ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
"ΘΕΩΡΗΤΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΘΕΩΡΙΑ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΕΛΕΓΧΟΥ"

Βάση Groebner και Εφαρμογές

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ραπτίδου Θ. Χριστίνα

Επιβλέπων: Καραμπετάκης Νικόλαος
Καθηγητής
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Θεσσαλονίκη, 2014

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
"ΘΕΩΡΗΤΙΚΗ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΘΕΩΡΙΑ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΕΛΕΓΧΟΥ"

Βάση Groebner και Εφαρμογές

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ραπτίδου Θ. Χριστίνα

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

.....	.....	.....
Καραμπετάκης Νικόλαος Καθηγητής	Ραχώνης Γεώργιος Αν.Καθηγητής	Πάπιστας Αθανάσιος Καθηγητής

Π Ε Ρ Ι Λ Η Ψ Η

Στην παρακάτω μελέτη αρχικά εισάγουμε την έννοια των αφινικών πολλαπλοτήτων, τα οποία είναι καμπύλες, επιφάνειες ή αντικείμενα μεγαλύτερης διάστασης και την έννοια των ιδεωδών τα οποία είναι σύνολα με συγκεκριμένες ιδιότητες. Παρακάτω τίθονται τα ερωτήματα του προβλήματος συμμετοχής των ιδεωδών, του προβλήματος περιγραφής των ιδεωδών και αυτό της πεπλεγμένης αναπαράστασης. Για την επίλυση αυτών μελετούμε τον αλγόριθμο της διαίρεσης για πολυώνυμα πολλών μεταβλητών και εισάγουμε την έννοια της βάσης Groebner. Η βάση Groebner έχει πολλά πλεονεκτήματα, καθώς με τη χρήση της απορρίπτονται ανεπιθύμητες ιδιότητες που προκύπτουν όταν χρησιμοποιούμε οποιαδήποτε άλλη βάση. Με τον αλγόριθμο Buchberger οδηγούμαστε στην κατασκευή μιας τέτοιας βάσης και έπειτα μελετούμε πώς απλοποιείται η βάση αυτή. Τέλος, γίνεται αναφορά στις εφαρμογές των ιδεωδών, των πολλαπλοτήτων και της βάσης Groebner στη θεωρία ελέγχου και συστημάτων.

Λέξεις κλειδιά: Αφινική πολλαπλότητα, αφινικός χώρος, ιδεώδες, βάση Groebner , πολυωνυμικές περιγραφές συστημάτων

A B S T R A C T

In the above study, we introduce the concept of affine varieties, which tend to be lines, surfaces and other objectives with higher dimension, as well as the concept of ideals, which are sets with special properties. Furthermore, we give solutions to the ideal memebership problem, to the ideal discription problem and to the implicit represantation problem. Some of those problems are resolved using Groebner basis, the division algorithm and its extention in multivariate polynomials. This basis is preferable, as it tends to exclude problems which arise when using any other bases. Moreover, there is a reference to Buchberger algorithm, used to construct such a basis. Finally, there is a survey on the applications of ideals, varieties and the Groebner basis in contol system theory.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΓΕΩΜΕΤΡΙΑ , ΑΛΓΕΒΡΑ ΚΑΙ ΑΛΓΟΡΙΘΜΟΙ

Στο κεφάλαιο αυτό, γίνεται αναφορά στις *αφινικές πολλαπλότητες* και στα *ιδεώδη*. Οι πολλαπλότητες ορίζονται από πολυωνυμικές εξισώσεις και η διάστασή τους διαφέρει. Συγκεκριμένα, μπορεί να είναι μονοδιάστατες, δηλαδή καμπύλες, δισδιάστατες, δηλαδή επίπεδα, ή μπορεί να έχουν μεγαλύτερη διάσταση. Τα ιδεώδη είναι σύνολα στον πολυωνυμικό δακτύλιο $K[x_1,...,x_n]$ που βοηθούν στην κατανόηση των πολλαπλοτήτων. Στο τέλος του κεφαλαίου δίνεται ο αλγόριθμος της διαίρεσης για πολυώνυμα μιας μεταβλητής και επέξηγείται η χρήση του στη μελέτη των ιδεωδών και συνεπώς, γίνεται μια πρώτη σύνδεση των πολλαπλοτήτων από τη γεωμετρία, με σύνολα από την άλγεβρα και με αλγόριθμους.

