<u>16/11/17</u>

Παραδείγματα πάνω στις Βάσεις Gröbner

1) Έστω ο δακτύλιος $Q[x,\psi]$ με διάταξη "lex" με $\psi > x$. Έστω ιδεώδες $I = \langle \psi x - x, \psi^2 - x \rangle$.
Είναι η $F = \{f_1 = \psi x - x,\ f_2 = \psi^2 - x\}$ βάση Gröbner του I.

Λύση

Έστω $f = \psi^2 x - x$ $\boxed{\text{! Την } f \text{ την "μαντεύω"}}$
Θα κάνω την διαίρεση $f \xrightarrow{F}_+ \boxed{r}$ → και ψάχνω το υπόλοιπο.
- Έστω επιλέγω το f_1 για την διαίρεση $\boxed{\text{! Εδώ παρόμοια και το } f_2}$
Άρα θα έχω:

$$f \xrightarrow{f_1} \psi^2 x - x - \frac{\psi^2 x}{\psi x}(\psi x - x) = \psi x - x \xrightarrow{f_1} \psi x - x - \frac{\psi x}{\psi x}(\psi x - x) = 0$$

Άρα $f = (\psi + 1)\underbrace{f_1}_{\in I} + 0 \xrightarrow{\text{άρα}} f \in I$ που το ξέρω ήδη.

- Έστω επιλέγω το f_2 για την διαίρεση.
Άρα θα έχω:

$$f \xrightarrow{f_2} \psi^2 x - x - \frac{\psi^2 x}{\psi^2}(\psi^2 - x) = x^2 - x$$

, το οποίο είναι ανάγωγο modulo F.

$\boxed{\text{! Άρα δεν μπορώ να συνεχίσω την διαίρεση.}}$

Άρα $\underbrace{f}_{\in I} = x \cdot \underbrace{f_2}_{\in I} + x^2 - x \xrightarrow{\text{άρα}} x^2 - x \in I$

! Το υπόλοιπο της διαίρεσης δεν

Έχω ότι $\mathrm{lm}(f_1) = \psi x \not| x^2$ και $\mathrm{lm}(f_2) = \psi^2 \not| x^2$ $\Big\}$ Άρα $F = \{f_1, f_2\}$ δεν είναι βάση Gröbner του I

21) Έστω ο δακτύλιος $\mathbb{Q}(x,\psi,z)$ με διάταξη "$>_{lex}$" με $z>\psi>x$.
Έστω $G = \{g_1 = z+x,\ g_2 = \psi - x\}$ και ιδεώδες $I = \langle g_1, g_2\rangle = \langle z+x, \psi - x\rangle$.
Νδο η G είναι βάση Gröbner του I.

<u>Λύση</u>

Έστω ότι $G = \{g_1, g_2\}$ δεν είναι βάση Gröbner του I $\Rightarrow$
$\Rightarrow \exists f \in \mathbb{Q}(x,\psi,z),\ f \in I,\ f \neq 0$ τέτοιο $\left.\begin{array}{l} \mathrm{lm}(g_1) = z \not| \mathrm{lm}(f) \\ \text{και } \mathrm{lm}(g_2) = \psi \not| \mathrm{lm}(f) \end{array}\right\}$ (1)

Προφανώς το $\mathrm{lm}(f)$ θα είναι της μορφής: $\mathrm{lm}(f) = x^{\alpha}\psi^{b}z^{\gamma}$, όπου από (1) $\Rightarrow$
$\Rightarrow \left.\begin{array}{l} z \not| x^{\alpha}\psi^{b}z^{\gamma} \Rightarrow \gamma = 0 \\ \text{και } \psi \not| x^{\alpha}\psi^{b}z^{\gamma} \Rightarrow b = 0 \end{array}\right\} \xRightarrow{\text{άρα}} \mathrm{lm}(f) = x^{\alpha}$

Για το
$f = c_{\alpha}x^{\alpha} + \dots$ Από τον ορισμό της διάταξης "$>_{lex}$" με $z>\psi>x$ δεν μπορεί να έχω μετά το $c_{\alpha}x^{\alpha}$ όρους με z και ψ αφού είναι μεγαλύτεροι και άρα θα έπρεπε να ήταν διατεταγμένοι πιο πριν.

