Università degli Studi di Roma "La Sapienza"

Dina Ghinelli

CORSO di MATEMATICHE ELEMENTARI DA UN PUNTO DI VISTA SUPERIORE

(Laurea Magistrale in Matematica)

(Anno Accademico 2013-2014)

1. Parte I

Dipartimento di Matematica

Facoltà di Scienze Matematiche, Fisiche e Naturali

Capitolo 1

Alcuni problemi Classici

In questo capitolo iniziale introduciamo alcuni problemi classici quali il *Problema della Duplicazione del cubo* e il problema diofanteo della ricerca delle soluzioni intere non banali $(X, Y, Z) \neq (0, 0, 0)$ dell'equazione $X^2 + Y^2 = Z^2$ che dà le terne pitagoriche. Questultimo problema ci porterà ad illustrare la parametrizzazione razionale della circonferenza e ad accennare all'ultimo teorema di Fermat. Faremo inoltre richiami sullo studio locale di curve algebriche piane allo scopo di generalizzare il procedimento con cui si ottiene la parametrizzazione razionale della circonferenza ad altre curve.

1.1 La duplicazione del cubo

Oggetto del nostro studio saranno alcuni argomenti di Geometria Algebrica concreta. La parola geometria viene dal greco $\gamma\epsilon\omega\mu\epsilon\tau\rho\iota\alpha$ che signica misura della terra. Dunque le sue origini molto concrete sono fuori di ogni dubbio. Si parla di geometria "algebrica" quando si vogliono studiare oggetti geometrici per mezzo dell'algebra. Un primo esempio risale a circa il 1700 a.C.: una tavoletta Babilonese descrive un problema riguardante un rettangolo (che è un oggetto geometrico) con l'uso di *numeri NON conosciuti*.

I matematici greci studiarono il problema della **duplicazione del cubo**: costruire lo spigolo x di un cubo di volume x^3 doppio del volume a^3 di un cubo assegnato, ossia risolvere la

$$x^3 = 2a^3 \tag{1.1}$$

con strumenti quali *riga e compasso* (tradotto in termini di geometria analitica: tracciando solo rette e circonferenze). Il problema non è risolubile con riga e compasso in quanto $(x/a) = 2^{\frac{1}{3}}$ è un numero algebrico di grado

3 ossia non è di grado 2^h per qualche h. Mentre un numero complesso è "euclideo" o costruibile con riga e compasso solo se è algebrico di grado 2^h per h opportuno.

Nel V secolo avanti Cristo il problema era attualissimo in quanto si diceva che la pestilenza a Delo sarebbe cessata se si fosse raddoppiato l'altare che era a forma di cubo. La (1.1) si può riscrivere

$$x\frac{x^2}{a} = 2a^2 \tag{1.2}$$

e il problema, posto $y = \frac{x^2}{a}$ si riconduce a quello di trovare le coppie (x, y) che risolvono il sistema

$$\begin{cases} y = \frac{x^2}{a}, \\ xy = 2a^2. \end{cases}$$

Già Menecmo (nel 350 a.c.) considerò il luogo dei punti (x, y) che soddisfano tale sistema e riconobbe la prima curva come una parabola, la seconda come un'iperbole e trovò la soluzione del problema di duplicazione del cubo intersecando queste due coniche (l'ascissa positiva del punto di intersezione delle due coniche ci dà il lato del cubo di volume doppio). Questo è quindi un tipico problema di Geometria Algebrica.

Nel XVII secolo Cartesio e Pierre de Fermat studiarono le sezioni coniche e videro che i punti dei loro luoghi geometrici soddisfacevano le equazioni algebriche di secondo grado. Isac Newton studiò le equazioni di terzo grado e classificò i corrispondenti luoghi, le cubiche in 72 specie. Cartesio, Fermat e Newton hanno quindi il credito di aver iniziato lo studio delle curve algebriche piane.

Definizione 1.1.1 *Sia k un campo e siano $f_1, \ldots, f_s$ s polinomi a coefficienti in k. Si dice* **varietà affine** *definita da $f_1, \ldots, f_s$ l'insieme:*

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0, \ \forall\ 1 \leq i \leq s\}.$$

Dai tempi di Cartesio in poi l'oggetto della Geometria Algebrica è stato lo studio delle soluzioni di sistemi di equazioni polinomiali in più variabili ossia dei punti $x = (x_1, \ldots, x_n)$ tali che

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0. \end{cases}$$

ove gli f_i sono polinomi a coefficienti in un fissato campo k, ossia delle varietà affini.

In origine gli f_i erano polinomi a coefficienti nel campo $\mathbf{R}$ dei numeri reali e si cercavano le soluzioni reali (ossia in $\mathbf{R}$). Ma presto ci si rese conto che per avere l'opportunità che esistano soluzioni aveva senso includere la ricerca di soluzioni complesse. Ad esempio la $x^2 + y^2 = 0$ ha solo la soluzione $(0, 0)$ in $\mathbf{R}$ mentre in $\mathbf{C}$ ha per soluzione la conica spezzata $(x + iy)(x - iy) = 0$ costituita dalla coppia di rette *isotrope* per l'origine.

Si cercheranno poi soluzioni nel campo $\mathbf{Q}$ dei razionali per far vedere la stretta connessione con la *teoria dei numeri*. Infatti, uno dei problemi centrali della teoria dei numeri, il problema della ricerca delle soluzioni intere non banali di equazioni polinomiali a coefficienti interi, equivale sostanzialmente alla ricerca di punti a coordinate razionali su curve algebriche. Vedremo ciò nel prossimo paragrafo su un esempio storicamente molto importante. Precisamente: vedremo che la ricerca delle terne pitagoriche si riduce alla ricerca dei punti razionali sulla circonferenza del piano euclideo di centro l'origine e raggio 1. Questo ci porterà a fare una breve digressione su l'ultimo teorema di Fermat.

1.2 Terne pitagoriche e ultimo teorema di Fermat

Si consideri nello spazio euclideo $\mathbf{R}^2$ la circonferenza di equazione implicita:

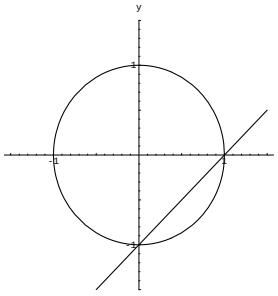
$$x^2 + y^2 = 1,$$

di cui una comune rappresentazione parametrica si ottiene sfruttando le funzioni trigonometriche :

$$\begin{cases} x = cos(t), \\ y = sin(t), \qquad 0 \leq t < 2\pi. \end{cases}$$

Per dare una parametrizzazione razionale fissiamo il punto $A = (0, -1)$ della circonferenza e consideriamo il fascio di rette passante per tale punto.

Ad ogni retta del fascio, diversa dalla tangente in A, corrisponde un unico punto della circonferenza diverso da A.



Precisamente, si ha una corrispondenza biunivoca α fra i punti della curva e le rette del fascio di centro A, che associa ad A la tangente in A alla curva, e ad ogni punto Q della circonferenza diverso da A la retta AQ del fascio. Si noti che tale corrispondenza è biunivoca in quanto l'inversa α^{-1} è quella corrispondenza tra le rette del fascio e la curva C tale che alla tangente in A alla circonferenza associa il punto A stesso di C, e ad ogni retta r passante per A del fascio e diversa dalla tangente fa corrispondere il punto diverso da A di $r \cap C$.

Sia $r_t : \ y + 1 = tx$ la retta di coefficiente direttore t del fascio di centro A. L'intersezione tra la retta r_t e la curva C è data dal sistema

$$\begin{cases} y = tx - 1, \\ x^2 + y^2 = 1, \end{cases}$$

da cui si ottiene l'equazione:

$$x[(1 + t^2)x - 2t] = 0.$$

Scartando la soluzione $x = 0$ corrispondente al punto $(0, -1)$ si ottiene il punto $(2t/(1 + t^2), (t^2 - 1)/(t^2 + 1))$ che al variare di $t \in \mathbf{R}$ descrive tutta la circonferenza ad eccezione del punto $A' = (0, 1)$ (che non è rappresentato in quanto le equazioni ridotte non rappresentano la retta $x = 0$ del fascio). La circonferenza ha la rappresentazione parametrica razionale

$$\begin{cases} x = \dfrac{2t}{1 + t^2}, \\ \\ y = \dfrac{t^2 - 1}{1 + t^2}, \qquad \forall\, t \in \mathbf{R}, \end{cases}$$

ed è ovviamente la più piccola varietà affine che contiene tali punti. Questo sopra descritto è un procedimento standard per trovare le equazioni

parametriche razionali di curve algebriche piane, come vedremo nel prossimo paragrafo.

Osservazioni.

1. L'esempio sopra descritto della parametrizzazione della circonferenza mostra molto bene lo stretto legame che esiste tra la *Geometria Algebrica* e la *Teoria dei Numeri*. Infatti, dal sistema:

$$\begin{cases} x = \dfrac{2t}{1+t^2}, \\ \\ y = \dfrac{t^2-1}{1+t^2}, \qquad \forall\, t \in \mathbf{R}, \end{cases}$$

per ogni $t \in \mathbf{Z}$ otteniamo un punto $Q = (p/q, r/s)$ a coordinate razionali su C. Si noti che l'esistenza del punto a coordinate razionali Q sulla circonferenza, implica che:

$$(p/q)^2 + (r/s)^2 = 1,$$

o equivalentemente:

$$(ps)^2 + (rq)^2 = (qs)^2.$$

Ciò risolve un tipico problema della teoria dei numeri: quello della ricerca delle soluzioni intere non banali dell'equazione a coefficienti interi (o diofantea): $X^2 + Y^2 = Z^2$.

I punti razionali di una curva ci permettono, dunque, di trovare soluzioni intere non banali di equazioni diofantee; infatti, siano (X, Y, Z) le coordinate omogenee associate ad x e y

$$\begin{cases} x = \frac{X}{Z}, \\ \\ y = \frac{Y}{Z}. \end{cases}$$

Se (l, m) sono i parametri direttori della retta di coefficiente direttore t si ha anche $t = \frac{m}{l}$. Sostituendo a x, y, t le loro espressioni in funzione di X, Y, Z, l, m nelle equazioni parametriche della circonferenza, si ottiene

$$\begin{cases} \dfrac{X}{Z} = \dfrac{\frac{2m}{l}}{\frac{l^2+m^2}{l^2}} = \dfrac{2ml}{l^2+m^2}, \\ \\ \dfrac{Y}{Z} = \dfrac{\frac{m^2-l^2}{l^2}}{\frac{m^2+l^2}{l^2}} = \dfrac{m^2-l^2}{m^2+l^2}, \end{cases}$$

da cui:

$$\begin{cases} X = 2ml, \\ Y = m^2 - l^2, \\ Z = m^2 + l^2, \end{cases}$$

cha dà tutte le soluzioni intere non banali, con $Z > 0$ e X pari dell'equazione diofantea $X^2 + Y^2 = Z^2$. Le terne (X, Y, Z) si dicono anche *terne pitagoriche* in quanto interpretate X e Y come lunghezze dei cateti e Z come lunghezza dell'ipotenusa di un triangolo rettangolo la $X^2 + Y^2 = Z^2$ esprime il Teorema di Pitagora.

2. Abbiamo trovato infinite soluzioni intere non banali dell'equazione

$$X^n + Y^n = Z^n,$$

nel caso particolare $n = 2$. È facile vedere che esistono infinite soluzioni intere non banali anche nel caso $n = 1$ dell'equazione diofantea $X + Y = Z$ (la retta $x + y = 1$ ha infatti infiniti punti razionali).

Per $n \geq 3$ si ha invece il teorema enunciato da Fermat nel 1637, e noto come l'*Ultimo Teorema di Fermat*, secondo cui l'equazione

$$X^n + Y^n = Z^n \qquad n \geq 3$$

non ammette soluzioni intere non banali.

Fermat scrisse l'enunciato di tale teorema nel margine di un libro di matematica con il commento "Ho scoperto una dimostrazione davvero notevole, che questo margine è troppo piccolo per contenere". Fermat poi non trovò mai posto per scrivere la dimostrazione generale, ma scrisse il caso $n = 4$.

Si noti come la condizione $n \geq 3$ possa essere sostituita dalla condizione $p \geq 3$, con p numero primo. Sia infatti $n = hp$ con p primo dispari. Allora l'equazione:

$$X^n + Y^n = Z^n,$$

si può riscrivere come:

$$X^{hp} + Y^{hp} = Z^{hp},$$

e se, per assurdo, tale equazione avesse una soluzione $(a, b, c) \neq (0, 0, 0)$ si avrebbe:

$$a^{hp} + b^{hp} = c^{hp},$$

e pertanto (a^h, b^h, c^h) risulterebbe soluzione intera non banale di $X^p + Y^p = Z^p$, in contraddizione con l'ipotesi che il teorema di Fermat valga per $n = p$ con $p \geq 3$ primo. Con un ragionamento simile si può dimostrare che se l'equazione avesse soluzioni per $n = 2^h$ con $h \geq 2$ anche l'equazione ottenibile per $n = 4$ dovrebbe averne, il che è assurdo, per quanto già dimostrato da Fermat.

Cento anni dopo Fermat, il matematico svizzero *Leonardo Eulero* eliminò il caso $n = 3$. Nel 1820 e 1830 il teorema fu provato per $n = 5, 7$.

La teoria fece poi passi da gigante per opera del matematico *E.E. Kummer*, cui si deve la teoria di Kummer, che divide i numeri primi in primi regolari e irregolari, e stabilisce l'ultimo teorema di Fermat per i primi regolari (che sembrano più frequenti di quelli irregolari, costituendo il 60% di tutti i primi). Ma, ironicamente, mentre si può dimostrare facilmente che i primi irregolari sono infiniti, non è mai stato dimostrato che i primi regolari lo sono (anche se questo è sicuramente vero).

Più tardi alcuni miglioramenti alla teoria di Kummer resero possibile studiare separatamente i primi irregolari, caso per caso, riducendo lo studio per vedere se il teorema di Fermat è vero ad un calcolo diretto ma lunghissimo, che sembra fatto a posta per i moderni calcolatori. Usando questi miglioramenti della teoria di Kummer vari ricercatori tra il 1970 e il 1993 hanno verificato che il teorema è vero per primi fino a 4.000.000. Estendere oltre il risultato è certamente possibile, ma farlo per questa strada richiederebbe nuove tecniche computazionali. Ciò non sarà necessario in quanto un ricercatore di teoria dei numeri Andrew Wiles nel settembre del 1994 ha completamente dimostrato il teorema, utilizzando comunque tecniche della teoria delle curve ellittiche che ai tempi di Fermat non esistevano ancora.

1.3 Richiami sulle curve algebriche piane

Scopo di questo paragrafo è mostrare come il procedimento utilizzato per dare la parametrizzazione razionale della circonferenza, si possa generalizzare a curve algebriche piane di ordine $n > 2$. Avremo bisogno, per questo scopo, di alcuni richiami.

Si consideri il piano affine reale $\mathbf{R}^2$, ampliato con gli elementi all'infinito e complessificato (si aggiungano cioè gli eventuali punti a coordinate complesse, considerando però sempre equazioni a coefficienti reali e sistemi di

riferimento reali). Indicheremo con $f(x,y) \in \mathbf{R}[x,y]$ un polinomio di grado n, con $C^n = \mathcal{V}(f(x,y))$ una curva algebrica di ordine n (o, meglio, la sua parte affine), con $P_0 = (x_0, y_0)$ un punto fissato di $\mathbf{R}^2$ e, infine, con r una retta del piano, di parametri direttori (l,m) passante per P_0 e non tutta contenuta in C^n. Si ha la seguente:

Definizione 1.3.1 *Si dice* **molteplicità di intersezione**, $\mu_{r\cap C}(P_0)$, *di una retta r con la curva C^n nel punto P_0 la molteplicità algebrica della soluzione $t = 0$, corrispondente al punto P_0, nell'equazione*

$$f(x_0 + lt, y_0 + mt) = 0,$$

risolvente il sistema

$$\begin{cases} x = x_0 + lt, \\ y = y_0 + mt, \\ f(x,y) = 0, \end{cases}$$

dato dalle equazioni della r e della C^n.

Osserviamo che $f(x_0+lt, y_0+mt)$, per ogni fissato (l,m), è un polinomio in t di grado positivo (poiché $P_0 \in C^n$) e, in generale, $\leq n$. Precisamente: avrà grado esattamente n, se la retta r è "generica" nel senso che il suo punto all'infinito di coordinate $(Z,X,Y) = (0,1,t)$ non soddisfa l'equazione omogenea $F(Z,X,Y) = Z^n f(X/Z, Y/Z) = 0$ della curva, ossia, non è un punto all'infinito della curva; avrà grado $n-h > 0$ se la curva passa per P_∞ con molteplicità h. Nel caso in cui r sia "generica", nel senso sopra precisato, l'equazione risolvente il sistema ha, per il teorema fondamentale dell'algebra, nel piano complessificato, esattamente n soluzioni da contare con la dovuta molteplicità. Questo sarà utile presto nella dimostrazione della Proposizione che ci darà il significato geometrico dell'ordine di $C^n = \mathcal{V}(f(x,y))$.

Un'ulteriore osservazione che, forse, andava fatta immediatamente è che tale definizione sembra dipendere sia dal sistema di riferimento scelto nel piano sia dalla parametrizzazione scelta per la retta. Si può dimostrare, tuttavia, che la molteplicità di intersezione (che è ovviamente 0 se $P_0 \notin r \cap C^n$) dipende solo dalla retta r, dalla curva C^n e dal punto P_0, e non dalla scelta del riferimento nel piano $\mathbf{R}^2$ o dalla scelta della parametrizzazione della retta r (ciò si può prevedere essendo ogni cambiamento del sistema di riferimento di primo grado).

La definizione di molteplicità di intersezione è quindi ben posta e da tale definizione, e dal teorema fondamentale dell'algebra segue subito la seguente:

Proposizione 1.3.1 *Sia $f(x,y) \in \mathbf{R}[x,y]$ un polinomio di grado n. L'ordine n di una curva algebrica C^n di equazione*

$$f(x,y) = 0,$$

ha il significato **geometrico***, di numero di punti, eventualmente contati con la dovuta molteplicità, comuni alla curva C^n e ad una retta generica r del piano non tutta contenuta in C^n.*

Se la curva è solo affine, si deve intendere il termine retta "generica" nel senso sopra precisato.

Definizione 1.3.2 *Sia P_0 un punto appartenente ad una curva algebrica piana C^n di ordine n definita dall'equazione $f(x,y) = 0$. P_0 si dice* **semplice** *per C^n se sono verificate le seguenti condizioni:*

1. *Ogni retta passante per P_0 è tale che $\mu_{r\cap C}(P_0) \geq 1$.*
2. *Esiste almeno una retta $\bar{r}$ passante per P_0 per cui $\mu_{\bar{r}\cap C}(P_0) = 1$.*

Dimostreremo ora il seguente teorema che caratterizza la retta tangente in un punto semplice di una C^n.

Teorema 1.3.1 *Se P_0 è un punto semplice di $C^n = \mathcal{V}(f(x,y))$, nel fascio di rette di centro P_0 esiste un'unica retta, detta tangente in P_0 alla C^n, avente molteplicità di intersezione maggiore o uguale a 2 con la C^n in P_0. Tale retta ha equazione*

$$\frac{\partial f}{\partial x}(P_0)(x - x_0) + \frac{\partial f}{\partial y}(P_0)(y - y_0) = 0,$$

ottenuta annullando i termini di grado minimo nello sviluppo di Taylor del polinomio $f(x,y)$ di punto iniziale P_0. Tutte le altre rette r passanti per P_0 diverse dalla tangente hanno molteplicità d'intersezione con la C^n in P_0 esattamente 1*.*

Dimostrazione. La generica retta r del fascio passante per P_0 ha equazioni:

$$\begin{cases} x = x_0 + lt, \\ y = y_0 + mt, \end{cases} \tag{1.3}$$

e la sua intersezione con la curva C^n è data dalle soluzioni del sistema:

$$\begin{cases} f(x,y) = 0, \\ x = x_0 + lt, \\ y = y_0 + mt, \end{cases}$$

la cui equazione risolvente è :

$$f(x_0 + lt, y_0 + mt) = 0.$$

Sviluppando $f(x, y)$ in formula di Taylor con punto iniziale P_0, si ha:

$$\begin{aligned} f(x,y) &= f(x_0,y_0) + [f_x^0(x-x_0) + f_y^0(y-y_0)] + \\ &+ \frac{1}{2!}[f_{xx}^0(x-x_0)^2 + 2f_{xy}^0(x-x_0)(y-y_0) + f_{yy}^0(y-y_0)^2] + \\ &+ \ldots + \frac{1}{n!}\{\frac{\partial f}{\partial x}(x-x_0) + \frac{\partial f}{\partial y}(y-y_0)\}_0^n, \end{aligned}$$

ove si è indicato con f_x^0 la derivata di f rispetto ad x calcolata nel punto P_0. e l'esponente n che figura nell'ultimo termine sta ad indicare una potenza simbolica n-esima del binomio che, quando agisce sull'operatore di derivazione ha il significato di derivata parziale n-esima.

Per ipotesi P_0 appartiene a C^n, quindi $f(x_0, y_0) = 0$. Inoltre dall'equazione della retta segue: $lt = x - x_0$, $mt = y - y_0$. L'equazione risolvente il sistema diventa quindi:

$$\begin{aligned} f(x_0 + lt, y_0 + mt) &= [f_x^0 l + f_y^0 m]t + \frac{1}{2!}[f_{xx}^0 l^2 + +2f_{xy}^0 lm + \\ &+ f_{yy}^0 m^2]t^2 + \ldots + \frac{1}{n!}\{\frac{\partial f}{\partial x}l + \frac{\partial f}{\partial y}m\}_0^n t^n. \end{aligned}$$

La soluzione $t = 0$ ha molteplicità algebrica esattamente 1 se e soltanto se è possibile mettere in evidenza t ma non t^2, ossia il coefficiente di t non è identicamente nullo. Poiché P_0 è semplice l'esistenza di una retta $\bar{r}$ passante per P_0 per cui $\mu_{\bar{r}\cap C}(P_0) = 1$ ci dice

$$f_x^0 \bar{l} + f_y^0 \bar{m} \neq 0.$$

Ne segue che $(f_x^0, f_y^0) \neq (0, 0)$, ossia in P_0 non si annullano simultaneamente le derivate prime (**condizione analitica** affinché un punto sia semplice). Ma allora, per valori generici di l e m

$$f_x^0 l + f_y^0 m \not\equiv 0,$$

e quindi il primo membro è un polinomio di primo grado in l e m e, come tale, ha un'unica radice. Esiste quindi un'unica retta i cui parametri direttori (l, m) soddisfano l'equazione

$$f_x^0 l + f_y^0 m = 0,$$

per la quale, nell'equazione risolvente il sistema si potrà mettere in evidenza almeno t^2; quindi tale retta avrà molteplicità di intersezione ≥ 2. Essendo (l, m) proporzionale secondo il fattore $1/t$ a $(x - x_0, y - y_0)$, tale retta, che dicesi *tangente* in P_0 a C^n, avrà equazione

$$f_x^0(x - x_0) + f_y^0(y - y_0) = 0.$$

Resta così anche dimostrato che P_0 è un punto semplice per C^n se e soltanto se $f(x_0, y_0) = 0$ e $(f_x^0, f_y^0) \neq (0, 0)$, (o anche se e solo se lo sviluppo di Taylor di punto iniziale P_0 ha termini di grado minimo 1) ossia se e soltanto se è un punto di C^n in cui esiste la retta tangente (la cui equazione si otttiene annullando tali termini di grado minimo 1 nello sviluppo di Tailor) in P_0 alla C^n ∎

Definizione 1.3.3 *Un punto P_0 si dice* **doppio** *per la curva algebrica $C^n = \mathcal{V}(f(x, y))$ se sono verificate le seguenti condizioni:*

1. *Ogni retta passante per P_0 di parametri direttori (l, m) è tale che: $\mu_{r_{(l,m)} \cap C}(P_0) \geq 2$.*
2. *Esiste almeno una retta $\bar{r}$ del fascio, passante per P_0 e di parametri direttori $(\bar{l}, \bar{m})$, per cui si ha: $\mu_{r_{(\bar{l},\bar{m})} \cap C}(P_0) = 2$.*

Come nel corso della dimostrazione del Teorema precedente si prova che P_0 è un punto doppio per C^n se e soltanto se:

- $f_x^0 l + f_y^0 m = 0$ per ogni coppia (l, m), ossia $(f_x^0, f_y^0) = (0, 0)$.
- Esiste almeno una coppia $(\bar{l}, \bar{m})$ per cui si ha:

$$f_{xx}^0 \bar{l}^2 + 2 f_{xy}^0 \bar{l}\bar{m} + f_{yy}^0 \bar{m}^2 \neq 0.$$

Ne segue che $f_{xx}^0 l^2 + 2 f_{xy}^0 lm + f_{yy}^0 m^2$ non è identicamente nullo, ed essendo quest'ultimo un polinomio di secondo grado in (l, m), ha esattamente due radici in $\mathbf{C}$ che corrispondono ai parametri direttori delle uniche due rette del fascio di centro P_0 aventi molteplicità di intersezione ≥ 3. Queste due rette ovviamente possono essere: reali distinte, reali coincidenti o complesse coniugate, in corrispondenza il punto doppio si dirà, rispettivamente *nodo, cuspide, punto doppio isolato.* Resta così dimostrato il seguente:

Teorema 1.3.2 *Se P_0 è un punto doppio per C^n allora tutte le rette del fascio, escluse le due rette di parametri direttori verificanti:*

$$f_{xx}^0 l^2 + 2 f_{xy}^0 lm + f_{yy}^0 m^2 = 0, \tag{1.4}$$

hanno molteplicità d'intersezione $\mu_{r\cap C}(P_0) = 2$.
Le due rette verificanti (1.4), per cui la $\mu_{r\cap C}(P_0) \geq 3$ *si chiamano* **tangenti principali** *alla curva nel punto doppio.*

La **condizione analitica** affinché un punto P_0 sia doppio è che siano tutte nulle le derivate prime di f in P_0, ma che non si annullino tutte le derivate seconde. Lo sviluppo di Taylor di punto iniziale P_0 ha quindi termini di grado minimo 2 e annullando tali termini si ottiene l'equazione complessiva delle due tangenti principali al punto doppio. Più in generale si ha:

Definizione 1.3.4 *Un punto* P_0 *si dice* $s-plo$ *(o di molteplicità* s*) per* C^n *se sono verificate le seguenti condizioni:*

1. *Ogni retta* r *passante per* P_0 *di parametri direttori* (l, m) *è tale che* $\mu_{r_{(l,m)}\cap C}(P_0) \geq s$.
2. *Esiste almeno una retta* $\bar{r}$ *del fascio passante per* P_0 *e di parametri direttori* $(\bar{l}, \bar{m})$ *per cui si ha:* $\mu_{r_{(\bar{l},\bar{m})}\cap C}(P_0) = s$.

Come si è visto nel caso $s = 2$, si ha in generale che tutte le rette per P_0, escluse le s rette i cui parametri direttori soddisfano la

$$\{\frac{\partial f}{\partial x}l + \frac{\partial f}{\partial y}m\}_0^s = 0,$$

che si dicono **tangenti principali** nel punto $s - plo$, hanno molteplicità d'intersezione con la curva C^n in P_0 uguale ad s, ossia $\mu_{r\cap C}(P_0) = s$.

La **condizione analitica** affinché un punto P_0 sia $s - plo$ è che siano nulle tutte le derivate in P_0 fino all'ordine $(s-1)$, ma non tutte nulle quelle di ordine s. Inoltre se P_0 è un punto $s - plo$ l'equazione:

$$\{\frac{\partial f}{\partial x}(x - x_0) + \frac{\partial f}{\partial y}(y - y_0)\}_0^s = 0,$$

ottenuta annullando i termini di grado minimo nello sviluppo di Taylor è l'equazione complessiva delle s tangenti principali in P_0; rappresenta, infatti, una curva algebrica di ordine s che si spezza nelle s tangenti principali.

