ESERCIZI SUL CAPITOLO VII

1. Si consideri un sistema lineare di m equazioni in n incognite: $\{f_1=0, f_2=0,\dots, f_m=0\}$ ove $f_i=a_{i1}x_1+\dots+a_{in}x_n-b_i$, per ogni $i=1,\dots,m$. Mostrare che
   a) cercare una base di Gröbner rispetto all'ordinamento LEX ($x_1>\dots>x_n$) dell'ideale $<f_1,f_2,\dots,f_m>$ equivale ad applicare il metodo di Gauss per la riduzione del sistema a forma pseudotriangolare;
   b) cercare la corrispondente base ridotta equivale proseguire nella riduzione della matrice completa del sistema (sottraendo multipli delle righe finali alle precedenti, in modo da evidenziare il maggior numero possibile di coefficienti nulli: metodo di Gauss-Jordan);
   c) calcolare le soluzioni di un sistema lineare con il metodo di Gauss-Jordan significa applicare la procedura di eliminazione ed estensione.

2. Trovare basi di Gröbner per gli ideali di eliminazione I_1 e I_2 dell'ideale I determinato dalle equazioni del sistema dell'esempio 1.1: $\begin{cases} x+y+z^2=1 \\ x+y^2+z=1 \\ x^2+y+z=1 \end{cases}.$

3. Mostrare che se due polinomi f e g di $k[x]$ sono primi tra loro esistono due polinomi a e b rispettivamente di grado minore del grado di g e di quello di f tali che $af+bg=1$.

4. Verificare che il rango della matrice di Sylvester Syl(f,g,x) vale
   - 5, se $f=x^2(x-1)(x+1)$ e $g=x^3(x-1)$
   - 4, se $f=(x-1)(x^2+x+1)$ e $g=(x^2-1)(x^2+x+1)$

   Più in generale, mostrare che se f e g sono due polinomi di $k[x]$ di gradi rispettivamente l e m (entrambi >0) che hanno come massimo comun divisore un polinomio di grado d, il rango di Syl(f,g,x) vale $l+m-d$. (Attenzione: questo non significa comunque che se il rango di Syl(f,g,x) vale r i polinomi abbiano in comune un fattore del tipo $(x-a)^{l+m-r}$, ma solo che hanno in comune un polinomio di grado $l+m-r$).

5. Si consideri in $\mathbf{C}[x,y,z]$ l'ideale I generato dai polinomi:
   $$f_1=xy+z,\ f_2=xz+y,\ f_3=y^2+z,\ f_4=yz+y,\ f_5=z^2+z$$
   a) si verifichi che l'insieme dei generatori è una base di Gröbner rispetto all'ordinamento LEX ($x>y>z$);
   b) si determinino gli ideali di eliminazione I_2 e I_1 e le corrispondenti varietà in $\mathbf{C}$ e $\mathbf{C}^2$;
   c) si verifichi che le condizioni espresse dal teorema di estensione (teorema 2.2) non sono verificate da tutte le coppie appartenenti a $V(I_1)$, anche se in realtà tutte le coppie soluzione sono estensibili;
   d) si verifichi che, se si passa alla base di Gröbner di I rispetto all'ordinamento LEX ($z>y>x$) e si ripete tutta la procedura, le condizioni espresse dal teorema di estensione (teorema 2.2) sono verificate da tutte le coppie appartenenti alla varietà $V(I_1)$ dell'ideale di eliminazione prima costruito rispetto al nuovo ordinamento.

