Capitolo IV. Divisioni in $A=k[x_1,\ldots,x_n]$ [1] e Teorema della base

Nel §7 del Cap. I si è visto che dati due polinomi a coefficienti in un anello (commutativo con unità) in *una* indeterminata il secondo dei quali abbia coefficiente direttore invertibile nell'anello esistono e sono unici il quoziente e il resto nella divisione del primo per il secondo. E se i polinomi hanno 2 o più indeterminate?
Talora si può pensare di leggere i polinomi di $k[x,y]$ come polinomi di $(k[x])[y]$ o di $(k[y])[x]$.
Ad esempio il polinomio $x^3y+6xy^3-2xy^2-x^2-y^2-x$ può essere diviso per $y^2-xy-y+x$, con l'algoritmo della divisione pur di [2] pensarli entrambi come polinomi di $(k[x])[y]$:

$$6xy^3-(2x+1)y^2+x^3y-(x^2+x)=[y^2-(x+1)y+x][6xy+(6x^2+4x-1)]+[(7x^3+4x^2+3x-1)y-(6x^3+5x^2)].$$

Ma lo stesso dividendo non può essere diviso da $-xy-y+x$, né pensando i due polinomi come elementi di $(k[x])[y]$, né pensandoli come elementi di $(k[y])[x]$, poiché in entrambi i modi il coefficiente direttore del divisore è un polinomio di primo grado e quindi non è invertibile.
Ancora, $x^3y+6xy^3-2xy^2-x^2-y^2-x$ può essere diviso per x^2+y^2 tanto pensando i due polinomi come elementi di $(k[x])[y]$ che pensandoli come elementi di $(k[y])[x]$. Ma nel primo caso il quoziente è $6xy-(2x+1)$ e il resto $-5x^3y+2x^3-x$, nel secondo il quoziente è $xy-1$ e il resto $5xy^3-2y^2-1$.

Questi esempi ci convincono che fare la divisione nell'anello dei polinomi a coefficienti in un anello di polinomi non è una strada efficiente.
Per di più noi abbiamo in mente di copiare, se possibile, la strategia vista in $k[x]$ per stabilire, dato un ideale, se un elemento dell'anello gli appartiene. Ora, in $A=k[x_1,\ldots,x_n]$ incontreremo qualche difficoltà in più, poiché certamente ci sono ideali non principali (ad esempio quelli generati da due indeterminate) e questo ci costringerà ad inventare un algoritmo della divisione che permetta di dividere un polinomio mediante due o più altri, cercando di pervenire ad un risultato "ragionevolmente unico"; il nostro obiettivo è di dire che, se dividendo un polinomio per un certo insieme di polinomi divisori il resto non è zero, allora il polinomio non sta nell'ideale generato dall'insieme dei divisori: quindi siamo interessati al resto più che ai quozienti, ma vorremmo che il resto fosse univocamente determinato, che non dipendesse ad esempio dall'ordine in cui si presentano i divisori.
Vedremo che questo progetto è in generale troppo ambizioso: resta comunque il problema di inventare la divisione per più di un divisore.

1. ALGORITMO DELLA DIVISIONE IN $A=k[x_1,\ldots,x_n]$

Che cosa vuol dire fare la divisione di un polinomio $f\in A$ per s polinomi, dati in un certo ordine: $f_1,\ldots,f_s$?
Rifacendosi al caso $n=1$, deve significare trovare - **in maniera unica** - in A dei quozienti $a_1,\ldots,a_s$ ed un resto r in modo che

(1) $$f= a_1f_1+\ldots+ a_sf_s+r$$

e il **resto "non sia più divisibile per nessuno degli** f_i".
Le due frasi in grassetto devono essere formalizzate.

I) Nel caso $n=1$, per dividere cerco il quoziente nella divisione del termine direttore del dividendo per il termine direttore del divisore e poi itero su un nuovo dividendo. Ma nel caso $n=1$ il termine direttore è semplicemente il termine di grado massimo: invece se $n>1$ ci possono essere monomi che hanno lo stesso grado totale massimo, pur non avendo lo stesso

[1] Con k si denota sempre un campo.
[2] Non funziona invece l'idea di pensarli come polinomi di $(k[y])[x]$ poiché il coefficiente direttore $(1-y)$ del polinomio divisore $x(1-y)+y^2-y$ non è invertibile in $k[y]$.

multigrado. Di qui la necessità di fissare nell'insieme $\mathbb{T}^n$ dei monomi di $\mathbf{A}$ un ordinamento monomiale, che permetta di individuare il monomio "massimo" in un polinomio f e quindi il termine direttore di f [3]. Precisiamo questa affermazione con la seguente

DEFINIZIONE 1.1 *Sia* $f=\sum c_\alpha \mathbf{x}^\alpha$ *un polinomio di* $\mathbf{A}$ *ed* S *il suo supporto. Fissato un ordinamento monomiale* σ *in* $\mathbb{T}^n$*, si dice* ***monomio direttore*** *(leading monomial) di* f *e si denota con* LM(f) *il monomio* $\mathbf{x}^\mu$ *di* S *massimo rispetto a* σ*. Si dice* ***termine direttore*** *(leading term) e si denota con* LT(f) *il prodotto* $c_\mu \mathbf{x}^\mu$ *del monomio direttore per il coefficiente* c_μ *con cui esso compare in f: tale coefficiente è detto* ***coefficiente direttore*** *di f e si denota con* Lc(f) [4].

II) Che il resto r non sia più divisibile per $f_1,\ldots,f_s$ significa o che r è il polinomio nullo oppure che r è combinazione lineare a coefficienti in k [5] di monomi nessuno dei quali è divisibile per uno dei termini LT(f_1),…, LT(f_s).

III) Per avere l'unicità bisogna evidenziare una regola univoca per procedere. L'idea è che in a_2LT(f_2) non devono poter comparire monomi divisibili per LT(f_1) (e che quindi potrebbero essere riassorbiti in una scrittura del tipo a_1LT(f_1)), che in a_3LT(f_3) non devono poter comparire monomi divisibili per LT(f_1) o per LT(f_2) e così via. Più formalmente: ogni polinomio quoziente a_i, se non è nullo, è combinazione k-lineare di monomi nessuno dei quali, moltiplicati per LT(f_i) dà un termine divisibile per LT(f_j) con $1 \le j \le i-1$.

Dimostriamo che, fissato l'ordine di entrata in scena di $f_1,\ldots,f_s$, le tre condizioni elencate sopra implicano l'unicità dei quozienti e dei resti; se ne proverà invece l'esistenza creando un algoritmo che rispetti le tre condizioni.

