23/11/17

Θεώρημα: Αν $G=\{g_1,g_2,\dots,g_t\}$ βάση Gröbner του ιδεώδους I, τότε το υπόλοιπο της διαίρεσης οποιουδήποτε $f\in k(x_1,x_2,\dots,x_n)$ modulo G είναι μοναδικό.

Απόδειξη

Έστω $f \xrightarrow{G}_{+} r_1$, με r_1: ανάγωγο

$f \xrightarrow{G}_{+} r_2$, με r_2: ανάγωγο

Θδο $r_1=r_2$ (είναι μοναδικό).

Έχω ότι:

$f \xrightarrow{G}_{+} r_1 \Rightarrow f = h_1 g_1 + h_2 g_2 + \dots + h_t g_t + r_1$

$f \xrightarrow{G}_{+} r_2 \Rightarrow f = h_1' g_1 + h_2' g_2 + \dots + h_t' g_t + r_2$ $(-)$

$$0 = (h_1-h_1')g_1+\dots+(h_t-h_t')g_t + r_1 - r_2 \Rightarrow$$

$$\Rightarrow r_1 - r_2 = \underbrace{(h_1'-h_1)}_{\in I}g_1+\dots+\underbrace{(h_t'-h_t)}_{\in I}g_t \in I$$

Άρα $r_1-r_2=0$ ή $r_1-r_2\neq 0$, αλλά $r_1-r_2\in I$.

• Αν $r_1-r_2\neq 0 \xrightarrow{\text{ορισμός Gröbner}} (\exists\, 1\le i\le t): lm(g_i) \mid lm(r_1-r_2) \Rightarrow$

$\Rightarrow lm(g_i)$ διαιρεί κάποιον όρο του r_1 ή του r_2.

Όμως αφού r_1, r_2 είναι ανάγωγα καταλήγω σε ΑΤΟΠΟ

• Άρα τελικά $r_1-r_2=0 \Rightarrow r_1=r_2$

Άρα το υπόλοιπο είναι μοναδικό.

Ορισμός: Έστω $X^a, X^b \in T^n$, όπου $a=(a_1,\dots,a_n)$ και $b=(b_1,\dots,b_n)$. Το μονώνυμο X^c, όπου $c=(c_1,\dots,c_n)$ με $c_i=\max\{a_i,b_i\}$ ονομάζεται Ελάχιστο Κοινό Πολλαπλάσιο των X^a και X^b.

Παράδειγμα.

$$\left.\begin{aligned} X^a &= x_1^3 x_2^2 x_3^5 x_4^7 x_7^3 \\ X^b &= x_1^4 x_2 x_4^2 x_5 x_6^4 \end{aligned}\right\} \xrightarrow{\text{Τότε}} X^c = \text{ΕΚΠ}(X^a, X^b) = x_1^4 x_2^2 x_3^5 x_4^2 x_5^7 x_6^4 x_7^3$$

Ορισμός: Έστω f, g δύο μη-μηδενικά πολυώνυμα του $k[x_1,\dots,x_n]$ και $L = \text{ΕΚΠ}(lm(f), lm(g))$. Το πολυώνυμο $S(f,g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$ ονομάζεται S-πολυώνυμο των f και g.

Παράδειγμα

- Έστω ο δακτύλιος $Q(x,\psi,z)$ με διάταξη "$>_{lex}$" με $x>\psi>z$.

Έστω
- $f = x\psi^3 - z^2$ (είναι καλά διατεταγμένα)
- $g = x^2\psi - z^3$

Άρα έχω:

$L = \text{ΕΚΠ}(lm(f), lm(g)) = \text{ΕΚΠ}(x\psi^3, x^2\psi) = x^2\psi^3$

Άρα $S(f,g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} \cdot g = \frac{x^2\psi^3}{x\psi^3}(x\psi^3 - z^2) - \frac{x^2\psi^3}{x^2\psi}(x^2\psi - z^3) =$

$= -xz^2 + \psi^2 z^3$ (το οποίο είναι καλά διατεταγμένο).