§1.1 ΠΟΛΥΩΝΥΜΑ ΚΑΙ ΑΦΙΝΙΚΟΙ ΧΩΡΟΙ

Τα σύνολα F όπου είναι εφοδιασμένα με δύο πράξεις (συνήθως πρόσθεση και πολλαπλασιασμό) ονομάζονται *σώματα* και ισχύουν οι εξής ιδιότητες:

1. $(a+b)+c=a+(b+c)$
2. $\exists 0\in \mathrm{F}:\ a+0=a,\ \forall a\in \mathrm{F}\ \kappa\alpha\iota\ \forall \alpha\in \mathrm{F},\ \exists b\in \mathrm{F}: a+b=0$
3. $a+b=b+a$
4. $(a*b)*c=a*(b*c)$
5. $\exists\ 1\in \mathrm{F}:\ a*1=a,\ \forall a\in \mathrm{F}\ \kappa\alpha\iota\ \forall \alpha\in \mathrm{F},\ \exists b\in \mathrm{F}: a*b=1$
6. $a*b=b*a$
7. $a*(b+c)=a*b+a*c$

Εύκολα συμπεραίνει κανείς ότι οι πραγματικοί αριθμοί αποτελούν σώμα, ενώ οι ακέραιοι όχι, αφού η διαίρεση δεν είναι καλά ορισμένη. Τα σώματα με τα οποία θα ασχοληθούμε περισσότερο είναι τα Q, R και C.

Ορισμός 1.1.1 [1]

Μονώνυμο είναι ένα γινόμενο της μορφης:

$$x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$$

Όπου όλοι οι εκθέτες $\alpha_1, \alpha_2, ..., \alpha_n$ είναι μη-αρνητικοί ακέραιοι. **Συνολικός βαθμός (total degree)** του μονωνύμου είναι το άθροισμα $\alpha_1 + \alpha_2 + ... + \alpha_n$.

Τα μονώνυμα μπορούμε επίσης να τα συμβολίσουμε με

$$x^a = x_1^{a_1} x_2^{a_2} \ldots . x_n^{\alpha_n},$$

όπου $\alpha = (\alpha_1, ..., \alpha_n)$ μια n-άδα μη-αρνητικών ακεραίων.

Ορισμός 1.1.2 [1]

Πολυώνυμο f με συντελεστές από το σώμα K είναι ένας γραμμικός συνδυασμός μονωνύμων. Το πολυώνυμο f συμβολίζεται με:

$$f = \sum_a a_a x^a, \ a_a \in K,$$

όπου το άθροισμα περιέχει πεπερασμένες n-άδες $\alpha = (\alpha_1, ..., \alpha_n)$. Το σύνολο όλων των πολυωνύμων με μεταβλητές $x_1, x_2, ..., x_n$ και συντελεστές από το σώμα K θα συμβολίζεται με $K[x_1, ..., x_n]$.

Για ευκολία, σε περιπτώσεις πολυωνύμων με λίγες μεταβλητές, δε θα χρησιμοποιούμε δείκτες αλλα τις μεταβλητές x, y, z.

