ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Υπολογιστική άλγεβρα

Ενότητα 9: Βάσεις Groebner ενός ιδεώδους II

Ράπτης Ευάγγελος

Σχολή Θετικών επιστημών

Τμήμα Μαθηματικών

Κεφάλαιο 9

Βάσεις Groebner ενός Ιδεώδους

9.1 Επαναλήψεις -σκέψεις -σχόλια

Τετάρτη 28 Μαΐου 2014

Ας θυμηθούμε ξανά εδώ τον ορισμό του ιδεώδους σε ένα δακτύλιο

Ορισμός 9.1.1. *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 μια πιο βαθειά μελέτη των ιδεωδών στο δακτύλιο των πολυωνύμων $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$*

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 μιας ομάδας. Το ιδεώδες ενός δακτυλίου θα μπορούσαμε να πούμε ότι αντιστοιχεί με την κανονική υποομάδα μιας ομάδας.

Ορισμός 9.1.2. *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[1] των πράξεων του αρχικού δακτυλίου στο S) εξακολουθεί να είναι δακτύλιος*

Δείτε επίσης τον ορισμό του υποδακτυλίου ενός δακτυλίου και *εδώ*

9.2 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 9.2.1. *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

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

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

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

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

Παρατηρούμε, λοιπόν, ότι το άθροισμα δύο οποιονδήποτε 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 του I

4. **Σχόλια**

   (α΄) *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*
   $< \{f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu)\} >$

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

   (γ΄) *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 A. Αυτό σημαίνει ότι από το σύνολο A επιλέγουμε κάθε φορά αυθαίρετα πεπερασμένα στοιχεία του και σχηματίζουμε τους πολυωνυμικούς συνδυασμούς μετά. Το σύνολο των πολυωνυμικών συνδυασμών όπως παραπάνω σηματίζει*[2] *το ιδεώδες* $< A >$.

   (δ΄) *Αν το σύνολο A είναι πεπερασμένο θα λέμε ότι το ιδεώδες I είναι* **πεπερασμένα παραγόμενο**

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

9.3 Βάσεις Groebner

Όπως είπαμε παραπάνω αν έχουμε να λύσουμε ένα σύστημα Σ, το 2.1 , το οποίο αποτελείται από μ πολυωνυμικές εξισώσεις με ν μεταβλητές, ορίζουμε το σύνολο λύσεων Λ(Σ). 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 πολύώνυμα του συστήματος*

2. *Όπως αποδείξαμε σε άλλο μάθημα (δες 2) το σύνολο λύσεων Λ(Σ) είναι ίσο με το σύνολο λύσεων Λ(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. *Το σύνολο ΟΛΩΝ 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 9.3.1. *Για κάθε ιδεώδες* $I \neq \mathbf{0}$ *του δακτυλίου* $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$, *υπάρχει πεπερασμένο πλήθος μονονύμων 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

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

   (β΄) *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*
   $g_i(x_1, x_2, \cdots, x_\nu) \in I$

(γ΄) *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*

(δ΄) *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*

9.4 Χαλαρή μελέτη χωρίς προθεσμίες

1. *Σκεφθείτε τα ιδεώδη στους δακτυλίους πολυωνύμων μιας μεταβλητής και βρείτε βάση Groebner χρησιμοποιώντας την παραπάνω συζήτηση*

2. *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*

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης

Διατήρηση Σημειωμάτων

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.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης