Βάσεις Gröbner

Διάλεξη Μάριου Μαγιολαδίτη
8 Απρίλη 2002

1. Εισαγωγή

Σε αυτή τη σειρά διαλέξεων θα μελετήσουμε τη μέθοδο των βάσεων Gröbner με σκοπό να λύσουμε προβλήματα σχετικά με πολυωνυμικά ιδεώδη με αλγοριθμικό ή υπολογιστικό τρόπο. Θα επικεντρώσουμε το ενδιαφέρον μας σε τέσσερα προβλήματα αυτού του είδους.

Προβλήματα

a. **Το πρόβλημα της περιγραφής ενός ιδεώδους.** Είναι κάθε ιδεώδες I του $K[\underline{X}] = K[X_1, X_2, \ldots, X_n]$ πεπερασμένα παραγόμενο; Με άλλα λόγια υπάρχουν πολυώνυμα
$f_1, f_2, \ldots, f_s$ του $K[\underline{X}]$ τέτοια ώστε $I = \langle f_1, f_2, \ldots, f_s \rangle$;
b. **Το πρόβλημα των στοιχείων ενός ιδεώδους.** Έστω ένα πολυώνυμο f του $K[\underline{X}] = K[X_1, X_2, \ldots, X_n]$ και ένα ιδεώδες $I = \langle f_1, f_2, \ldots, f_s \rangle$. Να εξεταστεί αν $f \in I$. Γεωμετρικά, αυτό το πρόβλημα είναι ανάλογο το να προσδιορίσουμε αν η πολλαπλότητα $V(f_1, f_2, \ldots, f_s)$ βρίσκεται στην πολλαπλότητα $V(f)$.
c. **Το πρόβλημα της λύσης πολυωνυμικών εξισώσεων.** Να βρεθούν οι λύσεις του συστήματος των πολυωνυμικών εξισώσεων

$$f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0.$$

d. **Το πρόβλημα του προσδιορισμού μιας πολλαπλότητας.** Έστω V ένα υποσύνολο του K^n το οποίο δίνεται παραμετρικά από

$$\begin{aligned} x_1 &= g_1(t_1, \ldots, t_m) \\ &\vdots \\ x_n &= g_n(t_1, \ldots, t_m) \end{aligned}$$

Αν τα $g_1, \ldots, g_n$ είναι πολυώνυμα (ή ρητές συναρτήσεις) των μεταβλητών $t_1, \ldots, t_m$, τότε V θα είναι μια αφινική πολλαπλότητα ή θα είναι μέρος μιας αφινικής πολλαπλότητας.. Να βρεθεί ένα σύστημα πολυωνυμικών εξισώσεων των $x_1, \ldots, x_n$ που να καθορίζει αυτή την πολλαπλότητα.

Για να ξεκινήσουμε την μελέτη των βάσεων Gröbner, ας δούμε κάποιες ειδικές περιπτώσεις των παραπάνω προβλημάτων και πως αντιμετωπίζονται από αλγοριθμικές τεχνικές.

Παράδειγμα 1 Έστω $I = \langle g \rangle$ ιδεώδες του K[X]. Για να εξετάσουμε αν ένα πολυώνυμο $f \in K[X]$, διαιρούμε το f με το g και έχουμε:

$$f = q\,g + r$$

για κάποια πολυώνυμα $q, r \in K[X]$ όπου $r = 0$ είτε $\deg(r) < \deg(g)$. Το f είναι στοιχείο του I αν και μόνο αν $r = 0$. Αυτός είναι ο αλγοριθμικός τρόπος λύσης του προβλήματος των στοιχείων ενός ιδεώδους για $n = 1$.

Παράδειγμα 1 Έστω το γραμμικό σύστημα

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0 \\ x_1 + x_2 - 1 &= 0 \\ x_1 + x_3 - 3 &= 0 \end{aligned}$$

του οποίο αναζητάμε το σύνολο των λύσεων. Χρησιμοποιούμε την μέθοδο της απαλοιφής του Gauss. Παίρνουμε τον αντίστοιχο πίνακα και τον μετατρέπουμε σε ανοιγμένο κλιμακωτό.

$$\begin{pmatrix} 2 & 3 & -1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Η μορφή του πίνακα μας δείχνει ότι το x_3 είναι ελεύθερη μεταβλητή και θέτουμε $x_3 = t$. Τότε έχουμε

$$\begin{aligned} x_1 &= -t + 3, \\ x_2 &= t - 2, \\ x_3 &= t. \end{aligned}$$

Το σύστημα των εξισώσεων παριστάνει μια αφινική πολλαπλότητα.
Η παραπάνω διαδικασία μας δείχνει και τον γενικό τρόπο στην περίπτωση της επίλυσης γραμμικού συστήματος.

2. Ταξινόμηση μονωνύμων στο $K[X_1, \ldots, X_n]$

Αν εξετάσουμε λεπτομερώς τον αλγόριθμο διαίρεσης στο $K[X]$ και την απαλοιφή του Gauss για συστήματα γραμμικών εξισώσεων, βλέπουμε ότι χρειάζεται να ορίσουμε ένα είδος ταξινόμησης των μονωνυμικών όρων ενός πολυωνύμου. Για παράδειγμα για να εκτελέσουμε τη διαίρεση δυο πολυωνύμων στο $K[X]$ πρέπει να γράψουμε τους μονωνυμικούς όρους τους σε φθίνουσα σειρά με βάση τη δύναμη του X που περιέχει κάθε όρος. Αντίστοιχα για την απαλοιφή του Gauss πρέπει να τοποθετήσουμε τους συντελεστές των αγνώστων σε ένα πίνακα επομένως χρειάζεται να γνωρίζουμε ποιον όρο θα βάλουμε πρώτο, ποιόν δεύτερο, κλπ.

