ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικό και Καποδιστριακό
Πανεπιστήμιο Αθηνών

Άλγεβρα

Ενότητα: Βάσεις Groebner

Ευάγγελος Ράπτης

Τμήμα Μαθηματικών

Άδειες Χρήσης

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αθηνών» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Περιεχόμενα ενότητας

3 Βάσεις Groebner I

3.1 Ιδεώδη μονωνύμων

Έχουμε ήδη δει οτι για ένα σύστημα **μ εξισώσεων** με **ν μεταβλητές** όπως το

$$(\Sigma) \qquad \left\{ \begin{array}{l} f_1(x_1, x_2, ..., x_\nu) = 0 \\ f_2(x_1, x_2, ..., x_\nu) = 0 \\ \vdots \\ f_\mu(x_1, x_2, ..., x_\nu) = 0 \end{array} \right\} \ , f_i \in \mathbb{F}[x_1, x_2, ..., x_\nu], \mathbb{F} \text{ σώμα}$$

το σύνολο των λύσεών του εξαρτάται από το ιδεώδες $I = \langle f_1, f_2, ..., f_\mu \rangle \lhd F[x_1, ..., x_\nu]$.

Υπενθύμιση 1. *Κάθε ιδεώδες I του $F[x]$ είναι της μορφής*

$I = \{f(x) \cdot g(x) \mid g(x) \in F[x]\}$, *δηλαδή* $I =< f(x) >$.

Ορισμός 3.1.1. *Έστω $F[x_1, x_2, ..., x_\nu]$ ο δακτύλιος των πολυωνύμων ν μεταβλητών, με συντελεστές από το σώμα F. Τότε θα καλούμε **ιδεώδες μονωνύμων** του $F[x_1, x_2, ..., x_\nu]$, ένα ιδεώδες που παράγεται από μονώνυμα, δηλαδή*

$$I =< {x_1}^{\alpha_1} {x_2}^{\alpha_2} \cdots {x_\nu}^{\alpha_\nu}, {x_1}^{\beta_1} {x_2}^{\beta_2} \cdots {x_\nu}^{\beta_\nu}, ... > .$$

Σχόλια

1. Τα μονώνυμα που παράγουν το I ενδέχεται να είναι άπειρα.

2. Τα ιδεώδη μονωνύμων στον δακτύλιο των πολυωνύμων μίας μεταβλητής είναι της μορφής

   $$< x^\lambda > \ , \ \lambda \in \mathbb{Z}_{\geq 0}$$

   Το παραπάνω αποδεικνύεται ως εξής: Αν I={0}, τότε ο ισχυρισμός είναι προφανής. Έστω τώρα $I \neq \{0\}$. Επειδή έχουμε μία μόνο μεταβλητή, δηλαδή $\nu = 1$, τότε $I = \langle x^{\xi_1}, x^{\xi_2}, ..., x^{\xi_i}, ... \rangle$. Θεωρούμε το σύνολο $\Xi = \{\xi_1, \xi_2, \xi_3, ...\} \subseteq \{0, 1, 2, ...\}$. Άρα στο Ξ υπάρχει ελάχιστο στοιχείο, έστω ξ. Θα αποδείξουμε οτι $I = \langle x^\xi \rangle$.
   Θεωρούμε το ιδεώδες $A = \langle x^\xi \rangle$. Τότε $x^\xi \in I$ και έτσι $A = \langle x^\xi \rangle \subseteq I$. Έστω $x^\lambda \in I$. Εκτελούμε τη διαίρεση του λ δια του ξ και έχουμε ότι $\lambda = \pi\xi + \upsilon$. Αν $\upsilon \neq 0$, τότε $x^\upsilon = x^\lambda x^{-\pi\xi} \in I$ και οδηγούμαστε σε άτοπο, διότι το ξ είναι ο ελάχιστος θετικός ακέραιος με $x^\xi \in I$. Άρα $\upsilon = 0$ και τελικά $x^\lambda \in I$ και $I \subseteq A$ άρα $A = I$.

3. Αν f είναι ένα στοιχείο του I, τότε το f είναι πολυώνυμο με ν μεταβλητές $x_1, x_2, ..., x_\nu$ και ισχύει ότι

   $$f(x_1, ..., x_\nu) = f_1(x_1, ..., x_\nu)h_1(x_1, ..., x_\nu) + \cdots + f_\kappa(x_1, ..., x_\nu)h_\kappa(x_1, ..., x_\nu),$$

   όπου τα $f_i \in F[x_1, x_2, ..., x_\nu]$ και τα h_i αποτελούν μονώνυμα του I.

4. Το ιδεώδες $I = \langle x^2 + x + 1 \rangle$ δεν είναι ιδεώδες μονωνύμων, διότι αν ήταν θα έπρεπε $I = \langle x^\lambda \rangle$, το οποίο είναι άτοπο αφού δεν υπάρχει πολυώνυμο $h(x)$, τέτοιο ώστε $x^2 + x + 1 = x^\lambda h(x)$.

Θεώρημα 3.1.2. *Έστω I ένα ιδεώδες μονωνύμων του $F[x_1, x_2, ..., x_\nu]$. Τότε υπάρχουν πεπερασμένα μονώνυμα του I έτσι ώστε $I = \langle {x_1}^{\xi_{1,1}} {x_2}^{\xi_{1,2}} \cdots {x_\nu}^{\xi_{1,\nu}}, {x_1}^{\xi_{2,1}} {x_2}^{\xi_{2,2}} \cdots {x_\nu}^{\xi_{2,\nu}}, ..., {x_1}^{\xi_{\lambda,1}} {x_2}^{\xi_{\lambda,2}} \cdots {x_\nu}^{\xi_{\lambda,\nu}} \rangle$.*

Απόδειξη

Συμβατικά θα γράφουμε ${x_1}^{\xi_{i,1}} {x_2}^{\xi_{i,2}} \cdots {x_\nu}^{\xi_{i,\nu}}$ ως x^{α_i}, όπου $\alpha_i = (\xi_{i,1}, \xi_{i,2}, ..., \xi_{i,\nu})$. Άρα $I = \langle x^{\alpha_i}, \alpha_i \in A, i \in K \rangle$, με K σύνολο δεικτών.

Επαγωγή στο πλήθος ν των μεταβλητών.

- Για $\nu = 1$ ισχύει (έχει αποδειχθεί προηγουμένως).
- Έστω ότι ισχύει για $\nu - 1$. Θα αποδείξουμε οτι ισχύει για ν. Γράφουμε $x_\nu = y$. Και έτσι κάθε μονώνυμο είναι της μορφής

  $$ {x_1}^{\xi_{i,1}} {x_2}^{\xi_{i,2}} \cdots {x_{\nu-1}}^{\xi_{i,\nu-1}} \cdot y^{m_i}. $$

  Θεωρούμε το ιδεώδες J των μονωνύμων του $F[x_1, x_2, ..., x_{\nu-1}]$, που παράγεται από όλα τα μονώνυμα της μορφής ${x_1}^{\xi_{i,1}} {x_2}^{\xi_{i,2}} \cdots {x_{\nu-1}}^{\xi_{i,\nu-1}}$ και ${x_1}^{\xi_{i,1}} {x_2}^{\xi_{i,2}} \cdots {x_{\nu-1}}^{\xi_{i,\nu-1}} \cdot y^{m_i} \in I$ για κάποιο $m_i \in \{0, 1, 2, ...\}$.
  Από την υπόθεση της επαγωγής έχουμε ότι

  $$ J = \langle x^{\alpha_1}, x^{\alpha_2}, ..., x^{\alpha_\lambda} \rangle, $$

  όπου με x^{α_i} δηλώσαμε ότι συμβολίζουμε το ${x_1}^{\xi_{i,1}} {x_2}^{\xi_{i,2}} \cdots {x_\nu}^{\xi_{i,\nu-1}}$ ως x^{α_i}.

  Θα έχουμε λοιπόν

  $$ \begin{aligned} x^{\alpha_1} \in J \Rightarrow \quad & x^{\alpha_1} \cdot y^{m_1} \in I \text{ για κάποιο } m_1 \in \{0, 1, 2, ...\} \\ x^{\alpha_2} \in J \Rightarrow \quad & x^{\alpha_2} \cdot y^{m_2} \in I \text{ για κάποιο } m_2 \in \{0, 1, 2, ...\} \\ & \vdots \\ x^{\alpha_\lambda} \in J \Rightarrow \quad & x^{\alpha_\lambda} \cdot y^{m_\lambda} \in I \text{ για κάποιο } m_\lambda \in \{0, 1, 2, ...\} \end{aligned} $$

  Έστω $m = max\{m_1, m_2, ..., m_\lambda\}$.
  Για $m = 0$ θεωρούμε τα μονώνυμα

  $$ x^{\alpha_{0,1}}, x^{\alpha_{0,2}}, ..., x^{\alpha_{0,\lambda}} \in I $$

  Για $m = 1$ θεωρούμε τα μονώνυμα

  $$ x^{\alpha_{1,1}} \cdot y, x^{\alpha_{1,2}} \cdot y, ..., x^{\alpha_{1,\lambda}} \cdot y \in I $$

  $$ \vdots $$

  Για $m - 1$ θεωρούμε τα μονώνυμα

  $$ x^{\alpha_{m-1,1}} \cdot y^{m-1}, x^{\alpha_{m-1,2}} \cdot y^{m-1}, ..., x^{\alpha_{m-1,\lambda}} \cdot y^{m-1} \in I $$

  Για m θεωρούμε τα μονώνυμα

  $$ x^{\alpha_{m,1}} \cdot y^m, x^{\alpha_{m,2}} \cdot y^m, ..., x^{\alpha_{m,\lambda}} \cdot y^m \in I $$

  Τότε θα έχουμε για ένα μονώνυμο του I, το οποίο θα έχει την μορφή $x^\alpha y^\sigma$. Αν $\sigma \geq m$, τότε το μονώνυμο παράγεται από το $I = \langle x^{\alpha_{m,1}} \cdot y^m, x^{\alpha_{m,2}} \cdot y^m, ..., x^{\alpha_{m,\lambda}} \cdot y^m \rangle$. Αν όμως $\sigma \leq m \Rightarrow \sigma = \{0, 1, ..., m-1\}$, τότε το μονώνυμο παράγεται από μονώνυμα των υπολοίπων προηγούμενων κατηγοριών.

Ορισμός 3.1.3. *Σε κάθε πολυώνυμο $f(x_1,x_2,...,x_\nu) \in F[x_1,x_2,...,x_\nu]$ έχουμε ένα μεγιστοβάθμιο όρο (σύμφωνα με τη λεξικογραφική διάταξη που εφαρμόζουμε) και τον συμβολίζουμε $\mathbf{MO(f)}$.*

Παράδειγμα 3.1.4. *Έστω το πολυώνυμο $f(x,y) = 3x^5y^4 + 4x^3y^5 + 6xy^7 + 7y + 8$. Σύμφωνα με τη διάταξη $x > y$, έχουμε ότι $\mathbf{MO(f)} = 3x^5y^4$.*

Ορισμός 3.1.5. *Έστω I ιδεώδες του $F[x_1,x_2,...,x_\nu]$ (όχι κατ' ανάγκη ιδεώδες μονωνύμων). Από το I φτιάχνουμε το ιδεώδες μονωνύμων $J = \langle MO(f) | f \in I\rangle = \langle \rho_1 x^{\alpha(1)}, \rho_2 x^{\alpha(2)}, ..., \rho_\lambda x^{\alpha(\lambda)}\rangle$. Άρα μπορούμε να βρούμε πεπερασμένο πλήθος πολυωνύμων $f_1, f_2, ..., f_\lambda \in I$ έτσι ώστε $J = \langle MO(f_1), MO(f_2), ...MO(f_\lambda)\rangle$. Το σύνολο $\{f_1, f_2, ..., f_\lambda\}$ λέγεται* ***βάση Groebner*** *του ιδεώδους I.*

Επανάληψη

Έστω $f_1(x_1,x_2,...,x_\nu),\ f_2(x_1,x_2,...,x_\nu),\ ...,\ f_\mu(x_1,x_2,...,x_\nu) \in F[x_1,x_2,...,x_\nu]$ δηλαδή $f_1, f_2, ..., f_\lambda$ πολυώνυμα με συντελεστές από το σώμα F. Τότε υπάρχει μία διαδικασία (αλγόριθμος) διαίρεσης έτσι ώστε:

1. $f(x_1,x_2,...,x_\nu) = \alpha_1(x_1,x_2,...,x_\nu)\cdot f(x_1,x_2,...,x_\nu) + ... + a_\kappa f_\kappa + \upsilon(x_1,x_2,...,x_\nu)$
2. Είτε $\upsilon(x_1,x_2,...,x_\nu) = 0$ είτε $\upsilon \neq 0$ κ' $\upsilon(x_1,x_2,...,x_\nu) = \lambda_1 x^{\xi_{11}}x^{\xi_{12}}...x^{\xi_{1\nu}} + ... + \lambda_\rho x^{\xi_{\rho 1}}x^{\xi_{\rho 2}}...x^{\xi_{\rho\nu}}$ το οποιο αποτελεί γραμμικό συνδυασμό μονωνύμων με $\lambda_i \in F$. Επίσης δεν υπάρχει μονώνυμο του υπολοίπου που να διαιρείται από κάποιο MO ενός $f_i, i = 1,...,k$.
3. Για κάθε $i = 1,2,...,k$, είτε $\alpha_i \cdot f_i = 0$ ή $\alpha_i f_i \neq 0$ και ισχύει ότι $deg(f) \geq deg(\alpha_i f_i)$.