Ορισμός 1.1.3 [1]

Έστω $f = \sum_a a_a x^a$ ένα πολυώνυμο στο $k[x_1,...,x_n]$.

i. Θα αποκαλούμε το α_α, **συντελεστή (coefficient)** του μονωνύμου x^a.

ii. Αν $\alpha_\alpha \neq 0$, τότε το $\alpha_\alpha x^a$ θα ονομάζεται **όρος (term)** του f.

iii. Ο **συνολικός βαθμός (total degree)** του f -επίσης συμβολίζεται και με $\deg(f)-$, είναι το μέγιστο $a = \alpha_1 + \cdots \alpha_n$, για το οποίο ισχύει ο συντελεστής α_α να είναι μη-μηδενικός.

Εφαρμογή

Το πολυώνυμο $f = -3x^3y^2z^2 + \frac{3}{2}y^3z^4 - 3x + 6xy^2z^2$, έχει τέσσερις όρους και συνολικό βαθμό εφτά. Παρατηρούμε ότι πρώτοι δύο όροι έχουν τον ίδιο συνολικό βαθμό, κάτι που δε μπορεί να συμβεί σε πολυώνυμα μιας μεταβλητής. ▵

Το $K[x_1,...,x_n]$ αποτελεί πολυωνυμικό (αντιμεταθετικό) δακτύλιο, καθώς με την πράξη της πρόσθεσης ισχύει η προσεταιριστικότητα, η αντιμεταθέτικότητα, η ύπαρξη αντιστρόφου και η ύπαρξη ουδέτερου στοιχείου, ενώ με την πράξη του πολλαπλασιασμού ισχύει η προσεταιριστικότητα και η ύπαρξη ουδέτερου στοιχείου. Επίσης ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση.

Ορισμός 1.1.4 [1]

Έστω ένα σώμα K και ένας θετικός ακέραιος n. **Αφινικό χώρο** θα ονομάζουμε το n-διάστατο διανυσματικό χώρο:

$$K^n = \{(a_1,...,a_n) : a_1,...,a_n \in K\}.$$

Για παράδειγμα, έστω ότι $K = \mathrm{R}$. Σε αυτήν την περίπτωση ο αφινικός χώρος είναι το R^n. Γενικά, το $K^1 = K$ ονομάζεται *αφινική ευθεία*, ενώ το K^2 *αφινικό επίπεδο*.

<u>Θεώρημα 1.1.5</u> [2]

Κάθε μη σταθερό πολυώνυμο $f \in \mathrm{C}[x]$ έχει μια ρίζα στο C.

Ένα σώμα για το οποίο ισχύει το παραπάνω θεώρημα, ονομάζεται *αλγεβρικά κλειστό, (algebraically closed)*. Συνεπώς, το R, σε αντίθεση με το R, δεν είναι αλγεβρικά κλειστό.

§1.2 ΑΦΙΝΙΚΕΣ ΠΟΛΛΑΠΛΟΤΗΤΕΣ

Ορισμός 1.2.1 [1]

Έστω K ένα σώμα και έστω $f_1,...,f_s$ πολυώνυμα στο $K[x_1,...,x_n]$. Τότε ορίζουμε ως

$$V(f_1,...,f_s)=\{(a_1,...,a_n)\in K^n : f_i(a_1,...,a_n)=0, \forall 1\le i\le s\}.$$

Το $V(f_1,...,f_s)$ ονομάζεται **αφινική πολλαπλότητα** που ορίζεται από τα $f_1,...,f_s$.

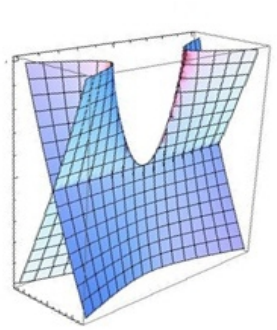
Άρα, η αφινική πολλαπλότητα $V(f_1,...,f_s)\subset K^n$, είναι το σύνολο των λύσεων του συστήματος με εξισώσεις:

$$\begin{aligned} f_1(x_1,...,x_n)&=0\\ &\vdots\\ f_s(x_1,...,x_n)&=0 \end{aligned}.$$

Συνήθως χρησιμοποιούμε τα γράμματα V,W για να συμβολίσουμε μια αφινική πολλαπλότητα. Επίσης σε πολλά παραδείγματα θεωρούμε $K=\mathrm{R}$ για να μπορούμε να απεικονίσουμε τον χώρο που μελετούμε.

