CAPITOLO V. BASI DI GRÖBNER

1. INTRODUZIONE

La dimostrazione del teorema della base di Hilbert mette anche in luce che *ogni ideale* I *dell'anello* $\mathbf{A}=k[x_1,\ldots,x_n]$ dei polinomi su un campo *può essere generato da* (un numero finito di) *polinomi* $g_1,\ldots,g_s$ *tali che i loro LT* (rispetto a un ordinamento monomiale fissato*) generano un ideale che contiene tutti i LT* (rispetto allo stesso ordinamento) *dei polinomi appartenenti a* I (vedi Prop. 1.2). Questa osservazione porta alla seguente

DEFINIZIONE 1.1 *Fissato un ordinamento monomiale in* $\mathbf{A}=k[x_1,\ldots,x_n]$, *un sottoinsieme finito* $G=\{g_1,\ldots,g_s\}$ *di un ideale* I *di* $\mathbf{A}$ *è detto detto* ***base di Gröbner per*** I *se*

- *l'ideale* $<LT(I)>$, *generato dai termini direttori dei polinomi di* I, *coincide con l'ideale* $<LT(G)>$ *generato dai termini direttori* $LT(g_1),\ldots, LT(g_s)$ *dei polinomi appartenenti a* G,

vale a dire, se

- ogni polinomio non nullo di I ha LT divisibile per uno dei termini $LT(g_1),\ldots, LT(g_s)$.

È opportuno sottolineare che

PROPOSIZIONE 1.2 *Ogni ideale non nullo* I *ha almeno una base di Gröbner rispetto all'ordinamento monomiale fissato* (che è una base per I).

Dimostrazione (È quella del teor. di Hilbert) $<LT(I)>$ 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 $<LT(I)>=<LT(g_1),\ldots,LT(g_s)>$. Dato un polinomio f di I, il 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 $<LT(g_1),\ldots,LT(g_s)>$, 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.

In generale vale $<LT(I)> \supseteq <LT(G)>$, ma non è vero che i due ideali coincidano.

ESEMPI 1.3

1) In $k[x,y]$, $G=\{g_1=xy^2-x,\ g_2=x-y^3\}$ rispetto a LEX non è una base di Gröbner poiché $f=g_2\cdot(y^2-1)-g_1\cdot 1=-y^5+y^3$ ha LT non divisibile per xy^2 né per x.
2) In $k[x,y]$, $G=\{g_1=y^2-1,\ g_2=xy-1\}$ rispetto a LEX non è di Gröbner poiché $f=g_1\cdot x - g_2\cdot y=-x+y$ ha LT non divisibile per y^2 né per xy.
3) Invece, se I è generato da un sol elemento g, in qualunque ordinamento, $\{g\}$ è una base di Gröbner.
4) Inoltre è una base di Gröbner ogni insieme di monomi che generi un ideale monomiale.
5) Ancora, in $k[x,y,z]$, comunque si scelgano a, b, c in k, $<x+ay+bz,\ y+cz>$ rispetto a LEX è di Gröbner.
   Verifico l'affermazione per un campo k infinito, rimandando la verifica generale a dopo il corollario 7.3 al teorema di caratterizzazione. Sia $f=A(x,y,z)(x+ay+bz)+B(x,y,z)(y+cz)$: se il suo LT non è divisibile per x né per y, f deve essere un polinomio nella sola z e quindi deve risultare inalterato sostituendo $x=act-bt$ e $y=-ct$, comunque si scelga t in k; si ha allora
   $$f=A(act-bt,-ct,z)(act-bt-act+bz)+B(act-bt,-ct,z)(-ct+cz)=$$
   $$=[bA(act-bt,-ct,z)+cB(act-bt,-ct,z)](-t+z).$$
   Se k è infinito ciò significa che f ha infinite radici $z=t$ e quindi è il polinomio nullo.

2. PROPRIETÀ [1]

In generale il resto $(f)^F$ nella divisione di f per la s-pla ordinata $F=(f_1,\ldots,f_s)$ è univocamente determinato, ma dipende dall'ordine dato alla s-upla. Invece

PROPOSIZIONE 2.1 *Sia* $G=\{g_1,\ldots,g_s\}$ *una base di Gröbner rispetto a un ordinamento monomiale fissato in* $\mathbf{A}$. *Per ogni polinomio* f *di* $\mathbf{A}$ *c'è un solo polinomio* r *tale che*

i) *nessun termine di* r *è divisibile per alcuno dei* $LT(g_i)$

ii) *esiste in* $<G>$ *un polinomio* g *tale che* $f=g+r$.

Dimostrazione Un polinomio r che rispetti le condizioni si costruisce con l'algoritmo della divisione:

$$f=a_1g_1+\ldots+a_sg_s+r$$

e $g=a_1g_1+\ldots+a_sg_s$. La parte importante è l'unicità: se $f=g+r=g'+r'$ il polinomio $r-r'=g'-g$ sta in $<G>$ e se non è nullo ha LT appartenente a $<LT(G)>$ cioè divisibile per un $LT(g_i)$. Ma né r né r' hanno termini divisibili per un $LT(g_i)$, per definizione di resto: quindi $r-r'=0$. C.V.D.

Per come viene costruito r nella dimostrazione, si può dire che se G è una base di Gröbner *un polinomio* r *come quello descritto dalla Proposizione* 2.1 *è il resto nella divisione per* G. I quozienti a_i invece cambiano a seconda dell'ordine, poiché ogni termine $a_iLT(g_i)$ non deve essere divisibile per i $LT(g_j)$ con $j<i$.

COROLLARIO 2.2 (Soluzione del problema dell'appartenenza) *Sia* $G=\{g_1,\ldots,g_s\}$ *una base di Gröbner. Un polinomio* f *appartiene a* $<G>$ *se e solo se il resto* $(f)^G$ *nella divisione per* G *è nullo.*

Dimostrazione Indipendentemente dal fatto che G sia una base di Gröbner, se $(f)^G=0$ il polinomio f sta in $<G>$.
Viceversa, se f sta in $<G>$, il resto $(f)^G=f-g$ della divisione di f per G sta in $<G>$. Se non fosse nullo, il suo LT dovrebbe essere divisibile per un $LT(g_i)$, visto che G è di Gröbner: ma questo è contrario alla definizione di resto. C.V.D.

Quando sapremo costruire, a partire dalla base di un ideale, una base per quell'ideale che sia di Gröbner, il corollario 2.2 fornirà un *algoritmo per la soluzione del problema dell'appartenenza* di un polinomio a un ideale.

COROLLARIO 2.3 (Prima caratterizzazione) $G=\{g_1,\ldots,g_s\}$ *è una base di Gröbner se e solo se per ogni polinomio* f *di* $<G>$, *il resto* $(f)^G$ *nella divisione per* G *è nullo.*

Dimostrazione La Proposizione 2.1 garantisce un verso della caratterizzazione.
Viceversa, se G non è di Gröbner, esiste almeno un f in $<G>$ il cui LT non è divisibile per nessuno dei $LT(g_1)$, …,$LT(g_s)$: quindi il resto $(f)^G$ non è nullo. C.V.D.

La richiesta espressa dal Corollario 2.3 è eccessiva. In realtà, vedremo che basta verificare l'annullarsi del resto di un numero finito di polinomi opportunamente costruiti (vedi il corollario 7.3 al teorema di caratterizzazione).

[1] Vedi Cox & C. Cap.II inizio § 6.

3. BASI DI GRÖBNER MINIMALI E RIDOTTE [(2)]

Fissato in $\mathbf{A}$ un ordinamento monomiale, quante sono le basi di Gröbner di un ideale I?
Infinite, almeno se il campo k è infinito: ad esempio in $k[x,y]$, con ordinamento LEX ($x>y$), tutti gli insiemi $\{x+cy,y\}$, con $c\in k$ sono basi di Gröbner di uno stesso ideale: $<x,y>$.
Per scopi computazionali sarebbe meglio averne una sola e possibilmente "ben fatta": ad esempio se mi serve per calcolare quozienti e resto, è opportuno che il Lc di ogni polinomio della base sia 1 (si evitano un po' di frazioni); inoltre è opportuno che ogni polinomio della base sia il più "scarno" possibile, per evitare ridondanze.

DEFINIZIONE 3.1 *Una* ***base*** *di Gröbner* G *per un ideale* I *di* $\mathbf{A}$ *è detta* ***minimale*** *se valgono entrambe le condizioni*
(i) *i polinomi di* G *sono monici, cioè* Lc(p)=1 *per ogni* p *di* G
(ii) *per ogni* p *di G, il* LT(p) *non appartiene a* <LT(G $\setminus$ {p})>.

Notare che la condizione (ii) dice che in una base di Gröbner minimale ogni polinomio ha LT non divisibile per quello degli altri e quindi, in particolare, *in una base di Gröbner minimale non ci sono due polinomi distinti con lo stesso LT.*

Il lemma che segue garantisce che è sempre possibile trovare una base di Gröbner minimale.

LEMMA 3.2 *Sia* G=$\{g_1,\dots,g_s\}$ *una base di Gröbner per un ideale* I *di* $\mathbf{A}$. *Se* p *sta in* G *e il suo* LT *appartiene all'ideale generato dai restanti polinomi di* G*:*

$$\mathrm{LT}(p) \in <\mathrm{LT}(G \setminus \{p\})>,$$

allora G $\setminus$ {p} *è ancora una base di Gröbner per* I *e quindi* p *può essere rimosso dalla base.*

Dimostrazione Sia ad es. G=$\{p,g_2,\dots,g_s\}$ la base di Gröbner di I e sia LT(p) un elemento di $<\mathrm{LT}(g_2),\dots,\mathrm{LT}(g_s)>$.
Innanzitutto $\{g_2,\dots,g_s\}$ è ancora una base di I, poiché p si può scrivere come combinazione polinomiale dei g_i. Infatti, dividendo p per $\{g_2,\dots,g_s\}$ si ha

$$p=a_2g_2+\dots+a_sg_s+r.$$

Se r fosse diverso da 0, [ogni suo termine e in particolare] LT(r) non sarebbe divisibile per nessuno dei LT(g_i), né per LT(p): dunque LT(r) non apparterrebbe a <LT(G)>. D'altra parte r appartiene a I=<G>: quindi la base di partenza non sarebbe di Gröbner.
Ora, la base $\{g_2,\dots,g_s\}$ è ancora di Gröbner, poiché se il LT di un polinomio f di I è divisibile per LT(p), è anche divisibile per un LT(g_i), essendo LT(p) un elemento di $<\mathrm{LT}(g_2),\dots,\mathrm{LT}(g_s)>$. C.V.D.

LEMMA 3.3 *Fissato in* $\mathbf{A}$ *un ordinamento monomiale, due basi di Gröbner minimali per lo stesso ideale* I *hanno gli stessi* LT *e quindi, essendo i* LT *di una stessa base minimale a due a due distinti, due basi di Gröbner minimali per lo stesso ideale* I *hanno lo stesso numero di elementi.*

Dimostrazione Siano G e G' due basi di Gröbner minimali di I. Poiché <LT(G)> = <LT(I)> = =<LT(G')>, si ha che

per ogni $g\in$ G esiste un $g'\in$ G' tale che LT(g') divide LT(g) e
per ogni $g'\in$ G' esiste un $g''\in$ G tale che LT(g'') divide LT(g'),

cioè i polinomi g e g'' così individuati sono elementi di G tali che LT(g'') divide LT(g): poiché G è una base minimale, deve essere LT(g)=LM(g)=LM(g'')=LT(g'').
Allora anche LT(g')=LM(g') deve coincidere con LM(g), poiché lo divide e ne è diviso: dunque LT(G)$\subseteq$LT(G').
L'inclusione opposta si dimostra allo stesso modo. C.V.D.

---

(2) Vedi Cox & C. Cap.II fine § 7.

DEFINIZIONE 3.4 *Una* ***base di Gröbner*** G *per un ideale* I *di* $\mathbf{A}$ *è detta* ***ridotta*** *se valgono entrambe le condizioni:*

(i) *per ogni p di* G, Lc(p)=1

(ii) *per ogni p di* G, *nessun monomio di p sta in* <LT(G $\setminus$ {p})>,

cioè la base G è minimale e, per ogni p di G, i monomi diversi dal LT(p) non appartengono a <LT(G)>.