TEOREMA DI UNICITÀ *Fissato in* $\mathbf{A}$ *un ordinamento monomiale* σ *e data la s-upla ordinata di divisori* $(f_1,\ldots,f_s)$*, se*

$$f = a_1f_1+\ldots+a_sf_s+r = b_1f_1+\ldots+b_sf_s+r'$$

e le due $(s+1)$*-uple ordinate* $(a_1,\ldots,a_s,r)$ e $(b_1,\ldots,b_s,r')$ *soddisfano le condizioni* (I)*,* (II)*,* (III)*, allora risulta*

$$a_1=b_1,\quad a_2=b_2,\quad \ldots\ldots,\ a_s=b_s,\quad r=r'.$$

Dimostrazione Nelle ipotesi del teorema risulta: $(a_1-b_1)f_1+\ldots+(a_s-b_s)f_s+(r-r')=0$ e per ogni i $(1\le i\le s)$, i monomi che compaiono in (a_i-b_i) compaiono in almeno uno dei polinomi a_i, b_i: dunque, moltiplicati per LT(f_i) non danno termini divisibili per LT(f_j) se $1\le j\le i-1$. Analogamente i monomi di $r-r'$ non sono divisibili per alcuno dei termini LT(f_1),…, LT(f_s).
Dunque la dimostrazione è ricondotta a mostrare che la divisione del polinomio nullo con le regole date dalle condizioni (I), (II), (III) dà quozienti e resto nulli.
Sia dunque $0=A_1f_1+\ldots+A_sf_s+R$. Supponiamo che per qualche i si abbia $A_i\neq 0$: allora LT(A_if_i) $\neq 0$. Tra questi i ne scegliamo uno per cui LM(A_if_i) è massimo: visto che la somma deve dare 0, ci deve essere qualche altro termine nella somma che si compensa con esso e, avendo scelto i in modo che il multigrado sia massimo, sicuramente questi termini "compensativi" devono essere dei LT (di A_jf_j o di R). Ma non può essere LM(R)=LM(A_if_i)=LM(A_i)LM(f_i), poiché per la condizione (II) nessun LM(f_i) divide LM(R); similmente non può essere LM(A_i)LM(f_i)=LM(A_if_i)=LM(A_jf_j)=LM(A_j)LM(f_j), poiché per la condizione (III) se $i<j$ LM(f_i) non divide LM(A_j)LM(f_j) e se $j<i$ LM(f_j) non divide LM(A_i)LM(f_i). Dunque per ogni i si ha $A_i=0$ e di conseguenza anche $R=0$. C.V.D.

---

[3] Non si affronta qui il problema della dipendenza dall'ordine delle variabili: per mostrarla, usare $f=x^2+y$ e $f_1=x+y$ con ordinamento LEX.

[4] Può essere utile osservare che, dati due polinomi f, g in $\mathbf{A}$, LM(fg)=LM(f) LM(g) ed, essendo k un campo, Lc(fg)=Lc(f)Lc(g), per cui anche LT(fg)= LT(f) LT(g).

[5] Invece di "combinazione lineare a coefficienti in k", nel seguito diremo più brevemente "combinazione k-lineare".

La dimostrazione data mette in evidenza un'altra particolarità della rappresentazione ottenuta.

OSSERVAZIONE 1.2 *Fissato in* A *un ordinamento monomiale* σ *e data la s-upla ordinata di divisori* $(f_1,\dots,f_s)$, *se*

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

e la $(s+1)$*-upla ordinata* $(a_1,\dots,a_s,r)$ *soddisfa le condizioni* (I), (II), (III), *allora gli* $s+1$ *monomi*

$$\mathrm{LM}(a_1f_1),\dots, \mathrm{LM}(a_sf_s), \mathrm{LM}(r)$$

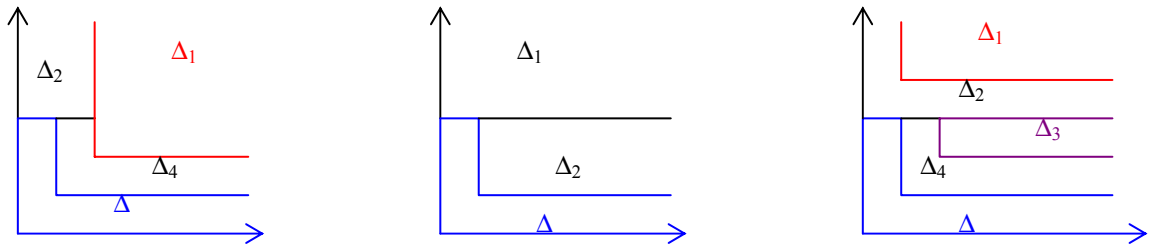
sono a due a due distinti e quindi il multigrado $\mathrm{Log}(\mathrm{LT}(f))$ *di* f *è non inferiore a* $\mathrm{Log}(\mathrm{LT}(a_if_i))$ [(6)].

NOTA Le condizioni (II) e (III) sono di fatto condizioni sui multigradi, poiché $\boldsymbol{x}^{\boldsymbol{\alpha}}$ divide $\boldsymbol{x}^{\boldsymbol{\beta}}$ se e solo se $\beta\in\alpha+\mathbf{N}^n$. Si può allora riorganizzare il discorso in questo modo. Osserviamo che, posto $\alpha(i)=\mathrm{Log}(\mathrm{LT}(f_i))$, i termini di $a_i\mathrm{LT}(f_i)$ sono divisibili per $\mathrm{LT}(f_i)$ e quindi il loro multigrado sta in $\alpha(i)+\mathbf{N}^n$; similmente chiedere che essi non siano divisibili per $\mathrm{LT}(f_j)$ per ogni $j<i$ significa che il loro multigrado non appartiene a nessuno degli insiemi $\alpha(1)+\mathbf{N}^n,\dots, \alpha(i-1)+\mathbf{N}^n$ e chiedere che i termini di r non siano divisibili per $\mathrm{LT}(f_i)$ significa che il loro multigrado non appartiene a nessuno degli insiemi $\alpha(1)+\mathbf{N}^n,\dots, \alpha(s)+\mathbf{N}^n$. Da queste considerazioni nasce una partizione di $\mathbf{N}^n$, che dipende dall'ordinamento monomiale σ e dall'ordine dei polinomi divisori:

$$\Delta_1=\alpha(1)+\mathbf{N}^n$$
$$\Delta_2=[\alpha(2)+\mathbf{N}^n] \setminus \Delta_1$$
$$\Delta_3=[\alpha(3)+\mathbf{N}^n] \setminus [\Delta_1\cup\Delta_2]$$
$$\dots..$$
$$\Delta_s=[\alpha(s)+\mathbf{N}^n] \setminus [\Delta_1\cup\Delta_2 \cup\dots\cup\Delta_{s-1}]$$
$$\Delta= \mathbf{N}^n \setminus [\Delta_1\cup\Delta_2 \cup\dots\cup\Delta_s].$$

Alcune di queste classi possono anche essere vuote: ciò succede alla classe Δ_i quando $\mathrm{LT}(f_j)$ divide $\mathrm{LT}(f_i)$ e quindi $\alpha(i)\in\alpha(j)+\mathbf{N}^n$ e $j<i$.

ESEMPIO DI PARTIZIONE
Consideriamo in $k[x,y]$ i 4 monomi direttori: $f=x^2y^2$, $g=y^3$, $h=xy^4$, $l=xy$, cioè le coppie: (2,2), (0,3), (1,4), (1,1). Vediamo come si ripartisce $\mathbf{N}^n$, considerando la quaterna di monomi direttori ordinata una prima volta come (f,g,h,l), una seconda volta come (g,l,f,h), una terza volta come (h,g,f,l).