Θεώρημα: 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 $I=\langle g_1,\dots,g_n\rangle$) $\overset{\text{αν-ν}}{\Longleftrightarrow}$ $\forall\, i\neq j$ ισχύει ότι: $S(g_i,g_j) \xrightarrow{G}_+ 0$ ∎

Το θεώρημα αυτό λέγεται Θεώρημα Buchberger.

Άσκηση - Παράδειγμα (SOS)

Έστω ο δακτύλιος $\mathbb{Q}(x,\psi,z)$ με διάταξη "$>_{lex}$" με $x>\psi>z>w$.
Έστω $G = \{g_1 = x-\psi^2 w,\ g_2 = \psi - zw,\ g_3 = z - w^2,\ g_4 = w^3 - w\}$.
Ν.δ.ο. η G είναι βάση Gröbner.

Λύση

Α' Μεθοδολογία
Σύμφωνα με το Θεώρημα Buchberger πρέπει να εξετάσω τα πολυώνυμα $S(g_1,g_2)$, $S(g_1,g_3)$, $S(g_1,g_4)$, $S(g_2,g_3)$, $S(g_2,g_4)$, $S(g_3,g_4)$ και ν.δ.ο. αν διαιρεθούν με την βάση G, μου δίνουν υπόλοιπο 0.

Αρχικά διατάσσω τα g_i (εδώ είναι ήδη διατεταγμένα).
Για το $S(g_i,g_j)$ έχω:

- $S(g_1,g_2) = \dfrac{x\psi}{x}(x-\psi^2 w) - \dfrac{x\psi}{\psi}(\psi - zw) = -\psi^3 w + xzw \overset{\text{διάταξη}}{=\!=} xzw - \psi^3 w$

Συνεχίζω με τη διαίρεση και έχω:

$$xzw - \psi^3 w \xrightarrow{g_1} xzw - \psi^3 w - \frac{xzw}{x}(x-\psi^2 w) = -\psi^3 w + \psi^2 z w^2 \xrightarrow{g_2}$$

$$\longrightarrow -\psi^3 w + \psi^2 z w^2 - \frac{-\psi^3 w}{\psi}(\psi - zw) = \psi^2 z w^2 - \psi^2 z w^2 = 0 \ ✓$$

- Συνεχίζω όμοια για τα υπόλοιπα $S(g_i,g_j)$ και πρέπει όλα να βγούν 0.

⋮

Θεώρημα: Αν $ΜΚΔ(lm(f), lm(g)) = 1 \overset{\text{τότε}}{\Longrightarrow} S(f,g) \xrightarrow{\{f,g\}}_{+} 0$.

! Υπενθύμιση: στον ΜΚΔ κοιτάω την μικρότερη δύναμη
Π.χ. $ΜΚΔ(x-\psi^2 w, \psi - zw) = x^0\psi^0 = 1$.

Ασκήσεις - Παραδείγματα.

1) "Πίσω στην προηγούμενη άσκηση"

Έχω αποδείξει ότι:

$S(g_1, g_2) \xrightarrow{G}_+ 0$, αφού ΜΚΔ$(lm(g_1), lm(g_2))$ = ΜΚΔ$(x, y) = 1$.

Όμοια εργάζομαι για όλα τα $S(g_i, g_j)$ σε αυτή την άσκηση

$\boxed{\text{! Άρα μπορώ να γλιτώνω τις πράξεις}}$

2) Έστω ο δακτύλιος $Q(x,y,z,w)$ με διάταξη "Degrevlex" με $x>y$, $z>w$.
Νδο το σύνολο $G = \{g_1 = x^2 - yw,\ g_2 = x - z,\ g_3 = xz - yw\}$ δεν είναι βάση Groebner (του $I = \langle g_1, g_2, g_3 \rangle$).