Σημείωση 1. *Υποθέτουμε ότι έχουμε σταθεροποιήσει μία διάταξη των μεταβλητών (π.χ. $x_1 > x_2 > ... > x_n$) η οποία επάγει μία διάταξη στα μονώνυμα.*

Έστω $F[x_1,...,x_\nu]$ ο δακτύλιος των πολυωνύμων. Ιδεώδες μονωνύμων είναι ένα ιδεώδες του $F[x_1,...,x_\nu]$ που παράγεται από μονώνυμα.

Θεώρημα 3.1.6. *Έστω $I =< x_1^{\alpha_{i1}}x_2^{\alpha_{i2}}\cdots x_\nu^{\alpha_{i\nu}}, (\alpha_{i1},\alpha_{i2},...,\alpha_{i\nu}) \in A >$ ένα ιδεώδες μονονύμων. Τότε το I είναι πεπερασμένα παραγόμενο, δηλαδή υπάρχει πεπερασμένο πλήθος μονωνύμων :*

$$x_1^{\alpha_{11}}x_2^{\alpha_{12}}\cdots x_\nu^{\alpha_{1\nu}}, ..., x_1^{a_{k1}}x_2^{a_{k2}}\cdots x_\nu^{a_{k\nu}}$$

που παράγουν το I.

Έστω $I =< x_1^{a_{i1}}x_2^{a_{i2}}\cdots x_\nu^{a_{i\nu}}, (\alpha_{i1},...,\alpha_{i\nu}) \in A >$ ένα ιδεώδες μονωνύμων και $x_1^{\beta_{\rho 1}}x_2^{\beta_{\rho 2}}\cdots x_\nu^{\beta_{\rho\nu}} \in I$. Τότε το $x_1^{\beta_{\rho 1}}x_2^{\beta_{\rho 2}}\cdots x_\nu^{\beta_{\rho\nu}}$ διαιρείται από κάποιο $x_1^{a_{i1}}x_2^{a_{i2}}\cdots x_\nu^{a_{i\nu}}$.

Απόδειξη

Το I είναι διανυσματικός χώρος (άπειρης διάστασης) επί του F (τα μονώνυμα του I είναι γραμμικά ανεξάρτητα). Επειδή το $x_1^{\gamma_{\rho 1}}x_2^{\gamma_{\rho 2}}\cdots x_\nu^{\gamma_{\rho\nu}} \in I$, τότε αυτό είναι γραμμικός συνδυασμός μονωνύμων της μορφής $x_1^{a_{i1}}x_2^{a_{i2}}...x_\nu^{a_{i\nu}}$.

Έστω $I \lhd F[x_1,...,x_\nu]$ όπου το I δεν είναι κατ' ανάγκη ιδεώδες μονωνύμων, τότε έχουμε τα εξής :

1. $MO(I) = \{\lambda \cdot x_1^{a1}x_2^{a2}...x_\nu^{a_\nu} \mid$ υπάρχει $f(x_1,...x_\nu) \in I$ του οποίου ο μεγιστοβάθμιος όρος είναι το $\lambda \cdot x_1^{a1}x_2^{a2}...x_\nu^{a_\nu}\}$. Αξίζει να παρατηρήσουμε ότι το σύνολο $MO(I)$ είναι άπειρο εάν $I \neq \{\emptyset\}$.
2. Το ιδεώδες $< MO(I) >$ είναι ιδεώδες μονωνύμων.

3. Έχουμε αποδείξει ότι το $< MO(I) >$ παράγεται από πεπεράσμενα μονώνυμα του συνόλου $MO(I)$. Δηλαδή $< MO(I) >=< x_1^{a_{11}} x_2^{a_{12}} \cdots x_\nu^{a_{1\nu}}, ..., x_1^{a_{k2}} x_1^{a_{k2}} \cdots x_\nu^{a_{k\nu}} >$. Το $x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_\nu^{a_{i\nu}}$ είναι ένα μονώνυμο του $< MO(I) >$. Χωρίς λάθος μπορούμε να υποθέσουμε ότι $\lambda \cdot x_1^{a_{11}} x_2^{a_{12}} \cdots x_\nu^{a_{1\nu}}$ ανήκει στο σύνολο που παράγει το $< MO(I) >$. Άρα υπάρχουν πολυώνυμα $g_1(x_1, ..., x_\nu) \in I$ με $MO(g_1) = \lambda_1 \cdot x_1^{a_{11}} x_2^{a_{12}} \cdots x_\nu^{a_{1\nu}}, g_2(x_1, ..., x_\nu) \in I$ με $MO(g_2) = \lambda_2 \cdot x_1^{a_{11}} x_2^{a_{12}} \cdots x_\nu^{a_{1\nu}}, ..., g_\kappa(x_1, ..., x_\nu) \in I$ με $MO(g_\kappa) = \lambda_1 \cdot x_1^{a_{11}} x_2^{a_{12}} \cdots x_\nu^{a_{1\nu}}$.

Ορισμός 3.1.7. *Το σύνολο των πολυωνύμων $\{g_1, g_2, .., g_\kappa\}$ λέγεται **βάση Groebner του ιδεώδους I.***

Έχουμε δηλαδή μέχρι στιγμής την ακολουθία καταστάσεων

$$\left\{ \begin{array}{l} \text{Σύστημα πολυωνύμων} \\ \text{ή σύστημα πολυωνυ-} \\ \text{μικών εξισώσεων} \end{array} \right\} \rightarrow \qquad \left\{ \begin{array}{l} \text{Ιδεώδες } I \text{ το} \\ \text{οποίο παράγεται} \\ \text{από τα πολυώνυμα} \end{array} \right\} \rightarrow$$

$$\left\{ \begin{array}{l} \text{Ιδεώδες μονωνύμων των} \\ \text{μεγιστοβαθμίων όρων} \\ \text{των πολυωνύμων του } I \end{array} \right\} \rightarrow \qquad \left\{ \textbf{ Βάση Groebner } \right\}$$

Παράδειγμα 3.1.8. *Έστω τα πολυώνυμα $f_1(x, y) = x^3 y - 2x^2 y^2 + x$ και $f_2(x, y) = 3x^4 - y$ και το ιδεώδες $I = \langle f_1, f_2 \rangle$. Τότε η **βάση Groebner** που προκύπτει είναι η εξής $\{252x - 624y^7 + 493y^4 - 3y \ , \ 6y^4 - 49y^7 + 48y_{10} - 9y\}$.*

Θεώρημα 3.1.9. *(Βάσης του Hilbert)*
Κάθε ιδεώδες I του $F[x_1, ..., x_\nu]$ είναι πεπερασμένο παραγόμενο. Δηλαδή υπάρχουν $g_1(x_1, x_2, ..., x_\nu)$, $g_2(x_1, x_2, ..., x_\nu)$, ..., $g_\kappa(x_1, x_2, ..., x_\nu)$ με $I = \langle g_1, g_2, ..., g_\kappa \rangle$
Απόδειξη
Εάν $I = \{0\}$,τότε είναι προφανές.
*Εάν $I \neq \{0\}$, τότε το I έχει μία **βάση Groebner** $\{g_1, g_2, ..., g_\kappa\}$.*
Έστω $g \in I$. Εκτελούμε τη διαίρεση του g διά τα $g_1, g_2, ..., g_\kappa$. Τότε $g = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_\kappa g_\kappa + \upsilon$. Θα έχουμε

- *Εάν $\upsilon = 0 \Rightarrow g \in I$.*
- *Εάν $\upsilon \neq 0$ καταλήγουμε στα εξής*

  (i) $\upsilon \in I$

  (ii) Το υ είναι άθροισμα μονωνύμων, κανένα εκ των οποίων ΔΕΝ διαιρείται με $MO(g_i)$, $\forall i = 1, 2, ..., \kappa$.

Έτσι έχουμε ότι το $\upsilon \in I$, άρα $MO(\upsilon) \in MO(I) \subseteq \langle MO(I) \rangle = \langle MO(g_1), MO(g_2), ..., MO(g_\kappa) \rangle$. Άρα ο $MO(\upsilon)$ διαιρείται με κάποιο $MO(g_i)$, με $i = 1, 2, ..., \kappa$. Άτοπο.

Συμπεράσματα
Έστω I ιδεώδες του $F[x_1, ..., x_\nu]$. Τότε θα ισχύουν

1. $\langle MO(I) \rangle = \langle MO(g_1), MO(g_2), ..., MO(g_\kappa) \rangle, (g_1, g_2, ..., g_\kappa$: ***βάση Groebner***$)$.

2. $\{g_1, g_2, ..., g_\kappa\}$ *είναι μία* ***βάση Groebner***

3. *Κάθε ιδεώδες* I *του* $F[x_1, ..., x_\nu]$ *έχει μία* ***βάση Groebner****.*

4. *Προφανώς* $I = \langle g_1, g_2, ..., g_\kappa \rangle$*.*

Παράδειγμα 3.1.10. *Έστω* $\langle g_1, g_2 \rangle = I \subseteq \mathbb{R}[x, y]$ *με* $g_1(x, y) = x^3 - 2xy, g_2(x, y) = x^2y - 2y^2 + x = x^2y + x - 2y^2$*.*

Ισχυρισμός
Το σύνολο $\{g_1, g_2\}$ ***δεν*** *είναι* ***βάση Groebner*** *του* I*.*
Για $x > y$ *έχουμε* $MO(g_1) = x^3, MO(g_2) = x^2y \Rightarrow \langle MO(g_1), MO(g_2) \rangle = \langle x^3, x^2y \rangle$*. Έχουμε ότι* $x \cdot g_2 - y \cdot g_1 = x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2$*, δηλαδή* $x^2 \in \langle MO(I) \rangle$*. Για να είναι* ***βάση Groebner****, θα πρέπει* $x^2 = \alpha(x, y) \cdot x^2 + \beta(x, y) \cdot (x^2y)$*. Άτοπο. Άρα δεν είναι* ***βάση Groebner****.*

Παράδειγμα 3.1.11. *Έστω τα πολυώνυμα* $g_1(x, y, z) = x + z \in \mathbb{R}[x, y, z]$ *και* $g_2(x, y, z) = y - z \in \mathbb{R}[x, y, z]$*. Τότε* $\{g_1, g_2\}$ *είναι μία* ***βάση Groebner*** *του* $I = \langle g_1, g_2 \rangle$*. Έστω το τυχαίο πολυώνυμο* $f \in I$*, όπου* I *το παραπάνω ιδεώδες. Τότε δεν είναι απαραίτητο ότι θα ισχύει* $MO(f) = max\{MO(g_1), MO(g_2)\}$*.*

Διαίρεση στο δακτύλιο $F(x_1, ..., x_\nu)$***.***
Αν $f(x_1, ..., x_\nu) \in F(x_1, ..., x_\nu)$*, όπου* F *σώμα και* $(f_1, f_2, ..., f_\nu)$ *μία διατεταγμένη κ-άδα στοιχείων του* $F(x_1, ..., x_\nu)$*. Τότε ο αλγόριθμος της διαίρεσης δίνει*

$$f(x_1, ..., x_\nu) = \alpha_1(x_1, ..., x_\nu) f_1(x_1, ..., x_\nu) + \cdots + \alpha_\nu(x_1, ..., x_\nu) f_\nu(x_1, ..., x_\nu) + \upsilon(x_1, ..., x_\nu).$$

Κάθε ιδεώδες μονωνύμων είναι πεπερασμένα παραγόμενο.

Θεώρημα 3.1.12. ***(βάσης του*** $Hilbert$***)***
Κάθε ιδεώδες $I \lhd F(x_1, x_2, ..., x_\nu)$ *είναι πεπερασμένα παραγόμενο.*

Βάσεις Groebner ενός ιδεώδους $I \lhd F(x_1, ..., x_\nu)$***.***
Τα βήματα τα οποία πρέπει να ακολουθήσουμε για να βρούμε μία ***βάση Groebner*** *είναι τα εξής :*

- *Βρίσκουμε το σύνολο* $\{M.O.(f), f \in I\}$*.*
- *Θεωρούμε το ιδεώδες* $\langle M.O.(f), f \in I \rangle$*.*
- *Το* $\{M.O.(f), f \in I\}$ *είναι πεπερασμένα παραγόμενο διότι είναι ιδεώδες μονωνύμων, άρα* $\langle M.O.(f), f \in I \rangle = \langle M.O.(g_1), M.O.(g_2), ..., M.O.(g_\kappa) \rangle$*, όπου* $g_1, g_2, ..., g_\kappa \in I$*. Το σύνολο* $G = \{g_1, g_2, ..., g_\kappa\}$ *λέγεται* ***βάση Groebner*** *του* I*. (Υποτίθεται οτι ακόμα δε γνωρίζουμε αλγόριθμο εύρεσης μίας* ***βάσης Groebner****, αλλά γνωρίζουμε οτι υπάρχει.)*

Για ένα τυχαίο $f \in I$*, η διαίρεσή του με δύο διαφορετικά πολυώνυμα* g_1 *και* g_2 *δίνει διαφορετικό υπόλοιπο από εκείνο της διαίρεσης με τα ίδια πολυώνυμα, αλλά με αντίστροφη σειρά, δηλαδή* g_2 *και* g_1*.*

Έστω $G = \{g_1, g_2, ..., g_\kappa\}$ *μία* ***βάση Groebner*** *ενός ιδεώδους* $I \lhd F(x_1, ..., x_\nu)$*,* $f \in F(x_1, ..., x_\nu)$ *και* $\upsilon_1(x_1, x_2, ..., x_\nu), \upsilon_2(x_1, x_2, ..., x_\nu)$ *τα υπόλοιπα της διαίρεσης του* f *με το* $\{g_1, g_2, ..., g_\kappa\}$*, ενδεχομένως*

αλλάζοντας τη διάταξη, π.χ. $\{g_2, g_1, ..., g_\kappa\}$. *Τότε* $\upsilon_1 = \upsilon_2$.

Απόδειξη
Έστω $\upsilon_1 - \upsilon_2 = 0$, *τότε ισχύει το ζητούμενο.*
Εαν όμως θεωρήσουμε ότι $\upsilon_1 - \upsilon_2 \neq 0$, *τότε η διαφορά* $\upsilon_1 - \upsilon_2$ *αποτελεί συνδυασμό των* $\{g_2, g_1, ..., g_\kappa\}$ *και άρα έχουμε* $\upsilon_1 - \upsilon_2 \in \langle g_2, g_1, ..., g_\kappa \rangle$. *Αλλά το σύνολο* $\{g_2, g_1, ..., g_\kappa\}$ *είναι μία* ***βάση Groebner*** *του* I. *Έτσι ο μεγιστοβάθμιος όρος του* $\upsilon_1 - \upsilon_2$ *(αν* $\upsilon_1 - \upsilon_2 \neq 0$*) διαιρείται από τουλάχιστον ένα μέγιστο όρο από τα* $g_2, g_1, ..., g_\kappa$. *Άτοπο από τον ορισμό της* ***βάσης Groebner***.

Υπάρχει αλγόριθμος ο οποίος αποφαίνεται εάν το $f \in F(x_1, ..., x_\nu)$ *ανήκει ή όχι στο ιδεώδες* $I \lhd F(x_1, ..., x_\nu)$, *ακολουθώντας τα παρακάτω βήματα :*

(i) Ο αλγόριθμος βρίσκει μία ***βάση Groebner***.

(ii) Διαιρούμε το f *δια* $\{g_2, g_1, ..., g_\kappa\}$.

(iii) $f \in I \Leftrightarrow$ *το υπόλοιπο της διαίρεσης του* f *διά* $\{g_2, g_1, ..., g_\kappa\}$ *είναι* 0.
(Στα (ii) και (iii) δεν μας ενδιαφέρει η σειρά των $g_2, g_1, ..., g_\kappa$.*)*

Συμβολισμός
Το υπόλοιπο του $f \in F[x_1, ..., x_\nu]$ *διά του διατεταγμένου συνόλου* $A = \{f_1(x), f_2(x), ..., f_\mu(x)\}$, *το συμβολίζουμε* $\overline{F^A}$. *Ιδιαίτερα αν* $A = G = \{g_2, g_1, ..., g_\kappa\}$, *τότε το συμβολίζουμε με* $\overline{F^G}$ *και το* G *δε χρειάζεται να είναι διατεταγμένο.*

Σημείωση 2. *Έστω το ιδεώδες* $I \lhd F(x_1, ..., x_\nu)$. *Τότε ορίζεται καλά ο δακτύλιος–πηλίκο* $F[x_1, ..., x_\nu]/I$.

Θεώρημα 3.1.13. *Έστω* $f_1(x_1, x_2, ..., x_\nu) = 0$, $f_2(x_1, x_2, ..., x_\nu) = 0$, ..., $f_\mu(x_1, x_2, ..., x_\nu) = 0$ *ένα σύστημα* ***μ πολυωνυμικών*** *εξισώσεων με* ***ν μεταβλητες*** *και* $I = \langle f_1, f_2, ..., f_\mu \rangle \lhd F[x_1, ..., x_\nu]$. *Το σύστημα έχει πεπερασμένες λύσεις* $\Leftrightarrow dim\, F[x_1, ..., x_\nu]/I < \infty$.

Κάθε στοιχείο του δακτυλίου πηλίκου $F(x_1, ..., x_\nu)/I$ *είναι σε* $1-1$ *και επί αντιστοιχία με τα υπόλοιπα* $\overline{F^G}$, *όπου* G *μία* ***βάση Groebner***.
Απόδειξη
Κάθε στοιχείο του $F(x_1, ..., x_\nu)/I$ *είναι της μορφής* $f + I$. *Ορίζουμε* $f + I \rightarrow \overline{F^G}$. *Η αντιστοίχια είναι* $1-1$ *και επί.*

Έστω $f(x) \in F(x)$ *μη σταθερό πολυώνυμο* ν*–οστού βαθμού και* $I = \langle f \rangle$. *Τότε* $F[x]/I$ *είναι το σύνολο των πολυωνύμων βαθμού* $\nu - 1$. *Τα μονώνυμα* $1, x, x^2, x^3, ..., x^{\nu-1}$ *είναι γραμμικά ανεξάρτητα, άρα* $dim_F F[x]/I = \nu$.

Λήμμα 3.1.14. *Έστω* $F[x_1, ..., x_\nu]$ *ο δακτύλιος των πολυωνύμων με* ν *μεταβλητές,* I *ιδεώδες και* $G = \{g_1, g_2, ..., g_\kappa\}$ *μία* ***βάση Groebner*** *του* I. *Επίσης* $M.O.(g_1) \in \langle M.O.(g_2), ..., M.O.(g_\kappa) \rangle$. *Τότε το σύνολο* $\{g_2, ..., g_\kappa\}$ *αποτελεί μία* ***βάση Groebner*** *του* I.
Απόδειξη
Έχουμε ότι $\langle M.O.(g_2), ..., M.O.(g_\kappa) \rangle = \langle M.O.(g_1), M.O.(g_2), ..., M.O.(g_\kappa) \rangle$. *Επιπλέον* $I = \langle g_2, ..., g_\kappa \rangle$. *Πράγματι έστω* $g_1 = \alpha_2 g_2 + \cdots + \alpha_\kappa g_\kappa + \upsilon$, *τότε* $\upsilon \in I$ *και δε διαιρείται ο* $M.O.(\upsilon)$ *από κανένα από τα* $M.O.(g_2, ..., g_\kappa)$, *άρα* $\upsilon = 0$ *από τον αλγοριθμο της διαίρεσης.*

3.2 *Ξανά το σύστημα*

Ας επανέλθουμε τώρα στον αρχικό μας στόχο: Να λύσουμε το σύστημα 3.1 . Βασικός σκοπός μας είναι να μετασχηματίσουμε το αρχικό σύστημα (Σ) και να οδηγηθούμε σε ένα άλλο σύστημα $(\Sigma^\star)$, το οποίο να είναι πιο εύκολο να λυθεί.

Το εύκολο αρχικό συστημα ήταν:

$$(\Sigma_1) \quad \begin{pmatrix} f_1(x)=0 \\ f_2(x)=0 \\ \cdots\cdots \\ f_\mu(x)=0 \end{pmatrix}$$

όπου τα πολυώνυμα $f_1(x), f_2(x), \cdots, f_\mu(x)$ είναι πολυώνυμα μίας μεταβλητής με συντελεστές από το σώμα $\mathbb{F}$[1]

1. *Έχοντας τα προηγούμενα πολυώνυμα $f_1(x), f_2(x), \cdots, f_\mu(x)$, για κάθε επιλογή πολυωνύμων $h_1(x), h_2(x), \cdots, h_\mu(x) \in \mathbb{F}[x]$ κατασκευάζουμε το πολυώνυμο:*

$$h_1(x)\cdot f_1(x) + h_2(x)\cdot f_2(x) + \cdots + h_\mu(x)\cdot f_\mu(x)$$

2. *Κάθε πολυώνυμο, όπως το προηγούμενο λέγεται* **πολυωνυμικός συνδυασμός** *των $f_1(x), f_2(x), \cdots, f_\mu(x)$.*

3. *Θυμηθείτε εδώ ότι αν έχουμε ένα διανυσματικό χώρο V με συντελεστές από το σώμα $\mathbb{F}$ και $v_1, v_2, \cdots, v_\kappa$ ένα σύνολο διανυσμάτων, κάθε διάνυσμα της μορφής $\lambda\cdot v_1 + \lambda_2\cdot v_2 + \cdots + \lambda_\kappa\cdot v_\kappa$ το λέμε* **γραμμικό συνδυασμό των διανυσμάτων** *$v_1, v_2, \cdots, v_\kappa$ και επίσης το σύνολο των γραμμικών συνδυασμών σχηματίζει ένα υπόχωρο του διανυσματικού χώρου, ο οποίος λέγεται* **υπόχωρος παραγόμενος από τα παραπάνω διανύσματα**.

4. *Ονομάζουμε $\Lambda(\Sigma_1)$ το σύνολο λύσεων του συστήματος (Σ_1), δηλαδή το σύνολο*

$$\Lambda(\Sigma_1) = \{\xi \in \mathbb{F} : f_1(\xi)=0, f_2(\xi)=0, \cdots, f_\mu(\xi)=0\}$$

5. *Το $\Lambda(\Sigma_1)$ προφανώς είναι ένα πεπερασμένο σύνολο, διότι ένα πολυώνυμο μίας μεταβλητής έχει πεπερασμένο σύνολο λύσεων. Επίσης είναι δυνατόν το $\Lambda(\Sigma_1)$ να είναι το κενό σύνολο, Στην περίπτωση αυτή λέμε ότι το σύστημα είναι* **αδύνατο**.