Questa traduzione delle condizioni (II) e (III) permette di dare un enunciato molto stringato del teorema di esistenza ed unicità (vedi Robbiano):

TEOREMA 1.3 *Fissato in* $\mathbf{N}^n$ *un ordinamento monomiale* σ *e dati un polinomio* $f\in\mathsf{A}$ *e la s-upla ordinata di divisori non nulli* $(f_1,\dots,f_s)$, *esiste ed è unica la* $(s+1)$*-upla di polinomi* $(a_1,\dots,a_s, r)$ *tali che*

(i) $f = a_1f_1 +\dots+ a_sf_s +r$

(ii) *i termini non nulli che compaiono in* $a_i\mathrm{LT}(f_i)$ *hanno multigrado in* Δ_i [(7)]

(iii) *i termini non nulli che compaiono in* r *hanno multigrado in* Δ *e il multigrado di* $\mathrm{LT}(f)$ *non è inferiore ai multigradi di* $\mathrm{LT}(a_if_i)$ *per nessun* $i=1,\dots,s$.

---

(6) Con questo abbiamo dato una spiegazione dell'enunciato di Cox & C. che, peraltro, trascurano la condizione (III) e l'unicità, pur ritrovandola come sottoprodotto dell'algoritmo.

(7) Se ne ricava che, se Δ_i è vuoto, $a_i\mathrm{LT}(f_i)=0$ e quindi il quoziente a_i è nullo.

Di questo enunciato noi dobbiamo ancora dimostrare la parte che riguarda l'esistenza.
Prima di scrivere l'algoritmo che prova l'esistenza, cerchiamo di capirne, anche su esempi, il funzionamento.
L'algoritmo che dà la (s+1)-upla di quozienti e il resto lavora in cicli successivi: in ognuno di essi si crea un termine di uno degli s quozienti facendo la divisione del LT del polinomio dividendo "corrente" (cioè in esame in quel momento) per il LT di uno dei divisori (nell'ordine prefissato), via via riducendo il multigrado del LT del dividendo, oppure si incontra un LT non divisibile per i LT di alcuno dei divisori: si scarica questo LT nel "cestino dei termini non divisibili" (che alla fine darà il resto) e si inizia un nuovo ciclo.
Il meccanismo mima quello della divisione di un polinomio in 1 variabile per 1 polinomio. Osserviamo però che:

- anche in presenza di un solo divisore, l'avere più di una variabile può determinare la necessità di eliminare resti parziali, senza che questo implichi che la divisione si fermi (si veda la parte evidenziata in giallo della divisione dell'esempio 1.5 nella quale entra in gioco il solo divisore f_1); ciò è legato al fatto che – mentre è vero che se $\mathbf{x}^{\alpha}$ divide $\mathbf{x}^{\beta}$ risulta $\alpha<\beta$ – non è vero che se $\alpha<\beta$ allora necessariamente $\mathbf{x}^{\alpha}$ debba dividere $\mathbf{x}^{\beta}$: quindi possono esistere termini aventi multigrado minore di quello del termine finito nel resto parziale ma che sono divisibili per il LT del divisore;
- l'avere più di un divisore fa sì che l'ordine di divisione sia cruciale. In particolare va osservato che ogni ciclo deve iniziare testando la divisibilità del LT del dividendo "corrente" per il LT del 1° divisore (passando solo in caso di insuccesso al LT del 2° ecc.), anche se nel ciclo immediatamente precedente si è diviso per il LT di un altro divisore e questo divide ancora il LT del dividendo "corrente".

ESEMPIO 1.4
Già se l'indeterminata è una sola l'ordine di divisione è cruciale. Siano $f=x^3+2x^2$, $f_1=x^2+x+1$ e $f_2=x-1$. Allora, con la divisione operata in quest'ordine e nell'ordine opposto, si hanno i due risultati seguenti

Quozienti:	$a_1=x+1$ $a_2=-2$	
Divisori: $f_1=x^2+x+1$ $f_2=x-1$	$\mathbf{x^3+2x^2}$ $-x^3-x^2-x$	1° ciclo: divido per LT(f_1)
	x^2-x $-x^2-x-1$	2° ciclo: divido per LT(f_1)
	$-2x-1$ $2x-2$	3° ciclo: MA **divido per LT(f_2)**
Resto:	-3	

Quozienti:	$a_2=x^2+3x+3$ $a_1=0$	
Divisori: $f_2=x-1$ $f_1=x^2+x+1$	$\mathbf{x^3+2x^2}$ $-x^3+x^2$	1° ciclo: divido per LT(f_2)
	$3x^2$ $-3x^2+3x$	2° ciclo: divido per LT(f_2)
	$3x$ $-3x+3$	3° ciclo: divido per LT(f_2)
Resto:	3	

Quindi $f=(x+1)f_1+(-2)f_2-3=(x^2+3x+3)f_2+0\bullet f_1+3$.

ESEMPIO 1.5
Vediamo ancora come può cambiare il risultato cambiando l'ordine dei polinomi divisori, nel caso di polinomi in più di una variabile. Approfittiamo di questo esempio per mettere in evidenza non solo i vari cicli che portano alla costruzione di quozienti e resto, ma anche i sottocicli: il significato dei commenti alle due tabelle di divisione sotto riportate sarà più chiaro una volta visto l'algoritmo. Non segnaliamo i "tentativi andati a vuoto": la presenza di un sottociclo successivo al primo o di un resto parziale confermerà che ce ne sono stati.

In $k[x,y]$ con l'ordinamento LEX e $x>y$ dividiamo $f=x^2y+xy^2+y^3$ per la coppia ordinata $(xy-1, y^2-1)$ e poi per la coppia ordinata $(y^2-1, xy-1)$.

Quozienti:	$a_1 = x+y$ $a_2 = y$		
Divisori: $f_1 = xy-1$ $f_2 = y^2-1$	$\mathbf{x^2y+xy^2+y^3}$ $-x^2y+x$	1° sottociclo [… /LT(f_1)]	1° ciclo
	xy^2+x+y^3 $-xy^2+y$	1° sottociclo [… /LT(f_1)]	2° ciclo
	$x+y^3+y$	Resto parz.→	3° ciclo x
	y^3+y $-y^3+y$	2° sottociclo [… /LT(f_2)]	4° ciclo
	$2y$	Resto parz.→	5° ciclo $2y$
	0	Resto:	$x+2y$

Quozienti:	$a_1 = x+y$ $a_2 = x$		
Divisori: $f_1 = y^2-1$ $f_2 = xy-1$	$\mathbf{x^2y+xy^2+y^3}$ $-x^2y+x$	2° sottociclo [… /LT(f_2)]	1° ciclo
	xy^2+x+y^3 $-xy^2+x$	1° sottociclo [… /LT(f_1)]	2° ciclo
	$2x+y^3$	Resto parz.→	3° ciclo $2x$
	y^3 $-y^3+y$	1° sottociclo [… /LT(f_1)]	4° ciclo
	y	Resto parz.→	5° ciclo y
	0	Resto:	$2x+y$

Ora, per descrivere i vari cicli che compongono l'algoritmo, osserviamo che:

- ogni nuovo ciclo principale comincia con un dividendo "corrente" p nuovo (tanto se al ciclo precedente è stato possibile dividere per un LT(f_i) che se non lo è stato): quindi si deve porre $i=1$ (infatti si deve dividere per LT(f_1)) e la variabile booleana iniziale – corrispondente alla domanda: è avvenuta la divisione del LT del dividendo "corrente" per qualche LT(f_i) – va posta =false.
- ogni ciclo è composto da un PASSO di DIVISIONE ed un eventuale PASSO di RESTO. Dei due rami di divisione, uno (IF) corrisponde al fatto che, per un certo i, LT(f_i) divide il LT del dividendo "corrente" e il suo realizzarsi fa ripartire un nuovo ciclo principale, l'altro (ELSE) è un passo che fa scattare il successivo sottociclo. Formalmente:

Input: σ, $(f_1, \ldots, f_s), f$ Output: $(a_1, \ldots, a_s, r)$			
$a_1 := 0;\ \ldots\ ; a_s := 0;\ r := 0$ $p := f$			inizializzazione
WHILE	$p \neq 0$ DO $i := 1$ divisionoccurred := false		Parametri iniziali Variab. Bool. iniz.