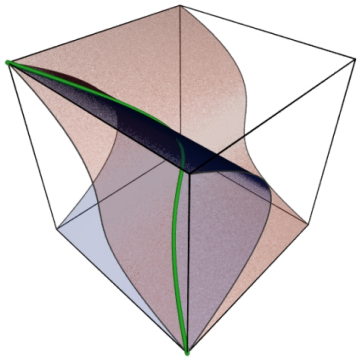
Γενικά, όλες οι γεωμετρικές κωνικές τομές (κύκλοι, ελλείψεις, παραβολές, υπερβολές) είναι αφινικές πολλαπλότητες, όπως επίσης και τα γραφήματα πολυωνυμικών και ρητών συναρτήσεων. Για παράδειγμα, εύκολα διαπιστώνει κανείς ότι η γραφική παράσταση της συνάρτησης $y=\dfrac{x^3-x^2+1}{x}$, αντιπροσωπεύει την αφινική πολλαπλότητα $V(x^3-x^2-xy+1)$.

Στον τρισδιάστατο χώρο $\mathbb{R}^3$, ο κώνος δίνεται από την πολλαπλότητα $V(z^2-x^2-y^2)$. Μια πιο πολύπλοκη επιφάνεια, δίνεται από την αφινική πολλαπλότητα $V(x^2-y^2z^2+z^3)$, όπως φαίνεται στο παρακάτω σχήμα:



Αυτά είναι χαρακτηριστικά παραδείγματα από τα οποία διαπιστώνεται ότι οι επιφάνειες δεν είναι παντού λείες.

Η αφινική πολλαπλότητα $V(y-x^2, z-x^3)$, προκύπτει από την τομή των επιφάνειων $y-x^2,\ z-x^3$ και η γραφική παράστασή της είναι καμπύλη στον $\mathbb{R}^3$, η οποία δίνεται από το παρακάτω σχήμα:



Η παραπάνω καμπύλη ονομάζεται *στριμμένη κυβική καμπύλη*. Μέχρι στιγμής στα παραδείγματα που είδαμε κάθε εξίσωση ρίχνει τη διάσταση του σώματος κατά μια μονάδα. Αυτό όμως δεν είναι κάτι που ισχύει για κάθε περίπτωση. Ειδικότερα, έστω η πολλαπλότητα $\mathrm{V}(xz, yz)$, που ορίζεται από τις εξισωσεις $xz = yz = 0$. Αυτές παριστάνουν την ένωση του $(x, y)-$ επιπέδου και του άξονα z και άρα αποτελείται από δύο αντικείμενα διαφορετικών διαστάσεων.

Έστω το σύστημα:

$$\begin{matrix} \alpha_{11}x_1 + \ldots + a_{1n} = b_1 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn} = b_m \end{matrix} \quad . \tag{1.2.1}$$

Την πολλαπλότητα $V \subset K^n$ που προκύπτει από τη λύση των παραπάνω εξισώσεων την ονομάζουμε *γραμμική πολλαπλότητα* και τη βρίσκουμε με τη μέθοδο αναγωγής σε κλιμακωτή μορφή (row reduction). Άν $V \neq \varnothing$, τότε η V θα έχει διάσταση $n - r$, όπου $r = rank(a_{ij})$. Επομένως, η διάσταση των γραμμικών πολλαπλοτήτων καθορίζεται από τον αριθμό των γραμμικά ανεξάρτητων εξισώσεων.

