28-11-16

Πρόταση: Έστω I μη μηδενικό ιδεώδες του $K[x_1,\dots,x_n]$ και $G=\{g_1,\dots,g_t\}\subset I$, όπου $g_i\neq 0$. Το G είναι βάση Gröbner του I $\Longleftrightarrow$ Το υπόλοιπο της διαίρεσης μέσω G οποιουδήποτε $f\in K[x_1,\dots,x_n]$ είναι μοναδικό.

Πρόταση: Αν $G=\{g_1,\dots,g_t\}$ είναι βάση Gröbner του I τότε είναι και βάση του I, δηλαδή $I=\langle g_1,\dots,g_t\rangle$

Απόδειξη

$g_i\in I \Rightarrow \langle g_1,g_2,\dots,g_t\rangle\subset I$

Έστω $f\in I \Rightarrow f=h_1g_1+\dots+h_tg_t\in\langle g_1,\dots,g_t\rangle \Rightarrow$

$I\subset\langle g_1,g_2,\dots,g_t\rangle$

Συνολικά, $I=\langle g_1,g_2,\dots,g_t\rangle$.

Ορισμός: Το $G=\{g_1,\dots,g_t\}$ είναι βάση Gröbner αν είναι βάση Gröbner του $I=\langle g_1,g_2,\dots,g_t\rangle$.

Π.χ. Αν η διάταξη του $\mathbb{Q}[x,y,z,w]$ είναι η λεξικογραφική με $x>y>z>w$, τότε το σύνολο $G=\{g_1=x-y^2w,\ g_2=y-zw,\ g_3=z-w^3,\ g_4=w^3-w\}$ είναι βάση Gröbner.

Λύση

- $S(g_1,g_2)=\dfrac{L}{lt(g_1)}g_1-\dfrac{L}{lt(g_2)}g_2=\dfrac{xy}{x}(x-y^2w)-\dfrac{xy}{y}(y-zw)$

$=-y^3w+xzw=xzw-y^3w\xrightarrow{g_1}$

$$\to \cancel{x}zw - y^3w - \frac{xzw}{x}(\cancel{x} - y^2w) = -y^3w + y^2zw^2 \xrightarrow{g_2}$$

$$\to -y^3\cancel{w} + y^2zw^2 - \frac{-y^3w}{y}(\cancel{y} - zw) = y^2zw^2 - y^2zw^2 = 0.$$

- $$S(g_1,g_3) = \frac{L}{lt(g_1)}g_1 - \frac{L}{lt(g_3)}g_3 = \frac{xz}{x}(\cancel{x} - y^2w) - \frac{xz}{z}(\cancel{z} - w^3)$$

$$= -y^2zw + xw^3 = xw^3 - y^2zw \xrightarrow{g_1}$$

$$\to \cancel{xw^3} - y^2zw - \frac{xw^3}{x}(\cancel{x} - y^2w) = -y^2zw + y^2w^4 \xrightarrow{g_2}$$

$$\to -y^2\cancel{z}w + y^2w^4 - \frac{-y^2zw}{y}(\cancel{y} - zw) = y^2w^4 - yz^2w^2 \to$$

$$\xrightarrow{g_2} y^2\cancel{w^4} - yz^2w^2 - \frac{y^2w^4}{y}(\cancel{y} - zw) = -yz^2w^2 + yzw^5$$

$$\xrightarrow{g_2} -yz^2\cancel{w^2} + yzw^5 - \frac{-yz^2w^2}{y}(\cancel{y} - zw) =$$

$$= yzw^5 - z^3w^3 \xrightarrow{g_2} yz\cancel{w^5} - z^3w^3 - \frac{yzw^5}{y}(\cancel{y} - zw) =$$

$$= -z^3w^3 + z^2w^6 \xrightarrow{g_3} -z^3\cancel{w^3} + z^2w^6 - \frac{-z^3w^3}{z}(\cancel{z} - w^3) =$$

$$= z^2w^6 - z^2w^6 = 0.$$

- $$S(g_1,g_4) = \frac{L}{lt(g_1)}g_1 - \frac{L}{lt(g_4)} \longrightarrow 0$$

- $S(g_2,g_3) \longrightarrow 0$
- $S(g_2,g_4) \longrightarrow 0$
- $S(g_3,g_4) \longrightarrow 0$

Άρα από Buchberger το G είναι βάση Gröbner.