Il bello delle basi ridotte è che

TEOREMA 3.4 *Fissato in* $\mathbf{A}$ *un ordinamento monomiale, ogni ideale non nullo* I *di* $\mathbf{A}$ *ha una e una sola base di Gröbner ridotta.*

Dimostrazione Mostriamo innanzi tutto che la base di Gröbner ridotta se esiste è unica. Siano G e G' due basi di Gröbner ridotte di I: esse sono minimali e quindi (lemma 3.3) sono formate da polinomi con gli stessi LT. Siano dunque $g \in$ G e $g' \in$ G' due polinomi con LT(g)=LT(g'). Il polinomio $g-g'$ non contiene termini divisibili per LT(g) (poiché LT(g)–LT(g')=0) e neppure per gli altri LT(p), $p \in$ G, poiché non lo sono i restanti termini di g e di g'; d'altra parte $g-g'$ sta in I e quindi il suo resto $(g-g')^{G}$ nella divisione per la base di Gröbner G è nullo: dunque deve essere $g-g'=0$. Dunque le due basi, a meno dell'ordine in cui si susseguono i polinomi, coincidono.

Per vedere che una base di Gröbner ridotta esiste la costruiamo passo per passo.

Partiamo da una base di Gröbner minimale G di I; per brevità diciamo **ridotto** un polinomio p appartenente a G se i suoi monomi non stanno in <LT(G $\setminus$ {p})>: se tale polinomio appartiene ad un'altra base di Gröbner minimale è ridotto anche in essa, visto che i LT coincidono (quest'osservazione permetterà di ridurre un polinomio alla volta).

Sia dunque g un polinomio di G; se non è ridotto, consideriamo il suo resto $g'=(g)^{G \setminus \{g\}}$ nella divisione per G $\setminus$ {g}: esso ha lo stesso LT di g (poiché la base è minimale) e i suoi termini non sono divisibili per LT(p) comunque si scelga p in G $\setminus$ {g}, per definizione di resto; dunque g' è ridotto per G. Inoltre l'insieme G'=(G $\setminus$ {g})$\cup${g'} è ancora una base di I (perché g si può scrivere come combinazione a coefficienti in $\mathbf{A}$ di g' e degli altri polinomi di G $\setminus$ {g}) di Gröbner minimale (poiché i LT dei suoi polinomi coincidono con quelli di polinomi di G). Ripartiamo quindi da G': in essa g' è ridotto, se poi G' contiene un altro polinomio non ridotto operiamo su di esso come abbiamo fatto su g. In un numero di passi al più pari al numero di elementi delle basi minimali di I si arriva così alla base ridotta. C.V.D.

COROLLARIO 3.5 *Due collezioni di polinomi* F={$f_1,\ldots,f_t$} *e* H={$h_1,\ldots,h_u$} *generano lo stesso ideale di* $\mathbf{A}$ *se e solo se, fissato in* $\mathbf{A}$ *un ordinamento monomiale, la base di Gröbner ridotta di* <F> *coincide con quella di* <H>.

Quando sapremo costruire, a partire da una base assegnata, una base di Gröbner, il corollario 3.5, insieme alla tecnica di riduzione illustrata nel teorema 3.4, ci darà un *algoritmo per stabilire se due collezioni di polinomi generano lo stesso ideale*. Ovviamente questo algoritmo è meno costoso di quello che si potrebbe desumere dall'algoritmo per la soluzione del problema dell'appartenenza (corollario 2.2) che richiede comunque di calcolare una base di Gröbner tanto per <F> che per <H> e poi di dividere ogni elemento di F per H e ogni elemento di H per F.

4. COMMENTI

Restano aperti due problemi:

- trovare dei criteri concreti per stabilire se una base è di Gröbner
- trovare degli algoritmi per costruire una base di Gröbner

Per avvicinarci a una soluzione del primo problema ci chiediamo: negli esempi fatti, quali erano le situazioni in cui una base non risultava di Gröbner? In uno dei casi esaminati un elemento della base aveva LT divisibile per quello dell'altro e il resto nella divisione aveva LT non divisibile per i LT della base. Nell'altro c'erano due elementi f, g della base che combinati mediante il prodotto per termini opportuni davano un polinomio $a\mathbf{x}^{\alpha}f-b\mathbf{x}^{\beta}g$ in cui i LT di f e di g si eliminano a vicenda, lasciando un LT che non è divisibile per nessuno dei LT degli elementi della base assegnata.

ESEMPIO 4.1 [(3)] In $k[x,y]$ con l'ordinamento grLEX ($x>y$) consideriamo $f=x^3-2xy$ e $g=x^2y-2y^2+x$. $yf-xg=-2xy^2+2xy^2-x^2=-x^2$ sta in $<f,g>$ ma il suo LT non è divisibile per LT(f)=x^3 né per LT(g)=x^2y. Possiamo aggiungere $h=x^2$ alla base dell'ideale e, proseguendo nello stesso modo calcolare $f-xh=-2xy$ e $g-yh=-2y^2+x$, che sono ancora polinomi dello stesso ideale con LT non divisibili per quelli di f, g, h. Possiamo aggiungere alla base anche questi due polinomi, anzi - visto che $f=xh-2xy$ e $g=yh-2y^2+x$ - possiamo sostituire questi due polinomi a f e g, ottenendo una base per lo stesso ideale che è così fatta: $< x^2, 2xy, 2y^2-x >$ e non presenta più i problemi visti sopra. È una base di Gröbner? Sembra abbastanza ragionevole che facendo combinazioni polinomiali di 3 polinomi di secondo grado (che hanno LT tutti distinti) non si possano ottenere polinomi di primo grado,… ma questa non è una dimostrazione.

Possiamo sistematizzare i discorsi fatti a braccio nell'esempio? La risposta è positiva ma passa attraverso il concetto di sizigia (o di polinomio sizigietico) ed eventualmente attraverso quello di riducibilità a zero modulo una base.
Volendo proseguire il discorso, si vada direttamente al § 7.

5. MODULO delle SIZIGIE dei LT di un insieme di polinomi

Sia F=$\{f_1,\ldots,f_s\}$ un insieme di polinomi appartenenti all'anello $k[x_1,\ldots,x_n]:=\mathbf{A}$ in cui si pensa introdotto un ordinamento monomiale.

DEFINIZIONE 5.1 *Chiamo* ***sizigia sui termini direttori della s-upla ordinata*** F=$(f_1,\ldots,f_s)$ *ogni elemento* S=$(h_1,\ldots,h_s)$ dell'$\mathbf{A}$-*modulo* $\mathbf{A}^s$ tale che

$$h_1\mathrm{LT}(f_1)+\ldots+h_s\mathrm{LT}(f_s)=0.$$

L'insieme delle sizigie sui LT(F) è un $\mathbf{A}$-*sottomodulo* di $\mathbf{A}^s$, che denoto con S(F).
Esso è nucleo dell'omomorfismo φ: $\mathbf{A}^s \to \mathbf{A}$ definito da $\varphi(h_1,\ldots,h_s)= h_1\mathrm{LT}(f_1)+\ldots+h_s\mathrm{LT}(f_s)$.

Denotata con $\mathbf{e}_i$ la s-pla le cui componenti sono tutte nulle tranne la i-esima che è l'unità di $\mathbf{A}$, S=$(h_1,\ldots,h_s)$ può essere rappresentata anche come $h_1\mathbf{e}_1+\ldots+h_s\mathbf{e}_s$. Ad es., se m.c.m.(LM($f_i$), LM($f_j$))=$\mathbf{x}^{\gamma}$, è una sizigia di F la s-pla

$$S_{ij} = [\mathbf{x}^{\gamma}/\mathrm{LT}(f_i)]\mathbf{e}_i - [\mathbf{x}^{\gamma}/\mathrm{LT}(f_j)]\mathbf{e}_j$$

che è detta ***sizigia elementare***. Al variare degli indici i, j ($1\le i<j\le s$) si ha un insieme di sizigie che, nel teorema 5.5, si proverà essere una base di S(F).

Il motivo per cui studiamo le sizigie è che
vogliamo arrivare a dimostrare che per verificare che una base F sia di Gröbner basta controllare che, per ogni sizigia elementare S_{ij}, il resto nella divisione per F del *polinomio sizigietico*

$$S(f_i,f_j) = S_{ij}\ (f_1,\ldots,f_s) = \mathbf{x}^{\gamma}\ f_i/\mathrm{LT}(f_i) - \mathbf{x}^{\gamma}\ f_j/\mathrm{LT}(f_j)$$

sia nullo. In realtà vedremo che bastano anche condizioni più deboli (ad es. non è necessario coinvolgere proprio tutte le sizigie elementari): in ogni modo le caratterizzazioni che troveremo delle basi di Gröbner permetteranno anche di pervenire a due algoritmi per il calcolo concreto di una base di Gröbner a partire da una base assegnata.

(3) Vedi Cox & C. Cap.II § 5, esempio 2.

Le sizigie elementari hanno componenti che o sono nulle o sono termini con la proprietà che ognuno dei loro monomi soddisfa la condizione:

$$\mathrm{Log}(\boldsymbol{x}^{\gamma}/\mathrm{LM}(f_l)) + \mathrm{Log}(\mathrm{LT}(f_l)) = \text{costante} = \gamma.$$

In generale

DEFINIZIONE 5.2 *Dico che una* ***sizigia*** $S \in S(F)$ *è* ***omogenea di multigrado*** $\alpha \in \mathbf{N}^n$ *se*

i) *è una s-pla di* <u>*termini*</u>: $S=(c_1\boldsymbol{x}^{\alpha(1)},\ldots, c_s\boldsymbol{x}^{\alpha(s)})$, *ove* $c_i \in k$

ii) *per ogni i, se* c_i *non è nullo, risulta* $\alpha(i) + \mathrm{Log}(\mathrm{LT}(f_i)) = \text{costante} = \alpha$.

LEMMA 5.3 *Ogni* $S \in S(F)$ *si può scrivere in maniera unica come somma di sizigie omogenee appartenenti a* $S(F)$.

Dimostrazione Sia $S=(h_1,\ldots,h_s)$. Per ogni multigrado $\alpha \in \mathbf{N}^n$ isolo in ciascuna componente h_i di S l'eventuale termine $h_{i\alpha}$ tale che $\mathrm{Log}(h_{i\alpha})+\mathrm{Log}(\mathrm{LT}(f_i))=\alpha$. Ovviamente solo un numero finito di tali termini è non nullo.

Da $h_1\mathrm{LT}(f_1) +\ldots+ h_s\mathrm{LT}(f_s) = 0$, sostituendo $h_i = \sum_\alpha h_{i\alpha}$, si trova $\sum_\alpha (h_{1\alpha}\mathrm{LT}(f_1) +\ldots+ h_{s\alpha}\mathrm{LT}(f_s)) = 0$, ove α varia nell'insieme dei multigradi cui corrisponde qualche termine non nullo e tra le parentesi sono sommati gli addendi di ugual multigrado. Quindi si deve avere:

$$h_{1\alpha}\mathrm{LT}(f_1) +\ldots+ h_{s\alpha}\mathrm{LT}(f_s) = 0,$$

il che significa che $S_\alpha = (h_{1\alpha},\ldots,h_{s\alpha})$ è una sizigia omogenea di multigrado α e $S = \sum_\alpha S_\alpha$.

Se risulta anche $S = \sum_\alpha S'_\alpha$, si ha $\sum_\alpha (S_\alpha - S'_\alpha) = (0,\ldots,0)$, cioè per ogni multigrado α si deve avere $S_\alpha - S'_\alpha = (0,\ldots,0)$ cioè deve essere $S_\alpha = S'_\alpha$, il che prova l'unicità della rappresentazione. C.V.D.

In pratica se dovessi individuare le componenti omogenee non mi comporterei esattamente come nella dimostrazione.

