Έστω $S = \mathbb{K}[x_1, \dots, x_n]$, $\mathbb{K}$ σώμα 18/11/19

Ορισμός: Ένα ιδεώδες $I \subseteq S$ καλείται μονωνυμικό αν παράγεται από μονώνυμα

π.χ. $I = \langle x^2, xy \rangle$ μονωνυμικό

$I = \langle x+y, xy \rangle$ όχι μονωνυμικό.

Λήμμα: Έστω $I = \langle x^{a_1}, x^{a_2}, \dots, x^{a_n} \rangle \subseteq S$ μονωνυμικό
Τότε, $x^{\beta} \in I$ αν-ν $\exists i \in \{1, \dots, n\}$ $x^{a_i} \mid x^{\beta}$

Θεώρημα: Έστω $I = \langle x^{a_1}, \dots, x^{a_n} \rangle \subseteq S$ και $f \in S$, f πολυώνυμο.
Τα παρακάτω είναι ισοδύναμα
i) $f \in I$
$\Updownarrow$
ii) κάθε όρος του f (κάθε μονώνυμο) ανήκει στο I
$\Updownarrow$
iii) το f γράφεται ως γραμ. συνδυασμός των μονωνύμων του I.

Λήμμα Dickson: Έστω I μη κενό μονωνυμικό ιδεώδες. Αυτό είναι πεπερασμένα παραγόμενο
($I = \langle x^a, a \in \mathbb{N}^n \rangle$ υπάρχει πεπ. $\{a_1, \dots, a_n\}$: $I = \langle x^{a_1}, \dots, x^{a_n} \rangle$)

Πόρισμα: Κάθε μονωνυμικό ιδεώδες έχει μοναδικό ελαχιστοτικό σύνολο γεννητόρων. (συμβ M_I)

Ελαχιστοτικό καλείται το σύνολο γεννητόρων όταν δεν υπάρχει γνήσιο υποσύνολο αυτού που να παράγει το ιδεώδες

π.χ. $I = \langle x^2, y^2, x^2 y^2 \rangle$ όχι ελαχιστοτικό.
$I = \langle x^2, y^2 \rangle$ ελαχιστοτικό

Απόδειξη: Έστω $I \subseteq S$ μονωνυμικό. (η ύπαρξη έπεται από το Λήμμα Dickson)

Μοναδικότητα: Έστω $I = \langle x^{a_1}, \dots, x^{a_n} \rangle$ και έστω $I = \langle x^{\beta_1}, \dots, x^{\beta_k} \rangle$ ελαχ. σύνολα γεννητόρων

Θδο $\langle x^{a_1}, \dots, x^{a_n} \rangle \subseteq \langle x^{\beta_1}, \dots, x^{\beta_k} \rangle$

$x^{a_i} \in I$ άρα $\exists$ δείκτης j : $x^{\beta_j} \mid x^{a_i}$ } $x^{a_n} \mid x^{a_i}$ $\overset{\text{ελαχ}}{\Longrightarrow}$ $\boxed{n=i}$.

$x^{\beta_j} \in I$ άρα $\exists$ δείκτης n : $x^{a_n} \mid x^{\beta_j}$ } $x^{\beta_j} \mid x^{a_i}$ και $x^{a_i} \mid x^{\beta_j}$

$\Downarrow$

$\boxed{x^{a_i} = x^{\beta_j}}$

Αντίστοιχα και το αντίστροφο.

