ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Υπολογιστική άλγεβρα

Ενότητα 11: Και άλλα για τις βάσεις Groebner

Ράπτης Ευάγγελος

Σχολή Θετικών επιστημών

Τμήμα Μαθηματικών

Κεφάλαιο 11

Και άλλα για τις βάσεις Groebner

Τετάρτη 4 Ιουνίου 2014

11.1 Γενικά

1. *Ας θυμηθούμε ξανά τον ορισμό της βάσης Groebner από το 10.1.1*

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

11.2 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*
   $x_1^{\xi_{\lambda_{11}}} x_2^{\xi_{\lambda_{12}}} \cdots x_\nu^{\xi_{\lambda_{1\nu}}}$ =*μεγιστοβάθμιος όρος του πολυωνύμου* $g_1(x_1, x_2, \cdots, x_\nu)$
   $x_1^{\xi_{\lambda_{21}}} x_2^{\xi_{\lambda_{22}}} \cdots x_\nu^{\xi_{\lambda_{2\nu}}}$ =*μεγιστοβάθμιος όρος του πολυωνύμου* $g_2(x_1, x_2, \cdots, x_\nu)$
   $\cdots$
   $x_1^{\xi_{\lambda_{\kappa 1}}} x_2^{\xi_{\lambda_{\kappa 2}}} \cdots x_\nu^{\xi_{\lambda_{\kappa\nu}}}$ =*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.*

8. *Το σύνολο των πολυωνύμων*

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

   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]

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

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

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*

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

Για το λόγο αυτό δίνουμε τον παρακάτω ορισμό:

12.

Ορισμός 11.2.1. *Έτσω* $I \lhd \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, *δηλαδή το* I *είναι ιδεώδες του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. *Το (πεπερασμένο) υποσύνύνολο* $G = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ *του* I, *ονομάζεται* **ελαχιστοποιημένη** *(minimal)* **βάση Groebner** *του ιδεώδους* I, *εάν*

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

(β΄) 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 11.2.2. *Έτσω* $I \lhd \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, *δηλαδή το* I *είναι ιδεώδες του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. *Το (πεπερασμένο) υποσύνύνολο* $G = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ *του* I, *ονομάζεται* **ανηγμένη** *(reduced)* **βάση Groebner** *του ιδεώδους* I, *εάν*

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

(β΄) 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*

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

[3]Γράψτε έναν αλγόριθμο για αυτό

15. *Το σημαντικό εδώ είναι το παρακάτω:*

Θεώρημα 11.2.3. *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*

11.3 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 11.3.1. *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:*

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

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 11.3.2. *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* $\alpha^4+\beta^4+\gamma^4 = 9$

11.4 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*

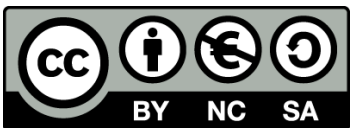
4. *Δείτε επίσης εδώ για αποδείξεις του θεωρήματος Cayley-Hamilton*

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

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης



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.