§1.3 ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΕΙΣ ΤΩΝ ΑΦΙΝΙΚΩΝ ΠΟΛΛΑΠΛΟΤΗΤΩΝ

Η παράγραφος αυτή αναφέρεται στην περιγραφή όλων των σημείων μιας αφινικής πολλαπλότητας $V(f_1,...f_s)$. Αναλύεται πώς παραμετροποιούμε μια πολλαπλότητα και πού βοηθά μια τέτοια παραμετροποίηση, αλλά και το αντίστροφο, δηλαδή πώς βρίσκουμε τις αρχικές εξισώσεις μιας πολλαπλότητας, δοθέντων των παραμετροποιημένων. Με την παραμετροποίηση θα μπορέσουμε να ελέγξουμε εάν υπάρχει τρόπος να βρούμε όλες τις λύσεις του συστήματος $f_1 = ... = f_s = 0$, είτε αυτό έχει πεπερασμένο πλήθος λύσεων, είτε έχει άπειρο.

Ξεκινώντας με ένα παράδειγμα από τη γραμμική άλγεβρα, έστω το σώμα R και έστω το σύστημα

$$(1.3.1) \qquad \begin{aligned} x + 2y - 3z &= 1 \\ x + y + 3z &= 0 \end{aligned}$$

Γεωμετρικά, οι παραπάνω εξισώσεις παριστάνουν μια ευθεία στο R^3 , η οποία είναι τομή των επιπέδων $x + 2y - 3z = 1$ και $x + y + 3z = 0$. Άρα το (1.3.1) έχει άπειρες λύσεις και για να τις περιγράψουμε αυτές τις λύσεις, εκτελούμε πράξεις. Συγκεκριμένα, αφαιρούμε από την πρώτη εξίσωση το διπλάσιο της δεύτερης για να διώξουμε το *y*, ενώ αν αφαιρέσουμε κατά μέλη φεύγει το *x* και παίρνουμε ισοδύναμα:

$$\begin{aligned} x &= \frac{1-3y}{2} \\ y &= 1 + 6z \end{aligned}$$

Θέτωντας $z = t$, όπου t μια αυθαίρετη σταθερά, συμπεραίνουμε ότι όλες οι λύσεις του (1.3.1) δίνονται από το:

$$(1.3.2) \qquad \begin{aligned} x &= -1 - 9t \\ y &= 1 + 6t \\ z &= t \end{aligned} \quad \text{, όπου } t \in \mathrm{R} \text{ .}$$

Το t το αποκαλούμε *παράμετρο* και το (1.3.2) *παραμετροποίηση* των λύσεων του (1.3.1).

Ορισμός 1.3.1 [1]

Έστω ένα σώμα *K*. Μια **ρητή συνάρτηση** με μεταβλητές $t_1,...,t_m$ και συντελεστές από το *K*, είναι το πηλίκο f/g δύο πολυωνύμων $f,g \in K[t_1,...,t_m]$, όπου το g δεν είναι το μηδενικό πολυώνυμο. Επιπλέον, δύο ρητές συναρτήσεις f/g και h/k, είναι ισοδύναμες εάν $kf = gh$ στο $K[t_1,...,t_m]$. Τέλος, το σύνολο όλων των ρητών συναρτήσεων με μεταβλητές $t_1,...,t_m$ και συντελεστές από το *K* συμβολίζεται με $K(t_1,...,t_m)$.

Η *ρητή παραμετρική αναπαράσταση* μιας πολλαπλότητας $V = \mathrm{V}(f_1,...f_s) \subset K^n$, αποτελείται από τις ρητές συναρτήσεις $r_1,...,r_n \in K(t_1,...,t_m)$, έτσι ώστε τα σημεία που περιγράφονται ως

$$\begin{aligned} x_1 &= r_1(t_1,...,t_m) \\ x_2 &= r_2(t_1,...,t_m) \\ &\vdots \\ x_n &= r_n(t_1,...,t_m) \end{aligned}$$

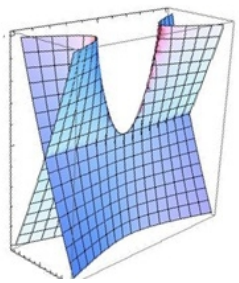
να ανήκουν στη *V*.

