ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Υπολογιστική άλγεβρα

Ενότητα 8: Βάσεις Groebner ενός ιδεώδους Ι

Ράπτης Ευάγγελος

Σχολή Θετικών επιστημών

Τμήμα Μαθηματικών

Κεφάλαιο 8

Βάσεις Groebner ενός ιδεώδους. Επανάληψη

8.1 *Ξανά το σύστημα*

Ας επανέλθουμε τώρα στον αρχικό μας στόχο: Να λύσουμε το σύστημα 2.1 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:

$$(\mathbf{\Sigma_1}) \quad \left(\begin{array}{l} f_1(x) = 0 \\ f_2(x) = 0 \\ \cdots\cdots \\ f_\mu(x) = 0 \end{array} \right)$$

όπου τα πολυώνυμα $f_1(x), f_2(x), \cdots, f_\mu(x)$ είναι πολυώνυμα μιας 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*

[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

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* $\mathbf{\Lambda(\Sigma_1)}$ *το σύνολο λύσεων του συστήματος* $(\mathbf{\Sigma_1})$*, δηλαδή το σύνολο*

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

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

6. **Σημαντική παρατήρηση I:** *Αν* $\xi \in \mathbf{\Lambda(\Sigma_1)}$*, 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 $\mathbf{\Lambda(\Sigma_1)}$ *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* $\mathbf{\Lambda(\Sigma_1)}$ *του αρχικού συστήματος είναι ίσο με το σύνολο λύσεων* $\mathbf{\Lambda(\Sigma^\star)}$ *του συστήματος*

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

το οποίο προκύπτει δια διαγραφής του πολυωνύμου $f_1(x)$
Απόδειξη: *Έστω* $\xi \in \mathbf{\Lambda(\Sigma)}$*. 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* $\xi \in \mathbf{\Lambda(\Sigma^\star)}$ *και έτσι* $\mathbf{\Lambda(\Sigma)} \sqsubseteq \mathbf{\Lambda(\Sigma^\star)}$ *Αντίστροφα έστω* $\rho \in \mathbf{\Lambda(\Sigma^\star)}$*. 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* $\mathbf{\Lambda(\Sigma^\star)} \sqsubseteq \mathbf{\Lambda(\Sigma)}$*. Τελικά*

$$\mathbf{\Lambda(\Sigma^\star)} = \mathbf{\Lambda(\Sigma)}$$

8.

Πρόταση 8.1.1. *Έστω* $(\mathbf{\Sigma_1})$ $\begin{pmatrix} f_1(x) = 0 \\ f_2(x) = 0 \\ \cdots\cdots \\ f_\mu(x) = 0 \end{pmatrix}$

ένα σύστημα πολυωνυμικών εξισώσεων μιας 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* $\mathbf{\Lambda(\Sigma)}$ *του συστήματος είναι υποσύνολο του συνόλου λύσεων* $\mathbf{\Lambda(g)}$ *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 μιας 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* $\mathbf{\Lambda(\Sigma_1)}$ *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 8.1.2. *Έστω* $f_1(x), f_2(x), \cdots, f_\mu(x)$ *πολυώνυμα του δακτυλίου* $\mathbb{F}[x]$*, δηλαδή πολυώνυμα μιας 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;*

8.2 Ευρύτερη μελέτη

1. *Μελετήστε τα σχετικά με τα ιδεώδη στη σελίδα εδώ*

2. *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) 2.1 και Λ(I), το σύνολο λύσεων του συστήματος, που λαμβάνεται, αν πάρουμε τα (άπειρα) πολυώνυμα του I, τότε Λ=Λ(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:
$g(x_1, x_2, \cdots, x_\nu) = h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) + h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) + \cdots h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu)$ *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 Λ(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 Λ(I), άρα θα μηδενίζει κάθε πολυωνυμικό συνδυασμό* $g(x_1, x_2, \cdots, x_\nu) = h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) + h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) + \cdots h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu)$
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 I=Λ(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* **Λ=Λ(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 8.2.1. *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 $\mathbf{0} \in I$
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* $\alpha \cdot x \in I$

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

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:

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

(β′) Το νέο σύστημα

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

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

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

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] 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

8.3 Ασκήσεις

Τα α,β,γ είναι τα τρία τελευταία ψηφία του Αριθμού Μητρώου σας, αρχίζοντας από το τέλος.

1. *Να αποδείξετε λεπτομερώς χωρίς χρήση κάποιου υπολογιστικού πακέτου ότι μία βάση Groebner του ιδεώδους*

   $I =< f(x,y) = x^2 + (\alpha+1)xy + x, g(x,y) = (\beta+1)x^2 - x, h(x,y) = y - x >$ *του δακτυλίου* $\mathbb{R}[x,y]$ *είναι ένα πεπερασμένο σύνολο πολυωνύμων*

2. *Να βρείτε μία βάση Groebner G του παραπάνω ιδεώδους I. Εδώ μπορείτε να κάνετε χρήση κάποιου υπολογιστικού πακέτου, αρκεί να γράψετε ποιο είναι αυτό, ποιες εντολές δώσατε και τι σας επέστρεψε το πακέτο*

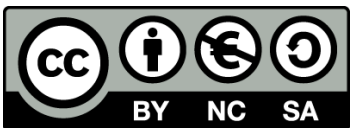
3. *Εξετάστε εάν ισχύει η πρόταση : Το πολυώνυμο* $\omega(x,y) \in \mathbb{R}[x,y]$ *ανήκει στο ιδεώδες I, εάν και μόνο εάν το υπόλοιπο της διαίρεσης του* $\omega(x,y)$ *με την βάση Groebner G είναι μηδέν. Οι αποδείξεις σας να είναι λεπτομερείς*

Τέλος του τετάρτου μαθήματος

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.