Osservazione Lo sviluppo di Taylor di centro $P_0 = (x_0, y_0)$ di un polinomio si ottiene effettuando le sostituzioni:

$$\begin{cases} x = x_0 + (x - x_0), \\ y = y_0 + (y - y_0), \end{cases}$$

e poi ordinando rispetto a $(x - x_0)$ e $(y - y_0)$. In particolare, nel caso in cui $P_0 \equiv O = (0, 0)$, lo sviluppo di Taylor del polinomio è il polinomio stesso. Ne segue che se il polinomio $f = f(x, y)$ è privo di termine noto, la curva $C = \mathcal{V}(f)$ passa per l'origine O; se f ha termini di grado minimo $s \geq 1$ l'origine è un punto s-plo e l'equazione complessiva delle s tangenti principali nel punto s-plo O si ottiene annullando il complesso dei termini di grado minimo.

Esempi

- Consideriamo la cubica:

$$y^3 - 3x^2 = 0.$$

  Si chiede di studiare la natura dell'origine $O = (0, 0)$ e di determinare equazioni parametriche razionali.

I termini di grado minimo del polinomio in questione sono quelli di secondo grado, quindi $O = (0, 0)$ è un punto doppio e le tangenti principali hanno equazione complessiva $3x^2 = 0$ (ossia sono due reali e coincidenti con l'asse delle y doppio e il punto è pertanto una cuspide). Per parametrizzare tale curva, osserviamo che ogni retta per O ha con la curva due intersezioni assorbite in O, trattandosi di una cubica, una tale retta ha dunque un un'unico punto di intersezione distinto da O con la cubica. Similmente a quanto fatto per determinare le equazioni parametriche della circonferenza, intersechiamo la cubica con il fascio di rette di centro O, ovvero consideriamo il sistema:

$$\begin{cases} y^3 - 3x^2 = 0, \\ y = tx, \end{cases}$$

la cui equazione risolvente è :

$$t^3x^3 - 3x^2 = x^2(t^3x - 3) = 0.$$

Scartando la soluzione (di molteplicità 2) $x = 0$ corrispondente all'origine, si ottiene l'ascissa dell'unico ulteriore punto di intersezione distinto da O. Sostituendo tale ascissa nella $y = tx$ si hanno per la cubica le equazioni parametriche razionali:

$$\begin{cases} x = \dfrac{3}{t^3}, \\ \\ y = \dfrac{3}{t^2}. \end{cases}$$

- Studiamo ora la quartica:

$$x^4 - x^3 + xy^2 = 0,$$

nell'origine $O = (0, 0)$.

Per quanto osservato sopra, lo sviluppo di Taylor del polinomio nell'origine è il polinomio stesso. I termini di grado minimo sono quelli di terzo grado, quindi $O = (0, 0)$ è un punto triplo e l'equazione complessiva delle tangenti principali è

$$xy^2 - x^3 = x(y - x)(y + x) = 0.$$

Pertanto, le tre tangenti principali sono le rette

$$x = 0, \qquad y = x, \qquad y = -x.$$

Una generica retta per O avrà con la curva oltre alle tre intersezioni assorbite in O, solo un'ulteriore intersezione (trattandosi di una quartica). Per parametrizzare tale curva possiamo quindi ragionare analogamente a quanto fatto sia per la circonferenza che per la cubica dell'esempio precedente. Precisamente, intersecando con la generica retta per O si ha il sistema:

$$\begin{cases} x^4 - x^3 + xy^2 = 0, \\ y = tx, \end{cases}$$

la cui equazione risolvente è :

$$x^3(x - 1 + t^2) = 0$$

Scartando la soluzione tripla $x = 0$ corrispondente all'origine, si ottiene l'ascissa $x = 1 - t^2$ dell'ulteriore punto di intersezione della retta $y = tx$ con la quartica. Sostituendo tale espressione nella $y = tx$ si hanno le equazioni parametriche razionali della curva:

$$\begin{cases} x = 1 - t^2, \\ y = t - t^3. \end{cases}$$

I due esempi generalizzano ad una cubica con un punto doppio e ad una quartica con un punto triplo il procedimento con cui abbiamo ottenuto la parametrizzazione razionale della circonferenza (che ha ordine 2 e in cui ogni punto è semplice). Tenendo presente il significato geometrico dell'ordine e la definizione di punto $(n - 1)$-plo, possiamo generalizzare il procedimento alle C^n con $n \geq 2$.

Teorema 1.3.3 *Una curva algebrica C^n con un punto $(n-1)-plo$ è razionale, ossia: ha equazioni parametriche razionali..*

Dimostrazione. Sia $P_0 = (x_0, y_0)$ il punto $(n-1)$-plo di C^n. Sviluppando in formula di Taylor di punto iniziale P_0, la equazione della curva si scrive nella forma

$$f(x,y) = \phi_n(x - x_0, y - y_0) + \phi_{n-1}(x - x_0, y - y_0) = 0,$$

dove $\phi_n(x-x_0, y-y_0)$ è la parte omogenea di grado n mentre $\phi_{n-1}(x-x_0, y-y_0)$ è la parte omogenea di grado $(n-1)$. Per quanto visto precedentemente $\phi_{n-1}(x - x_0, y - y_0) = 0$ è l'equazione complessiva delle $(n-1)$ tangenti principali in $P_0 = (x_0, y_0)$.

Per trovare una parametrizzazione razionale, studiamo l'intersezione tra la curva C^n e la generica retta del fascio passante per P_0:

$$\begin{cases} \phi_n(x - x_0, y - y_0) + \phi_{n-1}(x - x_0, y - y_0) = 0, \\ y - y_0 = t(x - x_0). \end{cases}$$

L'equazione risolvente tale sistema è:

$$\phi_n(x - x_0, t(x - x_0)) + \phi_{n-1}(x - x_0, t(x - x_0)) = 0.$$

Ricordiamo che una funzione $g(x,y)$ omogenea di grado α soddisfa per ogni t la

$$g(tx, ty) = t^\alpha g(x, y).$$

Essendo ϕ_n e ϕ_{n-1} due funzioni omogenee rispettivamente di grado n e $n-1$, si avrà

$$(x - x_0)^n \phi_n(1, t) + (x - x_0)^{n-1} \phi_{n-1}(1, t) = 0.$$

Mettendo in evidenza il termine $(x - x_0)^{n-1}$ si ottiene pertanto

$$(x - x_0)^{n-1}[(x - x_0)\phi_n(1, t) + \phi_{n-1}(1, t)] = 0.$$

Scartando la soluzione $(n-1)$-pla $(x = x_0)$ corrispondente al punto $(n-1)$-plo P_0, si ha l'ascissa dell'ulteriore punto Q_t di intersezione tra la retta r_t e la curva. Sostituendo nella $y - y_0 = t(x - x_0)$ si ha per la curva la parametrizzazione razionale:

$$\begin{cases} x = x_0 - \dfrac{\phi_{n-1}(1, t)}{\phi_n(1, t)}, \\ \\ y = y_0 - \dfrac{t\phi_{n-1}(1, t)}{\phi_n(1, t)}. \end{cases}$$

Come nel caso della circonferenza, non è detto che la parametrizzazione riempia tutta la varietà; non è infatti rappresentato il punto di intersezione con la retta $x = x_0$. ∎

Capitolo 2

Geometria, Algebra e Algoritmi

In questo capitolo si introducono i temi fondamentali del corso. Saremo interessati alla geometria delle *varietà affini*, che sono curve, superfici e oggetti di dimensione più alta definiti da equazioni polinomiali. Per questo scopo dovremo studiare gli *ideali* nell'anello dei polinomi $k[x_1, \ldots, x_n]$. Studieremo, in particolare, i polinomi in una variabile per poter illustrare il ruolo svolto dagli algoritmi.

2.1 Polinomi e Spazi Affini

Per collegare l'Algebra con la Geometria studieremo i polinomi a coefficienti in un campo. Utilizzeremo diversi campi a seconda degli scopi prefissati. I più comuni saranno:

- I numeri complessi $\mathbf{C}$, quando vorremo essere sicuri che un problema abbia soluzione.
- I numeri reali $\mathbf{R}$, per disegnare le varietà in dimensione 2 e 3.
- I numeri razionali $\mathbf{Q}$, più utili ad illustrare i collegamenti con la teoria dei numeri.
- I campi finiti, più adatti per fare un'implementazione sul computer. Ci riferiremo in particolare al campo fondamentale $\mathbf{Z}_p$ (con p primo ≥ 2) dei campi a caratteristica p, o, più in generale, al campo di Galois di ordine $q = p^h$ ottenuto a partire da $\mathbf{Z}_p$ aggiungendo le radici di un

polinomio $g(x)$ irriducibile su $\mathbf{Z}_p$ e di grado h, ovvero:

$$GF(q) = \frac{\mathbf{Z}_p}{(g(x))}$$

[cfr[15]].

Definizione 2.1.1 *Un* **monomio** *in $x_1, \ldots, x_n$ è un'espressione del tipo:*

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n},$$

dove tutti gli α_i sono interi non negativi. Il **grado totale** *di tale monomio è la somma $|\alpha| = \alpha_1 + \ldots + \alpha_n$.*

La notazione per i monomi verrà semplificata scrivendo

$$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n},$$

ove $\alpha = (\alpha_1, \ldots, \alpha_n)$ è una n-pla di interi non negativi, e se $\alpha = (0, \ldots, 0)$ si ha $x^\alpha = 1$. Con questa notazione il *grado totale* del monomio x^α sarà denotato con $|\alpha| = \alpha_1 + \ldots + \alpha_n$.
A partire dalla definizione di monomio, si può definire un *polinomio* come somma di monomi.

Definizione 2.1.2 *Un* **polinomio** *in $x_1, \ldots, x_n$ a coefficienti in un campo k è una combinazione lineare finita di monomi, ossia è del tipo*

$$f(x_1, \ldots, x_n) = \sum_\alpha a_\alpha x^\alpha, \qquad a_\alpha \in k,$$

ove $\alpha = (\alpha_1, \ldots, \alpha_n)$ varia in un insieme finito di n-ple di interi non negativi. L'insieme di tutti i polinomi a coefficienti in k si indica con $k[x_1, \ldots, x_n]$.

Se $n = 1$, $k[x] = \{f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0 \mid a_i \in k, a_m \neq 0\}$. L'intero m si dice grado del polinomio, l'elemento a_m si dice coefficiente direttore, e il termine $a_m x^m$ si indicherà con $LT(f)$ (Leading Term o termine direttore di f).

Nel caso generale ($n \geq 1$):

- Chiameremo a_α il **coefficiente** del monomio x^α.
- Se $a_\alpha \neq 0$ chiameremo $a_\alpha x^\alpha$ un **termine** di f.

- **Grado totale** di $f(x_1, \ldots, x_n)$ è definito come:

$$\partial f = \max_{a_\alpha \neq 0} \{ \mid \alpha \mid \}.$$

Useremo sempre le lettere f, g, h, p, q, r per indicare polinomi. Ad esempio il polinomio

$$3x^3y^2z + \frac{2}{3}x^4y^2 + 8xyz - 2y$$

è un polinomio in $\mathbf{Q}[x, y, z]$ che ha quattro termini e grado totale 6. Si noti che ci sono ben due termini di grado totale massimo 6, fatto che non può accadere per polinomi in una variabile. Per poter parlare anche nel caso di più variabili di termine direttore di F studieremo, nel prossimo Capitolo, come *ordinare* i termini di un polinomio.

Nell'anello $k[x_1, \ldots, x_n]$ si definiscono la somma e il prodotto fra polinomi con le regole usuali dell'algebra. Rispetto a tali operazioni $k[x_1, \ldots, x_n](+, \cdot)$ ha una struttura di anello commutativo dotato di unità e privo di divisori dello zero, o, come anche si dice, di *dominio*.

Così come dal dominio $\mathbf{Z}$ si costruisce il campo $\mathbf{Q}$ dei razionali:

$$\mathbf{Q} = \{ \frac{p}{q} \mid p, q \in \mathbf{Z},\ q \neq 0 \ e \ \frac{p}{q} = \frac{r}{s} \Leftrightarrow ps = qr \},$$

da ogni dominio si può costruire il campo dei quozienti. Con tale costruzione a partire dal dominio $k[x_1, \ldots, x_n]$ si ottiene il **campo dei quozienti polinomiali**:

$$\begin{aligned} k(x_1, \ldots, x_n) \quad = \quad & \{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x_1, \ldots, x_n], g(x) \neq 0 \ e \\ & \frac{f(x)}{g(x)} = \frac{f^1(x)}{g^1(x)} \Leftrightarrow f(x)g^1(x) = f^1(x)g(x) \}. \end{aligned}$$

Per i nostri scopi sarà sufficiente dare per lo spazio affine la seguente definizione.

Definizione 2.1.3 *Dato un campo k ed un intero positivo n, si dice* **spazio affine** *n-dimensionale l'insieme :*

$$k^n = \{ (a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k \}.$$

Ogni polinomio $f \in k[x_1, \ldots, x_n]$ individua una funzione polinomiale (che continueremo ad indicare con f):

$$f : k^n \longrightarrow k$$

che associa ad ogni elemento $a = (a_1, \ldots, a_n) \in k^n$ il valore $f(a) \in k$, che il polinomio $f(x)$ assume nel punto a.

Lo stesso discorso continua a valere se invece di f si considera il quoziente polinomiale $f(x)/g(x)$. Sia $W = \{a \in k^n \mid g(a) = 0\}$, si dice funzione *razionale* individuata da tale quoziente polinomiale l'applicazione

$$\frac{f}{g} : \ k^n - W \longrightarrow k$$

che associa ad ogni elemento $a = (a_1, \ldots, a_n) \in k^n - W$ l'elemento

$$f(a)/g(a) \in k.$$

Il campo delle funzioni razionali sarà indicato ancora con $k(x_1, \ldots, x_n)$.

Due polinomi $f, g \in k[x_1, \ldots, x_n]$ sono **uguali** se hanno i coefficienti tutti uguali, si dicono invece **identici** se individuano la stessa funzione polinomiale, ossia:

$$f(a) = g(a), \qquad \forall a \in k^n.$$

Ovviamente polinomi uguali individuano la stessa funzione polinomiale, difatti se $f = g$, allora f e g hanno gli stessi coefficienti e $f - g = \varphi = O_{k[x_1,\ldots,x_n]}$, da cui segue che $\varphi(a) = 0 \ \forall a \in k$, ossia $f(a) = g(a) \ \forall a \in k$. Il viceversa in generale non vale.

Se k è infinito vale il seguente **Principio d'identità dei polinomi**:

Proposizione 2.1.1 *Sia k un campo infinito ed $f \in k[x_1, \ldots, x_n]$. Allora f è lo zero dell'anello dei polinomi $f = O_{k[x_1,\ldots,x_n]}$ se e soltanto se la funzione polinomiale individuata da f è quella nulla:*

$$\begin{aligned} f : k^n &\longrightarrow k \\ a &\longrightarrow 0, \qquad \forall a \in k^n. \end{aligned}$$

Dimostrazione. ($\Rightarrow$) È ovvio che se $f = O_{k[x_1,\ldots,x_n]}$, allora $f(a) = 0 \ \forall a \in k^n$.
($\Leftarrow$) Si procede per induzione rispetto al numero n delle variabili.

Sia $n = 1$. Come dimostreremo nel paragrafo 2.4, un polinomio $f(x) = a_m x^m + \ldots + a_0$ di grado $m > 0$ ha al più m radici. Ora, se k è infinito e $f(a) = 0 \ \forall a \in k$, il polinomio f viene ad avere un numero infinito di radici, il che è assurdo se f ha grado positivo. L'unica possibilità è dunque che f sia lo zero dell'anello dei polinomi, ossia abbia coefficienti tutti nulli.

Sia $n \geq 2$. Per ipotesi induttiva assumiamo vera ($\Leftarrow$) per polinomi $g \in k[x_1, \ldots, x_{n-1}]$. Si osservi che, se abbiamo un polinomio in più variabili,

possiamo fissare la nostra attenzione su una di esse, ad esempio x_n, e considerare l'anello $k[x_1, \ldots, x_n] = A[x_n]$ come anello dei polinomi nell'unica variabile x_n, a coefficienti nell'anello $A = k[x_1, \ldots, x_{n-1}]$ dei polinomi nelle altre $n-1$ indeterminate. In altri termini si scrive:

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{\partial_{x_n} f} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

ove $\partial_{x_n} f$ è il grado, rispetto ad x_n, di f. Se $f : k^n \longrightarrow k$ è tale che $f(a) = 0,\ \forall a \in k^n$, dimostreremo che f ha coefficienti tutti uguali a zero, sfruttando l'ipotesi induttiva che sia vero per polinomi di grado $(n-1)$.

Infatti, fissato arbitrariamente $(a_1, \ldots, a_{n-1}) \in k^{n-1}$, il polinomio $\varphi(x_n) \in k[x_n]$, definito dalla:

$$\varphi(x_n) = f(a_1, \ldots, a_{n-1}, x_n) = \sum_{i=0}^{\partial_{x_n} f} g_i(a_1, \ldots, a_{n-1}) x_n^i$$

è tale che $\forall a\ \in k,\ \varphi(a) = f(a_1, \ldots, a_{n-1}, a) = 0$.

Poiché per $n = 1$ la proposizione è vera, sappiamo che $\varphi(x_n)$ ha coefficienti tutti nulli, quindi $\forall i = 1, \ldots, \partial_{x_n} f$, risulta $g_i(a_1, \ldots, a_{n-1}) = 0$. Essendo $(a_1, \ldots, a_{n-1})$ arbitrario in k^{n-1}, tutte le $g_i : k^{n-1} \longrightarrow k$ sono uguali alla funzione nulla.

L'ipotesi induttiva implica quindi che $g_i = O_{k[x_1,\ldots,x_{n-1}]}$, ossia per ogni i il polinomio g_i deve avere i coefficienti tutti nulli. Poiché tutti i coefficienti di g_i forniscono tutti i coefficienti di f si avrà che anche questi saranno a loro volta tutti nulli. ∎

L'ipotesi che k sia infinito è essenziale per la validità del teorema. Sia infatti $k = \mathbf{Z}_2 = \{0, 1\}$ e $f(x) = x^2 + x\ \in \mathbf{Z}_2[x]$. Si vede allora come, pur essendo $f(x) \neq O_{\mathbf{Z}_2[x]}$, si ha $f(0) = 0$ e $f(1) = 0$.

In generale si ha che se $k = GF(q)$ è un campo finito di ordine $q = p^h$ e $f : GF(q) \longrightarrow GF(q)$, allora f è la funzione polinomiale nulla se e solo se f è un multiplo del polinomio $g(x) = x^q - x = x(x^{q-1} - 1)$, come segue facilmente dal

Lemma 2.1.1 *Per ogni $a \in GF(q)$ vale l'identità $a^q = a$ e se $a \neq 0$ si ha $a^{q-1} = 1$.*

Dimostrazione. Il gruppo moltiplicativo $k - \{0\}$ è un gruppo di ordine $q - 1$. Sia $a \neq 0$ un arbitrario elemento di tale gruppo e sia $r = | < a > |$

il suo periodo (i.e. il minimo intero positivo tale che $a^r = 1$, che, come è noto dal corso di Algebra, coincide con l'ordine del sottogruppo ciclico $< a >$ generato da a). Dal teorema di Lagrange, [cfr[7]], segue subito che $q-1 = ir$ ove i è il numero delle classi laterali del sottogruppo $< a >$ quindi

$$a^{q-1} = a^{ir} = (a^r)^i = 1^i = 1.$$

Pertanto ogni elemento $a \in k - \{0\}$ soddisfa alla

$$a^{q-1} = 1.$$

Poiché banalmente lo zero soddisfa alla $a = 0$, si ha l'asserto. ∎

Se $a_0 = 0, a_1, \ldots, a_{q-1}$ sono i q elementi del campo finito si ha quindi che $g(x)$ ha su $GF(q)$ la fattorizzazione

$$g(x) = x(x - a_1) \cdot \ldots \cdot (x - a_{q-1}),$$

(infatti, come è noto e, comunque, richiameremo nel corso della dimostrazione del corollario 2.4.1, se α è radice di $g(x)$ necessariamente $(x - \alpha)$ divide $g(x)$). Ogni polinomio $f(x) \in GF(q)[x]$ che individui la funzione polinomiale nulla ammetterà le q radici distinte $a_0 = 0, a_1, \ldots, a_{q-1}$, e pertanto sarà divisibile per $g(x)$. Viceversa è ovvio che, se il polinomio f è multiplo di $g(x)$, risulta $f(a) = 0 \ \forall a \in GF(q)$.
Concludiamo questo paragrafo ricordando la proprietà che caratterizza il campo $\mathbf{C}$.

Teorema 2.1.1 (Teorema fondamentale dell'algebra) *Ogni polinomio $f(z)$ di $\mathbf{C}[z]$ di grado strettamente maggiore di zero ha almeno una radice in $\mathbf{C}$.*

Dimostrazione. Supponiamo per assurdo che $f(z)$ non ammetta radici in $\mathbf{C}$, ossia $f(z) \neq 0 \ \forall z \in \mathbf{C}$. In questa ipotesi $1/f(z)$ è una funzione olomorfa sull'intero piano della variabile complessa, o come anche si dice una funzione trascendente intera. Ovviamente il $\lim_{z\to\infty} 1/f(z) = 0$; ne segue facilmente che esiste una costante $M > 0$ tale che $|1/f(z)| < M$. Per il teorema di Liouville, ogni funzione trascendente intera limitata in modulo è costante, ma allora anche $f(z)$ dovrebbe essere costante, contro l'ipotesi che il grado di f è strettamente maggiore di zero. ∎

Ricordiamo che un campo k si dice *algebricamente chiuso* se vale in $k[x]$ il Teorema fondamentale dell'algebra ossia se ogni polinomio non costante ha almeno una radice in k.

2.2 Varietà Affini e Parametrizzazioni

Definizione 2.2.1 *Sia k un campo e siano $f_1, \ldots, f_s$ s polinomi in $k[x_1, \ldots, x_n]$. Si dice* **varietà affine** *definita da $f_1, \ldots, f_s$ l'insieme:*

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0, \ \forall\ 1 \leq i \leq s\}.$$

In altri termini, una varietà affine $\mathcal{V}(f_1, \ldots, f_s) \subset k^n$ è l'insieme di tutte le soluzioni del sistema:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ f_s(x_1, \ldots, x_n) = 0. \end{cases}$$

Esempio: Si consideri un sistema di m equazioni lineari in n incognite $x_1, \ldots, x_n$ a coefficienti in un campo k:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m. \end{cases}$$

L'insieme delle soluzioni di questo sistema è una varietà affine V in k^n, che chiameremo *varietà lineare*. Come è noto dal corso di Algebra lineare la sua **dimensione** è $n - r$, dove r è il rango della matrice dei coefficienti del sistema, ovvero il numero di equazioni linearmente indipendenti. Descriviamo ora alcune proprietà delle varietà affini.

Proposizione 2.2.1 *Se $V, W \subset k^n$ sono varietà affini, allora $V \cap W$ e $V \cup W$ sono anch'esse varietà affini.*

Dimostrazione. Se $V = \mathcal{V}(f_1, \ldots, f_s)$ e $W = \mathcal{V}(g_1, \ldots, g_t)$, si ha precisamente che

$$V \cap W = \mathcal{V}(f_1, \ldots, f_s, g_1, \ldots, g_t), \tag{2.1}$$
$$V \cup W = \mathcal{V}(f_i g_j \mid 1 \leq i \leq s, \ 1 \leq j \leq t). \tag{2.2}$$

La (2.1) segue banalmente dal fatto che in $V \cap W$ sia $f_1, \ldots, f_s$ che $g_1, \ldots, g_t$ si devono annullare, ovvero devono annullarsi simultaneamente tutte le $f_1, \ldots, f_s$, $g_1 \ldots, g_t$.

Dimostriamo ora la (2.2). Sia $a = (a_1, \ldots, a_n) \in V \cup W$. Se $a \in V$, tutte le f_i si annullano in a, per cui anche tutte le $f_i g_j$ si annulleranno in

tal punto e quindi $V \subset \mathcal{V}(f_i g_j)$. Similmente si vede che se $a \in W$, risulta necessariamente $W \subset \mathcal{V}(f_i g_j)$. Pertanto, $V \cup W \subset \mathcal{V}(f_i g_j)$.

Per dimostrare l'inclusione opposta consideriamo un punto b di $\mathcal{V}(f_i g_j)$ e supponiamo che sia $f_\alpha(b) \neq 0$ per qualche α (ossia $b \notin V$, altrimenti non c'è niente da dimostrare). Il fatto che $f_\alpha g_j$ si annulla in b per ogni j, ma $f_\alpha(b) \neq 0$ implica che tutti i g_j devono annullarsi in b, e quindi $b \in W \subset V \cup W$. ∎

Da questa proposizione segue che unioni ed intersezioni finite di varietà affini sono ancora varietà affini. Ovviamente $\mathcal{V}(0) = k^n$ e, ad esempio $\mathcal{V}(x, x-1) = \emptyset$ (in generale sarà vuota la varietà luogo degli zeri di un qualunque sistema incompatibile di equazioni polinomiali). Sarà uno dei nostri scopi quello di far vedere che le varietà affini sono i chiusi di una topologia di k^n, la cosidetta "Topologia di Zariski". A tale scopo resta solo da dimostrare che intersezioni qualsiansi di varietà affini sono varietà affini e questo seguirà dal Teorema della base di Hilbert.

Siano $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$, i problemi che si presentano nello studio delle varietà affini sono:

- il problema della **Compatibilità** del sistema, che consiste nello stabilire quando risulta $\mathcal{V}(f_i) \neq \emptyset$.
- il problema della **Finitezza**, ossia di determinare esplicitamente le soluzioni del sistema, cioè i punti di $V = \mathcal{V}(f_1, \ldots, f_s)$ e vedere se sono o meno in numero finito. Questo problema consiste sostanzialmente nel determinare le equazioni parametriche esplicite di V:

$$\begin{cases} x_1 = r_1(t_1, \ldots, t_m), \\ \vdots \\ x_n = r_n(t_1, \ldots, t_m). \end{cases}$$

- determinare la **Dimensione** di $\mathcal{V}(f_1, \ldots, f_s)$.

Osservazioni

1. La nozione intuitiva di dimensione (data dalla dimensione dello spazio ambiente meno il numero delle equazioni indipendenti) andrà modificata come mostra l'esempio della varietà di $\mathbf{R}^3$ data dall'unione fra l'asse z ($\mathcal{V}(x, y)$) e il piano (x, y) ($\mathcal{V}(z)$):

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

Dalla Proposizione precedente segue che tale unione è ancora una varietà affine, ottenuta tuttavia unendo una curva (asse z) ed una superficie (piano (x, y)), ossia un pezzo di dimensione intuitivamente 1 con un pezzo che intuitivamente ha dimensione 2.

2. La differenza di due varietà affini non sempre è una varietà affine.

   - Si consideri ad esempio in $\mathbf{R}^2$ la retta $y = x$ cui togliamo il punto $(1, 1)$:

     $$X = \{(x, x) \mid x \in \mathbf{R}, x \neq 1\} = \mathcal{V}(x - y) - \mathcal{V}(x - 1, y - 1).$$

     Se X fosse una varietà affine, dovrebbe essere del tipo:

     $$X = \mathcal{V}(f_1, \ldots, f_s) = \{a \in \mathbf{R}^2 \mid f_i(a) = 0, \forall\, i = 1, \ldots, s\}.$$

     Dovrebbero pertanto esistere s polinomi $\varphi_i(x) = f_i(x, x)$, nella variabile x e di gradi rispettivi n_i, che si annullano per ogni $x \neq 1$. Poiché il campo $k = \mathbf{R}$ è infinito e tali polinomi ammettono un numero di radici superiore al grado si ha che sono identicamente nulli, e pertanto anche $\varphi_i(1) = 0$. In altri termini: ogni polinomio che si annulla su tutti i punti di X deve necessariamente annullarsi anche in $(1, 1)$. Ne segue che non possono esistere s polinomi tali che $X = \mathcal{V}(f_1, \ldots, f_s)$. Questo è un particolare esempio di *retta bucata*, ma lo stesso discorso vale per qualsiasi altra retta privata di un suo punto.