	WHILE $i \leq s$ AND divisionoccurred = false DO
	IF LT(f_i) divide LT(p) THEN
	$a_i := a_i + \text{LT}(p)/\text{LT}(f_i)$
	$p := p - [\text{LT}(p)/\text{LT}(f_i)]\, f_i$
	divisionoccurred := true
		Ramo di IF: poiché la variabile Booleana è true, fa uscire dal ciclo secondario di WHILE	Passo di divisione

	ELSE $i := i+1$	Ramo di ELSE: fa scattare un nuovo i	
	IF (*) divisionoccurred = false THEN $r := r + \text{LT}(p)$ $p := p - \text{LT}(p)$		Passo di resto

Nota: questo è l'algoritmo proposto da Cox & C. ma in (*) sembra necessario aggiungere $i > s$.

Per garantire che l'algoritmo produca esattamente i quozienti e i resti bisogna mostrare che esso termina e soddisfa le condizioni (i), (ii), (iii) del teorema 1.3.
Innanzi tutto, **l'algoritmo termina**. Infatti ad ogni passo, se $p\neq 0$, Log(LT(p)) diminuisce (perché nei passi di divisione p e $[LT(p)/LT(f_i)]\,f_i$ hanno lo stesso LT e anche nel passo di resto, se $p\neq 0$, p e LT(p) hanno lo stesso LT): si crea così una catena strettamente decrescente di multigradi che deve essere finita, poiché l'ordinamento è monomiale e quindi, in particolare, buono (vedi Cap. III, lemma 1.2). Questo significa che esiste un passo in cui p diventa 0 (e quindi l'algoritmo termina).
Per **provare (i)** mostriamo che a ogni passo risulta $f=a_1f_1+\ldots+a_sf_s+p+r$ (ove gli a_i e r sono quelli "correnti" in quel passo).
Al passo iniziale si ha $f=0f_1+\ldots+0f_s+p+0$; nei passi intermedi, se il passo è di divisione significa che per un certo i si deve operare una sostituzione del tipo

$$f=a_1f_1+\ldots+a_sf_s+p+r=a_1f_1+\ldots+a_{i-1}f_{i-1}+[a_i+LT(p)/LT(f_i)]f_i+a_{i+1}f_{i+1}+\ldots+a_sf_s+p-[LT(p)/LT(f_i)]\,f_i+r$$

(evidenziati gli addendi nuovi che si sostituiscono a a_if_i), se il passo è di resto si sostituisce

$$f=a_1f_1+\ldots+a_sf_s+p+r=a_1f_1+\ldots+a_sf_s+[p-LT(p)]+[r+LT(p)].$$

Quando l'algoritmo termina, si ha $p=0$ e quindi $f=a_1f_1+\ldots+a_sf_s+r$.
Per **provare (ii)** si considerino i termini non nulli di $a_iLT(f_i)$: ognuno di essi era il LT(p) nel momento in cui (in un certo ciclo dell'algoritmo) si è diviso p per LT(f_i); ma se si è arrivati a dividere per LT(f_i) significa quel LT(p) non era divisibile per LT(f_1), ..., LT(f_{i-1}).
Infine **vale (iii)**, poiché i termini non nulli di r si ottengono esattamente raccogliendo i termini che non sono divisibili per alcun LT(f_i).
Ciò, insieme al teorema di unicità e all'osservazione 1.2 conclude la dimostrazione del teorema 1.3.

2. EQUIVOCI SULL'ALGORITMO

È facile fraintendere il senso del teorema 1.3. Qui di seguito sono elencati alcuni errori possibili.

1. Se posso scrivere $f=a_1f_1+\ldots+a_sf_s+r$ e
   (a) nessun LT(f_i) divide alcuno dei termini di r
   (b) Log(LT(f))≥Log(LT(a_if_i))
   allora ho rappresentato la divisione di f per $f_1,\ldots,f_s$ con quozienti $a_1,\ldots,a_s$ e resto r.

   Questo sembra quasi l'enunciato del Cox, ma in realtà Cox & C. affermano il contrario: essendoci l'algoritmo della divisione posso rappresentare f in un certo modo e soddisfacendo certe condizioni.
   D'altra parte possiamo fare due considerazioni concrete per convincerci che l'affermazione è falsa.
   - L'ordine di divisione è cruciale per cui può darsi che, mentre per la s-upla (f_1, …, f_s) la (s+1)-upla (a_1, …, a_s, r) rappresenta l'insieme dei quozienti e dei resti, ciò non sia più vero permutando l'ordine delle f (e coerentemente quello delle a).
     Vedere l'esempio 1.5 in cui $f=x^2y+xy^2+y^3$ (con σ=LEX, $x>y$): se si sceglie $f_1=xy-1$, $f_2=y^2-1$ si ha $a_1=x+y$, $a_2=y$ e $r=x+2y$, ma – anche se l'uguaglianza $f=yf_2+(x+y)f_1+(x+2y)$ è chiaramente vera, visto che è ottenuta permutando gli addendi della $f=a_1f_1+a_2f_2+r$ – la terna $(y,x+y,x+2y)$ non dà i quozienti e il resto nella divisione di f per (f_2,f_1), che sono invece $(x+y, x, 2x+y)$.
   - la (s+1)-upla (a_1, …, a_s, r) potrebbe non rappresentare i quozienti e il resto rispetto a nessun ordinamento dei divisori.
     Consideriamo ad esempio $f=2xy^2+y^3+1$ (con σ=LEX, $x>y$) e i divisori $g=x$ e $h=y$. Si può scrivere $f=y^2g+(xy+y^2)h+1$ e valgono le condizioni (a) e (b); ma quelli trovati non sono i quozienti e il resto nella divisione per (g,h) (che sarebbero $(2y^2, y^2, 1)$), né per (h,g) (che sarebbero $(2xy+y^2, 0, 1)$).

2. Quanto detto al punto 1 vale se aggiungo la condizione
   (c) nessun LT(f_j) divide alcuno dei termini di a_i, per ogni scelta di i e j.