Παρατηρούμε, ότι μπορούμε να αντιστοιχίσουμε κάθε μονώνυμο του $K[\underline{X}] = K[X_1, \ldots, X_n]$ με μοναδικό τρόπο σε μια διατεταγμένη n-άδα του $\mathbf{Z}_{\geq 0}^{n}$ ως εξής:

$$X^{\alpha} = X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n} \leftrightarrow \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$$

Ορισμός 1 Μια **μονωνυμική ταξινόμηση** του $K[X_1, \ldots, X_n]$ είναι μια σχέση $>$ στο $\mathbf{Z}^n_{\geq 0}$, ή ισοδύναμα στο σύνολο των μονωνύμων X^α, $\alpha \in \mathbf{Z}^n_{\geq 0}$ η οποία ικανοποιεί τα εξής:

(i) Η $>$ είναι ολική (ή γραμμική) ταξινόμηση του $\mathbf{Z}^n_{\geq 0}$. Δηλαδή αν $\alpha, \beta \in \mathbf{Z}^n_{\geq 0}$ ισχύει ακριβώς ένα από τα εξής $\alpha > \beta$ ή $\beta > \alpha$ ή $\alpha = \beta$.

(ii) Αν $\alpha, \beta, \gamma \in \mathbf{Z}^n_{\geq 0}$ με $\alpha > \beta$ τότε $\alpha + \gamma > \beta + \gamma$

(iii) Η $>$ είναι καλή ταξινόμηση δηλαδή κάθε μη-κενό υποσύνολο του $\mathbf{Z}^n_{\geq 0}$ έχει ελάχιστο στοιχείο ως προς την $>$.

Αναφέρουμε το παρακάτω

Λήμμα 2 Μια σχέση ταξινόμησης $>$ είναι καλή αν και μόνο αν κάθε γνησίως φθίνουσα ακολουθία του $\mathbf{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \ldots$$

τελικά τερματίζει.

Στη συνέχεια θα δώσουμε κάποιους ορισμούς μονωνυμικών ταξινομήσεων

Ορισμός 3 (Λεξικογραφική ταξινόμηση) Έστω $\alpha = (\alpha_1, \ldots, \alpha_n)$ και $\beta = (\beta_1, \ldots, \beta_n)$ στοιχεία του $\mathbf{Z}^n_{\geq 0}$. Θα λέμε ότι $\alpha >_{lex} \beta$ αν στο διάνυσμα $\alpha - \beta \in \mathbf{Z}^n$, το πρώτο από τα αριστερά μη-μηδενικό στοιχείο είναι θετικό. Θα γράφουμε $X^\alpha >_{lex} X^\beta$ αν $\alpha >_{lex} \beta$.

Παραδείγματα

a. $(1, 2, 0) >_{lex} (0, 3, 4)$ αφού $(1, 2, 0) - (0, 3, 4) = (1, -1, -4)$.
b. $(3, 2, 4) >_{lex} (3, 2, 1)$ αφού $(3, 2, 4) - (3, 2, 1) = (0, 0, 3)$.
c. Οι μεταβλητές $X_1, X_2, \ldots, X_n$ ταξινομούνται φυσιολογικά με την λεξικογραφική ταξινόμηση

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, \ldots, 0, 1)$$

επομένως $X_1 >_{lex} X_2 >_{lex} \ldots >_{lex} X_n$.

Ορισμός 4 (Βαθμωτή Λεξικογραφική ταξινόμηση) Έστω $\alpha = (\alpha_1, \ldots, \alpha_n)$ και $\beta = (\beta_1, \ldots, \beta_n)$ στοιχεία του $\mathbf{Z}^n_{\geq 0}$. Θα λέμε ότι $\alpha >_{grlex} \beta$ αν $|\alpha| > |\beta|$ είτε $|\alpha| = |\beta|$ και $\alpha >_{lex} \beta$. Όπου $|\alpha| = \sum_{i=1}^{n} \alpha_i$ και $|\beta| = \sum_{i=1}^{n} \beta_i$

Παραδείγματα

a. $(1, 2, 3) >_{lex} (3, 2, 0)$ αφού $|(1, 2, 3)| = 6 > |(3, 2, 0)| = 5$.
b. $(1, 2, 4) >_{lex} (1, 1, 5)$ αφού $|(1, 2, 4)| = 7 = |(1, 1, 5)|$ και $(1, 2, 4) >_{lex} (1, 1, 5)$.
c. Οι μεταβλητές $X_1, X_2, \ldots, X_n$ ταξινομούνται με βάση την λεξικογραφική ταξινόμηση.

Ορισμός 6 (Βαθμωτή Αντίστροφη Λεξικογραφική ταξινόμηση) Έστω α και β στοιχεία του $\mathbf{Z}_{\geq 0}^{n}$. Θα λέμε ότι $\alpha >_{grevlex} \beta$ αν $|\alpha| > |\beta|$ είτε $|\alpha| = |\beta|$ και στο διάνυσμα $\alpha - \beta \in \mathbf{Z}^n$, το πρώτο από τα δεξιά μη-μηδενικό στοιχείο είναι αρνητικό.

Παραδείγματα

a. $(4, 7, 1) >_{lex} (4, 2, 3)$ αφού $|(4, 7, 1)| > |(4, 2, 3)| = 9$.
b. $(1, 5, 2) >_{lex} (4, 1, 3)$ αφού $|(1, 5, 2)| = 8 = |(4, 1, 3)|$ και $(1, 5, 2) - (4, 1, 3) = (-3, 4, -1)$.
c. Οι μεταβλητές $X_1, X_2, \ldots, X_n$ ταξινομούνται φυσιολογικά όπως και στην λεξικογραφική ταξινόμηση.