6. **Σημαντική παρατήρηση I:** *Αν $\xi \in \Lambda(\Sigma_1)$, τότε*

$$h_1(\xi)\cdot f_1(\xi) + h_2(\xi)\cdot f_2(\xi) + \cdots + h_\mu(\xi)\cdot f_\mu(\xi) = 0$$

δηλαδή κάθε στοιχείο του $\Lambda(\Sigma_1)$ μηδενίζει κάθε πολυωνυμικό συνδυασμό των πολυωνύμων του συστήματος.

7. **Σημαντική παρατήρηση II:** *Αν ένα από τα πολυώνυμα του συστήματος είναι πολυωνυμικός συνδυασμός των υπολοίπων, για παράδειγμα αν $f_1(x) = \phi_2(x)\cdot f_2(x) + \phi_3(x)\cdot f_3(x) + \cdots + \phi_\mu(x)\cdot f_\mu(x)$, τότε το σύνολο λύσεων $\Lambda(\Sigma_1)$ του αρχικού συστήματος είναι ίσο με το σύνολο λύσεων $\Lambda(\Sigma^\star)$ του συστήματος*

$$(\Sigma^\star) \quad \begin{pmatrix} f_2(x)=0 \\ \cdots\cdots \\ f_\mu(x)=0 \end{pmatrix}$$

[1] Όπως ήδη έχουμε αναφέρει, συνήθως ως σώμα συντελεστών θα θεωρούμε το σώμα $\mathbb{R}$ των πραγματικών αριθμών ή το σώμα $\mathbb{C}$ των μιγαδικών αριθμών.

το οποίο προκύπτει διά διαγραφής του πολυωνύμου $f_1(x)$

Απόδειξη: *Έστω* $\xi \in \Lambda(\Sigma)$. *Τότε* $f_1(\xi) = 0, f_2(\xi) = 0, \cdots, f_\mu(\xi) = 0$, *οπότε και* $f_2(\xi) = 0, \cdots, f_\mu(\xi) = 0$, *άρα* $\xi \in \Lambda(\Sigma^\star)$ *και έτσι* $\Lambda(\Sigma) \subseteq \Lambda(\Sigma^\star)$ *Αντίστροφα έστω* $\rho \in \Lambda(\Sigma^\star)$. *Έχουμε ότι* $f_2(\rho) = 0, \cdots, f_\mu(\rho) = 0$ *και* $f_1(\rho) = \phi_2(\rho) \cdot f_2(\rho) + \phi_3(\rho) \cdot f_3(\rho) + \cdots + \phi_\mu(\rho) \cdot f_\mu(\rho) = 0$ *και έτσι* $\Lambda(\Sigma^\star) \subseteq \Lambda(\Sigma)$. *Τελικά*

$$\Lambda(\Sigma^\star) = \Lambda(\Sigma)$$

8.

Πρόταση 3.2.1. *Έστω* (Σ_1) $\begin{pmatrix} f_1(x) = 0 \\ f_2(x) = 0 \\ \cdots\cdots \\ f_\mu(x) = 0 \end{pmatrix}$

ένα σύστημα πολυωνυμικών εξισώσεων μίας μεταβλητής, όπως παραπάνω και $g(x) = h_1(x) \cdot f_1(x) + h_2(x) \cdot f_2(x) + \cdots + h_\mu(x) \cdot f_\mu(x)$ *ένας πολυωνυμικός συνδυασμός των πολυωνύμων του συστήματος. Τότε το σύνολο λύσεων* $\Lambda(\Sigma)$ *του συστήματος είναι υποσύνολο του συνόλου λύσεων* $\Lambda(\mathbf{g})$ *του* $g(x)$.

Απόδειξη: *Άμεση από το σημείο 6 (Σημαντική παρατήρηση I).*

9. Το παραπάνω μας λέει ότι αν έχουμε ένα σύστημα μ-πολυωνυμικών εξισώσεων μίας μεταβλητής και ψάχνουμε για το σύνολο λύσεων αυτού, μπορούμε να ψάχνουμε για το σύνολο λύσεων **ενός** *πολυωνύμου, ενός πολυωνυμικού συνδυασμού.*

10. **Σημαντικό ερώτημα I :** *Αφού για το σύνολο λύσεων* $\Lambda(\Sigma_1)$ *ενός συστήματος μ πολυωνυμικών εξισώσεων αρκεί να ψάχνουμε σε ένα πολυωνυμικό συνδυασμό, ποιός είναι ο πιο κατάλληλος πολυωνυμικός συνδυασμός;*

Υπόδειξη για σκέψη: Σκεφθείτε τον Μέγιστο Κοινό Διαιρέτη.

11. Δίνουμε και τον παρακάτω ορισμό:

Ορισμός 3.2.2. *Έστω* $f_1(x), f_2(x), \cdots, f_\mu(x)$ *πολυώνυμα του δακτυλίου* $\mathbb{F}[x]$, *δηλαδή πολυώνυμα μίας μεταβλητής με συντελεστές από το σώμα* $\mathbb{F}$. *Το σύνολο των πολυωνυμικών συνδυασμών των* $f_1(x), f_2(x), \cdots, f_\mu(x)$, *δηλαδή πολυωνύμων της μορφής* $h_1(x) \cdot f_1(x) + h_2(x) \cdot f_2(x) + \cdots + h_\mu(x) \cdot f_\mu(x)$ *με* $h_i(x) \in \mathbb{F}[x]$, *λέγεται* **ιδεώδες παραγόμενο από τα πολυώνυμα** $f_1(x), f_2(x), \cdots, f_\mu(x)$

12. **Σημαντικό ερώτημα II :** *Ποιός είναι ο καλύτερος τρόπος να περιγράψει κανείς ένα ιδεώδες;*

3.3 Ευρύτερη μελέτη

(i) Μελετήστε τα σχετικά με τα ιδεώδη στη σελίδα εδώ.

(ii) Μελετήστε επίσης τα αναγραφόμενα στη σελίδα εδώ.

1. Θεωρούμε το ιδεώδες $I =< f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu) >$.
Το I *είναι το ιδεώδες που* **παράγεται** *από τα πολυώνυμα του συστήματος στον δακτύλιο των πολυωνύμων* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. *Το* I *αποτελείται από όλους τους πολυωνυμικούς συνδυασμούς των πολυωνύμων* $f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu)$.

2. *Παρατηρούμε ότι το ιδεώδες I, περιέχει όλες τις πληροφορίες για το σύνολο λύσεων του συστήματος. Πράγματι αν Λ το σύνολο λύσεων του αρχικού συστήματος (Σ) 3.1 και $\Lambda(I)$, το σύνολο λύσεων του συστήματος, που λαμβάνεται, αν πάρουμε τα (άπειρα) πολυώνυμα του I, τότε $\Lambda = \Lambda(I)$.*

   Απόδειξη *Έστω $(\xi_1, \xi_2, \cdots, \xi_\nu) \in \Lambda$, τότε*

   $$f_1(\xi_1, \xi_2, \cdots, \xi_\nu) = 0 \ , \ f_2(\xi_1, \xi_2, \cdots, \xi_\nu) = 0 \ , \ \cdots \ , \ f_\mu(\xi_1, \xi_2, \cdots, \xi_\nu) = 0$$

   Ένα τυχαίο στοιχείο του I είναι της μορφής:

   $$\begin{aligned} g(x_1, x_2, \cdots, x_\nu) \ = \ & h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) \ + \\ & h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) \ + \\ & \cdots \ + \\ & h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu) \end{aligned}$$

   για κάποια αυθαίρετα πολυώνυμα $h_1(x_1, x_2, \cdots, x_\nu), h_2(x_1, x_2, \cdots, x_\nu), \cdots, h_\mu(x_1, x_2, \cdots, x_\nu) \in \mathbb{F}[x_1, x_2, \cdots, x_\nu]$.

   Παρατηρούμε ότι $g(\xi_1, \xi_2, \cdots, \xi_\nu) = 0$, άρα το $(\xi_1, \xi_2, \cdots, \xi_\nu)$ ανήκει στο $\Lambda(I)$, αφού μηδενίζει κάθε πολυώνυμο του I και άρα $\Lambda \subseteq \Lambda(I)$.
   Αντίστροφα έστω ότι $(\xi_1, \xi_2, \cdots, \xi_\nu)$ ανήκει στο $\Lambda(I)$, άρα θα μηδενίζει κάθε πολυωνυμικό συνδυασμό

   $$\begin{aligned} g(x_1, x_2, \cdots, x_\nu) \ = \ & h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) \ + \\ & h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) \ + \\ & \cdots \ + \\ & h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu) \end{aligned}$$

   Τώρα αν διαλέξουμε $h_1(x_1, x_2, \cdots, x_\nu) = 1$ και $h_i(x_1, x_2, \cdots, x_\nu) = \mathbf{0}, i = 2, 3, \cdots \mu$, έχουμε ότι το πολυώνυμο $f_1(x_1, x_2, \cdots, x_\nu)$ είναι πολυωνυμικός συνδυασμός και ομοίως και τα άλλα πολυώνυμα, άρα και τα πολυώνυμα του συστήματος είναι πολυωνυμικοί συνδυασμοί, άρα στοιχεία του ιδεώδους I, άρα $(\xi_1, \xi_2, \cdots, \xi_\nu)$ ανήκει στο I και τελικά $\Lambda = \Lambda(I)$.

3. *Δείτε εδώ το βίντεο. Το βίντεο αυτό συζητάει τις ιδέες που θα δείτε παρακάτω.*

4. *Στην πραγματικότητα δεν μας ενδιαφέρουν τα πολυώνυμα του συστήματος, αλλά το σύνολο λύσεων του συστήματος αυτού. Η βασική ιδέα, λοιπόν είναι να χρησιμοποιήσουμε το ιδεώδες, που παράγεται από τα πολυώνυμα του συστήματος, αφού ισχύει ότι $\Lambda = \Lambda(I)$. Όμως εδώ θα παρατηρούσε κανείς ότι είναι σαν να αντικαθιστούμε το σύστημα μ-πολυωνυμικών εξισώσεων με ένα σύστημα απείρων πολυωνυμικών εξισώσεων, διότι το ιδεώδες έχει άπειρα πολυώνυμα. Αυτό είναι ένα πρόβλημα. Το μόνο που κερδίζουμε από τη μετάβαση αυτή είναι ότι το ιδεώδες είναι ένα οργανωμένο σύνολο, έχει δηλαδή όπως λέμε στην άλγεβρα μία δομή. Ας θυμηθούμε εδώ τον ορισμό του ιδεώδους:*

   Ορισμός 3.3.1. *Έστω R ένας δακτύλιος. Το υποσύνολο I του R, λέγεται ιδεώδες του R και συμβολίζουμε $I \lhd R$ εάν*

   (i) Το μηδενικό στοιχείο του δακτυλίου R ανήκει στο I, δηλαδή $\mathbf{0} \in \mathbf{I}$

   (ii) Αν $\alpha, \beta \in I$, τότε $\alpha - \beta \in I$

   (iii) Αν $\alpha \in I$, $x \in R$ τότε[2] $x \cdot \alpha \in I$ και $\alpha \cdot x \in I$

5. **Βήματα στο βυθό του ιδεώδους :** *Αυτό που θα κάνουμε στα επόμενα είναι να επιλέξουμε ένα σύνολο πολυωνύμων*

   $$G = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\} \subseteq I$$

   με τις παρακάτω απαιτήσεις:

[2] Αν ο δακτύλιος είναι μεταθετικός, όπως ο δακτύλιος των πολυωνύμων, τότε στην τελευταία απαίτηση στον ορισμό του ιδεώδους,μπορούμε να έχουμε μόνο $\alpha \cdot x \in I$.