3. Risulta, invece, una varietà affine il **prodotto cartesiano** di due varietà affini

   $$V = \mathcal{V}(f_1, \ldots, f_s), \quad f_i \in k[x_1, \ldots, x_n], \quad V \subseteq k^n,$$

   $$W = \mathcal{V}(g_1, \ldots, g_t), \quad g_j \in k[y_1, \ldots, y_m], \quad W \subseteq k^m.$$

   Precisamente:

   $$V \times W = \{(a, b) \mid a \in V,\ b \in W\} \subseteq k^{n+m}.$$

   In altre parole, se $x \in k^n$ e $y \in k^m$ la varietà prodotto $V \times W$ è definita come l'insieme dei punti $(x, y) \in k^{n+m}$ che, con le loro coordinate risolvono il sistema:

   $$\begin{cases} f_i(x) = 0, & i = 1, \ldots, s, \\ g_j(y) = 0, & j = 1, \ldots, t. \end{cases}$$

- Si consideri il punto $x = 3$ in $\mathbf{R}$ e la parabola $z = y^2$ nel piano yz. La varietà di $\mathbf{R^3}$ prodotto del punto per la parabola

$$V \times W : \begin{cases} x = 3, \\ z = y^2. \end{cases}$$

è chiaramente anche l'intersezione del piano di equazione $x = 3$, parallelo al piano yz, con il cilindro $z = y^2$ con generatrici parallele all'asse x che proietta parallelamente all'asse x i punti della parabola $z = y^2$ del piano yz.

Diamo ora la seguente definizione

Definizione 2.2.2 *Si dice che una varietà affine $V = \mathcal{V}(f_1, \ldots, f_s)$, con $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, ammette una* **parametrizzazione razionale** *se esistono n funzioni razionali $r_1, \ldots, r_n$ in $k(t_1, \ldots, t_m)$, campo dei quozienti del dominio $k[t_1, \ldots, t_m]$, tali che:*
i) i punti di coordinate:

$$\begin{cases} x_1 = r_1(t_1, \ldots, t_m), \\ \vdots \\ x_n = r_n(t_1, \ldots, t_m), \end{cases}$$

siano tutti su $V = \mathcal{V}(f_1, \ldots, f_s)$
ii) V sia la più piccola varietà affine di k^n contenenti tali punti.
Se le $r_1, \ldots, r_n$ sono dei polinomi, si parlerà semplicemente di **rappresentazione parametrica polinomiale** *di V.*

Le equazioni $f_1 = \ldots = f_s = 0$ di V forniscono invece una *rappresentazione implicita* di V.

Attraverso queste ultime è più facile verificare l'appartenenza o meno di un punto ad una varietà: basterà infatti verificare se le equazioni della varietà sono soddisfatte dalle coordinate del punto in questione o meno. Le equazioni parametriche risultano più utili quando, per mezzo di un computer, si vuole disegnare il grafico della varietà. Il fatto di voler ottenere entrambe le rappresentazioni di una varietà affine, porta ai seguenti problemi:

- **Parametrizzazione**: stabilire cioè quando una varietà affine ammette una rappresentazione parametrica razionale;

- **Implicitizzazione**: data una rappresentazione parametrica di una varietà affine, vedere se è possibile passare alle equazioni cartesiane o implicite.

La risposta al primo problema è in generale negativa; saranno solo le varietà *unirazionali* a godere di questa proprietà. Per quanto riguarda invece il secondo problema si ha che è sempre possibile passare da una rappresentazione parametrica razionale ad una rappresentazione implicita, come vedremo nel capitolo sulla teoria dell'eliminazione.

Concludiamo questo paragrafo accennando ai seguenti esempi di curve e superfici dello spazio reale tridimensionale (ampliato e complessificato con l'aggiunta degli elementi impropri), che hanno rappresentazioni parametriche razionali o polinomiali

Esempi.

1. Si consideri la retta in $\mathbf{R}^3$ definita dalle equazioni:

$$\begin{cases} x+y+z=1, \\ x+2y-z=3. \end{cases}$$

   Si vede subito come le soluzioni siano infinite, essendo un sistema di 2 equazioni in 3 incognite. Ponendo, ad esempio, $z=t$, si ottiene il sistema

$$\begin{cases} x=-1-3t, \\ y=2+2t, \\ z=t, \end{cases}$$

   che dà, al variare di t in $\mathbf{R}$, le equazioni parametriche della retta.

2. Un altro esempio di varietà affine è dato da il *grafico di una funzione razionale* $y=\varphi(x)\in k(x)$ ossia $\varphi(x)=f(x)/g(x)$, con $f,g\in k[x]$, $g\neq 0$. Si ottiene in questo modo la varietà associata al polinomio $g(x)y-f(x)$

$$\mathcal{V}(g(x)y-f(x)).$$

   Assumendo come parametro $x=t$, si hanno le equazioni parametriche

$$\begin{cases} x=t, \\ y=\dfrac{f(t)}{g(t)}. \end{cases}$$

3. **Cubica sghemba** in $\mathbf{R}^3$. La curva di $\mathbf{R}^3$ di equazioni parametriche:

$$\begin{cases} x=t, \\ y=t^2, \\ z=t^3, \end{cases}$$

si dice *cubica sghemba*. Eliminando il parametro t dalle equazioni sopra scritte, si hanno le equazioni cartesiane:

$$\begin{cases} y = x^2, \\ z = x^3, \end{cases}$$

che ci mostrano come si tratti della varietà affine:

$$V = \mathcal{V}(y - x^2, z - x^3),$$

che risulta essere intersezione del cilindro quadrico $y - x^2 = 0$ e del cilindro cubico $z - x^3 = 0$ le cui generatrici sono, rispettivamente, parallele all'asse z e all'asse y.

Intersecando la curva con un piano

$$\pi : \quad ax + by + cz + d = 0,$$

si ottiene

$$at + bt^2 + ct^3 + d = 0,$$

che, per valori generici di $(a, b, c, d) \neq (0, 0, 0, 0)$, è un polinomio di terzo grado in t e, come tale, ha esattamente 3 soluzioni in $\mathbf{C}$ (il nome di "cubica trae la sua origine proprio dal fatto che un piano generico la incontra in 3 punti). Inoltre, non esiste nessun piano di $\mathbf{R}^3$ che contenga interamente la curva (o, come anche si dice, la curva è *sghemba*), in quanto se fosse

$$at + bt^2 + ct^3 + d = 0, \qquad \forall\ t \in \mathbf{R},$$

per il *principio d'identità dei polinomi*, si avrebbe $a = b = c = d = 0$, e $ax + by + cz + d = 0$ non potrebbe essere l'equazione di un piano.

In generale, l'ordine di una curva sghemba di $\mathbf{R}^3$ ha il significato geometrico di numero di punti complessi (da contarsi con la dovuta molteplicità) che la curva ha in comune con un generico piano di $\mathbf{R}^3$.

4. **Superficie tangenziale alla cubica sghemba** in $\mathbf{R}^3$.
   Abbiamo visto nell'esempio precedente come la cubica sghemba abbia equazioni parametriche:
   $$\begin{cases} x = t, \\ y = t^2, \\ z = t^3, \end{cases}$$

con $t \in \mathbf{R}$. Poiché il vettore tangente alla cubica ha per componenti le derivate prime

$$\begin{cases} \dot{x} = 1, \\ \dot{y} = 2t, \\ \dot{z} = 3t^2, \end{cases}$$

si ha che l'insieme delle tangenti alla curva in un generico punto è descritto dalle equazioni parametriche:

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

dove t ed u indicano rispettivamente la posizione sulla curva e sulla tangente. Eliminando i due parametri t ed u si ottiene l'equazione:

$$-4x^3z + 3x^2y^2 - 4y^2 + 6xyz - z^3 = 0.$$

della cosidetta Superficie tangenziale alla cubica sghemba.

2.3 Ideali

L'interesse degli ideali è che ci daranno un linguaggio per eseguire dei calcoli con varietà affini. In questo paragrafo, richiameremo la nozione di ideale direttamente nell'anello $A = k[x_1, \ldots, x_n]$, che è quello che a noi interessa, e inizieremo a vedere la relazione tra ideali di $k[x_1, \ldots, x_n]$ e varietà affini.

Definizione 2.3.1 *Un sottoinsieme I dell'anello $A = k[x_1, \ldots, x_n]$ è un* **ideale** *se soddisfa le seguenti condizioni:*

(i) $0 \in I$.

(ii) Se f e $g \in I$, anche $f + g \in I$.

(iii) Se $f \in I$ e $h \in k[x_1, \ldots, x_n]$, anche $hf \in I$.

Ovviamente, l'intersezione insiemistica di due ideali è ancora un ideale di A, mentre l'unione insiemistica non è, in generale, un ideale. Si dà allora la seguente

Definizione 2.3.2 *Sia S un sottoinsieme di un anello A. Si dice* **ideale generato da S** *e si indica con $< S >$, il minimo ideale di A contenente S.*

Si noti che che $< S >$ esiste come intersezione della famiglia, non vuota (in quanto contiene almeno A), di ideali di A contenenti S:

$$< S > \stackrel{\text{def}}{=} \bigcap_{A \geq I_h \supset S} I_h$$

Dati s polinomi $f_1, \ldots, f_s$ appartenenti all'anello $k[x_1, \ldots, x_n]$ ovviamente $< f_1, \ldots, f_s >$ contiene la totalità T delle combinazioni lineari, a coefficienti $h_i \in k[x_1, \ldots, x_n]$, degli elementi $f_1, \ldots, f_s$; basterà quindi verificare che T è un ideale perchè sia proprio l'ideale generato da $f_1, \ldots, f_s$.

Proposizione 2.3.1 *Sia $A = k[x_1, \ldots, x_n]$. Dati s polinomi $f_1, \ldots, f_s$ in A, l'insieme*

$$T = \{\sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in k[x_1, \ldots, x_n]\}$$

è un ideale dell'anello A, e coincide con l'ideale $< f_1, \ldots, f_s >$ generato da $f_1, \ldots, f_s$.

Dimostrazione. (i) Banalmente $0 \in T$, in quanto 0 si ottiene come combinazione lineare a coefficienti tutti nulli degli f_i.

Siano $f = \sum_{i=1}^{s} h_i f_i$ e $g = \sum_{i=1}^{s} q_i f_i$ e sia h un qualunque elemento di $k[x_1, \ldots, x_n]$.

(ii) Si ha che

$$f + g = \sum_{i=1}^{s} (h_i + q_i) f_i$$

è ancora una combinazione lineare dei polinomi $f_1, \ldots, f_s$, e quindi appartiene a T.

(iii) Sfruttando la proprietà distributiva dell'anello $k[x_1, \ldots, x_n]$, si ha poi

$$h(\sum_{i=1}^{s} h_i f_i) = \sum_{i=1}^{s} (h h_i) f_i$$

che di nuovo risulta essere una combinazione lineare a coefficienti $h h_i \in k[x_1, \ldots, x_n]$ di elementi di T. ∎

Nel caso in cui S sia costituito da un numero qualsiasi di polinomi basta osservare che ogni ideale contenente S dovrà contenere l'insieme T delle combinazioni lineari *finite* a coefficienti in $k[x_1, \ldots, x_n]$ di elementi di S e,

poiché è semplice dimostrare, analogamente, che T è un ideale, si avrà ancora che $< S >$ coincide con l'insieme T.
Diamo ora un'interpretazione, in termini di equazioni polinomiali, dell' ideale $< f_1, \ldots, f_s >$. A tal fine, consideriamo il sistema:

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

ove $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Moltiplicando tali equazioni, rispettivamente, per $h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$ e poi sommandole, otteniamo l'equazione:

$$h_1 f_1 + \ldots + h_s f_s = 0$$

e, per come abbiamo definito l'ideale $I =< f_1, \ldots, f_s >$, si ha anche che $h_1 f_1 + \ldots + h_s f_s \in I$, ossia $< f_1, \ldots, f_s >$ consiste di tutte le "conseguenze polinomiali" delle equazioni $f_1 = \ldots = f_s = 0$.

Esempio. Si consideri il sistema:

$$\begin{cases} x = 1 + t \\ y = 1 + t^2 \end{cases} \tag{2.3}$$

Eliminando il parametro t nel modo usuale, si ha l' equazione:

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

Possiamo però riscrivere la (2.3) nel modo seguente:

$$\begin{cases} f_1 = x - 1 - t = 0 \\ f_2 = y - 1 - t^2 = 0 \end{cases}$$

con $f_1, f_2 \in k[t, x, y]$. Moltiplicando f_1 per $g_1 = [(x - 1) + t]$ e sottraendo a tale termine f_2, si ottiene ancora l'equazione:

$$g_1 f_1 - f_2 = (x - 1)^2 - y + 1 = 0$$

Si ha quindi che

$$1 - y + (x - 1)^2 = g_1 f_1 - f_2 \in < x - 1 - t, y - 1 - t^2 >,$$

e non dipende da t. Allo stesso modo ogni altra conseguenza polinomiale di f_1 e f_2 è un elemento dell'ideale $< f_1, f_2 >$.

Definizione 2.3.3 *Un ideale I di $k[x_1, \ldots, x_n]$ si dice* **finitamente generato** *se esistono s polinomi $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ tali che $I =< f_1, \ldots, f_s >$. I polinomi $(f_1, \ldots, f_s)$ si dicono* **base** *di I.*

Nel capitolo successivo, vedremo che ogni ideale di A è finitamente generato (questo è noto come "teorema della base di Hilbert), ed è per questo che la proposizione 2.3.1 è stata dimostrata solo in questo caso. Vedremo anche come scegliere delle basi particolarmente utili: le *basi di Groebner*.

Analogie con l'algebra lineare

1. Si osservi che uno stesso ideale può avere basi diverse e con un numero di elementi diversi. Mostriamo ad esempio che:

   $$< x, y >=< x + xy, y > .$$

   Dobbiamo far vedere che $x, y \in < x+xy, y >$ e che $x+xy, y \in < x, y >$. Posto $f_1 = x + xy$, $f_2 = y$ e $g_1 = x$, si ha

   $$\begin{cases} x = f_1 - g_1 f_2, & \text{con } g_1 \in k[x, y], \\ y = f_2, \end{cases}$$

   ossia x, y sono una combinazione lineare a coefficienti polinomiali degli elementi dell' ideale $< x + xy, y >$. Viceversa, si vede facilmente come $x + xy, y \in < x, y >$.

2. La definizione di *ideale* è molto simile a quella di *sottospazio vettoriale*. Entrambi devono essere chiusi rispetto all'addizione e alla moltiplicazione per coefficienti polinomiali nel primo caso e per gli scalari nel secondo. Si ha, inoltre, che l'*ideale generato* dai polinomi $f_1, \ldots, f_s$ è simile al *sottospazio generato* dal numero finito di vettori $v_1, \ldots, v_s$. In ogni caso, infatti, bisogna studiarne le combinazioni lineari: a coefficienti polinomiali nel caso di ideali, a coefficienti in un campo, quando si opera con i sottospazi vettoriali.
   Il concetto di base è comunque diverso in quanto una base di un ideale è semplicemente un *sistema di generatori*.

Vediamo ora la seguente proposizione che mostra come una varietà affine dipenda unicamente dall'ideale generato dai polinomi che la definiscono.

Proposizione 2.3.2 *Se $f_1, \ldots, f_s$ e $g_1, \ldots, g_t$ sono due basi dello stesso ideale di $k[x_1, \ldots, x_n]$ ossia $< f_1, \ldots, f_s >=< g_1, \ldots, g_t >$, si ha necessariamente che $\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t)$.*

Dimostrazione. Poiché per ipotesi $< g_1, \ldots, g_t > \subseteq < f_1, \ldots, f_s >$, ogni g_j è combinazione lineare degli f_i, ossia $g_j = \sum_{i=1}^{s} h_i f_i$.

Se a è un elemento di $\mathcal{V}(f_i)$, risulta $f_i(a) = 0$ per ogni $i = 1, \ldots, s$; pertanto, $g_j(a) = \sum_{i=1}^{s} h_i(a) f_i(a) = 0$ per ogni $j = 1, \ldots, t$, il che dimostra, per l'arbitrarietà di a in $\mathcal{V}(f_i)$, che

$$\mathcal{V}(f_1, \ldots, f_s) \subseteq \mathcal{V}(g_1, \ldots, g_t).$$

L'inclusione inversa si dimostra allo stesso modo, partendo dall'ipotesi che $< f_1, \ldots, f_s > \subseteq < g_1, \ldots, g_t >$. ∎

Il risultato di questa proposizione è di grande utilità nelle applicazioni pratiche. In alcuni casi, infatti, cambiando base in un ideale si trovano più facilmente i punti della varietà, come mostra il seguente

Esempio:

- Si consideri l'ideale:

$$I =< 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 >=< x^2 - 4, y^2 - 1 >,$$

come si verifica facilmente. Dalla proposizione precedente segue che :

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

Utilizzando la seconda base scritta per l'ideale è, dunque, più semplice determinare la varietà.

Dalla proposizione precedente e dal sopracitato Teorema della base di Hilbert segue che ad un ideale I di $k[x_1, \ldots, x_n]$ (che, per il teorema di Hilbert è necessariamente del tipo $I =< f_1, \ldots, f_s >$) resta associata la varietà affine $V = \mathcal{V}(I)$. Viceversa:

Proposizione 2.3.3 *Se $V = \mathcal{V}(I)$ è una varietà affine di k^n, l'insieme*

$$\mathcal{I}(\mathcal{V}(I)) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \ \forall\, a \in V\}$$

dei polinomi che si annullano su V, è un ideale di $k[x_1, \ldots, x_n]$, che dicesi ideale associato a V

Dimostrazione. Lo 0 di $k[x_1, \ldots, x_n]$ appartiene a $\mathcal{I}(V)$ dato che si annulla in ogni punto di k^n e dunque in tutti i punti di V.

Se f e g sono due polinomi di $\mathcal{I}(V)$, per definizione di $\mathcal{I}(V)$ si ha $f(a) = g(a) = 0$ per ogni $a \in V$, da cui $f(a) + g(a) = 0 \ \forall\, a \in V$. Pertanto, anche $f + g$ appartiene a $\mathcal{I}(V)$.

Siano infine $h \in k[x_1, \ldots, x_n]$ ed $f \in \mathcal{I}(V)$. Di nuovo $f(a) = 0 \ \forall\, a \in V$, per cui anche $h(a)f(a) = 0 \ \forall\, a \in V$. Abbiamo così dimostrato che anche hf è un elemento di $\mathcal{I}(V)$. ∎

Si noti che se $V = \mathcal{V}(f_1, \ldots, f_s)$, sicuramente $f_1, \ldots, f_s \in \mathcal{I}(V)$.

Esempi:

1. Si consideri la varietà costituita dall'origine $\{(0,0)\}$ di k^2, definita ovviamente dal sistema:
$$\begin{cases} x = 0, \\ y = 0. \end{cases}$$
L'ideale associato a tale varietà , $\mathcal{I}(\mathcal{V}(x,y))$, è formato da tutti i polinomi appartenenti a $k[x,y]$ che si annullano in $\{(0,0)\}$.
Vogliamo provare che risulta:
$$\mathcal{I}(\mathcal{V}(x,y)) =< x, y > .$$
Banalmente, ogni polinomio appartenente all'ideale $< x, y >$ è della forma $A(x,y)x + B(x,y)y$, e quindi si annulla nell'origine. Risulta allora $< x, y > \subset \mathcal{I}$.
Per quanto riguarda l'inclusione inversa, si consideri un generico polinomio $f(x,y) = \sum_{i,j} a_{ij} x^i y^j$ appartenente a $k[x,y]$ e che si annulli nell'origine. Si ha $a_{00} = f(0,0) = 0$, per cui:
$$\begin{aligned} f &= a_{00} + \sum_{(i,j)\neq(0,0)} a_{ij} x^i y^j \\ &= 0 + (\sum_{i>0,j} a_{ij} x^{i-1} y^j)x + (\sum_{j>0} a_{0j} y^{j-1})y \ \in < x, y > . \end{aligned}$$
Si noti che $I =< f_1, \ldots, f_s > \subseteq \mathcal{I}(\mathcal{V}(I))$, ma in generale risulta
$$< f_1, \ldots, f_s > \neq \mathcal{I}(\mathcal{V}(I)).$$
Infatti, avremmo potuto determinare l'origine anche come soluzione del sistema:
$$\begin{cases} x^2 = 0, \\ y^2 = 0. \end{cases}$$

Per quanto visto sopra l'ideale

$$\mathcal{I}(\mathcal{V}(x^2, y^2)) =< x, y >,$$

e risulta $< x^2, y^2 > \subset < x, y >$ ma $< x^2, y^2 > \neq < x, y >$, dato che $x \notin < x^2, y^2 >$ e $y \notin < x^2, y^2 >$.

2. Ci proponiamo ora di studiare l'ideale associato alla cubica sghemba in $\mathbf{R^3}$, di equazioni parametriche:

$$\begin{cases} x = t, \\ y = t^2, \\ z = t^3, \end{cases}$$

e di equazioni cartesiane:

$$\begin{cases} y - x^2 = 0, \\ z - x^3 = 0. \end{cases}$$

In questo caso si vuole provare che:

$$\mathcal{I}(\mathcal{V}(I)) = I =< y - x^2, z - x^3 > .$$

Per arrivare a questo risultato dovremo fare vedere che per ogni $f \in k[x, y, z]$ tale che $f(t, t^2, t^3) = 0$ per ogni $t \in k$, risulta $f(x, y, z) = h_1(y - x^2) + h_2(z - x^3)$.

Proposizione 2.3.4 *Dato un polinomio $f \in k[x, y, z]$, è sempre possibile scrivere f nella forma:*

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

dove h_1 e h_2 sono polinomi nell'anello $k[x, y, z]$, mentre r è un polinomio nella sola x.

Dimostrazione. Sarà sufficiente dimostrare la proposizione nel caso in cui f sia un monomio, dato che ogni polinomio si può scrivere nella forma

$$f(x, y, z) = \sum_{\alpha,\beta,\gamma} c_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma$$

con $c_{\alpha\beta\gamma} \in k$.

Per un arbitrario monomio $x^\alpha y^\beta z^\gamma$, si può scrivere

$$\begin{aligned} x^\alpha y^\beta z^\gamma &= x^\alpha (x^2 + y - x^2)^\beta (x^3 + z - x^3)^\gamma \\ &= x^\alpha [x^2 + (y - x^2)]^\beta [x^3 + (z - x^3)]^\gamma \\ &= x^\alpha [x^{2\beta} + g_1(x,y,z)(y - x^2)][x^{3\gamma} + g_2(x,y,z)(z - x^3)] \\ &= x^{\alpha+2\beta+3\gamma} + h_1(x,y,z)(y - x^2) + h_2(x,y,z)(z - x^3) \end{aligned}$$

ove g_1, g_2, h_1, h_2 sono opportuni polinomi di $k[x, y, z]$. L'asserto è dunque vero per i monomi, il che completa la dimostrazione. ∎

Tornando ora all'esempio precedente della cubica sghemba $\mathcal{C}^3$, si ha che un polinomio f appartiene all'ideale $\mathcal{I}(\mathcal{C}^3)$ associato alla cubica se, e solo se, risulta $f(t, t^2, t^3) = r(t) = 0$ per ogni $t \in k$.

Abbiamo così trovato un polinomio della sola x, $r(x)$ che ammette infinite radici, ma, se k è infinito, per il principio d'identità dei polinomi, questo è possibile soltanto se $r(x) \equiv 0$.

Dunque ogni polinomio f appartenente all'ideale associato alla cubica sghemba si può scrivere:

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

e, pertanto, appartiene all'ideale $I =< y - x^2, z - x^3 >$, da cui l'uguaglianza:

$$\mathcal{I}(\mathcal{C}^3) =< y - x^2, z - x^3 > .$$

Si è visto tuttavia che, in generale, $< f_1, \ldots, f_s > \subset \mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$ ma $< f_1, \ldots, f_s > \neq \mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$, come mostra l'esempio dato dall'ideale $< x^2, y^2 >$. Per quanto possa essere diverso da $< f_1, \ldots, f_s >$, l'ideale $\mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$ contiene abbastanza informazione da determinare univocamente la varietà.

Proposizione 2.3.5 *Siano V e W due varietà affini in k^n. Allora:*
(i) $V \subset W$ se e soltanto se $\mathcal{I}(V) \supset \mathcal{I}(W)$,
(ii) $V = W$ se e soltanto se $\mathcal{I}(V) = \mathcal{I}(W)$.

Dimostrazione. (i) Se $V \subset W$, ogni polinomio che si annulla su W si annulla, in particolare, anche su V, per cui si ha $\mathcal{I}(V) \supset \mathcal{I}(W)$.

Viceversa, sia W la varietà affine definita dal sistema:

$$\begin{cases} g_1 = 0 \\ \vdots \\ g_t = 0 \end{cases}$$

e, per ipotesi, si abbia che tutte le funzioni nulle su W sono nulle anche su V, ossia $\mathcal{I}(V) \supset \mathcal{I}(W)$. Poiché $g_1, \ldots, g_t$ sono in $\mathcal{I}(W) \subset \mathcal{I}(V)$, si deve avere:

$$\begin{cases} g_1(a) = 0 \\ \vdots \\ g_t(a) = 0, \quad \forall\, a \in V \end{cases}$$

Pertanto, ogni $a \in V$ è soluzione del sistema:

$$\begin{cases} g_1 = 0 \\ \vdots \\ g_t = 0 \end{cases}$$

da cui segue necessariamente che $V \subset W$.
(ii) Se vale l'uguaglianza $V = W$ si ha che $V \subseteq W$ e $W \subseteq V$ e quindi, per quanto dimostrato sopra, si hanno le due inclusioni $\mathcal{I}(V) \supseteq \mathcal{I}(W)$, e $\mathcal{I}(W) \supseteq \mathcal{I}(V)$ da cui $\mathcal{I}(V) = \mathcal{I}(W)$. Viceversa, partendo da quest'ultima uguaglianza, sempre per la (i) già dimostrata si deduce analogamente che $V = W$. ∎

Per quanto riguarda gli ideali si presentano i seguenti problemi, che affronteremo, per l'anello dei polinomi in una variabile, nei paragrafi che seguono.

- **Descrizione dell'ideale**, che consiste nel determinare se un ideale I si possa scrivere come $< f_1, \ldots, f_s >$ per opportuni polinomi $f_1, \ldots, f_s$ di $k[x_1, \ldots, x_n]$.

- **Appartenenza**, che consiste nella ricerca di un algoritmo che ci permetta di stabilire se un polinomio f appartiene o meno all'ideale $< f_1, \ldots, f_s >$.

- **Nullstellensatz** che consiste nello stabilire l'esatta relazione tra l'ideale $< f_1, \ldots, f_s >$ e l'ideale $\mathcal{I}(\mathcal{V}(f_1, \ldots, f_s))$.

2.4 Polinomi in una variabile

Nel corso di questo paragrafo studieremo i polinomi in una variabile, analizzando sia l'*algoritmo di divisione* che l'*algoritmo euclideo delle divisioni successive per la ricerca del Massimo Comun Divisore di due polinomi*. Questo ci aiuterà a studiare la struttura degli ideali nell'anello $k[x]$ dei polinomi in una indeterminata.

Si intende per *algoritmo* un insieme di istruzioni che permettono di elaborare dati simbolici o numerici. La struttura di un algoritmo è caratterizzata da un *input*, costituito dai dati numerici che noi inseriamo, e da un *output*, che è, invece, il risultato dell'algoritmo stesso.

Presenteremo gli algoritmi in *pseudocodice*, ossia in un linguaggio molto simile al Pascal. Ciò permetterà una facile comprensione della loro struttura.