Λύση

Πρέπει να βρω ένα $S(g_i, g_j)$ τ.ω. $S(g_i, g_j) \xrightarrow{G}_+ r \neq 0$.
Αρχικά διατάσσω τα g_i (εδώ είναι σωστά διατεταγμένα)
Άρα θα εξετάσω τα $S(g_1, g_2)$, $S(g_1, g_3)$, $S(g_2, g_3)$, άρα έχω:

- $S(g_1, g_2) = \frac{x^2}{x^2}(x^2 - yw) - \frac{x^2}{x}(x - z) = -yw + xz \overset{\text{διατάσσω}}{=} xz - yw \longrightarrow$
$\xrightarrow{g_3} xz - yw - \frac{xz}{xz}(xz - yw) = -yw + yw = 0$ ✓

- $S(g_1, g_3) = \frac{x^2 z}{x^2}(x^2 - yw) - \frac{x^2 z}{xz}(xz - yw) = -zyw + xyw \overset{\text{διατάσσω}}{=} xyw - zyw \rightarrow$
$\xrightarrow{g_2} xyw - zyw - \frac{xyw}{x}(x - z) = -zyw + ywz = 0$.

- $S(g_2, g_3) = \frac{xz}{x}(x - z) - \frac{xz}{xz}(xz - yw) = -z^2 + yw \overset{\text{διατάσσω}}{=} -z^2 + yw$, το οποίο είναι ανάγωγο

Άρα $G = \{g_1, g_2, g_3\}$ δεν είναι βάση Groebner.

$\boxed{\text{! Αφού ούτε το } z^2 \text{ ούτε το } yw \text{ δεν διαιρεί τα } x^2, x, xz}$

Άσκηση - Παρατήρηση.

Για την άσκηση (2) θα προσπαθήσω να "λύσω" την G, βάση Gröbner

Λύση

Έχω ότι: $S(g_1,g_2) \xrightarrow{G}_+ 0$

$S(g_1,g_3) \xrightarrow{G}_+ 0$

$S(g_2,g_3) \xrightarrow{G}_+ -z^2+\psi w$

Θέτω ως $g_4 = -z^2+\psi w$ ή $g_4 = z^2-\psi w$ $\boxed{\text{! Είναι το ίδιο.}}$

Αφού $z^2-\psi w \in I$ έχω ότι:

$I = \langle g_1, g_2, g_3 \rangle = \langle g_1, g_2, g_3, g_4 \rangle$.

Άρα $G = \{g_1, g_2, g_3, g_4\}$

Άρα για το $S(g_2,g_3)$ μπορώ να συνεχίσω την διαίρεση με το g_4.

Άρα έχω:

$S(g_2,g_3) \xrightarrow{g_4} -z^2+\psi w - \frac{-z^2}{z^2}(z^2-\psi w) = \psi w - \psi w = 0.$

→ Αφού όμως πρόσθεσα το g_4 πρέπει να ελέγξω τα S-πολυώνυμα που προκύπτουν, δηλ τα $S(g_1,g_4)$, $S(g_2,g_4)$, $S(g_3,g_4)$

Άρα θα έχω:

- $S(g_1,g_4) \xrightarrow{G}_+ 0$ (Αφού ΜΚΔ$(x^2,z^2)=1$)
- $S(g_2,g_4) \xrightarrow{G}_+ 0$ (Αφού ΜΚΔ$(x,z^2)=1$)
- $S(g_3,g_4) \xrightarrow{G}_+ ;$ (Εδώ ΜΚΔ$(xz,z^2)\neq 1$, άρα δουλεύουμε με πράξεις)

Θα έχω:

$\cdot\ S(g_3,g_4) = \frac{xz^2}{xz}(xz-\psi w) - \frac{xz^2}{z^2}(z^2-\psi w) = -\psi zw + x\psi w \overset{\text{διάταξη}}{=}$

$= x\psi w - \psi zw \xrightarrow{g_2} x\psi w - \psi zw - \frac{x\psi w}{x}(x-z) = -\psi zw + \psi zw = 0.$

Άρα τελικά την $G = \{g_1, g_2, g_3, g_4\}$ η οποία είναι βάση Gröbner.