Ας πάρουμε το πολυώνυμο $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in K[X, Y, Z]$. Θα το ταξινομήσουμε με τους τρεις τρόπους ταξινόμησης που αναφέραμε παραπάνω. Θα θεωρήσουμε $X > Y > Z$.

a. Με την λεξικογραφική ταξινόμηση

$$f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$$

b. Με την βαθμωτή λεξικογραφική ταξινόμηση

$$f = 7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2$$

c. Με την βαθμωτή αντίστροφη λεξικογραφική ταξινόμηση

$$f = 4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2$$

Στη συνέχεια θα χρησιμοποιήσουμε την παρακάτω ορολογία

Ορισμοί 7 Έστω $f = \sum_{\alpha} \lambda_{\alpha} x^{\alpha}$ ένα μη-μηδενικό πολυώνυμο του $K[X_1, \ldots, X_n]$ και έστω > μια μονωνυμική ταξινόμηση.

(i) Ο **πολυβαθμός** (multideg) του f είναι

$$\text{multideg}(f) = \max\{\alpha \in \mathbf{Z}_{\geq 0}^{n} : \lambda_{\alpha} \neq 0\}$$

(ii) Η **οδηγός συντεταγμένη** (leading coefficient) του f είναι

$$LC(f) = \lambda_{\text{multideg}(f)} \in K$$

(iii) Το **οδηγό μονώνυμο** (leading monomial) του f είναι

$$LM(f) = X^{\text{multideg}(f)}$$

(iv) Ο **οδηγός όρος** (leading term) του f είναι

$$LT(f) = LC(f)LM(f)$$

Για παράδειγμα, αν $f = 4XY^2Z + 4Z^2 – 5X^3 + 7X^2Z^2 \in K[X, Y, Z]$ όπως και πριν και με > συμβολίσουμε την λεξικογραφική ταξινόμηση τότε

$$multideg(f) = (3, 0, 0)$$
$$LC(f) = –5$$
$$LM(f) = X^3$$
$$LT(f) = –5\, X^3$$

Ο πολυβαθμός του f έχει τις ακόλουθες χρήσιμες ιδιότητες

Λήμμα 8 Έστω $f, g \in K[X_1, …, X_n]$ δυο μη-μηδενικά πολυώνυμα. Τότε:

(i) $multideg(fg) = multideg(f) + multideg(g)$.
(ii) Αν $f + g \neq 0$ τότε $multideg(f + g) \leq \max\{multideg(f), multideg(f)\}$. Αν, επιπλέον, ισχύει $multideg(f) \neq multideg(g)$ τότε στην παραπάνω σχέση ισχύει η ταυτότητα.

3. Ένας αλγόριθμος διαίρεσης στο $K[X_1, …, X_n]$

Στην παράγραφο 1 είδαμε πως ο αλγόριθμος διαίρεσης μπορεί να χρησιμοποιηθεί για να λυθεί το πρόβλημα των στοιχείων ενός ιδεώδους για πολυώνυμα μιας μεταβλητής. Για να μελετήσουμε το πρόβλημα για περισσότερες μεταβλητές θα διαμορφώσουμε έναν αλγόριθμο διαίρεσης για πολυώνυμα στο $K[X_1, …, X_n]$ ο οποίος γενικεύει τον αλγόριθμο διαίρεσης στο $K[X]$. Στη γενική περίπτωση, ο στόχος είναι να διαιρέσουμε το πολυώνυμο $f \in K[X_1, …, X_n]$ με κάποια πολυώνυμα $f_1, …, f_s \in K[X_1, …, X_n]$. Θέλουμε δηλαδή να γράψουμε το f στη μορφή

$$f = \alpha_1 f_2 + … + \alpha_s f_s + r,$$

όπου τα «πηλίκα» $\alpha_1, …, \alpha_s$ και το υπόλοιπο r είναι στοιχεία του $K[X_1, …, X_n]$.

Θα δούμε πως δουλεύει ο αλγόριθμος μέσα από κάποια παραδείγματα.

Παράδειγμα 1 Αρχικά θα διαιρέσουμε το $f = XY^2 + 1$ με τα πολυώνυμα $f_1 = XY + 1$ και $f_2 = Y + 1$, χρησιμοποιώντας την λεξικογραφική ταξινόμηση με $X > Y$. Για να γνωρίζουμε το πηλίκο για κάθε διαιρέτη κατασκευάζουμε μια κάθετη στήλη με τα πηλίκα α_i ως εξής:

α_1: Y
α_2: –1

$XY^2 + 1$	$XY + 1$
	$Y + 1$
$– XY^2 – Y$	
$– Y + 1$	
$– Y – 1$	
2	

Αρχικά κάνουμε τη διαίρεση του $XY^2 + 1$ με το $XY + 1$. Μετά ελέγχουμε αν ο $LT(XY + 1)$ διαιρεί τον οδηγό όρο του υπολοίπου. Παρατηρούμε ότι δεν τον διαιρεί άρα συνεχίζουμε ελέγχοντας το ίδιο με τον $LT(Y + 1)$. Τα $LT(XY + 1)$ και $LT(Y + 1)$ δεν διαιρούν το 2 άρα το υπόλοιπο είναι 2 και έχουμε τελειώσει έχοντας γράψει το $f = XY^2 + 1$ στη μορφή