SOLUZIONI

1. Possiamo supporre $a_{11}=1$ (in caso contrario, dopo aver eventualmente cambiato l'ordine dei polinomi in modo che il primo abbia coefficiente $a_{11}\neq 0$, dividiamo il primo coefficiente per a_{11}). Allora ogni $S(f_1,f_i)=a_{i1}f_1-f_i=(a_{i1}a_{12}-a_{i2})x_2+\ldots+(a_{i1}a_{1n}-a_{in})x_n-(b_1-b_i)$ è un polinomio che non contiene la prima indeterminata (e quindi ha resto 0 nella divisione per i polinomi della base) e che andrebbe aggiunto alla base $\{f_1, f_2,\ldots, f_m\}$: in realtà è immediato verificare che esso può essere sostituito in tale base al polinomio f_i. A meno del segno dei polinomi, questo equivale ad aver ridotto a 0 tutti gli elementi diversi dal primo che compaiono nella prima colonna della matrice completa del sistema lineare e quindi al primo passo nel metodo di eliminazione di Gauss (e ad evidenziare un sistema di generatori dell'ideale di eliminazione I_1). Iterando sui polinomi $\{S(f_1,f_2),\ldots,S(f_1,f_m)\}$, cioè sulla matrice che si ottiene eliminando la prima riga e la prima colonna, si mostra che trovare una base di Gröbner equivale a ridurre la matrice completa a forma pseudotriangolare con il metodo di eliminazione di Gauss e d'altra parte, visto che ad ogni passo ciò evidenzia un sistema di generatori di un ideale di eliminazione che contiene meno variabili rispetto al passo precedente, è ovvio che questa è proprio una procedura di eliminazione. Per ridurre la base di Gröbner così trovata, bisogna cercare il resto della divisione di ogni polinomio per gli altri: visto che i LT dei primi polinomi sono maggiori di quelli degli ultimi, è sensato ridurre il penultimo polinomio mediante l'ultimo, quello immediatamente precedente mediante l'ultimo e il penultimo e via dicendo; si vede inoltre che il resto si trova semplicemente sottraendo multipli mediante elementi di k di tali polinomi (per un fatto di grado): e questo corrisponde esattamente a completare l'applicazione del metodo di Gauss-Jordan. Per finire osserviamo che nel procedimento di Gauss-Jordan si determinano i valori ammissibili per le incognite "minori" e si vanno via via ad estendere le soluzioni ricavando da questi i valori per le incognite "maggiori" (risalendo nella matrice completa dall'ultima riga non nulla alla prima): e questa è proprio la procedura di estensione.

2. Conviene partire dall'ideale $I=\langle x+y+z^2-1,\ x^2+y+z-1,\ y^2-y-z^2+z\rangle$ ed eliminare rispetto a LEX con $x>y>z$.
   $S(f_1,f_2)^G=(xf_1-f_2)^G=(xy+xz^2-x-y-z+1)^G=[(x+y+z^2-1)(y+z^2-1)-(y^2-y-z^2+z)-2yz^2-z^4+z^2]^G=$
   $=-2yz^2-z^4+z^2$:
   sostituire a f_2 cambiando segno:
   $G=\{x+y+z^2-1,\ 2yz^2+z^4-z^2,\ y^2-y-z^2+z\}$
   $S(f_2,f_3)^G=(yf_2-2z^2f_3)^G=(yz^4+yz^2+z^4-z^3)^G=[(2yz^2+z^4-z^2)(z^2+1)/2-z^6/2+2z^4-2z^3+z^2/2]^G=$
   $=-z^6/2+2z^4-2z^3+z^2/2$
   $G=\{x+y+z^2-1,\ 2yz^2+z^4-z^2,\ y^2-y-z^2+z,\ z^6-4z^4+4z^3-z^2\}$
   Anche se il grado totale del sistema aumenta considerevolmente (da 8° a 96°) le soluzioni sono le 5 trovate nell'esempio 1.1.
   Si ha $G_1=\{2yz^2+z^4-z^2,\ y^2-y-z^2+z,\ z^6-4z^4+4z^3-z^2\}$ e $G_2=\{z^6-4z^4+4z^3-z^2\}$.

3. Applichiamo ai due polinomi f e g di $k[x]$ l'algoritmo euclideo delle divisioni successive. Se sono primi tra loro, esisterà un opportuno indice i tale che
   $$f=gq_0+r_0,\quad g=r_0q_1+r_1,\quad r_0=r_1q_2+r_2,\quad r_1=r_2q_3+r_3,\ \ldots,\ r_{i-1}=r_iq_{i+1}+r_{i+1},$$
   con $0=\deg(r_{i+1})<\deg(r_i)<\deg(r_{i-1})<\ldots<\deg(r_3)<\deg(r_2)<\deg(r_1)<\deg(r_0)<\deg(g)$ e quindi
   $$\deg(f)=\deg(g)+\deg(q_0),\ \ \deg(g)=\deg(r_0)+\deg(q_1),\ \ldots,\ \deg(r_{i-1})=\deg(r_i)+\deg(q_{i+1}),$$
   cioè, sostituendo:
   $$\deg(g)=\deg(r_i)+[\deg(q_{i+1})+\ldots+\deg(q_2)+\deg(q_1)]$$
   e

$$\deg(f)=\deg(r_i)+[\deg(q_{i+1})+\ldots+\deg(q_2)+\deg(q_1)+\deg(q_0)].$$

D'altra parte, da

$$r_0=f-gq_0,\quad r_1=g-r_0q_1,\quad r_2=r_0-r_1q_2,\quad r_3=r_1-r_2q_3,\ \ldots,\ r_{i+1}=r_{i-1}-r_iq_{i+1},$$

per sostituzioni successive si trova:

$$r_1=-fq_1+g(1+q_0q_1),\quad r_2=f(1+q_1q_2)-g(q_0+q_2+q_0q_1q_2),$$
$$r_3=-f(q_1+q_3+q_1q_2q_3)+g(1+q_0q_1+q_0q_3+q_2q_3+q_0q_1q_2q_3),\ \ldots,\ r_{i+1}=fA+gB$$

ove A è un polinomio somma di $q_1q_2q_3\cdot\ldots\cdot q_{i+1}$ con altri polinomi di grado inferiore e B è un polinomio somma di $q_0q_1q_2q_3\cdot\ldots\cdot q_{i+1}$ con altri polinomi di grado inferiore. Ne segue che

$$\deg(A)=\deg(q_{i+1})+\ldots+\deg(q_2)+\deg(q_1)$$

e

$$\deg(B)=\deg(q_{i+1})+\ldots+\deg(q_2)+\deg(q_1)+\deg(q_0).$$

Dunque, visto che $\deg(r_i)\geq 1$, si ha

$$\deg(A)=\deg(g)-\deg(r_i)\leq\deg(g)-1 \qquad \text{e} \qquad \deg(B)=\deg(f)-\deg(r_i)\leq\deg(f)-1.$$

D'altra parte r_{i+1} è un elemento non nullo del campo k e quindi, dividendo per esso l'uguaglianza $r_{i+1}=fA+gB$ (e ponendo ad esempio $A=r_{i+1}a$ e $B=r_{i+1}b$) si vede che
$1=fa+gb$ con $\deg(a)\leq\deg(g)-1$ e $\deg(b)\leq\deg(f)-1$.

4. Se $f=x^2(x-1)(x+1)=x^4-x^2$ e $g=x^3(x-1)=x^4-x^3$, la matrice $\mathrm{Syl}(f,g,x)$ ha le ultime due righe nulle (e quindi, avendo ordine 4+4=8 ha rango $r\leq 6$). Inoltre se nella matrice ottenuta da $\mathrm{Syl}(f,g,x)$ rimuovendo le ultime 2 righe, si somma la prima riga alla seconda, la nuova seconda alla terza ecc., la sesta riga risulta nulla:

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

D'altra parte, è immediato che l'ultima colonna di questa nuova matrice è indipendente dalle prime 4 e quindi $r=5$.

Se $f=(x-1)(x^2+x+1)=x^3-1$ e $g=(x^2-1)(x^2+x+1)=x^4+x^3-x-1$, la matrice $\mathrm{Syl}(f,g,x)$ ha due coppie di righe (denotate con il quadretto e il triangolo) opposte e quindi riconducibili a due righe nulle, mentre sommando le due denotate con * all'ultima si ottiene una terza riga nulla:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 0 & 1 & -1 & 0 & 1 \\ 0 & -1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 \end{pmatrix} \begin{array}{c} * \\ \square \\ \nabla \\ * \\ \square \\ \nabla \\ \end{array} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

quindi $\mathrm{Syl}(f,g,x)$, visto che ha ordine 4+3=7, ha rango $r=4$.

Supponiamo infine che f e g siano due polinomi di $k[x]$ di gradi rispettivamente l e m ($l>m>0$) che hanno come massimo comun divisore un polinomio M di grado d: cioè sia

- $f=FM$ e $g=GM$ con $\mathrm{MCD}(F,G)=1$
- $F=a_0x^{l-d}+\ldots+a_{l-d}$, $G=b_0x^{m-d}+\ldots+b_{m-d}$, $M=x^d+c_1x^{d-1}+\ldots+c_d$,

Allora

$$FM=a_0x^l+(a_0c_1+a_1)x^{l-1}+(a_0c_2+a_1c_1+a_2)x^{l-2}\ldots+a_{l-d}\,c_d,$$
$$GM=b_0x^m+(b_0c_1+b_1)x^{m-1}+(b_0c_2+b_1c_1+b_2)x^{m-2}\ldots+b_{m-d}\,c_d$$