Falso. Ad esempio, consideriamo $f=x^2y+xy^2+y^2-2y-1$ (con σ=LEX, $x>y$), $g=y^2-1$, $h=xy-1$.
Si ha $f=(-x+1)g+(x+2y)h$; LT(g)=y^2 e LT(h)=xy non dividono ($-x+1$) né ($x+2y$).
Ma dividendo per (g,h) si troverebbe $f=(x+1)g+xh+2(x-y)$;
dividendo per (h,g) si troverebbe $f=(x+y)h+1g+(x-y)$.
Che cosa manca alla prima rappresentazione?

3. Quanto detto al punto 2 vale se aggiungo la condizione: r=0.

   Falso: vedi esempio precedente.

4. La divisione risolve il problema dell'appartenenza di un polinomio a un ideale.

   Falso.
   - L'esempio al punto 2 dice che $f=x^2y-xy^2+y^2-2y-1$ appartiene all'ideale generato da $g=y^2-1$ e $h=xy-1$; ma entrambe le divisioni danno resto diverso da zero.
   - Un altro esempio un po' meno sgradevole si ha nell'esempio 5 contenuto al §3 del Cap. II di Cox & C.
     Infatti se $f=xy^2-x$ (con σ=LEX, $x>y$), $g=xy+1$, $h=y^2-1$, la divisione per (g,h) dà (y, 0, $xy+1$), e quindi resto non nullo, ma la divisione per (h,g) dà (x, 0, 0) e quindi almeno una divisione evidenzia resto 0.
   - Ancora, se $f=x^3-x^2y-x^2z+x$ (con σ=LEX, $x>y>z$), $g=x^2y-z$, $h=xy-1$, la divisione per (h,g) dà ($-x$, 0, x^3-x^2z), la divisione per (g,h) dà (-1, 0, x^3-x^2z+x-z), e quindi si ha resto non nullo in entrambi i casi.
     Si vede però che l'ideale generato da g e h contiene $g-xh=x-z$, anzi si può pensare generato da $x-z$ e da h [8]; inoltre $f=x^2(x-z)-xh$ e quindi sta nell'ideale.

Dunque è vero che se quozienti e resto sono (a_1, …, a_s, 0) allora f appartiene all'ideale generato da f_1, …, f_s, mentre in generale il viceversa è falso. Chiedere che sia vero per ogni scelta dell'ordine dei divisori f_1, …, f_s equivale - come vedremo - a chiedere che f_1, …, f_s sia una base di Gröbner per l'ideale. L'ultimo esempio suggerisce già una strategia di alterazione della base che risulterà utile per costruire basi di Gröbner.

3. IDEALI MONOMIALI

Prima di arrivare a parlare di basi Gröbner è necessario provare che gli ideali, in un anello di polinomi a coefficienti in un campo, possono essere generati da un numero finito di elementi. Gli ingredienti per questa dimostrazione sono l'algoritmo della divisione e il lemma di Dickson che in sostanza riduce il problema a particolari ideali, che andiamo ora a definire.

DEFINIZIONE 3.1 *Un* ***ideale*** I *di* $\mathbf{A}$ *è detto* ***monomiale*** *se esiste un sottoinsieme* A *di* $\mathbf{N}^n$*, eventualmente infinito, tale che l'insieme di monomi* $\{\boldsymbol{x}^\alpha \mid \alpha\in A\}$ *sia un sistema di generatori per* I*, cioè ogni polinomio f appartenente a* I *è una somma finita del tipo* $\sum h_\alpha \boldsymbol{x}^\alpha$*, con* $\alpha\in A$ *e* $h_\alpha\in \mathbf{A}$.

Come sono fatti i monomi che appartengono ad un ideale monomiale [9]?

LEMMA 3.2 *Sia* I *un ideale monomiale generato da* $\{\boldsymbol{x}^\alpha \mid \alpha\in A\}$. *Allora* $\boldsymbol{x}^\beta\in I$ *se e solo se esiste* $\alpha\in A$ *tale che* $\boldsymbol{x}^\alpha$ *divide* $\boldsymbol{x}^\beta$ *cioè* $\beta\in \alpha+\mathbf{N}^n$.
È ovvio che se $\alpha\in A$ e $\beta\in \alpha+\mathbf{N}^n$ allora $\boldsymbol{x}^\beta\in I$. Viceversa, se $\boldsymbol{x}^\beta=\sum h_{\alpha(i)}\boldsymbol{x}^{\alpha(i)}$, consideriamo i termini che compongono la somma a destra: la loro somma non è nulla e i termini che rimangono avranno forma $c_{\gamma(i,j)\alpha(i)}\boldsymbol{x}^{\gamma(i,j)}\boldsymbol{x}^{\alpha(i)}$, con $\boldsymbol{x}^\beta=\boldsymbol{x}^{\gamma(i,j)}\boldsymbol{x}^{\alpha(i)}$. Quindi per ogni $\alpha(i)$ con $c_{\gamma(i,j)\alpha(i)}\neq 0$, $\boldsymbol{x}^{\alpha(i)}$ divide $\boldsymbol{x}^\beta$. C.V.D.

Come sono fatti i polinomi che appartengono ad un ideale monomiale?

---

[8] Infatti, $g=xh+(x-z)$, e quindi sta nell'ideale generato da $x-z$ e da h; ogni altro polinomio che si scriva come $ag+bh$ si può riscrivere come $a(x-z)+(ax+b)h$.
[9] Il lemma successivo non nega che un monomio appartenente a un ideale monomiale possa avere rappresentazioni complicate. Ad esempio l'ideale generato da x^2y e xy^2 contiene $x^2y\bullet y=x^2y^2=(x^2y/2)\bullet y+(xy^2/2)\bullet x$

LEMMA 3.3 *Siano* I *un ideale monomiale generato da* $\{\boldsymbol{x}^{\alpha} \mid \alpha \in A\}$ *ed f un polinomio di* $\boldsymbol{A}$. *Sono equivalenti le condizioni:*

(i) *f appartiene a* I, *cioè* $f=\sum h_{\alpha(i)}\boldsymbol{x}^{\alpha(i)}$, *con* $\alpha(i)\in A$

(ii) *ogni termine di f sta in* I,

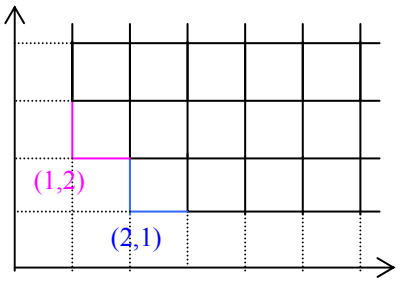
(iii) *f è combinazione k-lineare dei monomi di* I.

Dimostrazione (i)⇒(ii) poiché i termini di *f* hanno la forma $c_{\gamma(i,j)\alpha(i)}\boldsymbol{x}^{\gamma(i,j)}\boldsymbol{x}^{\alpha(i)}$ e quindi stanno in I.
(ii)⇒(iii) poiché se i termini di *f* stanno in I anche i corrispondenti monomi ci stanno ed *f* è somma di quei termini, cioè combinazione *k*-lineare di quei monomi.
(iii)⇒(i) per il lemma 3.2 ogni monomio di I ha la forma $\boldsymbol{x}^{\gamma}\boldsymbol{x}^{\alpha}$ con $\alpha\in A$. Raccogliendo per ciascun α i monomi che sono divisi da $\boldsymbol{x}^{\alpha}$ si ha la tesi.