$$XY^2 + 1 = Y(XY + 1) + (-1)(Y + 1) + 2.$$

Παράδειγμα 2 Σε αυτό το παράδειγμα ας θεωρούμε τα πολυώνυμα $f = X^2Y + XY^2 + Y^2$, $f_1 = XY - 1$ και $f_2 = Y^2 - 1$. Διαιρούμε το f με τα f_1 και f_2 όπως δείξαμε στο παράδειγμα 1 και παρατηρούμε ότι κατά τη διαίρεση προκύπτει το υπόλοιπο $X + Y^2 + Y$ του οποίου ο οδηγός όρος είναι $LT(X + Y^2 + Y) = X$ και ο οποίος δεν διαιρείται από τους $LT(f_1) = XY$ και $LT(f_2) = X$. Ωστόσο το $X + Y^2 + Y$ δεν είναι το υπόλοιπο της διαίρεσης αφού ο $LT(f_2)$ διαιρεί το Y^2. Για να αντιμετωπίσουμε το πρόβλημα δημιουργούμε μια ακόμα στήλη r όπου θα βάζουμε τους όρους που προκύπτουν κατά τη διαίρεση, δεν διαιρούνται από τα $LT(f_1)$ και $LT(f_2)$ και ανήκουν στο υπόλοιπο. Όπου γίνεται μεταφορά όρου στο υπόλοιπο στην αποκάτω γραμμή ξαναγράφουμε τους όρους που απομένουν. Για να γίνει πιο κατανοητή η μέθοδος να πως γίνεται η διαίρεση με αυτόν τον τρόπο:

α_1: $X + Y$
α_2: -1

$X^2Y + XY^2 + Y^2$	$XY - 1$ $Y^2 + 1$	
$-X^2Y - X$		r
$XY^2 + X + Y^2$ $-XY^2 + Y$		
$X + Y^2 + Y$	$\rightarrow$	X
$Y^2 + Y$ $-Y^2 + 1$		
$Y + 1$	$\rightarrow$	$X + Y$
1	$\rightarrow$	$X + Y + 1$
0		

Επομένως, το υπόλοιπο είναι $X + Y + 1$ και έχουμε γράψει το f στη μορφή:

$$X^2Y + XY^2 + Y^2 = (X + Y)(XY - 1) + 1(Y^2 + 1) + X + Y + 1.$$

Παρατηρήστε ότι το υπόλοιπο είναι άθροισμα μονωνύμων τα οποία δεν διαιρούνται από τα $LT(f_1)$ και $LT(f_2)$.

Το παραπάνω παράδειγμα μας βοηθάει να διατυπώσουμε το ακόλουθο γενικό θεώρημα για τον αλγόριθμο διαίρεσης.

Θεώρημα 3 (Αλγόριθμος Διαίρεσης στο $K[X_1, \ldots, X_n]$). Σταθεροποιούμε μια μονωμυνική ταξινόμηση $>$ στο $\mathbf{Z}^n_{\geq 0}$. Έστω $F = (f_1, \ldots, f_s)$ διατεταγμένη s-άδα πολυωνύμων του $K[X_1, \ldots, X_n]$. Κάθε πολυώνυμο $f \in K[X_1, \ldots, X_n]$ μπορεί να γραφτεί στη μορφή:

$$f = \alpha_1 f_2 + \ldots + \alpha_s f_s + r,$$

όπου τα «πηλίκα» $\alpha_1, \ldots, \alpha_s$ και το **υπόλοιπο** r είναι στοιχεία του $K[X_1, \ldots, X_n]$ και r = 0 ή r είναι K-γραμμικός συνδυασμός μονωνύμων, όπου κανένα από αυτά δεν διαιρείται από $LT(f_1), \ldots, LT(f_s)$. Επίσης, αν $\alpha_i f_i \neq 0$ τότε ισχύει

$$\text{multideg}(f) \geq \text{multideg}(\alpha_i f_i).$$

Η απόδειξη παραλείπεται.

4. Μονωνυμικά ιδεώδη και το λήμμα του Dickson

Σε αυτή την ενότητα θα μελετήσουμε το πρόβλημα της περιγραφής ενός ιδεώδους για μονωνυμικά ιδεώδη. Θα ξεκινήσουμε ορίζοντάς τα στο $K[X_1, \ldots, X_n]$.

Ορισμός 1 Ένα ιδεώδες I του $K[X_1, \ldots, X_n]$ θα λέγεται **μονωνυμικό** αν υπάρχει υποσύνολο A του $\mathbf{Z}_{\geq 0}^n$ (μπορεί και άπειρο) τέτοιο ώστε το I να αποτελείται από όλα τα πολυώνυμα τα οποία είναι πεπερασμένα αθροίσματα της μορφής $\sum_{\alpha \in A} h_\alpha X^\alpha$,όπου $h_\alpha \in K[X_1, \ldots, X_n]$. Τότε γράφουμε $I = \langle X^\alpha : \alpha \in A \rangle$.

Για παράδειγμα το $I = \langle X^4Y^2, X^3Y^4, X^2Y^5 \rangle$ είναι μονωνυμικό ιδεώδες του K[X, Y].

Στη συνέχεια θα χαρακτηρίσουμε όλα τα μονώνυμα τα οποία βρίσκονται σε ένα μονωνυμικό ιδεώδες.

Λήμμα 2 Έστω $I = \langle X^\alpha : \alpha \in A \rangle$ ένα μονωνυμικό ιδεώδες. Το μονώνυμο X^β ανήκει στο I αν και μόνο αν το X^β διαιρείται από το X^α για κάποιο $\alpha \in A$.

Από αυτό το λήμμα προκύπτει και το επόμενο.

Λήμμα 3 Έστω I ένα μονωνυμικό ιδεώδες και έστω $f \in K[X_1, \ldots, X_n]$. Τότε οι ακόλουθες προτάσεις είναι ισοδύναμες:

(i) $f \in I$.
(ii) Κάθε όρος του f ανήκει στο I.
(iii) Το f είναι K-γραμμικός συνδυασμός μονωνύμων του I.