Στις περιπτώσεις όπου έχουμε παραμετροποιήσεις των πολλαπλοτήτων και τα $r_1,...,r_n$, είναι πολυώνυμα αντί για ρητές συναρτήσεις θα λέμε ότι έχουμε *πολυωνυμική παραμετροποίηση* της *V*. Αντιθέτως τις αρχικές εξισώσεις $f_1 = ... = f_s = 0$ της V τις αποκαλούμε *πεπλεγμένη αναπαράσταση* της V.

Ένα από τα μεγαλύτερα πλεονεκτήματα της παραμετρικής αναπαράστασης, καμπύλης ή επιφάνειας, είναι ότι μπορούμε εύκολα να τη σχεδιάσουμε. Για παράδειγμα, στην §2, είδαμε την επιφάνεια $V(x^2 - y^2z^2 + z^3)$. Για το σχεδιασμό αυτής δεν κάνουμε χρήση της πεπλεγμένης αναπαράστασης $x^2 - y^2z^2 + z^3 = 0$, αλλά χρησιμοποιούμε την παραμετροποίηση:

$$\begin{aligned} x &= t(u^2 - t^2) \\ y &= u \\ z &= u^2 - t^2 \end{aligned} \qquad (1.3.3)$$

και παίρνουμε το σχήμα:



Οι παράμετροι t,u , $-1 \le t,u \le 1$ είναι δύο διότι περιγράφουμε επιφάνεια. Ωστόσο, είναι εξίσου σημαντικό να γνωρίζουμε την πεπλεγμένη αναπαράσταση μιας πολλαπλότητας. Για παράδειγμα, έστω ότι θέλουμε να ελέγξουμε εάν το σημείο (0,2,-1) ανήκει στην παραπάνω επιφάνεια. Αντικαθιστώντας τις συντεταγμένες αυτού του σημείου στην παραμετρική αναπαράσταση (1.3.3), πρέπει να λύσουμε το σύστημα

$$\begin{aligned} 0 &= t(u^2 - t^2) \\ 2 &= u \\ -1 &= u^2 - t^2 \end{aligned} \qquad (1.3.4) \quad .$$

Αντιθέτως, εάν ξέρουμε την πεπλεγμένη αναπαράσταση, αντικαθιστούμε τις συντεταγμένες του σημείου στην $x^2 - y^2 z^2 + z^3 = 0$ και παίρνουμε ότι

$$0^2 - 2^2(-1)^2 + (-1)^3 = 0 - 4 - 1 = -5 \neq 0 \, .$$

Άρα το (0,2,-1) δεν ανήκει στην επιφάνειά μας (και συνεπώς το σύστημα (1.3.4) δεν έχει λύσεις).

Δεν έχουν όλες οι αφινικές πολλαπλότητες παραμετρική αναπαράσταση. Αυτές που έχουν ονομάζονται *unirational*. Γενικά όμως είναι δύσκολο να αναγνωρίσουμε εάν μια πολλαπλότητα είναι unirational ή όχι. Παρόλα αυτά, πάντα μπορούμε να βρούμε την πεπλεγμένη αναπαράσταση όταν γνωρίζουμε την παραμετρική, όπως φαίνεται και στο παρακάτω παράδειγμα.

Έστω η παραμετρική αναπαράσταση

$$\begin{aligned} x &= 2t \\ y &= 1+t^2 \end{aligned} \qquad (1.3.5)$$

Αυτό το σύστημα παριστάνει μια καμπύλη πάνω σε ένα επίπεδο, αλλά δεν μας επιβεβαιώνει ότι η καμπύλη αυτή ανήκει στην αφινική πολλαπλότητα. Για να βρούμε την πεπλεγμένη αναπαράσταση, λύνουμε την πρώτη εξίσωση ως προς t και παίρνουμε