È conseguenza immediata del lemma 3.3 il seguente

COROLLARIO 3.4 *Due ideali monomiali coincidono se e solo se contengono gli stessi monomi.*

Ciò giustifica il fatto che per rappresentare un ideale monomiale di solito si usano solo i monomi in esso contenuti, anzi il reticolo dei multigradi dei monomi in esso contenuti.
Ad esempio, per rappresentare l'ideale (x^2y, xy^2) generato in $k[x,y]$ dai monomi x^2y e xy^2 si considerano i multigradi (2,1), (1,2) dei due generatori e gli insiemi $(2,1)+\mathbf{N}^2$, $(1,2)+\mathbf{N}^2$ di multigradi che corrispondono ai monomi divisibili per almeno uno dei due generatori e se ne fa l'unione. Il risultato grafico è un reticolato intero come quello disegnato sotto (sono elementi di $[(2,1)+\mathbf{N}^2]\cup[(1,2)+\mathbf{N}^2]$ i vertici del reticolato non tratteggiato, ovviamente pensato illimitato; in particolare, all'incrocio di due segmenti colorati c'è il punto che indica un generatore dell'ideale).



LEMMA DI DICKSON *Ogni ideale monomiale (generato da un insieme* S *di monomi di cardinalità qualsiasi) è finitamente generato, nel senso che esiste un sottoinsieme finito* S' *di* S *che genera lo stesso ideale generato da* S.

Dimostrazione[(10)]. Sia $A\subseteq\mathbf{N}^n$ l'insieme dei multigradi dei monomi di S. Si vuole provare che esiste un sottoinsieme finito $A'=\{\alpha(1),\ldots,\alpha(t)\}$ di A tale che per ogni α di A esistono un $i\in\{1,\ldots,t\}$ e un γ in $\mathbf{N}^n$ tali che $\alpha=\alpha(i)+\gamma$. Questo infatti permette di garantire che ogni $\boldsymbol{x}^{\alpha}$ di S è divisibile per un $\boldsymbol{x}^{\alpha(i)}$ e quindi che il sottoinsieme finito $\{\boldsymbol{x}^{\alpha(1)},\ldots,\boldsymbol{x}^{\alpha(t)}\}$, generando S, genera anche l'ideale generato da S: *diremo brevemente che* A' *genera* A.
Si procede per induzione su *n*.

(10) In Cox & C. si trova sostanzialmente la stessa dimostrazione, salvo che si fa uso dei monomi invece che dei multigradi e degli ideali generati invece che degli insiemi di multigradi. Questo complica un po' la dimostrazione poiché richiede di mostrare che ogni monomio dell'ideale monomiale può essere diviso da uno dei presunti generatori. Inoltre trovati gli analoghi dei generatori di A_n, sostanzialmente associa ad essi *n*-uple con ultima componente costante $m=\max(m_i)$; ma (vedi esempio 3.5) non sembra che si possa rinunciare a far variare l'ultima componente se si vuole che le *n*-uple generatrici appartengano tutte all'insieme di partenza.

Per n=1 basta applicare il principio del buon ordinamento: l'insieme A ha minimo $\alpha(1)$ e l'insieme A' formato da questo elemento genera tutto A.
Suppongo l'enunciato valido per i sottoinsiemi di $\mathbf{N}^{n-1}$ e considero l'insieme (ottenuto per proiezione di A su $\mathbf{N}^{n-1}$)

$$A_n=\{\alpha'\in \mathbf{N}^{n-1} \mid \exists\, h\in\mathbf{N}\colon (\alpha', h)\in A\}.$$

Per l'ipotesi induttiva, esistono delle $(n-1)$-uple $\alpha'(1),\ldots,\alpha'(s)\in A_n$ tali che ogni $\alpha'\in A_n$ si può scrivere come $\alpha'=\alpha'(i)+\gamma'$, pur di scegliere opportunamente $i\in\{1,\ldots, s\}$ e γ' in $\mathbf{N}^{n-1}$.
Si fissi i in $\{1,\ldots, s\}$: essendo $\alpha'(i)$ un elemento di A_n, esiste un h_i tale che $(\alpha'(i), h_i)$ sta in A: denotiamo con m_i il minimo h_i per cui ciò succede (ciò è possibile poiché gli h_i formano un sottoinsieme di $\mathbf{N}$): le n-uple $(\alpha'(1), m_1),\ldots, (\alpha'(s), m_s)$ sono una parte dei generatori che servono per costruire A'.
In effetti, fissato $\alpha = (\alpha', h)$ in A, per costruzione esiste almeno un $j\in\{1,\ldots, s\}$ tale che $\alpha'=\alpha'(j)+\gamma'$ (per un opportuno γ') e quindi, considerato il corrispondente generatore di A: $(\alpha'(j), m_j)$, si può scrivere $\alpha=(\alpha'(j), m_j)+(\gamma', h-m_j)$. Se in almeno una di tali rappresentazioni di α si ha $h-m_j\geq 0$, resta provato che α appartiene a $(\alpha'(j), m_j) + \mathbf{N}^n$ e quindi la tesi: ciò succede di certo se $h \geq \max(m_i)$.
Possono però esistere dei multigradi $\alpha=(\alpha', h)$ per i quali risulti $h<m_j$ in ciascuna di dette rappresentazioni. In tal caso, per non esaminare i multigradi $\alpha'(j)$ a 1 a 1, si considerano gli insiemi

$$B_k=\{\beta\in \mathbf{N}^{n-1} \mid (\beta, k)\in A\},$$

ove $k\in\{0,\ldots, m-1\}$ e si è posto $m = \max(m_i)$.
Poiché B_k è un sottoinsieme di $\mathbf{N}^{n-1}$, vale l'ipotesi induttiva cioè, per ogni $k\in\{0,\ldots, m-1\}$, si può trovare un sistema finito di generatori: $\beta_k(1),\ldots, \beta_k(s_k)$ di B_k.
Dunque un sistema di generatori, magari sovrabbondante, di A è costituito da
$(\beta_0(1), 0),\ldots, (\beta_0(s_0), 0);\ldots; (\beta_{m-1}(1), m-1),\ldots, (\beta_{m-1}(s_{m-1}), m-1); (\alpha'(1), m_1),\ldots, (\alpha'(s), m_s)$. C.V.D.