Άρα τελικά έχω ότι:
$f = c_{\alpha}x^{\alpha} + c_{\alpha-1}x^{\alpha-1} + \dots + c_1 x + c_0 \in \mathbb{Q}(x)$ (2)
Εφόσον $f \in I = \langle z+x, \psi-x\rangle \Rightarrow f$ είναι συνδυασμός των $z+x, \psi-x$
Άρα θα έχω:
$f = h_1(x,\psi,z)\cdot(z+x) + h_2(x,\psi,z)\cdot(\psi-x)$. (3)
Από τις (2),(3) έχω:
$c_{\alpha}x^{\alpha} + c_{\alpha-1}x^{\alpha-1} + \dots + c_1 x + c_0 = h_1(x,\psi,z)(z+x) + h_2(x,\psi,z)(\psi - x)$
Όμως για $z = -x$ και $\psi = x$ θα έχω:
$c_{\alpha}x^{\alpha} + c_{\alpha-1}x^{\alpha-1} + \dots + c_1 x + c_0 = 0 + 0 = 0$. Άτοπο, αφού $f \neq 0$ (υπόθεση).
Άρα $G = \{g_1, g_2\}$ είναι βάση Gröbner του I

3 ⚠ Παρατήρηση.

Αν αλλάξω την διάταξη στο παράδειγμα 2 και πάρω διάταξη: "$>_{lex}$" με $x>\psi>z$ θα έχω ότι η $G=\{g_1,g_2\}$ δεν είναι βάση Gröbner του I.

Απόδειξη

1 Αν διατάξω τα g_1, g_2 θα έχω $g_1 = x+z$

$g_2 = x+\psi$

Αν πάρω $g_1+g_2\in I$, με $g_1+g_2 = x+z-x+\psi = \psi+z \Rightarrow \psi+z\in I$.

Όμως $\mathrm{lm}(g_1)=\mathrm{lm}(g_2)=x$ X $\mathrm{lm}(\psi+z)=\psi$.

Άρα δεν είναι βάση Gröbner

• Πόρισμα: Για να απαντηθεί αν μια βάση είναι βάση Gröbner ενός ιδεώδους έχει σημασία η διάταξη.

Ορισμός: Έστω $S\subset K(x_1,x_2,\dots,x_n)$ με "$>$" μονωνυμική διάταξη. Το ιδεώδες $Lt(S)=\langle \mathrm{lm}(s)\mid s\in S\rangle$ ονομάζεται αρχικό ιδεώδες του S.

⚠ Παρατήρηση

• Έστω $G=\{g_1,g_2,\dots,g_t\}$, τότε:

$Lt(G)=\langle \mathrm{lm}(g_1),\mathrm{lm}(g_2),\dots,\mathrm{lm}(g_t)\rangle$ (Το αρχικό ιδεώδες του G)

• Έστω $I=\langle f_1,f_2,\dots\rangle$ ιδεώδες του $K(x_1,x_2,\dots,x_n)$, τότε.

$Lt(I)=\langle \mathrm{lm}(f_i)\mid f_i\in I\rangle$ (Το αρχικό ιδεώδες του I).

Scanned by CamScanner

Παραδείγματα

1) Έστω ο δακτύλιος $\mathbb{Q}[x,\psi,z]$ με διάταξη: "$>_{lex}$" με $z>\psi>x$.
Έστω $G=\{g_1=z+x,\ g_2=\psi-x\}$ και $I=\langle z+x, \psi-x\rangle$
Τότε έχω ότι
- $Lt(G)=\langle lm(g_1), lm(g_2)\rangle=\langle z,\psi\rangle$
- $Lt(I)=\langle z,\psi\rangle$

2) Έστω $\mathbb{Q}[x,\psi,z]$ με διάταξη "$>_{lex}$" με $x>\psi>z$
Έστω $G=\{g_1=x+z,\ g_2=-x+\psi\}$ και $I=\langle x+z, -x+\psi\rangle$.

! Δες ίδια με 1 αλλά με διαφορετική διάταξη.

Τότε έχω ότι
- $Lt(G)=\langle x,x\rangle=\langle x\rangle$
- $Lt(I)=\langle x,\psi\rangle$

- Μονωνυμικά ιδεώδη

Ορισμός: Ένα ιδεώδες $I\subset k[x_1,x_2,\dots,x_n]$ λέγεται μονωνυμικό αν υπάρχει $E\subset T^n$ τ.ω.: $I=\langle m \mid m\in E\rangle$.