Per studiare l'algoritmo di divisione fra polinomi dell'anello $k[x]$ richiamiamo la nozione di *termine direttore* (Leading Term) di un polinomio in una variabile.

Definizione 2.4.1 *Dato un polinomio non nullo $f \in k[x]$, ovvero:*

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$$

dove $a_i \in k$ e $a_m \neq 0$ (per cui il grado di f è uguale ad m), il termine $a_m x^m$ si dice **termine direttore** *(leading term) di f, e si indica con $LT(f) = a_m x^m$.*

Si osservi che, dati due polinomi $f, g \in k[x]$ non nulli, si ha:

$$deg(f) \leq deg(g) \Longleftrightarrow LT(f) \text{ divide } LT(g).$$

Passiamo ora a descrivere l'algoritmo di divisione fra polinomi.

Proposizione 2.4.1 *Sia k un campo e sia g un polinomio non nullo in $k[x]$. Ogni polinomio $f \in k[x]$ può essere scritto nella forma:*

$$f = gq + r,$$

dove q ed r appartengono a $k[x]$, e risulta o $r = 0$ oppure $deg(r) < deg(g)$. Inoltre, q ed r sono unici ed esiste un algoritmo per calcolarli.

Dimostrazione. Siano f e g due polinomi in $k[x]$ di gradi rispettivi n ed m:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \qquad \text{con } LT(f) = a_n x^n,\ a_n \neq 0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0, \qquad \text{con } LT(g) = b_m x^m,\ b_m \neq 0.$$

Si ponga inizialmente il resto della divisione di f per g uguale ad $r_0 = f$. Se il grado di f è minore del grado di g basterà porre $f = 0g + f$. Se il grado di f è maggiore o uguale al grado di g, allora si può procedere nella divisione ottenendo al passo successivo r_1.

$$\begin{array}{l|l} r_0 = f(x) = a_n x^n + \ldots + a_0 & b_m x^m + \ldots + b_0 \\ \hline r_1 = r_0 - [LT(r_0)/LT(g)]g(x) & LT(r_0)/LT(g)) \end{array}$$

Ad ogni passo si possono presentare 3 casi:

- r è uguale a zero;
- il grado di r è minore del grado di g;
- il grado di r è maggiore o uguale al grado di g.

Nei primi due casi la divisione si arresta, mentre nel terzo caso si va avanti fino a quando non si presenti uno dei primi due casi.

Diamo ora, in pseudocodice, un algoritmo per il calcolo di q ed r. Nell'algoritmo si è posto inizialmente $q = 0$ e $r = f$, come conseguenza del fatto che ogni polinomio f si può esprimere come $f = 0g + f$.

Input: g, f
$q := 0$
$r := f$
WHILE $r \neq 0$ AND $LT(g)$ divides $LT(r)$ DO
    $q := q + LT(r)/LT(g)$
    $r := r - [LT(r)/LT(g)]\ g$
Output : q, r

Una volta assegnato l'algoritmo per il calcolo effettivo della divisione resta da dimostrare:

1. che l'algoritmo si arresta,
2. che l'output è costituito da due polinomi q ed r tali che $f = qg + r$,
3. l'unicità del quoziente e del resto.

1. Si osservi che l'insieme dei gradi dei resti è un insieme di numeri non negativi che ad ogni passo decresce. All'inizio il grado del resto è uguale ad n

ma, dopo un numero finito di passi (al massimo $n-m+1$), sarà sicuramente inferiore al grado di g e, per quanto visto prima, in tal caso l'algoritmo si arresta.

2. La dimostrazione procede per induzione sul grado n di $f(x)$. Se $n = 0$, allora f è uguale ad una costante c, per cui $f = c = 0g + c$. Supponiamo allora che per ogni polinomio di grado $\leq n-1$ esistano due polinomi q ed r soddisfacenti alle condizioni di cui nell'enunciato, e dimostriamo che questo vale anche per polinomi di grado n.
Si può sempre riscrivere $f(x)$ come:

$$f(x) = [f(x) - \frac{LT(f)}{LT(g)}g(x)] + \frac{LT(f)}{LT(g)}g(x)$$

e l'espressione entro parentesi è di grado minore di n, in quanto si cancella il termine direttore di f. Quindi per l'ipotesi induttiva:

$$f - \frac{LT(f)}{LT(g)}g = q_1 g + r$$

per cui

$$f(x) = (\frac{LT(f)}{LT(g)} + q_1)g(x) + r.$$

Posto $q = LT(f)/LT(g) + q_1$ si ha la tesi.

3. Supponiamo per assurdo che il quoziente ed il resto non siano unici, ossia:

$$f = qg + r = q_1 g + r_1 \tag{2.4}$$

ove sia r che r_1 hanno grado minore del grado di g (oppure uno dei due o entrambi sono nulli). Ne segue che, se $r \neq r_1$, necessariamente, il grado di $r - r_1$ è minore del grado di g. Ma dall'uguaglianza (2.4) segue:

$$(q_1 - q)g = (r - r_1)$$

se $r - r_1 \neq 0$ non può essere $q - q_1 = 0$ e pertanto se $r \neq r_1$ si ha $\partial(r - r_1) = \partial(q - q_1) + \partial g \geq \partial g$, il che contraddice il fatto $\partial(r - r_1) < \partial g$. L'assurdo prova dunque che è necessariamente $r - r_1 = 0$ e $q_1 - q = 0$, da cui la tesi. ∎

Molti sistemi di algebra computazionale implementano l'algoritmo descritto per la divisione fra polinomi (cfr. Davenport, Siret e Tournier, (1988), [cfr[9]]).

Da questo teorema segue un utile corollario riguardo al numero di radici di un polinomio in una variabile.

Corollario 2.4.1 *Se k è un campo e $f(x) \in k[x]$ è un polinomio non nullo di grado $N = \partial f(x)$, si ha che $f(x)$ ha al più N radici in k.*

Dimostrazione. Si procede per induzione su N. Se $N = 0$, allora f è costante e l'equazione $f(x) = 0$ non ammette nessuna soluzione se non nel caso particolare $f = c = 0$.

Se $N = 1$, allora f si può scrivere come $f(x) = ax + b$ e l'equazione $f(x) = 0$ ammette l'unica soluzione $x = -(a)^{-1}b$.

Supposto vero l'enunciato per polinomi di grado $\leq N-1$, dimostriamolo vero per polinomi di grado N. A tale scopo faremo uso dell'algoritmo di divisione fra polinomi. Fissato comunque a in k, ogni polinomio f si può scrivere nella forma:

$$f(x) = (x - a)q(x) + r$$

dove o $r = 0$, oppure $\partial r < \partial(x - a) = 1$. Quindi se $r \neq 0$ si ha che r è una costante. In entrambi i casi valutando l'espressione in a si ottiene $f(a) = r$.

Se $f(a) = 0$, allora $(x-a)$ divide $f(x)$. In generale, se $f(x)$ non ha radici la tesi è banalmente verificata. Se invece $f(x)$ ha almeno una radice $a \in k$, allora:

$$f(x) = (x - a)q(x),$$

da cui, passando ai gradi si ottiene

$$\partial f = N = 1 + \partial(q(x)).$$

Pertanto $\partial(q(x)) = N - 1$ e, per ipotesi induttiva, $q(x)$ ha al più $N - 1$ radici. Dalla

$$f(x) = (x - a)q(x)$$

segue, valutando ambo i membri per una radice $b \neq a$ di $f(x)$, che ogni radice diversa da a di $f(x)$ è anche radice di $q(x)$. Infatti, essendo $b - a \neq 0$

$$0 = f(b) = (b - a)q(b) \ \Rightarrow q(b) = 0.$$

Resta così dimostrata la tesi. ∎

Dall'algoritmo di divisione dei polinomi segue anche il seguente corollario che fornisce una descrizione della struttura degli ideali in $k[x]$.

Corollario 2.4.2 *Sia k un campo. Ogni ideale $I \leq k[x]$ è* **principale**, *ossia generato da un polinomio $g(x)$:*

$$I =< g >= \{hg \mid h \in k[x]\}$$

ed è perciò costituito dai multipli secondo polinomi di $g(x)$. Inoltre, $g(x)$ è unico a meno di una costante moltiplicativa non nulla in k, ed è un polinomio di grado minimo tra quelli appartenenti all'ideale I.

Dimostrazione. Se $I = \{0\}$, allora il risultato è banale in quanto $I =< 0 >$. Se $I \neq \{0\}$. esiste almeno un $g(x) \neq 0$ tale che $g(x) \in I$. Quindi l'insieme S dei gradi dei polinomi $g(x) \neq 0$ appartenenti ad I è un sottoinsieme non vuoto dell'insieme $\mathbf{N}$ degli interi non negativi, e, per la proprietà di buon ordinamento di $\mathbf{N}$, S ammette un minimo. Sia ora $g(x) \neq 0$ un polinomio di grado minimo tra i polinomi che appartengono ad I.

Per ogni polinomio $f(x) \in k[x]$, possiamo eseguire la divisione di $f(x)$ per $g(x)$:

$$f(x) = q(x)g(x) + r(x)$$

e $r = 0$ oppure $\partial r < \partial g$. Se $r = 0$, necessariamente f appartiene all' ideale. Se fosse $\partial r < \partial g$, essendo $g(x)$ un polinomio di grado minimo fra quelli appartenenti ad I, si avrebbe che r non può appartenere ad I. Ma

$$r(x) = f(x) - q(x)g(x)$$

e se $f(x) \in I$, il resto $r(x)$ deve appartenere ad I in quanto combinazione lineare di elementi di I. Risulta, pertanto, che $r(x) = 0$ e per ogni $f \in I$ si ha $f(x) = q(x)g(x)$.

Vogliamo ora dimostrare che $g(x)$ è unico a meno di una costante moltiplicativa non nulla. Sia per assurdo $< g >=< g_1 >$. Deve quindi essere verificato sia che $g \in< g_1 >$, sia che $g_1 \in< g >$; in termini equivalenti, si avrà che esistono h e t in $k[x]$ tali che $g = hg_1$ e $g_1 = tg$. Prendendo i gradi si ottiene $\partial g = \partial h + \partial g_1$ (il che implica $\partial g \geq \partial g_1$) e $\partial g_1 = \partial t + \partial g$ (il che implica che $\partial g_1 \geq \partial g$). In definitiva, risulta $\partial g = \partial g_1$ e quindi $\partial h = \partial t = 0$. Da ciò segue necessariamente che t ed h sono due costanti moltiplicative e ovviamente risultano l'una inversa dell'altra, da cui la tesi. ∎

Da questo corollario segue un criterio per stabilire l'**appartenenza** di un polinomio ad un ideale I. Siano infatti $I =< g(x) >$ e $f(x) \in k[x]$.
Il resto della divisione di $f(x)$ per $g(x)$ è uguale a zero, se e solo se, $f(x) \in I$.

La dimostrazione del corollario precedente non è costruttiva in quanto non fornisce un metodo per il calcolo del polinomio $g(x)$, ovvero del

generatore dell'ideale I assegnato. Allo scopo di risolvere questo problema introduciamo la nozione di **massimo comun divisore** (MCD) fra polinomi.

Definizione 2.4.2 Un *massimo comun divisore dei polinomi f e g appartenenti all'anello $k[x]$ è un polinomio $h \in k[x]$ tale che:*

(i) h divide f e g,

(ii) se p è un altro polinomio che divide f e g, allora p divide h.

Se h è un polinomio che gode di tali proprietà, allora scriveremo:

$$h = MCD(f, g).$$

Studiamo ora alcune proprietà del massimo comun divisore.

Teorema 2.4.1 *Per ogni f e g appartenenti all'anello $k[x]$ si ha:*

(i) Esiste $h(x) = MCD(f, g)$ ed è unico a meno di una costante moltiplicativa non nulla.

(ii) $< h >=< f, g >$.

(iii) Esiste un algoritmo per calcolare $h(x)$ (l'algoritmo euclideo delle divisioni successive).

Dimostrazione. La (i) e la (ii) seguono dal fatto che l'ideale generato da due polinomi è principale, per il corollario 2.4.2. Se

$$< f, g >=< h >,$$

facciamo vedere che h è un massimo comun divisore tra f e g.

Dall'uguaglianza $< f, g >=< h >$, segue che $f \in < h >$ e $g \in < h >$, da cui $f = f_1 h$ e $g = g_1 h$, ossia h divide f e g.

D'altra parte, $h \in < f, g >$, quindi esistono A e B appartenenti a $k[x]$ tali che $h = Af + Bg$. Ne segue che ogni $p \in k[x]$ che divida f e g, necessariamente divide $Af + Bg = h$.

(iii) Siano N e M i gradi rispettivi di f e g. Scambiando, eventualmente, il ruolo di f e g, si può supporre, senza restrizioni, che $N \geq M$. Operiamo le seguenti divisioni:

$$\begin{aligned}
f &= q_1 g + r_1, \qquad \partial r_1 < \partial g, \\
g &= q_2 r_1 + r_2, \qquad \partial r_2 < \partial r_1, \\
r_1 &= q_3 r_2 + r_3, \qquad \partial r_3 < \partial r_2, \\
&\vdots \\
r_{n-1} &= q_{n+1} r_n + r_{n+1} \qquad \partial r_{n+1} < \partial r_n, \\
r_n &= q_{n+2} r_{n+1} + 0.
\end{aligned}$$

Non è difficile vedere che r_{n+1}, l'ultimo resto non nullo della divisione è un massimo comun divisore tra f e g. Infatti, partendo dall'ultima equazione e risalendo, via via fino alla prima, si vede che r_{n+1} divide r_n, ma allora divide anche $r_{n-1}, \ldots, r_3, r_2, r_1$ e quindi anche g ed f. Viceversa, partendo dalla prima equazione si vede che, se p è un divisore comune ad f e g, deve necessariamente dividere r_1, ma allora essendo un divisore comune a r_1 e a g si vede dalle successive che divide anche $r_2, r_3, \ldots, r_{n+1}$. Si ha quindi che r_{n+1} è un massimo comun divisore di f e g.

Dalle equazioni sopra scritte seguono le uguaglianze:

$$\begin{aligned} < f, g > &= < g, r_1 >, \\ < g, r_1 > &= < r_1, r_2 >, \\ &\vdots \\ < r_{n-1}, r_n > &= < r_n, r_{n+1} > . \end{aligned}$$

Mostriamo ora in pseudocodice l'algoritmo euclideo delle divisioni successive.

Abbiamo due variabili h e s che rappresentano il dividendo e, rispettivamente, il divisore delle divisioni. Indicheremo poi con rem il resto della divisione tra h e s:

Input: g, f
$h := f$
$s := g$
WHILE $s \neq 0$ DO
    $rem := rem(h, s)$
    $h := s$
    $s := rem$
Output: h

Si noti che l'algoritmo si arresta in quanto l'insieme dei gradi dei resti è un insieme di interi non negativi che ad ogni passo decresce. ∎

Si ricorda che esiste anche una versione dell'Algoritmo Euclideo per trovare il massimo comun divisore di due interi, o, più in generale, di due elementi di una anello euclideo. La maggior parte dei sistemi di algebra computazionale hanno un comando per il calcolo del MCD di due polinomi (o interi), che utilizza una versione modificata dell'Algoritmo Euclideo. Per maggiori dettagli si consiglia DAVENPORT, SIRET e TOURNIER (1988), [cfr[9]].

2.5 Nullstellensatz nel caso di una variabile

Abbiamo visto come nel caso dell'anello $k[x]$, l'ideale generato dai polinomi f e g coincida con $< h(x) >$, dove $h(x) = MCD(f, g)$. Nel caso in cui, invece di due polinomi, consideriamo una s-pla $f_1, \ldots, f_s$, si ha la seguente

Definizione 2.5.1 *Siano $f_1, \ldots, f_s \in k[x]$, si dice* **massimo comun divisore** *dei polinomi $f_1, \ldots, f_s$ 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 gode di queste proprietà, scriviamo $h = MCD(f_1, \ldots, f_s)$.

Non è difficile dimostrare la seguente Proposizione che estende al caso $s > 2$ quella già vista per $s = 2$ polinomi.

Proposizione 2.5.1 *Siano $f_1, \ldots, f_s \in k[x]$, con $s \geq 2$. Risulta:*
(i) esiste un $MCD(f_1, \ldots, f_s)$ ed è unico a meno di una costante moltiplicativa non nulla di k.
(ii) Un $MCD(f_1, \ldots, f_s)$ è un generatore dell'ideale $< f_1, \ldots, f_s >$.
(iii) Se $s \geq 3$, si ha

$$MCD(f_1, \ldots, f_s) = MCD(f_1, MCD(f_2, \ldots, f_s)).$$

(iv) Esiste un algoritmo per trovare un MCD tra s polinomi.

Si è visto inoltre come un generico polinomio $f \in k[x]$ appartiene all'ideale $I =< h(x) >$ se e soltanto se il resto della divisione fra f ed h è uguale a zero.

Vogliamo ora stabilire l'esatta relazione tra l'ideale I che definisce la varietà $V = \mathcal{V}(f_1, \ldots, f_s)$ e l'ideale ad essa associato $\mathcal{I}(V)$.

Si è già osservato in precedenza che $I \subset \mathcal{I}$. Sia ora k un *campo algebricamente chiuso* e V la varietà definita dal seguente sistema:

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

La varietà V è altrettanto ben definita da ogni altra base dell'ideale

$$I =< f_1, \ldots, f_s > .$$

Poiché in $k[x]$ ogni ideale è principale, dalla (ii) della proposizione precedente segue che V è anche definita da $h(x) = MCD(f_1, \ldots, f_s)$.

Sia n il grado di $h(x)$, ossia:

$$h(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0,$$

con $a_n = LC(h) \neq 0$. Se $n \geq 1$, dal teorema fondamentale dell'algebra segue che $h(x)$ ha almeno una radice α_1, e sia r_1 la sua molteplicità . Esiste allora $H(x) \in k[x] - \{0\}$ tale che

$$h(x) = (x - \alpha_1)^{r_1} H(x), \qquad \text{con } H(\alpha_1) \neq 0.$$

Ogni α_i radice di $h(x)$, con $\alpha_i \neq \alpha_1$, è radice di $H(x)$. Per induzione sul grado n di $h(x)$, segue che $h(x)$ si può decomporre nel modo:

$$h(x) = (x - \alpha_1)^{r_1} \cdot \ldots \cdot (x - \alpha_t)^{r_t} a_n.$$

L'ideale I che definisce la varietà V si può quindi riscrivere come:

$$I =< (x - \alpha_1)^{r_1} \cdot \ldots \cdot (x - \alpha_t)^{r_t} > .$$

Definizione 2.5.2 *Dato il polinomio* $h(x) = (x - \alpha_1)^{r_1} \ldots (x - \alpha_t)^{r_t}$, *si definisce* **riduzione** *di* $h(x)$ *il polinomio:*

$$h_{rid}(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_t),$$

ossia il polinomio monico che ha esattamente le stesse radici distinte di h, *ma con molteplicità uguale ad uno.*

Studiamo ora il teorema degli zeri di Hilbert nel caso di una variabile.

Teorema 2.5.1 (Nullstellensatz) *Sia* k *un campo algebricamente chiuso. Assegnati* s *polinomi* $f_1, \ldots, f_s$ *in* $k[x]$, *si denoti con* h *un loro massimo comun divisore. Allora, dette* $\alpha_1, \ldots, \alpha_t$ *le radici distinte di* h, *risulta:*

$$\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(h) = \{\alpha_1, \ldots, \alpha_t\}$$

$$\mathcal{I}(\mathcal{V}(f_1, \ldots, f_s)) = \mathcal{I}(\mathcal{V}(h)) =< h_{rid} >=< (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_t) > .$$

Dimostrazione. Se il campo è algebricamente chiuso il polinomio h ha almeno una radice α_i; ma allora è divisibile per il binomio $x - \alpha_i$. Tale osservazione porta per induzione alla fattorizzazione sopra citata per h e alla definizione di h_{rid}. L'ideale $\mathcal{I}(\mathcal{V}(h))$ è costituito, per definizione, dai polinomi che si annullano su $\alpha_1, \ldots, \alpha_t$ e come tali sono divisibili per $x - \alpha_1, \ldots, x - \alpha_t$ e, quindi, sono divisibili anche per il loro prodotto h_{rid}. Si ha pertanto $\mathcal{I}(\mathcal{V}(h)) \subseteq < h_{rid} >$. Viceversa, poiché $\mathcal{V}(h) = \{\alpha_1, \ldots, \alpha_t\}$, ogni multiplo

di h_{rid} è nullo su $\mathcal{V}(h)$ e, come tale, appartiene a $\mathcal{I}(\mathcal{V}(h))$ si ha pertanto che $\mathcal{I}(\mathcal{V}(h)) \supseteq < h_{rid} >$. Ovviamente, se k non è algebricamente chiuso non si ha la base per applicare l'induzione e arrivare alla fattorizzazione, in quanto esistono polinomi di grado positivo privi di radici. ∎

Nel caso di una variabile e se il campo è algebricamente chiuso, abbiamo così trovato la relazione tra I e l'ideale $\mathcal{I}(\mathcal{V}(I))$. Ma la risposta data non è soddisfacente in quanto è necessario saper fattorizzare completamente in fattori lineari il polinomio h per determinare h_{rid}. Vogliamo ora far vedere che si può determinare h_{rid} anche senza decomporre h nel prodotto dei suoi fattori lineari.

Dato un polinomio $h(x) = \sum_{i=0}^{n} a_i x^i \in k[x]$, si definisce il *derivato formale* mediante le formule usuali dell'analisi:

$$h' = \frac{dh(x)}{dx} = \sum_{i=1}^{n} i a_i x^{i-1}$$

e non è difficile provare che valgono le regole di derivazione:

$$(ah)' = ah', \qquad (h+g)' = h' + g', \qquad (hg)' = h'g + hg',$$

dove $a \in k$ mentre $h, g \in k[x]$.

Proposizione 2.5.2 *Se α è una radice di molteplicità r per $h(x)$, allora α è una radice di molteplicità $(r-1)$ per il suo derivato h'.*

Dimostrazione. Se α è una radice di molteplicità r per $h(x)$ si ha:

$$h(x) = (x-\alpha)^r H(x), \qquad \text{con } H(\alpha) \neq 0,$$

da cui, calcolando il derivato di ambo i membri si ottiene:

$$\begin{aligned} h' &= r(x-\alpha)^{r-1} H(x) + (x-\alpha)^r H'(x) \\ &= (x-\alpha)^{r-1}[rH(x) + (x-\alpha)H'(x)]. \end{aligned}$$

Si vede quindi che α ha almeno molteplicità $(r-1)$ per h'. Dobbiamo mostrare che tale molteplicità è esattamente $(r-1)$. Posto $p(x) = rH(x) + (x-\alpha)H'(x)$, risulta:

$$p(\alpha) = rH(\alpha) + 0 = rH(\alpha) \neq 0,$$

ossia p non ammette $x = \alpha$ come radice. Ne segue che α è uno zero di molteplicità esattamente $r-1$ per $h'(x) = (x-\alpha)^{r-1} p(x)$. ∎

In base a questa proposizione possiamo scrivere h_{rid} in funzione di h e del suo derivato h':

$$h_{rid} = \frac{h}{MCD(h, h')}.$$

L'ideale associato alla varietà definita da $f_1, \ldots, f_s$, è quindi

$$\mathcal{I}(\mathcal{V}(I)) =< \frac{h}{MCD(h, h')} >,$$

ove $h = MCD(f_1, \ldots, f_s)$.

Esempio: Si vuole trovare una base per l'ideale associato alla varietà affine definita dai due polinomi:

$$\begin{aligned} f_1(x) &= x^5 - 2x^4 + 2x^2 - x \\ f_2(x) &= x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \end{aligned}$$

Si ha:

$$\begin{aligned} f_1(x) &= x[(x^4 - 1) - 2x(x^2 - 1)] = x(x-1)^3(x+1) \\ f_2(x) &= (x-1)[x^4 - 2x^2 + 1] = (x-1)^3(x+1)^2 \end{aligned}$$

Un massimo comun divisore tra $f_1(x)$ e $f_2(x)$ è quindi:

$$h(x) = MCD(f_1, f_2) = (x-1)^3(x+1)$$

Per quanto osservato in precedenza $I =< (x-1)^3(x+1) >$. Risulta quindi $\mathcal{V}(I) = \{-1, 1\}$. Inoltre:

$$h' = (x-1)^2[4x + 2],$$

da cui:

$$MCD(h, h') = (x-1)^2.$$

Applicando quanto visto sulla *riduzione* di h si ha:

$$h_{rid} = \frac{h(x)}{MCD(h, h')} = \frac{(x-1)^3(x+1)}{(x-1)^2} = (x-1)(x+1).$$

In base a quanto affermato in precedenza, possiamo concludere che l'ideale associato alla varietà affine definita dai due polinomi f_1 ed f_2, si può scrivere come:

$$\mathcal{I}(\mathcal{V}(I)) =< (x-1)(x+1) > .$$

Capitolo 3

Basi di Groebner

3.1 Introduzione

Nel capitolo precedente abbiamo visto le connessioni tra l'anello dei polinomi $k[x_1, \ldots, x_n]$ e le varietà algebriche affini. In questo capitolo si studiano le basi di Groebner, con relative caratterizzazioni, e l'algoritmo di Buchberger per determinarle. In particolare, verranno risolti i seguenti problemi:

- **Descrizione dell'ideale**: ovvero un ideale I possiede sempre un insieme finito di generatori? In altre parole possiamo scrivere $I = < f_1, \ldots, f_s >$ con $f_i \in k[x_1, \ldots, x_n]$?

- **Problema di appartenenza**: dati nell'anello $k[x_1, \ldots, x_n]$ un polinomio f e un ideale $I =< f_1, \ldots, f_s >$, stabilire quando $f \in I$.

- **Risoluzione di equazioni polinomiali**. Trovare tutte le soluzioni in k^n di un sistema di equazioni polinomiali;

  $$f_1(x_1, \ldots, x_n) = \ldots = f_n(x_1, \ldots, x_n) = 0$$

  Notiamo che il chiedersi se $x = (x_1, \ldots, x_n)$ è soluzione del sistema di equazioni polinomiali è analogo a chiedere se il punto appartenga o meno, alla varietà $\mathrm{V}(f_1, \ldots, f_n)$.

- **Problema di implicitizzazione**. Sia V un sottoinsieme di k^n assegnato parametricamente dalle seguenti equazioni:

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

Se i g_i sono polinomi o funzioni razionali, nelle variabili t_i, l'insieme V sarà una varietà affine o parte di questa. Il problema di implicitizzazione consiste nel determinare equazioni polinomiali in x_i che definiscano la varietà V.

Osservazione.

I problemi nel terzo e quarto punto sono uno inverso dell'altro, infatti il terzo ci chiede di determinare l'insieme delle soluzioni di un sistema di equazioni polinomiali, mentre il quarto consiste nella ricerca del sistema di equazioni che definisca un dato insieme di soluzioni.

Prima di cominciare direttamente lo studio delle basi di Groebner illustriamo alcuni esempi significativi in cui vengono utilizzati algoritmi per risolvere i problemi esposti sopra.

Esempio 1.

Nel caso in cui $n = 1$ il problema di descrizione dell'ideale si risolve molto semplicemente. Sia $I \subset k[x]$, per la proprietà di $k[x]$ di essere principale si può scrivere $I =< g >$ per qualche $g \in k[x]$. Analogamente il problema di appartenenza in $k[x]$ si risolve con l'algoritmo di divisione, o meglio assegnato $f \in k[x]$ per verificare quando $f \in I =< g >$, si divide f per g:

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

dove $q, r \in k[x]$ e $r = 0$ o $deg(r) < deg(g)$.

Si vede che $f \in I$ se e soltanto se $r = 0$. Riassumendo, in $k[x]$ abbiamo un algoritmo, precisamente quello di divisione, che ci permette di risolvere il problema di appartenenza.

Vediamo cosa accade se il numero di variabili è maggiore di uno.

Esempio 2.

