ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Υπολογιστική άλγεβρα

Ενότητα 7: Βάσεις Groebner I

Ράπτης Ευάγγελος

Σχολή Θετικών επιστημών

Τμήμα Μαθηματικών

Κεφάλαιο 7

Βάσεις Groebner I

Τετάρτη 21 Μαϊου 2014

7.1 Ιδεώδη μονονύμων

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

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

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

Ορισμός 7.1.1. *Έστω $F[x_1, x_2, ..., x_\nu]$ ο δακτύλιος των πολυωνύμων ν μεταβλητών, με συντελεστές από το σώμα F. Τότε θα καλούμε* ***ιδεώδες μονονύμων*** *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

- **(α)** Τα μονώνυμα που παράγουν το I ενδέχεται να είναι άπειρα.

- **(β)** Τα ιδεώδη μονονύμων στον δακτύλιο των πολυωνύμων μιας 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 μια μόνο μεταβλητή, δηλαδή ν=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 $A = I$.

- **(γ)** 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.

- **(δ)** 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 7.1.2. *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 ν=1 ισχύει (έχει αποδειχθεί προηγουμένως)

- Έστω ότι ισχύει για ν-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 7.1.3. *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 7.1.4. *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 7.1.5. *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 μια 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. Ειτε $\upsilon(x_1, x_2, ..., x_\nu) = 0$ ειτε $\upsilon \neq 0$ 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 ΥΠΑΡΧΕΙ μονώνυμο του υπολοίπου που να διαιρείται από κάποιο ΜΟ 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 μια διάταξη των μεταβλητών (π.χ. $x_1 > x_2 > ... > x_n$) η οποία επάγει μια 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 7.1.6. *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 υπάρχουν 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 $I =< x_1^{a_{i1}} x_2^{a_{i2}} \cdots x_\nu^{a_{i\nu}}, (\alpha_{i1}, ..., \alpha i1) \in A >$ 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. $\text{MO}(I) = \{\lambda \cdot x_1^{a1} x_2^{a2} ... x_\nu^{a_\nu} \mid$ 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 $I \neq < \{\varnothing\} >$.

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

Έχουμε δηλαδή μέχρι στιγμής την ακολουθία καταστάσεων

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

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

Παράδειγμα 7.1.8. *Έστω τα πολυώνυμα* $f_1(x,y) = x^3y - 2x^2y^2 + x$ *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 7.1.9. *(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 μια* ***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*
  - $\upsilon \in I$
  - *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* $i = 1, 2, ..., \kappa$. *ΑΤΟΠΟ.*

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 μια* ***βάση Groebner***

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

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

Παράδειγμα 7.1.10. *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* $x^2 = \alpha(x, y) \cdot x^2 + \beta(x, y) \cdot (x^2y)$*. ΑΤΟΠΟ. Άρα δεν είναι* ***βάση Groebner****.*

Παράδειγμα 7.1.11. *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 μια* ***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* $(f_1, f_2, ..., f_\nu)$ *μια 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 7.1.12. ***(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 μια ***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 μιας* ***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 $G = \{g_1, g_2, ..., g_\kappa\}$ μια ***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 διαφορα $\upsilon_1 - \upsilon_2$ αποτελεί συνδυασμό των $\{g_2, g_1, ..., g_\kappa\}$ και άρα έχουμε $\upsilon_1 - \upsilon_2 \in \langle g_2, g_1, ..., g_\kappa \rangle$. Αλλα το σύνολο $\{g_2, g_1, ..., g_\kappa\}$ είναι μια ***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 $g_2, g_1, ..., g_\kappa$. ΑΤΟΠΟ 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 :

- ***(α)*** *Ο αλγόριθμος βρίσκει μια* ***βάση Groebner***
- ***(β)*** *Διαιρούμε το f δια $\{g_2, g_1, ..., g_\kappa\}$*
- ***(γ)*** *$f \in I \Leftrightarrow$ το υπόλοιπο της διαίρεσης του f δια $\{g_2, g_1, ..., g_\kappa\}$ είναι 0.*
  (Στα (β) και (γ) δεν μας ενδιαφέρει η σειρά των $g_2, g_1, ..., g_\kappa$.)

Συμβολισμός
Το υπόλοιπο του $f \in F[x_1, ..., x_\nu]$ δια 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 7.1.13. *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 μια ***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 νιοστού 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 7.1.14. *Έστω $F[x_1,...,x_\nu]$ ο δακτύλιος των πολυωνύμων με ν μεταβητές, I ιδεώδες και $G = \{g_1, g_2, ..., g_\kappa\}$ μια* ***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 μια* ***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.

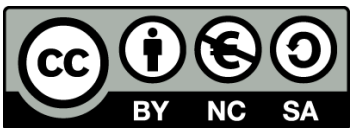
7.2 Ασκήσεις

1. *Να χρησιμοποιήσετε όποιο υπολογιστικό πακέτο θέλετε και να βρείτε μία βάση Groebner του ιδεώδους*
   $< f(x,y) = x^2 + (\alpha+1)xy + x, g(x,y) = (\beta+1)x^2 - x, h(x,y) = y - x >$
2. *Βρείτε μία βάση Groebner του ιδεώδους*
   $< (\alpha+\beta+1)x^5 - x, x^2 - 3x + 2 >$. *Είναι αναμενόμενο αυτό που βρήκατε;*
3. *Βρείτε μία βάση Groebner του ιδεώδους*
   $< (\alpha+1)x + 2y + 3z, (\beta+1)x + 5y + 6z, (\gamma+1)x + 8y + 9z >$
4. *Να σχολιάσετε τα ευρήματά σας στα ερωτήματα 1) 2) και 3)*

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης



[1] http://creativecommons.org/licenses/by-nc-sa/4.0/

Ως **Μη Εμπορική** ορίζεται η χρήση:

- που δεν περιλαμβάνει άμεσο ή έμμεσο οικονομικό όφελος από την χρήση του έργου, για το διανομέα του έργου και αδειοδόχο
- που δεν περιλαμβάνει οικονομική συναλλαγή ως προϋπόθεση για τη χρήση ή πρόσβαση στο έργο
- που δεν προσπορίζει στο διανομέα του έργου και αδειοδόχο έμμεσο οικονομικό όφελος (π.χ. διαφημίσεις) από την προβολή του έργου σε διαδικτυακό τόπο

Ο δικαιούχος μπορεί να παρέχει στον αδειοδόχο ξεχωριστή άδεια να χρησιμοποιεί το έργο για εμπορική χρήση, εφόσον αυτό του ζητηθεί.

Διατήρηση Σημειωμάτων

- Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:
- το Σημείωμα Αναφοράς
- το Σημείωμα Αδειοδότησης
- τη δήλωση Διατήρησης Σημειωμάτων
- το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει)

μαζί με τους συνοδευόμενους υπερσυνδέσμους.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στο πλαίσιο 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.