Παράδειγμα - Άσκηση
Έστω $I=\langle x^2\psi,\ \psi^2z,\ z^2x\rangle$ είναι μονωνυμικό ιδεώδες του $k[x,\psi,z]$.
Το ιδεώδες $J=\langle 2x^2\psi+\psi^2z+z^2x,\ x^2\psi+2\psi^2z+z^2x,\ x^2\psi+\psi^2z+2z^2x\rangle$ του $k[x,\psi,z]$ είναι μονωνυμικό;

Λύση

Για το J πρέπει να βρω κάποια μονώνυμα που το παράγουν.
Άρα ένας τρόπος είναι αρχικά να προσθέσω τα J_i
Άρα θα έχω:

$2x^2\psi + \psi^2 z + z^2 x \in J$ (1)

$x^2\psi + 2\psi^2 z + z^2 x \in J$ (2)

$x^2\psi + \psi^2 z + 2z^2 x \in J$ (+) (3)

$4x^2\psi + 4\psi^2 z + 4z^2 x \in J \xrightarrow{/4} x^2\psi + \psi^2 z + z^2 x \in J$ (4)

! Δεν μπορώ πάντα να διαιρώ

Άρα μπορώ να πάρω:

$$\left.\begin{array}{l} (1)-(4) \to 2x^2\psi + \psi^2 z + z^2 x - (x^2\psi + \psi^2 z + z^2 x) = x^2\psi \in J \\ (2)-(4) \to x^2\psi + 2\psi^2 z + z^2 x - (x^2\psi + \psi^2 z + z^2 x) = \psi^2 z \in J \\ (3)-(4) \to x^2\psi + \psi^2 z + 2z^2 x - (x^2\psi + \psi^2 z + z^2 x) = z^2 x \in J \end{array}\right\} (i)$$

Άρα θέλω $\langle x^2\psi, \psi^2 z, z^2 x\rangle = J$.

Άρα αρκεί νδο $\langle x^2\psi, \psi^2 z, z^2 x\rangle \subseteq$ και $\supseteq J$

· Από το (i) έχω ότι $\langle x^2\psi, \psi^2 z, z^2 x\rangle \subset J$.

· Έχω ότι:
$$\left.\begin{array}{l} \cdot\ 2x^2\psi + \psi^2 z + z^2 x \in \langle x^2\psi, \psi^2 z, z^2 x\rangle \\ \cdot\ x^2\psi + 2\psi^2 z + z^2 x \in \langle x^2\psi, \psi^2 z, z^2 x\rangle \\ \cdot\ x^2\psi + \psi^2 z + 2z^2 x \in \langle x^2\psi, \psi^2 z, z^2 x\rangle \end{array}\right\} \to J \subset \langle x^2\psi, \psi^2 z, z^2 x\rangle$$

Άρα τελικά:

$\langle x^2\psi, \psi^2 z, z^2 x\rangle = J \to J$ είναι μονωνυμικό ιδεώδες

Ορισμός: Λέμε ότι ένα σώμα έχει χαρακτηριστική λ, όταν το λ είναι ο μικρότερος φυσικός αριθμός τ.ω: $\lambda a = \underbrace{a + a + \ldots + a}_{\lambda \text{ φορές}} = 0$

Όταν δεν υπάρχει τέτοιος φυσικός αριθμός λέμε ότι η χαρακτηριστική του σώματος είναι 0.

Παραδείγματα:

- Τα σώματα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ έχουν χαρακτηριστική 0.
- Το $\mathbb{Z}_2$ έχει χαρακτηριστική 2.
- Το $\mathbb{Z}_p$ έχει χαρακτηριστική p, όπου p πρώτος.
- ! Το $\mathbb{Z}_4$ δεν είναι σώμα, άρα δεν μιλάμε για χαρακτηριστική.

Παράδειγμα – Άσκηση

Ν.δ.ο. σε χαρακτηριστική 2, το ιδεώδες J δεν είναι μονωνυμικό, όπου $J=\langle 2x^2y+y^2z+z^2x,\ x^2y+2y^2z+z^2x,\ x^2y+y^2z+2z^2x\rangle$.

Λύση.

Επειδή $char=2 \longrightarrow \cdot\ 2x^2y=0$

$\cdot\ 2y^2z=0$

$\cdot\ 2z^2x=0$.

Άρα $J=\langle y^2z+z^2x,\ x^2y+z^2x,\ x^2y+y^2z\rangle$.

Ισχυρίζομαι ότι το ιδεώδες J δεν περιέχει κανένα μονώνυμο και θα το αποδείξω.