Sia n uguale ad un numero arbitrario di variabili e vogliamo risolvere il seguente Sistema Lineare Non Omogeneo (in breve SLNO) di equazioni

polinomiali tutte di primo grado:

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

In forma matriciale scriveremo tale SLNO

$$AX = B$$

ove $A = (a_{ij})$ $(i = 1, \ldots, m,\ j = 1, \ldots, n)$ è la matrice ad m righe ed n colonne costituita dai coefficienti del sistema, $X = (x_1, \ldots, x_n)^t$ e $B = (b_1, \ldots, n_n)^t$ sono le matrici verticali (ad n righe ed 1 colonna) costituite rispettivamente dalle incognite $x_1, \ldots, x_n$ e dai termini noti $b_1, \ldots, b_m$, e il prodotto AX è il prodotto righe per colonne. La matrice "orlata" del sistema $(A \mid B)$ (di tipo $m \times (n+1)$) si riduce facilmente a *scala* tramite una successione di operazioni elementari sulle righe (e/o colonne) di uno dei seguenti tipi:

- R_{ij} $[C_{ij}]$ che consiste nello scambiare tra di loro le righe [colonne] i-esima e j-esima;
- $R_i(c)$ $[C_i(c)]$ che consiste nel sostituire alla riga [colonna] i-esima la riga [colonna] i-esima moltiplicata per $c \in k$;
- $R_{ij}(c)$ $[C_{ij}(c)]$ che consiste nel sostituire alla riga [colonna] i-esima la somma della la riga [colonna] i-esima e della riga [colonna] j-esima moltiplicata per $c \in k$;

Ricordiamo che una matrice si dice *a scala* se in ogni riga il primo elemento non nullo da sinistra è uguale ad 1 e gli elementi nella colonna contenente tale 1 direttore che si trovano al di sotto di esso sono nulli.

Ad esempio consideriamo, nel caso $n = 3$, il seguente sistema

$$\begin{cases} 2x_1 + 3x_2 - x_3 = 0 \\ x_1 + x_2 - 1 = 0 \\ x_1 + x_3 - 3 = 0 \end{cases}$$

Un sistema di questo tipo, può essere risolto utilizzando l'algoritmo di Gauss-Jordan, che partendo dalla matrice orlata del sistema lineare, effettuando

operazioni elementari sulle righe permette di ottenere la seguente matrice a scala:

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

La forma di questa matrice mostra che x_3 è una variabile libera, ponendo $x_3 = t$ si ha:

$$\begin{aligned} x_1 &= -t + 3 \\ x_2 &= t - 2 \\ x_3 &= t \end{aligned}$$

Queste sono le equazioni parametriche di una retta $\mathbf{L}$ in k^3. Il sistema di equazioni scritto inizialmente rappresenta $\mathbf{L}$ come varietà affine.

Tornando al caso generale si opera in modo analogo effettuando una riduzione a scala della matrice orlata del sistema $AX = B$

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

Riducendo la matrice a scala possiamo trovare tutte le soluzioni del sistema originario, tramite sostituzione di valori nelle variabili libere. In alcuni casi potrà esserci una o nessuna soluzione. Quest'ultimo caso accade, ad esempio, se la matrice contiene una riga $(0, \dots, 0, 1)$, corrispondente all'equazione incompatibile $0 = 1$.

Esempio 3.

Consideriamo un n arbitrario e un sottoinsieme $\mathbf{V}$ di k^n, assegnato parametricamente dalle seguenti equazioni:

$$\begin{cases} x_1 = a_{11}t_1 + \ldots + a_{1m}t_m + b_1 \\ \vdots \\ x_n = a_{n1}t_1 + \ldots + a_{nm}t_m + b_n. \end{cases}$$

Si vede che $\mathbf{V}$ è una varietà affine, sottospazio lineare di k^n, in quanto $\mathbf{V}$ è immagine dell'applicazione $F : k^m \longrightarrow k^n$ definita da:

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

Questa è una applicazione lineare seguita da una traslazione. Indicata con $T = (t_1, \ldots, t_m)^t$ la matrice verticale costituita dalle coordinate del punto generico di k^m, si può rappresentare la $F(T) = X$ nella forma matriciale

$$X = AT + B,$$

ove $A = (a_{ji})$ $(j = 1, \ldots, n,\ i = 1, \ldots, m)$, $X = (x_1, \ldots, x_n)^t$ e $B = (b_1, \ldots, b_n)^t$. Consideriamo, in questo caso, il problema di implicitizzazione. In altre parole ricerchiamo un sistema di equazioni lineari che abbia per soluzioni i punti di $\mathbf{V}$. Detta I_n la matrice unità di ordine n, la $X = AT + B$ si può scrivere

$$AT - I_n X = -B$$

che si può considerare un SLNO di n equazioni nelle $m + n$ incognite

$$(t_1, \ldots, t_m, x_1, \ldots, x_n).$$

Riducendo a scala la matrice orlata $n \times (m + n + 1)$

$$(A \mid -I_n \mid -B),$$

si otterrà un sistema a scala in cui le ultime righe coinvolgono solo le variabili $(x_1, \ldots, x_n)$ queste righe dànno le equazioni cartesiane della varietà.

Ad esempio si consideri il sottospazio lineare $\mathbf{V} \subset k^4$ definito da:

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

Riducendo a scala la matrice orlata

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

si ottiene:

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & -1 & 4 \\ 0 & 0 & 1 & 1 & -1 & 0 & 6 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & -3 \end{pmatrix}$$

Se consideriamo le ultime due righe della matrice sopra scritta possiamo ricavare le seguenti due equazioni

$$\begin{aligned} x_1 + x_2 - x_3 - 6 &= 0 \\ x_2 - (3/4)x_3 + (1/2)x_4 + 3 &= 0. \end{aligned}$$

che definiscono $\mathbf{V}$ in k^4.

Utilizzando il metodo di eliminazione di Gauss-Jordan si ha dunque una soluzione algoritmica per il problema di implicitizzazione. Il nostro obiettivo sarà quello di sviluppare ed estendere i metodi usati in questi esempi a sistemi di equazioni polinomiali di ogni grado e di ogni numero di variabili. Quello che vedremo è il metodo delle basi Groebner (che si può vedere come una specie di "combinazione" della riduzione a scala e della divisione per polinomi in più variabili). Questo metodo ci permetterà di gestire i problemi citati all'inizio del paragrafo.

3.2 Ordinamento monomiale

Se esaminiamo in dettaglio l'algoritmo di divisione in $k[x]$ e quello di Gauss-Jordan per sistemi di equazioni lineari, possiamo constatare che il fulcro principale è l'ordinamento dei termini del polinomio. Ad esempio se vogliamo dividere $f(x) = x^5 - 3x^2 + 1$ per $g(x) = x^2 - 4x + 7$, polinomi appartenenti a $k[x]$, i passi fondamentali sono:

- Scrivere i termini dei polinomi in ordine decrescente rispetto al grado della x.
- Se il termine di grado massimo di $f(x)$ è divisibile per il termine di grado massimo di $g(x)$, allora si sottrae $[LT(f)/LT(g)] \cdot g(x) = x^3 \cdot g(x)$, al fine di cancellare il termine di grado massimo di $f(x)$.
- Si ripete tale processo fino ad ottenere un polinomio di grado minore di due.

Per l'algoritmo di divisione è quindi utile come ordinamento dei monomi in una variabile

$$\ldots > x^{m+1} > x^m > \ldots > x > 1.$$

Il successo dell'algoritmo consiste in un lavoro sistematico, con i termini di grado massimo sia di $f(x)$ che di $g(x)$ e non in una rimozione a caso dei termini di f con i termini di g.

Analogamente, nella riduzione a scala di una matrice si opera sistematicamente sulle righe fino ad ottenere la forma desiderata. Si deve però ricordare che il tutto viene svolto usando il seguente ordinamento delle variabili

$$x_1 > x_2 \ldots > x_n.$$

Da tali considerazioni emerge la necessità di introdurre il concetto di ordinamento monomiale.

I monomi appartenti all'anello $k[x_1, \ldots, x_n]$ possono essere considerati in corrispondenza biunivoca con gli elementi di $\mathbf{Z}^n_{\geq 0}$, insieme delle n-ple ordinate costituite da interi non negativi. Infatti al monomio:

$$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n},$$

possiamo associare la n-pla ordinata di interi non negativi $(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}^n_{\geq 0}$.

Definizione 3.2.1 *Un ordine monomiale in $k[x_1, \ldots, x_n]$ è una relazione $>$ su $\mathbf{Z}^n_{\geq 0}$ tale che:*

1. *$>$ è un ordine totale, ossia per ogni coppia α, β si avrà necessariamente una delle seguenti relazioni*

$$\alpha = \beta$$
$$\alpha < \beta$$
$$\alpha > \beta$$

2. *$>$ è compatibile con la moltiplicazione in $k[x_1, \ldots, x_n]$, ossia:*

$$\forall \alpha, \beta, \gamma \in \mathbf{Z}^n_{\geq 0} \text{ se risulta } \alpha > \beta \text{ allora } \alpha + \gamma > \beta + \gamma$$

3. *$>$ è un buon ordinamento o equivalentemente ogni sottoinsieme non vuoto di $\mathbf{Z}^n_{\geq 0}$ possiede un elemento minimo.*

La terza condizione serve ad assicurare che gli algoritmi terminano.

Lemma 3.2.1 *Una relazione d'ordine su $\mathbf{Z}^n_{\geq 0}$ è un buon ordinamento se e soltanto se ogni successione strettamente decrescente in $\mathbf{Z}^n_{\geq 0}$*

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

termina.

Dimostrazione. Per dimostrare il lemma dimostreremo la seguente affermazione:

> "$>$ non è un buon ordinamento se, e soltanto se, esiste una successione infinita strettamente decrescente in $\mathbf{Z}^n_{\geq 0}$".

Se $>$ non è un buon ordinamento allora esiste qualche sottoinsieme non vuoto $S \subset \mathbf{Z}^n_{\geq 0}$ che non possiede un elemento minimo. Prendiamo $\alpha(1) \in S$, per quanto detto prima, tale elemento non risulterà il minimo allora possiamo trovare un altro elemento $\alpha(2) \in S$ tale che risulti $\alpha(1) > \alpha(2)$ in S. Ma anche $\alpha(2)$ non sarà il minimo di S, quindi possiamo ancora considerare un altro elemento $\alpha(3) \in S$ tale che $\alpha(2) > \alpha(3)$; continuando con tale procedimento otteniamo una successione strettamente decrescente infinita:

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

Per dimostrare l'implicazione inversa consideriamo una successione strettamente decrescente infinita. L'insieme

$$S = \{\alpha(1), \alpha(2), \alpha(3), \dots\}.$$

è un sottoinsieme non vuoto di $\mathbf{Z}^n_{\geq 0}$ che non possiede minimo, quindi $>$ non è un buon ordinamento. ∎

Osservazione.

In qualunque ordine monomiale $1 < x^\alpha \ \forall \alpha$.

Infatti, se per assurdo fosse $1 > x^\alpha$ moltiplicando per x^α si avrebbe $x^\alpha > x^{2\alpha}$ e continuando a moltiplicare per x^α si otterrebbe $1 > x^\alpha > x^{2\alpha} > x^{3\alpha} > \dots > x^{n\alpha} > \dots$ in contraddizione con il fatto che un ordinamento monomiale è un buon ordinamento.

Osservazione.

Se x^α divide x^β, in qualunque ordinamento monomiale, allora $x^\alpha \leq x^\beta$. Quindi ogni ordine monomiale può essere concepito come raffinamento dell'ordine parziale definito dalla divisibilità.

Definizione 3.2.2 Ordinamento lessicografico (LEX).
Siano $\alpha = (\alpha_1, \dots, \alpha_n)$ e $\beta = (\beta_1, \dots, \beta_n) \in \mathbf{Z}^n_{\geq 0}$. Diremo che $\alpha >_{lex} \beta$ se il vettore differenza $\alpha - \beta$ ha come primo elemento, non nullo, partendo da sinistra, un numero positivo.

Scriveremo:

$$x^{\alpha} >_{lex} x^{\beta} \quad se \quad \alpha >_{lex} \beta$$

Sostanzialmente in questo caso $x_1 > x_2 > \ldots > x_n$ e si ordina rispetto alle potenze decrescenti di x_1, per termini con la stessa potenza di x_1 si guarda alla x_2 e si ordina rispetto alle potenze decrescenti di x_2, etc.

Esempio.

Consideriamo i seguenti monomi: $x^{\alpha} = x^3y^2z$, $x^{\beta} = x^2y^5z^7$.
Avremo quindi: $\alpha = (3, 2, 1)$ mentre $\beta = (2, 5, 7)$ e il vettore differenza sarà $\alpha - \beta = (1, -3, -6)$ allora si può concludere che:

$$x^3y^2z >_{lex} x^2y^5z^7.$$

Proposizione 3.2.1 *L'ordinamento lessicografico in* $\mathbf{Z}^n_{\geq 0}$ *è un ordine monomiale.*

Dimostrazione. Per dimostrare che LEX è un ordinamento monomiale si devono verificare le tre proprietà che caratterizzano un ordinamento monomiale.

(i) LEX è un ordine totale come segue direttamente dalla definizione. Infatti l'usuale ordine numerico in $\mathbf{Z}_{\geq 0}$ è un ordine totale.

(ii) Se $\alpha >_{lex} \beta$ allora in $\alpha - \beta$ il primo elemento non nullo da sinistra è positivo. Ma $x^{\alpha} \cdot x^{\gamma} = x^{\alpha+\gamma}$ e $x^{\beta} \cdot x^{\gamma} = x^{\beta+\gamma}$. Allora in $(\alpha+\gamma)-(\beta+\gamma) = \alpha-\beta$ il primo elemento non nullo da sinistra è lo stesso che in $\alpha - \beta$ e, come tale è positivo. Questo prova la compatibilità di LEX con la moltiplicazione.

(iii) Si deve verificare che LEX è un buon ordinamento. Supponiamo per assurdo che ciò non sia vero. Per il Lemma 3.2.1 dovrebbe esistere una successione strettamente decrescente infinita

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

di elementi di $\mathbf{Z}^n_{\geq 0}$. Questo porta ad una contraddizione. Consideriamo, infatti, i primi elementi dei vettori $\alpha(i) \in \mathbf{Z}^n_{\geq 0}$. Per la definizione di ordinamento lessicografico, questi elementi formano una successione non crescente di interi non negativi e poiché $\mathbf{Z}_{\geq 0}$ è ben ordinato, i primi elementi di $\alpha(i)$ devono stabilizzarsi, ovvero esiste un elemento k tale che le prime componenti di $\alpha(i)$, con $i \geq k$, sono tutte uguali. Analogo discorso può essere fatto per il secondo elemento di $\alpha(i)$, ottenendo sempre una successione non crescente che si stabilizza. Continuando allo stesso modo si vede che per qualche l, $\alpha(l)$, $\alpha(l+1) \cdots$ sono tutti uguali. Questo naturalmente contraddice il fatto che $\alpha(l) > \alpha(l+1)$. ∎

Osservazione.

E' importante comprendere che esistono molti ordinamenti lessicografici, a seconda di come vengono ordinate le variabili. Abbiamo sopra definito l'ordinamento lessicografico corrispondente all'ordinamento $x_1 > x_2 > x_3 > \ldots > x_n$ delle variabili. Dando un altro ordine alle variabili $x_1, \ldots, x_n$ possiamo ottenere un ordinamento lessicografico diverso. Ad esempio date le variabili x, y, z possiamo definire LEX con $x > y > z$ ma anche $x > z > y$ o con $y > x > z$ etc.

In generale, avendo n variabili possiamo definire ben $n!$ ordini lessicografici. Nel seguito, quando parleremo di un ordinamento senza specificare l'ordine fissato per le variabili intenderemo sempre di considerare quello corrispondente a $x_1 > x_2 > x_3 > \ldots > x_n$.

Definizione 3.2.3 Ordinamento lessicografico graduato (DEGLEX). *Siano $\alpha, \beta \in \mathbf{Z}^n_{\geq o}$. Diremo che $\alpha \geq_{deglex} \beta$ se:*

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

Sostanzialmente si ordina prima rispetto al grado, poi, per monomi dello stesso grado si ordina rispetto all'ordinamento lessicografico.

Esempio.

Consideriamo i seguenti monomi: xy^2z^3 e x^3y^2. In base alla definizione precedente possiamo concludere che $(1,2,3) >_{deglex} (3,2,0)$, infatti $|(1,2,3)| = 6 > |(3,2,0)| = 5$. Mentre per i monomi dello stesso grado x^2 e z^2, se $x > y > z$ è l'ordine scelto per le variabili si avrà $x^2 >_{deglex} z^2$.

Definizione 3.2.4 Ordinamento lessicografico graduato inverso (DEGREVLEX). *Siano $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$. Diremo che $\alpha >_{degrevlex} \beta$ se:*

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

il primo elemente non nullo da destra è negativo.

Sostanzialmente, prima si ordinano i monomi rispetto al grado e poi, a parità di grado, rispetto alle potenze crescenti della variabile più piccola.

Esempio.

Consideriamo i seguenti monomi x^4y^7z e $x^4y^2z^3$. Risulta $(4,7,1) >_{degrevlex} (4,2,3)$. Infatti, $|(4,7,1)| = 12 > |(4,2,3)| = 9$. Se invece prendiamo i monomi xy^5z^2 e x^4yz^3 poiché risulta $|(1,5,2)| = |(4,1,3)|$ e $\alpha - \beta = (-3,4,-1)$ si ha:

$$(1,5,2) >_{degrevlex} (4,1,3)$$

ovvero $xy^5z^2 >_{degrevlex} x^4yz^3$.

Osservazione.

Un ordine monomiale si dice graduato se $x^\alpha > x^\beta$ quando $|\alpha| > |\beta|$. DEGLEX e DEGREVLEX sono ordinamenti graduati mentre LEX non lo è; anche per questi esistono $n!$ possibili modi per definirli, e si dimostra che valgono le 3 condizioni della definizione di ordinamento monomiale, il che viene lasciato per esercizio al lettore.

Vediamo ora come un ordinamento monomiale ci permette di ordinare senza ambiguità i termini di un polinomio $f = \sum_\alpha a_\alpha x^\alpha$ di $k[x_1, \ldots, x_n]$.

Ad esempio, se abbiamo $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x,y,z]$ e $x > y > z$. Con LEX otteniamo:

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

Con DEGLEX

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

Con DEGREVLEX

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

Useremo la seguente terminologia.

Definizione 3.2.5 *Fissato un ordine monomiale $>$, sia f un polinomio non nullo di $k[x_1, \ldots, x_n]$. Il* **multigrado** *di f, è:*

$$multideg(f) = max(\alpha \in \mathbf{Z}^n_{\geq 0} \mid a_\alpha \neq 0)$$

Il coefficiente direttore (in inglese, **leading coefficient***) di f è:*

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

Il monomio direttore (in inglese, **leading monomial***) di f è:*

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

Il termine direttore (in inglese, **leading term** *di f) è:*

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

Per comprendere meglio questa serie di definizioni possiamo considerare il seguente:

Esempio.

Per il polinomio $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$, sopra considerato, risulta, rispetto all'ordinamento lessicografico:

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

Non è difficile provare, per esercizio, che

Lemma 3.2.2 *Siano f, g polinomi non nulli di $k[x_1, \ldots, x_n]$. Risulta:*

$$multideg(fg) = multideg(f) + multiged(g).$$

Se $f + g \neq 0$, allora

$$multideg(f+g) \leq max\ (multideg(f),\ multideg(g)).$$

dove vale il segno uguale quando $multideg(f) \neq multideg(g)$

3.3 Algoritmo di divisione

Nel Capitolo 1 abbiamo visto come l'algoritmo di divisione poteva essere utilizzato per risolvere il problema di appartenenza di un polinomio ad un ideale, nel caso dell'anello dei polinomi ad una sola indeterminata. Per studiare tale problema in più variabili, formuleremo un algoritmo di divisione per polinomi di $k[x_1, \ldots, x_n]$ che generalizza quello noto in $k[x]$.

Il nostro obiettivo principale è quello di poter definire in $k[x_1, \ldots, x_n]$ la divisione di f per $f_1, \ldots, f_s$, ossia vogliamo poter scrivere:

$$f = a_1f_1 + \ldots + a_sf_s + r$$

dove il *dividendo* f, i *divisori* $f_1, \ldots, f_s$, i *quozienti* $a_1, \ldots, a_s$ e il *resto* r appartengano tutti all'anello $k[x_1, \ldots, x_n]$.

L'idea alla base dell'algoritmo è simile a quella del caso di una variabile. Per comprendere meglio come si opera forniamo il seguente:

Esempio.

Consideriamo $f = xy^2 + 1$, $f_1 = xy + 1$, $f_2 = y + 1$ e utilizziamo come ordinamento monomiale quello lessicografico, con $x > y$. Si vuole seguire lo schema della divisione per polinomi in una indeterminata, con la differenza che si ha un numero maggiore di divisori e quozienti. In questo caso particolare, i divisori sono: f_1, f_2 e i quozienti, da determinare, saranno a_1, a_2. Graficamente possiamo rappresentare tale situazione nel modo seguente:

$xy^2 + 1$	$xy + 1$	$y + 1$	RESTO
$-xy^2 - y$	y		

Il leading term di f_1 è xy e quello di f_2 è y, ordiniamo i divisori utilizzando prima f_1 e poi f_2. Dividiamo xy^2 per xy scrivendo y come primo quoziente e sottraendo $y \cdot f_1$ da f

$xy^2 + 1$	$xy + 1$	$y + 1$	RESTO
$-xy^2 - y$	y		
$-y + 1$			

Ripetiamo ora il processo per $-y+1$; questa volta dobbiamo però usare il polinomio f_2 perché $LT(f_1) = xy$ non divide il $LT(-y+1) = -y$. Otteniamo:

xy^2+1	$xy+1$	$y+1$	RESTO
$-xy^2-y$	y	-1	
$-y+1$			
$y+1$			
2			2

A questo punto $LT(f_1)$ e $LT(f_2)$ non dividono 2 allora $r = 2$ passa alla colonna dei resti e possiamo scrivere il polinomio f nel seguente modo:

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

Proviamo ora a cambiare l'ordine dei divisori e vediamo cosa accade:

xy^2+1	$y+1$	$xy+1$	RESTO
$-xy^2-xy$	$xy-x$		
$-xy+1$			
$xy+x$			
$x+1$			$x+1$

Si può pertanto scrivere:

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

Questo esempio mostra come *l'espressione di f può variare cambiando l'ordine dei divisori.*

Teorema 3.3.1 *Fissato un ordimanento monomiale in* $\mathbf{Z}^n_{\geq 0}$ *consideriamo una s-pla ordinata* $F = (f_1, \ldots, f_s)$ *di polinomi in* $k[x_1, \ldots, x_n]$. *Ogni* $f \in k[x_1, \ldots, x_n]$ *può essere scritto come:*

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

dove $a_i, r \in k[x_1, \ldots, x_n]$ *e* $r = 0$ *oppure* r *è combinazione k-lineare di monomi, nessuno dei quali è divisibile per uno dei* $LT(f_1), \ldots, LT(f_s)$. *Chiameremo* r *il* **resto** *della divisione di* f *per* F. *Inoltre, se* $a_i f_i \neq 0$ *si ha*

$$\text{multideg(f)} \geq \text{multideg}(\text{a}_\text{i}\text{f}_\text{i}).$$

Dimostrazione. Proveremo l'esistenza di $a_1, \ldots, a_s, r$ fornendo l'algoritmo che permette di determinarli e dimostrando che tale algoritmo opera correttamente.

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0,\ r := 0$
$p := f$

WHILE $p \neq 0$ DO
$i := 1$
division.occurred:=false
WHILE $i \leq s$ AND division.occurred:=false
DO
IF $LT(f_i)$ divides $LT(p)$ THEN
$a_i := a_i + LT(p)/LT(f_i)$
$p := p - (LT(p)/LT(f_i))f_i$
division.occured:=true
ELSE
$i := i + 1$
IF division.occurred:=false THEN
$r := r + LT(p)$
$p := p - LT(p)$

Verifichiamo che l'algoritmo di divisione sopra dato opera correttamente, ossia che

(a) L'algoritmo funziona.

(b) L'algoritmo termina.

Osserviamo preliminarmente che la variabile p rappresenta il dividendo intermedio in ciascuno dei passi dell'algoritmo, la variabile r rappresenta il resto ed è nella colonna di destra e le variabili $a_1, \ldots, a_s$ sono i quozienti, elencati sotto a ciascuno dei divisori $f_1, \ldots, f_s$. Infine, la variabile booleana "division.occurred ci dice quando qualche $LT(f_i)$ divide il leading term del dividendo intermedio. E' facile verificare che ogni volta che si attraversa il WHILE ... DO viene eseguito uno solo dei due passi seguenti:

- (Passo di divisione) Se qualche $LT(f_i)$ divide $LT(p)$, l'algoritmo procede come nel caso di una variabile.
- (Passo di formazione del resto) Se nessun $LT(f_i)$ divide $LT(p)$ l'algoritmo aggiunge $LT(p)$ al resto e lo sottrae da p

(a) Per dimostrare che *l'algoritmo funziona*, verifichiamo che la

$$f = a_1 f_1 + \ldots + a_s f_s + p + r, \tag{3.1}$$

sussiste ad ogni passo. Questo è chiaramente vero per i valori iniziali $a_1 = \ldots = a_s = r = 0$ e $f = p$. Supponiamo che l'uguaglianza sopra scritta sia soddisfatta ad un generico passo dell'algoritmo e dimostriamo che questa rimane inalterata anche al passo successivo. Se risulta che qualche $LT(f_i)$ divide $LT(p)$ cioè il passo successivo è di divisione per f_i, gli unici termini che cambiano nella (3.1) sono a_i, che diventa $a_i + LT(p)/LT(f_i)$ e p, che diventa $p - [LT(p)/LT(f_i)]f_i$, gli altri termini restano inalterati. Ma aggiungendo e togliendo ad $a_i f_i + p$ il termine $[LT(p)/LT(f_i)]f_i$ la somma $a_i f_i + p$ non cambia e

$$a_i f_i + p = (a_i + \tfrac{LT(p)}{LT(f_i)})f_i + (p - \tfrac{LT(p)}{LT(f_i)}f_i)$$

mostra che $a_i f_i + p$ rimane inalterato e la (3.1) resta valida.

Se invece il passo successivo è un passo di formazione del resto (ossia se $LT(f_i)$ non divide $LT(p)$), allora p ed r cambiano in $p - LT(p)$ e $r + LT(p)$, ma la loro somma $p + r$ resta inalterata in quanto

$$p + r = (p - LT(p)) + (r + LT(p)).$$

L'algoritmo si ferma quando $p = 0$; in tale situazione allora la (2.1) diventerà:

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

Poiché si aggiungono termini al resto solo quando non sono divisibili per nessuno dei $LT(f_i)$, quando l'algoritmo termina $a_1, \ldots, a_s$ e r hanno le proprietà richieste.

(b) Per dimostrare che *l'algoritmo termina*, osserviamo che ogni volta che ridefiniamo p, o il multigrado diminuisce, oppure p diventa zero. Infatti, in un passo di divisione p è ridefinito come

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

e, per per il Lemma 3.2.2 risulta

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

Quindi p e $[LT(p)/LT(f_i)]f_i]$ hanno lo stesso termine direttore, per cui la loro differenza p' ha un multigrado strettamente minore se $p' \neq 0$.

Durante un passo di formazione del resto, p è ridefinito come

$$p' = p - LT(p)$$

e, ovviamente $multideg(p') < multideg(p)$ quando $p' \neq 0$.

In entrambi i casi il multigrado deve decrescere. Se l'algoritmo non terminasse si avrebbe una successione decrescente infinita di multigradi, il che è assurdo, per l'ipotesi di buon ordinamento di $>$ (cfr. il Lemma 3.2.1). Dopo un numero finito di passi, necessariamente p diventa zero e l'algoritmo termina.

