torniamo ancora una volta all'ideale studiato nel primo esempio di questa sezione. Utilizzando l'ordine grlex, abbiamo trovato la base di Groebner

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

Poiché alcuni dei coefficienti direttivi sono diversi da 1, il primo passo è moltiplicare i generatori per costanti opportune per renderli monici. Dopodichè notiamo che $\text{LT}(f_1) = x^3 = -x \cdot \text{LT}(f_3)$. Per il Lemma 2, possiamo eliminare f_1 nella base di Groebner minimale. Analogamente, dal momento che $\text{LT}(f_2) = x^2y = -(1/2)x \cdot \text{LT}(f_4)$, possiamo eliminare anche f_2. Non vi sono altri casi in cui il termine direttivo di un generatore divida il termine direttivo di un altro generatore. Quindi,

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

è una base di Groebner ridotta per I.

Le basi di Groebner minimali hanno importanti proprietà: ne dimostriamo una che sarà utile in seguito.

Proposizione 4. *Fissato un ordine monomiale, siano* G *e* G' *basi di Groebner minimali per l'ideale* I*: dimostrare che* $\text{LT}(G) = \text{LT}(G')$.

Dimostrazione. Per assurdo, consideriamo un $\overline{g} \in G$ tale che $\text{LT}(\overline{g}) \neq \text{LT}(g')$ per ogni $g' \in G'$. Dal momento che G' è una base di Groebner, vale $\text{LT}(\overline{g}) \in \langle \text{LT}(G') \rangle = \text{in}(I)$ e, dal momento che $\text{in}(I)$ è un ideale monomiale, per il Lemma 2 della Sezione 2.4$\text{LT}(\overline{g})$ è divisibile per $\text{LT}(g')$ per almeno un $g' \in G'$, poniamo $\tilde{g}$. Vale quindi $\langle \text{LT}(\overline{g}) \rangle \subset \langle \text{LT}(\tilde{g}) \rangle$. Inversamente, $\langle \text{LT}(\tilde{g}) \rangle \subset \langle \text{LT}(G) \rangle = \text{in}(I)$ in quanto G è base di Groebner, e quindi $\text{LT}(\tilde{g})$ è divisibile per $\text{LT}(g)$ per almeno uno degli elementi di G, poniamo g. Vogliamo ora mostrare che $\text{LT}(g) = \text{LT}(\overline{g})$.

Dal momento che G è una base di Groebner ridotta, abbiamo $\text{LT}(\overline{g}) \notin \langle \text{LT}(G \setminus \{\overline{g}\}) \rangle = \text{in}(G \setminus \{\overline{g}\})$, e poichè $\text{LT}(\tilde{g})$ divide $\text{LT}(\overline{g})$, anche $\text{LT}(\tilde{g}) \notin$

$\big\langle \operatorname{LT}(G \setminus \{\overline{g}\}) \big\rangle = \operatorname{in}(G \setminus \{\overline{g}\})$. Quindi nessun elemento di $\operatorname{LT}(G \setminus \{\overline{g}\})$ divide $\operatorname{LT}(\tilde{g})$; allora $\operatorname{LT}(\overline{g})$ deve dividere $\operatorname{LT}(\tilde{g})$.

Poichè $\operatorname{LT}(\tilde{g})$ e $\operatorname{LT}(\overline{g})$ si dividono a vicenda, abbiamo $\operatorname{LM}(\tilde{g}) = \operatorname{LM}(\overline{g})$; ma essi sono entrambi elementi di basi di Groebner ridotte, e quindi $\operatorname{LC}(\tilde{g}) = \operatorname{LC}(\overline{g}) = 1$, da cui segue $\operatorname{LT}(\tilde{g}) = \operatorname{LT}(\overline{g})$, il che va contro la nostra prima ipotesi. □

Sfortunatamente, un dato ideale può avere più di basi di Groebner minimali distinte. Ad esempio, nell'ideale I appena considerato, è facile verificare che

$$\tilde{f}_3 = x^2 + axy, \quad \tilde{f}_4 = xy, \quad \tilde{f}_5 = y^2 - (1/2)x \tag{2.19}$$

è anch'essa una base di Groebner minimale, dove $a \in \mathbb{K}$ è una costante generica. Quindi, possiamo produrre infinite basi di Groebner minimali (supponendo $\mathbb{K}$ infinito). Fortunatamente, possiamo isolare una base minimale "migliore" delle altre, secondo la seguente definizione.

