Περιεχόμενα

Μέρος I

Έναρξη μαθήματος

Υπολογιστική Άλγεβρα (439))

Ευάγγελος Ράπτης [1]

1. Τα παρακάτω κείμενα γράφονται και ενημερώνονται καθημερινά σε όλη την διάρκεια του Εαρινού εξαμήνου 2015-16 για τις ανάγκες του μαθήματος **Υπολογιστική Άλγεβρα,** που διδάσκεται στο Προπτυχιακό πρόγραμμα (*τέταρτο εξάμηνο*) του Τμήματος Μαθηματικών του Πανεπιστημίου Αθηνών.

2. Καλούνται οι φοιτητές να επισημαίνουν λάθη και παραλείψεις.

Παράπλευρες σελίδες συζήτησης

Μπορείτε να διατυπώνετε τις απορίες σας και τις σκέψεις σας:

Στην **Τηλεσυνεργασία**, είναι ο σύνδεσμος αριστερά στη σελίδα του μαθήματος. Στη σελίδα αυτή έχετε τη δυνατότητα να γράφετε και λίγα μαθηματικά σύμβολα.

Τηλεδιασκέψεις

Κατά τη διάρκεια του μαθήματος θα γίνουν πολλές **Τηλεδιασκέψεις**. Θα σας ενημερώσουμε σύντομα για αυτές. Πρέπει να διαθέτετε εκτός από υπολογιστή και σύνδεση στο internet, μία web camera και ένα μικρόφωνο.

[1] Ηλεκτρονική διεύθυνση: eraptis@math.uoa.gr
Γραφείο: 211, τηλ. 2107276347 Ηλεκτρονική διεύθυνση Ηλεκτρονικής τάξης του μαθήματος: http://eclass.uoa.gr/courses/MATH117/index.php

Κεφάλαιο 1

Πολυωνυμικές σχέσεις και ταυτότητες, μέρος Ι

Τετάρτη 17 Φεβρουαρίου 2016[1]

1.1 Εισαγωγή

Σκοπός[2] του πρώτου μέρους του μαθήματος αυτού είναι να διερευνήσει διαδικασίες που θα μπορούσαμε να τις ονομάσουμε « *πολυωνυμικές σχέσεις* ». Συνήθως τα ερωτήματα-προβλήματα εμφανίζονται ως εξής:

Πρόβλημα 1.
Από ένα ***Σύνολο Υποθέσεων*** *που διατυπώνονται με πολυώνυμα θέλουμε να καταλήξουμε σε ένα* ***Σύνολο συμπερασμάτων****, τα οποία επίσης διατυπώνονται με πολυώνυμα .*

Πρίν προχωρήσουμε ας δούμε μερικά παραδείγματα:

Παράδειγμα 1.1.1. *Υποθέτουμε ότι τρείς αριθμοί x, y, z ικανοποιούν τις σχέσεις*

$$\begin{aligned} x+y+z &= 3 \\ x^2+y^2+z^2 &= 5 \\ x^3+y^3+z^3 &= 7 \end{aligned}$$

Δείξτε ότι:

$$\begin{aligned} x^4+y^4+z^4 &= 9 \\ x^5+y^5+z^5 &\neq 11 \end{aligned}$$

[1] Ευάγγελος Ράπτης

[2] Το κείμενο αυτό γράφεται και συμπληρώνεται καθημερινά κατά τη διάρκεια του Εαρινού εξαμήνου 2015-16 για τις ανάγκες του μαθήματος **Υπολογιστική Άλγεβρα(439)**

Να υπολογίσετε επίσης τα παρακάτω αθροίσματα:

$$x^5 + y^5 + z^5$$
$$x^6 + y^6 + z^6$$

Παράδειγμα 1.1.2. *Να εξετάσετε εάν υπάρχει πεπερασμένο σύνολο τριάδων* x, y, z *με*

$$x^7 + y^9 + z^8 = 1$$
$$x^{12} + y^{25} + z^2 = 1$$
$$x^{13} + y^{23} + z^{33} = 1$$

Παράδειγμα 1.1.3. *Δίνονται οι πολυωνυμικές σχέσεις* $f(x) = 3x^6+2x^5+2x^4-x^3-8x^2+11x-9, g(x) = x^2-4x+3$

Προκύπτει η πολυωνυμική σχέση $h(x) = x^4 - 7x^2 + 6$ *από τις προηγούμενες;*

Παράδειγμα 1.1.4. *Δίνονται οι παρακάτω πολυωνυμικές «γραμμικές» σχέσεις:*

$$x + 2y + 3x = 0$$
$$4x + 5y + 6z = 0$$
$$7x + 8y + 9z = 0$$

Προκύπτει από τις σχέσεις αυτές η σχέση $12x + 13y + 18z = 0$*;*

1.2 Στον δρόμο για έναν ορισμό

Τα παραπάνω παραδείγματα μας βάζουν το ερώτημα για έναν ορισμο-οδηγό για την αντιμετώπισή τους.

1. **Πρώτη προσέγγιση** Θα λέμε ότι το συμπέρασμα

   $$f(x_1, x_2, \cdots, x_\nu) = 0$$

   (το οποίο είναι ένα πολυώνυμο με ν μεταβλητές) **προκύπτει** από τις υποθέσεις

   $$f_1(x_1, x_2, ..., x_\nu) = 0, f_2(x_1, x_2, ..., x_\nu) = 0, \cdots, f_\mu(x_1, x_2, ..., x_\nu) = 0$$

   (τα οποία είναι πολυώνυμα με ν μεταβλητές), εάν οποιαδήποτε ν-άδα $(\xi_1, \xi_2, \cdots, \xi_\nu)$ που «ικανοποιεί» τα πολυώνυμα

   $$f_1(x_1, x_2, ..., x_\nu) = 0, f_2(x_1, x_2, ..., x_\nu) = 0, \cdots, f_\mu(x_1, x_2, ..., x_\nu) = 0,$$

   «ικανοποιεί» και το

   $$f(x_1, x_2, \cdots, x_\nu) = 0$$

2. **Δεύτερη προσέγγιση** Θα λέμε ότι το συμπέρασμα

$$f(x_1, x_2, \cdots, x_\nu) = 0$$

(το οποίο είναι ένα πολυώνυμο με ν μεταβλητές) **προκύπτει** από τις υποθέσεις

$$f_1(x_1, x_2, ..., x_\nu) = 0, f_2(x_1, x_2, ..., x_\nu) = 0, \cdots, f_\mu(x_1, x_2, ..., x_\nu) = 0$$

(τα οποία είναι πολυώνυμα με ν μεταβλητές), εάν

$f(x_1, x_2, \cdots, x_\nu) =$
$h_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) + h_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu)$
$+ \cdots + h_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu),$
δηλαδή το «συμπέρασμα» είναι ένας **πολυωνυμικός συνδυασμός** των «υποθέσεων»

1.3 Ασκήσεις και προβληματισμοί

1. «Πειραματισθείτε» με πολυώνυμα μιας ή δύο μεταβλητών για να καταλήξετε σε έναν σωστό ορισμό

2. Σκεφθείτε έναν τρόπο διδασκαλίας των παραπάνω εννοιών στους μαθητές Γυμνασίων-Λυκείων

3. Να μελετήσετε και να βρείτε πληροφορίες για το σύνολο λύσεων στο $\mathbb{R}$ του παρακάτω συστήματος
$x^{\alpha+7} + y^{\beta+5} = 1$
$x^{\gamma+6} + y^{\alpha+10} = 1$, όπου α,β,γ τα τελευταία ψηφία του Αριθμού Μητρώου σας αρχίζοντας από το τέλος

   Εξετάστε εάν το παραπάνω σύστημα έχει πεπερασμένο σύνολο λύσεων

4. Να λυθεί το παρακάτω σύστημα στο $\mathbb{R}$
$(\alpha + 7)x^3 + 5x^2 + (6 + \beta)x + (\gamma + 13) = 0$
$(\alpha + 9)x^7 + 12x^3 + (16 + \beta)x + (2\gamma + 13) = 0$
όπου α,β,γ τα τελευταία ψηφία του Αριθμού Μητρώου σας αρχίζοντας από το τέλος.
Να γράψετε επίσης έναν τρόπο που προτείνετε να διδαχθεί η λύση της άσκησης αυτής στο Λύκειο

Τέλος του πρώτου μαθήματος

Κεφάλαιο 2

Πολυωνυμικές σχέσεις και ταυτότητες, μέρος ΙΙ

Μάθημα 2, Τετάρτη 24 Φεβρουαρίου 2016

2.1 Τα συστήματα

Οι παραπάνω προβληματισμοί μας οδηγούν να ασχοληθούμε με τις μεθόδους λύσεων συστημάτων
μ εξισώσεων με **ν αγνώστους** (μεταβλητές) της μορφής

$$\left\{ \begin{array}{c} f_1(x_1, x_2, ..., x_\nu) = 0 \\ f_2(x_1, x_2, ..., x_\nu) = 0 \\ \vdots \\ f_\mu(x_1, x_2, ..., x_\nu) = 0 \end{array} \right\} (\Sigma),$$

όπου $f_i(x_1, x_2, ..., x_\nu)$ είναι πολυώνυμα με **ν αγνώστους** (μεταβλητές) και συντελεστές από το $\mathbb{F}$ (όπου το $\mathbb{F}$ είναι ένα σώμα)[1].

1. Δείτε στο σημείο αυτό της μελέτης σας ένα σχετικό βίντεο. Το βίντεο θα το δείτε κάνοντας κλίκ εδώ

2. Αν το παραπάνω σύστημα είναι γραμμικό, δηλαδή αποτελείται από γραμμικά πολυώνυμα[2], τότε η Γραμμική Άλγεβρα είναι η κατάλληλη μαθηματική θεωρία

[1] Συνήθως στα παραδείγματα και στις ασκήσεις θα χρησιμοποιούμε το σώμα των πραγματικών αριθμών $\mathbb{R}$, το σώμα των μιγαδικών $\mathbb{C}$, το σώμα των ρητών $\mathbb{Q}$ και σπανιότερα το σώμα των ακεραίων modp όπου p ακέραιος πρώτος)

[2] Ένα γραμμικό πολυώνυμο με ν μεταβλητές είναι της μορφής $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_\nu x_\nu + \beta$, όπου $\alpha_i, \beta \in \mathbb{F}$

για την εύρεση των λύσεων αυτού[3] .

3. Αν το παραπάνω σύστημα έχει μόνο μία μεταβλητή και μία μόνο εξίσωση, δηλαδή ν=1 και μ=1, τότε ουσιαστικά έχουμε να βρούμε τις ρίζες ενός πολυωνύμου. Σημειώνεται εδώ ότι μεταξύ άλλων κατάλληλη θεωρία για την μελέτη των ριζών του είναι η θεωρία Galois.

Έτσι σχηματικά και για λόγους αναφοράς παρακάτω αυτό που θα μας απασχολήσει είναι το

Πρόβλημα 2.1.1. *Να λυθεί ένα σύστημα* ***μ πολυωνυμικών εξισώσεων με ν μεταβλητές*** *και συντελεστές από το σώμα* $\mathbb{F}$
Δύο είναι κυρίως οι μέθοδοι επίλυσης του παραπάνω προβλήματος :

1. Αλγεβρικές, μελέτη δηλαδή της δομής του δακτυλίου πολυωνύμων $\mathbb{F}[x_1, x_2, ..., x_\nu]$. Εδώ θα συναντήσουμε και θα ασχοληθούμε με τα θεωρήματα **Hilbert**

2. Γεωμετρικές, μελέτη δηλαδή της δομής του συνόλου λύσεων πολυωνυμικών συστημάτων π.χ μελέτη επιφανειών, γραμμών, σημείων τομής. Υπενθυμίζουμε εδώ ότι το σύνολο λύσεων ενός ομογενούς γραμμικού συστήματος είναι ένας υπόχωρος. Το τελευταίο είναι ένα αρκετά σημαντικό αποτέλεσμα, διότι μπορούμε έτσι, βρίσκοντας μία βάση να κατανοήσουμε πλήρως τη δομή του συνόλου των λύσεων.

Σκοπός μας επίσης είναι η μελέτη και η κατασκευή αλγορίθμων οι οποίοι θα μας δίνουν τις λύσεις των συστημάτων. Η χρήση των μαθηματικών υπολογιστικών πακέτων γίνεται έτσι αναγκαία.

Θα χρησιμοποιούμε το υπολογιστικό πακέτο $wolframalpha$. Δείτε στην διεύθυνση εδώ

2.1.1 Υποδείξεις για ερύτερη μελέτη

1. Να μελετήσετε τα αναγραφόμενα για τα πολυώνυμα στην σελίδα εδώ

2. Να μελετήσετε τα αναγραφόμενα για τις πολυωνυμικές εξισώσεις και τα συστήματα εξισώσεων στη σελίδα εδώ

2.1.2 Άσκηση

Προαιρετική άσκηση για σκέψη και μελέτη

[3] Για καλή κατανόηση των θεμάτων που διαπραγματεύεται το βιβλίο αυτό είναι αναγκαίο ο αναγνώστης να έχει αρκετές γνώσεις από την Γραμμική άλγεβρα

1. Να μελετήσετε και να βρείτε πληροφορίες για το σύνολο λύσεων στο $\mathbb{R}$ του παρακάτω συστήματος
   $x^{\alpha+7} + y^{\beta+5} = 1$
   $x^{\gamma+6} + y^{\alpha+10} = 1$, όπου α,β,γ είναι τα τρία τελευταία ψηφία του Αρ. Μητρώου σας, αρχίζοντας από το τέλος.

   Εξετάστε εάν το παραπάνω σύστημα έχει πεπερασμένο ή άπειρο σύνολο λύσεων

2. Να λυθεί το σύστημα
   $(\alpha + 7)x^3 + 5x^2 + (6 + \beta)x + (\gamma + 13) = 0$
   $(\alpha + 9)x^7 + 12x^3 + (16 + \beta)x + (2\gamma + 13) = 0$
   όπου α,β,γ είναι τα τρία τελευταία ψηφία του Αρ. Μητρώου σας, αρχίζοντας από το τέλος.

2.1.3 Υποδείξεις για την παραπάνω άσκηση

1. Εδώ έχουμε ένα σύστημα δύο πολυωνυμικών εξισώσεων με πραγματικούς συντελεστές. Το σύστημα αυτό έχει λύσεις, για παράδειγμα $x = 1, y = 0$ είναι μία λύση Αυτό είναι προφανές και έτσι με την παρατήρηση αυτή δεν χρειάζεται να χάσουμε χρόνο να εξετάσουμε αν το σύνολο λύσεων Λ είναι μη-κενό. Παραμένει όμως το σημαντικό ερώτημα:
   Πότε ένα σύστημα πολυωνυμικών εξισώσεων έχει μή-κενό σύνολο λύσεων;

   Δείτε στην αρχή το σύστημα ποιοτικά. Αν ήταν γραμμικό, τότε θα ήταν γνωστής μορφής και το σύνολο λύσεων θα ήταν εύκολο να περιγραφεί. Σκεφθείτε γιατί.