Resta da studiare la relazione tra il multigrado di f e quello di $a_i f_i$. Ogni termine in a_i è del tipo $LT(p)/LT(f_i)$ per qualche valore della variabile p che, inizialmente, è f. Si è appena dimostrato che il multigrado di p diminuisce quindi $LT(p) \leq LT(f)$. Ne segue facilmente (come si può verificare per esercizio, usando il fatto che un ordine monomiale è compatibile), che se $a_i f_i \neq 0$ risulta

$$multideg(a_i f_i) \leq multideg(f),$$

il che completa la dimostrazione del Teorema. ∎

Osservazioni.

È sorprendente, dato che l'algebra usata è del tipo di quella studiata alla scuola media inferiore, che questo algoritmo sia stato individuato ed utilizzato solo negli ultimi cinquanta anni. Purtroppo non ha le stesse buone proprietà dell'algoritmo di divisione per polinomi in una indeterminata e raggiunge il massimo della sua potenzialità solo se accoppiato con il metodo delle basi di Groebner che, come vedremo nei paragrafi successivi, sono sostanzialmente le basi "buone" rispetto all'algoritmo di divisione (nel senso

che il resto sarà univocamente determinato qualunque sia l'ordine in cui si esegue la divisione). Non solo, siano, ad esempio, $f_1 = xy + 1,\ f_2 = y^2 - 1$. Dividendo $f = xy^2 - x$ per $F = (f_1, f_2)$ si ottiene

$$f = yf_1 + 0f_2 + (-x - y) \tag{3.2}$$

mentre eseguendo la divisione per $F' = (f_2, f_1)$ si ha

$$f = xf_2 + 0f_1 + 0.$$

Ciò mostra che $f \in I =< f_1, f_2 >$, ma da (3.2) segue che $r = 0$ non è una condizione necessaria per l'appartenenza di f a I ma è solo sufficiente. Vedremo che le basi di Groebner sono basi di ideali per cui tale condizione diventa necessaria e sufficiente.

3.4 Ideali monomiali e Lemma di Dickson

In questo paragrafo risolveremo il problema di descrizione dell'ideale nel caso particolare di ideali monomiali.

Definizione 3.4.1 *Un ideale $I \subset k[x_1, \ldots, x_n]$ è un* **ideale monomiale** *se esiste un sottoinsieme $A \subseteq \mathbf{Z}^n_{\geq 0}$ (eventualmente infinito) tale che I è costituito da polinomi del tipo*

$$\sum_{i=1}^{s} h_{\alpha(i)} x^{\alpha(i)}, \text{con } h_{\alpha(i)} \in k[x_1, \ldots, x_n], \forall i = 1, \ldots, s$$

e per $\alpha(i) \in A$. In tal caso, scriveremo

$$I =< x^\alpha \mid \alpha \in A \subseteq \mathbf{Z}^n_{\geq 0} >$$

Un esempio di ideale monomiale è: $I =< x^4y^2, x^3y, x^5y^2 > \subset k[x, y]$.

Il seguente lemma caratterizza i monomi appartenenti ad un ideale monomiale.

Lemma 3.4.1 *Sia $I =< x^\alpha \mid \alpha \in A \subseteq \mathbf{Z}^n_{\geq 0} >$ un ideale monomiale. Il monomio $x^\beta \in I$ se e soltanto se x^β è divisibile per qualche x^α con $\alpha \in A$.*

Dimostrazione. Se x^β è multiplo di qualche x^α per qualche $\alpha \in A$ allora $x^\beta \in I$, per definizione di ideale.

Viceversa, se $x^\beta \in I$, allora

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)} \tag{3.3}$$

dove $h_i \in k[x_1, \ldots, x_n]$ e $\alpha(i) \in A$. Ma h_i è una combinazione lineare di monomi; quindi, distribuendo i prodotti $h_i x^{\alpha(i)}$ si vede che ogni termine che figura nel secondo membro della (3.3) è divisibile per qualche $x^{\alpha(i)}$. Ma allora anche ogni monomio che figura a primo membro della (3.3) deve godere della stessa proprietà. ∎

Osservazione.

Se x^β è divisibile per x^α allora $x^\beta = x^\alpha x^\gamma$ per qualche $\gamma \in \mathbf{Z}^n_{\geq 0}$, questo è equivalente a scrivere $\beta = \alpha + \gamma$. Pertanto l'insieme:

$$\alpha + \mathbf{Z}^n_{\geq 0} = \{\alpha + \gamma \mid \gamma \in \mathbf{Z}^n_{\geq 0}\}$$

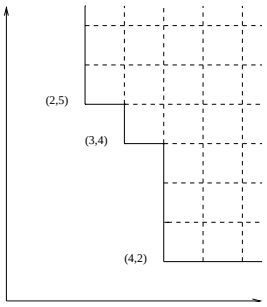
è costituito dagli esponenti di tutti i monomi divisibili per il monomio x^α. Questa osservazione e il lemma 3.4.1 permettono di ricavare una rappresentazione grafica degli ideali monomiali, tenendo conto della corrispondenza biunivoca tra gli esponenti dei monomi e i punti di k^n. Ad esempio, se

$$I =< x^2y^5, x^3y^4, x^4y^2 > .$$

Gli esponenti dei monomi di I formano l' insieme:

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

che è l'unione dei punti a coordinate intere nelle tre copie traslate del primo quadrante nel piano



$x^2y^5 \leftrightarrow (2,5)$
$x^3y^4 \leftrightarrow (3,4)$
$x^4y^2 \leftrightarrow (4,2)$

Tutti i punti a coordinate intere che si trovano nella zona in alto a destra della poligonale disegnata sono esponenti di monomi appartenenti ad I.

Mostriamo ora che un polinomio appartenente ad un ideale monomiale è determinato dai suoi monomi.

Lemma 3.4.2 *Siano I un ideale monomiale e f in $k[x_1, \ldots, x_n]$. Le seguenti affermazioni sono equivalenti*

(i) $f \in I$.

(ii) Ogni termine di f è in I.

(iii) f è combinazione k-lineare di monomi di I.

Dimostrazione. Le implicazioni (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) sono banali. La dimostrazione della (i) $\Rightarrow$ (iii) è simile a quella del Lemma 3.4.1. Precisamente, sviluppando i prodotti $h_{\alpha(i)}x^{\alpha(i)}$ che figurano nel secondo membro della (3.3)

si vede che ogni termine di f è combinazione k-lineare di monomi del tipo $x^{\gamma+\alpha(i)}$ con $\alpha(i) \in A$. Tali monomi, per il Lemma 3.4.1 sono tutti in I. ∎

Una conseguenza immediata di (iii) è che un ideale monomiale è univocamente determinato dai suoi monomi.

Corollario 3.4.1 *Due ideali monomiali coincidono se e solo se contengono gli stessi monomi.*

Il risultato principale di questo paragrafo è che tutti gli ideali monomiali sono finitamente generati.

Teorema 3.4.1 Lemma di Dickson *Un ideale monomiale*

$$I =< x^\alpha \mid \alpha \in A >\leq k[x_1, \ldots, x_n]$$

può essere scritto nella forma

$$I =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$$

ove $\alpha(1), \ldots, \alpha(s) \in A$. *In particolare,* I *è a base finita.*

Dimostrazione. La dimostrazione è per induzione sul numero delle variabili. Se $n = 1$, I è generato da monomi x^α, con $\alpha \in A \subset \mathbf{Z}_{\geq 0}$. Se β è il minimo di A, allora x^β divide tutti gli altri generatori dell'ideale, quindi

$$I =< x^\beta > .$$

Sia ora $n > 1$ e si supponga vero il teorema per gli ideali monomiali dell'anello $k[x_1, \ldots, x_{n-1}]$. Posto per comodità $x_n = y$, i monomi di $k[x_1, \ldots, x_{n-1}, y]$ si possono scrivere come $x^\alpha y^m$, essendo $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbf{Z}_{\geq 0}^{n-1}$ e $m \in \mathbf{Z}_{\geq 0}$.

Per determinare i generatori di un ideale monomiale $I \subset k[x_1, \ldots, x_{n-1}, y]$ consideriamo l'ideale J di $k[x_1, \ldots, x_{n-1}]$ generato dai monomi x^α per i quali risulta $x^\alpha y^m \in I$ per qualche $m \geq 0$. Essendo J un ideale monomiale in $k[x_1, \ldots, x_{n-1}]$, per ipotesi induttiva J è a base finita, e pertanto:

$$J =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} > .$$

L'ideale J si può considerare la *proiezione* di I in $k[x_1, \ldots, x_{n-1}]$.

Per ogni fissato i, con $1 \leq i \leq s$, 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 tra gli m_i. Per ogni indice h tra 0 e $m-1$, consideriamo l'ideale $J_h \leq k[x_1, \ldots, x_{n-1}]$, generato dai monomi

x^β tali che $x^\beta y^h \in I$. Per comprendere meglio possiamo pensare J_h come la porzione di I generata dai monomi che contengono y esattamente alla potenza h-esima. Usando nuovamente l'ipotesi induttiva J_h ha un numero finito s_h di monomi generatori

$$J_h =< x^{\alpha_h(1)}, \ldots, x^{\alpha_h(s_h)} >,$$

inoltre, per come è definito J_h,

$$x^{\alpha_h(1)}y^h, \ldots, x^{\alpha_h(s_h)}y^h \ \in \ I.$$

Vogliamo dimostrare che I è generato dagli $s + s_0 + \ldots + s_{m-1}$ monomi della seguente lista in cui figurano scelti

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

Ogni monomio $x^\alpha y^p \in I$ è , infatti, divisibile per un monomio della lista di cui sopra. Questo si vede considerando che: se $p \geq m$, allora $x^\alpha y^p$ è divisibile per qualche $x^{\alpha(i)}y^m$, per costruzione di J; mentre se $p \leq m-1$, il monomio $x^\alpha y^p$ è divisibile per $x^{\alpha_p(j)}y^p$, per costruzione di J_p.

Per completare la dimostrazione resta da far vedere che l'insieme finito di generatori può essere scelto da un assegnato insieme di generatori di I.

Scriviamo di nuovo le variabili come $x_1, \ldots, x_n$ e l'ideale monomiale

$$I =< x^\alpha \mid \alpha \in A >\leq k[x_1, \ldots, x_n].$$

Per quanto sopra dimostrato

$$I =< x^{\beta(1)}, \ldots, x^{\beta(s)} > \text{ per opportuni monomi } x^{\beta(i)} \ \in I.$$

Ciascun $x^{\beta(i)} \in I =< x^\alpha \mid \alpha \in A >$ e quindi, per il Lemma 3.4.1, si ha che esistono $\alpha(1), \ldots, \alpha(t) \in A$ tali che $x^{\beta(i)}$ è divisibile per $x^{\alpha(i)}$ per $i = 1, \ldots, t$. Ne segue

$$I =< x^{\beta(1)}, \ldots, x^{\beta(s)} >\subseteq< x^{\alpha(1)}, \ldots, x^{\alpha(s)} > .$$

Poiché $x^{\alpha(i)} \in I$ è anche, ovviamente,

$$< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >\subseteq I.$$

Pertanto $I =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$. ∎

Per capire meglio la dimostrazione del Teorema 3.4.1, applichiamolo all'ideale considerato precedentemente. Dalla rappresentazione grafica degli esponenti, si vede che la "proiezione è $J =< x^2 >\leq k[x]$. Poiché $x^2y^5 \in I$, si ha $m = 5$. Si ottengono allora le "porzioni J_h, per $0 \leq h \leq 4 = m - 1$ generate dai monomi contenenti y^h:

$$J_0 = J_1 = \{0\}, \quad J_2 = J_3 =< x^4 >, \quad J_4 =< x^3 > .$$

Queste porzioni si vedono facilmente utilizzando la rappresentazione grafica degli esponenti. La dimostrazione del Lemma di Dickson dà quindi

$$I =< x^2y^5, x^4y^2, x^4y^3, x^3y^4 > .$$

Il Lemma di Dickson risolve il *problema di descrizione* per gli ideali monomiali in quanto ci dice che ogni tale ideale ha una base finita. Questo, a sua volta ci permette di risolvere il *problema di appartenenza* di un polinomio ad un ideale monomiale. Precisamente, utilizzando i Lemmi 3.4.1 e 3.4.2 si può dimostrare facilmente che f appartiene ad un ideale monomiale $I =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} >$ se, e solo se, il resto della divisione di f per $x^{\alpha(1)}, \ldots, x^{\alpha(s)}$ è zero.

Il Lemma di Dickson si può anche usare per dimostrare il corollario seguente, estremamente importante per poter provare quando è che un ordinamento totale e compatibile è anche un buon ordinamento e quindi è monomiale.

Corollario 3.4.2 *Sia $>$ una relazione su $\mathbf{Z}^n_{\geq 0}$ soddisfacente le seguenti proprietà:*
(i) $>$ è un ordinamento totale in $\mathbf{Z}^n_{\geq 0}$.
(ii) se $\alpha \geq \beta$ e $\gamma \in \mathbf{Z}^n_{\geq 0}$ allora $\alpha + \gamma \geq \beta + \gamma$.

La relazione $>$ è un buon ordinamento se e soltanto se $\alpha \geq 0$, $\forall \alpha \in \mathbf{Z}^n_{\geq 0}$.

Dimostrazione. $\Rightarrow$: Assumendo che $>$ sia un buon ordinamento, consideriamo il più piccolo elemento α_0 di $\mathbf{Z}^n_{\geq 0}$. Basterà dimostrare che $\alpha_0 \geq 0$. Se fosse $\alpha_0 < 0$, per l'ipotesi (ii), aggiungendo $m\alpha_0$ ad entrambi i lati si avrebbe $(m+1)\alpha_0 < m\alpha_0$. Si costruirebbe così la successione discendente infinita

$$0 > \alpha_0 > 2\alpha_0 > \cdots > m\alpha_0 > (m+1)\alpha_0 > \cdots,$$

il che è assurdo perché contraddice l'ipotesi che $>$ è un buon ordinamento.

$\Leftarrow$: Sia $\alpha \geq 0$ per ogni $\alpha \in \mathbf{Z}^n_{\geq 0}$ e sia A un qualunque insieme non vuoto di $\mathbf{Z}^n_{\geq 0}$. Si deve dimostrare che A è dotato di minimo.

L'ideale monomiale $I =< x^\alpha \mid \alpha \in A >$, per il Lemma di Dickson, è finitamente generato, ovvero esistono $\alpha(1), \ldots, \alpha(s) \in A$ tali che

$$I =< x^{\alpha(1)}, \ldots, x^{\alpha(s)} > .$$

Non è restrittivo supporre (rinumerando eventualmente gli α) che sia

$$\alpha(1) < \alpha(2) < \ldots < \alpha(s).$$

Dimostriamo che $\alpha(1)$ è il minimo di A.

Fissato $\alpha \in A$, risulta $x^\alpha \in I$; quindi, per il Lemma 3.4.1, x^α è divisibile per qualche $x^{\alpha(i)}$. Questo ci dice che

$$\alpha = \alpha(i) + \gamma \text{ con } \gamma \in \mathbf{Z}^n_{\geq 0} \text{ e } \gamma \geq 0$$

Per l'ipotesi risulta $\gamma \geq 0$ e possiamo scrivere:

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

il che implica che $\alpha(1)$ è il minimo di A. ∎

Dal corollario segue che la definizione data di ordine monomiale si può semplificare sostituendo alla condizione di buon ordinamento la condizione, estremamente più semplice da verificare, che $\alpha \geq 0$ per ogni $\alpha \in \mathbf{Z}^n_{\geq 0}$

3.5 Teorema di Hilbert e basi di Groebner

In questo paragrafo risolveremo completamente il problema della descrizione dell'ideale, fornendo una base "buona" rispetto all'algoritmo di divisione.

Definizione 3.5.1 *Sia $I \leq k[x_1, \ldots, x_n]$ un ideale non nullo, e sia assegnato un ordine monomiale. Denotiamo con $LT(I)$ l'insieme di tutti i termini direttori di polinomi di I*

$$LT(I) = \{cx^\alpha \mid \text{esiste } f \in I \text{ con } LT(f) = cx^\alpha\},$$

e con $< LT(I) >$ l'ideale generato dagli elementi di $LT(I)$.

Osservazione

Osserviamo che se $I =< f_1, \ldots, f_s >$, sicuramente

$$< LT(f_1), \ldots, LT(f_s) > \subseteq < LT(I) >,$$

ma non è detto che i due ideali coincidano, come mostra il seguente esempio. Sia

$$I =< \{f_1, f_2\} > =< \{x^3 - 2xy, x^2y - 2y^2 + x\} > .$$

Rispetto all'ordinamento DEGLEX, in $k[x, y]$, risulta

$$xf_2 - yf_1 = x^2 \in I,$$

quindi $x^2 \in < LT(I) >$, ma x^2 non è divisibile né per $LT(f_1) = x^3$, né per $LT(f_2) = x^2y$ e pertanto $x^2 \notin < LT(f_1), LT(f_2) >$, per il Lemma 3.4.1.

Dimostreremo ora che $LT(I)$ è un ideale monomiale, il che permetterà di applicare i risultati del paragrafo precedente. In particolare, ne seguirà che $LT(I)$ è generato da un numero finito di termini direttori.

Proposizione 3.5.1 *Se $I \leq k[x_1, \ldots, x_n]$ è un ideale,*
(i) $< LT(I) >$ è un ideale monomiale.
(ii) Esistono $g_1, \ldots, g_t \in I$ tali che $< LT(I) > =< LT(g_1), \ldots, LT(g_t) >$.

Dimostrazione. I monomi direttori $LM(g)$ di polinomi non nulli $g \in I - \{0\}$ generano l'ideale monomiale $< LM(g) \mid g \in I - \{0\} >$. Poiché, per ogni $g \neq 0$, il monomio direttore e il termine direttore differiscono soltanto per la costante moltiplicativa non nulla $LC(g)$ si vede che

$$LT(g) = LC(g)LM(g), \qquad LM(g) = [LC(g)]^{-1}LT(g),$$

pertanto

$$< LM(g) \mid g \in I - \{0\} >=< LT(g) \mid g \in I - \{0\} >=< LT(I) >,$$

e, quindi, anche $< LT(I) >$ è un ideale monomiale.

Poiché $< LT(I) >$ è generato dai monomi $LM(g)$ con $g \in I - \{0\}$, il Lemma di Dickson ci dice che $< LT(I) >=< LM(g_1), \ldots, LM(g_t) >$ per un numero finito di $g_1, \ldots, g_t$. Ma, di nuovo, $LM(g_i)$ differisce da $LT(g_i)$ per la costante moltiplicativa, $LC(g_i)$, diversa zero. Ne segue che $< LT(I) >=< LT(g_1), \ldots, LT(g_t) >$, il che completa la dimostrazione. ∎

Si può ora usare la Proposizione 3.5.1 e l'algoritmo di divisione per dimostrare l'esistenza di un insieme finito di generatori per *ogni* ideale polinomiale, dando così risposta affermativa al *problema di descrizione dell'ideale*. Come sempre, si suppone fissato, una volta per tutte, un particolare ordine monomiale da utilizzare nell'algoritmo di divisione e nel calcolo dei termini direttori.

Teorema 3.5.1 Teorema della base di Hilbert
Ogni ideale $I \leq k[x_1, \ldots, x_n]$ ha un insieme finito di generatori, ovvero si può scrivere come

$$I =< g_1, \ldots, g_t >$$

con $g_1, \ldots, g_t \in I$.

Dimostrazione. Se $I = 0$, l'insieme che genera I è costituito dal solo $\{0\}$ che è un insieme finito. Se I contiene dei polinomi diversi dal polinomio nullo, per la Proposizione 3.5.1 esistono $g_1, \ldots, g_t \in I$ tali che

$$< LT(I) >=< LT(g_1), \ldots, LT(g_t) > .$$

Vogliamo dimostrare che $I =< g_1, \ldots, g_t >$.

E' chiaro che $< g_1, \ldots, g_t > \subseteq I$ dato che ogni $g_i \in I$. Viceversa, sia f un qualsiasi polinomio di I. Applicando l'algoritmo di divisione in $k[x_1, \ldots, x_n]$, per dividere f per $g_1, \ldots, g_t$, si ha

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

dove o $r = 0$, oppure nessun termine di r può essere divisibile per qualche $LT(g_i)$. Dimostriamo per assurdo che $r = 0$; infatti:

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

Se fosse $r \neq 0$ allora il $LT(r) \in < LT(g_1), \ldots, LT(g_t) >$ e per il Lemma 3.4.1 si avrebbe che $LT(r)$ è divisibile per qualche $LT(g_i)$. Questo è assurdo in quanto r soddisfa alle proprietà del resto della divisione per i g_i. L'assurdo prova che r è necessariamente uguale a zero, e pertanto:

$$f = a_1 g_1 + \ldots + a_t g_t + 0 \in < g_1, \ldots, g_t >,$$

da cui $I \subseteq < g_1, \ldots, g_t >$. ∎

La base $\{g_1, \ldots, g_t\}$ usata nel Teorema, oltre a dare una soluzione al problema di descrizione dell'ideale, gode della proprietà che

$$< LT(I) > = < LT(g_1), \ldots, LT(g_t) >$$

e, come già visto nell'osservazione che segue la Definizione 3.5.1, non ogni base ha questa proprietà.

Definizione 3.5.2 *Sia fissato un ordine monomiale. Un sottoinsieme finito $G = \{g_1, \ldots, g_t\}$ di un ideale I si dice* **base di Groebner** *(o* **base standard***) se:*

$$< LT(I) > = < LT(g_1), \ldots, LT(g_t) > .$$

Equivalentemente, ma in modo meno formale, possiamo dire che un sottoinsieme $G = \{g_1, \ldots, g_t\} \subset I$ è una base di Groebner per I, se e solo se il termine direttore di ogni elemento di I è divisibile per uno dei $LT(g_i)$ (ciò segue dal Lemma 3.4.1). Dalla dimostrazione del Teorema della base di Hilbert segue immediatamente il:

Corollario 3.5.1 *Fissato un ordine monomiale, ogni ideale non nullo I di $k[x_1, \ldots, x_n]$ ha una base di Groebner. Inoltre, una base di Groebner di un ideale I è, effettivamente, una* base *per I.*

Dimostrazione. Assegnato un ideale non nullo, l'insieme $G = \{g_1, \ldots, g_t\}$ costruito nella dimostrazione del teorema precedente è una base di Groebner per definizione.

Per dimostrare la seconda affermazione, si osservi che se $< LT(I) > = < LT(g_1), \ldots, LT(g_t) >$ allora la stessa argomentazione data nel corso della dimostrazione del Teorema mostra che

$$I = < g_1, \ldots, g_t > .$$

Pertanto G è una base per I. ∎

Nel paragrafo 6 studieremo in dettaglio le proprietà delle basi di Groebner, in particolare, vedremo come possano essere utilizzate per risolvere il problema di appartenenza. Illustriamo ora alcuni esempi.

Esempi

(I) Riprendiamo in esame l'ideale

$$I =< f_1, f_2 >=< x^3 - 2xy, x^2y - 2y^2 + x >$$

già considerato nell'osservazione che segue la Definizione 3.5.1. Rispetto all'ordine lessicografico graduato DEGLEX, l'insieme $\{f_1, f_2\}$ non è una base di Groebner per I, poiché $x^2 \in < LT(I) >$, ma $x^2 \notin < LT(f_1), LT(f_2) >$. Nel paragrafo 7 impareremo a determinare, a partire da $\{f_1, f_2\}$, una base di Groebner per I.
(II) Consideriamo l'ideale $J =< g_1, g_2 >=< x+z, y-z >$ e dimostriamo che $\{g_1, g_2\}$ è una base di Groebner, rispetto all'ordine lessicografico in $\mathbf{R}[x, y, z]$. Dobbiamo dimostrare che la parte iniziale di ogni elemento non nullo di J appartiene all'ideale $< LT(g_1), LT(g_2) >=< x, y >$. Per il Lemma 3.4.1 ciò equivale a dimostrare che il termine direttore di ogni elemento non nullo di J è divisibile o per x o per y.

Per assurdo, supponiamo che esista un $f = Ag_1 + Bg_2 \in J$, con termine direttore non divisibile né per x né per y. Per come è definito l'ordine lessicografico, f deve essere un polinomio nella sola variabile z. Inoltre, dato che appartiene a J, il polinomio f è identicamente nullo sulla retta $L = \mathcal{V}(x + z, y - z) \subset \mathbf{R}^3$, il cui punto generico è, al variare di t in $\mathbf{R}$, il punto $(x, y, z) = (-t, t, t)$. Essendo k infinito, l'unico polinomio nella sola z che svanisce su tutti questi punti è il polinomio nullo, il che è assurdo perché contrario all'ipotesi $f \neq 0$. Ne segue che $< g_1, g_2 >$ è una base di Groebner per J.

Osserviamo, per inciso, che i generatori dell'ideale J hanno, per matrice dei coefficienti, la matrice a scala

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

Ciò non è casuale: per ideali generati da polinomi lineari una base di Groebner, rispetto all'ordinamento lessicografico, si ottiene riducendo a scala la matrice dei coefficienti.

Le basi di Groebner sono state introdotte intorno al 1960 da H.Hironaka (che le chiamò "basi standard) e, indipendentemente, verso il 1965 da B.

Buchberger nella sua Tesi di Ph.D. Il termine "basi di Groebner, usato in molti sistemi di computer algebra, fu introdotto da Buchberger in onore del suo relatore di Tesi.

Concludiamo questo paragrafo illustrando due applicazioni del teorema della base di Hilbert. La prima è di carattere algebrico e riguarda gli ideali in $k[x_1, \ldots, x_n]$.

Una **catena ascendente** di ideali è una successione crescente:

$$I_1 \subset I_2 \subset I_3 \subset \ldots.$$

Ad esempio, la successione:

$$< x_1 > \subset < x_1, x_2 > \subset, \ldots, \subset < x_1, \ldots, x_n > \tag{3.4}$$

è una catena ascendente (finita) di ideali.

Se vogliamo provare ad *estendere* questa catena includendo un ideale con ulteriori generatori, si presenteranno due alternative. Se $f \in < x_1, \ldots, x_n >$ allora $< x_1, \ldots, x_n, f >= < x_1, \ldots, x_n >$; Se invece $f \notin < x_1, \ldots, x_n >$ non è difficile dimostrare, per esercizio, che $< x_1, \ldots, x_n, f >= k[x_1, \ldots, x_n]$. Ne risulta che la catena ascendente (3.4) può essere prolungata solo in due modi, o ripetendo l'ultimo ideale all'infinito, o aggiungendo $k[x_1, \ldots, x_n]$ e poi ripetendolo all'infinito. In entrambi i casi la catena si sarà "stabilizzata dopo un numero finito di passi, nel senso che tutti gli ideali della catena, da quel punto in poi, risulteranno uguali. Nel prossimo Teorema faremo vedere che ciò si verifica in *ogni* catena ascendente di ideali.

Teorema 3.5.2 (Condizione della catena ascendente di ideali) *Se*

$$I_1 \subset I_2 \subset I_3 \subset \ldots$$

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

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

ossia $I_N = I_{N+i}$, per ogni $i \geq 0$.

Dimostrazione. Data una catena ascendente di ideali $I_1 \subset I_2 \subset I_3 \subset \ldots$ consideriamo $I = \bigcup_{i=1}^{\infty} I_i$. Vogliamo per prima cosa dimostrare che I è ancora un ideale di $k[x_1, \ldots, x_n]$; infatti, poiché gli I_i sono ideali, contengono tutti lo 0 e quindi $0 \in I$. Se $f, g \in I$, esisteranno degli indici i e j tali che $f \in I_i$ e $g \in I_j$. Se ad esempio è $i \leq j$, sia f che g apparterranno a I_j, e, essendo I_j un ideale, anche $f + g \in I_j \subset I$. Analogamente, se $f \in I$ e

$r \in k[x_1, \ldots, x_n]$ si ha che $f \in I_i$ per qualche i e, essendo I_i un ideale, sarà ancora $f \cdot r \in I_i \subset I$.