Definizione 5. *Una **base di Groebner ridotta** per un ideale di polinomi I è una base di Groebner G tale che:*

(i) $\operatorname{LC}(p) = 1$ *per ogni* $p \in G$.

(ii) Per ogni $p \in G$, *nessun monomio di* p *giace in* $\operatorname{in}(G \setminus \{p\})$.

Osserviamo che per le basi di Groebner fornite in (2.19), solo quella con $a = 0$ è ridotta. In generale, le basi di Groebner ridotte hanno la seguente comoda proprietà.

Proposizione 6. *Sia $I \neq \{0\}$ un ideale di polinomi. Allora, per un dato ordinamento monomiale, I ammette una e una sola base di Groebner ridotta.*

Dimostrazione. Sia G una base di Groebner minimale per I. Diremo che $g \in G$ è *ridotto per* G se nessun monomio di g appartiene a $\operatorname{in}(G \setminus \{g\})$. Il nostro obiettivo è modificare G fino a quando tutti i suoi elementi sono ridotti.

Una prima osservazione è che se g è ridotto per G, allora g è ugualmente ridotto per ogni altra base di Groebner minimale di I che contenga g e abbia lo stesso insieme di termini direttivi. Questo è dato dal fatto che la definizione di riduzione coinvolge esclusivamente i termini direttivi.

Ora, dato $g \in G$, sia $g' = \overline{g}^{G \setminus \{g\}}$ e poniamo $G' = (G \setminus \{g\}) \cap \{g'\}$. Vogliamo dimostrare che G' è una base di Groebner minimale per I. Per vedere ciò, innanzitutto osserviamo che $\operatorname{LT}(g') = \operatorname{LT}(g)$, poiché quando dividiamo g per $G \setminus \{g\}$, $\operatorname{LT}(g)$ finisce al resto dal momento che non è divisibile per nessun

elemento di $\text{LT}(G \setminus \{g\})$. Questo implica $\text{in}(G') = \text{in}(G)$. Poiché G è evidentemente contenuta in I, notiamo che G' è una base di Groebner, e ne segue la minimalità. Infine, osserviamo che g' è ridotto per G' per costruzione.

Ora, prendiamo gli elementi di G e applichiamo il processo appena descritto fino a quando non sono tutti ridotti. La base di Groebner può cambiare ogni volta che iteriamo il processo, ma le nostre precedenti osservazioni mostrano che, una volta che un elemento è ridotto, rimane ridotto in quanto non vengono modificati i termini direttivi. Ne risulta quindi una base di Groebner ridotta.

Infine, per dimostrare l'unicità, supponiamo che G e $\tilde{G}$ siano entrambe basi di Groebner ridotte per I. Allora, in particolare, G e $\tilde{G}$ sono basi di Groebner minimali, e per la Proposizione 4 hanno gli stessi termini direttivi, ovvero

$$\text{LT}(G) = \text{LT}(\tilde{G}).$$

Quindi, dato $g \in G$, esiste $\tilde{g} \in \tilde{G}$ tale che $\text{LT}(g) = \text{LT}(\tilde{g})$. Se riusciamo a dimostrare che $g = \tilde{g}$, ne seguirà $G = \tilde{G}$, ed avremo dimostrato l'unicità.

Per mostrare che $g = \tilde{g}$, consideriamo la differenza $g - \tilde{g}$. Esso è un elemento di I, e poiché G è una base di Groebner, ne segue che $\overline{g - \tilde{g}}^G = 0$. Ma sappiamo anche che $\text{LT}(g) = \text{LT}(\tilde{g})$, quindi i termini direttivi si cancellano in $g - \tilde{g}$ ed i termini rimanenti non sono divisibili per alcun $\text{LT}(G) = \text{LT}(\tilde{G})$, dal momento che G e $\tilde{G}$ sono ridotte. Questo implica $\overline{g - \tilde{g}}^G = g - \tilde{g}$, e quindi $g - \tilde{g} = 0$ completa la dimostrazione. □

Diversi sistemi informatici di algebra implementano una versione dell'algoritmo di Buchberger per calcolare basi di Groebner, e tali sistemi calcolano sempre una base di Groebner ridotta, fornendo così un risultato univocamente determinato ad ogni problema. In questo modo, i risultati possono essere facilmente confrontati tra sistemi diversi.

