ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Υπολογιστική άλγεβρα

Ενότητα 10: Βάσεις Groebner ενός ιδεώδους ΙΙΙ

Ράπτης Ευάγγελος

Σχολή Θετικών επιστημών

Τμήμα Μαθηματικών

Κεφάλαιο 10

Βάσεις Groebner ενός ιδεώδους

10.1 Τρίτο μέρος

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

Ορισμός 10.1.1. *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 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 $\}$

   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 βίντεο1 για περισσότερες πληροφορίες.*

10.2 Η περίπτωση του δακτυλίου πολυωνύμων μίας μεταβλητής

Πριν αρχίσετε τη μελέτη της παραγράφου αυτής δείτε το βίντεο2

Έστω $\mathbb{F}[x]$ ο δακτύλιος των πολυωνύμων μιας 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 πολυώνυμα 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

10.3 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:*
$MO(I) = \{x^\kappa y^\lambda$, *όπου* $x^\kappa y^\lambda$ *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[1] *:*
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 10.2 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* $x^\mu y^\rho = x^{\mu-\nu} y^{\rho-\xi} \cdot x^\mu y^\rho$[2]

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

1. *Για τον ακέραιο ξ-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* $J_{\xi-1} =< x^{\nu_{\xi-1}} >$

2. *Για τον ακέραιο ξ-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* $J_{\xi-2} =< x^{\nu_{\xi-2}} >$

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

[2] 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 $\mu \geq \nu$

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

$x^\nu y^\xi$
$x^{\nu_{\xi-1}} y^{\xi-1}$
$\cdots\cdots$
$x^{\nu_1} y$
x^{ν_0}

Απόδειξη *Η απόδειξη θα γίνει σε επόμενο μάθημα*

Θεώρημα 10.3.2. *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 10.3.3. *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*

Τέλος του πέμπτου μαθήματος

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