21-11-16

Ασκ

$f = x^3y^3 - x^3 - y^3$, $f_1 = -x^2 + xy^2$, $f_2 = x^2y - y^2 \in \mathbb{Q}[x,y]$

με lex $x > y$. Διαιρέστε τον F με τα $\{f_1, f_2\}$

Λύση

$$F = (-xy^3+x-y^5+y^2)f_1 + (\quad 0 \quad)f_2 + (xy^7-xy^4-y^3)$$

$$F = x^3y^3 - x^3 - y^3 \xrightarrow{f_1} x^3y^3 - x^3 - y^3 - \frac{x^3y^3}{-x^2}(-x^2+xy^2) =$$

$$= -x^3 - y^3 + x^2y^5 = -x^3 + x^2y^5 - y^3 \xrightarrow{f_1} -x^3 + x^2y^5 - y^3 -$$

$$- \frac{-x^3}{-x^2}(-x^2+xy^2) = x^2y^5 - y^3 - x^2y^2 = x^2y^5 - x^2y^2 - y^3 \xrightarrow{f_1}$$

$$\rightarrow x^2y^5 - x^2y^2 - y^3 - \frac{x^2y^5}{-x^2}(-x^2+xy^2) = -x^2y^2 - y^3 + xy^7 =$$

$$= -x^2y^2 + xy^7 - y^3 \xrightarrow{f_1} -x^2y^2 + xy^7 - y^3 - \frac{-x^2y^2}{-x^2}(-x^2+xy^2) =$$

$$= xy^7 - y^3 - xy^4 = xy^7 - xy^4 - y^3 \xrightarrow{\text{υπόλ.}} -xy^4 - y^3 \xrightarrow{\text{υπόλ.}} -y^3 \rightarrow 0$$

Ως ΑΣΚ την ίδια με deglex $x>y$

Βάσεις Gröbner

Ορισμός: Ένα σύνολο μη μηδενικών πολυωνύμων $G=\{g_1,\dots,g_t\}$ που περιέχεται σ'ένα ιδεώδες I λέγεται βάση Gröbner του I αν για κάθε μη μηδενικό $f\in I$ υπάρχει $i\in\{1,2,\dots,t\}$ έτσι ώστε: $lm(g_i) \mid lm(f)$

g_1 g_2
|| ||

πχ) $\mathbb{Q}[x,y,z]$, lex $x>y>z$. Ν.δ.ό το $G=\{x-y+z, y+z^2\}$ είναι βάση Gröbner του $I=\langle x-y+z, y+z^2\rangle$

Λύση

$lm(g_1)=x$, $lm(g_2)=y$.

Έστω $f\neq 0$ και $f\in I$. Θέτω ν.δ.ό $lm(f)$ είναι πολλαπλάσιο του $lm(g_1)=x$ ή του $lm(g_2)=y$.

Έστω $f\neq 0$, $f\in I$ και $lm(f)$ δεν είναι πολ/σιο του x ή του y.

$f\in I \Rightarrow f = h_1\cdot g_1 + h_2 g_2 = h_1(x-y+z) + h_2(y+z^2)$

$lm(f) = x^a y^b z^\gamma$ το οποίο δεν είναι πολ/σιο του x και y

άρα $a=0$ και $b=0 \Rightarrow lm(f)=z^\gamma \Rightarrow$

$\Rightarrow f = C_\gamma z^\gamma + C_{\gamma-1} z^{\gamma-1} + \dots + C_1 z + C_0$

Άρα, $C_\gamma 2^\gamma + C_{\gamma-1} 2^{\gamma-1} + \cdots + C_1 2 + C_0 = h_1 (x-y+2) + h_2 (y+7z)$ (1)

Θα ίσχυε το $\begin{cases} x-y+2=0 \Rightarrow x=-8z \\ y+7z=0 \Rightarrow y=-7z \end{cases}$

Όπότε από (1): $C_\gamma 2^\gamma + \cdots + C_1 2 + C_0 \equiv 0 \Rightarrow f=0$. Άτοπο!
Έτσι το G είναι βάση Gröbner.