Per il teorema della base di Hilbert, l'ideale I deve avere un insieme finito di generatori: $I =< f_1, \ldots, f_s >$, ma ciascuno dei generatori è contenuto in qualche ideale I_j, sia $f_i \in I_{j_i}$ per qualche j_i, $i = 1, \ldots, s$. Prendendo il massimo N degli indici j_i, per definizione di catena ascendente di ideali, si ha che $f_i \in I_N$ per ogni i. Quindi

$$I =< f_1, \ldots, f_s > \subset I_N \subset I_{N+1} \subset \ldots \subset I$$

e la catena si stabilizza in I_N. ∎

L'affermazione che una catena ascendente di ideali di $k[x_1, \ldots, x_n]$ si stabilizza è chiamata spesso **condizione della catena ascendente** o, più brevemente, **CCA**. Dimostreremo nella Proposizione3.5.3 che se vale la CCA allora ogni ideale è finitamente generato, quindi la CCA è in realtà equivalente alla validità del teorema della base di Hilbert. Utilizzeremo la CCA nell'algoritmo di Buchberger per la costruzione delle basi di Groebner e nello studio delle varietà affini.

Proposizione 3.5.2 *Per un insieme parzialmente ordinato Σ le due proprietà che seguono sono equivalenti:*
(i) **Condizione della catena ascendente** *Se $a_1 \leq a_2 \leq \ldots \leq a_i \leq \ldots$ sono elementi di Σ, allora esiste un intero N tale che $a_i = a_N$, per ogni $i \geq N$ (ovvero: ogni catena ascendente di elementi di Σ è stazionaria).*
(ii) **Condizione massimale** *ogni sottoinsieme non vuoto S di Σ ha un elemento massimale ossia esiste un elemento a in S con la proprietà*

$$b \in S \text{ e } b \geq a \implies b = a.$$

Dimostrazione. (i) $\Longrightarrow$ (ii). Se, per assurdo, (ii) fosse falsa, esisterebbe un sottoinsieme non vuoto S di Σ privo di elementi massimali. Scelto un $a_1 \in S \neq \emptyset$, poiché a_1 non è massimale esisterà un $a_2 \neq a_1$ in S tale che $a_1 < a_2$. Ma anche a_2 non è massimale in S, quindi esisterà un a_3 tale che $a_2 < a_3$ e così via. Si otterrà in tal modo una successione infinita strettamente crescente $a_1 < a_2 < a_3 < \ldots$ di elementi di S, il che è contrario alla (i).

(ii) $\Longrightarrow$ (i). Sia S l'insieme di tutti gli a_i. Per la (ii) l'insieme S ha un elemento massimale, sia a_N; chiaramente $a_i = a_N$ per ogni $i \geq N$. ∎

Analogamente, si possono definire, su un insieme parzialmente ordinato, la *condizione della catena discendente* e la condizione *minimale*; si può poi dimostrare che sono condizioni equivalenti.

Proposizione 3.5.3 *Se A è un arbitrario anello (commutativo) le condizioni che seguono sono equivalenti:*
(i) L'insieme degli ideali di A (ordinato per inclusione) soddisfa alla condizione della catena ascendente.
(ii) L'insieme degli ideali di A (ordinato per inclusione) soddisfa alla condizione massimale.
(iii) Ogni ideale di A ha una base finita, ossia è finitamente generato.

Dimostrazione. (i) $\Longleftrightarrow$ (ii) segue dalla Proposizione3.5.2.
(ii) $\Longrightarrow$ (iii). Sia Σ l'insieme di tutti gli ideali finitamente generati di A contenuti in un fissato ideale I di A. Σ è non vuoto, in quanto $(0) \in \Sigma$. Se $J =< f_1, \dots f_n >$ è un elemento massimale di Σ non può essere $J \neq I$. Infatti, se così fosse, esisterebbe $f_0 \in I$ con $f_0 \notin J$, e l'ideale $< f_0, J >=< f_0, f_1, \dots, f_n >$, che è finitamente generato e contenuto in I, conterrebbe propriamente J, il che è contrario all'ipotesi di massimalità per J. Pertanto, l'ideale $I = J$ è finitamente generato.
(iii) $\Longrightarrow$ (i) Sia $I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$ una catena ascendente di ideali di A. L'unione I di tutti gli I_n è un ideale, e quindi ha una base finita, sia $f_1, \dots, f_r$. Se $f_i \in I_{n_i}$, $(i = 1, \dots, r)$, poniamo $N = \max(n_1, \dots, n_r)$. Ovviamente tutti gli f_i sono in I_N, il che implica che $I_N = I_{N+1} = \dots = I$.
∎

Un anello A che goda di una delle tre proprietà equivalenti di cui nella Proposizione 3.5.3 (e quindi di tutte) si dice **Noetheriano** (in ricordo di Emmy Noether (1882-1935)). Ad esempio, ogni campo è un anello Noetheriano, o anche ogni dominio ad ideali principali. Per quanto ci riguarda, il fatto basilare sugli anelli Noetheriani è

Teorema 3.5.3 *(***Altra versione del Teorema Della Base Di Hilbert***) Se A è un anello Noetheriano, anche l'anello $A[t]$ dei polinomi in una indeterminata a coefficienti in A è Noetheriano.*

Dimostrazione. (H. Sarges, 1976) Sia A un anello noetheriano e consideriamo (per assurdo) un ideale $I \subset A[x]$ non finitamente generato. Scegliamo $f_1 \in I$ di grado minimo. Scegliamo poi $f_2 \in I - < f_1 >$ ancora di grado minimo e procedendo in questo modo troviamo $f_h \in I - < f_1, \dots, f_{h-1} >$ di grado minimo. Sia $n_h := deg\ f_h$ e sia $f_h = a_h x^{n_h} + \dots$ Abbiamo ovviamente

$n_1 \leq n_2 \leq \ldots$ e $< a_1 > \subset < a_1, a_2 > \subset \ldots$. Per ipotesi esiste p tale che $< a_1, \ldots, a_p > = < a_1, \ldots, a_{p+1} >$ e quindi si può scrivere $a_{p+1} = \sum_{i=1}^{p} b_i a_i$ con $b_i \in A$. Poniamo $g := f_{p+1} - \sum_{i=1}^{p} x^{n_{p+1}-n_i} b_i f_i$. Quindi il termine di grado massimo di g è

$$a_{p+1} x^{n_{p+1}} - \sum_{i=1}^{p} b_i a_i x^{n_{p+1}} = 0$$

da cui $deg\ g < n_{p+1}$. D'altronde $g \in I$ e $g \notin < f_1, \ldots, f_p >$ (altrimenti $f_{p+1} \in < f_1, \ldots f_p >$). Questa è una contraddizione perché f_{p+1} era stato scelto come un polinomio di grado minimo in $I - < f_1, \ldots, f_p >$. ∎

Dal Teorema 3.5.3, per induzione su n, segue che

$$A \text{ Noetheriano} \quad \Longrightarrow \quad A[x_1, \ldots, x_n] \ Noetheriano.$$

In particolare, essendo un campo Noetheriano, si ha:

Corollario 3.5.2 *L'anello $k[x_1, \ldots, x_n]$ dei polinomi a coefficienti in un campo k è Noetheriano.*

Una seconda applicazione del teorema della base di Hilbert è di carattere geometrico. Abbiamo definito le varietà affini come insiemi di soluzioni di sistemi finiti di equazioni polinomiali:

$$\mathcal{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \ \forall i\}.$$

Il teorema della base di Hilbert mostra che, in realtà, ha senso parlare di varietà affini definite da un ideale $I \leq k[x_1, \ldots, x_n]$.

Definizione 3.5.3 *Se $I \subset k[x_1, \ldots, x_n]$ è un ideale, denoteremo con $\mathcal{V}(I)$ l'insieme*

$$\mathcal{V}(I) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \ \forall \ f \in I\}.$$

Anche se un ideale non nullo contiene un numero infinito di polinomi, $\mathcal{V}(I)$ può essere ancora definito come l'insieme dei punti di k^n che risolvono un sistema *finito* di equazioni polinomiali.

Proposizione 3.5.4 *$\mathcal{V}(I)$ è una varietà affine. In particolare, se $I = < f_1, \ldots, f_s >$, risulta $\mathcal{V}(I) = \mathcal{V}(f_1, \ldots, f_s)$.*

Dimostrazione. Per il teorema della base di Hilbert $I =< f_1, \ldots, f_s >$ ha un insieme finito di generatori. Per dimostrare l'uguaglianza dei due insiemi $\mathcal{V}(I)$ e $\mathcal{V}(f_1, \ldots, f_s)$, dimostriamo le due inclusioni opposte. Poiché $f_i \in I$, se $f(a_1, \ldots, a_n) = 0$ per ogni $f \in I$ allora $f_i(a_1, \ldots, a_n) = 0$, quindi $\mathcal{V}(I) \subset \mathcal{V}(f_1, \ldots, f_s)$. Viceversa, se $(a_1, \ldots, a_n) \in \mathcal{V}(f_1, \ldots, f_s)$ e $f \in I$, possiamo scrivere

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

per qualche $h_i \in k[x_1, \ldots, x_n]$. Questo implica

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

da cui $\mathcal{V}(f_1, \ldots, f_s) \subset \mathcal{V}(I)$. Quindi i due insiemi sono uguali. ∎

Osservazione.

La più importante conseguenza di questa Proposizione è che le varietà affini sono determinate dagli ideali. Nel Capitolo 1 avevamo dimostrato che:

$$\mathcal{V}(f_1, \ldots, f_s) = \mathcal{V}(g_1, \ldots, g_t) \text{ se } < g_1, \ldots, g_t >=< f_1, \ldots, f_s > .$$

Questo è un corollario della Proposizione 3.5.4. La relazioni esistente tra varietà ed ideali verrà illustrata più dettagliatamente nel Capitolo 4.

3.6 Proprietà delle basi di Groebner

Abbiamo visto che ogni ideale non nullo $I \leq k[x_1, \ldots, x_n]$ possiede una base di Groebner. In questo paragrafo studieremo le proprietà delle basi di Groebner e impareremo a verificare se una data base sia o non sia di Groebner. Iniziamo con il far vedere che gli inconvenienti dell'algoritmo di divisione non si presentano se si divide per una base di Groebner; in particolare, il resto è univocamente determinato.

Proposizione 3.6.1 *Sia $G = \{g_1, \ldots, g_t\}$ una base di Groebner per l'ideale $I \leq k[x_1, \ldots, x_n]$ e sia $f \in k[x_1, \ldots, x_n]$. Esiste un unico polinomio r di $k[x_1, \ldots, x_n]$ che soddisfa le seguenti proprietà:*

(i) nessun termine di r è divisibile per uno tra $LT(g_1), \ldots, LT(g_t)$.
(ii) Esiste $g \in I$ tale che $f = g + r$.
In particolare, r è il resto della divisione di f per G qualunque sia l'ordine dei g_i nell'eseguire la divisione.

Dimostrazione. L'algoritmo di divisione dà

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

dove r soddisfa le condizioni (i) e (ii) con $g = a_1 g_1 + \ldots + a_t g_t \in I$. Questo prova l'esistenza di r.

Per provare l'unicità, supponiamo che $f = g_1 + r_1 = g_2 + r_2$ soddisfi (i) e (ii). Allora $r_1 - r_2 = g_2 - g_1 \in I$, così se $r_1 \neq r_2$ allora il $LT(r_1 - r_2) \in < (LT(I) >=< LT(g_1), \ldots, LT(g_t >$. Dal Lemma 3.4.1 segue che $LT(r_1 - r_2)$ è divisibile per qualche $LT(g_i)$, ma questo è assurdo perché nessun termine di r_1, r_2 è divisibile per qualche $LT(g_1), \ldots, LT(g_t)$. Ciò prova che $r_1 - r_2$ deve essere necessariamente uguale a zero, il che dimostra l'unicità.

La parte finale della Proposizione segue dall'unicità di r. ∎

Per quanto r sia unico, anche per una base di Groebner, i quozienti a_i dati dall'algoritmo di divisione possono cambiare se si elencano i g_i in ordine diverso. Per vederlo basta considerare l'esempio

$$G = \{g_1, g_2\} = \{x + z, y - z\}$$

di base di Groebner dato nel paragrafo precedente. Dividendo, in $k[x, y]$ con l'ordine lessicografico il polinomio $f = xy$ prima per $(g_1, g_2) = (x + z, y - z)$ e poi per (g_2, g_1) si ottiene sempre lo stesso resto, ma i quozienti cambiano.

Corollario 3.6.1 *Sia $G = \{g_1, \ldots, g_t\}$ una base di Groebner per l'ideale $I \leq k[x_1, \ldots, x_n]$ e sia $f \in k[x_1, \ldots, x_n]$. Allora $f \in I$ se e solo se il resto della divisione di f per G è uguale a zero.*

Dimostrazione. Se il resto della divisione è zero, banalmente $f \in I$. Viceversa, assegnato $f \in I$, allora $f = f + 0$ soddisfa le due condizioni della Proposizione precedente. Dall'unicità segue che il resto della divisione di f per G è necessariamente uguale a zero. ∎

Osservazione.

La proprietà fornita dal Corollario sopra dimostrato talora è data come definizione di base di Groebner in quanto si può dimostrare, per esercizio, equivalente alla condizione $< LT(G) >=< LT(I) >$.

Utilizzando, il Corollario 3.6.1, si può dare un algoritmo per risolvere il problema di appartenenza ad un ideale I, una volta noto un algoritmo per determinare una base di Groebner G di I. Infatti, basterà calcolare il resto della divisione di f per G per decidere se $f \in I$. Nel paragrafo 7 daremo tale algoritmo, risolvendo così completamente il problema di appartenenza.

Definizione 3.6.1 *Denoteremo con $\bar{f}^F$ il resto della divisione di f per una s-pla ordinata $F = (f_1, \ldots, f_s)$. Se F è una base di Groebner per $< f_1, \ldots, f_s >$ allora possiamo considerare F come un insieme non ordinato, per la Proposizione 3.6.1.*

Si noti che l'*ostruzione* per $\{f_1, \ldots, f_s\}$ all'essere una base di Groebner è data dalla presenza di combinazioni lineari (a coefficienti polinomi) degli f_i i cui termini direttori non sono nell'ideale generato dagli $LT(f_i)$. Ciò può accadere quando un'opportuna combinazione lineare

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

cancella i termini direttori, lasciando solo termini più piccoli. D'altro canto $ax^\alpha f_i - bx^\beta f_j \in I$, e quindi il suo termine direttore è in $LT(I)$. Per studiare questo fenomeno di cancellazione introduciamo le seguenti combinazioni.

Definizione 3.6.2 *Siano $f, g \in k[x_1, \ldots, x_n]$ polinomi non nulli.*
(i) Se il $multideg(f) = \alpha$ e $multideg(g) = \beta$, sia

$$\gamma = (\gamma_1 \ldots, \gamma_n), \quad \text{con} \quad \gamma_i = max\{\alpha_i, \beta_i\}, \ \forall \ i.$$

Chiameremo x^γ il **minimo comune multiplo** *tra i monomi direttori $LM(f)$ e $LM(g)$ e scriveremo*

$$x^\gamma = m.c.m.(LM(f), LM(g)).$$

*(ii) Si dice S-***polinomio** *di f e g la combinazione:*

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

(Osserviamo che qui si invertono anche i coefficienti direttori).

Esempio.

Siano $f = x^3y^2 - x^2y^3 + x$ e $g = 3x^4y + y^2$ in $\mathbf{R}[x, y]$, con l'ordinamento lessicografico graduato. Risulta $\gamma = (4, 2)$ 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 $S(f,g)$ è concepito per causare la cancellazione del termine direttore. Il seguente lemma dimostra che *ogni cancellazione di termini direttori tra polinomi dello stesso multigrado* è il risultato di questo tipo di cancellazione.

Lemma 3.6.1 *Supponiamo di avere una somma del tipo* $\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i$, *dove* $c_1, \ldots, c_t$ *sono delle costanti di* k *e, se* $\beta(i)$ *è il multigrado di* g_i *risulta*

$$\alpha(i) + \beta(i) = \delta \in \mathbf{Z}^n_{\geq 0} \quad \forall\ i, \text{ per cui } c_i \neq 0.$$

Se la somma ha un multigrado strettamente più piccolo, ossia

$$multideg(\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i) < \delta,$$

allora esistono costanti c_{jh} *tali che*

$$\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i = \sum_{j,h} c_{jh} x^{\delta - \gamma_{jh}} S(g_j, g_h), \tag{3.5}$$

ove $x^{\gamma_{jh}} = m.c.m.(LM(g_j), LM(g_h))$. *Inoltre, ciascun* $x^{\delta-\gamma_{jh}} S(g_j, g_h)$ *ha multigrado minore di* δ.

Dimostrazione. Sia $d_i = LC(g_i)$, così che $c_i d_i$ è il coefficiente direttore di $c_i x^{\alpha(i)} g_i$. Poiché i termini $c_i x^{\alpha(i)} g_i$ hanno ciascuno multigrado δ, mentre la loro somma ha multigrado strettamente minore di δ, è necessariamente

$$\sum_{i=1}^{t} c_i d_i = 0.$$

Per definizione di $S-$polinomio, ed essendo $LT(g_i) = d_i x^{\beta(i)}$, risulta

$$\begin{aligned} S(g_j, g_h) &= \frac{x^{\gamma_{jh}}}{LT(g_j)} g_j - \frac{x^{\gamma_{jh}}}{LT(g_h)} g_h = \\ &= \frac{x^{\gamma_{jh} - \beta(j)}}{d_j} g_j - \frac{x^{\gamma_{jh} - \beta(h)}}{d_h} g_h. \end{aligned}$$

Quindi, moltiplicando ambo i membri per $x^{\delta - \gamma_{jh}}$ e ricordando che $\alpha(i) = \delta - \beta(i)$ per ogni i, si ha

$$x^{\delta - \gamma_{jh}} S(g_j, g_h) = \frac{x^{\alpha(j)}}{d_j} g_j - \frac{x^{\alpha(h)}}{d_h} g_h.$$

Posto per semplicità

$$p_i = \frac{x^{\alpha(i)}}{d_i} g_i, \quad \forall i = 1, \ldots, t,$$

è dunque

$$x^{\delta - \gamma_{jh}} S(g_j, g_h) = p_j - p_h. \tag{3.6}$$

Osserviamo che p_i ha il coefficiente direttore uguale a 1. Consideriamo la somma telescopica:

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

Ricordando la Formula (3.6) e il fatto che $\sum_{i=1}^{t} c_i d_i = 0$, la somma telescopica diventa:

$$\begin{aligned} \sum_{i=1}^{t} c_i x^{\alpha(i)} g_i &= c_1 d_1 x^{\delta - \gamma_{12}} S(g_1, g_2) + \ldots \\ &+ \ldots + (c_1 d_1 + \ldots + c_{t-1} d_{t-1}) x^{\delta - \gamma_{t-1,t}} S(g_{t-1}, g_t). \end{aligned}$$

che è una somma del tipo desiderato.

Poiché p_j e p_h hanno multigrado minore di δ e coefficiente direttore 1, la differenza $p_j - p_h$ ha multigrado minore di δ. Per la Formula (3.6), possiamo affermare che ciò è vero anche per $x^{\delta - \gamma_{jh}} S(g_j, g_h)$ e il lemma è completamente dimostrato. ∎

Per capire l'equazione (3.5) del Lemma 3.6.1, esaminiamo quando si ha cancellazione. Nella somma a primo membro, ogni addendo ha multigrado δ, quindi la cancellazione avviene dopo la somma. Nella somma a secondo membro, ogni addendo ha multigrado minore di δ e, quindi, la cancellazione è già avvenuta. Intuitivamente questo significa che ogni cancellazione si può ottenere da S-polinomi.

Usando S-polinomi e il Lemma 3.6.1 si può dimostrare il seguente criterio per stabilire se una data base di un ideale è di Groebner.

Teorema 3.6.1 Criterio di Buchberger *Sia $I \leq k[x_1, \ldots, x_n]$ un ideale. Una base $G = \{g_1, \ldots, g_t\}$ di I è una base di Groebner per I se, e solo se, per tutte le coppie (j, h) con $j \neq h$, il resto della divisione di $S(g_j, g_h)$ per G è uguale a zero.*

Dimostrazione. $\Rightarrow$ Se G è una base di Groebner, dato che $S(g_j, g_h) \in I$, per il Corollario 3.6.1, il resto della divisione per G degli $S(g_j, g_h)$ è uguale a zero.

$\Leftarrow$ Si deve dimostrare che, dall'ipotesi che tutti gli $S(g_j, g_h)$ hanno resto zero nella divisione per G, segue che ogni polinomio non nullo f di I è tale che

$$LT(f) \in < LT(g_1), \ldots, LT(g_t) > = < LT(G) > . \tag{3.7}$$

Dato $f \in I = < g_1, \ldots, g_t >$ esistono polinomi $a_i \in k[x_1, \ldots, x_n]$ tali che:

$$f = \sum_{i=1}^{t} a_i g_i. \tag{3.8}$$

Per il Lemma 3.2.2 possiamo scrivere

$$multideg(f) \leq max\{m(i)\}, \quad \text{ove} \quad m(i) = multideg(a_i g_i). \tag{3.9}$$

Se per qualche i si ha $multideg(f) = max(multideg(a_i g_i))$ allora $LT(f)$ è divisibile per $LT(g_i)$ e quindi resta provato che $LT(f) \in < LT(G) >$ e G è di Groebner. Se invece non si ha l'uguaglianza, allora qualche cancellazione è avvenuta trai termini direttori dell' espressione (3.8) di f come combinazione dei g_i. La strategia della dimostrazione consiste nell'utilizzare il Lemma 3.6.1 per riscrivere f in termini di S-polinomi e utilizzare il fatto che questi, divisi per G, dànno resto zero per sostituirli con espressioni che implicano meno cancellazione dei termini direttori, fino ad arrivare ad un'espressione di f come combinazione lineare dei g_i in cui nella diseguaglianza (3.9) vale il segno uguale, caso in cui $LT(f) \in < LT(G) >$, e, come già osservato, G risulta di Groebner.

Dato $f = \sum_{i=1}^{t} a_i g_i$ poniamo

$$\delta = max(m(1), \ldots, m(t)), \quad \text{ove} \quad m(i) = multideg(a_i g_i),$$

di modo che la diseguaglianza (3.9) diventi

$$multideg(f) \leq \delta.$$

Consideriamo, ora tutti i possibili modi in cui possiamo scrivere f nella forma (3.8). Per ogni tale espressione di f, si ottiene un corrispondente δ. Poiché un ordinamento monomiale è un buon ordinamento, possiamo scegliere un'espressione di f tale che il corrispondente δ sia minimale. Dimostreremo ora, per assurdo, che, con tale scelta, risulta $multideg(f) = \delta$, il che, per quanto sopra osservato, dimostra il Teorema.

Sia, per assurdo, il $multideg(f) < \delta$, con δ minimale. Isolando, nella espressione di f, i termini con multigrado minore di δ si ottiene

$$\begin{aligned} f &= \sum_{m(i)=\delta} a_i g_i + \sum_{m(i)<\delta} a_i g_i = \\ &= \sum_{m(i)=\delta} LT(a_i) g_i + \sum_{m(i)=\delta} (a_i - LT(a_i)) g_i + \sum_{m(i)<\delta} a_i g_i. \end{aligned} \tag{3.10}$$

I monomi che appaiono, nella seconda e terza somma dell'ultima riga hanno multigrado strettamente minore di δ. Se, per assurdo, fosse $multideg(f) < \delta$, si avrebbe che anche la prima somma avrebbe multigrado minore di δ.

Posto $LT(a_i) = c_i x^{\alpha(i)}$, la prima somma può essere riscritta come

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

ossia ha esattamente la forma descritta nel Lemma 3.6.1, in quanto i $c_i x^{\alpha(i)} g_i$ hanno tutti lo stesso multigrado δ, mentre la loro somma ha grado strettamente minore. L'equazione (3.5) del Lemma 3.6.1 implica

$$\sum_{m(i)=\delta} LT(a_i) g_i = \sum_{j,h} c_{jh} x^{\delta - \gamma_{jh}} S(g_j, g_h). \tag{3.11}$$

ove $c_{jh} \in k$ e $x^{\gamma_{jh}} = m.c.m.(LM(g_i), LM(g_h))$. Il prossimo passo è quello di utilizzare l'ipotesi che il resto della divisione di $S(g_j, g_h)$ per G è zero. Usando l'algoritmo di divisione, si può scrivere ciascun S-polinomio nella forma:

$$S(g_j, g_h) = \sum_{i=1}^{t} a_{ijh} g_i, \tag{3.12}$$

ove $a_{ijh} \in k[x_1, \ldots, x_n]$. L'algoritmo di divisione dice inoltre che

$$multideg(a_{ijh} g_i) \leq multideg(S(g_j, g_h)) \quad \forall\ i, j, h. \tag{3.13}$$

Intuitivamente ciò significa che quando il resto della divisione è zero, si può trovare una espressione per $S(g_j, g_h)$ in termini di G in cui non tutti i termini direttori si cancellano. Per utilizzare ciò, moltiplichiamo l'espressione di $S(g_j, g_h)$ data sopra per $x^{\delta - \gamma_{jh}}$; si ottiene così

$$x^{\delta - \gamma_{jh}} S(g_j, g_h) = \sum_{i=1}^{t} b_{ijh} g_i \tag{3.14}$$

dove $b_{ijh} = x^{\delta-\gamma_{jh}} a_{ijh}$. Allora per la (3.13) e per il Lemma 3.6.1 si ha

$$multideg(b_{ijh}g_i) \leq multideg(x^{\delta-\gamma_{jh}} S(g_j, g_h)) < \delta. \tag{3.15}$$

Sostituendo l'Espressione (3.14) nell'equazione (3.11) si deduce

$$\sum_{m(i)} LT(a_i)g_i = \sum_{j,h} c_{j,h} x^{\delta-\gamma_{jh}} S(g_j, g_h) = \sum_{j,h} c_{j,h} (\sum_i b_{ijh} g_i) = \sum_i \tilde{a}_i g_i.$$

ove $\tilde{a}_i = \sum_{j,h} c_{j,h} b_{ijh}$, e per la disuguaglianza 3.15,

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

in quanto le c_{jh} sono costanti. Il passo finale consiste nel sostituire

$$\sum_{m(i)} LT(a_i)g_i = \sum_i \tilde{a}_i g_i$$

nell'equazione (3.10) avendo così la

$$f = \sum_i \tilde{a}_i g_i + \sum_{m(i)=\delta} (a_i - LT(a_i))g_i + \sum_{m(i)<\delta} a_i g_i,$$

che esprime f come combinazione polinomiale dei g_i, in cui *tutti* i termini hanno multigrado minore di δ. Ma ciò è assurdo perché contraddice l'ipotesi di minimalità per δ. Questo completa la dimostrazione. ∎

Il criterio di Buchberger è estremamente utile in quanto fornisce un algoritmo per verificare se una base è di Groebner.

Esempio.

Consideriamo l'ideale $I =< y - x^2, z - x^3 >$ che definisce la cubica sghemba in $\mathbf{R^3}$; vogliamo dimostrare che $G = \{y - x^2, z - x^3\}$ è
(a) una base di Groebner rispetto all'ordine lessicografico LEX con $y > z > x$, mentre
(b) non è una base di Groebner rispetto a LEX quando si sceglie come ordine delle variabili quello usuale $x > y > z$.

Nel caso (a), l'S-polinomio da considerare è

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

Dividendo per G si ottiene

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

ossia $\overline{S(y - x^2, z - x^3)}^G = 0$, e, per il criterio di Buchberger, G è una base di Groebner per I.

Nel caso (b) $G = \{g_1, g_2\} = \{-x^2 + y, -x^3 + z\}$ quindi

$$m.c.m.(LM(g_1), LM(g_2)) = x^3$$

e risulta

$$S(g_1, g_2) = -xg_1 + g_2 = -xy + z = \overline{S(g_1, g_2)}^G \neq 0.$$

Sempre per il criterio di Buchberger, G non è di Groebner.