Πρόταση ① Έστω $I = \langle x^{a_1}, \dots, x^{a_n} \rangle \subseteq S$ και $J = \langle x^{\beta_1}, \dots, x^{\beta_k} \rangle \subseteq S$

Τότε: i) $I + J = \langle x^{a_1}, \dots, x^{a_n}, x^{\beta_1}, \dots, x^{\beta_k} \rangle$

ii) $I \cdot J = \langle x^{a_i} x^{\beta_j}, \ i = \{1, \dots, n\} \ j = \{1, \dots, k\} \rangle$

② Έστω $I, J \subseteq S$ ιδεώδη μονωνυμικά με $M_I = \langle x^{a_1}, \dots, x^{a_n} \rangle$, $M_J = \langle x^{\beta_1}, \dots, x^{\beta_k} \rangle$

Τότε: i) $I \cap J = \langle \text{ΕΚΠ}(x^{a_i}, x^{\beta_j}), \ i = 1, \dots, n$ και $j = 1, \dots, k \rangle$

ii) $I : J = \bigcap_{j=1}^{k} I : x^{\beta_j}$ όπου $I : x^{\beta_j} = \left\langle \dfrac{x^{a_i}}{\text{μκδ}(x^{a_i}, x^{\beta_j})}, \ i = 1, \dots, n \right\rangle$

iii) $\sqrt{I} = \langle \sqrt{x^{a_i}}, \ i = 1, \dots, n \rangle$, όπου $\sqrt{x^{a_i}} = \prod_{k \in \{1, \dots, n\}}^{a_k \neq 0} x_k$

ΠΧ $I = \langle x_1^2 x_2^2 x_4, x_1 x_2 x_3, x_2^2 \rangle$, $J = \langle x_1^2 x_4, x_1 x_2 \rangle \subseteq \mathbb{K}[x_1, x_2, x_3, x_4]$

$M_I = \langle x_1 x_2 x_3, x_2^2 \rangle$, $M_J = \langle x_1^2 x_4, x_1 x_2 \rangle$

(διαιρώ το πρώτο με το x_2^2 και φεύγει)

→ $I + J = \langle x_1 x_2 x_3, x_2^2, x_1^2 x_4, x_1 x_2 \rangle = \langle x_2^2, x_1^2 x_4, x_1 x_2 \rangle$

→ $I \cdot J = \langle x_1^3 x_2 x_3 x_4, x_1^2 x_2^2 x_3, x_1^2 x_2^2 x_4, x_1 x_2^3 \rangle$

→ $I \cap J = \langle \text{ΕΚΠ}(x_1 x_2 x_3, x_1^2 x_4) = x_1^2 x_2 x_3 x_4, x_1 x_2 x_3, x_1^2 x_2^2 x_4, x_1 x_2^2 \rangle$

$= \langle x_1 x_2 x_3, x_1 x_2^2 \rangle$ (το 2ο διαιρεί το 1ο & το 4ο το 3ο)

→ $I : J = \bigcap_{j=1}^{2} I : x^{\beta_j} = (I : x^{\beta_1}) \cap (I : x^{\beta_2})$

$= (\langle x_1 x_2 x_3, x_2^2 \rangle : x_1^2 x_4) \cap (\langle x_1 x_2 x_3, x_2^2 \rangle : x_1 x_2)$

$= \left\langle \frac{x_1x_2x_3}{\mu\kappa\delta(x_1x_2x_3,\, x_1^2x_4)}, \frac{x_2^2}{\mu\kappa\delta(x_2^2,\, x_1^2x_4)} \right\rangle \cap \left\langle \frac{x_1x_2x_3}{\mu\kappa\delta(x_1x_2x_3,\, x_1x_2)}, \frac{x_2^2}{\mu\kappa\delta(x_2^2,\, x_1x_2)} \right\rangle$

$= \langle x_2x_3, x_2^2 \rangle \cap \langle x_3, x_2 \rangle$

$= \langle \text{ΕΚΠ}(x_2x_3, x_3), \text{ΕΚΠ}(x_2x_3, x_2), \text{ΕΚΠ}(x_2^2, x_3), \text{ΕΚΠ}(x_2^2, x_2) \rangle$

$= \langle x_2x_3, x_2x_3, x_2^2x_3, x_2^2 \rangle = \langle x_2x_3, x_2^2 \rangle$