ESEMPIO 3.5 Cerchiamo di capire la dimostrazione su un esempio. Sia

$$A=\{(2h,1,0), (0,2k,1), (1,1,2l)\colon h, k, l\in\mathbf{N}\setminus\{0\}\}.$$

Risulta

$$A_3=\{(2h,1), (0,2k), (1,1)\colon h, k\in\mathbf{N}\setminus\{0\}\}:$$

non essendo in grado di trovare i generatori di questo insieme di multigradi, riapplico la procedura:

$$(A_3)_2=\{2h\colon h\in\mathbf{N}\setminus\{0\}\}\cup\{0,1\}.$$

Gli elementi di $(A_3)_2$ sono generati da 0; gli elementi di A_3 che contengono 0 come prima componente sono quelli della forma $(0,2k)$ e la seconda componente è minima per k=1: dunque (0,2) deve essere considerato tra i generatori di A_3. Questo elemento da solo non genera però tutto A_3, ad esempio non genera (1,1) né (2,1).
Allora cerco $(B_3)_0=\{\beta\in\mathbf{N} \mid (\beta, 0)\in A_3\}=\varnothing$ e $(B_3)_1=\{\beta\in\mathbf{N} \mid (\beta, 1)\in A_3\}=\{2h\colon h\in\mathbf{N}\setminus(0)\}\cup\{1\}$: $(B_3)_1$ è generato da 1 e quindi (1,1) è il secondo generatore di A_3.
Quindi i generatori di A_3 sono (0,2) e (1,1) e da essi, minimizzando la terza componente, si ricavano due generatori di A: (0,2,1) e (1,1,2).
Ma in questo modo vengono trascurate le terne con terza componente nulla. La dimostrazione del teorema dice di considerare addirittura m=max(1,2)=2 e poi considerare
$B_0=\{\beta\in \mathbf{N}^2 \mid (\beta, 0)\in A\}=\{(2h,1,0)\colon h\in\mathbf{N}\setminus(0)\}$ che ha per generatore (2,1,0) e
$B_1=\{\beta\in \mathbf{N}^2 \mid (\beta, 1)\in A\}=\{(0,2k,1)\colon k\in\mathbf{N}\setminus(0)\}$ che ha per generatore (0,2,1).
Mettendo insieme i generatori si vede che uno è ripetuto e quindi i generatori indispensabili sono (chi l'avrebbe mai detto!) (2,1,0), (0,2,1) e (1,1,2).
Attenzione: se avessi scelto (0,2,2) e (1,1,2) come terne generatrici provenienti da A_3 (come sembra suggerire la dimostrazione di Cox) avremmo sì quattro terne distinte ma una di queste (0,2,2) non è un elemento di A, contro quanto viene asserito nella tesi!

Dal lemma di Dickson si ricava uno *strumento per verificare il buon ordinamento in un ordinamento monoidale*.

COROLLARIO 3.6 *Sia* $>$ *una relazione d'ordine in* $\mathbf{N}^n$ *che sia un ordinamento monoidale. Allora* $>$ *è un buon ordinamento se e solo se* $\alpha \geq \mathbf{0}$ *per ogni* $\alpha \in \mathbf{N}^n$.

Dimostrazione È già stato provato (Cap. III conseguenza 2 del Lemma 1.2) che se è un buon ordinamento si ha $\alpha \geq \mathbf{0}$ per ogni $\alpha \in \mathbf{N}^n$. Viceversa sia A un sottoinsieme di $\mathbf{N}^n$. Per il lemma di Dickson, c'è un sottoinsieme finito A' di A che genera A. Visto che l'ordinamento è totale si possono ordinare tali generatori in ordine crescente $\alpha(1) < \ldots < \alpha(t)$. Se $\mathbf{0}$ è il minimo in $\mathbf{N}^n$, $\alpha(1)$ è il minimo in A. Infatti sia $\alpha \in$ A: visto che A' genera A, esistono un $i \in \{1,\ldots,t\}$ e un $\gamma \in \mathbf{N}^n$ tali che $\alpha = \alpha(i) + \gamma$; poiché $\gamma \geq \mathbf{0}$ e per l'additività di $>$ risulta: $\alpha = \alpha(i) + \gamma \geq \alpha(i) \geq \alpha(1)$. C.V.D.

4. IL TEOREMA DELLA BASE DI HILBERT E LA C.C.A.

Il lemma di Dickson combinato con l'algoritmo della divisione ci permetterà di provare che ogni ideale di $\mathbf{A}$ (e non solo quelli monomiali) è finitamente generato. Visto che si vuol applicare l'algoritmo della divisione, bisogna *fissare in* $\mathbf{A}$ *un ordinamento monomiale* σ: ciò permette di individuare per ogni $f \in \mathbf{A}$ un LT e quindi

dato un ideale I *non nullo di* $\mathbf{A}$*, ha senso considerare l'insieme dei* LT *dei polinomi di* I:

$$\mathrm{LT}(\mathrm{I}) = \{c\boldsymbol{x}^{\alpha} : \text{esiste } f \in \mathrm{I} \text{ con } \mathrm{LT}(f) = c\boldsymbol{x}^{\alpha}\}.$$

L'ideale da esso generato sarà monomiale (i monomi generatori sono proprio gli $\boldsymbol{x}^{\alpha}$*) e verrà denotato con* $<\mathrm{LT}(\mathrm{I})>$.

OSSERVAZIONE 4.1 Se $\mathrm{I} = <f_1,\ldots,f_t>$, ovviamente si ha $<\mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_t)> \subseteq <\mathrm{LT}(\mathrm{I})>$, ma non sempre vale l'uguaglianza, poiché in I possono esistere polinomi con multigrado inferiore a quello dei $\mathrm{LT}(f_i)$. Ad esempio in $k[x,y]$ con grLEX ($x > y$) l'ideale $\mathrm{I} = <x^3 - 2xy,\ x^2y - 2y^2 + x>$ contiene anche l'elemento $x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2$ e $\mathrm{LT}(x^2) = x^2$ non appartiene a $<x^3, x^2y>$.

Ma, tenuto conto del lemma di Dickson [(11)], si vede che dall'insieme di generatori LT(I) se ne può estrarre uno finito, cioè

PROPOSIZIONE 4.2 *Sia* I *un ideale non nullo di* $\mathbf{A}$. *L'ideale monomiale* $<\mathrm{LT}(\mathrm{I})>$ *è finitamente generato da termini della forma* $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)$*, con* $g_1, \ldots, g_s \in \mathrm{I}$.

Siamo così pronti per la dimostrazione del

[(11)] In realtà tale lemma si applica ai monomi: d'altra parte è ovvio che se I contiene un polinomio f con coefficiente direttore $c \neq 1$ contiene anche f/c che ha coefficiente direttore 1 e quindi si può pensare che il LT generatori siano esattamente dei monomi.

TEOREMA DELLA BASE [12] **DI HILBERT** *Ogni ideale* I *di* $\mathbf{A}$ *è finitamente generato.*

Dimostrazione <LT(I)> è un ideale monomiale e quindi, per il lemma di Dickson, generato da un numero finito di suoi monomi, ciascuno dei quali è il LT di un polinomio g_i di I: dunque esiste un numero finito di elementi $g_1,\ldots, g_s$ di I tali che $<LT(I)> = <LT(g_1),\ldots, LT(g_s)>$ (vedi proposizione 4.2).
Dato un polinomio f di I, il suo resto $r = f - (a_1g_1 + \ldots + a_sg_s)$ nella divisione per $g_1,\ldots, g_s$, appartiene a I e quindi $LT(r)$ appartiene a $<LT(g_1),\ldots, LT(g_s)>$, cioè esiste un i tale che $LT(g_i)$ divide $LT(r)$; ma per definizione di resto ciò è impossibile se $r\neq 0$.
Dunque $f = a_1g_1 + \ldots + a_sg_s$ sta in $<g_1,\ldots, g_s>$, cioè $I=<g_1,\ldots, g_s>$. C.V.D.