   Αν ήταν επίσης της μορφής:
   $x^2 + y^2 = 1$
   $x^2 - y^2 = 1$

   θα θέσουμε $x^2 = X, y^2 = Y$ και θα το λύσουμε ως γραμμικό. Η δυσκολία επίλυσης βρίσκεται στους εκθέτες λοιπόν. Προσπαθήστε να ανακαλύψετε δικές σας μεθόδους ή χρησιμοποιείστε και το AXIOM αλλά να ερμηνεύσετε το αποτέλεσμα

2. **Γιατί το σύστημα του ερωτήματος 1 έχει πεπερασμένο σύνολο λύσεων**

   Σκεφθείτε πάνω στο ερώτημα αυτό

Μέρος II

Πολυώνυμα μίας μεταβλητής

Κεφάλαιο 3

Πολυώνυμα τρίτου βαθμού

3.1 Μάθημα 2, συνέχεια

3.1.1 Έρευνα στο διαδίκτυο

Πριν αρχίσετε την μελέτη ρίξτε μία ματιά εδώ

3.1.2 Εξίσωση τρίτου βαθμού-μέθοδος *Cardano*

Ας θεωρήσουμε την εξίσωση τρίτου βαθμού:

$$f(x) = \alpha \cdot x^3 + \beta \cdot x^2 + \gamma \cdot x + \delta = 0, \;\; \alpha, \beta, \gamma, \delta \in \mathbb{R}, \;\; \alpha \neq 0 \tag{3.1}$$

Σκοπός μας είναι να βρούμε τις τιμές (τις ρίζες δηλαδή) που μηδενίζουν το παραπάνω πολυώνυμο και επίσης να βρούμε ιδιότητες αυτών.

1. Αφού το α είναι διαφορετικό από το μηδέν μπορούμε να διαιρέσουμε το $f(x)$ με το α, να βρούμε το $f^\star(x) = \frac{f(x)}{\alpha}$ και να έχουμε την εξίσωση

   $$f^\star(x) = \frac{f(x)}{\alpha} = x^3 + \frac{\beta}{\alpha} \cdot x^2 + \frac{\gamma}{\alpha} \cdot x + \frac{\delta}{\alpha} = 0, \;\; \alpha, \beta, \gamma, \delta \in \mathbb{R}, \;\; \alpha \neq 0 \tag{3.2}$$

2. Προφανώς οι ρίζες του $f(x)$ είναι ίδιες με τις ρίζες του $f^\star(x)$

3. Επειδή το πολυώνυμο $f^\star(x)$ είναι πολυώνυμο τρίτου βαθμού με πραγματικούς συντελεστές, θα υπάρχει τουλάχιστον μία ριζα πραγματική[1]. Επίσης ή θα έχουμε ακόμη δύο ρίζες πραγματικές ή δύο ρίζες συζυγείς μιγαδικές

4. Ας υποθέσουμε, λοιπόν, ότι έχουμε να λύσουμε την παρακάτω εξίσωση:

   $$x^3 + Ax^2 + Bx + \Gamma = 0 \tag{3.3}$$

[1] Να βρείτε μία πειστική εξήγηση για αυτό

5. Κάνουμε τον μετασχηματισμό

(3.4) $$x = t - \frac{A}{3}$$

6. Καταλήγουμε στην εξίσωση:

(3.5) $$t^3 + tp + q = 0$$

με

(3.6) $$p = B - \frac{A^2}{3}, \quad q = \Gamma + \frac{2A^3 - 9AB}{27}$$

7. Θέλοντας να λύσουμε την εξίσωση 3.5 εργαζόμαστε ως εξής:
Θεωρούμε ξ, ω με

(3.7) $$\xi^3 - \omega^3 = q, \quad \xi \cdot \omega = \frac{p}{3}$$

8. Έχουμε τώρα τα εξής:

(3.8) $$\xi^3 - \omega^3 = q, \quad (\xi \cdot \omega)^3 = \xi^3 \cdot \omega^3 = \frac{p^3}{27}$$

9. Οι παραπάνω εξισώσεις μας λένε ότι γνωρίζουμε τη διαφορά $\xi^3 - \omega^3 = q$ και το γινόμενο $\xi^3 \cdot \omega^3 = \frac{p^3}{27}$ δύο ποσοτήτων. Εύκολο είναι να τις βρούμε οδηγούμενοι σε ένα δευτεροβάθμιο τριώνυμο. Βρίσκουμε, λοιπόν, τα παρακάτω:

(3.9) $$\xi^3 = \frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \quad \omega^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

10. Ας θεωρήσουμε την ταυτότητα:

(3.10) $$(\omega - \xi)^3 = \omega^3 - 3\omega^2 \cdot \xi + 3\omega \cdot \xi^2 - \xi^3 \Rightarrow (\omega - \xi)^3 = \omega^3 - 3\omega\xi(\omega - \xi) - \xi^3$$

11. Η τελευταία σχέση γράφεται

(3.11) $$(\omega - \xi)^3 + (\xi^3 - \omega^3) + 3\omega\xi(\omega - \xi) = 0$$

Και αντικαθιστώντας τις σχέσεις από 2.7 έχουμε

12.

(3.12) $$(\omega - \xi)^3 + q + p(\omega - \xi) = 0$$

13. Παρατηρούμε από την τελευταία σχέση ότι οι ρίζες που ψάχνουμε είναι της μορφής $\omega - \xi$, αλλά τις τιμές των ω, ξ τις έχουμε ήδη υπολογίσει. Παρατηρούμε επίσης, ότι από τις σχέσεις 3.9, οδηγούμαστε σε τρείς τιμές για το ξ και τρεις τιμές για το ω. Όμως το πολυώνυμο έχει ακριβώς τρείς ρίζες[2] στο σύνολο $\mathbb{C}$

[2] όχι κατ ανάγκη διακεκριμένες

των μιγαδικών αριθμών. Συνεχίζουμε ως εξής:

(α′) Οι τρείς ρίζες της μονάδας, δηλαδή του πολυωνύμου x^3-1 στο σύνολο $\mathbb{C}$ των μιγαδικών αριθμών είναι οι
$\{z_0=1, z_1=-\frac{1}{2}+\frac{i\cdot\sqrt{3}}{2}, z_2=-\frac{1}{2}-\frac{i\cdot\sqrt{3}}{2}\}$

(β′) Από τις σχέσεις 3.9 έχουμε για το ξ τρεις τιμές τις:
$\xi_0=\sqrt[3]{\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},\ \xi_1=z_1\cdot\sqrt[3]{\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$
$\xi_2=z_2\cdot\sqrt[3]{\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$

(γ′) Επίσης για το ω έχουμε άλλες τρείς τιμές τις:
$\omega_0=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},\ \omega_1=z_1\cdot\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$
$\omega_2=z_2\cdot\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$

(δ′) Οι εξισώσεις 3.7 μας λένε τελικά ότι οι τρεις ρίζες του πολυωνύμου, που ψάχνουμε είναι:
$\omega_0-\xi_0,\ \omega_2-\xi_1,\ \omega_1-\xi_2$

3.2 Ασκήσεις και προβληματισμοί

1. Να θεωρήσετε το πολυώνυμο $f(x)=(\alpha+7)x^3+(\beta+5)x^2+(\gamma+2)x+2\in\mathbb{Q}[x]$ και να βρείτε τις τρείς ρίζες του με ριζικά

2. Να μελετήσετε την έννοια της **Διακρίνουσας** πολυωνύμων τρίτου βαθμού από τη διεύθυνση Διακρίνουσα και μετά να κάνετε εφαρμογή στο παραπάνω πολυώνυμο $f(x)$

3. Μελετήστε σε βάθος την έννοια του Δακτυλίου-πηλίκο. Μετά να μελετήσετε τον δακτύλιο-πηλίκο $\mathbb{Q}[x]/I$ και $\mathbb{R}[x]/I$, όπου I είναι το ιδεώδες που παράγεται από το πολυώνυμο $f(x)$

4. Να μελετήσετε τον δακτύλιο-πηλίκο $\mathbb{Z}[x]/I$ όπου I είναι το ιδεώδες που παράγεται από το πολυώνυμο $f(x)$

5. Να λυθεί το σύστημα
$(\alpha+7)x^3+5x^2+(6+\beta)x+(\gamma+13)=0$
$(\alpha+9)x^3+12x^2+(16+\beta)x+(2\gamma+13)=0$

6. **Ελεύθερο θέμα** Πείτε τρόπους διδασκαλίας των παραπάνω «δύσκολων» εννοιών για τον δακτύλιο-πηλίκο

3.3 Σκέψεις για επίλυση ενός συστήματος με δύο εξισώσεις τρίτου βαθμού

Ας υποθέσουμε ότι έχουμε το παρακάτω πρόβλημα:

Πρόβλημα

Να λυθεί το σύστημα

$(\alpha+7)x^3+5x^2+(6+\beta)x+(\gamma+13)=0$
$(\alpha+9)x^3+12x^2+(16+\beta)x+(2\gamma+13)=0$

1. Η πρώτη σκέψη μας είναι να βρούμε τις ρίζες και του πρώτου πολυωνύμου και του δεύτερου, σύμφωνα με αυτά που περιγράψαμε παραπάνω και να βρούμε τις κοινές ρίζες. Να κάνετε αυτή τη διαδικασία και σκεφθείτε τις δυσκολίες, οι οποίες είναι μεγάλες (δείτε γιατί).

2. Μία άλλη προσέγγιση πιο καλή είναι αυτή που προκύπτει από την εξής ιδέα: Αν έχουμε γενικά να λύσουμε το σύστημα $\{f(x)=0, g(x)=0\}$, όπου τα $f(x), g(x)$ είναι πολυώνυμα μίας μεταβλητής, εκτελούμε τον αλγόριθμο της διαίρεσης του $f(x)$ διά του $g(x)$ (ή αντίστροφα ανάλογα με τον βαθμό των πολυωνύμων). Αν,λοιπόν, $f(x)=g(x)\pi(x)+\upsilon(x)$, είναι εύκολο να διαπιστώσουμε ότι το σύνολο λύσεων του συστήματος $\{f(x)=0, g(x)=0\}$ είναι ίσο με το σύνολο λύσεων του συστήματος $\{\upsilon(x)=0, g(x)=0\}$. Εδώ σκεφθείτε μία πιθανή γενίκευση και κατασκευή αλγορίθμου

3. Παρακολουθήστε επίσης το βίντεο[3] εδώ και σκεφθείτε νέες μεθόδους.

Τέλος του δευτέρου μαθήματος

[3] Όποιος βρεί την μουσική υπόκρουση θα τον παραδεχθώ

Κεφάλαιο 4

Πολυώνυμα τετάρτου και μεγαλυτέρου βαθμού

4.1 Εξίσωση τετάρτου βαθμού

Τετάρτη 2 Μαρτίου 2016 [1]

4.1.1 Έρευνα στο *internet*

1. Δείτε και μελετήστε τις πληροφορίες εδώ
2. Δείτε επίσης στην διεύθυνση εδώ

4.1.2 Επίλυση με ριζικά

Θεωρούμε τώρα το πολυώνυμο τετάρτου βαθμού: 

$$f(x) = \alpha \cdot x^4 + \beta \cdot x^3 + \gamma \cdot x^2 + \delta \cdot x + \epsilon, \;\; \alpha \neq 0$$

με συντελεστές από το σώμα $\mathbb{F}^2$

1. Διαιρούμε το $f(x)$ με τον μη-μηδενικό αριθμό α και έχουμε το πολυώνυμο $\frac{1}{\alpha} \cdot f(x)$. Οι τιμές, που μηδενίζουν (οι ρίζες) το $f(x)$ είναι ίδιες που μηδενίζουν το $\frac{1}{\alpha} \cdot f(x)$.
2. Το $\frac{1}{\alpha} \cdot f(x)$ έχει τη μορφή:

$$x^4 + A \cdot x^3 + B \cdot x^2 + \Gamma \cdot x + \Delta$$

[1] Το βιβλίο αυτό γράφεται και *σκίζεται* ηλετρονικά καθημερινά για τις ανάγκες του μαθήματος Υπολογιστική άλγεβρα
Ε.Ράπτης

[2] Θεωρείστε ότι το σώμα των συντελεστών είναι το σώμα των πραγματικών αριθμών

3. Κάνουμε το μετασχηματισμό $x = t - \frac{A}{4}$, οπότε το πολυώνυμο παίρνει τη μορφή[3]:

$$t^4 + pt^2 + qt + r$$

4. Γράφουμε τώρα

$$t^4 + pt^2 + qt + r = (t^2 + \kappa t + \lambda) \cdot (t^2 + \mu t + \xi)$$

και προσπαθούμε να υπολογίσουμε τα κ,λ,μ,ξ

5. Έχουμε
$\mu + \kappa = 0$
$\lambda + \kappa \cdot \mu + \xi = p$
$\lambda \cdot \mu + \kappa \cdot \xi = q$
$\lambda \cdot \xi = r$

6. Έχουμε επίσης:
$\lambda + \xi = p + \kappa^2$
$\kappa \cdot (\xi - \lambda) = q$
$\lambda \cdot \xi = r$

7. Θεωρούμε την ταυτότητα:

$$(\lambda + \xi)^2 - (\xi - \lambda)^2 = 4\lambda\xi \tag{4.1}$$

και αντικαθιστώντας στην ταυτότητα αυτή
$\lambda + \xi = p + \kappa^2$, $\xi - \lambda = \frac{q}{\kappa}$, $\lambda\xi = r$ έχουμε μία εξίσωση τρίτου βαθμού ως προς κ^2.

8. Όταν λύσουμε την εξίσωση τρίτου βαθμού, με τη βοήθεια του προηγουμένου μαθήματος, ως προς κ^2 βρίσκουμε το κ και μετά τα λ και ξ και μετά τις ρίζες που ψάχνουμε[4]

4.1.3 Η δυστυχία του να μήν υπάρχει αλγόριθμος!

Όπως είδαμε παραπάνω αν μας δοθεί ένα πολυώνυμο δευτέρου, τρίτου, ή τετάρτου βαθμού, μπορούμε να βρούμε τις ρίζες του. Πιο αυστηρά μπορούμε να πούμε το παρακάτω:

[3] Διαπιστώστε ότι για κάθε πολυώνυμο $f(x) = x^\nu + \alpha_{\nu-1} \cdot x^{\nu-1} + \alpha_{\nu-2} \cdot x^{\nu-2} + \cdots + \alpha_1 \cdot x + \alpha_0$ ο μετασχηματισμός $x = t - \frac{\alpha_{\nu-1}}{\nu}$ οδηγεί σε ένα πολυώνυμο χωρίς όρο βαθμού $\nu - 1$

[4] Πρέπει εδώ να κάνουμε την κατάλληλη διερεύνηση, όπως στην εξίσωση τρίτου βαθμού και να απορρίψουμε μερικές ρίζες που εμφανίζονται

Θεώρημα 4.1.1. *Έστω $f(x) \in \mathbb{C}[x]$ βαθμού έως 4. Τότε υπάρχει αλγόριθμος, ο οποίος έχει ως είσοδο το πολυώνυμο (στην πραγματικότητα τους συντελεστές του) και ως έξοδο τις τιμές που το μηδενίζουν (ρίζες του). Οι ρίζες αυτές περιγράφονται χρησιμοποιώντας τις 4 πράξεις του σώματος (πρόσθεση,αφαίρεση,πολλαπλασιασμό, διαίρεση) και εξαγωγή ρίζας*

1. Υπενθυμίζουμε ότι η έννοια του αλγορίθμου συναντιέται σχεδόν σε όλους τους επιστημονικούς κλάδους και είναι μία μάθηματική έννοια. Να διαβάσετε οπωσδήποτε το άρθρο εδώ

2. Ο Galois απέδειξε ότι **δεν υπάρχει αλγόριθμος,** ο οποίος να έχει ως είσοδο ένα οποιοδήποτε[5] πολυώνυμο βαθμού μεγαλύτερου ή ίσου με 5 και ως έξοδο περιγραφή των ριζών με τη βοήθεια των 4 πράξεων του σώματος των συντελεστών και εξαγωγή ρίζας.