Σαν άμεση συνέπεια του (iii) του λήμματος 2 είναι το γεγονός ότι κάθε μονωνυμικό ιδεώδες ορίζεται μονοσήμαντα από τα μονώνυμα που περιέχει. Επομένως, προκύπτει η ακόλουθη πρόταση.

Πρόταση 4 Δύο μονωνυμικά ιδεώδη ταυτίζονται αν και μόνο αν περιέχουν τα ίδια μονώνυμα.

Το βασικό αποτέλεσμα αυτής της ενότητας είναι ότι όλα τα μονωνυμικά ιδεώδη του $K[X_1, \ldots, X_n]$ είναι πεπερασμένα παραγόμενα.

Θεώρημα 5 (Λήμμα του Dickson) Ένα μονωνυμικό ιδεώδες $I = \langle X^{\alpha} : \alpha \in A \rangle$ του $K[X_1, \ldots, X_n]$ μπορεί να γραφεί στη μορφή

$$I = \langle X^{\alpha(1)}, \ldots, X^{\alpha(s)} \rangle,$$

όπου $\alpha(1), \ldots, \alpha(s) \in A$. Πιο συγκεκριμένα το I έχει πεπερασμένη βάση.

Η απόδειξη του θεωρήματος γίνεται με επαγωγή ως προς τον αριθμό των μεταβλητών. Μπορούμε να χρησιμοποιήσουμε το λήμμα του Dickson για να αποδείξουμε την παρακάτω

Πρόταση 6 Έστω > μια σχέση στο $\mathbf{Z}_{\geq 0}^{n}$ η οποία ικανοποιεί τις παρακάτω προτάσεις:

(i) Η > είναι ολική (ή γραμμική) ταξινόμηση του $\mathbf{Z}_{\geq 0}^{n}$. Δηλαδή αν $\alpha, \beta \in \mathbf{Z}_{\geq 0}^{n}$ ισχύει ακριβώς ένα από τα εξής $\alpha > \beta$ ή $\beta > \alpha$ ή $\alpha = \beta$.

(ii) Αν $\alpha, \beta, \gamma \in \mathbf{Z}_{\geq 0}^{n}$ με $\alpha > \beta$ τότε $\alpha + \gamma > \beta + \gamma$

Τότε η > είναι καλή ταξινόμηση αν και μόνο αν $\alpha \geq 0$ για κάθε $\alpha \in \mathbf{Z}_{\geq 0}^{n}$.

Άμεσο αποτέλεσμα της πρότασης 6 είναι η απλοποίηση του ορισμού της μονωνυμικής ταξινόμησης με την αντικατάσταση της συνθήκης (iii) με την ισοδύναμή της. Με αυτό τον τρόπο μπορούμε να εξετάζουμε πολύ πιο εύκολα αν μια ταξινόμηση είναι μονωνυμική ταξινόμηση.

5. Το θεώρημα βάσης Hilbert και βάσεις Gröbner

Σε αυτή την ενότητα θα δώσουμε μια πλήρη λύση στο πρόβλημα της περιγραφής ενός ιδεώδους.. Θα οδηγηθούμε σε βάσεις ιδεωδών με «καλές» ιδιότητες ως προς τον αλγόριθμο διαίρεσης όπως τον παρουσιάσαμε στην ενότητα 3. Η κεντρική ιδέα η οποία θα χρησιμοποιήσουμε είναι ότι από τη στιγμή που έχουμε ορίζει μια μονωνυμική ταξινόμηση κάθε πολυώνυμο του $K[X_1, \ldots, X_n]$ έχει μοναδικό οδηγό όρο. Επομένως, για κάθε ιδεώδες I, μπορούμε να ορίσουμε το ιδεώδες των οδηγών όρων του ως εξής:

Ορισμός 1 Έστω I ένα μη-μηδενικό ιδεώδες του $K[X_1, \ldots, X_n]$.

(i) Θα συμβολίζουμε με LT(I) το σύνολο των οδηγών όρων του I. Με άλλα λόγια

$$LT(I) = \{cX^{\alpha} : \text{υπάρχει } f \in I \text{ με } LT(f) = cX^{\alpha}\}$$

(ii) Θα συμβολίζουμε με $\langle LT(I) \rangle$ το ιδεώδες που παράγεται από τα στοιχεία του LT(I).

Ας πάρουμε $I = \langle f_1, f_2, \ldots, f_s \rangle$. Τότε θα θέλαμε τα ιδεώδη $\langle LT(f_1), LT(f_2), \ldots, LT(f_s) \rangle$ και $\langle LT(I) \rangle$ να ταυτίζονται. Από τον ορισμό επειδή $f_1, f_2, \ldots, f_s \in I$ έχουμε ότι $LT(f_1), LT(f_2), \ldots, LT(f_s) \in LT(I)$ και επομένως $\langle LT(f_1), LT(f_2), \ldots, LT(f_s) \rangle \subseteq \langle LT(I) \rangle$. Ωστόσο η ισότητα δεν ισχύει πάντοτε. Αυτό φαίνεται από το ακόλουθο παράδειγμα.