ESEMPIO 5.4 F sia formato da $f_1 = x^3 - xyz, f_2 = xy - z^2, f_3 = x^2z - y^2w$. Innanzitutto si verifichi che, pensando come ordinamento monomiale grLEX con $x>y>z>w$,

$$S = (yzw^2 + xyz - zw + y,\ -x^2zw^2 - x^2 + xz, -x^2y + xw - y)$$

costituisce una sizigia dei LT di F. Per scomporla in somma di sizigie omogenee, invece di esaminare a caso ogni $\alpha \in \mathbf{N}^n$, metto in evidenza i multigradi dei LT degli f_i, che sono rispettivamente (3,0,0,0), (1,1,0,0), (2,0,1,0) e cerco, a partire dalla prima componente, quali sono le somme dei multigradi in gioco, come dalla tabella sottostante:

Log dei termini di $h_1\mathrm{LT}(f_1)$	Log dei termini di $h_2\mathrm{LT}(f_2)$	Log dei termini di $h_3\mathrm{LT}(f_3)$	α
(0,1,1,2)+(3,0,0,0)=(3,1,1,2)	(2,0,1,2)+(1,1,0,0)=(3,1,1,2)		(3,1,1,2)
(1,1,1,0)+(3,0,0,0)=(4,1,1,0)		(2,1,0,0)+(2,0,1,0)=(4,1,1,0)	(4,1,1,0)
(0,0,1,1)+(3,0,0,0)=(3,0,1,1)		(1,0,0,1)+(2,0,1,0)=(3,0,1,1)	(3,0,1,1)
(0,1,0,0)+(3,0,0,0)=(3,1,0,0)	(2,0,0,0)+(1,1,0,0)=(3,1,0,0)		(3,1,0,0)
	(1,0,1,0)+(1,1,0,0)=(2,1,1,0)	(0,1,0,0)+(2,0,1,0)=(2,1,1,0)	(2,1,1,0)

associando poi i termini che danno ugual multigrado totale

$S_{(3,1,1,2)} = (yzw^2, -x^2zw^2, 0)$

$S_{(4,1,1,0)} = (xyz, 0, -x^2y)$

$S_{(3,0,1,1)} = (-zw, 0, xw)$

$S_{(3,1,0,0)} = (y, -x^2, 0)$

$S_{(2,1,1,0)} = (0, xz, -y)$.

Queste sono le sizigie omogenee di cui S è somma.

TEOREMA 5.5 *Ogni sizigia omogenea* S *appartenente a* S(F) *si può scrivere* in generale *in maniera* non unica *come combinazione a coefficienti polinomiali di sizigie elementari:*

$$S = u_{12}S_{12} + \ldots + u_{(s-1)s}\,S_{(s-1)s} \qquad u_{ij} \in \mathbf{A}.$$

Tenendo conto del lemma 5.3 si vede che *la stessa cosa vale per ogni sizigia, anche non omogenea, appartenente a* S(F) e quindi le sizigie elementari costituiscono una base per S(F).

Dimostrazione Se $S \in S(F)$ è la sizigia nulla, l'affermazione è banale.
In caso contrario la sizigia omogenea S deve contenere almeno due componenti non nulle (una sola non basta, essendo $LT(f_i)$ non nullo, per ogni i): l'idea è di ricondurre a zero in passi successivi le coppie di componenti non nulle contigue (lavorando da sinistra a destra), facendo uso delle sizigie elementari. Mostro come si realizza la cosa su un esempio: $s = 3$, ogni componente non nulla (nel caso generale, le componenti nulle è come se non esistessero, mentre se ci sono più di 3 componenti non nulle, si itera il procedimento che qui mostreremo per le prime 2 e si conclude come concludiamo qui per la terza). Sia dunque:

$$S = (c_1 \boldsymbol{x}^{\alpha(1)}, c_2 \boldsymbol{x}^{\alpha(2)}, c_3 \boldsymbol{x}^{\alpha(3)}) \quad \text{con } c_i \neq 0 \quad \text{e} \quad \alpha(i) + \mathrm{Log}(LT(f_i)) = \alpha.$$

Considero la sizigia elementare che coinvolge le prime due componenti:

$$S_{12} = (\boldsymbol{x}^{\gamma(1,2)}/LT(f_1), -\boldsymbol{x}^{\gamma(1,2)}/LT(f_2), 0) \qquad \text{ove } \boldsymbol{x}^{\gamma(1,2)} = \text{m.c.m.}(LM(f_1), LM(f_2)).$$

Sottraendo un suo multiplo da S, posso ottenere un'altra sizigia omogenea con la prima componente nulla

$$S - b_1\boldsymbol{x}^{\beta(1)}S_{12} = (0, d_2\boldsymbol{x}^{\alpha(2)}, c_3\boldsymbol{x}^{\alpha(3)})$$

pur di porre

$$c_1\boldsymbol{x}^{\alpha(1)} - [b_1\boldsymbol{x}^{\beta(1)+\gamma(1,2)}/\,\mathrm{Lc}(f_1)LM(f_1)] = 0,$$

cioè

$$b_1 = c_1\mathrm{Lc}(f_1) \qquad \text{e} \quad \beta(1) + \gamma(1,2) = \alpha(1) + \mathrm{Log}(LM(f_1)) = \alpha.$$

Corrispondentemente la seconda componente diventa:

$$c_2\boldsymbol{x}^{\alpha(2)} + c_1\mathrm{Lc}(f_1)[\boldsymbol{x}^{\beta(1)}\boldsymbol{x}^{\gamma(1,2)}/LT(f_2)] = c_2\boldsymbol{x}^{\alpha(2)} + [c_1\mathrm{Lc}(f_1)/\mathrm{Lc}(f_2)][\boldsymbol{x}^{\alpha}/LM(f_2)] = [c_2 + c_1\mathrm{Lc}(f_1)/\mathrm{Lc}(f_2)]\boldsymbol{x}^{\alpha(2)}$$

cioè

$$d_2 = c_2 + c_1\mathrm{Lc}(f_1)/\mathrm{Lc}(f_2).$$

Se $d_2 \neq 0$, itero la procedura usando la sizigia S_{23} che coinvolge la seconda e la terza componente. Si rifanno gli stessi conti - sostituire la coppia ordinata (1,2) con la coppia (2,3) e c_1 con d_2 - ottenendo

$$b_2 = d_2\mathrm{Lc}(f_2) \qquad \text{e} \qquad \beta(2) + \gamma(2,3) = \alpha(2) + \mathrm{Log}(LM(f_2)) = \alpha.$$

Dunque

$$S = b_1\boldsymbol{x}^{\beta(1)}S_{12} + b_2\boldsymbol{x}^{\beta(2)}S_{23} + (0, 0, [c_3 + d_2\mathrm{Lc}(f_2)/\mathrm{Lc}(f_3)]\,\boldsymbol{x}^{\alpha(3)}),$$

dove - visto che anche l'ultima terna è una sizigia - si deve avere $c_3 + d_2\mathrm{Lc}(f_2)/\mathrm{Lc}(f_3) = 0$, cioè, in termini un po' più generali, quando si arriva ad aver ricondotto a zero tutte le componenti tranne due, l'addendo che manca per completare la rappresentazione della sizigia è un multiplo della sizigia elementare dei LT dei 2 polinomi aventi in F la stessa posizione delle restanti due componenti non nulle.
Nell'esempio qui discusso si ha quindi:

$$S = c_1\mathrm{Lc}(f_1)\,\boldsymbol{x}^{\alpha-\gamma(1,2)}S_{12} + (c_2\mathrm{Lc}(f_2) + c_1\mathrm{Lc}(f_1))\,\boldsymbol{x}^{\alpha-\gamma(2,3)}S_{23}$$

cioè in breve

$$S = b_1\,\boldsymbol{x}^{\beta(1)}S_{12} + b_2\boldsymbol{x}^{\beta(2)}S_{23}$$

e, in generale, S può essere scritta come combinazione (a coefficienti che sono termini) di al più $(s-1)$ sizigie elementari. C.V.D.

CONTROESEMPIO 5.6 (all'unicità della rappresentazione) Si consideri in $k[x,y,z]$, con l'ordinamento LEX ($x > y > z$), l'insieme $F = \{x^2y^2 + z,\ xy^2 - y,\ x^2y + yz\}$. Si vede che $S_{13} = (1,0,-y)$, $S_{23} = (0,x,-y)$ e quindi la sizigia elementare $S_{12} = (1,-x,0)$ si può anche rappresentare come $S_{13} - S_{23}$.

Generalizzando l'esempio, vale il seguente enunciato, la cui utilità emerge allorché si fornisce l'algoritmo (fine) di Buchberger per il calcolo delle basi di Gröbner:

PROPOSIZIONE 5.7 *Sia* $\mathcal{S}$ *un sottoinsieme dell'insieme delle sizigie elementari sui* LT *di* F, *che sia una base per* S(F). *Dati tre elementi distinti* f_1, f_2, f_3 *di* F (*eventualmente con indici variati rispetto a quelli assegnati inizialmente in* F), *se* S_{12}, S_{13} *e* S_{23} *stanno in* $\mathcal{S}$ *e se*

$$\mathrm{LT}(f_3) \text{ divide } \mathrm{m.c.m.}(\mathrm{LT}(f_1), \mathrm{LT}(f_2))$$

Allora esistono monomi $\boldsymbol{x}^{\alpha}, \boldsymbol{x}^{\beta}$ *tali che* $S_{12} = \boldsymbol{x}^{\alpha} S_{13} - \boldsymbol{x}^{\beta} S_{23}$ *cioè anche* $\mathcal{S} \setminus \{S_{12}\}$ *è una base per* S(F).

Dimostrazione Basta mostrare che S_{12} si scrive come combinazione polinomiale di S_{13} e S_{23}. Come nella dimostrazione precedente, pongo $\boldsymbol{x}^{\gamma(i,j)} = \mathrm{m.c.m.}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))$, comunque si scelgano i e j con $1 \le i < j \le 3$. Per ipotesi $\mathrm{LM}(f_3)$ divide $\boldsymbol{x}^{\gamma(1,2)}$ e quindi anche $\boldsymbol{x}^{\gamma(1,3)}$ e $\boldsymbol{x}^{\gamma(2,3)}$ dividono $\boldsymbol{x}^{\gamma(1,2)}$. Dunque

$$\begin{aligned}
S_{12} &= [\boldsymbol{x}^{\gamma(1,2)}/\mathrm{LT}(f_1)]\mathbf{e}_1 - [\boldsymbol{x}^{\gamma(1,2)}/\mathrm{LT}(f_2)]\mathbf{e}_2 = \\
&= [(\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(1,3)})(\boldsymbol{x}^{\gamma(1,3)}/\mathrm{LT}(f_1))]\mathbf{e}_1 - [(\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(2,3)})(\boldsymbol{x}^{\gamma(2,3)}/\mathrm{LT}(f_2))]\mathbf{e}_2 = \\
&= [(\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(1,3)})(\boldsymbol{x}^{\gamma(1,3)}/\mathrm{LT}(f_1))]\mathbf{e}_1 - [\boldsymbol{x}^{\gamma(1,2)}/\mathrm{LT}(f_3)]\mathbf{e}_3 + [\boldsymbol{x}^{\gamma(1,2)}/\mathrm{LT}(f_3)]\mathbf{e}_3 + \\
&\qquad - [(\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(2,3)})(\boldsymbol{x}^{\gamma(2,3)}/\mathrm{LT}(f_2))]\mathbf{e}_2 = \\
&= (\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(1,3)})\{[(\boldsymbol{x}^{\gamma(1,3)}/\mathrm{LT}(f_1))]\mathbf{e}_1 - [\boldsymbol{x}^{\gamma(1,3)}/\mathrm{LT}(f_3)]\mathbf{e}_3\} + \\
&\quad - (\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(2,3)})\{[\boldsymbol{x}^{\gamma(2,3)}/\mathrm{LT}(f_2)]\mathbf{e}_2 - [\boldsymbol{x}^{\gamma(2,3)}/\mathrm{LT}(f_3)]\mathbf{e}_3\} = (\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(1,3)})S_{13} - (\boldsymbol{x}^{\gamma(1,2)}/\boldsymbol{x}^{\gamma(2,3)})S_{23}
\end{aligned}$$

C.V.D.

Per rendere più spedita la dimostrazione del teorema di caratterizzazione conviene anche premettere la

OSSERVAZIONE 5.8 *Siano* $\mathcal{S}$ *una base per* S(F) *formata da sizigie omogenee ed* S *una sizigia omogenea, di multigrado* δ *anche non appartenente a* $\mathcal{S}$. *Esistono*

- *un insieme di sizigie omogenee* $S_1, \ldots, S_m$, *rispettivamente di multigrado* $\gamma_1, \ldots, \gamma_m$, *appartenenti alla base* $\mathcal{S}$ *ed*
- *un insieme di termini* $u_1, \ldots, u_m$, *rispettivamente di multigrado* $\delta - \gamma_1, \ldots, \delta - \gamma_m$,

tali che $S = \sum_1^m u_j S_j$.