Quindi la matrice di Sylvester Syl(FM,GM,x) può essere ridotta sommando via via a una riga la combinazione lineare delle precedenti (che contengono solo i coefficienti di F e di G) tramite i coefficienti $c_1,\dots, c_d$ che compaiono in quella riga in almeno una componente, pervenendo a una matrice che ha le ultime d righe nulle e contiene nelle prime m colonne i coefficienti di F (ordinati in colonne e slittati a ogni colonna di 1 verso il basso come si farebbe per costruire Syl(F,G,x)) e nelle restanti l i coefficienti di G (analogamente ordinati). Togliendo dalla matrice così ottenuta le ultime d righe e le colonne dalla (m+1)-esima alla (m+d)-esima si trova una matrice quadrata di ordine $l+m-d$ che ha determinante non nullo, poiché ha la forma $\left(\begin{array}{c|c} \mathrm{A} & \mathrm{O} \\ \hline \mathrm{B} & \mathrm{Syl}(F,G,x) \end{array}\right)$ ove A è una matrice triangolare bassa di ordine d avente gli elementi sulla diagonale tutti $=a_0$ e $|\mathrm{Syl}(F,G,x)|\neq 0$, poiché MCD($F$,$G$)=1. Dunque il rango di Syl(f,g,x) vale $l+m-d$. Si consiglia di provare a riscrivere i passaggi del ragionamento nel caso particolare $F=a_0x^2+a_1x+a_2$, $G=b_0x+b_1$, $M=x^2+c_1x+c_2$.

5. Consideriamo in $\mathbf{C}[x,y,z]$ l'ideale $\mathrm{I} = < f_1 = xy+z,\ f_2 = xz+y,\ f_3 = y^2+z,\ f_4 = yz+y,\ f_5 = z^2+z >$.
   a) L'insieme $\{f_1,\ f_2,\ f_3,\ f_4,\ f_5\}$ è una base di Gröbner rispetto all'ordinamento LEX (x>y>z) poiché i 10 polinomi sizigietici $S(f_i, f_j)$ hanno resto nullo nella divisione per gli elementi dell'insieme;
   b) $\mathrm{I}_2 = < z^2+z>$, $\mathrm{I}_1 = < y^2+z,\ yz+y,\ z^2+z>$;
   in $\mathbf{C}$ si ha $V(\mathrm{I}_2)= \{0,\ -1\}$ e in $\mathbf{C}^2$ si ha $V(\mathrm{I}_1)= \{(0,0),\ (\pm 1, -1)\}$ e si può applicare il teorema di estensione (teorema 2.2) poiché i coefficienti dei termini di grado massimo in y generano l'ideale $<1, z>=<1>$ cui corrisponde la varietà vuota;
   c) Nessuno dei coefficienti del termine di grado massimo in x nei polinomi della base è costante: essi generano l'ideale $<y, z>$ e quindi $V(\mathrm{I}_1)\cap V(y, z)$ contiene la coppia (0, 0) a cui non si può perciò applicare il teorema di estensione: a priori questa coppia potrebbe non essere estendibile, cioè potrebbe non appartenere a $\pi_1(V(\mathrm{I}))$. È però facile vedere che le due restanti equazioni $f_1 = 0$, $f_2 = 0$ sono verificate da tutte le terne (h, 0, 0) e quindi complessivamente
   $$V(\mathrm{I}) = \{(-1, -1, -1), (1, 1, -1)\}\cup\{(h, 0, 0), h \in\mathbf{C}\};$$
   d) la base di Gröbner di I rispetto all'ordinamento LEX (z>y>x) è $\{z + y^2,\ y^2 - yx,\ yx^2 - y\}$ per cui $\mathrm{I}_2 = <0>$, $\mathrm{I}_1 = < y^2 - yx,\ yx^2 - y>$.
   Allora in $\mathbf{C}$ si ha $V(\mathrm{I}_2) = \mathbf{C}$ e in $\mathbf{C}^2$ si ha $V(\mathrm{I}_1)= \{(\pm 1, \pm 1), (\pm 1, 0)\}\cup\{(h, 0), h \in\mathbf{C}\}$; a queste soluzioni si può applicare il teorema di estensione poiché nella base evidenziata i coefficienti dei termini di grado massimo in z generano l'ideale <1> cui corrisponde la varietà vuota; ovviamente $V(\mathrm{I})$ è la stessa evidenziata sopra.