3. Η απόδειξη[6] του Galois στηρίζεται στην πρωτοποριακή (για την εποχή της) μαθηματική σύλληψη ότι κάθε πολυώνυμο (όπως και κάθε μαθηματικό αντικείμενο) χαρακτηρίζεται από τις « συμμετρίες του», τις «αρμονίες του». Αυτές οι « συμμετρίες» αποτελούν μία ομάδα. Η ομάδα που επισυνάπτεται κατά φυσιολογικό τρόπο στο πολυώνυμο $f(x)$ και το χαρακτηρίζει λέγεται **ομάδα Galois** του πολυωνύμου και συμβολίζεται $G(f)$

4. Μία ομάδα Γ λέγεται **επιλύσιμη** εάν υπάρχει πεπερασμένη ακολουθία υποομάδων $\Gamma_0 = \{e\}, \Gamma_1, \Gamma_2, \cdots \Gamma_\nu = \Gamma$ έτσι ώστε $\Gamma_i \lhd \Gamma_{i+1}$, και κάθε ομάδα-πηλίκο Γ_{i+1}/Γ_i είναι αβελιανή ομάδα. Με λόγια μία ομάδα είναι επιλύσιμη εάν υπάρχει «σκάλα» που φθάνουμε από την τετριμμένη υποομάδα στην αρχική ομάδα, τα « σκαλοπάτια» είναι υποομάδες, κάθε υποομάδα είναι κανονική υποομάδα της επόμενης και η ομάδα-πηλίκο είναι αβελιανή ομάδα. Δείτε περισσότερα για τις επιλύσιμες ομάδες εδώ

5. Κατά κάποιον τρόπο μία ομάδα Γ είναι επιλύσιμη εάν «χτίζεται » από τα «θεμέλια », δηλαδή την τετριμμένη υποομάδα έως την «οροφή », δηλαδή την ίδια την ομάδα Γ και τα « υλικά » είναι αβελιανές ομάδες. Για να « σταθεί » καλά το « οικοδόμημα » πρέπει κάθε υποομάδα από τις $\Gamma_0 = \{e\}, \Gamma_1, \Gamma_2, \cdots \Gamma_\nu = \Gamma$ να είναι κανονική στην επόμενη και η ομάδα-πηλίκο να είναι αβελιανή

6. Ο Galois, λοιπόν απέδειξε ότι ένα πολυώνυμο $f(x)$ λύνεται με ριζικά (όπως παραπάνω) **εάν και μόνο εάν** η ομάδα Galois $G(f)$ είναι επιλύσιμη.

7. Θα αναρωτηθεί βέβαια κανείς σε τι βοηθάει αυτή η μετάφραση του προβλήματος. Αυτό που αποδεικνύει κανείς είναι ότι η ομάδα Galois του πολυωνύμου

[5] **Προσοχή:** Το θεώρημα αυτό αναφέρεται σε όλα τα πολυώνυμα. Υπάρχουν όμως και πολυώνυμα βαθμού 5 ή παραπάνω που οι ρίζες τους εκφράζονται με ριζικά π.χ. $f(x) = x^5 - 1 \in \mathbb{Q}[x]$

[6] Συστήνω ανεπιφύλακτα και με θέρμη να εγγραφείτε στο μάθημα **Θεωρία Galois** που διδάσκεται στο Τμήμα Μαθηματικών του Πανεπιστημίου Αθηνών

$G(f)$ είναι πεπερασμένη και μάλιστα ισόμορφη με μία υποομάδα της ομάδας μεταθέσεων S_ν , όπου ν είναι ο βαθμός του πολυωνύμου. Αφού κάθε ομάδα Galois είναι πεπερασμένη, μπορούμε να εξετάσουμε σχετικά εύκολα αν είναι επιλύσιμη. Επίσης μπορούμε να αποδείξουμε ότι κάθε υποομάδα της S_3 και της S_4 είναι επιλύσιμη. Όμως η S_5 δεν είναι επιλύσιμη. Επισημαίνουμε ότι ο δείκτης στην ομάδα S_ν σχετίζεται με τον βαθμό του πολυωνύμου.

8. Σύμφωνα με τα παραπάνω δεν υπάρχει αλγόριθμος που να δίνει τις ρίζες ενός πολυωνύμου χρησιμοποιώντας ριζικά. Δείτε το 2 για πιο αυστηρή διατύπωση. Δείτε επίσης το άρθρο εδώ σχετικά με τη θεωρία Galois .

4.1.4 Πάντα υπάρχει ελπίδα!

1. Ας θεωρήσουμε το πολυώνυμο $f(x) = x^5 - 9x + 3 \in \mathbb{Q}[x]$ Με τη βοήθεια παραγώγων μπορούμε να διαπιστώσουμε ότι η παραπάνω συνάρτηση έχει τρεις ρίζες πραγματικές. Οι άλλες δύο θα είναι συζυγείς μιγαδικές

2. Δείτε πληροφορίες για την γραφική παράσταση του πολυωνύμου δίνοντας την εντολή *plot* x^5-9x+3 στο υπολογιστικό πακέτο που βρίσκεται στο internet στη διεύθυνση εδώ

3. Δείτε επίσης πληροφορίες για τις ρίζες του πολυωνύμου στο παραπάνω υπολογιστικό πακέτο, δίνοντας την εντολή $x^5 - 9x + 3 = 0$.

4. Από τις παραπάνω πληροφορίες μπορούμε να βρούμε ότι η ομάδα Galois του $f(x)$ είναι η S_5. Η ομάδα αυτή **δεν** είναι επιλύσιμη διότι περιέχει ως υποομάδα την A_5. Δες πληροφορίες εδώ Το συμπέρασμα είναι ότι δεν υπάρχει ελπίδα να βρούμε τύπο για τις ρίζες του $f(x)$ όπως έχουμε βρει για τα πολυώνυμα τρίτου και τετάρτου βαθμού.

5. Όμως υπάρχει ο κλάδος των Μαθηματικών Αριθμητική ανάλυση[7] ο οποίος δίνει αλγορίθμους για εύρεση προσεγγίσεων των ριζών. Δες εδώ για περισσότερες πληροφορίες. εδώ

6. Το συμπέρασμα είναι ότι παρακάμπτοντας την δυσκολία της μη-ύπαρξης αλγορίθμων για εύρεση ριζών πολυωνύμων βαθμού μεγαλύτερου ή ίσου του 5 (ως αποτέλεσμα της θεωρίας Galois) κατασκευάζουμε άλλους αλγορίθμους που βρίσκουν με προσεγγίσεις τις ρίζες

[7]Συστήνω ανεπιφύλακτα και με θέρμη να εγγραφείτε στο μάθημα Αριθμητική ανάλυση που διδάσκεται στο Τμήμα Μαθηματικών του Πανεπιστημίου Αθηνών

4.2 Σχετικά με τους κοινούς παράγοντες

Στο σημείο αυτό θα ασχοληθούμε με το παρακάτω ερώτημα **Ερώτημα** Δίνονται τα πολυώνυμα μία ς μεταβλητής :

$$g(x) = \alpha_\nu x^\nu + \alpha_{\nu-1}x^{\nu-1} + \cdots + \alpha_0, \nu > 0$$
$$h(x) = \beta_\mu x^\mu + \beta_{\mu-1}x^{\mu-1} + \cdots + \beta_0, \mu > 0$$

Έχουν τα πολυώνυμα $g(x), h(x)$ κοινό παράγοντα;

4.2.1 Η μέθοδος με τον Μέγιστο Κοινό Διαιρέτη

Μία πρώτη απάντηση είναι η εύρεση του Μέγιστου Κοινού Διαιρέτη $d(x) = MK\Delta(g(x), h(x))$. Στην περίπτωση αυτή έχουμε:

1. Υπολογίζουμε τον Μέγιστου Κοινού Διαιρέτη $d(x) = MK\Delta(g(x), h(x))$ με την μέθοδο του Ευκλείδη ή με όποια άλλη μέθοδο.

2. Έχουμε $g(x) = d(x) \cdot \kappa(x)$ και $h(x) = d(x) \cdot \lambda(x)$,με $MK\Delta(\kappa(x), \lambda(x)) = 1$

3. Αν $\gamma(x)$ κάποιος κοινός παράγοντας των $g(x), h(x)$,τότε το πολυώνυμο $\gamma(x)$, θα διαιρεί τον ΜΚΔ $d(x)$.

4. Από τα παραπάνω φαίνεται καθαρά το πρόβλημα της εύρεσης κοινού παράγοντα, ανάγεται στην εύρεση των παραγόντων του $d(x) = MK\Delta(g(x), h(x))$

4.2.2 Η ορίζουσα του *Sylvester*

Λήμμα 4.2.1. *Τα πολυώνυμα $g(x), h(x)$ έχουν κοινό παράγοντα, εάν και μόνον εάν υπάρχουν $A(x)$ και $B(x)$ έτσι ώστε:*

1. *Τα $A(x)$ και $B(x)$ δεν είναι ταυτόχρονα μηδέν.*

2. *Το $A(x)$ είναι βαθμού το πολύ $\mu - 1$ και το $B(x)$ είναι βαθμού το πολύ $\nu - 1$*

3. *$A(x)g(x) - B(x)h(x) = 0$*

Ορισμός 4.2.2. *Ο πίνακας Sylvester δύο πολυωνύμων $g(x), h(x)$ ορίζεται όπως φαίνεται στη διεύθυνση εδώ και συμβολίζεται $Syl(g, h, x)$. Η ορίζουσα του πίνακα αυτού ονομάζεται* **απαλοίφουσα** *των δύο πολυωνύμων και συμβολίζεται με $Res(g, h, x)$.*

Θεώρημα 4.2.3. *Τα πολυώνυμα $g(x), h(x)$, έχουν κοινό παράγοντα εάν και μόνο εάν $Res(g, h, x) = 0$*

4.3 Άσκηση

Παρακάτω τα α,β,γ είναι τα ψηφία του Αρ Μητρώου σου αρχίζοντας από το τέλος

1. Δίνεται το πολυώνυμο $f(x) = x^4+(\alpha+1)x^3+(\beta+8)x^2+(\gamma+1)x+2 \in \mathbb{R}[x]$. Να περιγράψετε τις 4 ρίζες του με ριζικά. Να συγκρίνετε με την απάντηση που θα σας δώσει κάποιο υπολογιστικό πακέτο.

2. Δίνεται το πολυώνυμο $g(x) = (\alpha+7)x^3+(\beta+3)x^2+(\gamma+4)x+2 \in \mathbb{R}[x]$. Να περιγράψετε τις 3 ρίζες του με ριζικά. Να συγκρίνετε με την απάντηση που θα σας δώσει κάποιο υπολογιστικό πακέτο.

3. Να αποδείξετε λεπτομερώς το Λήμμα 4.2.1

4. Να αποδείξετε λεπτομερώς το Θεώρημα 4.2.3

5. Να εφαρμόσετε την μέθοδο του ΜΚΔ και την μέθοδο του Sylvester για να εξετάσετε εάν τα πολυώνυμα $f(x), g(x)$ έχουν κοινό παράγοντα

Τέλος του τρίτου μαθήματος

Κεφάλαιο 5

Ο αλγόριθμος της διαίρεσης

5.1 Γενικά για τον δακτύλιο των πολυωνύμων

Τετάρτη 9 Μαρτίου 2016

1. Αν $\mathbb{F}$[1] το σώμα των συντελεστών, το σύνολο των πολυωνύμων μιας μεταβλητής με συντελεστές από το $\mathbb{F}$, θα το συμβολίζουμε με $\mathbb{F}[x]$.

2. Δες πληροφορίες για τα σώματα στα μαθηματικά εδώ

3. Το σύνολο των πολυωνύμων $\mathbb{F}[x]$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο.

4. Δες πληροφορίες για τους δακτυλίους στα μαθηματικά εδώ

5. **Θεώρημα 5.1.1.** *Έστω $\Delta(x) \in \mathbb{F}[x]$ και $\delta(x) \in \mathbb{F}[x]$ με $\delta(x) \neq \mathbf{0}(\mathbf{x})$. Υπάρχουν μοναδικά πολυώνυμα $\pi(x)$ και $\upsilon(x)$ με τις παρακάτω ιδιότητες*

   (α΄) $\Delta(x) = \delta(x) \cdot \pi(x) + \upsilon(x)$

   (β΄) *Είτε $\upsilon(x) = \mathbf{0}(\mathbf{x})$, δηλαδή είναι το μηδενικό πολυώνυμο, είτε $\upsilon(x) \neq \mathbf{0}(\mathbf{x})$ και βαθμός ($\upsilon(x)$)< βαθμός ($\delta(x)$)*

   Απόδειξη

   (α΄) Ας θεωρήσουμε ότι:

      i. $\Delta(x) = \alpha_\nu \cdot x^\nu + \alpha_{\nu-1} \cdot x^{\nu-1} + \cdots + \alpha_1 \cdot x + \alpha_0$ με $\alpha_\nu \neq 0$, δηλαδή το $\Delta(x)$ έχει βαθμό ν.