Παράδειγμα 2 Έστω $I = \langle f_1, f_2 \rangle$ όπου $f_1 = X^3 - 2XY$ και $f_2 = X^2Y - 2Y^2 + X$. Θα χρησιμοποιήσουμε την βαθμωτή λεξικογραφική ταξινόμηση στο $K[X, Y]$. Ισχύει

$$X(X^2Y - 2Y^2 + X) - Y(X^3 - 2XY) = X^2$$

επομένως $X^2 \in I$. Επομένως $X^2 = LT(X^2) \in LT(I)$. Ωστόσο το X^2 δεν διαιρείται ούτε από το $LT(f_1) = X^3$ ούτε από το $LT(f_2) = X^2Y$ επομένως δεν ανήκει στο μονωνυμικό ιδεώδες $\langle LT(f_1), LT(f_2) \rangle$. (Δες λήμμα 2, ενότητα 4)

Πρόταση 3 Έστω I ιδεώδες του $K[X_1, \ldots, X_n]$.

(i) Το $\langle LT(I) \rangle$ είναι μονωνυμικό ιδεώδες.
(ii) Υπάρχουν $g_1, \ldots, g_t \in I$ τέτοια ώστε $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$.

Απόδειξη (i) Το οδηγά μονώνυμα $LM(g)$ των πολυωνύμων $g \in I - \{0\}$ παράγουν το μονωνυμικό ιδεώδες $\langle LM(g) : g \in I - \{0\} \rangle$. Επειδή τα $LM(g)$ και $LT(g)$ διαφέρουν μόνο κατά μη-μηδενική σταθερά έχουμε ότι

$$\langle LM(g) : g \in I - \{0\} \rangle = \langle LT(g) : g \in I - \{0\} \rangle.$$

Αποδεικνύεται ότι $\langle LT(g) : g \in I - \{0\} \rangle = \langle LT(I) \rangle$. Δηλαδή, $\langle LT(I) \rangle = \langle LM(g) : g \in I - \{0\} \rangle$ και επομένως το $\langle LT(I) \rangle$ είναι μονωνυμικό ιδεώδες.

(ii) Επειδή $\langle LT(I) \rangle$ παράγεται από τα μονώνυμα $LM(g)$ για $g \in I - \{0\}$ το λήμμα του Dickson μας λεει ότι $\langle LT(I) \rangle = \langle LM(g_1), \ldots, LM(g_t) \rangle$ για πεπερασμένα σε πλήθος πολυώνυμα $g_1, \ldots, g_t \in I$. Επειδή τα $LM(g_i)$ διαφέρουν από τα $LT(g_i)$ κατά μια μη-μηδενική σταθερά έπεται ότι $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ το οποίο ολοκληρώνει την απόδειξη.

Μπορούμε τώρα να χρησιμοποιήσουμε την πρόταση 3 και τον αλγόριθμο διαίρεσης για να αποδείξουμε ότι κάθε πολυωνικό ιδεώδες είναι πεπερασμένα παραγόμενο, δίνοντας έτσι θετική απάντηση στο πρόβλημα της περιγραφής ενός ιδεώδους. Έστω I ιδεώδες του $K[X_1, \ldots, X_n]$ και ας θεωρήσουμε το αντίστοιχο ιδεώδες $\langle LT(I) \rangle$. Επιλέγουμε μια μονωνυμική ταξινόμηση την οποία θα χρησιμοποιήσουμε στον αλγόριθμο διαίρεσης και στον υπολογισμό των οδηγών όρων.

Θεώρημα 4 (Θεώρημα βάσης Hilbert) Κάθε ιδεώδες I του $K[X_1, \ldots, X_n]$ είναι πεπερασμένα παραγόμενο. Δηλαδή, υπάρχουν πολυώνυμα $g_1, \ldots, g_t \in I$ τέτοια ώστε $I = \langle g_1, \ldots, g_t \rangle$.

Απόδειξη Αν $I = \{0\}$ το θεώρημα ισχύει. Αν $I \neq \{0\}$ τότε περιέχει κάποιο μη-μηδενικό πολυώνυμο. Τότε ένα σύνολο από πολυώνυμα του I που να το παράγουν μπορεί να δημιουργηθεί ως εξής: Από την πρόταση 3 (ii) υπάρχουν $g_1, \ldots, g_t \in I$ τέτοια ώστε $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Ισχυριζόμαστε ότι $I = \langle g_1, \ldots, g_t \rangle$.

Αρχικά παρατηρούμε ότι $\langle g_1, \ldots, g_t \rangle \subseteq I$, αφού $g_1, \ldots, g_t \in I$. Αρκεί να δείξουμε ότι $I \subseteq \langle g_1, \ldots, g_t \rangle$. Έστω ένα πολυώνυμο $f \in I$. Εφαρμόζουμε τον αλγόριθμο διαίρεσης διαιρώντας το f με τα $g_1, \ldots, g_t$ και παίρνουμε μια έκφραση της μορφής

$$f = \alpha_1 g_1 + \ldots + \alpha_t g_t + r$$

όπου κάθε όρος του r δεν διαιρείται με κανένα από τα $LT(g_1)$, …, $LT(g_t)$. Αν δείξουμε ότι r = 0 θα έχουμε τελειώσει. Παρατηρούμε ότι

$$r = f - \alpha_1 g_1 + \ldots + \alpha_t g_t \in I.$$

Αν $r \neq 0$ τότε $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ και από το λήμμα 2 της ενότητας 4 αυτό έπεται ότι το LT(r) διαιρείται από κάποιο $LT(g_i)$ το οποίο είναι άτοπο από τον τρόπο που έχουμε ορίσει το υπόλοιπο. Επομένως, r = 0. Οπότε

$$f = \alpha_1 g_1 + \ldots + \alpha_t g_t \in \langle g_1, \ldots, g_t \rangle$$

και η απόδειξη ολοκληρώθηκε.