Dimostrazione Per definizione di base esistono m sizigie $S_1, \ldots, S_m$, di $\mathcal{S}$ e m polinomi $q_1, \ldots, q_m$ tali che $S = \sum_1^m q_j S_j$. Ogni S_j, essendo omogenea di multigrado γ_j, ha la forma

$$(c_{j1}\,\boldsymbol{x}^{\alpha(j,1)}, \ldots, c_{js}\,\boldsymbol{x}^{\alpha(j,s)}), \quad \text{con } \gamma_j = \mathrm{Log}(\mathrm{LT}(f_i)) + \alpha(j,i) \quad \text{per ogni } i \in \{1,\ldots,s\} \text{ tale che } c_{ji} \neq 0$$

Quindi, se il polinomio q_j contiene t_j monomi distinti con coefficienti non nulli: $q_j = \sum_{l=1}^{t_j} b_{\beta(j,l)} \mathbf{x}^{\beta(j,l)}$,

risulta $S = \left(\sum_{j=1}^m q_j c_{j1} \mathbf{x}^{\alpha(j,1)}, \ldots, \sum_{j=1}^m q_j c_{js} \mathbf{x}^{\alpha(j,s)} \right) = \left(\sum_{j=1}^m \sum_{l=1}^{t_j} b_{\beta(j,l)} c_{j1} \mathbf{x}^{\alpha(j,1)+\beta(j,l)}, \ldots, \sum_{j=1}^m \sum_{l=1}^{t_j} b_{\beta(j,l)} c_{js} \mathbf{x}^{\alpha(j,s)+\beta(j,l)} \right)$.

Essendo S omogenea, la sua componente i-esima $\sum_{j=1}^m \sum_{l=1}^{t_j} b_{\beta(j,l)} c_{ji} \mathbf{x}^{\alpha(j,i)+\beta(j,l)}$ deve essere un termine; in più, visto che S è omogenea di multigrado δ, per tutti gli $i \in \{1,\ldots,s\}$ tali che $b_{\beta(j,l)} c_{ji} \neq 0$ si deve avere:

$$\beta(j,l) + \alpha(j,i) = \delta - \mathrm{Log}(\mathrm{LT}(f_i)),$$

cioè

$$\beta(j,l) = \delta - \mathrm{Log}(\mathrm{LT}(f_i)) - \alpha(j,i) = \delta - \gamma_j .$$

Dunque il multigrado $\beta(j,l)$ non dipende da l, cioè ogni q_j consiste in realtà di un solo termine

$$u_j = b_j \boldsymbol{x}^{\delta - \gamma_j}.$$

C.V.D.

Questa osservazione non implica che una sizigia omogenea non si possa anche rappresentare come combinazione a coefficienti che non sono termini delle sizigie omogenee prescelte.

ESEMPIO 5.9 In $k[x,y]$ con l'ordinamento LEX ($x > y$) consideriamo $F = (f_1 = y - 1, f_2 = x - y)$. Una base per S(F) è data $\{S_{12} = (x, -y)\}$, quindi certamente l'insieme $\mathsf{S} = \{S_{12}, S_2 = (-xy, y^2)\}$ è ancora una base per S(F), le cui sizigie sono omogenee rispettivamente di multigrado (1,1) e (1,2). La sizigia $S = 3xy\, S_{12} + 2x\, S_2 = (x^2y, -xy^2)$ è omogenea di multigrado (2,2), ma può anche essere riscritta come $S = (3xy + xy^2)S_{12} + (2x + xy)S_2$.

Si consiglia di svolgere ora l'esercizio sulle sizigie contenuto nel file di ESERCIZI sul CAPITOLO V.

6. RIDUCIBILITÀ A ZERO MODULO UNA BASE

DEFINIZIONE 6.1 *Fissato in* $\mathsf{A} = k[x_1,\ldots,x_n]$ *un ordinamento monomiale, dico che* ***un polinomio*** $f \in \mathsf{A}$ ***si riduce a zero modulo una base*** $G=\{g_1, \ldots, g_s\}$ *di polinomi di* A *se esistono s polinomi* $a_1, \ldots, a_s \in \mathsf{A}$ *per i quali valgono le due condizioni:*

1) $f = a_1g_1 + \ldots + a_sg_s$ [e quindi f appartiene all'ideale generato da G]

2) *se* $a_ig_i \neq 0$ *risulta* $\mathrm{Log}(\mathrm{LT}(f)) \geq \mathrm{Log}(\mathrm{LT}(a_ig_i))$.

Si scrive: $f \to_G 0$.

Ovvio che se il resto $(f)^G$ nella divisione di f per G è 0 allora $f \to_G 0$.
Il viceversa può essere falso, se G non è una base di Gröbner.

ESEMPIO 6.2 (Cap. 4 §2 esempio 2) In $k[x,y]$ con l'ordinamento LEX ($x>y$) il polinomio $f=x^2y+xy^2+y^2-2y-1$ si riduce a zero modulo la base $G=\{xy-1, y^2-1\}$, poiché
$f = (xy-1)(x+2y)+(y^2-1)(-x+1)$ e $\mathrm{Log}(\mathrm{LT}(f)) = (2,1) = \mathrm{Log}(\mathrm{LT}(x+2y)g_1) > (1,2) = \mathrm{Log}(\mathrm{LT}(-x+1)g_2)$, ma i 2 resti che si ottengono facendo la divisione per i polinomi di G (nell'ordine dato o nell'ordine inverso) sono rispettivamente $x-y$ e $2x-2y$.

Ancora: per la riducibilità a 0, non basta che f stia nell'ideale generato da G: la condizione sul multigrado è fondamentale. Ad es. considero $k[x,y,z]$ con l'ordinamento LEX ($x>y>z$): se $g_1=x^2y^2+z$ e $g_2=xy^2-y$, il polinomio sizigietico (vedi §5) $f=S(g_1,g_2)=g_1-xg_2=xy+z$ soddisfa la condizione (1) ma non la (2) e quindi non si riduce a zero modulo G.

Visto che i polinomi sizigietici entrano pesantemente nella costruzione delle basi di Gröbner, vale la pena di stabilire se alcuni di essi si riducono automaticamente a zero.

PROPOSIZIONE 6.3 *Siano* g_1 *e* g_2 *due polinomi di* G (non necessariamente il primo e il secondo) *con* $\mathrm{LM}(g_1)$ *e* $\mathrm{LM}(g_2)$ *primi tra loro. Risulta:* $S(g_1, g_2) \to_G 0$.

Dimostrazione Poiché i due polinomi sono primi tra loro,

$$\boldsymbol{x}^\gamma = \mathrm{m.c.m.}(\mathrm{LM}(g_1), \mathrm{LM}(g_2)) = \mathrm{LM}(g_1)\cdot\mathrm{LM}(g_2).$$

Posso supporre che entrambi i coefficienti direttori di g_1 e g_2 siano 1: quindi ho

$$S(g_1, g_2) = \mathrm{LM}(g_2)\cdot g_1 - \mathrm{LM}(g_1)\cdot g_2$$

e posto $g_i = \mathrm{LM}(g_i) + p_i$, cioè $\mathrm{LM}(g_i) = g_i - p_i$ $(i=1,2)$ si trova

$$S(g_1, g_2) = (-p_2)\cdot g_1 + (p_1)\cdot g_2.$$

Dunque vale la prima condizione affinché $S(g_1, g_2) \to_G 0$.
Per mostrare che vale anche la seconda, osservo che $(-p_2)\cdot g_1$ e $(p_1)\cdot g_2$ non possono avere lo stesso LM (dando luogo all'eventualità che i due LT si elidano), poiché in caso contrario, cioè se

$$\mathrm{LM}(p_2)\cdot\mathrm{LM}(g_1) = \mathrm{LM}(p_1)\cdot\mathrm{LM}(g_2),$$

$\mathrm{LM}(g_1)$, non avendo fattori in comune con $\mathrm{LM}(g_2)$, dovrebbe dividere $\mathrm{LM}(p_1)$, cosa assurda poiché $\mathrm{Log}(\mathrm{LM}(g_1)) > \mathrm{Log}(\mathrm{LM}(p_1))$.
Ne consegue che il LT di $(-p_2)\cdot g_1 + (p_1)\cdot g_2$ coincide con uno dei due LT di $(-p_2)\cdot g_1$ e di $(p_1)\cdot g_2$ e ha quindi multigrado uguale a uno dei due e maggiore dell'altro. C.V.D.

Anche nelle ipotesi della Proposizione 6.3, il resto nella divisione per G di $S(g_1,g_2)$ può non essere nullo.

ESEMPIO 6.4 Considero $k[x,y,z]$ con l'ordinamento grLEX ($x>y>z$) e la base ordinata $G=(g_1=yz+1, g_2=x^3+y, g_3=z^4)$: per la Proposizione 6.3, si ha $S(g_2, g_3) \to_G 0$, mentre $(S(g_2, g_3))^G = (yz^4)^G = -z^3$.

I fenomeni di abbassamento del multigrado del $\mathrm{LT}(S(g_1,g_2))$ che si verificano nella dimostrazione della Proposizione 6.3 sono chiariti dal seguente

LEMMA 6.5 *Se* $S = (h_1,\ldots,h_s)$ *è una sizigia omogenea di multigrado* γ *sui LT di una s-upla ordinata* $G = (g_1,\ldots,g_s)$ *di polinomi, allora risulta*

$$\mathrm{Log}\ \mathrm{LT}(h_1g_1 + \ldots + h_sg_s) < \gamma\ .$$

Dimostrazione Se S è una sizigia omogenea (vedi §5) di multigrado γ si ha

$h_1\mathrm{LT}(g_1) + \ldots + h_s\mathrm{LT}(g_s) = 0$ e $\mathrm{Log}(h_j) + \mathrm{Log}(\mathrm{LT}(g_j)) = \gamma$ per ogni j tale che $h_jg_j \neq 0$,

per cui nella somma $S\ G = h_1g_1 + \ldots + h_s g_s$ i termini formalmente di multigrado massimo si annullano. Quindi, per tutti gli indici j tali che h_jg_j non si annulli, si ha

$$\mathrm{Log}(\mathrm{LT}(S\ G)) < \mathrm{Log}(\mathrm{LT}(h_jg_j)) = \mathrm{Log}(h_j) + \mathrm{Log}(\mathrm{LT}(g_j)) = \gamma. \quad \text{C.V.D}$$

COROLLARIO 6.6 *Se* $S =(h_1,\ldots, h_s)$ *è una sizigia omogenea di multigrado* γ *sui LT di una s-upla ordinata* $G = (g_1,\ldots, g_s)$ *di polinomi e* $S\ G \to_G 0$, *esiste una s-upla ordinata* $(a_1,\ldots, a_s)$ *di polinomi tali che*

i) $S\ G = a_1g_1 + \ldots + a_sg_s$

ii) $\mathrm{Log}\ \mathrm{LT}(a_ig_i) < \gamma$ *per tutti gli indici* $i \in \{1,\ldots,s\}$ *per i quali i prodotti* a_ig_i *non sono nulli*.

Dimostrazione Poiché $S\ G \to_G 0$, esiste una s-upla $(a_1,\ldots,a_s)\in \mathbb{A}^s$ tale che

$$S\ G = a_1g_1 + \ldots + a_sg_s \text{ e, se } a_ig_i \neq 0, \text{ risulta } \mathrm{Log}(\mathrm{LT}(a_ig_i)) \leq \mathrm{Log}(\mathrm{LT}(S\ G)).$$

Visto che valgono le ipotesi del lemma 6.5, per tutti gli indici i tali che a_ig_i non si annulli, si ha

$$\mathrm{Log}(\mathrm{LT}(a_ig_i)) \leq \mathrm{Log}(\mathrm{LT}(S\ G)) < \gamma. \quad \text{C.V.D.}$$

7. CARATTERIZZAZIONI DELLE BASI DI GRÖBNER

TEOREMA 7.1 (di Caratterizzazione[4]**)** *Si fissi in* $\mathbb{A}$ *un ordinamento monomiale. Sono equivalenti le condizioni:*

i) $G = \{g_1,\ldots,g_s\}$ *è una base di Gröbner per l'ideale* $<G>$

ii) *esiste un insieme* $\mathbb{S}$ *di sizigie omogenee dei* LT *di* G (vedi §5) *tale che*

- $\mathbb{S}$ *sia una base per il sottomodulo* S(G) *delle sizigie dei* LT *di* G
- *per ogni* $S = (h_1,\ldots,h_s)$ *appartenente a* $\mathbb{S}$ *si abbia* (vedi §6)

$$S\ G = h_1g_1 + \ldots + h_sg_s \ \to_G\ 0.$$

[4] Vedi Cox & C. Cap.II § 9, teorema 9. In prima lettura conviene saltare la dimostrazione e andare al corollario 7.2.