[1] Στο μάθημα αυτό ως σώμα συντελεστών θα έχουμε το σώμα $\mathbb{R}$ των πραγματικών αριθμών, εκτός εάν αναφέρουμε κάτι διαφορετικό. Πάντως οι περισσότερες προτάσεις και θεωρήματα ισχύουν για όλα τα σώματα.

ii. $\delta(x) = \beta_\mu \cdot x^\mu + \beta_{\mu-1} \cdot x^{\mu-1} + \cdots + \beta_1 \cdot x + \beta_0$ με $\beta_\nu \neq 0$, δηλαδή το $\Delta(x)$ έχει βαθμό μ.

iii. Εάν $\nu < \mu$, δηλαδή ο βαθμός του $\Delta(x)$ είναι γνήσια μικρότερος του $\delta(x)$, τότε θέτουμε
$\pi(x) = \mathbf{0(x)}$ και $\upsilon(x) = \Delta(x)$ και οι απαιτήσεις του θεωρήματος ικανοποιούνται πλήρως.

iv. Έστω[2] ότι $\nu \geq \mu$. Στην περίπτωση αυτή θεωρούμε το μονώνυμο $\frac{\alpha_\nu}{\beta_\mu} \cdot x^{\nu-\mu}$

v. Παρατηρούμε ότι το πολυώνυμο:

$$\upsilon_1(x) = \Delta(x) - \frac{\alpha_\nu}{\beta_\mu} \cdot x^{\nu-\mu} \cdot \delta(x) \tag{5.1}$$

έχει βαθμό γνήσια μικρότερο του βαθμού του $\Delta(x)$, δηλαδή έχει βαθμό γνήσια μικροτέρου του ν, διότι ο μεγιστοβάθμιος όρος του $\Delta(x)$ διαγράφθηκε.

vi. Ας υποθέσουμε ότι το $\upsilon_1(x)$ είναι ένα πολυώνυμο της μορφής:

$$\upsilon_1(x) = \lambda_\xi \cdot x^\xi + \lambda_{\xi-1} \cdot x^{\xi-1} + \cdots + \lambda_1 \cdot x + \lambda_0 \tag{5.2}$$

με $\lambda_\xi \neq 0$ και $\xi < \nu$

vii. α) Αν ο βαθμός του $\upsilon_1(x)$ είναι γνήσια μικρότερος του βαθμού του $\delta(x)$, δηλαδή του μ, τότε θεωρούμε ως $\pi(x)$ το $\frac{\alpha_\nu}{\beta_\mu} \cdot x^{\nu-\mu}$ και ως $\upsilon(x)$ το $\upsilon_1(x)$. Με έλεγχο διαπιστώνουμε ότι ικανοποιούνται πλήρως οι απαιτήσεις του πρώτου μέρους του θεωρήματος

β) Αν ξ =βαθμός του $\delta(x) > \mu$, θεωρούμε το μονώνυμο $\frac{\lambda_\xi}{\beta_\mu} \cdot x^{\xi-\mu}$

viii. Στην περίπτωση β) θεωρούμε το πολυώνυμο:

$$\upsilon_2(x) = \upsilon_1(x) - \frac{\lambda_\xi}{\beta_\mu} \cdot x^{\xi-\mu} \cdot \delta(x) = \Delta(x) - \frac{\alpha_\nu}{\beta_\mu} \cdot x^{\nu-\mu} \cdot \delta(x) - \frac{\lambda_\xi}{\beta_\mu} \cdot x^{\xi-\mu} \cdot \delta(x) \tag{5.3}$$

ix. Για το $\upsilon_2(x)$ εξετάζουμε πάλι εάν ο βαθμός του (ο οποίος είναι γνήσια μικρότερος από τον βαθμό του $\upsilon_1(x)$) είναι μικρότερος από τον βαθμό μ του $\delta(x)$ ή όχι και συνεχίζουμε ανάλογα όπως προηγουμένως

x. Επειδή η ακολουθία ($\upsilon_1(x), \upsilon_2(x), \upsilon_3(x), \cdots,$) είναι γνησίως φθίνουσα στους βαθμούς, θα υπάρχει η **πρώτη** φορά, που ο βαθμός του $\upsilon_i(x)$ γίνεται γνήσια μικρότερος του μ. Στην περίπτωση αυτή σταματάμε και θέτουμε:
$\upsilon(x) = \upsilon_i(x)$ και $\pi(x) = \frac{\alpha_\nu}{\beta_\mu} \cdot x^{\nu-\mu} + \frac{\lambda_\xi}{\beta_\mu} \cdot x^{\xi-\mu} + \cdots$

[2]Στη θεωρία πολυωνύμων **δεν επιτρέπονται** αρνητικοί εκθέτες

xi. Παρατηρούμε ότι το πρώτο (το υπαρξιακό) μέρος του θεωρήματος αποδείχθηκε

(β′) Έστω τώρα ότι έχουμε:
$\Delta(x) = \delta(x) \cdot \pi(x) + \upsilon(x)$ και
$\Delta(x) = \delta(x) \cdot \pi'(x) + \upsilon'(x)$
Αφαιρώντας κατά μέλη έχουμε $\delta(x)\left(\pi(x) - \pi'(x)\right) = \upsilon'(x) - \upsilon(x)$
Αν $\pi(x) - \pi'(x) \neq \mathbf{0(x)}$ τότε και $\upsilon'(x) - \upsilon(x) \neq \mathbf{0(x)}$ και εξετάζοντας τους βαθμούς και των δύο μελών καταλήγουμε σε άτοπο.
Τελικά καταλήγουμε ότι $\pi(x) - \pi'(x) = \mathbf{0(x)}$ και $\upsilon'(x) - \upsilon(x) = \mathbf{0(x)}$ και έτσι έχουμε αποδείξει και το δεύτερο μέρος του θεωρήματος

6.

Ορισμός 5.1.2. *Έστω $\Delta(x), \delta(x), \pi(x), \upsilon(x)$ τα πολυώνυμα του προηγουμένου θεωρήματος.*

(α′) Το πολυώνυμο $\Delta(x)$ θα λέγεται **Διαιρετέος**

(β′) Το πολυώνυμο $\delta(x)$ θα λέγεται **διαιρέτης**

(γ′) Το πολυώνυμο $\pi(x)$ θα λέγεται **πηλίκο** *της διαίρεσης*

(δ′) Το πολυώνυμο $\upsilon(x)$ θα λέγεται **υπόλοιπο** *της διαίρεσης*

(ε′) Αν το υπόλοιπο της διαίρεσης του $\Delta(x)$ δια του $\delta(x)$ είναι το μηδενικό πολυώνυμο $\mathbf{0(x)}$, θα λέμε ότι το $\delta(x)$ **διαιρεί** *το $\Delta(x)$ και θα γράφουμε $\delta(x) \mid \Delta(x)$*

5.2 Προαιρετική άσκηση για εξάσκηση

1. Δίνεται το σύστημα:

$$\mathbf{(\ \Sigma)}\quad \begin{array}{l} f(x) = (\alpha+7)x^3 + 5x^2 + (6+\beta)x + (\gamma+13) = 0 \\ g(x) = (\alpha+2\beta)x^4 + (\alpha+7)x^3 + 5x^2 + (6+\beta)x + (\gamma+13) = 0 \end{array}$$

όπου α,β,γ τα τρία τελευταία ψηφία του Αρ. Μητρώου σας αρχίζοντας από το τέλος

(α′) Να εκτελέσετε τη διαίρεση του $g(x)$ δια του $f(x)$ και να βρείτε το πηλίκο $\pi(x)$ και το υπόλοιπο $\upsilon(x)$

(β′) Να αποδείξετε ότι το σύνολο λύσεων του συστήματος **(Σ)** είναι ίσο με το σύνολο λύσεων του συστήματος:

$$(\ \Sigma^{\star}\ )\quad \begin{array}{l} f(x) = (\alpha+7)x^3 + 5x^2 + (6+\beta)x + (\gamma+13) = 0 \\ \upsilon(x) = 0 \end{array}$$

(γ′) Με βάση τα προηγούμενα να βρείτε το σύνολο λύσεων του συστήματος **(Σ)**

2. (α′) Δείτε το βίντεο[3] στη διεύθυνση εδώ Σκεφθείτε πάνω στο βασικό στόχο του μαθήματος με αφορμή το βίντεο και προσαρμόστε τον στόχο αυτό σε συστήματα πολυωνύμων μιας μεταβλητής.

   (β′) Να θεωρήσετε το σύστημα:

$$(\ \Sigma^*\ )\quad \begin{aligned} f(x) &= (\alpha+7)x^3+5x^2+(6+\beta)x+(\gamma+13)=0\\ g(x) &= (\alpha+2\beta)x^4+(\alpha+7)x^3+5x^2+(6+\beta)x+(\gamma+13)=0\\ h(x) &= x^5-9x+3=0 \end{aligned}$$

   όπου α,β,γ τα τρία τελευταία ψηφία του Αρ. Μητρώου σας αρχίζοντας από το τέλος.

   i. Χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο να βρείτε τρία πολυώνυμα $\kappa(x), \lambda(x), \xi(x) \in \mathbb{R}[x]$ έτσι ώστε:

$$MK\Delta(f(x), g(x), h(x)) = \kappa(x)\cdot f(x) + \lambda(x)\cdot g(x) + \xi(x)\cdot h(x)$$

   Στοιχεία για τον Ευκλείδειο αλγόριθμο μπορείτε να βρείτε είτε εδώ είτε στο βιβλίο Βασικής άλγεβρας εδώ

   ii. Να λύσετε το σύστημα $(\ \Sigma^*\ )$ με τη βοήθεια του ΜΚΔ παραπάνω

   iii. Διατυπώστε και αποδείξτε ένα θεώρημα επίλυσης συστημάτων πολυωνύμων μιας μεταβλητής με τη βοήθεια του ΜΚΔ.

[3] Ο σκηνοθέτης ζητάει συγνώμη για την ποιότητα του βίντεο.

Μέρος III

Πολυώνυμα πολλών μεταβλητών

Κεφάλαιο 6

Ο αλγόριθμος της διαίρεσης

6.1 Γενικά

Η πράξη της διαίρεσης στον δακτύλιο $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$,[1] όπου $\mathbb{F}$ είναι ένα σώμα, είναι καθοριστικής σημασίας για τη συνέχεια. Υπενθυμίζουμε ότι στον δακτύλιο των πολυωνύμων μιας μεταβλητής για να γίνει η διαίρεση χρειαζόμαστε:

1) Να έχουμε ένα διαιρετέο $\Delta(x) \in \mathbb{F}[x]$ και ένα διαιρέτη $\delta(x) \in \mathbb{F}[x]$ με $\delta(x) \neq 0$

2) Να διατάξουμε τα μονώνυμα του διαιρετέου και τα μονώνυμα του διαιρέτη χρησιμοποιώντας την φυσική διάταξη των δυνάμεων των μονονύμων.

Μετά την εκτέλεση της διαίρεσης έχουμε

$$\Delta(x) = \delta(x)\pi(x) + \upsilon(x) \text{ με } \left\{ \begin{array}{c} \upsilon(x) = 0 \\ \text{ή} \\ \upsilon(x) \neq 0 \text{ και } deg(\upsilon(x)) < deg(\delta(x)) \end{array} \right\}$$

Κάτι που πρέπει να τονισθεί ιδιαίτερα εδώ είναι ότι το πηλίκο $\pi(x)$ και το υπόλοιπο $\upsilon(x)$ είναι μοναδικά. Δες σχετικά στο 5 Σε όλες τις περιπτώσεις[2] αν $I =< f(x), g(x) >$ είναι το ιδεώδες του δακτυλίου $\mathbb{F}[x]$ που παράγεται από τα δύο πολυώνυμα $f(x), g(x)$ θα έχουμε ότι $\upsilon(x) \in I$. Με τα ιδεώδη θα ασχοληθούμε αναλυτικά στα επόμενα μαθήματα. Δείτε όμως τον ορισμό του ιδεώδους ενός δακτυλίου για καλύτερη κατανόηση του μαθήματος.

[1] Υπενθυμίζουμε ότι το σύνολο $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$, συμβολίζει το σύνολο των πολυωνύμων με μεταβλητές $x_1, x_2, \cdots, x_\nu$ και συντελεστές στοιχεία από το σώμα $\mathbb{F}$. Στο σύνολο αυτό, έχουν ορισθεί δύο πράξεις, η πράξη της πρόσθεσης πολυωνύμων και η πράξη του πολλαπλασιασμού πολυωνύμων. Η τριάδα $(\mathbb{F}[x_1, x_2, \cdots, x_\nu], +, \cdot)$ αναφέρεται ως *δακτύλιος των πολυωνύμων με ν μεταβλητές και συντελεστές από το σώμα* $\mathbb{F}$

[2] Υπενθυμίζουμε εδώ από την Βασική Άλγεβρα, ότι στο μηδενικό πολυώνυμο δεν επισυνάπτουμε βαθμό και τα σταθερά μη-μηδενικά πολυώνυμα έχουν βαθμό μηδέν

Θα μπορούσαμε να πούμε ότι κατά την εύρεση του υπολοίπου, η προσπάθειά μας επικεντρώνεται στην εύρεση ενός πολυωνύμου μέσα στο ιδεώδες $I =< f(x), g(x) >$, το οποίο να έχει τον ελάχιστο βαθμό.

Υπενθυμίζουμε επίσης ότι κάθε στοιχείο $h(x)$ του I είναι της μορφής $h(x) = \kappa(x)f(x) + \lambda(x)g(x)$, όπου $\kappa(x), \lambda(x) \in \mathbb{F}[x]$.

Δες επίσης και ένα σχετικό βίντεο εδώ

6.2 Βήματα διαίρεσης

Θα ορίσουμε τώρα μία διαδικασία διαίρεσης (αλγόριθμο διαίρεσης) στον δακτύλιο $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$ έτσι ώστε δοθέντων των πολυωνύμων

1. $\Delta(x_1, x_2, \cdots, x_\nu)$

2. $f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), f_3(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu)$

ο αλγόριθμος να δίνει:

1. Μία έκφραση του πολυωνύμου $\Delta(x_1, x_2, \cdots, x_\nu)$ ως εξής:

   $\Delta(x_1, x_2, \cdots, x_\nu) = \pi_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) +$
   $\pi_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) + \cdots + \pi_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu) +$
   $\upsilon_\mu(x_1, x_2, \cdots, x_\nu)$

2. Το πολυώνυμο $\upsilon_\mu(x_1, x_2, \cdots, x_\nu)$, το οποίο θα το λέμε **υπόλοιπο** της διαίρεσης και τη διατεταγμένη μ-άδα πολυωνύμων
   $(\pi_1(x_1, x_2, \cdots, x_\nu), \pi_2(x_1, x_2, \cdots, x_\nu), \cdots, \pi_\mu(x_1, x_2, \cdots, x_\nu))$, τήν οποία θα λέμε **πηλίκο** της διαίρεσης.

Στη συνέχεια θα προσπαθήσουμε να δούμε ένα παράδειγμα διαίρεσης ενός πολυωνύμου $\Delta(x, y)$ διά ενός ζεύγους πολυωνύμων $(f_1(x, y), f_2(x, y))$. Για ευκολία θεωρούμε και τα τρία πολυώνυμα με πραγματικούς συντελεστές.

Όπως είπαμε παραπάνω θέλουμε να οδηγηθούμε σε μια σχέση της μορφής:

$$\Delta(x, y) = \pi_1(x, y) \cdot f_1(x, y) + \pi_2(x, y) \cdot f_2(x, y) + \upsilon(x, y)$$

όπου:
$\Delta = \Delta(x, y)$: Διαιρετέος
$\delta = (f_1(x, y), f_2(x, y))$: διαιρέτης
$\pi = (\pi_1(x, y), \pi_2(x, y))$:πηλίκο
$\upsilon(x, y)$: υπόλοιπο

6.3 Παράδειγμα διαίρεσης στον δακτύλιο $\mathbb{F}[x,y]$

Παράδειγμα 6.3.1. *Να υπολογιστεί το αποτέλεσμα της διαίρεσης του πολυωνύμου* $\Delta(x,y) = g(x,y) = xy^2 + 1$ *με τα πολυώνυμα* $(f_1(x,y) = xy + 1, f_2(x,y) = y + 1)$.

Διαδικασία διαίρεσης

Βήμα 1 Δες εδώ το βίντεο μάθημα 4 βίντεο 1 για βοήθεια πριν τη μελέτη Θεωρούμε τώρα μία διάταξη στις μεταβλητές (π.χ. $x > y$). Η διάταξη αυτή επάγει μία διάταξη, την **λεξικογραφική**, στα μονώνυμα ως εξής: Παρατηρούμε ότι κάθε μονώνυμο είναι της μορφής $x^\kappa y^\lambda$, όπου κ και λ είναι μή αρνητικοί ακέραιοι[3]. Έτσι κάθε μονώνυμο καθορίζεται πλήρως από ένα ζεύγος $(\kappa,\lambda) \in \mathbb{Z}_{\geq 0}$. Ορίζουμε τώρα

$$(\kappa_1,\lambda_1) > (\kappa_2,\lambda_2) \Longleftrightarrow_{ορσ} \kappa_1 > \kappa_2 \ \ η' \ \ \kappa_1 = \kappa_2 \ \ και \ \ \lambda_1 > \lambda_2$$

και

$$x^{\kappa_1}y^{\lambda_1} > x^{\kappa_2}y^{\lambda_2} \Longleftrightarrow_{ορσ} (\kappa_1,\lambda_1) > (\kappa_2,\lambda_2)$$

Βήμα 2 Κατασκευάζουμε το παρακάτω διάγραμμα προκειμένου να αρχίσουμε την διαίρεση, γράφοντας τα πολυώνυμα που λαμβάνουν μέρος στη διαίρεση ως γραμμικό συνδυασμό μονονύμων με φθίνουσα σειρά.