Η βάση $\langle g_1, \ldots, g_t \rangle$ την οποία διαλέξαμε στο θεώρημα για να λύσουμε το πρόβλημα της περιγραφής ενός ιδεώδους I είχε την παραπάνω ιδιότητα $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Έχουμε δει ότι αυτό δεν ισχύει για όλες τις βάσεις ενός ιδεώδους. Θα δώσουμε στις βάσεις που ικανοποιούν αυτή την συνθήκη το παρακάτω όνομα.

Ορισμός 5 Σταθεροποιούμε μια μονωνυμική ταξινόμηση. Ένα πεπερασμένο υποσύνολο $G = \{g_1, \ldots, g_t\}$ ενός ιδεώδους I θα λέγεται **βάση Gröbner** (ή **κανονική βάση**) αν ισχύει

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle.$$

Από την απόδειξη του θεωρήματος 4 προκύπτει το ακόλουθο αποτέλεσμα

Πρόταση 6 Σταθεροποιούμε μια μονωνυμική ταξινόμηση. Κάθε μη-μηδενικό ιδεώδες I του $K[X_1, \ldots, X_n]$ έχει βάση Gröbner. Επιπλέον, κάθε βάση Gröbner ενός ιδεώδους I είναι βάση του I.

Απόδειξη Έστω I ένα μη-μηδενικό ιδεώδες του $K[X_1, \ldots, X_n]$. Στην απόδειξη του θεωρήματος βάσης Hilbert δείξαμε ότι πάντα μπορούμε να κατασκευάσουμε ένα σύνολο $G = \{g_1, \ldots, g_t\}$ το οποίο είναι βάση Gröbner. Για το δεύτερο μέρος της πρότασης παρατηρήστε ότι στην απόδειξη του θεωρήματος βάσης Hilbert δείξαμε ότι αν $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$ τότε $I = \langle g_1, \ldots, g_t \rangle$ και επομένως το G είναι βάση του I.

Ας θεωρήσουμε το ιδεώδες $I = \langle f_1, f_2 \rangle$ του δακτυλίου K[X, Y] όπου $f_1 = X^3 - 2XY$ και $f_2 = X^2Y - 2Y^2 + X$. Το σύνολο $\{f_1, f_2\}$ είναι βάση του I αλλά δεν είναι βάση Gröbner με βάση την βαθμωτή λεξικογραφική ταξινόμηση αφού, όπως δείξαμε και στο παράδειγμα 2, το X^2 δεν ανήκει στο ιδεώδες $\langle LT(f_1), LT(f_2) \rangle$.

Στη συνέχεια ας θεωρήσουμε το ιδεώδες $J = \langle g_1, g_2 \rangle = \langle X + Z, Y - Z \rangle$. Ισχυριζόμαστε ότι τα g_1, g_2 σχηματίζουν μια βάση Gröbner του J αν θεωρήσουμε την λεξικογραφική ταξινόμηση στο **R**[X, Y, Z]. Με άλλα λόγια θα δείξουμε ότι για κάθε μη-μηδενικό στοιχείο f του J το LT(f) βρίσκεται στο ιδεώδες $\langle LT(g_1, LT(g_2) \rangle = \langle X,$

Y>. Από το λήμμα 2 ενότητα 4 μπορούμε ισοδύναμα να δείξουμε ότι το LT(f) διαιρείται είτε με X είτε με Y.

Έστω λοιπόν, ένα μη-μηδενικό πολυώνυμο $f = Ag_1 + Bg_2 \in J$. Υποθέτουμε ότι το LT(f) δεν διαιρείται ούτε από το X ούτε από το Y. Από τον ορισμό της λεξικογραφικής ταξινόμησης αυτό σημαίνει ότι είναι πολυώνυμο του Z. Ωστόσο, επειδή $f \in J$ το f μηδενίζεται στο γραμμικό υπόχωρο $L = V(J) = V(X + Z, Y - Z) \subset \mathbf{R}^3$. Επειδή οι λύσεις στον L παραμετρικοποιούνται ως εξής: $(x, y, z) = (-t , t, t) \in L$, για κάθε πραγματικό αριθμό t το μόνο πολυώνυμο του Z το οποίο μηδενίζεται στον L είναι το μηδενικό πολυώνυμο και καταλήξαμε σε άτοπο. Επομένως, το $\{g_1, g_2\}$ είναι βάση Gröbner του J.

Οι βάσεις Gröbner εισάχθηκαν για πρώτα φορά στα μέσα της δεκαετίας του ’60 από τον H. Hironaka, ο οποίος της αποκαλούσε «κανονικές βάσεις» (standard bases) και ανεξάρτητα λίγο αργότερα από τον B. Buchberger στη διδακτορική διατριβή του. Το όνομα «βάσεις Gröbner» δόθηκε από τον Buchberger προς τιμήν του επιπλέποντα καθηγητή και δασκάλου του W. Gröbner (1899 – 1980).

Θα κλείσουμε την πρώτη διάλεξη με δύο εφαρμογές του θεωρήματος βάσης Hilbert.

Μια αύξουσα αλυσίδα ιδεωδών του $K[X_1, X_2, \ldots, X_n]$ είναι μια αύξουσα ακολουθία

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

Για παράδειγμα, η ακολουθία

$$\langle X_1 \rangle \subseteq \langle X_1, X_2 \rangle \subseteq \ldots \subseteq \langle X_1, X_2, \ldots, X_n \rangle$$