(i) *Τα πολυώνυμα αυτά να ανήκουν στο ιδεώδες I το παραγόμενο από τα πολυώνυμα $f_1(x_1,x_2,\cdots,x_\nu), f_2(x_1,x_2,\cdots,x_\nu),\cdots,f_\mu(x_1,x_2,\cdots,x_\nu)$*

(ii) *Το νέο σύστημα*

$$(\Sigma^\star)\left\{\begin{array}{rcl} g_1(x_1,x_2,...,x_\nu) & = & 0 \\ g_2(x_1,x_2,...,x_\nu) & = & 0 \\ & \vdots & \\ g_\kappa(x_1,x_2,...,x_\nu) & = & 0 \end{array}\right\}$$

έχει ως σύνολο λύσεων το $\Lambda(I)=\Lambda$, άρα αν λύσουμε το σύστημα $(\Sigma^\star)$ λύσαμε και το αρχικό.

(iii) *Το σύστημα $(\Sigma^\star)$ είναι πιο εύκολο να λυθεί και οι ιδιότητες του συνόλου λύσεων Λ είναι πιο διαφανείς.*

6. *Το σύνολο $G=\{g_1(x_1,x_2,\cdots,x_\nu), g_2(x_1,x_2,\cdots,x_\nu),\cdots,g_\kappa(x_1,x_2,\cdots,x_\nu)\}$ με τις ιδιότητες που περιγράψαμε θα το λέμε* **Βάση Groebner του ιδεώδους** *I*

7. *Αν I ένα ιδεώδες του δακτυλίου των πολυωνύμων $\mathbb{F}[x]$, διαφορετικό του μηδενικού ιδεώδους $\{\mathbf{0}\}$, τότε το I έχει πολλές βάσεις Groebner.*[3]*. Μία όμως βάση Groebner, όπως θα δούμε έχει τις πιο κατάλληλες ιδιότητες και επίσης είναι μοναδική. Την μοναδική αυτή βάση Groebner θα τη λέμε* **ανηγμένη βάση Groebner** *.*

8. *Δείτε γενικές πληροφορίες για τις βάσεις Groebner εδώ.*

9. *Δείτε εδώ επίσης μία σύντομη εισαγωγή από τον καθηγητή B. Buchberger , που ανακάλυψε το 1965 τις βάσεις Groebner.*

10. *Στα επόμενα μαθήματα θα κάνουμε πλήρεις αποδείξεις και για την ύπαρξη βάσεων Groebner και για τη σχέση μεταξύ τους και για την μοναδικότητα της ανηγμένης βάσης Groebner.*

3.4 Δεύτερο μέρος

Ας θυμηθούμε ξανά εδώ τον ορισμό του ιδεώδους σε ένα δακτύλιο

Ορισμός 3.4.1. *Έστω R ένας δακτύλιος και I ένα υποσύνολό του. Το I θα λέγεται* **ιδεώδες του** *R εάν*

1. *$I\neq\emptyset$ ή $\mathbf{0}\in\mathbf{I}$*
2. *Αν $\alpha,\beta\in I$, τότε και η διαφορά τους $\alpha-\beta$ ανήκει στο I*
3. *Αν $\alpha\in I$ και $r\in R$, τότε $r\cdot\alpha\in I$ και $\alpha\cdot r\in I$*

Δείτε τον ορισμό του ιδεώδους ενός δακτυλίου και εδώ .

Θα χρησιμοποιούμε πολύ τα ιδεώδη στο μάθημα αυτό. Ο λόγος αναλύθηκε στο προηγούμενο μάθημα. Αναφέρουμε ξανά εδώ ότι το ιδεώδες πολυωνύμων στον δακτύλιο πολυωνύμων $\mathbb{F}[x_1,x_2,\cdots,x_\nu]$ είναι ένα μέσο μετάβασης, μία γέφυρα από το σύστημα πολυωνυμικών εξισώσεων σε ένα άλλο σύστημα πολυωνυμικών εξισώσεων πιο εύκολο να λυθεί.

Αυτό δημιουργεί την ανάγκη για μία πιο βαθειά μελέτη των ιδεωδών στο δακτύλιο των πολυωνύμων $\mathbb{F}[x_1,x_2,\cdots,x_\nu]$.

[3] Συνδυάστε το αντίστοιχο γνωστό αποτέλεσμα από τη Γραμμική άλγεβρα : Αν V είναι ένας διανυσματικός χώρος και I ένας μη-μηδενικός υπόχωρος τότε ο I έχει πολλές βάσεις.

Βέβαια υπάρχουν και άλλα οργανωμένα υποσύνολα ενός δακτυλίου, των οποίων η μελέτη γίνεται αναγκαία ανάλογα με το ερώτημα, που μας απασχολεί.

Δίνουμε εδώ για πληρότητα και τον ορισμό του υποδακτυλίου. Μπορείτε να συνδυάσετε τον υποδακτύλιο ενός δακτυλίου με τον υπόχωρο ενός διανυσματικού χώρου όπως επίσης με την υποομάδα μίας ομάδας. Το ιδεώδες ενός δακτυλίου θα μπορούσαμε να πούμε ότι αντιστοιχεί με την κανονική υποομάδα μίας ομάδας.

Ορισμός 3.4.2. *Έστω R ένας δακτύλιος και S ένα υποσύνολό του. Το S θα λέγεται* **υποδακτύλιος του** *R εάν*

1. $S \neq \emptyset$
2. *Το S (με τον περιορισμό[4] των πράξεων του αρχικού δακτυλίου στο S) εξακολουθεί να είναι δακτύλιος.*

Δείτε επίσης τον ορισμό του υποδακτυλίου ενός δακτυλίου και εδώ.

3.5 Πολυωνυμικοί συνδυασμοί

Έστω $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$ ο δακτύλιος πολυωνύμων ν μεταβλητών με συντελεστές από το σώμα $\mathbb{F}$

1. *Έχοντας τα πολυώνυμα $f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu)$, για κάθε επιλογή πολυωνύμων $h_1(x_1, x_2, \cdots, x_\nu), h_2(x_1, x_2, \cdots, x_\nu), \cdots, h_\mu(x_1, x_2, \cdots, x_\nu) \in \mathbb{F}[x]$ κατασκευάζουμε το πολυώνυμο:*

   $$h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) + h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) + \cdots + h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu)$$

2. *Κάθε πολυώνυμο, όπως το προηγούμενο λέγεται* **πολυωνυμικός συνδυασμός** *των $f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu)$.*

3. **Πρόταση 3.5.1.** *Έστω $\{f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu)\}$ ένα σύνολο πολυωνύμων του δακτυλίου $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. Το σύνολο I των πολυωνυμικών συνδυασμών του παραπάνω συνόλου είναι ένα ιδεώδες.*

   Απόδειξη *Αν επιλέξουμε $h_1(x_1, x_2, \cdots, x_\nu) = h_2(x_1, x_2, \cdots, x_\nu) \cdots = h_\nu(x_1, x_2, \cdots, x_\nu) = \mathbf{0}$, τότε βρίσκουμε ότι το μηδενικό πολυώνυμο $\mathbf{0}$ ανήκει στο I.*

   Ας θεωρήσουμε δύο πολυωνυμικούς συνδυασμούς:

   $$h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) + h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) + \cdots + h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu)$$

   και

   $$\xi_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) + \xi_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) + \cdots + \xi_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu)$$

   Αυτή τη μορφή έχουν δύο στοιχεία του I. Αν προσθέσουμε τα στοιχεία αυτά θα βρούμε:

[4] Μην ξεχνάμε ότι πράξη σε ένα σύνολο R είναι μία συνάρτηση $R \times R \longrightarrow R$, οπότε δικαιολογείται η λέξη περιορισμός στο S.

$(h_1(x_1,x_2,\cdots,x_\nu)+\xi_1(x_1,x_2,\cdots,x_\nu))\cdot f_1(x_1,x_2,\cdots,x_\nu)+$
$(h_2(x_1,x_2,\cdots,x_\nu)+\xi_2(x_1,x_2,\cdots,x_\nu))\cdot f_2(x_1,x_2,\cdots,x_\nu)+\cdots+$
$(h_\mu(x_1,x_2,\cdots,x_\nu)+\xi_\mu(x_1,x_2,\cdots,x_\nu))\cdot f_\mu(x_1,x_2,\cdots,x_\nu)$

Παρατηρούμε, λοιπόν, ότι το άθροισμα δύο οποιωνδήποτε στοιχείων του I ανήκει στο I.

Έστω $h_1(x_1,x_2,\cdots,x_\nu)\cdot f_1(x_1,x_2,\cdots,x_\nu)+h_2(x_1,x_2,\cdots,x_\nu)\cdot f_2(x_1,x_2,\cdots,x_\nu)+\cdots+h_\mu(x_1,x_2,\cdots,x_\nu)\cdot f_\mu(x_1,x_2,\cdots,x_\nu)$ ένα στοιχείο του I και $g(x_1,x_2,\cdots,x_\nu)$ ένα οποιοδήποτε στοιχείο του δακτυλίου $\mathbb{F}[x_1,x_2,\cdots,x_\nu]$.

Πολλαπλασιάζοντας έχουμε:

$\{g(x_1,x_2,\cdots,x_\nu)\cdot h_1(x_1,x_2,\cdots,x_\nu)\}\cdot f_1(x_1,x_2,\cdots,x_\nu)+\{g(x_1,x_2,\cdots,x_\nu)\cdot h_2(x_1,x_2,\cdots,x_\nu)\}\cdot f_2(x_1,x_2,\cdots,x_\nu)+\cdots+\{g(x_1,x_2,\cdots,x_\nu)h_\mu(x_1,x_2,\cdots,x_\nu)\}\cdot f_\mu(x_1,x_2,\cdots,x_\nu)$

Καταλήγουμε και εδώ σε ένα πολυωνυμικό συνδυασμό και αφού το I ικανοποιεί και τα τρία κριτήρια είναι ιδεώδες.

4. **Σχόλια**

   (i) *Το ιδεώδες I, όπως παραπάνω, θα το λέμε ιδεώδες παραγόμενο από το σύνολο $\{f_1(x_1,x_2,\cdots,x_\nu),f_2(x_1,x_2,\cdots,x_\nu),\cdots,f_\mu(x_1,x_2,\cdots,x_\nu)\}$ και θα συμβολίζουμε με $<\{f_1(x_1,x_2,\cdots,x_\nu),f_2(x_1,x_2,\cdots,x_\nu),\cdots,f_\mu(x_1,x_2,\cdots,x_\nu)\}>$*

   (ii) *Αξίζει να σημειωθεί ότι ένας πολυωνυμικός συνδυασμός είναι πάντα ένα* **πεπερασμένο** *άθροισμα. Δεν έχει νόημα εδώ άπειρο άθροισμα.*

   (iii) *Μπορούμε να θεωρήσουμε ένα άπειρο σύνολο πολυωνύμων A και να ορίσουμε το σύνολο $<A>$ ως το σύνολο όλων (των πεπερασμένων φυσικά) πολυωνυμικών συνδυασμών στοιχείων του Α. Αυτό σημαίνει ότι από το σύνολο Α επιλέγουμε κάθε φορά αυθαίρετα πεπερασμένα στοιχεία του και σχηματίζουμε τους πολυωνυμικούς συνδυασμούς μετά. Το σύνολο των πολυωνυμικών συνδυασμών όπως παραπάνω σχηματίζει[5] το ιδεώδες $<A>$.*

   (iv) *Αν το σύνολο Α είναι πεπερασμένο θα λέμε ότι το ιδεώδες I είναι* **πεπερασμένα παραγόμενο**.

3.6 Βάσεις Groebner

Όπως είπαμε παραπάνω αν έχουμε να λύσουμε ένα σύστημα (Σ), το 3.1 , το οποίο αποτελείται από μ πολυωνυμικές εξισώσεις με ν μεταβλητές, ορίζουμε το σύνολο λύσεων $\Lambda(\Sigma)$. Αυτό το σύνολο είναι το πρωταρχικό που μας ενδιαφέρει.