$f_1(x,y) = xy + 1$	$g(x,y) = xy^2 + 1$
$f_2(x,y) = y + 1$	
$\pi_1(x,y) =$	
$\pi_2(x,y) =$	
$\upsilon(x,y) =$	

[3] Όπως έχουμε ξαναπεί στα πολυώνυμα δεν επιτρέπονται αρνητικοί εκθέτες

Βήμα 3 Θεωρούμε το μεγιστοβάθμιο όρο του Διαιρετέου (μαζί με τον συντελεστή του), ο οποίος στην περίπτωσή μας είναι ο xy^2 και τον μεγιστοβάθμιο όρο του πρώτου κατά σειρά πολυωνύμου του διαιρέτη (μαζί με τον συντελεστή του), που είναι ο xy. Εκτελούμε τη διαίρεση $xy^2 : xy$ και βρίσκουμε y. Εδώ σημειώνουμε ότι αν υπήρχαν και αριθμητικοί συντελεστές θα είχαμε και το πηλίκο αυτών, δηλαδή αν είχαμε $7xy^2$ δια $5xy$, τότε το αποτέλεσμα είναι $(7/5)y$. Θέτουμε στον πρώτο όρο του πηλίκου $\pi_1(x, y)$ μετά το $=$ το y. Έχουμε την παρακάτω εικόνα:

$f_1(x, y) = xy + 1$	$g(x, y) = xy^2 + 1$
$f_2(x, y) = y + 1$	
$\pi_1(x, y) = y$	
$\pi_2(x, y) =$	
$\upsilon(x, y) =$	

Βήμα 4 Πολλαπλασιάζουμε το πολυώνυμο $f_1(x, y) = xy + 1$ επί y και το αφαιρούμε από το $g(x) = xy^2 + 1$. Έχουμε την παρακάτω εικόνα:

$f_1(x, y) = xy + 1$	$g(x, y) = xy^2 + 1$
$f_2(x, y) = y + 1$	$y(xy + 1) = xy^2 + y, \quad g(x) - (xy^2 + y) = -y + 1$
$\pi_1(x, y) = y$	
$\pi_2(x, y) =$	
$\upsilon(x, y) =$	

Βήμα 5 Προέκυψε το πολυώνυμο $-y+1$, το οποίο είναι ένα **ενδιάμεσο υπόλοιπο**. Ο μεγιστοβάθμιος όρος του(μαζί με τον συντελεστή του) είναι ο $-y$. Ο

μεγιστοβάθμιος όρος του πρώτου όρου του διαιρέτη $f_1(x,y) = xy+1$ είναι ο xy. Παρατηρούμε ότι ο μεγιστοβάθμιος όρος xy του $f_1(x,y)$ δεν διαιρεί τον y.

Θεωρούμε τώρα τον μεγιστοβάθμιο όρο του $f_2(x,y) = y+1$, ο οποίος είναι ο y. Ο όρος αυτός διαιρεί τον $-y$, που είναι ο μεγιστοβάθμιος όρος του ενδιάμεσου υπολοίπου $-y+1$ και το πηλίκο είναι -1.

Κατόπιν πολλαπλασιάζουμε το -1 με το $f_2(x,y) = y+1$ και το αφαιρούμε από το ενδιάμεσο υπόλοιπο $-y+1$. Βρίσκουμε έτσι τον πρώτο όρο του πηλίκου $\pi_2(x,y)$, ο οποίος είναι ο -1 και το υπόλοιπο, που είναι ο αριθμός 2.

Τελικά έχουμε την παρακάτω εικόνα:

$f_1(x,y) = xy+1$	$g(x,y) = xy^2+1$
$f_2(x,y) = y+1$	$y(xy+1) = xy^2+y, \quad g(x) - (xy^2+y) = -y+1$ $-1\cdot(y+1) = -y-1, \quad -y+1-(-y-1) = 2$
$\pi_1(x,y) = y$	
$\pi_2(x,y) = -1$	
$\upsilon(x,y) = 2$	

Βήμα 6 Εδώ αναγκαστικά σταματάει η διαδικασία αυτή, διότι ο μεγιστοβάθμιος όρος του υπολοίπου $\upsilon(x,y) = 2$ είναι ο $2 \equiv 2\cdot x^0y^0$, ο οποίος δεν διαιρείται ούτε από τον μεγιστοβάθμιο όρο του $f_1(x,y)$ ούτε από τον μεγιστοβάθμιο όρο του $f_2(x,y)$.

Διατυπώνουμε το τελικό συμπέρασμά μας λέγοντας ότι το πηλίκο της διαίρεσης του πολυωνύμου $g(x,y) = xy^2+1$ δια του διατεταγμένου ζεύγους πολυωνύμων $(f_1(x,y) = xy+1, f_2(x,y) = y+1)$ είναι το διατεταγμένο ζεύγος πολυωνύμων $(\pi_1(x,y) = y, \pi_2(x,y) = -1)$ και το υπόλοιπο $\upsilon(x,y) = 2$. Δηλαδή ισχύει

$$g(x) = xy^2+1 = f_1(x,y)\cdot\pi_1(x,y) + f_2(x,y)\cdot\pi_2(x,y) + \upsilon(x,y)$$

Μετά τη μελέτη του παραδείγματος αυτού δείτε το βίντεο εδώ

6.4 Παράδειγμα διαίρεσης στον δακτύλιο $\mathbb{F}[x, y, z]$

Δίνουμε ακόμη ένα παράδειγμα διαίρεσης με τρείς μεταβλητές

Παράδειγμα 6.4.1. *Να υπολογιστεί το αποτέλεσμα της διαίρεσης του πολυωνύμου* $g(x, y, z) = 3x^5y^2z - xy^3z + 7yz + 18$ *με το ζεύγος πολυωνύμων* $(f_1(x, y, z) = x^3yz^5 + 1, f_2(x, y, z) = yz + 1)$.

Διαδικασία διαίρεσης

Βήμα 1 Θεωρούμε μία διάταξη στις μεταβλητές (π.χ. $x > y > z$). Η διάταξη αυτή επάγει μία διάταξη, την **λεξικογραφική**, στα μονώνυμα και αυτή με τη σειρά της μία διάταξη κατά φθίνουσα σειρά των μονονύμων στα πολυώνυμα. Έτσι έχουμε

$g(x, y, z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_1(x, y, z) = x^3yz^5 + 1$
$f_2(x, y, z) = yz + 1$

Βήμα 2 Κατασκευάζουμε το παρακάτω διάγραμμα προκειμένου να αρχίσουμε την διαίρεση.

$f_1(x, y, z) = x^3yz^5 + 1$	$g(x, y, z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_2(x, y) = yz + 1$	
$\pi_1(x, y) =$	
$\pi_2(x, y) =$	
$\upsilon(x, y) =$	

Βήμα 3 Θεωρούμε το μεγιστοβάθμιο όρο του Διαιρετέου (μαζί με τον συντελεστή του), ο οποίος στην περίπτωσή μας είναι ο $3x^5y^2z$ και τον μεγιστοβάθμιο όρο του πρώτου κατά σειρά πολυωνύμου του διαιρέτη (μαζί με τον συντελεστή του), που είναι ο x^3yz^5. Προσπαθούμε να εκτελέσουμε τη διαίρεση $3x^5y^2z : x^3yz^5$.

Η διαίρεση δεν γίνεται, διότι ο εκθέτης της μεταβλητής z είναι μεγαλύτερος στον δεύτερο όρο και για το λόγο αυτό επιχειρούμε να διαιρέσουμε το

μεγιστοβάθμιο όρο του Διαιρετέου (μαζί με τον συντελεστή του) με τον μεγιστοβάθμιο όρο του δευτέρου κατά σειρά πολυωνύμου του διαιρέτη (μαζί με τον συντελεστή του), που είναι ο yz.

Η διαίρεση τώρα γίνεται και έχουμε ως αποτέλεσμα $3x^5y$.
Το $3x^5y$ το τοποθετούμε στο πηλίκο, που αντιστοιχεί στο δεύτερο πολυώνυμο διαίρεσης.
Πολλαπλασιάζουμε το $3x^5y$ επί το $f_2(x, y) = yz + 1$ και το αφαιρούμε από το $g(x) = 3x^5y^2z - xy^3z + 7yz + 18$. Έχουμε έτσι την παρακάτω εικόνα:

$f_1(x, y, z) = x^3yz^5 + 1$	$g(x, y, z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_2(x, y, z) = yz + 1$	$g(x, y, z) - 3x^5yf_2(x, y, z)$
	$= 3x^5y^2z - xy^3z + 7yz + 18 - 3x^5y(yz + 1)$
$\pi_1(x, y, z)$	$= -xy^3z + 7yz + 18 - 3x^5y$
$\pi_2(x, y, z) = 3x^5y$	
$\upsilon(x, y, z) =$	

Βήμα 4 Προέκυψε το πολυώνυμο $-xy^3z+7yz+18-3x^5y$, το οποίο είναι ένα **ενδιάμεσο υπόλοιπο**. Γράφουμε το πολυώνυμο αυτό ως γραμμικό συνδυασμό μονονύμων με φθίνουσα σειρά χρησιμοποιώντας τη λεξικογραφική διάταξη, δηλαδή $-3x^5y - xy^3z + 7yz + 18$. Ο μεγιστοβάθμιος όρος του(μαζί με τον συντελεστή του) είναι ο $-3x^5y$. Ο μεγιστοβάθμιος όρος του πρώτου όρου του διαιρέτη $f_1(x, y, z) = x^3yz^5 + 1$ είναι ο x^3yz^5. Παρατηρούμε ότι ο μεγιστοβάθμιος όρος x^3yz^5 του $f_1(x, y, z)$ δεν διαιρεί τον $-3x^5y^4$.

Θεωρούμε τώρα τον μεγιστοβάθμιο όρο του $f_2(x, y, z) = yz + 1$, ο οποίος είναι ο yz. Ο όρος αυτός δεν διαιρεί τον $-3x^5y$, που είναι ο μεγιστοβάθμιος όρος του ενδιάμεσου υπολοίπου $-3x^5y - xy^3z + 7yz + 18$.

Στο σημείο αυτό **τοποθετούμε τον όρο $-3x^5y$ στο υπόλοιπο** και μένει ως ενδιάμεσο υπόλοιπο το $-xy^3z + 7yz + 18$.

Έτσι έχουμε την εικόνα:

[4] Υπενθυμίζουμε ότι στα πολυώνυμα δεν επιτρέπονται αρνητικοί εκθέτες στις μεταβλητές

$f_1(x,y,z) = x^3yz^5 + 1$	$g(x,y,z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_2(x,y,z) = yz + 1$	$g(x,y,z) - 3x^5yf_2(x,y,z)$
	$= 3x^5y^2z - xy^3z + 7yz + 18 - 3x^5y(yz+1)$
$\pi_1(x,y,z)$	$= -3x^5y - xy^3z + 7yz + 18$
$\pi_2(x,y,z) = 3x^5y$	$-xy^3z + 7yz + 18$
$\upsilon(x,y,z) = \mathbf{-3x^5y}$	

Βήμα 5 Προέκυψε το πολυώνυμο $-xy^3z+7yz+18$, το οποίο είναι ένα ακόμη **ενδιάμεσο υπόλοιπο**. Γράφουμε το πολυώνυμο αυτό ως γραμμικό συνδυασμό μονονύμων με φθίνουσα σειρά χρησιμοποιώντας τη λεξικογραφική διάταξη, δηλαδή $-xy^3z+7yz+18$. Ο μεγιστοβάθμιος όρος του(μαζί με τον συντελεστή του) είναι ο $-xy^3z$. Ο μεγιστοβάθμιος όρος του πρώτου όρου του διαιρέτη $f_1(x,y,z) = x^3yz^5 + 1$ είναι ο x^3yz^5. Παρατηρούμε ότι ο μεγιστοβάθμιος όρος x^3yz^5 του $f_1(x,y,z)$ δεν διαιρεί τον $-xy^3z$.

Θεωρούμε τώρα τον μεγιστοβάθμιο όρο του $f_2(x,y,z) = yz + 1$, ο οποίος είναι ο yz. Ο όρος αυτός διαιρεί τον $-xy^3z$, που είναι ο μεγιστοβάθμιος όρος του ενδιάμεσου υπολοίπου $-xy^3z+7yz+18$. Βρίσκουμε ως πηλίκο $-xy^2$ και το τοποθετούμε στο $\pi_2(x,y,z)$.

Έχουμε την εικόνα:

$f_1(x,y,z) = x^3yz^5 + 1$	$g(x,y,z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_2(x,y,z) = yz + 1$	$g(x,y,z) - 3x^5yf_2(x,y,z)$
	$= 3x^5y^2z - xy^3z + 7yz + 18 - 3x^5y(yz+1)$
$\pi_1(x,y,z)$	$= -3x^5y - xy^3z + 7yz + 18$
$\pi_2(x,y,z) = 3x^5y - xy^2$	$-xy^3z + 7yz + 18$
$\upsilon(\mathbf{x},\mathbf{y},\mathbf{z}) = \mathbf{-3x^5y}$	$-xy^3z + 7yz + 18$

Βήμα 6 Πολλαπλασιάζουμε το πηλίκο $-xy^2$ επί το $f_2(x,y,z) = yz + 1$ και το αφαιρούμε από το $-xy^3z + 7yz + 18$. Βρίσκουμε το $xy^2 + 7yz + 18$, το οποίο είναι το νέο μας ενδιάμεσο υπόλοιπο.