$\Rightarrow \sqrt{I} = \sqrt{\langle x_1x_2x_3, x_2^2 \rangle} = \langle \sqrt{x_1x_2x_3}, \sqrt{x_2^2} \rangle = \langle x_1x_2x_3, x_2 \rangle = \langle x_2 \rangle$

πρώτο

Ένα μονωνυμικό ιδεώδες είναι πρώτο αν-ν παράγεται από

Ελέγξε αν ένα μονωνυμικό ιδεώδες είναι πρώτο : μεμονωμένη

μεταβλητή του δακτυλίο

Βάσεις Gröbner

Ορισμός: Έστω ιδεώδες I του $\mathbb{K}[x_1, \dots, x_n]$ και $<$ με μονωνυμική διάταξη με $x_1 > x_2 > \dots > x_n$

Ορίζουμε ως αρχικό ιδεώδες του I (συμβ $in_<(I)$) το μονωνυμικό ιδεώδες $in_<(I) = \langle lt(f), f \in I \rangle$ ($lt(f) = lc(f) \cdot lm(f)$)

Παρατήρηση: Έστω $I = \langle \varphi_1, \dots, \varphi_s \rangle$ όπου $\varphi_i \in \mathbb{K}[x_1, \dots, x_n]$ και έστω $<$ μονωνυμική διάταξη με $x_1 > \dots > x_n$

το αρχ ιδεώδες είναι το $\{\varphi_1, \dots, \varphi_s\}$

ΛΑΘΟΣ $in_<(I) = \langle lt(\varphi_1), \dots, lt(\varphi_s) \rangle$

(διατάσω τους όρους των φ_1, φ_2 λεξικ.)

Πχ $I = \langle \underbrace{x_1^2x_2 + x_3x_4^2}_{=\varphi_1}, \underbrace{x_1x_2^2 - x_3x_4^2}_{=\varphi_2} \rangle \subseteq \mathbb{K}[x_1, x_2, x_3, x_4]$, $<_{lex}$ με $x_1 > x_2 > x_3 > x_4$

Έστω $in_<(I) = \langle lt(\varphi_1), lt(\varphi_2) \rangle = \langle x_1^2x_2, x_1x_2^2 \rangle$

Έστω $f = x_2\varphi_1 - x_1\varphi_2 \in I$

$f = x_2(x_1^2x_2 + x_3x_4^2) - x_1(x_1x_2^2 - x_3x_4^2)$

$= \cancel{x_1^2x_2^2} + x_2x_3x_4^2 - \cancel{x_1^2x_2^2} + x_1x_3x_4^2$

$= x_2x_3x_4^2 + x_1x_3x_4^2 = \underbrace{x_1x_3x_4^2}_{lt(f)} + x_2x_3x_4^2$

αλλά $lt(f) \notin \langle x_1^2x_2, x_1x_2^2 \rangle$ άρα $in_<(I) \neq \langle lt(\varphi_1), \dots, lt(\varphi_s) \rangle$

Άρα, $\boxed{in_<(I) \supseteq \langle lt(\varphi_1), \dots, lt(\varphi_s) \rangle}$

Θεώρημα: (Κάθε) Ένα ιδεώδες $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ έχει πεπερασμένο πλήθος διαφορετικά αρχικά ιδεώδη

Ορισμός: A) Έστω I ιδεώδες του $\mathbb{K}[x_1, \dots, x_n]$ → εφοδιάσει μονωμ. διατ. $<$ με $x_1 > \dots > x_n$

Ένα σύνολο $G = \{g_1, \dots, g_k\} \subseteq I$ καλείται **βάση Gröbner** του I αν $in_<(I) = \langle lt(g_1), \dots, lt(g_k) \rangle$

B) Έστω I ιδεώδες του $\mathbb{K}[x_1, \dots, x_n]$ → εφοδιασμένος με μονων διατ.
Ένα σύνολο $G = \{g_1, \dots, g_k\} \subseteq I$ καλείται **βάση Gröbner** του I αν $\forall f \in I$, υπάρχει δείκτης $\in \{1, \dots, k\}$: $lm(g_i) \mid lm(f)$.