1. *Θεωρούμε το ιδεώδες $<\{f_1(x_1,x_2,\cdots,x_\nu),f_2(x_1,x_2,\cdots,x_\nu),\cdots,f_\mu(x_1,x_2,\cdots,x_\nu)\}>$, το παραγόμενο από τα πολυώνυμα του συστήματος.*

2. *Όπως αποδείξαμε σε άλλο μάθημα (δες 2) το σύνολο λύσεων $\Lambda(\Sigma)$ είναι ίσο με το σύνολο λύσεων $\Lambda(I)$.*

3. *Τώρα το ιδεώδες I, που κατασκευάσαμε περιέχει άπειρα πολυώνυμα.*

4. *Έχοντας επιλέξει μία λεξικογραφική διάταξη, σε κάθε πολυώνυμο $f(x_1,x_2,\cdots,x_\nu)$ που ανήκει στο I επισυνάπτουμε τον* **μεγιστοβάθμιο όρο του** .

[5] Με τον ίδιο ακριβώς τρόπο αντιμετωπίζεται η έννοια *υπόχωρος παραγόμενος από ένα άπειρο υποσύνολο ενός διανυσματικού χώρου*

5. *Το σύνολο όλων των μεγιστοβαθμίων όρων των πολυωνύμων του I το συμβολίζουμε $MO(I)$, δηλαδή $MO(I) = \{x_1^{\kappa_1} x_2^{\kappa_2} \cdots x_\nu^{\kappa_\nu}$, όπου $x_1^{\kappa_1} x_2^{\kappa_2} \cdots x_\nu^{\kappa_\nu}$ μεγιστοβάθμιος όρος κάποιου πολυωνύμου του I $\}$.*

6. *Σημειώνουμε εδώ ότι τα στοιχεία του $MO(I)$ είναι* **μονώνυμα πολλών μεταβλητών** *και προφανώς υπάρχουν άπειρα τέτοια μονώνυμα στο $MO(I)$.*

7. *Θεωρούμε το ιδεώδες $< MO(I) >$ που παράγεται από όλα τα μονώνυμα του συνόλου $MO(I)$.*

8.

   Θεώρημα 3.6.1. *Για κάθε ιδεώδες $I \neq \mathbf{0}$ του δακτυλίου $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$, υπάρχει πεπερασμένο πλήθος μονωνύμων του I, το σύνολο $B = \{x_1^{\lambda_{i_1}} x_2^{\lambda_{i_2}} \cdots x_\nu^{\lambda_{i_\nu}}, i = 1, 2, \cdots, \kappa\}$ με την ιδιότητα $< B >=< MO(I) >$*

   Απόδειξη: *Θα γίνει σε επόμενο μάθημα.*

   (i) *Το παραπάνω θεώρημα μας λέει ότι αρκεί πεπερασμένο πλήθος μονονύμων για να παράγει το ιδεώδες $< MO(I) >$*

   (ii) *Κάθε μονώνυμο του B είναι μεγιστοβάθμιος όρος κάποιου πολυωνύμου του ιδεώδους I, έχουμε δηλαδή $x_1^{\lambda_{i_1}} x_2^{\lambda_{i_2}} \cdots x_\nu^{\lambda_{i_\nu}}$ είναι μεγιστοβάθμιος όρος του πολυωνύμου $g_i(x_1, x_2, \cdots, x_\nu) \in I$.*

   (iii) *Τα πολυώνυμα $g_i(x_1, x_2, \cdots, x_\nu) \in I$ δεν είναι μοναδικά, ενδέχεται δηλαδή να υπάρχουν πολλά πολυώνυμα του I με τον ίδιο μεγιστοβάθμιο όρο.*

   (iv) *Το πεπερασμένο σύνολο πολυωνύμων $G = \{g_i(x_1, x_2, \cdots, x_\nu), i = 1, 2, \cdots, \kappa\}$ είναι ένα πεπερασμένο σύνολο πολυωνύμων του I και λέγεται* ***βάση Groebner*** *του ιδεώδους I.*

9. *Όπως είπαμε και στο προηγούμενο μάθημα μεταξύ πολλών βάσεων Groebner του ιδεώδους I υπάρχει (με κάποιες απαιτήσεις) μία μοναδική* **ανηγμένη βάση Groebner** *. Συνήθως, όπως επίσης είπαμε, τα συστήματα, όπως το AXIOM υπολογίζουν την ανηγμένη βάση Groebner.*

10. *Μία από τις σημαντικές ιδιότητες των βάσων Groebner που θα αποδείξουμε σε επόμενο μάθημα είναι ότι το σύνολο λύσεων $\Lambda(\Sigma)$ του αρχικού συστήματος, που ξεκινήσαμε είναι ίσο με το σύνολο λύσεων του πολυωνυμικού συστήματος που σχηματίζεται με τα πολυώνυμα της βάσης Groebner. Το τελευταίο σύστημα είναι η πιο απλή μορφή του αρχικού συστήματος.*

- *Σκεφθείτε τα ιδεώδη στους δακτυλίους πολυωνύμων μίας μεταβλητής και βρείτε βάση Groebner χρησιμοποιώντας την παραπάνω συζήτηση.*
- *Σκεφθείτε το ιδεώδες που παράγεται από τα $3x + 5y$ και $x + y$ στον δακτύλιο $\mathbb{R}[x, y]$. Περιγράψτε τα στοιχεία του ιδεώδους και βρείτε μία βάση Groebner του ιδεώδους.*
- *Μελετήστε τις εντολές του AXIOM για εύρεση βάσεων Groebner.*
- *Δείτε εδώ για παραπάνω σκέψη.*
- *Δείτε το βίντεο[6] εδώ πάνω στις βάσεις Groebner.*
- *Ακόμη ένα βίντεο με εικόνα υψηλής ποιότητας πάνω στις βάσεις Groebner εδώ.*

[6] Βίντεο με εικόνα υψηλής ποιότητας.

3.7 Τρίτο μέρος

Επαναλαμβάνουμε τον ορισμό μίας βάσης Groebner ενός ιδεώδους $I \triangleleft \mathbb{F}[x_1, x_2, \cdots, x_\nu]$.

Ορισμός 3.7.1. *Έστω* I *ένα μη μηδενικό ιδεώδες του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. **Βάση Groebner** *του ιδεώδους* I *λέγεται ένα πεπερασμένο σύνολο πολυωνύμων* $G = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ *του* I *με την ιδιότητα* $< MO(I) >=< MO(g_1), MO(g_2), \cdots, MO(g_\kappa) >$.

1. *Υπενθυμίζουμε εδώ από το προηγούμενο μάθημα ότι το σύνολο όλων των μεγιστοβαθμίων όρων των πολυωνύμων του I το συμβολίζουμε* $MO(I)$, *δηλαδή*

   $MO(I) = \{x_1^{\kappa_1} x_2^{\kappa_2} \cdots x_\nu^{\kappa_\nu}$, *όπου* $x_1^{\kappa_1} x_2^{\kappa_2} \cdots x_\nu^{\kappa_\nu}$ *μεγιστοβάθμιος όρος κάποιου πολυωνύμου του I* $\}$

   Σημειώνουμε επίσης ότι τα στοιχεία του $MO(I)$ *είναι* **μονώνυμα πολλών μεταβλητών** *και προφανώς υπάρχουν άπειρα τέτοια μονώνυμα στο* $MO(I)$. *Το ιδεώδες* $< MO(I) >$ *παράγεται από όλα τα μονώνυμα του συνόλου* $MO(I)$.

2. *Το ιδεώδες* $< MO(g_1), MO(g_2), \cdots, MO(g_\kappa) >$ *παράγεται από τα μονώνυμα που είναι μεγιστοβάθμιοι όροι των πολυωνύμων* $g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)$.

3. *Δείτε στο σημείο αυτό το βίντεο για περισσότερες πληροφορίες.*

3.8 Η περίπτωση του δακτυλίου πολυωνύμων μίας μεταβλητής

Πριν αρχίσετε τη μελέτη της παραγράφου αυτής δείτε το βίντεο.

Έστω $\mathbb{F}[x]$ *ο δακτύλιος των πολυωνύμων μίας μεταβλητής με συντελεστές από το σώμα* $\mathbb{F}$. *Αν* I *ένα μη μηδενικό ιδεώδες, τότε γνωρίζουμε από τη Βασική Άλγεβρα ότι σε κάθε μη μηδενικό πολυώνυμο αυτού επισυνάπτεται βαθμός. Ο βαθμός ενός πολυωνύμου είναι ένας μη-αρνητικός ακέραιος. Μεταξύ όλων των μη αρνητικών ακεραίων που εμφανίζονται ως βαθμοί πολυωνύμων του* I *υπάρχει, σύμφωνα με την αρχή του ελαχίστου, ελάχιστος. Αυτό σημαίνει ότι στο μη μηδενικό ιδεώδες* I *υπάρχει πολυώνυμο , έστω* $f(x)$ *ελαχίστου βαθμού. Έστω τώρα* $h(x)$ *ένα πολυώνυμο του ιδεώδους* I. *Κάνουμε τη διαίρεση του* $h(x)$ *δια του* $f(x)$. *Απο τον αλγόριθμο της διαίρεσης έχουμε*

$$h(x) = f(x) \cdot \pi(x) + \upsilon(x)$$

Αν το $\upsilon(x)$ *είναι το μηδενικό πολυώνυμο, τότε το* $h(x)$ *θα είναι ένα πολλαπλάσιο του* $f(x)$. *Αν το* $\upsilon(x)$ *είναι διαφορετικό από το μηδενικό πολυώνυμο, τότε έχουμε* $h(x) - f(x) \cdot \pi(x) = \upsilon(x)$. *Από τον ορισμό του ιδεώδους βρίσκουμε ότι* $\upsilon(x) \in I$ *κάτι που οδηγεί σε άτοπο, διότι το υπόλοιπο εξ ορισμού έχει βαθμό μικρότερο από το διαιρέτη.*

Συμπέρασμα *Κάθε μη μηδενικό ιδεώδες* I *του* $\mathbb{F}[x]$ *έχει ένα πολυώνυμο* $f(x)$ *ελαχίστου βαθμού. Κάθε άλλο πολυώνυμο* $h(x)$ *του* I *είναι πολλαπλάσιο του* $f(x)$, *δηλαδή* $I =< f(x) >$.

Στην περίπτωση αυτή λέμε ότι το I *είναι* **κύριο ιδεώδες** *και επίσης ο δακτύλιος* $\mathbb{F}[x]$ *είναι δακτύλιος κυρίων ιδεωδών.*

Εφαρμόζουμε τώρα τη διαδικασία για να βρούμε κάποια βάση Groebner του I.

1. *Οι μεγιστοβάθμιοι όροι πολυωνύμων του* I *είναι δυνάμεις του* x. *Οι δυνάμεις αυτές του* x, *θα σχηματίζουν το σύνολο* $MO(I) = \{x^\kappa$, *όπου* x^κ *μεγιστοβάθμιος όρος κάποιου πολυωνύμου του* $I\}$.

2. *Θεωρούμε το ιδεώδες του $\mathbb{F}[x]$ που παράγεται από το $MO(I)$ και την ελάχιστη δύναμη του x που βρίσκεται στο $MO(I)$, έστω x^ν. Θα αποδείξουμε ότι $< MO(I) >=< x^\nu >$.*

3. *Πράγματι αφού ο ακέραιος ν είναι ελάχιστος, έχουμε ότι για κάθε $x^\xi \in < MO(I) >$ ισχύει $x^\xi = x^\nu \cdot x^{\xi-\nu} \in < x^\nu >$ και έτσι $< MO(I) > \subseteq < x^\nu >$. Από την άλλη μεριά το $< x^\nu >$ ανήκει εξ ορισμού στο $< MO(I) >$ και τελικά έχουμε $< MO(I) >=< x^\nu >$.*

4. *Φθάσαμε, λοιπόν, σε θέση να βρούμε βάσεις Groebner. Έχουμε την απαραίτητη συνθήκη $< MO(I) > \subseteq < x^\nu >$. Αρκεί να βρούμε ένα πολυώνυμο με μεγιστοβάθμιο όρο το $< x^\nu >$. Όμως από την προηγούμενη ανάλυση ένα πολυώνυμο με μεγιστοβάθμιο όρο αυτό είναι το $f(x)$ ελαχίστου βαθμού, που παράγει το I. Τελικά μία βάση Groebner (διότι δεν είναι μοναδική), είναι το σύνολο $\{f(x)\}$.*

Συμπέρασμα: *Κάθε μη-μηδενικό ιδεώδες I του $\mathbb{F}[x]$ έχει (τουλάχιστον μία) βάση Groebner. Μία από αυτές είναι το σύνολο $\{f(x)\}$, όπου $f(x)$ πολυώνυμο ελαχίστου βαθμού του I.*

3.9 Η περίπτωση του δακτυλίου πολυωνύμων δύο μεταβλητών

Δείτε εδώ το παρακάτω βίντεο πριν από τη μελέτη του κεφαλαίου. Έστω τώρα ο δακτύλιος $\mathbb{F}[x,y]$ των πολυωνύμων δύο μεταβλητών με συντελεστές από το σώμα $\mathbb{F}$ και I ένα μη μηδενικό ιδεώδες του. Θέλουμε να αποδείξουμε ότι το I έχει (τουλάχιστον μία) βάση Groebner.