Η εικόνα μας γίνεται τώρα η εξής:

$f_1(x,y,z) = x^3yz^5 + 1$	$g(x,y,z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_2(x,y,z) = yz + 1$	$g(x,y,z) - 3x^5yf_2(x,y,z)$
	$= 3x^5y^2z - xy^3z + 7yz + 18 - 3x^5y(yz+1)$
$\pi_1(x,y,z)$	$= -3x^5y - xy^3z + 7yz + 18$
$\pi_2(x,y,z) = 3x^5y - xy^2$	$-xy^3z + 7yz + 18$
$\upsilon(\mathbf{x},\mathbf{y},\mathbf{z}) = \mathbf{-3x^5y}$	$-xy^3z + 7yz + 18 - (-xy^2(yz+1)) = xy^2 + 7yz + 18$

Βήμα 7 Συνεχίζουμε ξανά τη διαδικασία. Ο μεγιστοβάθμιος όρος του ενδιάμεσου υπολοίπου είναι ο xy^2, ο οποίος δεν διαιρείται με τον μεγιστοβάθμιο όρο του

πρώτου πολυωνύμου του διαιρέτη. Για το λόγο αυτό εξακολουθούμε να έχουμε το μηδενικό πολυώνυμο $\mathbf{0}(\mathbf{x})$, στο πρώτο πηλίκο. Η διαίρεση δεν συνεχίζεται ούτε με το δεύτερο πολυώνυμο-διαιρέτη. Για το λόγο αυτό βάζουμε το xy^2 στο υπόλοιπο και έχουμε την εικόνα ξανά

$f_1(x,y,z) = x^3yz^5 + 1$	$g(x,y,z) = 3x^5y^2z - xy^3z + 7yz + 18$
$f_2(x,y,z) = yz + 1$	$g(x,y,z) - 3x^5yf_2(x,y,z)$
	$= 3x^5y^2z - xy^3z + 7yz + 18 - 3x^5y(yz+1)$
$\pi_1(x,y,z)$	$= -3x^5y - xy^3z + 7yz + 18$
$\pi_2(x,y,z) = 3x^5y - xy^2$	$-xy^3z + 7yz + 18$
$\upsilon(\mathbf{x},\mathbf{y},\mathbf{z}) = \mathbf{-3x^5y + xy^2}$	$-xy^3z + 7yz + 18 - (-xy^2(yz+1)) = xy^2 + 7yz + 18$ $7yz + 18$

Βήμα 8 Τώρα φαίνεται πως θα συνεχίσουμε. Βρίσκουμε λοιπόν:

(α′) πηλίκο $\pi_1(x,y,z) = \mathbf{0}(\mathbf{x})$, το μηδενικό πολυώνυμο

(β′) πηλίκο $\pi_2(x,y,z) = 3x^5y - xy^2 + 7$

(γ′) υπόλοιπο $\upsilon(x,y,z) = -3x^5y + xy^2 + 11$

Βήμα 9 Επιβεβαιώνουμε το αποτέλεσμα:

$$\Delta(x,y,z) = g(x,y,z) = \pi_1(x,y,z)\cdot f_1(x,y,z) + \pi_2(x,y,z)\cdot f_2(x,y,z) + \upsilon(x,y,z)$$

6.5 Σχόλια πάνω στον αλγόριθμο της δαίρεσης πολυωνύμων πολλών μεταβλητών

6.5.1 Η λεξικογραφική διάταξη

Η λεξικογραφική[5] διάταξη ορίζεται στο σύνολο:

$$E = \{(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) \mid \alpha_i \in \{0, 1, 2, 3, \cdots, \} = \mathbb{N}\}$$

ως εξής:
$(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) > (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu) \Longleftrightarrow$

$\alpha_1 > \beta_1 \ \eta' \ (\alpha_1 = \beta_1 \ \kappa\alpha\iota \ \alpha_2 > \beta_2) \ \eta' \ (\alpha_1 = \beta_1 \ \kappa\alpha\iota \ \alpha_2 = \beta_2 \ \kappa\alpha\iota \ \alpha_3 > \beta_3)$
$\eta' \ \cdots \ (\alpha_1 = \beta_1 \ \kappa\alpha\iota \ \alpha_2 = \beta_2 \ \kappa\alpha\iota \ \alpha_3 = \beta_3, \cdots \kappa\alpha\iota \ \alpha_{\nu-1} = \beta_{\nu-1} \ \kappa\alpha\iota \ \alpha_\nu > \beta_\nu)$

1. Από τον ορισμό έχουμε ότι $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) > (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu) \Longleftrightarrow$ στη διαφορά $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) - (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu)$ η πρώτη μη-μηδενική συντεταγμένη είναι θετικός ακέραιος

2. Η λεξικογραφική διάταξη που ορίσαμε είναι ολική διάταξη, δηλαδή αν έχουμε δύο στοιχεία του E τα $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu)$ και $(\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu)$, τότε ακριβώς μία σχέση από τις παρακάτω ισχύει:

   (α') $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) > (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu)$

   (β') $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) < (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu)$

   (γ') $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) = (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu)$

3. Η λεξικογραφική διάταξη είναι συμβατή με την πρόσθεση διανυσμάτων δηλαδή εάν $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu), (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu) \ \kappa\alpha\iota \ (\gamma_1, \gamma_2, \cdots, \gamma_\nu)$ τρία στοιχεία του E και $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) > (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu)$, τότε

   $$(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) + (\gamma_1, \gamma_2, \cdots, \gamma_\nu) > (\beta_1, \beta_2, \beta_3, \cdots, \beta_\nu) + (\gamma_1, \gamma_2, \cdots, \gamma_\nu)$$

4. Κάθε πολυώνυμο $f(x_1, x_2, \cdots, x_\nu) \in \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, δηλαδή κάθε πολυώνυμο ν-μεταβλητών με συντελεστές από το σώμα $\mathbb{F}$, είναι άθροισμα μονονύμων της μορφής

   $$\lambda \cdot x_1^{\alpha_1} x_2^{\alpha_2} ... x_\nu^{\alpha_{nu}}$$

   όπου $\lambda \in \mathbb{F}$ και $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) \in E$
   Το λ λέγεται συντελεστής του μονονύμου
   και το διάνυσμα $(\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_\nu) \in E$ λέγεται βαθμός του μονονύμου.

[5] Σκεφθείτε πως βάζουμε τις λέξεις σε ένα λεξικό και θα δικαιολογήσετε το όνομα

5. Κάθε πολυώνυμο $f(x_1, x_2, \cdots, x_\nu) \in \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, με τη βοήθεια της λεξικογραφικής διάταξης στο Ε, μπορεί να τεθεί στη μορφή αθροίσματος μονονύμων με φθίνουσα διάταξη. Η μορφή αυτή είναι μοναδική.

6.

Θεώρημα 6.5.1. *Κάθε μή κενό υποσύνολο του Ε έχει ελάχστο*

ΑπόδειξηΈστω A_1 το σύνολο των ακεραίων που εμφανίζονται στην πρώτη συντεταγμένη στοιχείων του Ε. Το σύνολο αυτό είναι μη-κενό σύνολο φυσικών αριθμών, άρα θα έχει ελάχιστο έστω κ_1. Έστω A_2 το σύνολο των ακεραίων που εμφανίζονται στην δεύτερη συντεταγμένη στοιχείων του Ε. Το σύνολο αυτό είναι μη-κενό σύνολο φυσικών αριθμών, άρα θα έχει ελάχιστο έστω κ_2. Συνεχίζοντας βρίσκουμε μία ν-άδα φυσικών $(\kappa_1, \kappa_2, \cdots, \kappa_\nu)$. Η ν-άδα αυτή είναι στοιχείο του Ε και είναι το ελάχιστο στοιχείο του Ε (γιατί;;)

7.

Θεώρημα 6.5.2. *Ο αλγόριθμος τερματίζει σε πεπερασμένα βήματα*

Απόδειξη Άμεση από τα προηγούμενα

6.6 *Πηλίκο και υπόλοιπο*

Όταν ο αλγόριθμος της διαίρεσης του $\Delta(x_1, x_2, \cdots, x_\nu)$ δια του διανύσματος πολυωνύμων
$(f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), f_3(x_1, x_2, \cdots, x_\nu), \cdots, f_\mu(x_1, x_2, \cdots, x_\nu))$
τερματίσει έχουμε τη σχέση:

$$\begin{aligned}
&\Delta(x_1, x_2, \cdots, x_\nu) = \\
&\pi_1(x_1, x_2, \cdots, x_\nu) \cdot f_1(x_1, x_2, \cdots, x_\nu) \\
&+ \pi_2(x_1, x_2, \cdots, x_\nu) \cdot f_2(x_1, x_2, \cdots, x_\nu) \\
&+ \pi_3(x_1, x_2, \cdots, x_\nu) \cdot f_3(x_1, x_2, \cdots, x_\nu) \\
&+ \cdots + \pi_\mu(x_1, x_2, \cdots, x_\nu) \cdot f_\mu(x_1, x_2, \cdots, x_\nu)) \\
&+ \upsilon(x_1, x_2, \cdots, x_\nu)
\end{aligned}$$

1. Το πολυώνυμο $\Delta(x_1, x_2, \cdots, x_\nu)$
   το λέμε **Διαιρετέο**,
   Τη μ-άδα
   $(f_1(x_1, x_2, \cdots, x_\nu), f_2(x_1, x_2, \cdots, x_\nu), f_3(x_1, x_2, \cdots, x_\nu), \cdots,$
   $f_\mu(x_1, x_2, \cdots, x_\nu))$ τη λέμε **πηλίκο**
   και το πολυώνυμο
   $\upsilon(x_1, x_2, \cdots, x_\nu)$ το λέμε **υπόλοιπο** της διαίρεσης.

6.7 Ασκήσεις

Παρακάτω τα α,β,γ είναι τα ψηφία του Αρ Μητρώου σου αρχίζοντας από το τέλος

1. Να γίνει η διαίρεση του πολυωνύμου $f(x,y) = (\alpha+2)x^3y^5+(\beta+2)x^3y^2+xy+2$ δια του ζεύγους $g_1(x,y) = xy+1, g_2(x,y) = x+y^2-1$
2. Να γίνει η διαίρεση του πολυωνύμου $f(x,y) = (\alpha+2)x^3y^5+(\beta+2)x^3y^2+xy+2$ δια του ζεύγους $g_2(x,y) = x+y^2-1, g_1(x,y) = xy+1$
3. **Προαιρετικό** Τι θα λέγατε σε μία τάξη για να πείσετε ότι έχει ενδιαφέρον να μάθουν διαίρεση;;

Τέλος του τετάρτου μαθήματος

Κεφάλαιο 7

Βάσεις Groebner I

Τετάρτη 16 Μαρτίου 2016

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)*

Τέλος του πέμπτου μαθήματος

Κεφάλαιο 8

Βάσεις Groebner ενός ιδεώδους. Επανάληψη

8.1 *Ξανά το σύστημα*

Τετάρτη 30 Μαρτίου 2016

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 (Σ), 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** $f_1(x), f_2(x), \cdots, f_\mu(x)$.

[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

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 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*

Κεφάλαιο 9

Βάσεις Groebner ενός Ιδεώδους

9.1 Επαναλήψεις -σκέψεις -σχόλια

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*

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*

Κεφάλαιο 11

Και άλλα για τις βάσεις Groebner

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*
   $\mathbf{MO(I)}$=$\{\lambda \cdot x_1^{\xi_1} x_2^{\xi_2} \cdots x_\nu^{\xi_\nu}$, *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* $\mathbf{MO(I)}$ *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]

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*

[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

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

$$MO(g_i) \not< MO(g_1), MO(g_2), \cdots, MO(g_{i-1}), MO(g_{i+1}), \cdots, MO(g_\kappa)$$

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

$$Ορος(g_i) \not< MO(g_1), MO(g_2), \cdots, MO(g_{i-1}), MO(g_{i+1}), \cdots, MO(g_\kappa)$$

[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*

Τέλος του πέμπτου μαθήματος

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

Κεφάλαιο 12

Ο Αλγόριθμος του Buchberger

12.1 Ο Αλγόριθμος του Buchberger

Ως τώρα έχουμε συζητήσει και αποδείξει την ύπαρξη βάσης Groebner ενός ιδεώδους I. Παρακάτω θα διατυπώσουμε έναν αλγόριθμο εύρεσης βάσης Groebner, που οφείλεται στον Buchberger μαθητή του Groebner. Υπενθυμίζουμε ότι βάση Groebner ενός ιδεώδους I του δακτυλίου πολυωνύμων $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$ είναι ένα πεπερασμένο σύνολο πολυωνύμων του I.

Μία βάση Groebner του ιδεώδους I έχει πολλές χρήσιμες ιδιότητες, μεταξύ άλλων και την ιδιότητα να παράγουν το I. Οι βάσεις Groebner ορίσθηκαν αρχικά το 1965 από τον μαθητή του W. Groebner (1899-1980) τον B.Buchberger. Επίσης ο H.Hironaka το 1965 μελετώντας δακτυλίους δυναμοσειρών ανακάλυψε ανεξάρτητα από τον B.Buchberger την ίδια έννοια της βάσης Groebner. Χρειάσθηκαν μερικά χρόνια για να αναπτυχθούν και οι υπολογιστές, ώστε η θεωρία και οι εφαρμογές των βάσεων να λάβουν τη σημερινή μορφή

1. *Έστω $f_1(x_1, x_2, \cdots, x_\nu)$ και $f_2(x_1, x_2, \cdots, x_\nu)$ δύο πολυώνυμα του δακτυλίου $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$ Υποθέτουμε ότι οι μεγιστοβάθμιοι όροι των παραπάνω πολυωνύμων (μαζί με τους συντελεστές τους) είναι:*
   $\alpha \cdot x_1^{\kappa_1} x_2^{\kappa_2} \cdots x_\nu^{\kappa_\nu}$ του $f_1(x_1, x_2, \cdots, x_\nu)$ και
   $\beta \cdot x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_\nu^{\lambda_\nu}$ του $f_2(x_1, x_2, \cdots, x_\nu)$
   Υπενθυμίζουμε ότι πρέπει $\alpha \neq 0, \beta \neq 0, \kappa_i \geq 0, \lambda_i \geq 0, i = 1, 2, \cdots, \nu$

   Ορισμός 12.1.1. Ελάχιστο κοινό πολλαπλάσιο *των μονονύμων $x_1^{\kappa_1} x_2^{\kappa_2} \cdots x_\nu^{\kappa_\nu}$ και $x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_\nu^{\lambda_\nu}$ είναι το*
   $x_1^{\xi_1} x_2^{\xi_2} \cdots x_\nu^{\xi_\nu}$ όπου $\xi_i = max(\kappa_i, \lambda_i), i = 1, 2, 3, \cdots \nu$

2. *Συνεχίζουμε με ακόμη ένα ορισμό:*

   Ορισμός 12.1.2. *Έστω $f_1(x_1, x_2, \cdots, x_\nu)$ και $f_2(x_1, x_2, \cdots, x_\nu)$ δύο πολυώνυμα, όπως παραπάνω* ***S-πολυώνυμο*** *των f_1, f_2 είναι το πολυώνυμο*

$$S(f_1,f_2)=\frac{x_1^{\xi_1}x_2^{\xi_2}\cdots x_\nu^{\xi_\nu}}{\alpha\cdot x_1^{\kappa_1}x_2^{\kappa_2}\cdots x_\nu^{\kappa_\nu}}\cdot f_1-\frac{x_1^{\xi_1}x_2^{\xi_2}\cdots x_\nu^{\xi_\nu}}{\beta\cdot x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_\nu^{\lambda_\nu}}\cdot f_2$$

3. *Ένα σημαντικό θεώρημα εδώ είναι το παρακάτω*

   Θεώρημα 12.1.3. *Έστω $\mathbb{F}[x_1,x_2,\cdots,x_\nu]$ ο δακτύλιος των πολυωνύμων και $I=<f_1,f_2,\cdots,f_\mu>$ ένα ιδεώδες αυτού. Το σύνολο $G=\{f_1,f_2,\cdots,f_\mu\}$ είναι βάση Groebner του ιδεώδους I, εάν και μόνο εάν το υπόλοιπο της διαίρεσης του $S(f_i,f_j)$ διά του G είναι μηδέν για κάθε ζεύγος $i,j,i\neq j,1,j=1,2,\cdots,\nu$*

   Απόδειξη *Για την απόδειξη του βασικού αυτού θεωρήματος, το οποίο θα γίνει προσεχώς, χρειαζόμαστε μερικές προτάσεις και λήμματα:*

   Το παραπάνω θεώρημα οδηγεί στον αλγόριθμο του Buchberger.