Un'altra conseguenza dell'unicità dimostrata nella Proposizione 6 è che possiamo costruire un **algoritmo di uguaglianza tra ideali** per verificare se due insiemi di polinomi $\{f_1, \ldots, f_s\}$ e $\{g_1, \ldots, g_t\}$ generano lo stesso ideale: semplicemente, fissiamo un ordine monomiale e calcoliamo le basi ridotte per $\langle f_1, \ldots, f_s \rangle$ e $\langle g_1, \ldots, g_t \rangle$. Allora, gli ideali sono uguali se e solo se le basi di Groebner coincidono.

Per concludere questa sezione, indicheremo brevemente alcune delle connessioni tra l'algoritmo di Buchberger e l'algoritmo di riduzione matriciale (eliminazione di Gauss) per sistemi di equazioni lineari. Il fatto interessante è che l'algoritmo di riduzione matriciale è essenzialmente un caso particolare dell'algoritmo che abbiamo discusso.

Esempio 3 : Per concretezza, discuteremo il caso particolare corrispondente al sistema di equazioni

$$\begin{cases} 3x & - & 6y & - & 2z & & & = & 0, \\ 2x & - & 4y & & & + & 4w & = & 0, \\ x & - & 2y & - & z & - & w & = & 0. \end{cases}$$

Se utilizziamo la riduzione matriciale sulla matrice dei coefficienti per trasformarla in triangolare superiore, otteniamo la matrice

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.20}$$

Per ottenere una matrice triangolare superiore *ridotta*, dobbiamo verificare che ogni 1 direttivo sia il solo valore non nullo nella propria colonna. Questo conduce alla matrice

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.21}$$

Per trasferire questi calcoli all'algebra, sia I l'ideale

$$I = \langle 3x - 6y - 2z, 2x - 4y + 4w, x - 2y - z - w \rangle \in \mathbb{K}[x, y, z]$$

corrispondente al sistema di equazioni originario. Utilizzeremo l'ordine lex con $x > y > z > w$. Dalla matrice (2.20) otteniamo una base di Groebner minimale

$$I = \langle x - 2y - z - w, z + 3w \rangle,$$

mentre la matrice in forma triangolare ridotta ci porta alla base di Groebner ridotta

$$I = \langle x - 2y + 2w, z + 3w \rangle.$$

Ricordiamo, dall'algebra, il fatto che ogni matrice può essere messa in forma triangolare superiore in maniera unica. Questo può essere visto come un caso particolare dell'unicità delle basi di Groebner ridotte.

2.8 Prime applicazioni delle basi di Groebner

Nella Sezione 2.1, abbiamo posto quattro problemi riguardanti ideali e varietà. Il primo era il problema di descrizione dell'ideale, risolto dal Teorema della base di Hilbert nella Sezione 2.5. Consideriamo ora i tre problemi restanti e discutiamo su come possiamo affrontarli utilizzando le basi di Groebner.

2.8.1 Problema di appartenenza all'ideale

Se combiniamo le basi di Groebner con l'algoritmo della divisione, otteniamo il seguente **algoritmo di appartenenza**: dato un ideale $I = \langle f_1, \ldots, f_s \rangle$,

possiamo stabilire se un dato polinomio f appartenga o meno ad I nel modo seguente. Prima di tutto, utilizzando un algoritmo simile al Teorema 1 della Sezione 2.7, troviamo una base di Groebner $G = \{g_1, \ldots, g_t\}$ per I. Allora, il Corollario 2 della Sezione 2.6 implica che

$$f \in I \quad \Leftrightarrow \quad \overline{f}^G = 0.$$

Esempio 1 : Sia $I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^2 \rangle \in \mathbb{C}[x, y, z]$, ed utilizziamo l'ordine grlex. Sia $f = -4x^2y^2z^2 + y^6 + 3z^5$. La nostra domanda è: $f \in I$?