π.χ] Έστω $I = \langle y-x^2, z-x^3 \rangle \subseteq \mathbb{Q}[x,y,z]$ με lex $z>y>x$. Δ.ότι $G=\{g_1 = y-x^2, g_2 = z-x^3\}$ είναι βάση Gröbner

<u>Λύση</u>

$$S(g_1,g_2) = \frac{yz}{y}(y-x^2) - \frac{yz}{z}(z-x^3) = -zx^2+yx^3 \xrightarrow{g_2}$$

$$\xrightarrow{g_2} -zx^2+yx^3 - \frac{-zx^2}{z}(z-x^3) = yx^3 - x^5 \xrightarrow{g_1}$$

$$\to yx^3 - x^5 - \frac{yx^3}{y}(y-x^2) = -x^5+x^5 = 0$$

Άρα, το G είναι βάση Gröbner.

<u>Πρόταση</u>

Έστω $I=\langle g \rangle$, $g \neq 0$ τότε $G=\{g\}$ είναι βάση Gröbner του I.

<u>Απόδειξη</u>

Έστω $f\neq 0$ και $f \in I = \langle g \rangle \Rightarrow f = hg$

$f = lt(f)+\dots$

$h = lt(h)+\dots$

$g = lt(g)+\dots$

$hg = lt(h)\cdot lt(g)+\dots$

Δηλαδή $lt(hg) = lt(h)\cdot lt(g)$

Οπότε $lt(g) \mid lt(g)\cdot lt(h) = lt(f)$

Άρα G βάση Gröbner του I.

π.χ] Έστω $I = \langle y-x^2, z-x^3 \rangle \subseteq \mathbb{Q}[x,y,z]$ με lex $x>y>z$. Βρείτε μια βάση Gröbner για το I

Λύση

$I = \langle g_1 = -x^2+y,\ g_2 = -x^3+z \rangle$.

$$S(g_1,g_2) = \frac{x^3}{-x^2}(\cancel{-x^2}+y) - \frac{x^3}{-x^3}(\cancel{-x^3}+z) =$$

$= -xy + z$ Δεν διαιρείται με κάποιο

Άρα, $-xy+z$ είναι το υπόλοιπο, οπότε δεν είναι βάση Gröbner.

[Παρατήρηση: Το $S(f,g) \in \langle f,g \rangle$]

Εγώ θέλω όμως μια βάση Gröbner

Αν πάρω $g_3 = -xy+z$

Κοιτάζω αν $\{g_1, g_2, g_3\}$ είναι βάση Gröbner του $I = \langle g_1, g_2, g_3 \rangle = \langle g_1, g_2 \rangle$.

$$S(g_1,g_2) = g_3 = -xy+z \xrightarrow{g_3} \cancel{-xy}+z - \frac{-xy}{-xy}(\cancel{-xy}+z) =$$

$= z - z = 0$

$$S(g_1,g_3) = \frac{x^2y}{-x^2}(\cancel{-x^2}+y) - \frac{x^2y}{-xy}(\cancel{-xy}+z) =$$

$= -y^2 + xz = xz - y^2 = g_4$.

Άρα, τώρα θα κοιτάξω για βάση το $\{g_1, g_2, g_3, g_4\}$

Δηλαδή, $I = \langle -x^2+y, -x^3+z, -xy+z, xz-y^2 \rangle$.

$S(g_1,g_2) \to 0$

$S(g_1,g_3) \to 0$

$$S(g_2,g_3) = \frac{x^3y}{-x^3}(\cancel{-x^3}+z) - \frac{x^3y}{-xy}(\cancel{-xy}+z) =$$

$= -yz + x^2z = +x^2z - yz \xrightarrow{g_1} \cancel{x^2}z - yz - \frac{x^2z}{-x^2}(\cancel{-x^2}+y) =$

$= -yz + yz = 0.$

$S(g_1, g_4) = \frac{x^2z}{-x^2}(\cancel{-x^2}+y) - \frac{x^2z}{xz}(\cancel{xz}-y^2) =$