Θεώρημα: Έστω I ιδεώδες του $\mathbb{K}[x_1, \dots, x_n]$ ($<$ μονων. διάταξη) και $G = \{g_1, \dots, g_k\} \subseteq I$. Τα ακόλουθα είναι ισοδύναμα:

1) Το G είναι βάση Gröbner του I
2) $f \in I$ αν-ν $f \xrightarrow{G}_+ 0$
3) $f \in I$ αν-ν $f = \sum_{i=1}^{k} \lambda_i g_i$
4) $in_<(G) = in_<(I)$

Πρόταση: 1) Κάθε ιδεώδες I έχει βάση Gröbner

Απόδειξη: Έστω $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ ιδεώδες και έστω $in_<(I)$
Από λήμμα Dickson $\exists\, \varphi_1, \dots, \varphi_s \in I$ $in_<(I) = \langle lt(\varphi_1), \dots, lt(\varphi_s) \rangle$
Θεωρώ το $G = \{\varphi_1, \dots, \varphi_s\}$. Παρατηρώ ότι $in_<(G) = \underbrace{\langle lt(\varphi_1), \dots, lt(\varphi_s) \rangle}_{= in_<(I)}$

$\Leftrightarrow$ Το G βάση Gröbner του I.

2) Έστω I ιδεώδες του S και $G=\{g_1, \dots, g_k\} \subseteq I$ βάση Gröbner του I. Το σύνολο G αποτελεί σύνολο γεννητόρων του I.

Απόδειξη: G βάση Gröbner $\Rightarrow$ (Θεωρ.) $\forall f \in I : f = \sum \lambda_i g_i$
$\Rightarrow$ το G σύνολο γεννητόρων

Θεώρημα: Έστω σύνολο πολυωνύμων $G=\{g_1, \dots, g_k\} \subseteq \mathbb{K}[x_1, \dots, x_n]$
Το G βάση Gröbner $\Leftrightarrow$ το υπόλοιπο της διαίρεσης οποιουδήποτε $f \in \mathbb{K}[x_1, \dots, x_n]$ μόδιο G είναι μοναδικό.

Παράδειγμα: $G=\{g_1 = x_1^3 - x_2^2,\ g_2 = 2x_1^3 - 2x_3^2,\ g_3 = x_2^2 + x_3\} \subseteq \mathbb{Q}[x_1, x_2, x_3]$
$<_{lex}$ με $x_1 > x_2 > x_3$
Θδο το G όχι βάση Gröbner

$in_<(G) = \langle x_1^3, 2x_1^3, x_2^2 \rangle = \langle x_1^3, x_2^2 \rangle$
$I = \langle g_1, g_2, g_3 \rangle$
Έστω $f \in I$

$$\left.\begin{array}{l} g_1 - \frac{1}{2} g_2 = \cancel{x_1^3} - x_2^2 - \cancel{x_1^3} + x_3^2 = -x_2^2 + x_3^2 \in I \\ \text{και } g_3 = x_2^2 + x_3 \in I \end{array}\right\} \Rightarrow f + g_3 \in I \Rightarrow x_3^2 + x_3 \in I$$

$in_<(I) = \langle lt(f), f \in I \rangle$
$\Rightarrow lt(\ ) = x_3^2 \in I$ αλλά $x_3^2 \notin in_<(G) \Rightarrow in_<(I) \neq in_<(G)$
$\Rightarrow$ G όχι βάση Gröbner.

(*) Αν $in(G) = \langle x_1^3, x_2^2, x_3^? \rangle$ θα έπαιρνα μεταβλητή με μικρότερη δύναμη, όπως πχ το x_3^2.