σχηματίζει μια (πεπερασμένη) αύξουσα αλυσίδα ιδεωδών του $K[X_1, X_2, \ldots, X_n]$. Αν προσταθούσαμε να επεκτείνουμε αυτή την αλυσίδα ιδεωδών προσθέτοντας ένα ιδεώδες με περισσότερους γεννήτορες, θα είχαμε δύο περιπτώσεις. Έστω το ιδεώδες $\langle X_1, X_2, \ldots, X_n, f \rangle$. Στη πρώτη περίπτωση αν $f \in \langle X_1, X_2, \ldots, X_n \rangle$ τότε θα είχαμε ότι $\langle X_1, X_2, \ldots, X_n, f \rangle = \langle X_1, X_2, \ldots, X_n \rangle$ και τίποτα δεν θα άλλαζε. Στην άλλη περίπτωση αν $f \notin \langle X_1, X_2, \ldots, X_n \rangle$ τότε θα είχαμε ότι $\langle X_1, X_2, \ldots, X_n, f \rangle = K[X_1, X_2, \ldots, X_n]$. Επομένως, η αλυσίδα ιδεωδών που κατασκευάσαμε μπορεί να συνεχιστεί μόνο με δύο τρόπους. Είτε με την επανάληψη του τελευταίου ιδεώδους επ’ άπειρο είτε προσθέτοντας το $K[X_1, X_2, \ldots, X_n]$ και με την επανάληψη αυτού επ’ άπειρο. Σε κάθε περίπτωση μετά από πεπερασμένα βήματα η αλυσίδα συνεχίζει με την επανάληψη του τελευταίου ιδεώδους επ’ άπειρο.

Θεώρημα 7 (Συνθήκη Αύξουσας Αλυσίδας) Έστω

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

μια αύξουσα ακολουθία ιδεωδών του $K[X_1, X_2, \ldots, X_n]$. Υπάρχει φυσικός $N \geq 1$ τέτοιος ώστε

$$I_N = I_{N+1} = I_{N+2} = \ldots$$

Απόδειξη Έχοντας τον ακολουθία $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ θεωρούμε το σύνολο $I = \bigcup_{i=1}^{\infty} I_i$. Εύκολα μπορούμε να δείξουμε ότι το I είναι ιδεώδες. Από το θεώρημα βάσης του Hilbert το ιδεώδες I είναι πεπερασμένα παραγόμενο. Έστω ότι $I = <f_1, \ldots, f_s>$ για κάποια $f_1, \ldots, f_s \in K[X_1, X_2, \ldots, X_n]$. Αλλά κάθε ένα τα $f_1, \ldots, f_s$ ανήκει σε κάποια I_j, έστω $f_i \in I_{j_i}$, i = 1, …, s. Έστω N είναι το μέγιστο από τα j_i. Τότε από τον ορισμό της της αύξουσας αλυσίδας ισχύει ότι $f_i \in I_N$ για κάθε i = 1, …, s. Οπότε έχουμε

$$I = < f_1, \ldots, f_s> \subseteq I_N \subseteq I_{N+1} \subseteq \ldots \subseteq I.$$

Από την τελευταία σχέση φαίνεται ότι η αύξουσα αλυσίδα σταθεροποιείται στο I_N. Όλα τα υπακολουθιακά ιδεώδη στην αλυσίδα είναι ίσα.

Η δεύτερη συνέπεια του θεωρήματος βάσης Hilbert είναι γεωμετρικοί.

Ορισμός 8 Έστω I ιδεώδες του $K[X_1, \ldots, X_n]$. Θα συμβολίζουμε με **V**(I) το σύνολο

$$\mathbf{V}(I) = \{(\alpha_1, \ldots, \alpha_n) \in K^n : f(\alpha_1, \ldots, \alpha_n) = 0 \text{ για κάθε } f \in I\}.$$

Μια χρήσιμη παρατήρηση είναι ότι αν και κάθε μη-μηδενικό ιδεώδες I περιέχει άπειρα στο πλήθος πολυώνυμα, το σύνολο **V**(I) μπορεί να ορισθεί από ένα πεπερασμένο σύνολο πολυωνυμικών εξισώσεων.

Πρόταση 9 Το **V**(I) είναι μια αφινική πολλαπλότητα. Πιο συγκεκριμένα, αν $I = <f_1, \ldots, f_s>$ τότε $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.

Απόδειξη Έστω I ιδεώδες του $K[X_1, X_2, \ldots, X_n]$. Από το θεώρημα βάσης Hilbert $I = <f_1, \ldots, f_s>$ για κάποια $f_1, \ldots, f_s \in I$. Ισχυριζόμαστε ότι $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$. Κατ' αρχήν επειδή $f_1, \ldots, f_s \in I$ αν $f(\alpha_1, \ldots, \alpha_n) = 0$ για κάθε $f \in I$ τότε ισχύει και για τα f_i δηλαδή $f_i(\alpha_1, \ldots, \alpha_n) = 0$ για κάθε i = 1, …, s. Επομένως, $\mathbf{V}(I) \subseteq \mathbf{V}(f_1, \ldots, f_s)$. Από την άλλη έστω $(\alpha_1, \ldots, \alpha_n) \in \mathbf{V}(f_1, \ldots, f_s)$ και έστω $f \in I$. Επειδή $I = <f_1, \ldots, f_s>$ υπάρχουν πολυώνυμα $h_1, \ldots, h_s$ του $K[X_1, X_2, \ldots, X_n]$ τέτοια ώστε

$$f = h_1 f_1 + \ldots + h_s f_s$$

αλλά τότε $f(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{s} h_i(\alpha_1,\ldots,\alpha_n) f_i(\alpha_1,\ldots,\alpha_n) = \sum_{i=1}^{s} h_i(\alpha_1,\ldots,\alpha_n) \cdot 0 = 0.$
Δηλαδή, $\mathbf{V}(f_1, \ldots, f_s) \subseteq \mathbf{V}(I)$ και επομένως ισχύει η ισότητα.

Η σημαντικότερη συνέπεια αυτής της πρότασης είναι ότι οι πολλαπλότητες ορίζονται από ιδεώδη.