(! Αν κάποιο από τα νέα S-πολυώνυμα δεν έκανε 0 θα έκανα την ίδια διαδικασία)

Θεώρημα: Αν $g_1 = x^{a_1}, g_2 = x^{a_2}, \dots, g_t = x^{a_t}$ είναι t μονώνυμα του $K[x_1, \dots, x_n]$ τότε το σύνολο $G = \{g_1, g_2, \dots, g_t\}$ είναι βάση Gröbner του $I = \langle g_1, g_2, \dots, g_t \rangle$. Η διάταξη δεν μας ενδιαφέρει.

Απόδειξη.

Έχω ότι για το $S(x^{a_i}, x^{a_j})$ ισχύει: $L = \text{ΕΚΠ}(x^{a_i}, x^{a_j})$.

Άρα $S(x^{a_i}, x^{a_j}) = \dfrac{L}{x^{a_i}} x^{a_i} - \dfrac{L}{x^{a_j}} x^{a_j} = L - L = 0$

Άρα $\{g_1, g_2, \dots, g_t\}$ είναι βάση Gröbner.

Ερώτημα: Αν $I = \langle g \rangle$, με $g \neq 0$ τότε το g είναι βάση Gröbner του I;

Απάντηση: ΝΑΙ.

- Με το Θεώρημα Buchberger βγαίνει άμεσα.
- Με ορισμό:

Έστω $f \in I = \langle g \rangle \Rightarrow f = h \cdot g = (lt(h) + \overbrace{\dots}^{x}) \cdot (lt(g) + \overbrace{\dots}^{\psi})$.

Έχω ότι: $\left.\begin{matrix} lm(h) \geq x \\ lm(g) \geq \psi \end{matrix}\right\} \Rightarrow lm(h) \cdot lm(g) \geq \psi \cdot x$.

Άρα για το f έχω ότι:

$lt(f) = lt(h) \cdot lt(g) \Rightarrow lm(g) \mid lm(f) \Rightarrow \{g\}$: βάση Gröbner

• **Αλγόριθμος του Buchberger**

Είσοδος: $F = \{f_1, f_2, \dots, f_s\} \subseteq k(x_1, \dots, x_n)$ με $f_i \neq 0$.
Έξοδος: $G = \{g_1, g_2, \dots, g_t\}$ μια βάση Gröbner του $I = \langle f_1, f_2, \dots, f_s \rangle$.

Αρχή
$G = F$
$\mathcal{G} = \{ S(f_i, f_j) \mid f_i \neq f_j$ με $f_i, f_j \in G \}$
Όσο $\mathcal{G} \neq \emptyset$ επανέλαβε
  Διαλέξτε οποιοδήποτε $S(f,g) \in \mathcal{G}$ και θέσε $\mathcal{G} = \mathcal{G} - \{S(f,g)\}$
  $S(f,g) \xrightarrow{G} h$, όπου h ανάγωγο ως προς G.
  Αν $h \neq 0$ τότε
    $\mathcal{G} = \mathcal{G} \cup \{ S(u,h) \mid u \in G \}$
    $G = G \cup \{h\}$
  Τέλος
Τέλος

Άσκηση - Παράδειγμα

Έστω $\mathbb{Q}(x, \psi, z)$ με διάταξη "$>_{deglex}$" με $x > \psi > z$.
Έστω $I = \langle x^2\psi + z, xz + \psi \rangle$.
Να βρω την βάση Gröbner του I.

Λύση

Αρχικά διατάσσω τα g_1, g_2 (ήδη είναι καλά)
Σύμφωνα με τον αλγόριθμο Buchberger, σχηματικά θα έχω:

G	$g_1 = x^2\psi + z$, $g_2 = xz + \psi$, $g_3 = -x\psi^2 + z^2$, $g_4 = \psi + z$	$\mathcal{G}$	$S(g_1, g_2)$, $S(g_1, g_3)$, $S(g_2, g_3)$, $S(g_1, g_4)$, $S(g_2, g_4)$, $S(g_3, g_4)$

Scanned by CamScanner

Έχω ότι:

• $S(g_1,g_2) = \frac{x^2\psi z}{x^2\psi}(x^2\psi+z) - \frac{x^2\psi z}{xz}(xz+\psi) = z^2 - x\psi^2 \xrightarrow{\text{διαίρεση}}$

$= -x\psi^2+z^2$, το οποίο είναι ανάγωγο, δηλ. $\neq 0$.