Θεωρούμε, λοιπόν όλα τα μονώνυμα του I. Αυτά είναι της μορφής $x^\kappa y^\lambda$ με $\kappa, \lambda \in \{0,1,2,3,\cdots\}$ Σχηματίζεται το σύνολο:

$$MO(I) = \{x^\kappa y^\lambda, \text{ όπου } x^\kappa y^\lambda \text{ μεγιστοβάθμιος όρος κάποιου πολυωνύμου του } I\}$$

Θα αποδείξουμε ότι το ιδεώδες $< MO(I) >$ είναι πεπερασμένα παραγόμενο.

Προς τούτο, το πρώτο που θα κάνουμε είναι να πάρουμε μία «προβολή» του ιδεώδους $< MO(I) >$ στον δακτύλιο πολυωνύμων $\mathbb{F}[x]$.

Θεωρούμε το ιδεώδες[7] : J =ιδεώδες του $\mathbb{F}[x]$, που παράγεται από όλα τα x^κ για τα οποία υπάρχει y^λ με $x^\kappa y^\lambda \in < MO(I) >$.

Σύμφωνα με το 3.8 το J είναι κύριο ιδεώδες άρα υπάρχει ακέραιος $\nu \in \{0,1,2,\cdots\}$ με $J =< x^\nu >$.

Για τον ακέραιο ν υπάρχει ακέραιος $\xi \in \{0,1,2,\cdots\}$ με $x^\nu y^\xi \in < MO(I) >$.

Μπορούμε εδώ να κάνουμε μία ενδιάμεση παρατήρηση ότι αν $x^\mu y^\rho \in MO(I)$ και $\rho \geq \xi$ τότε το $x^\nu y^\xi$ διαιρεί το $x^\mu y^\rho$, δηλαδή $x^\mu y^\rho = x^{\mu-\nu} y^{\rho-\xi} \cdot x^\mu y^\rho$[8].

Εδώ προκύπτει το ερώτημα: Τι θα κάνουμε αν $x^\mu y^\rho \in MO(I)$ και $\rho < \xi$;

1. *Για τον ακέραιο $\xi - 1$, θεωρούμε το ιδεώδες $J_{\xi-1}$ = ιδεώδες του $\mathbb{F}[x]$, που παράγεται από όλα τα x^κ με $x^\kappa y^{\xi-1} \in < MO(I) >$. Όμως ο δακτύλιος $\mathbb{F}[x]$ είναι δακτύλιος κυρίων ιδεωδών, άρα υπάρχει $\nu_{\xi-1} \in \{0,1,2,\cdots\}$ με $J_{\xi-1} =< x^{\nu_{\xi-1}} >$.*

[7] Σκεφθείτε ένα λόγο που δικαιολογεί τη λέξη «προβολή».

[8] Εδώ δηλαδή έχουμε ότι όλοι οι εκθέτες ανήκουν στο σύνολο $\{0,1,2,\cdots\}$ και το μόνο που έχουμε επι πλέον να αποδείξουμε είναι ότι $\mu \geq \nu$.

2. *Για τον ακέραιο $\xi-2$, θεωρούμε το ιδεώδες $J_{\xi-2}$ = ιδεώδες του $\mathbb{F}[x]$, που παράγεται από όλα τα x^κ με $x^\kappa y^{\xi-2} \in < MO(I) >$. Όμως ο δακτύλιος $\mathbb{F}[x]$ είναι δακτύλιος κυρίων ιδεωδών, άρα υπάρχει $\nu_{\xi-2} \in \{0,1,2,\cdots\}$ με $J_{\xi-2} =< x^{\nu_{\xi-2}} >$.*

3. $\cdots\cdots$

4. *Για τον ακέραιο 1, θεωρούμε το ιδεώδες J_1 = ιδεώδες του $\mathbb{F}[x]$, που παράγεται από όλα τα x^κ με $x^\kappa y^1 = x^\kappa y \in < MO(I) >$. Όμως ο δακτύλιος $\mathbb{F}[x]$ είναι δακτύλιος κυρίων ιδεωδών, άρα υπάρχει $\nu_1 \in \{0,1,2,\cdots\}$ με $J_1 =< x^{\nu_1} >$.*

5. *Για τον ακέραιο 0, θεωρούμε το ιδεώδες J_0 = ιδεώδες του $\mathbb{F}[x]$, που παράγεται από όλα τα x^κ με $x^\kappa y^0 = x^\kappa \in < MO(I) >$. Όμως ο δακτύλιος $\mathbb{F}[x]$ είναι δακτύλιος κυρίων ιδεωδών, άρα υπάρχει $\nu_0 \in \{0,1,2,\cdots\}$ με $J_0 =< x^{\nu_0} >$*

Θεώρημα 3.9.1. *Το μη μηδενικό ιδεώδες $< MO(I) >$ του δακτυλίου $\mathbb{F}[x,y]$ παράγεται από το παρακάτω* **πεπερασμένο** *σύνολο μονωνύμων*

$$\begin{array}{l} x^\nu y^\xi \\ x^{\nu_{\xi-1}} y^{\xi-1} \\ \cdots\cdots \\ x^{\nu_1} y \\ x^{\nu_0} \end{array}$$

Απόδειξη *Η απόδειξη θα γίνει σε επόμενο μάθημα.*

Θεώρημα 3.9.2. *Υπάρχουν πολυώνυμα $g_0(x,y), g_1(x,y), \cdots, g_\xi(x,y)$ τα οποία ανήκουν στο ιδεώδες I με την παρακάτω ιδιότητα:*

1. *Μεγιστοβάθμιος όρος του $g_0(x,y) = x^{\nu_0}$*

2. *Μεγιστοβάθμιος όρος του $g_1(x,y) = x^{\nu_1} y$*

3. *Μεγιστοβάθμιος όρος του $g_2(x,y) = x^{\nu_2} y^2$*

4. $\cdots\cdots$

5. *Μεγιστοβάθμιος όρος του $g_\xi(x,y) = x^\nu y^\xi$*

Πρόταση 3.9.3. *Το σύνολο πολυωνύμων $\{g_0(x,y), g_1(x,y), \cdots, g_\xi(x,y)\} \subseteq I$ είναι ένα πεπερασμένο υποσύνολο του I και ικανοποιεί τη σχέση*

$$< MO(I) >=< MO(g_0(x,y)), MO(g_1(x,y)), \cdots, MO(g_\xi(x,y)) >$$

και έτσι είναι μία βάση Groebner του I.

Απόδειξη *Προκύπτει από την προηγούμενη συζήτηση.*

4 Και άλλα για τις βάσεις Groebner

4.1 Γενικά

1. *Ας θυμηθούμε ξανά τον ορισμό της βάσης Groebner από το 3.7.1.*
2. *Σύμφωνα με το προηγούμενο μάθημα για κάθε μη-μηδενικό ιδεώδες* $I \triangleright \mathbb{F}[x_1, x_2, \cdots, x_\nu]$ *υπάρχει (τουλάχιστον μία) βάση Groebner.*
3. *Αν* I *ένα μη-μηδενικό ιδεώδες του* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$*, μία βάση Groebner αυτού είναι ένα σύνολο πολυωνύμων του* I*, το* $G = \{g_0(x_1, x_2, \cdots, x_\nu), g_1(x_1, x_2, \cdots, x_\nu), \cdots, g_\xi(x_1, x_2, \cdots, x_\nu)\}$ *με την ιδιότητα:*

$$< MO(I) >=< MO(g_0(x_1, x_2, \cdots, x_\nu)), MO(g_1(x_1, x_2, \cdots, x_\nu)), \cdots, MO(g_\xi(x_1, x_2, \cdots, x_\nu)) >$$

4.2 Ελαχιστοποιημένες και ανηγμένες βάσεις Groebner

Θεωρούμε ένα ιδεώδες I *του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$*, διαφορετικό από το τετριμμένο ιδεώδες* $\{\mathbf{0}\}$*. Τα βήματα για να συμπεράνουμε την ύπαρξη βάσης Groebner είναι τα παρακάτω:*

1. *Θεωρούμε το σύνολο* **όλων** *των πολυωνύμων του* I*.*
2. *Δηλώνουμε μία λεξικογραφική διάταξη στις μεταβλητές. Η διάταξη αυτή μας επιτρέπει να έχουμε διάταξη στα μονώνυμα των πολυωνύμων.*
3. *Θεωρούμε το σύνολο* $MO(I) = \{\lambda \cdot x_1^{\xi_1} x_2^{\xi_2} \cdots x_\nu^{\xi_\nu}$*, όπου* $\lambda \in \mathbb{F}, \lambda \neq 0$ *και* $\lambda \cdot x_1^{\xi_1} x_2^{\xi_2} \cdots x_\nu^{\xi_\nu}$ *μεγιστοβάθμιος όρος κάποιου πολυωνύμου του* $I\}$*.*
4. *Παρατηρούμε ότι το σύνολο* $MO(I)$ *είναι άπειρο. Θεωρούμε το ιδεώδες* $< MO(I) >$*, που παράγεται από αυτό το άπειρο σύνολο.*
5. *Σύμφωνα με το προηγούμο μάθημα το ιδεώδες* $< MO(I) >$ *είναι πεπερασμένα παραγόμενο, δηλαδή υπάρχουν μονώνυμα* $x_1^{\xi_{\lambda_{11}}} x_2^{\xi_{\lambda_{12}}} \cdots x_\nu^{\xi_{\lambda_{1\nu}}}, x_1^{\xi_{\lambda_{21}}} x_2^{\xi_{\lambda_{22}}} \cdots x_\nu^{\xi_{\lambda_{2\nu}}}, \cdots, x_1^{\xi_{\lambda_{\kappa 1}}} x_2^{\xi_{\lambda_{\kappa 2}}} \cdots x_\nu^{\xi_{\lambda_{\kappa\nu}}}$ *τα οποία εξακολουθούν να παράγουν το ιδεώδες*[1] $< MO(I) >$*.*
6. *Τα παραπάνω μονώνυμα είναι μεγιστοβάθμιοι όροι κάποιων πολυωνύμων του αρχικού ιδεώδους* I*. Έστω*

$$x_1^{\xi_{\lambda_{11}}} x_2^{\xi_{\lambda_{12}}} \cdots x_\nu^{\xi_{\lambda_{1\nu}}} = \text{μεγιστοβάθμιος όρος του πολυωνύμου } g_1(x_1, x_2, \cdots, x_\nu)$$
$$x_1^{\xi_{\lambda_{21}}} x_2^{\xi_{\lambda_{22}}} \cdots x_\nu^{\xi_{\lambda_{2\nu}}} = \text{μεγιστοβάθμιος όρος του πολυωνύμου } g_2(x_1, x_2, \cdots, x_\nu)$$
$$\cdots$$
$$x_1^{\xi_{\lambda_{\kappa 1}}} x_2^{\xi_{\lambda_{\kappa 2}}} \cdots x_\nu^{\xi_{\lambda_{\kappa\nu}}} = \text{μεγιστοβάθμιος όρος του πολυωνύμου } g_\kappa(x_1, x_2, \cdots, x_\nu)$$

7. *Τα πολυώνυμα* $g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), g_\kappa(x_1, x_2, \cdots, x_\nu)$ *ανήκουν στο ιδεώδες* I*.*

[1] Οι συντελεστές των μονωνύμων δεν παίζουν ρόλο, λόγω των ιδιοτήτων του ιδεώδους. Σκεφθείτε γιατί.