L'insieme di generatori dato non è una base di Groebner di I poiché $\text{LT}(I)$ contiene anche polinomi come $\text{LT}(S(f_1, f_2)) = \text{LT}(x^2y^2 - z^3) = x^2y^2$ che non appartengono all'ideale $\langle \text{LT}(f_1), \text{LT}(f_2) \rangle = \langle xz, x^3 \rangle$. Quindi, cominciamo cominciamo con il calcolare una base di Groebner per I. Utilizzando un programma di calcolo algebrico, troviamo la base di Groebner

$$G = (f_1, f_2, f_3, f_4, f_5) = (xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5).$$

Osserviamo che questa è una base di Groebner ridotta.

Possiamo ora verificare l'appartenenza di polinomi ad I. Ad esempio, dividendo il polinomio sopra citato f per G, otteniamo

$$f = 0 \cdot f_1 + 0 \cdot f_2 - 4z^2 f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Dal momento che il resto è zero, abbiamo $f \in I$.

Esempio 2 : Consideriamo $f = xy - 5z^2 + x$ e l'ideale I dell'esempio precedente. Anche senza eseguire tutto il calcolo del resto di f diviso G, possiamo vedere dalla forma degli elementi di G che $f \notin I$. Infatti, $\text{LT}(f) = xy$ evidentemente non è contenuto nell'ideale $\text{in}(G) = \langle xz, x^3, x^2y^2, xy^4, y^6 \rangle$. Quindi, $\overline{f}^G \neq 0$, che implica $f \notin G$.

Questa ultima osservazione illustra il modo in cui le proprietà di un ideale sono rivelate dalla forma degli elementi di una sua base di Groebner.

2.8.2 Risoluzione di equazioni polinomiali

Ora analizzeremo il modo in cui la tecnica delle basi di Groebner può essere applicata per risolvere sistemi di equazioni polinomiali in più variabili. Cominciamo con l'esposizione di qualche esempio.

Esempio 3 : Consideriamo le equazioni

$$\begin{aligned} x^2 + y^2 + z^2 &= 1, \\ x^2 + z^2 &= y, \\ x &= z \end{aligned} \tag{2.22}$$

in $\mathbb{C}^3$. Queste equazioni determinano $I = \langle x^2+y^2+z^2-1, x^2+z^2-y, x-z\rangle \subset \mathbb{C}[x,y,z]$, e vogliamo trovare tutti i punti di $\mathbf{V}(I)$. La Proposizione 8, Sezione 2.5 implica che possiamo calcolare $\mathbf{V}(I)$ utilizzando una *qualsiasi* base di I. Vediamo quindi cosa accade utilizzando una base di Groebner.

Sebbene al momento non abbiamo stretta necessità di farlo, calcoleremo una base di Groebner per I rispetto all'ordine lex. La base è

$$\begin{aligned} g_1 &= x - z, \\ g_2 &= -y + 2z^2, \\ g_3 &= z^4 + (1/2)z^2 - 1/4. \end{aligned}$$

Se esaminiamo attentamente questi polinomi, troviamo qualcosa di notevole: prima di tutto, il polinomio g_3 dipende esclusivamente dalla z, e le sue radici possono essere calcolate utilizzando il metodo della bi-quadratica, ottenendo

$$z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5}-1}.$$

Questo ci dà quattro valori per z. Ora, sostituendo questi valori nelle equazioni $g_2 = 0$ e $g_1 = 0$, possiamo risolvere queste ultime unicamente per y e x rispettivamente. Quindi, abbiamo quattro soluzioni del sistema $g_1 = g_2 = g_3 = 0$, due reali e due complesse. Dal momento che $\mathbf{V}(I) = \mathbf{V}(g_1, g_2, g_3)$ per la Proposizione 8 della Sezione 2.5, abbiamo trovato *tutte* le soluzioni delle equazioni originarie (2.22).