3.7 Algoritmo di Buchberger

In questo paragrafo faremo vedere come, dato un ideale $I \leq k[x_1, \ldots, x_n]$, si possa effettivamente costruire una base di Groebner per I. Per capire le idee alla base del metodo che useremo, consideriamo di nuovo l'ideale dell'esempio (I) del paragrafo 5.

Esempio.

In $k[x, y]$ con l'ordinamento DEGLEX, $x > y$, consideriamo

$$I =< f_1, f_2 >=< x^3 - 2xy, x^2y - 2y^2 + x > .$$

Sappiamo già che $F = \{f_1, f_2\}$ non è una base di Groebner per I, in quanto $LT(S(f_1, f_2)) = -x^2 \notin < LT(f_1), LT(f_2) >$ e, pertanto, fa parte del resto $r = \overline{S(f_1, f_2)}^F$ (che quindi è non nullo) della divisione di $S(f_1, f_2)$ per F.

Per ottenere una base di Groebner, un'idea naturale è quella di provare ad estendere la base originaria F, con polinomi di I fino ad ottenere una base di Groebner. Se includiamo nell'insieme dei generatori di I tale resto non nullo e poniamo $F := \{f_1, f_2, f_3\}$, ove

$$f_3 = -x^2 = \overline{S(f_1, f_2)}^F,$$

si ha $S(f_1, f_2) = f_3$ e quindi

$$\overline{S(f_1, f_2)}^F = 0.$$

Volendo verificare se la nuova F è di Groebner dobbiamo calcolare

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

Aggiungendo $f_4 = -2xy$ all'insieme dei generatori, si ha un nuovo insieme $F := (f_1, f_2, f_3, f_4)$. Ora

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

Aggiungendo $f_5 = \overline{S(f_2, f_3)}^F = -2y^2 + x$ ad F e calcolando

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

si avrà, per il criterio di Buchberger che

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

è una base di Groebner per I.

Il procedimento, seguito nell'esempio, di aggiungere $\overline{S(f_i, f_j)}^F$ ad F se è non nullo, può essere formalizzato in un algoritmo per costruire basi di Groebner. Questo algoritmo di Buchberger è la pietra miliare della geometria algebrica computazionale.

Teorema 3.7.1 *Sia $I =< f_1, \ldots, f_s >\neq 0$ un ideale di $k[x_1, \ldots, x_n]$. Si può costruire una base di Groebner per I in un numero finito di passi, con il seguente algoritmo.*

Input: $F = (f_1, \ldots, f_s)$
Output: Una base di Groebner $G = \{g_1, \ldots, g_t\}$ per I, con $F \subset G$

$G := F$
REPEAT

$G' := G$
FOR each pair(p, q), $p \neq q$ *in* G' DO

$S := \overline{S(p,q)}^{G'}$
IF $S \neq 0$ THEN $G := G \cup S$

UNTIL $G := G'$

Dimostrazione. Per brevità scriveremo $I =< G >$ e $< LT(G) > = < LT(g_1), \ldots, LT(g_t) >$. Dimostriamo, in primo luogo, che $G \subset I$ *sussiste ad ogni passo dell'algoritmo*. Questo è vero per i valori iniziali, e continua ad essere vero quando G diventa sempre più grande per l'aggiunta dei resti $\overline{S(p,q)}^{G'}$ con $p, q \in G'$. Infatti, essendo $G \subset I$ sia p, q che $S(p,q)$ sono in I, e dividendo per $G' \subset I$ si ha ancora $G \cup S \ \subset I$. Possiamo poi osservare che G contiene la data base F di I, pertanto G *è sicuramente una base per* I.

L'algoritmo funziona in quanto allo stadio finale è $G = G'$, il che significa che $\overline{S(p,q)}^{G} = 0$ per tutti i p, q in G. Quindi, per il criterio di Buchberger, G è una base di Groebner per I.

Resta da dimostrare che l'algoritmo termina. Ogni volta che si passa attraverso la parte da ripetere dell'algoritmo, l'insieme G è costituito da G' (ossia il vecchio G) e dai resti non nulli delle divisioni di S-polinomi per G'. Dato che $G' \subset G$, si avrà sempre

$$< LT(G') > \subset < LT(G) > . \tag{3.16}$$

Inoltre, se $G' \neq G$ tale inclusione è stretta. Infatti, se r è un resto non nullo nella divisione di un S-polinomio per G', allora $LT(r)$ non è divisibile per nessuno dei termini direttori di elementi di G', ovvero $LT(r) \notin < LT(G') >$, anche se $LT(r) \in < LT(G) >$.

Per la (3.16), gli ideali $< LT(G') >$ via via ottenuti formano una catena ascendente di ideali in $k[x_1, \ldots, x_n]$, anello noetheriano come prova il teorema della base di Hilbert. La CCA in $k[x_1, \ldots, x_n]$ implica che dopo un numero finito di passi la catena si stabilizza, ossia $< LT(G') > =< LT(G) >$. Ne segue che $G = G'$, e, quindi l'algoritmo termina dopo un numero finito di passi. ∎

Osservazioni

(I) L'algoritmo dato non è sicuramente il più pratico. Come primo miglioramento notiamo che, non appena $\overline{S(p,q)}^{G'} = 0$, tale resto rimane non nullo anche aggiungendo altri elementi all'insieme dei generatori. Quindi non c'è motivo di ricalcolare tali resti nei passi successivi. Invero, aggiungendo i nuovi generatori f_j uno per volta, gli unici resti che devono essere controllati sono $\overline{S(f_i, f_j)}^{G'}$ con $i \leq j - 1$. Ulteriori raffinamenti, per migliorare

l'efficienza dell'algoritmo, sono stati fatti negli anni '70 e '80 da Buchberger e dai suoi collaboratori (si veda ad esempio [8], capitolo 2, paragrafo 9)

(II) Le basi di Groebner ottenute con tale algoritmo sono spesso più grandi di quanto sia necessario. Si possono eliminare alcuni tra i generatori usando il risultato seguente.

Lemma 3.7.1 *Sia G una base di Groebner per l'ideale polinomiale I. Se $p \in G$ è un polinomio tale che $LT(p) \in < LT(G - \{p\}) >$, anche $G - \{p\}$ è una base di Groebner per I.*

Dimostrazione. Sappiamo che $< LT(G) >=< LT(I) >$. Se $LT(p)$ appartiene a $< LT(G - \{p\}) >$, allora $< LT(G - \{p\}) >=< LT(G) >$. Dalla definizione segue quindi che anche $G - \{p\}$ è una base di Groebner per I. ∎

Definizione 3.7.1 *Una base di Groebner* **minimale** *per l'ideale polinomiale I è una base di Groebner G per I tale che:*

(i) $LC(p) = 1 \quad \forall\ p \in G$
(ii) $\forall\ p \in G \quad LT(p) \notin < LT(G - \{p\}) >$.

Si può costruire una base di Groebner minimale, per un ideale non nullo, applicando l'algoritmo di Buchberger (cfr. Teorema 3.7.1) e poi usando il Lemma 3.7.1 per eliminare tutti i generatori che non sono necessari. Per illustrare tale procedimento forniamo il seguente

Esempio.

Una base di Groebner per l'ideale $I =< x^3 - 2xy, x^2y - 2y^2 + x >$ è:

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

Poiché alcuni dei coefficienti direttori sono diversi da 1, il primo passo è quello di moltiplicare ciascun generatore p per $LC(p)^{-1}$ in modo da ridursi a polinomi monici. Osservando poi che $LT(f_1) = x^3 = -x \cdot LT(f_3)$, si può, per il Lemma 3.7.1, eliminare f_1 dalla base di Groebner. Analogamente, poiché $LT(f_2) = x^2y = -(1/2)x \cdot LT(f_4)$ è lecito eliminare f_2. Non essendoci altri

casi in cui il termine direttore di un generatore divida quello di un altro generatore, si ha che

$$\tilde{f_3} = x^2, \quad \tilde{f_4} = xy, \quad \tilde{f_5} = y^2 - (1/2)x,$$

costituiscono una base di Groebner minimale per I.

Sfortunatamente, un dato ideale I può avere più di una base minimale. Ad esempio per l' ideale I sopra considerato è semplice verificare che:

$$\tilde{f_3} = x^2 + axy, \quad \tilde{f_4} = xy, \quad \tilde{f_5} = y^2 - (1/2)x,$$

per ogni costante $a \in k$, è ancora una base di Groebner minimale. Si può pertanto, se k è infinito, dare un numero infinitodi basi di Groebner minimali. Fortunatamente tra tutte queste basi, ne esiste una che è migliore delle altre.

Definizione 3.7.2 *Una base di Groebner* **ridotta** *per un ideale polinomiale I è una base di Groebner G tale che:*

(i) $LC(p) = 1 \ \forall \ p \in G$.
(ii) $\forall \ p \in G$ *nessun monomio di* $p \in < LT(G - \{p\}) >$.

Nell'esempio precedente, solo la base con $a = 0$ è una base ridotta. In generale, le basi di Groebner ridotte godono della seguente proprietà.

Proposizione 3.7.1 *Fissato un ordine monomiale, ogni ideale non nullo I di $k[x_1, \ldots, x_n]$ ha un'*unica *base di Groebner ridotta.*

Dimostrazione. Sia G una base di Groebner minimale di I. Diremo che un elemento $g \in G$ è *ridotto* per G, se nessun monomio di g appartiene all'ideale $< LT(G - \{g\}) >$. Il nostro obiettivo è quello di modificare G fino a quando tutti i suoi elementi siano ridotti.

Una prima osservazione è che se g è ridotto per G, allora g è ridotto per qualsiasi altra base di Groebner minimale di I che contenga g e che possieda lo stesso insieme di termini direttori. Questo è vero in quanto la definizione di ridotto coinvolge solo i termini direttori.

Definiamo, ora, l'insieme $G' = (G - \{g\}) \cup \{g'\}$, ove $g \in G$ e $g' = \bar{g}^{G-\{g\}}$. Vogliamo dimostrare che G' è una base di Groebner minimale per I. Infatti, $LT(g') = LT(g)$, in quanto dividendo g per $G - \{g\}$ il $LT(g)$ va a formare il resto, non essendo divisibile per nessuno elemento di $LT(G - \{g\})$. Questo dimostra che $< LT(G) > = < LT(G') >$. Poiché G' è chiaramente contenuto

in I, si vede poi che G' è una base di Groebner ed è anche minimale. Si noti infine che, per costruzione, g' è ridotto per G'.

Continuando ad applicare agli elementi di G il procedimento sopra esposto, si arriverà ad ottenere elementi tutti ridotti. La base di Groebner può cambiare ogni volta che si applica il procedimento, ma una volta ridotto, un elemento rimane tale poiché non si cambia mai il suo termine direttore. Si arriva così a una base di Groebner ridotta.

Per dimostrare l'unicità, supponiamo di avere G e $\tilde{G}$, due basi ridotte per I. In particolare G e $\tilde{G}$ saranno basi minimali per I, il che implica, come si può provare per esercizio, che

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

Quindi, dato $g \in G$ esiste un $\tilde{g} \in \tilde{G}$ tale che $LT(g) = LT(\tilde{g})$. Se si può provare che $g = \tilde{g}$, seguirà che $G = \tilde{G}$, e l'unicità sarà dimostrata.

Per vedere che $g = \tilde{g}$, consideriamo l'elemento $g - \tilde{g}$ di I. Essendo G una base di Groebner, risulta $\overline{g - \tilde{g}}^G = 0$. Ma $LT(g) = LT(\tilde{g})$, quindi i termini direttori si cancellano in $g - \tilde{g}$ e nessuno dei termini rimanenti è divisibile per qualche elemento di $LT(G) = LT(\tilde{G})$, poiché G e $\tilde{G}$ sono ridotte. Questo dimostra che $\overline{g - \tilde{g}}^G = g - \tilde{g} = 0$, da cui segue che $g = \tilde{g}$. ∎

Osservazione.

Molti sistemi di algebra computazionale, implementano una versione dell'algoritmo di Buchberger per il calcolo di basi di Groebner ridotte. L'unicità ora dimostrata implica quindi che tali sistemi dànno tutti la stessa risposta.

Un'altra conseguenza dell'unicità, è che si può ottenere un **algoritmo di uguaglianza per ideali** che permetta di verificare quando due dati insiemi di polinomi $\{f_1, \ldots, f_s\}$ e $\{g_1, \ldots, g_t\}$ generano lo stesso ideale. L'algoritmo è semplicissimo: fissato un ordine monomiale, si calcolano le basi di Groebner ridotte per $< f_1, \ldots, f_s >$ e $< g_1, \ldots, g_t >$ i due ideali risulteranno uguali se e solo se le basi di Groebner coincidono.

Per concludere questo paragrafo, illustriamo qualcuna delle *connessioni tra l'algoritmo di Buchberger e l'eliminazione di Gauss per sistemi di equazioni lineari*. Il fatto interessante è che l'algoritmo di Gauss-Jordan, che dà la riduzione a scala di una matrice, è essenzialmente un caso particolare dell'algoritmo di Buchberger. Per concretezza, discuteremo un caso particolare di sistema di equazioni lineari.

Esempio.

Si consideri il sistema di equazioni lineari

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

Con operazioni elementari sulle righe della matrice si ottiene

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

Per ottenere una matrice a scala *ridotta* si deve essere sicuri che ciascun 1 direttore sia l'unico 1 nella propria colonna. Questo dà la matrice

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

In algebra tali calcoli si traducono come segue: sia I l'ideale

$$I =< 3x - 6y - 2z, 2x - 4y + 4w\,,\, x - 2y - z - w > \leq k[x, y, z, w]$$

corrispondente al sistema di equazioni assegnato. La prima matrice ci fornisce la seguente base di Groebner

$$I =< x - 2y - z - w\,,\, z + 3w >,$$

che è *minimale*, mentre la seconda matrice fornisce l'unica base di Groebner *ridotta*

$$I =< x - 2y + 2w\,,\, z + 3w > .$$

Il fatto, noto in algebra lineare, che ogni matrice si possa porre, in modo unico, nella forma ridotta a scala può essere visto come un caso particolare dell' unicità delle basi di Groebner ridotte.

3.8 Applicazioni delle basi di Groebner

All'inizio del capitolo sono stati presentati quattro problemi. Il primo tra questi, il problema della descrizione dell'ideale, è stato risolto tramite il teorema della base di Hilbert. In questo paragrafo esamineremo gli altri tre problemi e faremo vedere come si possano risolvere utilizzando le basi di Groebner.

3.8.1 Problema di appartenenza

Combinando insieme l'algoritmo di divisione con le basi di Groebner, si ha il seguente **algoritmo di appartenenza ad un ideale**: Dato un ideale polinomiale $I =< f_1, \ldots, f_s >$, e fissato un ordine monomiale, si può decidere se un polinomio f appartiene o meno ad I nel seguente modo.

(I) Utilizzando l'algoritmo di Buchberger, si trova una base di Groebner $G = \{g_1, \ldots, g_t\}$ per l'ideale I.

(II) Utilizzando l'algoritmo di divisione si calcola il resto $\bar{f}^G$ della divisione di f per G. Per il Corollario 3.6.1 si ha che

$$f \in I \Longleftrightarrow \bar{f}^G = 0.$$

Esempio 1.

Fissato l'ordinamento DEGLEX con $x > y > z$ in $\mathbf{C}[x, y, z]$, consideriamo il problema di appartenenza del polinomio $f = -4x^2y^2z^2 + y^6 + 3z^5$ all'ideale $I =< f_1, f_2 >=< xz - y^2\,,\, x^3 - z^2 >$. L'insieme di generatori indicato per I non è una base di Groebner, in quanto $LT(I)$ contiene anche polinomi del tipo $LT(S(f_1, f_2)) = LT(-x^2y^2 + z^3) = x^2y^2$ che non sono nell'ideale $< LT(f_1), LT(f_2) >=< xz\,,\, x^3 >$. Calcolando una base di Groebner per I si trova la base di Groebner ridotta

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

Dividendo f per la base G si trova

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

Poiché il resto è nullo si può affermare che $f \in I$. Se invece consideriamo $f = xy - 5z^2 + x$ anche senza eseguire la divisione per G si vede che il $LT(f) = xy$ non è chiaramente un elemento di $< LT(G) >=< xz, x^2y^2, xy^4y^6 >$. Quindi $\bar{f}^G \neq 0$ e, pertanto, $f \notin I$.

3.8.2 Risoluzione di equazioni polinomiali

Vediamo ora come il metodo delle basi di Groebner si possa utilizzare nella risoluzione di equazioni polinomiali, in più variabili.

Esempio 2.

Consideriamo le equazioni

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

in $\mathbf{C}^3$. Queste equazioni determinano l'ideale di $\mathbf{C}[x,y,z]$

$$I =< x^2+y^2+z^2-1\,,\, x^2+z^2-y\,,\, x-z > .$$

Per trovare tutti i punti della varietà $\mathcal{V}(I)$, si può usare una qualsiasi base di I. Tuttavia, la base di Groebner ridotta, rispetto all'ordinamento lessicografico con $x > y > z$

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

presenta il vantaggio che il polinomio g_3 dipende solo dalla variabile z. Si può ricavare z^2 utilizzando la formula risolutiva delle equazioni di secondo grado, estraendo poi la radice quadrata si ha che le soluzioni dell'equazione $g_3 = 0$ sono

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

Questo fornisce quattro valori per z, sostituendo questi valori nelle equazioni $g_2 = 0$ e $g_1 = 0$, possiamo ricavare sia la x che la y. Si ottengono in tal modo *tutte* le soluzioni del sistema iniziale e, quindi, tutti i punti di $\mathcal{V}(I) = \mathbf{V}(g_1, g_2, g_3)$.

Esempio 3.

Supponiamo di voler determinare il massimo ed il minimo della funzione $x^3+2xyz-z^2$ soggetta al vincolo $x^2+y^2+z^2=1$. Applicando la teoria

dei moltiplicatori di Lagrange, si ricava il seguente sistema di equazioni polinomiali:

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

Fissato in $\mathbf{R}[x, y, z, \lambda]$ l'ordine LEX con $\lambda > x > y > z$ e calcolando la base di Groebner ridotta per l'ideale definito da tali equazioni, si ottiene

$$\begin{array}{ll} \lambda & -\frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 - \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ x^2 & +y^2 + z^2 - 1, \\ xy & -\frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ xz & +yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ y^3 & +yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ y^2z & -\frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ yz^3 & -yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{188}z^2, \\ z^7 & -\frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z. \end{array}$$

A prima vista questa collezione di polinomi sembra orribile, ma, se si osserva meglio, ci si rende conto che, ad esempio, l'ultimo polinomio dipende dall'unica variabile z e le sue radici sono

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

Sostituendo ciascuno di questi valori negli altri polinomi della base di Groebner e uguagliando a zero, è possibile determinare *tutte* le soluzioni del sistema

$$z = 0, \quad y = 0, \quad x = \pm 1.$$

$$z = 0, \quad y = \pm 1, \quad x = 0.$$

$$z = \pm 1, \quad y = 0, \quad x = 0.$$

$$z = \frac{2}{3}, \quad y = \frac{1}{3}, \quad x = \frac{-2}{3}.$$

$$z = \frac{-2}{3}, \quad y = \frac{-1}{3}, \quad x = \frac{-2}{3}.$$
$$z = \frac{\sqrt{11}}{8\sqrt{2}}, \quad y = \frac{-3\sqrt{11}}{8\sqrt{2}}, \quad x = \frac{-3}{8}.$$
$$z = \frac{-\sqrt{11}}{8\sqrt{2}}, \quad y = \frac{3\sqrt{11}}{8\sqrt{2}}, \quad x = \frac{-3}{8}.$$

Da queste è semplice scegliere il minimo ed il massimo. Gli esempi 2 e 3 mostrano che determinare una base di Groebner di un ideale I, rispetto all' ordine lessicografico semplifica la forma delle equazioni della varietà $\mathcal{V}(I)$. In particolare si trovano equazioni in cui le variabili si eliminano successivamente. L'ordine di eliminazione sembra corrispondere all'ordine scelto per le variabili. Nell'esempio 3 è $\lambda > x > y > z$ e se si guarda la base di Groebner, si vede che λ è eliminata per prima, x per seconda e così via.

Un sistema di equazioni di questo tipo è facilmente risolvibile, specialmente quando l'ultima equazione contiene solo una variabile. Si possono, naturalmente, applicare tecniche usate nel caso di una variabile per provare a determinarne le soluzioni e sostituire poi tali valori nelle altre fino a determinare l'insieme di tutte le soluzioni. Si noti l' analogia tra questo procedimento e il metodo di Gauss Jordan per la risoluzione di sistemi di equazioni lineari.

Nel Capitolo 3 vedremo perché l'ordine lessicografico dà una base di Groebner che elimina successivamente le variabili

3.8.3 Problema di implicitizzazione

Supponiamo che le seguenti equazioni parametriche:

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

definiscano un sottoinsieme di una varietà algebrica $\mathbf{V}$ di k^n. Si possono utilizzare le basi di Groebner per determinare le equazioni polinomiali nelle x_i che definiscono $\mathbf{V}$, anche se una soluzione completa al problema di implicitizzazione potrà essere data solo nel capitolo 3.

Per semplicità, ci restringiamo al caso in cui le f_i sono polinomi. Si può studiare la varietà di k^{n+m} definita dalle seguenti equazioni:

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

ossia la $\mathcal{V}(I)$ definita dall'ideale

$$I =< x_1 - f_1(t_1, \ldots, t_m) \, , \ldots, x_n - f_n(t_1, \ldots, t_m) >$$

di $A = k[t_1, \ldots, t_m, x_1, \ldots, x_n]$. L'idea è quella di eliminare le variabili $t_1, \ldots, t_m$ dalle equazioni sopra scritte.

Usando nell'anello $k[t_1, \ldots, t_m, x_1, \ldots, x_n]$, l'ordine LEX con

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

si determina una base di Groebner dell'ideale I e, come prima, in questa base ci saranno polinomi che dipendono solo solo dalle variabili $x_1, \ldots, x_n$. Tali generatori ci forniranno le equazioni di una varietà che sicuramente contiene i punti della parametrizzazione.

Le idee appena descritte verranno esaminate in dettaglio nel capitolo 3, in cui studieremo la teoria dell'eliminazione. Per il momento ci accontenteremo di alcuni esempi.

Esempio 4.

Consideriamo le equazioni parametriche

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

che definiscono una curva in $\mathbf{C}^3$. Una base di Groebner G, rispetto a LEX, con $t > x > y > z$ dell'ideale

$$I =< x - t^4 \, , \, y - t^3 \, , \, z - t^2 >$$

è data da

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

Gli ultimi due polinomi dipendono soltanto da x, y, z e definiscono una varietà di $\mathbf{C}^3$, che contiene la curva assegnata parametricamente.

Esempio 5.

Consideriamo, in $\mathbf{R}^3$, la superficie $\Sigma(t, u)$ tangenziale alla cubica sghemba. Tale superficie ha la rappresentazione parametrica

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

Una base di Groebner, rispetto all'ordinamento lessicografico con $t > u > x > y > z$ contiene, come vedremo presto, sette elementi tra cui uno, sia g_7, dipende solo dalle variabili x, y, z. La varietà definita dall'equazione

$$g_7 = -(4/3)x^3z + x^2y^2 + 2xyz - (4/3)y^3 - (1/3)z^2 = 0$$

contiene la $\Sigma(t, u)$. E' comunque possibile che la superficie definita dall'equazione $g_7 = 0$ sia più grande della superficie tangenziale alla cubica sghemba, ossia esistano punti della $\mathcal{V}(g_7)$ le cui coordinate non soddisfino le equazioni della $\Sigma(t, u)$. Ritorneremo su ciò nel capitolo 3.

Riassumendo i risultati di questo paragrafo: si è visto che le basi di Groebner e l'algoritmo di divisione dànno una soluzione completa al problema di appartenenza di un polinomio f ad un ideale I, ossia, geometricamente, risolvono il problema di stabilire se la varietà $\mathcal{V}(I)$ è una sottovarietà dell'ipersuperficie $\mathcal{V}(f)$. Inoltre, si è visto come dare soluzioni di sistemi di equazioni polinomiali e come trovare equazioni implicite (o cartesiane) di un sottoinsieme dello spazio affine assegnato tramite equazioni parametriche. Ci siamo riusciti in quanto le basi di Groebner, se calcolate rispetto all'ordine LEX, sembrano eliminare le variabili in un modo "buono". Nel prossimo capitolo vedremo che ciò succede sempre ed esploreremo altri aspetti di quella che si chiama Teoria dell'eliminazione.

Bibliografia

[1] C. Bajaj, T. Garrity e J. Warren, *On the applications of multi-equational resultants*, Technical Report CSD-TR-826, 1988, Department of Computer Science, Purdue University.

[2] D. Becker e V. Weispfenning, *Groebner bases*, Springer-Verlag, New York-Berlin-Heidelberg.

[3] J.W. Bruce e P.J. Giblin, *Curves and Singularities*, 1984, Cambridge University Press, Cambridge.

[4] B. Buchberger, *Groebner bases: an algorithmic method in polynomial ideal theory*, 1985, N.K. Bose, D. Reidel Publishing Company, Dordrecht.

[5] J. Canny e D. Manocha, Multipolynomial resultant algorithms, *J. Symbolic Comput.***15**, 1993, 99-122.

[6] S.C. Chou, *Mechanical Geometry Theorem Proving*, D. Reidel Publishing Company, Dordrecht, 1988.

[7] R. Ciampi Procesi, *Elementi di algebra lineare*, 1982, Decibel, Padova.

[8] D. Cox, J. Little e D. O'Shea, *Ideals, Varieties and Algorithms*, 1991, Springer-Verlag, New York Berlin Heidelberg.

[9] J.H. Davenport, Y.Siret e E.Tournier, *Computer Algebra*, 1988, Academic Press, New York.

[10] D. Eisenbud, C. Huneke e W. Vasconcelos, Direct methods for primary decomposition, Invent. Math. **110**, 1992, 207–235.

[11] R. Gebauer e H.M. Möller, *On an installation of Buchberger' s algorithm*, in *Computational Aspects Of Commutative Algebra*, edited by L.Robbiano,1988, Academic Press, New York, 141–152.

[12] I. Gelfand, M. Kapranov e A.Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*, 1994, Birkhäuser, Basel Boston Berlin.

[13] P. Gianni, B. Trager e G. Zacharias, *Groebner bases and primary decomposition of polynomial ideals*, in *Computational Aspects of Commutative Algebra*, edited by L. Robbiano, 1988, Academic Press, New York, 15–33.

[14] G. Hermann, Der Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Annalen* **95**, 1926, 736–788.

[15] I.N. Herstein, *Algebra*, 1994, Editori Riuniti, Roma.

[16] J. Jouanolou, Le formalisme du résultant, *Advances in Math.***90**, 1991, 117-263.

[17] F. Macaulay, On some formula in elimination, *Proc. London Math. Soc.***3**, 1902, 3-27.

[18] M. Mignotte, *Mathematics for Computer Algebra*, 1992, Springer-Verlag, New York Berlin Heidelberg.

[19] R. Mines, F. Richman e W. Ruitenburg, *A Course in Constructive Algebra*, 1988, Springer-Verlag, New York Berlin Heidelberg.

[20] R.B. Miskra (1993)*Algorithmic Algebra* Text and Monographs in computer Science, Pringer-Varlag, New York-Berlin-Heidelberg.

[21] R. Paul, *Robot Manipulator: Mathematics, Programming and Control*, MIT Press, Cambridge, Massachusetts.

[22] A. Seidenberg, Constructions in Algebra, *Trans. Amer, Math. Soc.* **197**, 1974, 273–313.

[23] A. Seidenberg, On the Lasker-Noether decomposition theorem, *Am. J. math.* **106**, 1984, 611–638.

[24] van der Waerden, *Modern Algebra, Volume II*, 1931, Springer-Verlag, Berlin.

[25] D. Wang, *Characteristic sets and zero structure of polinomial sets*, RISC-LINZ, Johannes Kepler University, Linz, Austria.

Indice