$= -yz + xy^2 = xy^2 - yz \xrightarrow{g_3} \cancel{xy^2} - yz - \frac{xy^2}{-xy}(\cancel{-xy}+z) =$

$= -yz + yz = 0.$

$S(g_2, g_4) = \frac{x^3z}{-x^3}(\cancel{-x^3}+z) - \frac{x^3z}{xz}(\cancel{xz}-y^2) =$

$= -z^2 + x^2y^2 = x^2y^2 - z^2 \xrightarrow{g_B}$ 0

$S(g_3, g_4) = \frac{xyz}{-xy}(\cancel{-xy}+z) - \frac{xyz}{xz}(\cancel{xz}-y^2) = y^3 - z^2 = g_5$

Άρα, ούτε αυτή είναι. Θα ελέγξω:

$I \langle -x^2+y, -x^3+z, -xy+z, xz-y^2, y^3-z^2 \rangle$

Άρα, όλα τα προηγούμενα S πολυώνυμα πάνε στο 0.

Θα ελέγξω $S(g_1,g_5)$, $S(g_2,g_5)$, $S(g_3,g_5)$, $S(g_4,g_5)$.

[Πρόταση: Έστω $f, g \in K[x_1, \dots, x_n]$ με $f \neq 0 \neq g$.
Αν ΜΚΔ$(lm(f), lm(g)) = 1$, τότε $S(f,g) \xrightarrow{\{f,g\}}_{+} 0$]

ΜΚΔ$(lm(g_1), lm(g_5))$ = ΜΚΔ$(x^2, y^3) = 1 \Rightarrow$
$S(g_1, g_5) \longrightarrow 0$

ΜΚΔ$(x^3, y^3) = 1 \Rightarrow S(g_2, g_5) \longrightarrow 0$

και $S(g_4, g_5) \to 0$.
Αρκεί να δω το $S(g_3, g_5)$ που δεν δουλεύει η πρόταση.

$S(g_3, g_5) = \frac{xy^3}{-xy}(-x\cancel{y}+z) - \frac{xy^3}{y^3}(\cancel{y^3}-z^2) =$

$= -y^2z + xz^2 = xz^2 - y^2z \xrightarrow{g_4} \cancel{xz^2} - y^2z - \frac{xz^2}{xz}(\cancel{xz}-y^2) =$

$= -y^2z + y^2z = 0.$

Άρα, το $\{g_1, g_2, g_3, g_4, g_5\}$ είναι βάση Gröbner για το $I = \langle g_1, g_2, g_3, g_4, g_5 \rangle = \langle g_1, g_2 \rangle$.

• Γνωρίζουμε ότι $Lt(I) = Lt(G) =$
$= \langle lm(g_1), lm(g_2), lm(g_3), lm(g_4), lm(g_5) \rangle =$
$= \langle x^2, x^3, xy, xz, y^3 \rangle = \langle x^2, xy, xz, y^3 \rangle$.
Δηλαδή, το $G' = \{g_1, g_3, g_4, g_5\}$ είναι βάση Gröbner του I, αφού $LT(G') = LT(I)$

Αλγόριθμος του Buchberger για τον υπολογισμό μιας βάσης Gröbner

Είσοδος: $F = \{f_1, \dots, f_s\} \subset K[x_1, \dots, x_n]$, $f_i \neq 0$.
Έξοδος: $G = \{g_1, \dots, g_t\}$ μια βάση Gröbner του ιδεώδους $I = \langle f_1, \dots, f_s \rangle$
Αρχή: $G := F$, $\mathcal{G} = \{S(f_i, f_j) \mid f_i \neq f_j \in G\}$

Όσο $\mathcal{G} \neq \emptyset$, Επανάλαβε:
Διάλεξε οποιοδήποτε $S(f, g) \in \mathcal{G}$ και θέσε

$G := G - \{S(f,g)\}$, $S(f,g) \xrightarrow{G}_{+} h$, όπου h ανάγωγο modulo G.
Αν $h \neq 0$ τότε
$G := G \cup \{S(u,h) \mid u \in G\}$
$G := G \cup \{h\}$.

Ακριβώς αυτόν τον αλγόριθμο χρησιμοποιήσαμε στο προηγούμενο παράδειγμα.