Esempio 4 : Consideriamo ora il sistema di equazioni polinomiali (1.2) della Sezione 1.1, ottenuto applicando i moltiplicatori di Lagrange per trovare minimo e massimo di $x^3 + 2xyz - z^2$ soggetto al vincolo $x^2 + y^2 + z^2 = 1$:

$$\begin{cases} 3x^2 + 2yz - 2x\lambda &= 0 \\ 2xz - 2y\lambda, &= 0 \\ 2xy - 2z - 2z\lambda, &= 0 \\ x^2 + y^2 + z^2 - 1 &= 0 \end{cases}$$

Di nuovo, seguiamo il nostro solito procedimento ed iniziamo calcolando una base di Groebner per l'ideale in $\mathbb{R}[x,y,z,\lambda]$ generato dai primi membri delle quattro equazioni, utilizzando l'ordine lex con $\lambda > x > y > z$. Troviamo la seguente base di Groebner:

$$\begin{aligned} &\lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 - \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ &x^2 + y^2 + z^2 - 1, \\ &xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ &xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ &y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ &y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ &yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2, \\ &z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z. \end{aligned} \tag{2.23}$$

A prima vista, questa collezione di polinomi sembra poco gestibile (i coefficienti degli elementi delle basi di Groebner possono essere significativamente più complicati dei coefficienti dell'insieme di generatori). Tuttavia, osservando attentamente, notiamo che ancora una volta l'ultimo polinomio dipende esclusivamente dalla variabile z. Abbiamo "eliminato" le altre variabili nel processo di ricerca di una base di Groebner. (Per miracolo,) l'equazione ottenuta ponendo questo polinomio uguale a zero ha le radici

$$z = 0, \quad \pm 1, \quad \pm 2/3, \quad \pm\sqrt{11}/8\sqrt{2}.$$

Se poniamo z uguale ad ognuno di questi valori per volta, le rimanenti equazioni possono essere risolte per x, y (e λ, sebbene i suoi valori non siano rilevanti per i nostri scopi). Otteniamo le seguenti soluzioni:

$$\begin{aligned}
z &= 0; \quad y = 0; \quad x = \pm 1. \\
z &= 0; \quad y = \pm 1; \quad x = 0. \\
z &= \pm 1 \quad y = 0; \quad x = 0. \\
z &= 2/3; \quad y = 1/3; \quad x = -2/3. \\
z &= -2/3; \quad y = -1/3; \quad x = -2/3. \\
z &= \sqrt{11}/8\sqrt{2}; \quad y = -3\sqrt{11}/8\sqrt{2}; \quad x = -3/8. \\
z &= -\sqrt{11}/8\sqrt{2}; \quad y = 3\sqrt{11}/8\sqrt{2}; \quad x = -3/8.
\end{aligned}$$

Da questo punto, è semplice determinare massimo e minimo.

Gli esempi appena visti indicano che trovare una base di Groebner per un ideale rispetto all'ordine lex semplifica la forma delle equazioni considerevolmente; in particolare, sembra che otteniamo equazioni in cui le variabili sono eliminate in successione. Notiamo inoltre che l'*ordine* di eliminazione sembra corrispondere all'ordinamento delle variabili. Infatti, quando avevamo le variabili $\lambda > x > y > z$ notiamo che λ è eliminata per prima, x per seconda, e via di questo passo.

Un sistema di equazioni in questa forma è facilmente risolubile, specialmente quando l'ultima equazione contiene una sola variabile: possiamo applicare le tecniche di risoluzione per equazioni di una variabile, poi ri-sostituire nelle altre equazioni del sistema e risolvere rispetto alle altre variabili, utilizzando una procedura simile agli esempi precedenti. Osserviamo quindi una analogia tra questa procedura di risoluzione di sistemi di equazioni polinomiali ed il metodo di "retro-sostituzione" utilizzato per risolvere un sistema lineare in forma triangolare superiore.

2.8.3 Forma implicita

Supponiamo che le equazioni parametriche

$$\begin{cases}
x_1 &= f_1(t_1, \ldots, t_m), \\
&\vdots \\
x_n &= f_n(t_1, \ldots, t_m)
\end{cases} \tag{2.24}$$

definiscano un sottoinsieme di una varietà algebrica V in $\mathbb{K}^n$. Ad esempio, questo accade ogni volta che le f_i sono funzioni razionali in $t_1, \ldots, t_m$. Come possiamo trovare equazioni polinomiali nelle x_i che definiscano V? Questo problema può essere risolto utilizzando le basi di Groebner, sebbene una completa dimostrazione del procedimento richieda strumenti che non abbiamo introdotto.