Άρα το προσθέτω στο G, σαν g_3 και άρα στο G προκύπτουν τα $S(g_1,g_3)$, $S(g_2,g_3)$

Άρα έχω:

• $S(g_1,g_3) = \frac{x^2\psi^2}{x^2\psi}(x^2\psi+z) - \frac{x^2\psi^2}{-x\psi^2}(-x\psi^2+z^2) = \psi z + xz^2 \xrightarrow{\text{διαίρεση}} xz^2+\psi z$

Το οποίο μπορώ να διαιρέσω με το g_2, άρα:

$xz^2+\psi z \xrightarrow{g_2} xz^2+\psi z - \frac{xz^2}{xz}(xz+\psi) = \psi z - \psi z = 0.$

Άρα δεν προσθέτω τίποτα καινούριο.

Άρα θα εξετάσω το επόμενο, δηλ. το $S(g_2,g_3)$

Άρα έχω:

$S(g_2,g_3) = \frac{x\psi^2 z}{xz}(xz+\psi) - \frac{x\psi^2 z}{-x\psi^2}(-x\psi^2+z^2) = \psi^3+z^3 \xrightarrow{\text{διαίρεση}} \psi^3+z^3.$ το οποίο είναι ανάγωγο, δηλ. $\neq$

Άρα το προσθέτω στο G σαν g_4 και άρα στο G προκύπτουν τα $S(g_1,g_4)$, $S(g_2,g_4)$, $S(g_3,g_4)$

Άρα έχω:

• $S(g_2,g_4) \xrightarrow{G} 0$ (Αφού ΜΚΔ$(xz,\psi^3)=1$).

• $S(g_1,g_4) = \frac{x^2\psi^3}{x^2\psi}(x^2\psi+z) - \frac{x^2\psi^3}{\psi^3}(\psi^3+z^3) = \psi^2 z - x^2z^3 \xrightarrow{\text{διαίρεση}} -x^2z^3+\psi^2 z$

Το οποίο μπορώ να διαιρέσω με το g_2 άρα:

$-x^2z^3+\psi^2 z \xrightarrow{g_2} -x^2z^3+\psi^2 z - \frac{-x^2z^3}{xz}(xz+\psi) = \psi^2 z + xz^2\psi \xrightarrow{\text{διαίρεση}} xz^2\psi+\psi^2 z$

$\xrightarrow{g_2} xz^2\psi+\psi^2 z - \frac{xz^2\psi}{xz}(xz+\psi) = \psi^2 z - \psi^2 z = 0.$

Άρα δεν προσθέτω τίποτα καινούριο

Άρα θα εξετάσω το επόμενο, δηλ. το $S(g_3,g_4)$.

Άρα έχω:

- $S(g_3, g_4) = \frac{x\psi^3}{-x\psi^2}(-x\psi^2 + z^2) - \frac{x\psi^3}{\psi^3}(\psi^3 + z^3) = -\psi z^2 - xz^3 \overset{\text{διάτ.}}{=} -xz^3 - \psi z^2$.

Το οποίο μπορώ να διαιρέσω με το g_2, άρα.

$-xz^3 - \psi z^2 \xrightarrow{g_2} -xz^3 - \psi z^2 - \frac{-xz^3}{xz}(xz + \psi) = -\psi z^2 + z^2\psi = 0$.

Άρα δεν προσθέτω τίποτα καινούριο

Άρα τελείωσα τον έλεγχο.

Άρα $G = \{g_1, g_2, g_3, g_4\}$ είναι βάση Gröbner του I