Άσκ
$\mathbb{Q}[x,y,z]$, με $x > z > y > x$. Δείξτε ότι το $G = \{g_1 = x-y+2, g_2 = y+7z\}$ δεν είναι βάση Gröbner για το ιδεώδες $I = \langle x-y+2, y+7z \rangle$
Λύση
$G = \{g_1 = 2-y+x, g_2 = 7z+y\}$
Αν πάρω $7g_1 - g_2 = 7(2-y+x) - 7z - y = -8y + 7x \in I \neq \emptyset$
$\Rightarrow -8y + 7x \neq 0$
$-8y + 7x \in I$
$lm(-8y+7x) = y$, όπου $lm(g_1) = lm(g_2) = z \nmid y$
Οπότε G δεν είναι βάση Gröbner.

Ορισμός: Έστω $S \subset K[x_1, \ldots, x_n]$ το ιδεώδες
$Lt(S) = \langle lt(s) \mid s \in S \rangle$ ονομάζεται αρχικό ιδεώδες του S

π.χ. $G = \{g_1 = x-y+2, g_2 = y+7z\}$, τότε (στο $\mathbb{Q}[x,y,z]$ με $x>y>z$)
$Lt(G) = \langle lt(g_1), lt(g_2) \rangle = \langle x, y \rangle$
Αν πάρω το $I = \langle g_1, g_2 \rangle$, τότε
$Lt(I) = \langle lt(f), f \in I \rangle \overset{\text{πριν}}{=\!=} \langle x, y \rangle$

Παρατήρηση: $Lt(S) = \langle lm(s) \mid s \in S \rangle$

Θεώρημα: Έστω I ένα μη μηδενικό ιδεώδες του $K[x_1,\dots,x_n]$ και $G=\{g_1,g_2,\dots,g_t\}$ μη μηδενικά πολυώνυμα του I. Τα επόμενα είναι ισοδύναμα:

i) G είναι βάση Gröbner του I

ii) $f\in I$ αν $f \xrightarrow{G}_+ 0$

iii) $f\in I$ αν $f=\sum h_i g_i$, με $lm(f)=\max\{lm(h_i)lm(g_i)/1\le i\le t\}$

iv) $Lt(G)=Lt(I)$

Απόδειξη

(i) $\Rightarrow$ (ii)

$\Rightarrow$) G είναι βάση Gröbner του I. Έστω $f\in I$

$f \xrightarrow{G}_+ r$, τυπόβιπο. Θέλω ν.δ.ό $r=0$

Από τον αλγόριθμο διαίρεσης: $f=u_1g_1+u_2g_2+\dots+u_tg_t+r \Rightarrow$

$\Rightarrow r=\underbrace{f}_{\in I}-\underbrace{u_1g_1}_{\in I}-\dots-\underbrace{u_tg_t}_{\in I}\in I$

Έστω ότι $r\neq 0$, $r\in I \xrightarrow{G \text{ βάση Gröbner}} (\exists i)\ lm(g_i)/lm(r)$, Άτοπο!

Άρα, $r=0$ αφού καταλήξαμε σε υπόβιπο

$\Leftarrow$) Έστω $f \xrightarrow{G}_+ 0$. Από τον αλγόριθμο διαίρεσης:

$f=\underbrace{u_1g_1}_{\in I}+\dots+\underbrace{u_tg_t}_{\in I}+0\in I \Rightarrow f\in I$

(ii) $\Rightarrow$ (iii)

$\Rightarrow$) $f\in I \xrightarrow{ii)} f \xrightarrow{G}_+ 0 \Rightarrow f=h_1g_1+\dots+h_tg_t+0$, Από αλγόριθμο διαίρεσης:

$lm(f)=\max\{lm(h_1)lm(g_1),lm(h_2)lm(g_2),\dots,lm(h_t)lm(g_t),\underbrace{lm(r)}_{0}\}$