Immediata conseguenza:

TEOREMA 4.3 (validità della **condizione catenaria ascendente sugli ideali di** $\mathbf{A}$) *Se*

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

è una catena ascendente di ideali di $\mathbf{A}$*, essa è definitivamente stabile, cioè esiste un* $k\in \mathbf{N}$, $k > 1$ *tale che* $I_k = I_{k+1} = I_{k+2} = \ldots..$

Dimostrazione[13] L'unione I di tutti gli ideali della catena è ancora un ideale (poiché due elementi comunque presi in I devono appartenere a due ideali della catena, anzi a uno solo, visto che ognuno è contenuto nei successivi). Per il teorema di Hilbert l'ideale I ha una base finita $\{g_1,\ldots, g_s\}$; ognuno di questi polinomi sta in qualche I_j e non negli ideali che lo precedono nella catena: sia k il più grande degli indici j. Allora $\{g_1,\ldots, g_s\} \subseteq I_k$ e quindi $I = < g_1,\ldots,g_s > \subseteq I_k \subseteq I$, per cui $I_k = I$ e quindi $I_k = I_{k+1} = I_{k+2} = \ldots$ C.V.D.

Un altro modo di enunciare la condizione catenaria ascendente è:
ogni catena strettamente ascendente $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ *di ideali di* $\mathbf{A}$*, è finita.*

Si può provare che la condizione catenaria ascendente è equivalente al teorema della base [14].

Non abbiamo ancora stabilito una corrispondenza tra polinomi ed enti geometrici (anche se un po' di esperienza in geometria analitica ci dice ad esempio che l'insieme dei punti del piano in cui si annulla $x+y$ è una retta e ci suggerisce di associare tale retta al polinomio). Ci occuperemo di questo problema nel Capitolo 6: qui conviene cominciare a osservare che una conseguenza geometrica del teorema di Hilbert è che si può parlare di **varietà affine associata ad un ideale**. Infatti l'ideale è generato da un numero finito di polinomi e quindi si può associare ad esso la varietà affine definita dall'annullarsi da tale insieme finito di polinomi: di più visto che, se si cambia il sistema di generatori dell'ideale la varietà non cambia, pare più corretto legare la varietà all'ideale.
Una conseguenza geometrica della condizione catenaria ascendente sugli ideali è invece la condizione catenaria discendente sulle varietà: ma vedremo meglio queste conseguenze nel capitolo sulle varietà.

---

[12] Ogni sistema, anche non minimale, di generatori di un ideale viene detto ***base dell'ideale***.

[13] La dimostrazione è in tutto simile a quella già vista nei PID.

[14] Infatti: sia R un anello contenente un ideale I che non ammette alcun sistema finito di generatori.
Se $\{f_c\}_{c\in\Gamma}$ è un sistema minimale di generatori di I (cioè tale che nessuno dei suoi elementi può essere scartato), la catena di ideali formata dagli ideali generati da sottoinsiemi finiti di tale sistema:

$$<f_{c(1)}> \subset <f_{c(1)}, f_{c(2)}> \subset \ldots \subset <f_{c(1)}, f_{c(2)},\ldots, f_{c(k)}> \subset \ldots$$

è sicuramente infinita e composta di ideali a due a due distinti.

5. ESERCIZI

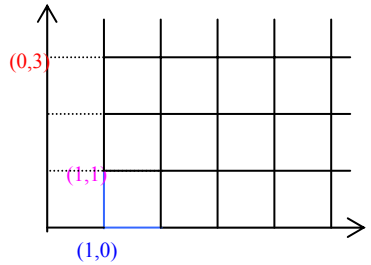
1. Si considerino i tre polinomi $f = x^2 + y^3 + xy - 1, f_1 = xy - 1, f_2 = x - y^2$
   (a) si scrivano i termini di tali polinomi in ordine decrescente, prima rispetto all'ordinamento lessicografico (LEX) e poi rispetto al graduato lessicografico (grLEX), in entrambi i casi con $x > y$.
   (b) si evidenzino il LT di tali polinomi nei due ordinamenti
   (c) si determinino quozienti e resto nella divisione di f per la coppia ordinata (f_1,f_2) usando come ordinamento una prima volta LEX e una seconda grLEX (eventualmente dopo aver costruito allo scopo un programma, basato sullo pseudocodice illustrato a §1!)
   (d) si disegni nel piano $\mathbf{N}^2$ l'insieme dei multigradi dei monomi appartenenti all'ideale monomiale generato da LT(f_1) e LT(f_2), prima usando come ordinamento LEX, poi usando grLEX
   (e) L'ideale monomiale < LT(f_1), LT(f_2) > contiene tutti i LT dei polinomi dell'ideale generato da f_1 e f_2? Anche in questo caso distinguere quanto succede nei due ordinamenti.

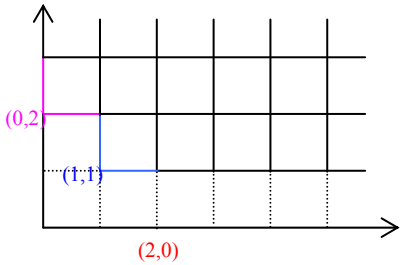
2. Si consideri in $\mathbf{A}$ un qualunque ordinamento monomiale >. Mostrare che se
   - I è un ideale monomiale,
   - A è l'insieme dei multigradi dei suoi generatori,
   - S è l'insieme di tutti i multigradi dei monomi di I,

   allora il più piccolo dei multigradi di S appartiene ad A.

6. SOLUZIONI

1. (a) LEX: $f=x^2+xy+y^3-1, f_1=xy-1, f_2=x-y^2$ grLEX: $f=y^3+x^2+xy-1, f_1=xy-1, f_2=-y^2+x$;
(b) LEX: LT(f)=x^2, LT(f_1)=xy, LT(f_2)=x grLEX: LT(f)=y^3, LT(f_1)=xy, LT(f_2)=$-y^2$;
(c) LEX: $f=(y+1)f_1+xf_2+(y^3+y) \Rightarrow (a_1, a_2, r)=(y+1, x, y^3+y)$ grLEX: $f=2f_1+(-y)f_2+(x^2+1) \Rightarrow (a_1, a_2, r)=(2, -y, x^2+1)$
(d) LEX: grLEX:





(e) LEX: l'ideale generato da f_1 e f_2 contiene $g=(xy-1)-y(x-y^2)=y^3-1$, ma LT(y^3-1) non appartiene a $<x, xy>=<x>$
grLEX: l'ideale generato da f_1 e f_2 contiene $g=y(xy-1)+x(-y^2+x)=x^2-y$, ma LT($x^2-y$) non appartiene a $<xy, -y^2>$
(vedi i multigradi in rosso nei diagrammi precedenti).

2. Sia β il più piccolo dei multigradi di S: visto che x^β è diviso da un opportuno generatore x^α dell'ideale deve esistere un multigrado γ tale che $\beta=\alpha+\gamma$. D'altra parte $S \supseteq A$ e quindi se β è il più piccolo dei multigradi di S si ha $\beta \le \alpha$. Usando l'ipotesi che l'ordinamento sia monoidale si ha allora $\beta+\gamma \le \alpha+\gamma=\beta$, e anche, visto che $\gamma \ge 0$, $\beta+\gamma \ge \beta$: dunque $\beta+\gamma=\beta$, cioè $\gamma=\mathbf{0}$.