8. *Το σύνολο των πολυωνύμων*

$$G = \{g_1(x_1, x_2, \ldots, x_\nu), g_2(x_1, x_2, \ldots, x_\nu), \ldots, g_\kappa(x_1, x_2, \ldots, x_\nu)\}$$

ονομάζεται **βάση Groebner** *του ιδεώδους* I.

9. *Σύμφωνα με τα προηγούμενα δεν προκύπτει από τον ορισμό ότι έχουμε μοναδική βάση Groebner . Και αυτό είναι σωστό, ότι γενικά ένα ιδεώδες έχει πολλές βάσεις Groebner .*

10. **Σημαντική παρατήρηση ξανά**: *Η κρίσιμη ιδιότητα για να είναι ένα σύνολο πολυωνύμων* $\{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ *βάση Groebner του ιδεώδους* I, *είναι:*

$$< MO(I) >=< MO(g_1(x_1, x_2, \cdots, x_\nu), MO(g_2(x_1, x_2, \cdots, x_\nu), \cdots, MO(g_\kappa(x_1, x_2, \cdots, x_\nu) >$$[2]

11. *Είναι φανερό από τα προηγούμενα ότι εάν*

$$MO(g_1(x_1, x_2, \cdots, x_\nu) \in < MO(g_2(x_1, x_2, \cdots, x_\nu), \cdots, MO(g_\kappa(x_1, x_2, \cdots, x_\nu) >$$

τότε μπορούμε να διαγράψουμε το πολυώνυμο $g_1(x_1, x_2, \cdots, x_\nu)$ *και να έχουμε μία νέα βάση Groebner το σύνολο*

$$G = \{g_2(x_1, x_2, \cdots, x_\nu), g_3(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\}$$

Για το λόγο αυτό δίνουμε τον παρακάτω ορισμό:

12.

Ορισμός 4.2.1. *Έστω* $I \lhd \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, *δηλαδή το* I *είναι ιδεώδες του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. *Το (πεπερασμένο) υποσύνολο* $G = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ *του* I, *ονομάζεται* **ελαχιστοποιημένη** *(minimal)* **βάση Groebner** *του ιδεώδους* I, *εάν*

(i) Όλοι οι συντελεστές των μεγιστοβαθμίων όρων των πολυωνύμων του συνόλου G *είναι* 1

(ii) Για κάθε $i \in \{1, 2, \cdots, \kappa\}$ *έχουμε ότι ο μεγιστοβάθμιος όρος του πολυωνύμου* $g_i(x_1, x_2, \cdots, x_\nu)$ *δεν ανήκει στο ιδεώδες που παράγουν οι υπόλοιποι μεγιστοβάθμιοι όροι, δηλαδή*

$$MO(g_i) \notin < MO(g_1), MO(g_2), \cdots, MO(g_{i-1}), MO(g_{i+1}), \cdots, MO(g_\kappa) >$$

13. *Από κάθε βάση Groebner του ιδεώδους* I, *μπορούμε να καταλήξουμε σε μία ελαχιστοποιημένη βάση Groebner του ιδεώδους* I, *αφαιρώντας όλα τα πολυώνυμα που δεν χρειάζονται*[3]. *Αλλά ούτε και η ελαχιστοποιημένη βάση Groebner είναι μοναδική σε ένα ιδεώδες.*

14.

Ορισμός 4.2.2. *Έστω* $I \lhd \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, *δηλαδή το* I *είναι ιδεώδες του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. *Το (πεπερασμένο) υποσύνολο* $G = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ *του* I, *ονομάζεται* **ανηγμένη** *(reduced)* **βάση Groebner** *του ιδεώδους* I, *εάν*

(i) Όλοι οι συντελεστές των μεγιστοβαθμίων όρων των πολυωνύμων του συνόλου G *είναι 1 (όπως και στην ελαχιστοποιημένη βάση Groebner)*

[2] Με MO(φ) θα συμβολίζουμε το μεγιστοβάθμιο όρο του πολυωνύμου φ

[3] Γράψτε έναν αλγόριθμο για αυτό.

(ii) Για κάθε $i \in \{1,2,\cdots,\kappa\}$ έχουμε ότι κανένας όρος του πολυωνύμου $g_i(x_1,x_2,\cdots,x_\nu)$ (όχι μόνο ο μεγιστοβάθμιος όπως στην ελαχιστοποιημένη βάση) δεν ανήκει στο ιδεώδες που παράγουν οι υπόλοιποι μεγιστοβάθμιοι όροι, δηλαδή

$$Ορος(g_i) \notin < MO(g_1), MO(g_2), \cdots, MO(g_{i-1}), MO(g_{i+1}), \cdots, MO(g_\kappa) >$$

15. Το σημαντικό εδώ είναι το παρακάτω:

Θεώρημα 4.2.3. *Έστω I ιδεώδες του δακτυλίου $\mathbb{F}[x_1,x_2,\cdots,x_\nu]$, με $I \neq \{\mathbf{0}\}$. Τότε το I έχει μία μοναδική ανηγμένη βάση Groebner .*

Απόδειξη *Η απόδειξη θα γίνει προσεχώς.*

4.3 Ταυτότητες στο Γυμνάσιο-Λύκειο

Συνήθως στο Γυμνάσιο και στο Λύκειο μας δίνουν να λύσουμε κάποιες ασκήσεις που έχουν κάποιες υποθέσεις και μας ζητούν να καταλήξουμε σε κάποιο συμπέρασμα. Τις περισσότερες φορές οι υποθέσεις είναι σχέσεις πολυωνυμικού τύπου, έστω $f_1(x_1,\cdots,x_\nu)=0, f_2(x_1,\cdots,x_\nu)=0,\cdots,f_\mu(x_1,\cdots,x_\nu)=0$ και μας ζητούν να αποδείξουμε αν ισχύει η σχέση $g(x_1,\cdots,x_\nu)=0$ πολυωνυμικού τύπου και αυτή.

Μπορούμε να διατυπώσουμε το ερώτημά μας ως εξής:

Πρόταση 4.3.1. *Η σχέση $g(x_1,\cdots,x_\nu)=0$ προκύπτει από τις σχέσεις $f_1(x_1,\cdots,x_\nu)=0, f_2(x_1,\cdots,x_\nu)=0,\cdots,f_\mu(x_1,\cdots,x_\nu)=0$ εάν το πολυώνυμο $g(x_1,\cdots,x_\nu)$ ανήκει στο ιδεώδες*

$$< f_1(x_1,\cdots,x_\nu), f_2(x_1,\cdots,x_\nu),\cdots,f_\mu(x_1,\cdots,x_\nu) >$$

Απόδειξη. *Αν το πολυώνυμο $g(x_1,\cdots,x_\nu)$ ανήκει στο ιδεώδες $< f_1(x_1,\cdots,x_\nu), f_2(x_1,\cdots,x_\nu),\cdots, f_\mu(x_1,\cdots,x_\nu) >$, τότε το $g(x_1,\cdots,x_\nu)$ θα γράφεται ως πολυωνυμικός συνδυασμός των πολυωνύμων που παράγουν το ιδεώδες. Έχουμε δηλαδή ότι:*

$$\begin{aligned} g(x_1,\cdots,x_\nu) &= h_1(x_1,\cdots,x_\nu)\cdot f_1(x_1,\cdots,x_\nu) + h_2(x_1,\cdots,x_\nu)\cdot f_2(x_1,\cdots,x_\nu) + \cdots + \\ &\quad h_\mu(x_1,\cdots,x_\nu)\cdot f_\mu(x_1,\cdots,x_\nu) \end{aligned}$$

Αν τώρα οι δεδομένες σχέσεις ισχύουν, αν δηλαδή $f_1(x_1,\cdots,x_\nu)=0, f_2(x_1,\cdots,x_\nu)=0,\cdots, f_\mu(x_1,\cdots,x_\nu)=0$, τότε μηδενίζεται και το $g(x_1,\cdots,x_\nu)$ δηλαδή ισχύει και η σχέση $g(x_1,\cdots,x_\nu)=0$.

Προχωράμε τώρα σε ένα παράδειγμα:

Παράδειγμα 4.3.2. *Έστω ότι οι αριθμοί α,β,γ ικανοποιούν τις σχέσεις:*

$$\begin{aligned} \alpha+\beta+\gamma &= 3 \\ \alpha^2+\beta^2+\gamma^2 &= 5 \\ \alpha^3+\beta^3+\gamma^3 &= 7 \end{aligned}$$

Να αποδείξετε ότι $\alpha^4+\beta^4+\gamma^4=9$.

Απόδειξη. *Για να αποδείξουμε αυτό που μας ζητάνε στο παράδειγμα κάνουμε τα παρακάτω:*

1. *Παρατηρούμε ότι οι δεδομένες σχέσεις είναι πολυωνυμικού τύπου μεταξύ των* α, β, γ

2. *Θεωρούμε τα πολυώνυμα*
   $f_1(\alpha,\beta,\gamma) = \alpha + \beta + \gamma - 3,$
   $f_2(\alpha,\beta,\gamma) = \alpha^2 + \beta^2 + \gamma^2 - 5,$
   $f_3(\alpha,\beta,\gamma) = \alpha^3 + \beta^3 + \gamma^3 - 7$

3. *Θεωρούμε το ιδεώδες* $I =< f_1(\alpha,\beta,\gamma), f_2(\alpha,\beta,\gamma), f_3(\alpha,\beta,\gamma) >.$

4. *Βρίσκουμε μία βάση Groebner G του ιδεώδους* I.

5. *Διαιρούμε το πολυώνυμο* $h(\alpha,\beta,\gamma) = \alpha^4 + \beta^4 + \gamma^4 - 9$ *με τα πολυώνυμα της βάσης Groebner G. Το αποτέλεσμα, που βρίσκουμε είναι μηδέν*[4].

6. *Στηριζόμενοι στα επιχειρήματα της πρότασης παραπάνω καταλήγουμε στην απόδειξη αυτού που θέλουμε να αποδείξουμε.*

Σχόλιο: *Στην περίπτωση που δεν ξέραμε πόσο κάνει το άθροισμα* $\alpha^4 + \beta^4 + \gamma^4$ *αν διαιρέσουμε το πολυώνυμο* $\alpha^4 + \beta^4 + \gamma^4$ *με την βάση Groebner G θα βρούμε υπόλοιπο 9, οπότε στηριζόμενοι στα επιχειρήματα της πρότασης παραπάνω καταλήγουμε στην απόδειξη*[5] *ότι* $\alpha^4 + \beta^4 + \gamma^4 = 9$

4.4 Καί άλλα για πολυωνυμικές ταυτότητες

Στο θέμα των πολυωνυμικών ταυτοτήτων υπάρχει μεγάλη ποικιλία κατευθύνσεων, ερωτημάτων και αναπάντητων προβλημάτων.

1. **Θεώρημα Schwartz, Zippel** *Δείτε το Θεώρημα Schwartz, Zippel στη διεύθυνση εδώ. Σκεφθείτε ότι είναι μία «πιθανοθεωρητική προσέγγιση των πολυωνυμικών ταυτοτήτων».*

2. **Θεώρημα Tarski,Seidenberg** *Σημαντικό θεώρημα που διαπραγματεύεται εκτός από ισότητες και ανισότητες. Δείτε στην διεύθυνση εδώ.*

3. *Δείτε επίσης εδώ για τις λεγόμενες ταυτότητες του Νεύτωνα.*

4. *Δείτε επίσης εδώ για αποδείξεις του θεωρήματος Cayley-Hamilton.*

[4] Να το επιβεβαιώσετε και εσείς με όποιον τρόπο μπορείτε.
[5] Αποδείξτε το λεπτομερώς.