$=\max\{lm(h_1)lm(g_1),\dots,lm(h_t)lm(g_t)\}$

$\Leftarrow$) $f=\underbrace{h_1g_1}_{\in I}+\dots+\underbrace{h_tg_t}_{\in I}\in I \Rightarrow f\in I$

(iii) $\Rightarrow$ (iv)

$G\subset I \Rightarrow Lt(G)=\langle lt(g_1),\dots,lt(g_t)\rangle \subset \langle lt(f)/f\in I\rangle = Lt(I)$

αφού $g_i\in I \Rightarrow lt(g_i)\in Lt(I)$

Άρα, $Lt(G)\subseteq Lt(I)$ ①

Ζωρα Εστω $lt(f) \in Lt(I)$, με $f \in I$
Αν $f=0$, τοτε $lt(f)=0 \in Lt(G)$
Αν $f \neq 0 \Rightarrow lm(f) = lm(h_i)\, lm(g_i)$, για καποιο $1 \leq i \leq t \Rightarrow$
$\Rightarrow lm(f) \in Lt(G)$
Αρα $Lt(I) \subseteq Lt(G)$ (2)
Από (1),(2): $Lt(G) = Lt(I)$
(iv) $\Rightarrow$ (i)
Εστω $f \neq 0 \in I$, τοτε $lm(f) \in Lt(I) = Lt(G) = \langle lm(g_1), \dots, lm(g_t) \rangle$
$\Rightarrow lm(f) = u_1 lm(g_1) + u_2 lm(g_2) + \dots + u_t lm(g_t) \Rightarrow$
$\Rightarrow$ Για καποιο $1 \leq i \leq t$: $lm(g_i) \mid lm(f) \Rightarrow G$ βαση Groebner του I

Ορισμος: Εστω x^a, x^b μονωνυμα του T^n, οπου $a=(a_1,\dots,a_n)$ και $b=(b_1,\dots,b_n)$, το μονωνυμο $x^\gamma = x^{(\gamma_1,\dots,\gamma_n)}$, με $\gamma_i = \max(a_i, b_i)$ ονομαζεται ελαχιστο κοινο πολλαπλασιο των μονωνυμων x^a, x^b και συμβολιζεται με $E.K.\Pi(x^a, x^b)$

Π.χ. $x^{(1,3,0,7)}, x^{(2,2,2,5)} \in T^4$
$x^{(1,3,0,7)} = x_1 x_2^3 x_4^7$, $x^{(2,2,2,5)} = x_1^2 x_2^2 x_3^2 x_4^5$
$E.K.\Pi(x_1 x_2^3 x_4^7, x_1^2 x_2^2 x_3^2 x_4^5) = x_1^2 x_2^3 x_3^2 x_4^7$

Ορισμος: Εστω f, g δυο μη μηδενικα πολυωνυμα του $K[x_1,\dots,x_n]$ και $L = E.K.\Pi(lm(f), lm(g))$. Το πολυωνυμο $S(f,g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$ λεγεται S-πολυωνυμο των f, g.

Π.χ. $f = 3x^2yz - y^3z^3$, $g = xy^2 + z^2 \in K[x,y,z]$,
οπου Κοινωνα χαρακτηριστικης διαφορο του 3, lex $x>y>z$
$lm(f) = x^2yz$, $lm(g) = xy^2$
$L = E.K.\Pi(x^2yz, xy^2) = x^2y^2z$
$S(f,g) = \frac{x^2y^2z}{3x^2yz}(3x^2yz - y^3z^3) - \frac{x^2y^2z}{xy^2}(xy^2 + z^2) = -xz^3 - \frac{1}{3}y^4z^3$

Θεώρημα (Buchberger)

Έστω $G = \{g_1, \dots, g_t\}$ ένα σύνολο μη μηδενικών πολυωνύμων του $K[x_1, \dots, x_n]$. Το G είναι βάση Gröbner του ιδεώδους $I = \langle g_1, \dots, g_t \rangle$ αν $\forall i \neq j$ έχουμε $S(g_i, g_j) \xrightarrow{G}_+ 0$