Per semplicità, restringeremo la nostra attenzione a casi in cui le f_i sono in realtà *polinomi*. Possiamo studiare la varietà affine in $\mathbb{K}^{m+n}$ definita dalle equazioni (2.24) oppure

$$\begin{cases} x_1 - f_1(t_1, \ldots, t_m) &= 0, \\ & \vdots \\ x_n - f_n(t_1, \ldots, t_m) &= 0. \end{cases}$$

L'idea basilare è eliminare le variabili $t_1, \ldots, t_m$ da queste equazioni. Questo dovrebbe darci le equazioni per V.

Da quello che abbiamo visto negli ultimi due esempi, ha senso utilizzare una base di Groebner per eliminare le variabili. Considereremo l'ordine lex in $\mathbb{K}[t_1, \ldots, t_m, x_1, \ldots, x_n]$ definito dall'ordinamento delle variabili

$$t_1 > \cdots > t_m > x_1 > \cdots > x_n.$$

Ora supponiamo di avere una base di Groebner per l'ideale $\tilde{I} = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$. Dal momento che stiamo utilizzando l'ordine lex, ci aspettiamo che la base di Groebner abbia polinomi che eliminano variabili, e le $t_1, \ldots, t_m$ dovrebbero essere eliminate per prime poiché sono le maggiori nel nostro ordine monomiale. Quindi, le basi di Groebner per $\tilde{I}$ dovrebbero contenere polinomi esclusivamente nelle $x_1, \ldots, x_n$. Questi ultimi sono i nostri candidati come equazioni per V.

Vediamo ora qualche esempio per comprendere il funzionamento del processo.

Esempio 5 : Consideriamo la curva parametrica V:

$$\begin{aligned} x &= t^4, \\ y &= t^3, \\ z &= t^2 \end{aligned}$$

in $\mathbb{C}^3$. Calcoliamo una base di Groebner G di $I = \langle t^4 - x, t^3 - y, t^2 - z \rangle$ rispetto all'ordine lex in $\mathbb{C}[x, y, z]$, e otteniamo

$$G = \{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}.$$

Gli ultimi due polinomi dipendono solo da x, y, z, quindi definiscono una varietà affine di $\mathbb{C}^3$ contenente la nostra curva V. Per l'intuizione sulla dimensione che abbiamo sviluppato

nel Capitolo 1, ci aspettiamo che due equazioni in $\mathbb{C}^3$ definiscano una curva (una varietà uno-dimensionale). L'ultima domanda a cui rispondere è se V è l'intera intersezione delle due superfici

$$x - z^2 = 0, \quad y^2 - z^3 = 0.$$

Possono esserci altre curve (o addirittura superfici) nell'intersezione? Si dimostra che la risposta è no (per una trattazione dell'argomento, si veda [**?**]).

Esempio 6 : Ora consideriamo la superficie tangente la cubica gobba in $\mathbb{R}^3$, che abbiamo studiato nel Capitolo 1. Questa superficie è parametrizzata da

$$\begin{aligned} x &= t + u, \\ y &= t^2 + 2tu, \\ z &= t^3 + 3t^2u. \end{aligned}$$

Calcoliamo una base di Groebner G per questo ideale relativamente all'ordine lex definito da $t > u > x > y > z$, e troviamo che G ha 6 elementi in totale. Se facciamo i calcoli, vediamo che solo uno contiene solo termini in x, y, z:

$$-(4/3)x^3z + x^2y^2 - (4/3)y^3 + 2xyz - (1/3)z^2 = 0. \tag{2.25}$$

La varietà definita da questa equazione è una superficie contenente la superficie tangente la cubica gobba. Tuttavia, è possibile che la superficie data da (2.25) sia strettamente maggiore della superficie tangente: possono esserci soluzioni di (2.25) che non corrispondono a punti sullo spazio tangente.