Dimostrazione Se G è di Gröbner, S G, in quanto elemento di <G>, ha resto zero nella divisione per G (in qualunque ordine) e quindi S G $\to_G$ 0 per ogni *s*-upla S di polinomi e in particolare per ogni sizigia di un insieme $\mathcal{S}$ quale quello dell'enunciato.

Viceversa si deve mostrare che, nelle ipotesi fatte su $\mathcal{S}$, ogni polinomio $f \in$ <G> ha LT appartenente all'ideale <LT(G)>, cioè che esiste un g_i tale che LT(g_i) divide LT(f).
Allo scopo si consideri una scrittura del polinomio f di <G> come $f = k_1 g_1 + \ldots + k_s g_s$ tale che, posto

$$m(i) := \text{Log}\,(\text{LT}(k_i\, g_i)) \quad \text{per ogni } i \in \{1,\ldots, s\} \qquad \text{e} \qquad \delta := \max\{m(i), i \in \{1,\ldots, s\}\},$$

δ sia il minimo [5] possibile; ciò significa che si evita di tenere nei k_i termini ridondanti che, moltiplicati per quelli dei g_i, finiscano per elidersi. Ad es. si esclude di scrivere il polinomio $f = g_1 + g_2$ come $f = (g_2+1)g_1 + (-g_1+1)g_2$ ma se $g_1 = xy^2+x$ e $g_2 = x^2y+y$ non si esclude di scrivere $f = x^2 - y^2 = xg_1 - yg_2$ [6].
È ovvio che Log (LT(f)) ≤ max {Log (LT($k_i\, g_i$)}: se vale l'uguaglianza esiste un i tale che

$$\text{Log}\,(\text{LT}(f)) = \delta = \text{Log}\,(\text{LT}(k_i)) + \text{Log}(\text{LT}(g_i))$$

e quindi LT(g_i) divide LT(f): che è la tesi.
Si deve quindi escludere che possa essere Log(LT(f)) < δ e lo si fa lavorando per assurdo e facendo cadere l'ipotesi di minimo. Tappe successive:

a) si mettono in evidenza nella scrittura di f i termini che hanno sicuramente multigrado minore di δ; poiché:

$$f = \sum_{i:\, m(i)=\delta} \text{LT}(k_i) g_i \quad + \sum_{i:\, m(i)=\delta} (k_i - \text{LT}(k_i)) g_i \quad + \sum_{i:\, m(i)<\delta} k_i g_i$$

gli ultimi due addendi, avendo multigrado minore di δ, si possono cestinare. Salvo rinominare gli elementi della base, si può supporre che gli i per i quali si ha m(i)=δ siano i primi r.

b) Resta quindi da esaminare $\sum_1^r \text{LT}(k_i) g_i$, di cui l'ipotesi assurda asserisce che ha LT con multigrado minore di δ: visto che il LT di ogni addendo, LT(k_i)LT(g_i), ha multigrado δ, ciò è possibile solo se

$$\sum_1^r \text{LT}(k_i)\text{LT}(g_i) = 0\,.$$

c) Ciò evidenzia una sizigia sui LT(G), omogenea, di multigrado δ per come sono stati scelti gli i:

$$S = (\text{LT}(k_1),\ldots,\text{LT}(k_r),0,\ldots,0)$$

che in virtù dell'osservazione 5.8 può essere espressa come $S = \sum_1^m u_j S_j$ ove ogni S_j è una sizigia omogenea di multigrado γ_j appartenente alla base $\mathcal{S}$ e ogni $u_j = b_j \boldsymbol{x}^{\delta-\gamma_j}$ è un termine di multigrado $\delta - \gamma_j$.

d) Torniamo a (b): $\sum_1^r \text{LT}(k_i) g_i = S \bullet G = \left(\sum_1^m u_j S_j\right) \bullet G = \sum_1^m b_j \boldsymbol{x}^{\delta-\gamma_j} (S_j \bullet G)$.

Ora si sfrutta l'ipotesi sulla base e il corollario 6.6 applicato a S_j per mostrare che si può riscrivere $\sum_1^r \text{LT}(k_i) g_i$ (e quindi f) come somma di prodotti del tipo $f_i g_i$, i cui LT hanno tutti multigrado < δ, il che fa cadere l'ipotesi che si sia scelta la rappresentazione di f in cui i LT dei prodotti hanno multigrado minimo.

---

[5] La cosa è possibile poiché nell'anello dei polinomi si è introdotto un ordinamento monomiale (e quindi buono).
[6] Ovviamente in questo caso f non sarebbe riducibile a zero modulo $\{g_1, g_2\}$, cadendo l'ipotesi sul multigrado.

In dettaglio: ogni S_j è per ipotesi una sizigia omogenea dei LT(G) tale che $S_j \bullet G \to_G 0$ e quindi per il corollario 6.6 esistono dei polinomi $a_{j1},\ldots, a_{js}$ tali che

$$S_j \bullet G = a_{j1}g_1 + \ldots + a_{js}g_s \qquad \text{e,} \quad \text{se } a_{ji}\,g_i \neq 0, \qquad \text{Log LT}(a_{ji}\,g_i) < \gamma_j.$$

Quindi

$$\sum_{i=1}^{r} \mathrm{LT}(k_i)g_i = \sum_{j=1}^{m} b_j \boldsymbol{x}^{\delta-\gamma_j}\left(\sum_{i=1}^{s} a_{ji}g_i\right) = \sum_{i=1}^{s}\sum_{j=1}^{m} b_j \boldsymbol{x}^{\delta-\gamma_j} a_{ji}g_i$$

ha tutti gli addendi di multigrado $<\delta$, per cui

$$f = \sum_{i=1}^{s}\left(\sum_{j=1}^{m} b_j \boldsymbol{x}^{\delta-\gamma_j} a_{ji}\right)g_i + \sum_{i=1}^{r}(k_i - \mathrm{LT}(k_i))g_i + \sum_{i=r+1}^{s} k_i g_i\,,$$

una volta raccolti i polinomi coefficienti di ciascun g_i si può scrivere come $\sum_{i=1}^{s} f_i g_i$ con

$\mathrm{Log}(\mathrm{LT}(f_i g_i)) < \delta$ per ogni i: contro l'ipotesi di minimalità. C.V.D.

Visto che, se G è una base di Gröbner, ogni polinomio f appartenente a <G> (e in particolare S G) ha resto $(f)^G$ nullo nella divisione per G, e che ciò implica la riducibilità a zero di f, si deduce il

COROLLARIO 7.2 *Sono equivalenti le condizioni:*

1) $G = \{g_1,\ldots,g_s\}$ *è una base di Gröbner per l'ideale* <G>.

2) Per ogni S *appartenente a una qualunque base* S *di sizigie omogenee di* S(G) *risulta* $(S\ G)^G=0$.

3) Per ogni S *appartenente a una qualunque base* S *di sizigie omogenee di* S(G) *risulta* $S\ G \to_G 0$.

Attenzione: Nel corollario le affermazioni riguardano una qualunque base S con le proprietà elencate (mentre nel teorema si chiede che le proprietà valgano per almeno una base). In particolare l'insieme S può essere formato da (tutte o una parte di) sizigie elementari (vedi teorema 5.5). Se ne ricavano le seguenti utili caratterizzazioni

COROLLARIO 7.3 *Sono equivalenti le condizioni*:

1) $G=\{g_1,\ldots,g_s\}$*è una base di Gröbner per l'ideale* <G>.

2) *Esiste una base* S *di sizigie elementari tali che per ogni* S_{ij} *appartenente a* S *risulta* $(S_{ij}\ G)^G=0$.

3) *Esiste una base* S *di sizigie elementari tali che per ogni* S_{ij} *appartenente a* S *risulta* $S_{ij}\ G \to_G 0$.

A partire di qui si individua un primo algoritmo (vedi §8) per il calcolo delle basi di Gröbner che fa uso di tutte le sizigie elementari, migliorabile usando in maniera appropriata le proprietà sulle sizigie e sulla riducibilità a zero (algoritmo fine).

8. ALGORITMO INGENUO PER IL CALCOLO DI BASI DI GRÖBNER

Questo e il successivo algoritmo fine sono dovuti a Buchberger.
Spieghiamo l'idea su un esempio.

ESEMPIO 8.1 Consideriamo $k[x,y,z]$ con l'ordinamento grLEX ($x>y>z$) e in esso la base

$$F := (f_1 = yz + y, f_2 = x^3 + y, f_3 = z^4).$$

Calcoliamo S_{ij} F=S(f_i,f_j) per ogni coppia di indici e poi il suo resto nella divisione per F.
S(f_1,f_2)=$x^3(yz+y)-yz(x^3+y)=x^3y-y^2z=f_1(-y)+f_2y$: ha resto zero;
S(f_1,f_3)=$z^3(yz+y)-yz^4=yz^3=(yz+y)(z^2-z+1)-y$: ha resto $-y$:
il LT y manca tra i LT(f_i) e visto che il polinomio $-y$ sta in <F> bisogna aggiungerlo, se si vuole che nella base ci siano polinomi sufficienti a descrivere tutti i possibili LT dei polinomi di <F>:

$$F := (f_1 = yz + y, f_2 = x^3 + y, f_3 = z^4, f_4 = y).$$

Riprendiamo:
S(f_1,f_2)=$x^3(yz+y)-yz(x^3+y)=x^3y-y^2z=f_1(-y)+f_2y$: ha resto zero;
S(f_1,f_3)=$z^3(yz+y)-yz^4=yz^3=(yz+y)(z^2-z+1)-y$: ha resto zero rispetto alla nuova base
S(f_2,f_3)=$z^4(x^3+y)-x^3(z^4)=yz^4=(yz+y)(z^3-z^2+z-1)+y$: ha resto zero rispetto alla nuova base
S(f_1,f_4)=$yz+y-yz$: ha resto zero rispetto alla nuova base
S(f_2,f_4)=$y(x^3+y)-x^3y=y^2$ ha resto zero rispetto alla nuova base
S(f_3,f_4)=$yz^4-yz^4=0$.

Non nascono nuovi LT e quindi, tenuto conto del corollario 7.3, quella trovata è una base di Gröbner.
Ovviamente non è una base minimale (f_1=f_4 (z+1)), né tanto meno ridotta.
La base ridotta corrispondente è $\{x^3, y, z^4\}$, cioè <F> è un ideale monomiale.

Abbiamo visto la strategia da usare. Veniamo all'algoritmo.

TEOREMA 8.2 *Una base di Gröbner dell'ideale* I=<f_1,...,f_s> *di* **A** *può essere costruita in un numero finito di passi mediante il seguente algoritmo:*

Input: F=$\{f_1,...,f_s\}$
Output: una base di Gröbner G per I, con F⊂G

G:= F
REPEAT
    G':=G
    FOR $\{p,q\}$, $p \neq q$ comunque presi in G' DO
        S:=(S(p,q))$^{G'}$
        IF S≠0 THEN G:=G'∪{S}
UNTIL G=G'.