Άρα έχω:

Έστω ότι το J περιέχει κάποιο μονώνυμο, το οποίο είναι της μορφής:

$x^a y^b z^\gamma = h_1(x,y,z)(y^2z+z^2x)+h_2(x,y,z)(x^2y+z^2x)+h_3(x,y,z)(x^2y+y^2z)$

Αν πάρω ως $y=x \wedge z=x$ θα έχω:

$x^a\cdot x^b\cdot x^\gamma = 0+0+0 \Rightarrow x^{a+b+\gamma}=0$. ΑΤΟΠΟ

Άρα το J δεν είναι μονωνυμικό.

Πρόταση: Έστω $M\in T^n$ και I ένα μονωνυμικό ιδεώδες του $K(x_1,\dots,x_n)$, δηλ $I=\langle m \mid m\in\Sigma(T^n)\rangle$. Τότε $M\in I \iff \exists\, m\in\Sigma$ τ.ώ. $m|M$

Απόδειξη

$(\rightarrow)$ Έχω ότι $M\in I=\langle m\mid m\in\Sigma(T^n)\rangle$

Άρα $M=h_1m_1+h_2m_2+\dots+h_tm_t$, με $h_i\in K(x_1,\dots,x_n) \wedge m_i\in\Sigma$

Το M δηλαδή θα πρέπει να εμφανίζεται μέσα στο "$h_1m_1+h_2m_2+\dots+h_tm_t$".

Έστω δηλαδή εμφανίζεται στο $h_im_i \longrightarrow M$ είναι πολλαπλάσιο του m_i.

Άρα $m|M$.

$(\leftarrow)$ Έχω ότι $m|M$

Άρα $m|M \Rightarrow M=m'\cdot \underbrace{m}_{\in I} \Rightarrow M\in I$.

Πρόταση: Έστω $f = c_1 X^{a_1} + c_2 X^{a_2} + \dots + c_t X^{a_t}$, με $c_i \neq 0 \wedge X^{a_i} \in T^n$.
Έστω I ένα μονωνυμικό ιδεώδες του $k[x_1,\dots,x_n]$, δηλ. $I = \langle m \mid m \in E \subset T^n \rangle$.
Τότε $f \in I \overset{\text{ανν}}{\iff} X^{a_i} \in I,\ \forall\, 1 \le i \le t$

Απόδειξη.

($\rightarrow$) Έχω ότι $f \in I$
Άρα $c_1 X^{a_1} + c_2 X^{a_2} + \dots + c_i X^{a_i} + \dots + c_t X^{a_t} = h_1 m_1 + h_2 m_2 + \dots + h_i m_i + h_s m_s$.
με $h_i \in k[x_1,\dots,x_n]$ και $m_i \in E$.
Το $c_i X^{a_i}$ εμφανίζεται στο αριστερό μέρος της εξίσωσης, άρα θα εμφανίζεται και στο δεξιό.
Αν εμφανίζεται στο $h_i m_i \Rightarrow c_i X^{a_i}$ είναι πολλαπλάσιο του m_i
και επειδή $m_i \in I$ $\Big\} \Rightarrow c_i X^{a_i} \in I$

($\leftarrow$) Έχω $X^{a_i} \in I$, $\forall\, 1 \le i \le t$
Το f είναι της μορφής
$f = \underbrace{c_1 X^{a_1}}_{\in I} + \underbrace{c_2 X^{a_2}}_{\in I} + \dots + \underbrace{c_t X^{a_t}}_{\in I} \Rightarrow f \in I.$

Παράδειγμα - Άσκηση.

Έστω δακτύλιος $\mathbb{Q}[x,y,z]$ με $I = \langle x^2 y,\ y^2 z,\ z^2 x \rangle$.
Έστω $f = 3x^3 y + 7x^2 y^2 z^2 + 5z^3 x$
$g = -11x^2 y + 8x^2 y^2 z^5 + 3z^2$
Ποιο από τα f, g ανήκει στο ιδεώδες I;

Λύση

Για το f έχω:
$f = \underbrace{3x^3 y}_{\text{πολλαπλάσιο ενός όρου του } I} + \underbrace{7x^2 y^2 z^2}_{\text{όμοια}} + \underbrace{5z^3 x}_{\text{όμοια}} \Rightarrow f \in I.$

· Για το g έχω:

$g = -11x^2\psi + 8x^2\psi^2 z^5 + 3z^2 \Rightarrow g \notin I$

Δεν είναι πολλαπλάσιο
κάποιου όρου του I

<u>Θεώρημα</u>: Έστω I μονωνυμικό ιδεώδες του $k[x_1, \dots, x_n]$, τότε υπάρχουν $m_1, m_2, \dots, m_t$ μονώνυμα του I τ.ω: $I = \langle m_1, m_2, \dots, m_t \rangle$

Δηλ. πεπερασμένου πλήθους

<u>Απόδειξη</u>

Έχω ότι $I = \langle x^a \mid a \in \mathbb{Z}^n \rangle \subseteq k[x_1, \dots, x_n]$: Ιδιότητα της Noether

Άρα $I = \langle f_1, f_2, \dots, f_s \rangle$, όπου $f_1 = c_{11}x^{a_{11}} + c_{12}x^{a_{12}} + \dots + c_{1n_1}x^{a_{1n_1}}$

$\vdots$

$f_s = c_{s1}x^{a_{s1}} + c_{s2}x^{a_{s2}} + \dots + c_{sn_s}x^{a_{sn_s}}$

Ισχυρίζομαι ότι $I = \langle f_1, f_2, \dots, f_s \rangle = \langle x^{a_{11}}, x^{a_{12}}, \dots, x^{a_{1n_1}}, x^{a_{21}}, \dots, x^{a_{s1}}, \dots, x^{a_{sn_s}} \rangle$

Για να το αποδείξω έχω:

$$\left.\begin{array}{l} f_1 = c_{11}x^{a_{11}} + \dots + c_{1n_1}x^{a_{1n_1}} \Rightarrow f_1 \in \langle x^{a_{11}}, x^{a_{12}}, \dots \rangle \\ \vdots \\ f_s = c_{s1}x^{a_{s1}} + c_{s2}x^{a_{s2}} + \dots + c_{sn_s}x^{a_{sn_s}} \Rightarrow f_s \in \langle x^{a_{11}}, x^{a_{12}}, \dots \rangle \end{array}\right\} \Rightarrow I \subseteq \langle x^{a_{11}}, x^{a_{12}}, \dots \rangle \quad (1)$$

Επίσης έχω ότι:

$$\left.\begin{array}{l} f_1 \in I \Rightarrow x^{a_{11}} \in I,\ x^{a_{12}} \in I, \dots, x^{a_{1n}} \in I \\ \vdots \\ f_s \in I \Rightarrow x^{a_{s1}} \in I,\ x^{a_{s2}} \in I, \dots, x^{a_{sn_s}} \in I \end{array}\right\} \Rightarrow \langle x^{a_{11}}, x^{a_{12}}, \dots \rangle \subseteq I \quad (2)$$

Άρα $(1),(2) \Rightarrow I = \langle x^{a_{11}}, x^{a_{12}}, \dots, x^{a_{sn_s}} \rangle$; δηλ. έχει πεπερασμένο πλήθος

Scanned by CamScanner

Θεώρημα: Έστω ένα μη-μηδενικό ιδεώδες του $k(x_1,\dots,x_n)$ και $G=\{g_1,\dots,g_t\}\subset I$.
Το G είναι βάση Gröbner του $I \overset{\text{αν-ν}}{\Longleftrightarrow} Lt(I)=Lt(G)$

Απόδειξη

$(\rightarrow)$: Έχω ότι G είναι βάση Gröbner του I.
Θέλω $Lt(I) \overset{?}{=} Lt(G)$
Προφανώς $G \subset I \Rightarrow Lt(G) \subseteq Lt(I)$. (1)
Έστω $f \in I$, $f \neq 0 \Rightarrow lm(f) \in Lt(I)$
Έχω ότι:
G: βάση Gröbner του $I \xrightarrow{\text{ορισμός}} \exists\, g_i$ τ.ω.: $lm(g_i) \mid lm(f) \Rightarrow lm(f) \in Lt(G)$.
Άρα $Lt(I) \subseteq Lt(G)$ (2)
Άρα (1),(2) $\Rightarrow Lt(I)=Lt(G)$.

$(\leftarrow)$: Έχω ότι $Lt(I)=Lt(G)=\langle lm(g_1), lm(g_2),\dots, lm(g_t)\rangle$
Έστω $f\in I$, $f\neq 0 \Rightarrow lm(f)\in Lt(I) \Rightarrow lm(f)\in Lt(G)=\langle lm(g_1),\dots,lm(g_t)\rangle$
$\Rightarrow \exists\, g_i$ τ.ω.: $lm(g_i) \mid lm(f)$.
Άρα G είναι βάση Gröbner του I