   Για τη ζωή και το έργο του Buchberger δείτε εδώ

4. **Αλγόριθμος του Buchberger**

Βήμα 1 *Τοποθετούμε σε μία σειρά τα πολυώνυμα $f_1,f_2,\cdots,f_\mu$*

Βήμα 2 *Υπολογίζουμε το πολυώνυμο $S(f_1,f_2)$*

Βήμα 3 *Υπολογίζουμε το υπόλοιπο της διαίρεσης του $S(f_1,f_2)$ διά του συνόλου $\{f_1,f_2,\cdots,f_\mu\}$.*

Βήμα 4 *Εάν το προηγούμενο υπόλοιπο είναι μηδέν, τότε συνεχίζουμε με το $S(f_1,f_3)$ διαιρώντας το με το σύνολο $\{f_1,f_2,\cdots,f_\mu\}$.*
Εάν όμως δεν είναι μηδέν θεωρούμε το νέο σύνολο $\{f_1,f_2,\cdots,f_\mu,\upsilon(S(f_1,f_2))\}$[1] στη θέση του παλαιού.

Βήμα 5 *Συνεχίζουμε τον αλγόριθμο ελέγχοντας όλα τα $S(f_i,f_j)$ (Τα υπόλοιπά τους) και προσθέτοντας στο αρχικό σύνολο και τα πολυώνυμα $\upsilon(S(f_i,f_j))$ αν χρειάζεται.*

Βήμα 6 *Ο αλγόριθμος τερματίζει αν σε όλους τους ελέγχους που περιγράψαμε ΟΛΑ τα υπόλοιπα είναι μηδέν*

Δείτε στο internet τα παρακάτω για ευρύτερη μελέτη:

1. *Στη διεύθυνση εδώ για ένα αρκετά κατατοπιστικό άρθρο*

2. *Στη διεύθυνση εδώ το άρθρο από την εγκυκλοπαίδεια Wikipedia*

[1] Με $\upsilon(S(f_1,f_2))\}$ θα συμβολίζουμε το υπόλοιπο της διαίρεσης του $S(f_1,f_2)$ με τα υπόλοιπα πολυώνυμα

12.2 Ασκήσεις

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

1. *Να εφαρμόσετε τον αλγόριθμο του Buchberger για το ιδεώδες*
   $< f(x) = (\alpha + 2)x^3 + 5x + 3, (\beta + 2)x^2 + x + 1 > \lhd \mathbb{R}[x]$
2. *Να εφαρμόσετε τον αλγόριθμο του Buchberger για το ιδεώδες*
   $< h(x, y) = (\gamma + 2)x + (\alpha + 1)y - \alpha - \gamma - 3, \kappa(x, y) = x + y - 2 > \lhd \mathbb{R}[x, y]$

Τέλος του εβδόμου μαθήματος

Μέρος IV

Εφαρμογές

12.3 Τεχνητή Νοημοσύνη

Στο κεφάλαιο αυτό θα ασχοληθούμε με τη γενική μαθηματική ιδέα της τεχνητής νοημοσύνης .

12.4 Το Θεώρημα βάσης του Hilbert

Θεώρημα 12.4.1. *Έστω I ένα ιδεώδες του δακτυλίου πολυωνύμων $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$. Υπάρχει πεπερασμένο πλήθος πολυωνύμων του $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$, το οποίο παράγει το I.*

Απόδειξη: *Αν το I είναι το μηδενικό ιδεώδες, δηλαδή $I = \{\mathbf{0}\}$, τότε μπορούμε να πούμε ότι το μηδενικό πολυώνυμο του $\mathbb{F}[x_1, x_2, \cdots, x_\nu]$ παράγει το I και έτσι το θεώρημα ισχύει.*

Έστω τώρα ότι $I \neq \{\mathbf{0}\}$. Όπως έχουμε αποδείξει το I έχει (τουλάχιστον) μία βάση Groebner, έστω
$B = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), g_3(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\}$.

Θα αποδείξουμε ότι το B παράγει το I, δηλαδή το σύνολο των πολυωνυμικών συνδυασμών του B είναι ίσο με το I.

Έστω $f(x_1, x_2, \cdots, x_\nu)$ ένα πολυώνυμο του ιδεώδους I. Κάνουμε τη διαίρεση του $f(x_1, x_2, \cdots, x_\nu)$ διά του συνόλου B. Έχουμε:

$f(x_1, x_2, \cdots, x_\nu) =$
$h_1(x_1, x_2, \cdots, x_\nu) \cdot g_1(x_1, x_2, \cdots, x_\nu) + \cdots + h_\kappa(x_1, x_2, \cdots, x_\nu) \cdot g_\kappa(x_1, x_2, \cdots, x_\nu) +$
$\Upsilon(x_1, x_2, \cdots, x_\nu)$, *όπου $\Upsilon(x_1, x_2, \cdots, x_\nu)$ τουπόλοιπο της διαίρεσης.*

Την τελευταία σχέση μπορούμε να την γράψουμε:

$\Upsilon(x_1, x_2, \cdots, x_\nu) = f(x_1, x_2, \cdots, x_\nu) - h_1(x_1, x_2, \cdots, x_\nu) \cdot g_1(x_1, x_2, \cdots, x_\nu) -$
$\cdots - h_\kappa(x_1, x_2, \cdots, x_\nu) \cdot g_\kappa(x_1, x_2, \cdots, x_\nu)$

Επειδή τα πολυώνυμα $f(x_1, x_2, \cdots, x_\nu), g_1(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)$ ανήκουν στο ιδεώδες I θα ανήκει επίσης στο ιδεώδες και το πολυώνυμο $\Upsilon(x_1, x_2, \cdots, x_\nu)$

Όμως το σύνολο $B = \{g_1(x_1, x_2, \cdots, x_\nu), g_2(x_1, x_2, \cdots, x_\nu), g_3(x_1, x_2, \cdots, x_\nu), \cdots, g_\kappa(x_1, x_2, \cdots, x_\nu)\}$ είναι μία βάση Groebner του I, άρα ο μεγιστοβάθμιος όρος του $\Upsilon(x_1, x_2, \cdots, x_\nu)$ θα ανήκει στο ιδεώδες που παράγουν οι μεγιστοβάθμιοι όροι των πολυωνύμων του συνόλου B (δες τον ορισμό της βάσης Groebner .)

Υπάρχουν τώρα δύο περιπτώσεις:

1. *Το πολυώνυμο $\Upsilon(x_1, x_2, \cdots, x_\nu)$ να είναι το μηδενικό πολυώνυμο, οπότε έχουμε ότι το $f(x_1, x_2, \cdots, x_\nu)$ ανήκει στο ιδεώδες που παράγεται από το σύνολο B, κάτι στο οποίο θέλαμε να καταλήξουμε.*

2. *Το πολυώνυμο $\Upsilon(x_1, x_2, \cdots, x_\nu)$ να μήν είναι το μηδενικό πολυώνυμο, οπότε έχει κάποιον μη-μηδενικό μεγιστοβάθμιο όρο. Ο τελευταίος θα διαιρείται από κάποιον μεγιστοβάθμιο όρο κάποιου πολυωνύμου του B. Για να δείτε ότι ισχύει ο τελευταίος ισχυρισμός, δείτε το βίντεο εδώ ή εδώ. Όμως αν συνέβαινε*

κάτι τέτοιο η αρχική διαίρεση θα είχε προχωρήσει και δεν θα είχαμε αυτό το υπόλοιπο. Καταλήγουμε έτσι σε άτοπο.

Πόρισμα 12.4.2. *Ένα πολυώνυμο $f(x_1, x_2, \cdots, x_\nu) \in \mathbb{F}[x_1, x_2, \cdots, x_\nu]$, ανήκει στο ιδεώδες I εάν και μόνο εάν το υπόλοιπό του από τη διαίρεση με μία βάση Groebner του I είναι μηδέν.*

Απόδειξη *άμεση από τα προηγούμενα*
Η πρώτη εφαρμογή σχετίζεται με το ερώτημα:

Ερώτημα 1. *Μπορεί ο υπολογιστιστής να αποδεικνύει μαθηματικά θεωρήματα;*

12.5 Αυτόματη απόδειξη Γεωμετρικών Θεωρημάτων

Η ιδέα της αυτόματης απόδειξης είναι η παρακάτω:
Εάν οι υποθέσεις και τα συμπεράσματα ενός θεωρήματος μπορούν να διατυπωθούν με πολυώνυμα, τότε η απόδειξη του θεωρήματος συνίσταται στην εξέταση εάν κάποια πολυώνυμα βρίσκονται σε ένα ιδεώδες ή όχι
Δείτε πληροφορίες για τον επιστημονικό κλάδο
Automated theorem proving εδώ
Παρακάτω δίνουμε ένα παράδειγμα για να φανεί η ιδέα:

Παράδειγμα 12.5.1. *Έστω Α,Β,Δ,Γ οι κορυφές ενός παραλληλογράμμου*[2] *(με τη σειρά που δίδονται). Να δειχθεί ότι οι διαγώνιες ΑΔ και ΒΓ διχοτομούνται*

Αυτόματη γεωμετρική απόδειξη

1. *Θεωρούμε ένα παλληλόγραμμο ΑΒΔΓ με ΑΒ παράλληλο του ΔΓ και ΒΔ παράλληλο του ΑΓ (***προσοχή στο σχήμα***)*

2. *Οι ιδιότητες των σχημάτων στην Ευκλείδεια Γεωμετρία παραμένουν οι ίδιες αν εφαρμόσουμε σε αυτά στροφές ή μεταφορές. Έτσι μπορούμε να θεωρήσουμε ότι η κορυφή Α είναι στην αρχή των αξόνων (0,0) και η ακμή ΑΒ στον οριζόντιο άξονα με $B = (u_1, 0)$ για κάποιο $u_1 \neq 0$*

3. *Μπορούμε να θεωρούμε το u_1 ως ανεξάρτητη μεταβλητή.*

4. *Η κορυφή $\Gamma = (u_2, u_3)$ εισάγει δύο νέες μεταβλητές u_2 και u_3. Η κορυφή Δ δεν εισάγει νέες ανεξάρτητες μεταβλητές, διότι η δήλωση ότι το ΑΒΓΔ είναι παραλληλόγραμμο, σημαίνει, μεταξύ άλλων, ότι η θέση του Δ προσδιορίζεται πλήρως από τη θέση των Α,Β και Γ*

[2] Ευχαριστώ θερμά τον Στέλιο Βιτωράκη για την σχεδίαση

5. *Ας συμβολίσουμε με* $\Delta = (x_1, x_2)$ *τις συντεταγμένες του* Δ

6. *Έχουμε ότι* AB *παράλληλος της* $\Delta\Gamma$, *άρα* $x_2 - u_3 = 0$ 

7. *Έχουμε* $A\Gamma$ *παράλληλος της* $B\Delta$, *άρα* $\frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1}$

8. *Θεωρούμε δύο πολυώνυμα* $h_1(u_1, u_2, u_3, x_1, x_2) = x_2 - u_3$ *και* $h_2(u_1, u_2, u_3, x_1, x_2) = (x_1 - u_1)u_3 - x_2u_2$. *Τα πολυώνυμα αυτά ανήκουν στον δακτύλιο* $\mathbb{R}[u_1, u_2, u_3, x_1, x_2]$ *των πολυωνύμων πέντε μεταβλητών με συντελεστές πραγματικούς αριθμούς. Από τα παραπάνω έχουμε ότι:*

Το $AB\Delta\Gamma$ *είναι παραλληλόγραμμο εάν και μόνο εάν* $h_1(u_1, u_2, u_3, x_1, x_2) = 0$ *και* $h_1(u_1, u_2, u_3, x_1, x_2) = 0$

9. *Ας υποθέσουμε τώρα ότι το σημείο τομής των διαγωνίων είναι το* $N = (x_3, x_4)$. *Η δήλωση ότι το* N *είναι το σημείο τομής των διαγωνίων είναι ισοδύναμη με τη δήλωση ότι οι τριάδες σημείων (A,N,Δ) και (B,N,Γ) αποτελούνται από συγγραμμικά σημεία.*

10. *Έχουμε:*

    (α′) *Τα A,N,Δ συγγραμμικά εάν και μόνο εάν* $\frac{x_4}{x_3} = \frac{u_3}{x_1}$

    (β′) *Τα B,N,Γ συγγραμμικά εάν και μόνο εάν* $\frac{x_4}{x_3 - u_1} = \frac{u_3}{u_2 - u_1}$

11. *Θεωρούμε τα πολυώνυμα* $h_3(u_1, u_2, u_3, x_1, x_2) = x_4x_1 - x_3u_3$ *και* $h_4(u_1, u_2, u_3, x_1, x_2) = x_4(u_2 - u_1) - (x_3 - u_1)u_3$

12. *Μπορούμε εδώ να σκεφθούμε και να αποδείξουμε εύκολα ότι οι υποθέσεις ισχύουν εάν και μόνο εάν*
δηλαδή μετατρέψαμε τις υποθέσεις του θεωρήματος σε σχέσεις πολυωνύμων.

13. *Τώρα σκεφτόμαστε σχετικά με τα ζητούμενα, δηλαδή την διερεύνηση του ερωτήματος εάν οι διαγώνιοι διχοτομούνται. Έχουμε ότι*

Οι διαγώνιοι διχοτομούνται εάν και μόνο εάν $AN = N\Delta$ *και* $BN = N\Gamma$.

Το παραπάνω είναι ισοδύναμο με τα εξής:

(α′) $AN = N\Delta$ *εάν και μόνο εάν* $x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2$

(β′) $BN = N\Gamma$ *εάν και μόνο εάν* $(x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2$

14. *Θεωρούμε τα πολυώνυμα:*
$g_1(u_1, u_2, u_3, x_1, x_2) = -x_3^2 - x_4^2 + (x_3 - x_1)^2 + (x_4 - x_2)^2$ *και*
$g_2(u_1, u_2, u_3, x_1, x_2) = (x_3 - u_2)^2 + (x_4 - u_3)^2 - (x_3 - u_1)^2 - x_4^2$

15. *Προφανώς τα συμπεράσματα που θέλουμε να αποδείξουμε κωδικοποιούνται στα πολυώνυμα* $g_1(u_1, u_2, u_3, x_1, x_2)$ *και* $g_2(u_1, u_2, u_3, x_1, x_2)$ *με*
$g_1(u_1, u_2, u_3, x_1, x_2) = x_1^2 - 2x_1x_3 - 2x_4x_2 + x_2^2$ *και*
$g_2(u_1, u_2, u_3, x_1, x_2) = 2x_3u_1 - 2x_3u_2 - 2x_4u_3 - u_1^2 + u_2^2 + u_3^2$

16. *Αναλύουμε λίγο περισσότερο τα παραπάνω: Οι υποθέσεις μας είναι ότι το σχήμα* $AB\Delta\Gamma$ *είναι παραληλλόγραμμο και ότι οι ευθείες* $A\Delta$ *και* $B\Gamma$ *τέμνονται στο* N*. Οι υποθέσεις αυτές ισοδυναμούν με τον μηδενισμό των πολυωνύμων*

$$\begin{matrix} h_1(u_1, u_2, u_3, x_1, x_2) \\ h_2(u_1, u_2, u_3, x_1, x_2) \\ h_3(u_1, u_2, u_3, x_1, x_2) \\ h_4(u_1, u_2, u_3, x_1, x_2) \end{matrix}$$