Dimostrazione L'algoritmo ha termine. Infatti ad ogni passo si ha G'⊆G e se G'≠G anche <LT(G')> risulta contenuto propriamente in <LT(G)>, poiché il resto S (nella divisione per G') che si aggiunge a G' ha LT che non è divisibile per alcuno dei LT(G'): quindi si crea una catena strettamente ascendente di ideali

$$\ldots \subset <LT(G')> \subset <LT(G'), LT(S)> \subset \ldots$$

Per la condizione catenaria ascendente sugli ideali, tale catena ha termine, cioè si deve arrivare ad un punto in cui non c'è più nessun resto diverso da 0 da aggiungere.
L'insieme G che si ottiene in uscita contiene F per costruzione e, visto che ogni nuovo polinomio di G si ottiene per combinazione polinomiale di elementi di F, è contenuto in I, di cui quindi risulta una base.
Tale base è di Gröbner, poiché l'algoritmo ha termine solo quando, per ogni coppia di polinomi p, q di G, il resto nella divisione per G di S(p,q) è nullo (cfr. corollario 7.3). C.V.D.

Come osservato nell'esempio, l'algoritmo qui descritto prevede che, ogni volta che si introduce nella base un nuovo polinomio, la procedura ricominci daccapo. D'altra parte è chiaro che i polinomi sizigietici composti con i vecchi polinomi rimangono gli stessi (è il resto S che se non è nullo cambia, poiché, il resto nella divisione per G'∪{S} risulta 0). Dunque si può migliorare un po' l'algoritmo non ripetendo il test con le coppie di polinomi p, q già esaminati.

ESEMPIO 8.3
Consideriamo $k[x,y]$ con l'ordinamento grLEX ($x>y$) e in esso la base $F=\{f_1=x^3-2xy, f_2=x^2y-y^2+x\}$.
$S(f_1,f_2) = y(x^3-2xy)-x(x^2y-y^2+x) = -xy^2-x^2$: è il resto e va aggiunto;

$G := \{f_1 = x^3-2xy, f_2 = x^2y-y^2+x, f_3 = xy^2+x^2\}$.
$S(f_1,f_3) = y^2(x^3-2xy)-x^2(xy^2+x^2) = -x^4-2xy^3 = -x(f_1)-2y(f_3)$: ha resto zero;
$S(f_2,f_3) = y(x^2y-y^2+x)-x(xy^2+x^2) = -x^3-y^3+xy = -(f_1)-y^3-xy$: c'è un resto che va aggiunto;

$G := \{f_1 = x^3-2xy, f_2 = x^2y-y^2+x, f_3 = xy^2+x^2, f_4 = y^3+xy\}$.
$S(f_1,f_4) = y^3(x^3-2xy)-x^3(y^3+xy) = -x^4y-2xy^4 = -xy(f_1)-2y^2(f_3)$: ha resto zero;
$S(f_2,f_4) = y^2(x^2y-y^2+x)-x^2(y^3+xy) = -x^3y-y^4+xy^2 = -y(f_1+f_4)$: ha resto zero
$S(f_3,f_4) = y(xy^2+x^2)-x(y^3+xy) = 0$.
Non nascono nuovi polinomi e quindi $G = \{f_1 = x^3-2xy, f_2 = x^2y-y^2+x, f_3 = xy^2+x^2, f_4 = y^3+xy\}$
è una base di Gröbner per l'ideale <F>, per di più ridotta.

Vedere ora l'esercizio con ugual base e differente ordinamento contenuto nel file ESERCIZI sul CAPITOLO V.

ESEMPIO 8.4 Consideriamo come sopra $k[x,y]$ con l'ordinamento grLEX ($x>y$)

- Calcolando come sopra la base di Gröbner dell'ideale generato da
  $F = \{f_1 = x^3-2xy, f_2 = x^2y-2y^2+x\}$, si perviene a
  $G = \{f_1 = x^3-2xy, f_2 = x^2y-2y^2+x, f_3 = x^2, f_4 = 2xy, f_5=2y^2-x\}$ che non è ridotta, visto che
  $f_1 = xf_3-f_4, f_2 = 2f_3-f_5$ sono sovrabbondanti tanto per generare <F> che per generare <LT(<F>)>.
  La base ridotta corrispondente è $G := (f_3 = x^2, f_4 = xy, f_5 = y^2-x/2)$.

- Possiamo rifare il calcolo tenendo conto della riduzione intanto che si aggiungono nuovi polinomi: ad es. avendo aggiunto $-S(f_1,f_2)=x^2$, si possono dividere per questo polinomio i due polinomi f_1 ed f_2, pervenendo direttamente alla base ridotta.

Questi sono miglioramenti di poco conto nell'economia generale del calcolo delle basi di Gröbner.
Meglio tener conto delle potenzialità espresse dal teorema di caratterizzazione (7.1): in particolare scegliendo un sottoinsieme S dell'insieme delle sizigie elementari (e non tutte come si è fatto con questo algoritmo ingenuo) con la sola condizione che $S_{ij}\ G\to_G 0$.
Questo permette innanzitutto di non testare le S_{ij} che dipendono da altre (vedi Proposizione 5.7) e in secondo luogo di non testare le S_{ij} corrispondenti a polinomi aventi LT primi tra loro (che sicuramente si riducono a zero modulo G, vedi Proposizione 6.3).
L'idea vincente per la costruzione di un algoritmo migliore è quella di impostare l'algoritmo sulle sizigie elementari, anzi sulle coppie di indici che le individuano, costruendo un insieme B di coppie (i,j) (con $1\le i<j\le$ numero di polinomi in giuoco) che si altera ad ogni passo dell'algoritmo, perdendo le coppie già esaminate ed arricchendosi di quelle che nascono dall'eventuale polinomio aggiunto alla base.

9. ALGORITMO DI BUCHBERGER PER IL CALCOLO DI UNA BASE DI GRÖBNER

Input: F=($f_1,\dots,f_s$)
Output: G base di Gröbner per $<f_1,\dots,f_s>$
Inizializzazione
B:= $\{(i,j)\mid 1\le i<j\le s\}$
G:= F
t:= s
iterazione
WHILE B≠∅
    Scegli $(i,j)\in$ B
    IF m.c.m.(LT(f_i), LT(f_j)) ≠ LT(f_i)·LT(f_j) AND il criterio (f_i, f_j, B) è FALSO
    │ THEN S:= S(f_i, f_j)^G
    │ IF S≠0 THEN
    │ │ t:=t+1; f_t:=S
    │ │ G:=G∪{f_t}
    │ │ B:=B∪{(i, t) │ $1\le i\le t-1$}
    B:=B {(i, j)}

ove il criterio (f_i, f_j, B) vale se esiste $k\in\{1,\dots,t\}$ $\{i,j\}$ tale che LT(f_k) divide m.c.m.(LT(f_i),LT(f_j)) e B non contiene nessuna delle due coppie $[i,k]$ e $[j,k]$, che scriviamo con le parentesi quadre per ricordare di ordinarle in maniera inversa se k è minore di i o di j [(7)].

Dimostrazione in 3 parti:
1) terminazione dell'algoritmo
2) a ogni passo dell'algoritmo, B è tale che
   se $1\le i<j\le t$, ma $(i,j)\notin$ B allora S(f_i, f_j) $\to_G 0$ oppure vale il criterio (f_i, f_j, B)
3) all'ultimo passo, cioè quando B=∅, la corrispondente base G è di Gröbner.

1) L'algoritmo produce a ogni passo una base G dell'ideale I=$<f_1,\dots,f_s>$, uguale o ampliata rispetto al passo precedente. Inoltre, se il resto S è diverso da 0, l'ideale <LT(G∪{f_t})> contiene propriamente l'ideale <LT(G)>: per la CCA sugli ideali, la catena costituita dagli ideali generati dai LT deve stabilizzarsi, cioè da un certo momento in poi non devono più comparire resti non nulli. Ciò implica che G non cresce più e quindi il ramo di IF secondario non produce più nuove coppie: da quel momento il loop WHILE…DO rimuove a ogni passo una coppia da B (senza aggiungerne) e quindi, dopo un numero finito di passi, B si vuota.

2) Per provare (2) osservo che al passo iniziale tutte le coppie sono in B e quindi non devo fare verifiche. Assumo come *ipotesi ricorsiva* che per B valga la proprietà
   se $1\le i<j\le t$, ma $(i,j)\notin$ B allora S(f_i, f_j) $\to_G 0$ oppure vale il criterio (f_i, f_j, B)
   e *mostro che la stessa proprietà vale per l'insieme* B' *che si determina al passo successivo*.
   Conviene notare subito che se vale il criterio (f_i, f_j, B), cioè esiste un $k\notin\{i,j\}$ tale che $[i,k]\notin$ B e $[j,k]\notin$ B e LT(f_k) divide m.c.m.(LT(f_i),LT(f_j)), questo k corrisponde a un polinomio f_k già presente nella base G e quindi $[i,k]$ e $[j,k]$ non coincidono con nessuna delle nuove coppie (h,t) che possono essere aggiunte a B per formare B': quindi *l'eventuale validità del criterio passa da* B *a* B'.

(7) Per come è definito l'algoritmo, il fatto che le coppie non stiano più in B significa che le sizigie con gli indici corrispondenti sono già state esaminate ed appartengono alla base di sizigie, ovvero sono esprimibili attraverso tale base. Se si vuole avere subito un'idea del funzionamento dell'algoritmo, guardare l'esempio a §10 e le note per il calcolo immediatamente precedenti.

Analogamente, *se* $S(f_i,f_j) \to_G 0$ *allora risulta anche* $S(f_i,f_j) \to_{G'} 0$ *tanto nel caso in cui sia* G'=G *che nel caso in cui sia* $G'=G\cup\{f_t\}$.
Dividiamo ora la dimostrazione in due casi:

I) $(i,j)\notin B$ e $(i,j)\notin B'$.
Ciò significa che al passo precedente non ho esaminato (i, j) ma un'altra coppia (h, l) e applicando l'ipotesi ricorsiva trovo che, come detto sopra, se vale il criterio (f_i, f_j, B), vale anche (f_i, f_j, B'), mentre se $S(f_i,f_j) \to_G 0$ anche $S(f_i,f_j) \to_{G'} 0$, poiché
- o $B' \subset B$, cioè $B'=B\ \{(h, l)\}$ e G' = G
- oppure $B'\not\subset B$, cioè $B'=(B\ \{(h, l)\})\cup\{(1,t),\ldots,(t-1,t)\}$ e $G' = G\cup\{S\}$

II) $(i,j)\in B$ e $(i,j)\notin B'$. In questo caso non posso applicare l'ipotesi ricorsiva, poiché non è vero che $(i,j)\notin B$. Ma le ipotesi significano che al passo precedente ho esaminato (i,j) e
- o $\text{m.c.m.}(LT(f_i), LT(f_j)) = LT(f_i)\cdot LT(f_j)$ o il criterio (f_i, f_j, B) è valido o S=0: allora $B'=B\ \{(i,j)\}$ e G = G';
- oppure non vale nessuna delle condizioni precedenti: allora $B'\supset B\ \{(i,j)\}$, propriamente poiché a B per ottenere B' sono state aggiunte le coppie $(1,t),\ldots,(t-1,t)$, e $G'= G\cup\{f_t\}$.

Ora,
- se vale il criterio (f_i,f_j, B), come detto sopra vale (f_i,f_j, B');
- se $\text{m.c.m.}(LT(f_i), LT(f_j)) = LT(f_i)\cdot LT(f_j)$, allora, per la proposizione 6.3 (sulla riduzione a zero), si ha $S(f_i,f_j) \to_G 0$ e, poiché G=G', $S(f_i,f_j) \to_{G'} 0$;
- se $S=S(f_i,f_j)^G=0$, si ha $S(f_i,f_j) \to_G 0$ e, poiché G=G', $S(f_i,f_j) \to_{G'} 0$;
- se $S=S(f_i,f_j)^G\neq 0$, si ha $G'=G\cup\{S\}$ e $S(f_i,f_j)=a_1f_1+\ldots+a_{t-1}f_{t-1}+S\to_{G'} 0$, poiché se i quozienti e il resto nella divisione per $(f_1,\ldots,f_{t-1})$ sono $(a_1,\ldots,a_{t-1};S)$, allora $(a_1,\ldots,a_{t-1},1;0)$ sono quozienti e resto nella divisione per $G'=(f_1,\ldots,f_{t-1},S)$.

Ciò conclude la seconda parte della dimostrazione: si sarà notato che l'unico punto in cui non si riescono ad applicare considerazioni generali o l'ipotesi induttiva è l'ultimo, che peraltro è il più significativo, visto che dice che cosa succede nel caso critico in cui si aggiunge alla base un nuovo elemento.

3) Per verificare che quando B=∅ l'insieme $G = \{f_1,\ldots,f_t\}$ è una base di Gröbner, si utilizza la caratterizzazione (7.1) delle basi di Gröbner. Si pone in evidenza una base $\mathcal{S}$ di sizigie omogenee per il modulo S(G) delle sizigie dei LT di G e si mostra che per ogni $S\in\mathcal{S}$ si ha $S\ G\to_G 0$.
Come $\mathcal{S}$ si considera il sottoinsieme delle sizigie elementari $\{S_{ij},\ 1\le i<j\le t\}$ formato togliendo ogni S_{ij} tale che quando nell'algoritmo si è considerata la coppia (i, j) il criterio (f_i, f_j, B) è risultato valido.
Si deve *provare che* $\mathcal{S}$ *è una base di* S(G).
Riscriviamo le coppie a ritroso cominciando dall'ultima eliminata per arrivare a B=∅. A meno del nome dato agli indici si ha una tabella di questo tipo

$(t-1,t)$	…..	$(3,t)$	$(2,t)$	$(1,t)$
…..	…..	…..	…..
	$(3,4)$	$(2,4)$	$(1,4)$
		$(2,3)$	$(1,3)$
			$(1,2)$

Attenzione: *per nessuna* delle coppie $(1, j)$ nel riquadro il *criterio* (f_1, f_j, B) può essere *valido*, poiché *j* non può essere elemento delle coppie nelle righe sottostanti.

che dobbiamo ora percorrere da sinistra a destra, dall'alto in basso, cancellando le coppie per cui il criterio (f_i,f_j, B) è risultato valido al passo (i,j).

ATTENZIONE In questo processo di cancellazione, l'insieme B da tener presente ad ogni passo è quello in cui la prima coppia da esaminare nell'algoritmo è proprio (i, j), mentre le coppie che in tabella si trovano sotto o a destra rispetto a (i, j) erano già state esaminate (e poi eliminate da B) quando ci si è posti il problema della validità del criterio. Ad es. "valeva (f_2, f_4, B) e quindi si è tolto (2,4)" significa che c'era un k diverso da 2 e 4 tale che $[2,k]$ e $[4,k]$ non stavano più in B quando si è esaminato (2,4) (e quindi k è necessariamente 1) e $LT(f_k)$ divideva m.c.m.$(LT(f_2), LT(f_4))$.

Si parte avendo tutte le coppie, cioè la base delle sizigie elementari: *si vuole mostrare che ogni volta che nella tabella si rimuove (dall'alto) una coppia*, e quindi una sizigia, *si ha ancora una base per* S(G).
Se dopo un certo numero di rimozioni si ha ancora una base e, prendendo in esame (i, j), si trova che il criterio (f_i, f_j, B) è valido, si rimuove la sizigia S_{ij}: per il criterio, denotato con $r \in \{s, s+1,\ldots,t\}$ il numero degli elementi presenti in G quando si va a considerare (i, j), esiste un $k \in \{1,\ldots,r\} \setminus \{i, j\}$ tale che $LT(f_k)$ divide m.c.m.$(LT(f_i), LT(f_j))$ e *le coppie* $[i,k]$ *e* $[j,k]$ *non stanno più in* B: ciò significa che nell'algoritmo le due coppie sono già state esaminate e quindi nella tabella le coppie $[i,k]$ e $[j,k]$ si trovano a valle di (i, j). Di conseguenza, le sizigie S_{ik} e S_{jk} non sono ancora state rimosse, per cui si può scrivere $S_{ij} = \boldsymbol{x}^{\alpha(i,k)}S_{ik} - \boldsymbol{x}^{\alpha(j,k)}S_{jk}$ e quindi anche rimuovendo S_{ij} dalla base si continua ad avere una base per S(G).
Ciò prova che $\mathcal{S}$ è una base di S(G): resta da *verificare che per ogni* S_{ij} di $\mathcal{S}$ *risulta* $S_{ij}\ G \to_G 0$.
Ora si è visto nella parte (2) che, ad ogni stadio dell'algoritmo, B ha la proprietà che se $(i, j) \notin B$ allora $S_{ij}\ G = S(f_i, f_j) \to_G 0$ oppure vale il criterio (f_i, f_j, B). Quando si considera G al passo intermedio che corrisponde a prendere in esame la coppia (i, j) e successivamente eliminarla da B, il criterio non può valere, altrimenti nella costruzione di $\mathcal{S}$ a partire dalle sizigie elementari avremmo rimosso la sizigia S_{ij} che quindi non apparterrebbe a $\mathcal{S}$: quindi si deve avere per quella base G, e a maggior ragione per la base che si ottiene alla fine, $S_{ij}\ G \to_G 0$. C.V.D.

QUALCHE NOTA PER IL CALCOLO
Sembra che la maniera efficiente per attaccare il ramo di IF principale sia:

- Calcola m.c.m.$(LT(f_i), LT(f_j)) = \boldsymbol{x}^{\gamma(i,j)}$
- Se $\boldsymbol{x}^{\gamma(i,j)} = LT(f_i) \cdot LT(f_j)$ chiudi il ramo di IF principale
- In caso contrario, per ogni $k \notin \{i, j\}$ vedi se $LT(f_k)$ divide $\boldsymbol{x}^{\gamma(i,j)}$

1. Quando ne trovi uno, verifica se $[i,k] \notin B$:
   a) in caso affermativo verifica se $[j,k] \notin B$ e in tal caso
      α) se sì chiudi il ramo di IF principale
      β) se no prendi in esame un altro k
   b) in caso negativo prendi in esame un altro k
2. Se non ne trovi nessuno o se nessuno verifica le condizioni successive calcola $S(f_i, f_j)$

- Ecc. come da algoritmo.

Insomma non ha senso verificare a priori se certe coppie stanno in B, se non si sa se vale la condizione $LT(f_k)$ divide $\boldsymbol{x}^{\gamma(i,j)}$.

L'algoritmo appena descritto non fornisce una base minimale e comunque può essere reso più efficiente.

- Si può cercare di "ridurre" sistematicamente la base G che si costruisce ad ogni passo, dividendo ogni elemento della base per la base privata dell'elemento stesso e sostituire, al posto del polinomio in esame, il resto. Questo dovrebbe evitare l'esplosione del numero dei polinomi della base e dovrebbe anche mantenere ragionevolmente basso il multigrado dei polinomi in gioco.
- Pare che per migliorare l'algoritmo sia comunque opportuno elencare i polinomi della base in ordine di LT crescente rispetto all'ordinamento monomiale prescelto.

- Buchberger (1985) ha dimostrato che si risparmia un po' se si prendono le coppie (i,j) in modo che sia minimo m.c.m.(LT(f_i), LT(f_j)).

Per un esempio concreto di calcolo vedi il paragrafo successivo.

10. UN ESEMPIO di applicazione DELL'ALGORITMO DI BUCHBERGER

Sia F la base data dai 3 polinomi: $f_1=x^2y+yz, f_2=xy^2-y, f_3=x^2y^2+z$, con l'ordinamento grLEX ($x>y>z$).

Prima di partire con l'algoritmo, verifichiamo se *è possibile sostituire ai polinomi assegnati dei polinomi più semplici, che generino lo stesso ideale*. Ciò succede sicuramente *se almeno uno dei polinomi ha LT divisibile per il LT di un altro*, poiché in tal caso il primo polinomio può essere sostituito dal resto nella divisione per il secondo.

Nel nostro caso LT(f_2) divide LT(f_3) e $f_3 = xf_2 + xy + z$, per cui alla base F sostituiamo la base

$$F' = \{f_1 = x^2y + yz, f_2 = xy^2 - y, f_3 = xy + z\}.$$

Di nuovo, LT(f_3) divide LT(f_1) e LT(f_2); inoltre $f_1 = xf_3 - xz + yz$ e $f_2 = yf_3 - yz - y$ per cui a F' sostituiamo la base

$$F''=\{f_1 = xz - yz, f_2 = yz + y, f_3 = xy + z\},$$

o meglio, sostituendo a f_1 il suo resto nella divisione per f_2, e riscrivendo i polinomi in ordine di LT crescente

$$F'''=\{f_1 = yz + y, f_2 = xz + y, f_3 = xy + z\}.$$

Ora possiamo partire con l'algoritmo di Buchberger.

I passo

G:		B={(1,2), (1,3), (2,3)}
$f_1=yz+y$	LT(f_1)=yz	(1,2): m.c.m.(yz, xz)=$xyz\neq xyz^2$
$f_2=xz+y$	LT(f_2)=xz	criterio (f_1, f_2, B) FALSO *poiché tutte le coppie stanno in* B
$f_3=xy+z$	LT(f_3)=xy	$S(f_1, f_2)^G= (xy-y^2)^G= (f_3-y^2-z)^G=-y^2-z$ *aggiungere a* G

II passo

G:		B={(1,3), (2,3), (1,4), (2,4), (3,4)}
$f_1=yz+y$	LT(f_1)=yz	(1,3): m.c.m.(yz, xy)=$xyz\neq xy^2z$, LT(f_2) *lo divide ma*
$f_2=xz+y$	LT(f_2)=xz	criterio (f_1, f_3, B) FALSO *poiché* (2,3) *sta in* B
$f_3=xy+z$	LT(f_3)=xy	$S(f_1, f_3)^G= (xy-z^2)^G= (f_3-z^2-z)^G=-z^2-z$ *aggiungere a* G
$f_4=y^2+z$	LT(f_4)=y^2	

III passo

G:		B={(2,3), (1,4), (2,4), (3,4), (1,5), (2,5), (3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(2,3): m.c.m.(xz, xy)=$xyz\neq x^2yz$, LT(f_1) *lo divide e quindi*
$f_2=xz+y$	LT(f_2)=xz	criterio (f_2, f_3, B) VERO *poiché* (1,2), (1,3) *non stanno in* B
$f_3=xy+z$	LT(f_3)=xy	
$f_4=y^2+z$	LT(f_4)=y^2	*niente da aggiungere a* G
$f_5=z^2+z$	LT(f_5)=z^2	

IV passo

G:		B={(1,4), (2,4), (3,4), (1,5), (2,5), (3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(1,4): m.c.m.(yz, y^2)=$y^2z\neq y^3z$, *solo* LT(f_1) *e* LT(f_4) *lo dividono e quindi*
$f_2=xz+y$	LT(f_2)=xz	criterio (f_1, f_4, B) FALSO
$f_3=xy+z$	LT(f_3)=xy	$S(f_1, f_4)^G= (y^2-z^2)^G= (f_4-z^2-z)^G=0$ *niente da aggiungere a* G
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

V passo

G:		B={(2,4), (3,4), (1,5), (2,5), (3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(2,4): m.c.m.(xz, y^2)=xy^2z, *niente da aggiungere a* G
$f_2=xz+y$	LT(f_2)=xz	
$f_3=xy+z$	LT(f_3)=xy	
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

VI passo

G:		B={(3,4), (1,5), (2,5), (3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(3,4): m.c.m.(xy, y^2)=$xy^2\neq xy^3$, *solo* LT(f_3) *e* LT(f_4) *lo dividono e quindi*
$f_2=xz+y$	LT(f_2)=xz	criterio (f_3, f_4, B) FALSO
$f_3=xy+z$	LT(f_3)=xy	$S(f_3, f_4)^G=(yz-xz)^G=(f_1-f_2)^G=0$ *niente da aggiungere a* G
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

VII passo

G:		B={(1,5), (2,5), (3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(1,5): m.c.m.(yz, z^2)=$yz^2\neq yz^3$, *solo* LT(f_1) *e* LT(f_5) *lo dividono e quindi*
$f_2=xz+y$	LT(f_2)=xz	criterio (f_1, f_5, B) FALSO
$f_3=xy+z$	LT(f_3)=xy	$S(f_1, f_5)^G=(yz-yz)^G=0$ *niente da aggiungere a* G
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

VIII passo

G:		B={(2,5), (3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(2,5): m.c.m.(xz, z^2)=$xz^2\neq xz^3$, *solo* LT(f_2) *e* LT(f_5) *lo dividono e quindi*
$f_2=xz+y$	LT(f_2)=xz	criterio (f_2, f_5, B) FALSO
$f_3=xy+z$	LT(f_3)=xy	$S(f_2, f_5)^G=(yz-xz)^G=(f_1-f_2)^G=0$ *niente da aggiungere a* G
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

IX passo

G:		B={(3,5), (4,5)}
$f_1=yz+y$	LT(f_1)=yz	(3,5): m.c.m.(xy, z^2)=xyz^2 *niente da aggiungere a* G
$f_2=xz+y$	LT(f_2)=xz	
$f_3=xy+z$	LT(f_3)=xy	
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

X passo

G:		B={(4,5)}
$f_1=yz+y$	LT(f_1)=yz	(4,5): m.c.m.(y^2, z^2)=y^2z^2 *niente da aggiungere a* G
$f_2=xz+y$	LT(f_2)=xz	
$f_3=xy+z$	LT(f_3)=xy	
$f_4=y^2+z$	LT(f_4)=y^2	
$f_5=z^2+z$	LT(f_5)=z^2	

A questo punto B si vuota. Quindi la base di Gröbner (ridotta) è:

$$\{f_1=yz+y, f_2=xz+y, f_3=xy+z, f_4=y^2+z, f_5=z^2+z\}.$$

11. COMPLESSITÀ DI CALCOLO

Per queste valutazioni rimandiamo alle ultime due pagine del Cap. 2 di Cox & C. (§9, pp. 110, 111).
Il grado cresce velocemente, anche quando si usa uno degli ordinamenti che maggiormente contengono il grado (come gREVLEX).
Visto che le basi di Gröbner sono solo uno strumento (ed entro certi limiti l'ordinamento monomiale da scegliere è arbitrario) una delle possibili vie di soluzione del problema dell'esplosione del grado è un algoritmo che cambi ordinamento cammin facendo, in modo da ottenere basi di Gröbner più efficienti.

Un esempio che mostra come anche con l'ordinamento gREVLEX il grado può esplodere si trova negli esercizi contenuti nel file ESERCIZI sul CAPITOLO V.

12. UN'APPLICAZIONE ALGEBRICA DELLE BASI DI GRÖBNER

Abbiamo già visto che saper calcolare la base di Gröbner ridotta (rispetto ad un ordinamento monomiale conveniente) di un ideale di $k[x_1,\ldots,x_n]$ permette di rispondere a due domande:

- Il polinomio f di $k[x_1,\ldots,x_n]$ appartiene all'ideale I di $k[x_1,\ldots,x_n]$?
- I due ideali I e J di $k[x_1,\ldots,x_n]$ coincidono?

Illustriamo ora come usare le basi di Gröbner per risolvere un altro problema algebrico:

- Dati due ideali $I=\langle f_1, \ldots, f_r\rangle$ e $J=\langle g_1, \ldots, g_s\rangle$ di $k[x_1, \ldots, x_n]$, quali sono i generatori dell'ideale intersezione $I\cap J$?

Se $r = s = 1$ si vede facilmente che $I\cap J$ è l'ideale principale generato dal minimo comune multiplo m dei due generatori f e g: infatti m appartiene all'intersezione e ogni altro polinomio, dovendo essere divisibile tanto per f che per g è un multiplo di m. Questa caratterizzazione non è comunque molto operativa, se non si conosce una scomposizione in fattori irriducibili f e g.
Per aggirare il problema si può aggiungere un'indeterminata y e tradurre l'intersezione di ideali in intersezione tra un ideale di $k[t, x_1, \ldots, x_n]$ e il sottoanello $k[x_1, \ldots, x_n]$.

Dati un ideale I di $k[x_1, \ldots, x_n]$ e un polinomio p di $k[t]$, denotiamo con

$$p\mathrm{I}$$

l'ideale di $k[t, x_1,\ldots, x_n]$ generato dai prodotti pf ove f è un qualunque polinomio di I.

OSSERVAZIONE 12.1 *Se in* $k[x_1, \ldots, x_n]$ *l'ideale* I *è generato da* $f_1, \ldots, f_r$, *l'ideale* pI *di* $k[t, x_1,\ldots, x_n]$ *è generato da* $pf_1, \ldots, pf_r$. *Inoltre, se* g *è un polinomio di* pI, *per tutti i* $c\in k$ *il polinomio* $g(c, x_1, \ldots, x_n)$ *appartiene a* I.
Infatti ogni elemento g di pI si scrive come somma di polinomi del tipo phf ove $h\in k[t, x_1, \ldots, x_n]$ e f, appartenendo a I, ha la forma $a_1f_1+\ldots+a_rf_r$, con $a_i\in k[x_1,\ldots,x_n]$: quindi g è somma di polinomi del tipo pha_if_i (con $i = 1, \ldots, r$) cioè combinazione tramite i polinomi $ha_i \in k[t, x_1, \ldots, x_n]$ di pf_i (ove i=1,…, r). Questo stesso ragionamento dice che

$$g(c, x_1, \ldots, x_n) = \sum p(c)\, h_\alpha(c, x_1, \ldots, x_n)\, a_{\alpha i}(x_1, \ldots, x_n)\, f_i(x_1, \ldots, x_n)$$

appartiene a $k[x_1, \ldots, x_n]$.

TEOREMA 12.2 *Siano* I *e* J *due ideali di* $k[x_1, \ldots, x_n]$. *La loro intersezione è l'insieme dei polinomi di* $k[x_1,\ldots,x_n]$ *che appartengono all'ideale* $t\mathrm{I} + (1-t)\mathrm{J}$ *di* $k[t, x_1,\ldots, x_n]$:

$$\mathrm{I}\cap\mathrm{J} = [t\mathrm{I} + (1-t)\mathrm{J}] \cap k[x_1,\ldots,x_n].$$

Dimostrazione Ogni $f\in \mathrm{I}\cap\mathrm{J}$ appartiene a $k[x_1,\ldots,x_n]$. Inoltre, $tf\in t\mathrm{I}$ e $f=tf+(1-t)f$ e quindi f appartiene a $t\mathrm{I} + (1-t)\mathrm{J}$. Viceversa, se $f\in [t\mathrm{I} + (1-t)\mathrm{J}] \cap k[x_1, \ldots, x_n]$ si può scrivere

$$f(x_1, \ldots, x_n)=g(t, x_1, \ldots, x_n) + h(t, x_1, \ldots, x_n) \text{ con } g\in t\mathrm{I},\ h\in (1-t)\mathrm{J}.$$

Applicando l'osservazione con $t = c = 0$ si ha che il polinomio

$$f(x_1, \ldots, x_n) = g(0, x_1, \ldots, x_n) + h(0, x_1,\ldots, x_n)$$

è somma del polinomio nullo di I (infatti $g(t, x_1, \ldots, x_n)$, in quanto multiplo di t, si annulla se $t = 0$) e di un polinomio che appartiene a J: dunque f sta in J.
Similmente applicando l'osservazione con $t = c = 1$ si ha che il polinomio

$$f(x_1, \ldots, x_n) = g(1, x_1, \ldots, x_n) + h(1, x_1, \ldots, x_n)$$

è somma di un polinomio che appartiene a I e del polinomio nullo di J (infatti $h(t, x_1, \ldots, x_n)$, in quanto multiplo di $(1-t)$, si annulla in $t = 1$): dunque f sta in I. C.V.D.

Siano ora I e J due ideali di $k[x_1, \ldots, x_n]$ generati rispettivamente da $\{f_1, \ldots, f_r\}$ e da $\{g_1, \ldots, g_s\}$. In base all'osservazione, gli ideali $t\mathrm{I}$ e $(1-t)\mathrm{J}$ di $k[t, x_1, \ldots, x_n]$ sono generati rispettivamente da $\{tf_1, \ldots, tf_r\}$ e da $\{(1-t)g_1, \ldots, (1-t)g_s\}$ e quindi $t\mathrm{I} + (1-t)\mathrm{J}$ è generato da

$$\mathrm{F} = \{tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s\}.$$

Allora, per trovare un **sistema di generatori di I∩J**, calcoliamo a partire da F una base di Gröbner G rispetto ad un ordinamento "di eliminazione prima" (cioè un ordinamento in cui tutti i monomi contenenti la prima indeterminata sono maggiori degli altri, come ad esempio LEX [8] con $t > >x_1>\ldots>x_n$): usando l'algoritmo della divisione si prova [9] che il sottoinsieme G* di G formato dai polinomi di G che non contengono l'indeterminata t è una base di $[t\mathrm{I} + (1-t)\mathrm{I}] \cap k[x_1, \ldots, x_n]$ e quindi, per il teorema 12.2, di I∩J.

ESEMPIO 12.3 Per trovare i generatori di $<x^2y>\cap<xy^2>$, calcoliamo la base di Gröbner (ridotta) rispetto a LEX con $t > x > y$ di $<tx^2y, (1-t)xy^2>$. Essa è $\{tx^2y, txy^2-xy^2, x^2y^2\}$ e quindi l'intersezione è generata da x^2y^2 che (come osservato all'inizio del paragrafo) è mcm(x^2y, xy^2).

La procedura appena illustrata per il calcolo dei generatori dell'intersezione suggerisce una strategia per ricavare il **minimo comune multiplo di due polinomi** f e g di $k[x_1, \ldots, x_n]$ senza conoscerne la scomposizione in fattori primi. Infatti un generatore di $<f>\cap<g>$ è mcm(f,g) - e tutti gli altri sono i suoi multipli mediante gli elementi non nulli di k - e quindi basta trovare l'elemento non contenente t della base di Gröbner ridotta, rispetto a LEX con $t > x_1 >\ldots> x_n$, dell'ideale $<tf, (1-t)g>$.
Questo algoritmo permette anche di trovare il **massimo comun divisore di due polinomi** f e g di $k[x_1, \ldots, x_n]$ senza conoscerne la scomposizione in fattori primi. Infatti $k[x_1, \ldots, x_n]$ è un UFD e si è visto nel Capitolo II proposizione 2.2 che in tali anelli MCD$(f, g)\cdot$mcm$(f, g)=f\cdot g$.

---

[8] In realtà per i nostri scopi non è necessario usare l'ordinamento LEX: basta usare un ordinamento prodotto, con LEX sulla prima variabile e un ordinamento graduato sulle rimanenti. Questo rende un po' meno lungo il calcolo della base di Gröbner.

[9] Se non si vuol provare a indovinare come, si veda la dimostrazione del teorema di eliminazione (teorema 1.2 del capitolo VII). Si tenga presente che in tale sede viene detto ***ideale di eliminazione prima*** *di un ideale assegnato* in $k[t,x_1,\ldots,x_n]$ l'ideale di $k[x_1,\ldots,x_n]$ ottenuto - come $[t\mathrm{I}+(1-t)\mathrm{J}]\cap k[x_1,\ldots,x_n]$ - individuando, tra tutti i polinomi dell'ideale dato, quelli che non contengono la prima indeterminata.

Va però detto che tale algoritmo per il calcolo del massimo comun divisore è tutt'altro che "computazionalmente pratico".
La situazione peggiora poi quando $n>1$ [(10)] e il numero s di polinomi di cui calcolare il mcm o il MCD è maggiore di 2. L'osservazione 2.3 del Capitolo II dice che mcm(f_1, f_2, ..., f_s) è "il" generatore dell'ideale $(f_1)\cap(f_2)\cap...\cap(f_s)$: quindi per trovare il mcm bisogna iterare la procedura precedente $s-1$ volte, mentre per trovare il MCD bisogna utilizzare $s-1$ volte la relazione $\text{MCD}(f, g)\cdot\text{mcm}(f, g) = f\cdot g$ con $f = \text{MCD}(f_1,\ldots,f_i)$ e $g = f_{i+1}$, ogni volta facendo riferimento all'algoritmo per la determinazione del mcm.

[(10)] Per $n=1$ l'anello $k[x]$ è un PID e quindi per trovare il MCD di s polinomi $f_1,\ldots,f_s$, basta (per la proposizione 3.6 del Capitolo II) trovare il generatore dell'ideale da essi generato ad esempio calcolandone la base di Gröbner ridotta, oppure usando ripetutamente l'algoritmo euclideo. Invece il mcm potrà essere calcolato utilizzando ripetutamente la relazione $\text{MCD}(f,g)\cdot\text{mcm}(f,g)=f\cdot g$ con $f=\text{mcm}(f_1,\ldots,f_i)$ e $g=f_{i+1}$.