. Εμείς θέλουμε να αποδείξουμε ότι οι διαγώνιες διχοτομούνται. Αυτό είναι ισοδύναμο με τον μηδενισμό των πολυωνύμων $g_1(u_1, u_2, u_3, x_1, x_2)$ *και* $g_2(u_1, u_2, u_3, x_1, x_2)$ *Αν τα πολυώνυμα* g_1 *και* g_2 *ανήκουν στο ιδεώδες* $< h_1, h_2, h_3, h_4 >$*, τότε τα* g_1 *και* g_2 *είναι πολυωνυμικοί συνδυασμοί των* $\{h_1, h_2, h_3, h_4\}$*. Αν για παράδειγμα έχουμε*
$g_1(u_1, u_2, u_3, x_1, x_2) = \xi_1(u_1, u_2, u_3, x_1, x_2) \cdot h_1(u_1, u_2, u_3, x_1, x_2) + \cdots +$
$\xi_4(u_1, u_2, u_3, x_1, x_2) \cdot h_4(u_1, u_2, u_3, x_1, x_2)$*, τότε ο μηδενισμός των* $\{h_1, h_2, h_3, h_4\}$ *συνεπάγεται τον μηδενισμό του* g_1

17. *Ο υπολογιστής μας, λοιπόν, προκειμένου να αποδείξει το θεώρημα, θα υπολογίσει μία βάση Groebner του ιδεώδους* $I =< h_1, h_2, h_3, h_4 >$*, και μετά το υπόλοιπο της διαίρεσης των* g_1 *και* g_2 *με τη βάση αυτή. Γνωρίζουμε ότι τα υπόλοιπα της διαίρεσης με βάση Groebner είναι μοναδικά και τα πολυώνυμα ανήκουν στο ζητούμενο ιδεώδες εάν και μόνο εάν το υπόλοιπο είναι το μηδενικό πολυώνυμο. (***Να κάνετε εσείς τον έλεγχο** *).*

12.6 Τεχνητή Νοημοσύνη και Γραμμική άλγεβρα

Μια γνωστή μας άσκηση από την γραμμική άλγεβρα είναι ότι αν έχουμε έναν πίνακα $A \in \mathbb{R}^{2\times 2}$ *με* $A^3 = 0$ *τότε* $A^2 = 0$*. Προσπαθήστε αρχικά να την λύσετε με τη βοήθεια των γνώσεών σας από τη Γραμμική άλγεβρα.*

Για τη λύση της παραπάνω άσκησης στη Γραμμική άλγεβρα χρησιμοποιούμε το χαρακτηριστικό και το ελάχιστο πολυώνυμο. Εργαζόμαστε ως εξής: Ο πίνακας A *μηδενίζει το πολυώνυμο* $f(x) = x^3$*. Αν* $m(x)$ *είναι το ελάχιστο πολυώνυμο του πίνακα, γνωρίζουμε ότι το* $m(x)$ *θα είναι το πολύ δευτέρου βαθμού και θα διαιρεί το* $f(x) = x^3$*. Οι μόνες περιπτώσεις είναι οι* $m(x) = x$ *και* $m(x) = x^2$*. Όμως ο πίνακας* A *μηδενίζει το ελάχιστο πολυώνυμό του. Τελικά είτε A=0 είτε* $A^2 = 0$*. Και στις*

δύο περιπτώσεις μπορούμε να αποδείξουμε ότι $A^2 = 0$. *Σχόλιο: Εδώ εργασθήκαμε όπως συνήθως εργαζόμαστε στη Γραμμική άλγεβρα*[3]

Θα παρουσιάσουμε τώρα μια προσέγγιση με τη θεωρία βάσεων Grobner που έχουμε μάθει. Έστω λοιπόν ότι ο πινακάς μας είναι ο

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Με την υπόθεση ότι

$$A^3 = \begin{pmatrix} a^3 + 2abc + bcd & a^2b + b^2c + abd + bd^2 \\ a^2c + acd + c^2d + gd^2 & abc + 2bcd + d^3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

θα δείξουμε ότι

$$A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & cb + d^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Η υπόθεση της άσκησης μπορεί να εκφραστεί με την γλώσσα των πολυωνύμων ως

$$\begin{aligned} f_1 &= a^3 + 2abc + bcd = 0 \\ f_2 &= a^2b + b^2c + abd + bd^2 = 0 \\ f_3 &= a^2c + acd + c^2d + cd^2 = 0 \\ f_4 &= abc + 2bcd + d^3 = 0 \end{aligned}$$

και το συμπέρασμα ως

$$\begin{aligned} g_1 &= a^2 + bc \\ g_2 &= ab + bd \\ g_3 &= ac + cd \\ g_4 &= bc + d^2 \end{aligned}$$

Θεωρούμε το ιδεώδες $I =< f_1, f_2, f_3, f_4 >$ *και βρίσκουμε μια βάση Grobner* G. *Εκτελέστε τις διαιρέσεις* g_1 *με* G, g_2 *με* G, g_3 *με* G *και* g_4 *με* G *και βρείτε το υπόλοιπο τους. Τι παρατηρείτε*;

1. *Στο ορθογώνιο τρίγωνο ΑΒΓ(με ορθή γωνία την Α), σχηματίζουμε το ύψος ΑΗ. Εξετάστε εάν ένας υπολογιστής με την « γλώσσα των πολυωνύμων», μπορεί να αποδείξει, ότι τα τρία μέσα των πλευρών και το σημείο Η βρίσκονται στην περιφέρεια κάποιου κύκλου.*

[3]Ξεφυλίστε στα γρήγορα εδώ ένα βιβλίο Γραμμικής άλγεβρας για να θυμηθείτε τα σχετικά θεωρήματα

2. *Εξετάστε εάν ένας υπολογιστής με την « γλώσσα των πολυωνύμων», μπορεί να αποδείξει, ότι οι τρείς διάμεσοι οποιουδήποτε τριγώνου διέρχονται από το ίδιο σημείο.*

3. *Εξετάστε εάν ένας υπολογιστής με την « γλώσσα των πολυωνύμων», μπορεί να αποδείξει, ότι οι τρείς διχοτόμοι οποιουδήποτε τριγώνου διέρχονται από το ίδιο σημείο.*

4. *Εξετάστε εάν ένας υπολογιστής με την « γλώσσα των πολυωνύμων», μπορεί να αποδείξει, ότι τα τρία ύψη οποιουδήποτε τριγώνου διέρχονται από το ίδιο σημείο.*

5. *Εξετάστε εάν ένας υπολογιστής με την « γλώσσα των πολυωνύμων», μπορεί να αποδείξει το παρακάτω θεώρημα του Euler: Σε κάθε τρίγωνο το ορθόκεντρο (σημείο τομής των υψών), το κέντρο του περιγεγραμμένου κύκλου και το σημείο τομής των διαμέσων είναι συγγραμμικά σημεία*

Κεφάλαιο 13

Βάσεις Groebner και Ρομποτική

Στο κεφάλαιο αυτό θα μελετήσουμε επίπεδα ρομπότ για να κατανοήσουμε τις μαθηματικές ιδέες που απαιτούνται για τη λειτουργία τους.

Για ευρύτερη μελέτη μπορεί κανείς να δεί εδώ
και επίσης στο βιβλίο εδώ σελίδα 261. Στην πραγματικότητα δεν υπάρχουν επίπεδα ρομπότ και έτσι θεωρούμε ουσιαστικά την προβολή ενός τρισδιάστατου ρομπότ επί ενός επιπέδου.

Ένα ρομπότ, λοιπόν, θα είναι ένα σύνολο βραχιόνων, οι οποίοι συνδέονται με αρθρώσεις. Θα θεωρούμε ότι οι βραχίονες έχουν σταθερό μήκος και οι αρθρώσεις αφήνουν τους βραχίονες να περιστραφούν πλήρως.

Για να φανεί η μέθοδος μελέτης θα περιγράψουμε ένα παράδειγμα

Παράδειγμα 13.0.1. *Να μελετηθεί ένα επίπεδο ρομπότ με ένα σταθερό βραχίονα και δύο μετακινούμενους.*

Το μήκος του σταθερού βραχίονα είναι α_0. Το μήκος του πρώτου κινητού βραχίονα είναι α_1 και του δεύτερου α_2. Σε κάθε άρθρωση θεωρούμε ένα σύστημα συντεταγμένων. Έτσι έχουμε ένα σταθερό σύστημα συντεταγμένων στον αρχικό βραχίονα (στην σταθερή άρθρωση) και ένα σύστημα συντεταγμένων σε κάθε άλλη άρθρωση. *Σύστημα συντεταγμένων σημαίνει δύο άξονες. Σε κάθε άρθρωση ο ένας άξονας είναι ο άξονας που προσδιορίζει ο προηγούμενος βραχίονας και ο άλλος ο κάθετος. Σε αθε άρθρωση έχουμε και μία γωνία, η οποία είναι η γωνία που πρέπει να περιστραφεί ο προηγούμενος βραχίονας με φορά αντίθετη των δεικτών του ρολογιού για να συμπέσει στον επόμενο βραχίονα. Δες και τα σχήματα παρακάτω.*

Μπορείτε επίσης να δείτε τα σχήματα:
εδώ

και
εδώ
Δείτε *επίσης στην σελίδα του μαθήματος τις συνδέσεις robot*1 *και robot*2

Εδώ[1] *μας ενδιαφέρει η θέση του τελευταίου σημείου (χεριού). Είναι γεγονός επίσης ότι η διαφορετική κατασκευή του άκρου απαιτεί από ένα μαθηματικό να λύσει ενδεχομένως διαφορετικές εξισώσεις. Για να προσδιορίσουμε τη θέση του ακραίου σημείου, αρκεί να βρούμε τις συντεταγμένες ως προς το σταθερό σύστημα συντεταγμένων. Αν λοιπόν έχουμε δύο κινητούς βραχίονες έχουμε ότι η προβολή στον οριζόντιο άξονα είναι*

$$x_0 = \alpha_1 \cdot \sigma\upsilon\nu(\theta_1) + \alpha_2 \cdot \sigma\upsilon\nu(\theta_1 + \theta_2)$$

Ομοίως στον κάθετο άξονα του σταθερού συστήματος συντεταγμένων έχουμε:

$$y_0 = \alpha_1 \cdot \eta\mu(\theta_1) + \alpha_2 \cdot \eta\mu(\theta_1 + \theta_2)$$

Δύο είναι τα προβλήματα που φυσιολογικά εμφανίζονται

1. **Το ευθύ κινηματικό πρόβλημα**
   Το πρόβλημα αυτό διατυπώνεται ως εξής: Δεδομένου του ρομπότ (δηλαδή των βραχιόνων, αρθρώσεων κλπ) και επίσης δεδομένων των συντεταγμένων (x_0, y_0) να βρεθεί αν το χέρι, φτάνει στο σημείο αυτό και με πόσους τρόπους. Αυτό είναι ισοδύναμο αν το σύστημα

   $$\begin{aligned} x_0 &= \alpha_1 \cdot \sigma\upsilon\nu(\theta_1) + \alpha_2 \cdot \sigma\upsilon\nu(\theta_1 + \theta_2) \\ y_0 &= \alpha_1 \cdot \eta\mu(\theta_1) + \alpha_2 \cdot \eta\mu(\theta_1 + \theta_2) \end{aligned}$$

   έχει λύσεις και πόσες. Το πρόβλημα είναι όμως ότι στο σύστημα εμπλέκονται τριγωνομετρικές συναρτήσεις (οι οποίες **δεν** *είναι πολυωνυμικές)*[2]*. Μία πρόσθετη δυσκολία είναι ότι εμφανίζονται τριγωνομετρικοί αριθμοί αθροίσματος. Για να αντιμετωπίσουμε τα παραπάνω εμπόδια εργαζόμαστε ως εξής:*

   Κατ΄ αρχήν είναι γνωστές οι τριγωνομετρικές σχέσεις:
   $\sigma\upsilon\nu(\theta_1 + \theta_2) = \sigma\upsilon\nu(\theta_1) \cdot \sigma\upsilon\nu(\theta_2) - \eta\mu(\theta_1) \cdot \eta\mu(\theta_2)$
   $\eta\mu(\theta_1 + \theta_2) = \eta\mu(\theta_1) \cdot \sigma\upsilon\nu(\theta_2) + \eta\mu(\theta_2) \cdot \sigma\upsilon\nu(\theta_1)$
   Θέτουμε $\sigma\upsilon\nu(\theta_1) = x_1, \eta\mu(\theta_1) = y_1, \sigma\upsilon\nu(\theta_2) = x_2, \eta\mu(\theta_1) = y_2$

[1] Ευχαριστώ θερμά τον Στέλιο Βιτωράκη για την σχεδίαση

[2] Ένας εύκολος τρόπος για να δεί κανείς ότι η συνάρτηση $f(x) = \eta\mu(x)$ δεν είναι πολυωνυμική είναι η παραγώγιση. Παραγωγίζοντας πολλές φορές ένα πολυώνυμο μιας μεταβλητής με πραγματικούς συντελεστές γίνεται η μηδενική συνάρτηση, ενώ η συνάρτηση $f(x) = \eta\mu(x)$ δεν γίνεται ποτέ

και έχουμε το παρακάτω σύστημα πολυωνυμικών εξισώσεων

$$\begin{aligned} x_0 &= \alpha_1 \cdot x_1 + \alpha_2 \cdot (x_1 x_2 - y_1 y_2) \\ y_0 &= \alpha_1 \cdot y_1 + \alpha_2 (x_1 y_2 + x_2 y_1) \\ x_1^2 + y_1^2 &= 1 \\ x_2^2 + y_2^2 &= 1 \end{aligned}$$

Αν τα x_0, y_0 είναι δεδομένα, τότε αναγόμαστε σε ένα σύστημα πολυωνυμικών εξισώσεων, το οποίο το λύνουμε χρησιμοποιώντας κάποιο υπολογιστικό πακέτο (π.χ το Axiom). Μπορούμε επίσης να βρούμε και τη βάση Groebner του συστήματος και να κάνουμε διερεύνηση για το σύνολο λύσεων. Μη κενό σύνολο λύσεων του συστήματος, σημαίνει ότι το άκρο του Ρομπότ φθάνει στο συγκεκριμένο σημείο. Κάθε λύση δίνει και έναν διαφορετικό τρόπο προσέγγισης.

Είναι ενδεχόμενο επίσης να έχουμε τρείς κινούμενους βραχίονες, οπότε θα εμφανισθούν τριγωνομετρικοί αριθμοί της μορφής
$συν(\theta_1 + \theta_2 + \theta_3), ημ(\theta_1 + \theta_2 + \theta_3)$. Στην περίπτωση αυτή αναπυσσουμε τον τριγωνομετρικό αριθμό του αθροίσματος και εργαζόμαστε όπως πρίν.

2. **Το αντίστροφο κινηματικό πρόβλημα**

   Το αντίστροφο κινηματικό πρόβλημα διατυπώνεται ως εξής: Δεδομένου ενός Ροπμότ όπως παραπάνω, να βρεθεί το σύνολο των σημείων, στα οποία προσεγγίζει το άκρο του Ρομπότ. Ποια είναι τα γεωμετρικά χαρακτηριστικά αυτού του συνόλου; Εδώ στην πραγματικότητα έχουμε να βρούμε το πεδίο τιμών μιάς συνάρτησης

13.1 Ασκήσεις

1. *Δίνεται ένα επίπεδο ρομπότ με δύο βραχίονες. Οι βραχίονες έχουν μήκη $l_1 = \alpha + 3$ και $l_2 = \beta + \gamma + 5$. Να εξετασθεί εάν το χέρι του ρομπότ μπορεί να προσεγγίσει το σημείο $(\gamma + 10, \alpha + 10)$.*

2. *Δίνεται ένα επίπεδο ρομπότ με τρεις ίσους βραχίονες, ο καθένας έχει μήκος $l = \alpha + \beta + \gamma + 1$. Να βρεθούν οι συντεταγμένες των σημείων που μπορεί να προσεγγίσει*

Τέλος του ογδόου μαθήματος