$$t = \frac{x}{2}.$$

Αντικαθιστώντας στη δεύτερη εξίσωση, έχουμε:

$$y = 1+\left(\frac{x}{2}\right)^2 = \frac{x^2}{4}+1$$

Ως εκ τούτου, οι παραμετρικές εξισώσεις (1.3.5) περιγράφουν την αφινική πολλαπλότητα

$$\mathrm{V}\left(y-\frac{x^2}{4}-1\right).$$

Βασικός μας στόχος ήταν η απαλοιφή του t, έτσι ώστε να προκύψει ένα σύστημα εξισώσεων που να περιέχει μόνο x και y και να οδηγηθούμε στην αφινική πολλαπλότητα.

§1.4 ΙΔΕΩΔΗ

Στην παράγραφο αυτή γίνεται μια εισαγωγή στα σύνολα που αποκαλούνται *ιδεώδη* και στη σύνδεσή τους με τις αφινικές πολλαπλότητες.

Ορισμός 1.4.1 [1]

Ένα υποσύνολο $I \subset K[x_1,...,x_n]$ είναι **ιδεώδες** εάν:

i. $0 \in I$

ii. Αν $f, g \in I \Rightarrow f + g \in I$

iii. Αν $f \in I$ και $h \in K[x_1,...,x_n]$, τότε $hf \in I$.

Ορισμός 1.4.2 [1]

Έστω $f_1,...,f_s$ πολυώνυμα στο $K[x_1,\ldots,x_n]$. Τότε, ορίζουμε ως:

$$\langle f_1,...,f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1,...,h_s \in K[x_1,...,x_n] \right\}$$

Το παραπάνω σύνολο αποτελεί ιδεώδες.

Λήμμα 1.4.3 [1]

Έστω $f_1,...,f_s \in K[x_1,...,x_n]$. Τότε το $\langle f_1,...,f_s \rangle$, αποτελεί ιδεώδες του $K[x_1,\ldots,x_n]$, το οποίο θα ονομάζουμε **παραγόμενο ιδεώδες** από τα $f_1,...,f_s$.

Απόδειξη

Ότι $0 \in \langle f_1,...,f_s \rangle$, αφού $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Έπειτα, θεωρούμε τις $f = \sum_{i=1}^{s} p_i f_i$ και $g = \sum_{i=1}^{s} q_i f_i$, και έστω $h \in K[x_1,...,x_n]$. Οι εξισώσεις

$$f+g=\sum_{i=1}^{s}(p_i+q_i)f_i$$

$$hf=\sum_{i=1}^{s}(hp_i)f_i$$

ικανοποιούν τις προυποθέσεις των ιδεωδών και άρα το $\langle f_1,...,f_s\rangle$ αποτελεί ιδεώδες. $\triangle$

Έστω $f_1,...,f_s\in K[x_1,...,x_n]$ και παίρνουμε το σύστημα εξισώσεων

$$f_1=\cdots=f_s=0\,.$$

Πολλαπλασιάζοντας την πρώτη εξίσωση με $h_1\in K[x_1,...,x_n]$, τη δεύτερη με $h_2\in K[x_1,...,x_n]$, κτλ και προσθέτοντας παίρνουμε:

$$h_1f_1+...+h_sf_s=0\,,$$

Το αριστερό μέλος είναι στοιχείο του $\langle f_1,...,f_s\rangle$, συνεπώς, μπορούμε να θεωρούμε το $\langle f_1,...,f_s\rangle$ ως το σύνολο που αποτελείται από όλα τα αποτελέσματα των πράξεων που έγιναν στις αρχικές εξισώσεις $f_1=...=f_s=0\,.$

Το ιδεώδες *I* θα λέγεται πεπερασμένο παραγόμενο, εάν υπάρχουν $f_1,...,f_s\in K[x_1,...,x_n]$, τέτοια ώστε $I=\langle f_1,...,f_s\rangle$ και επίσης τα $f_1,...,f_s$ θα λέγονται *βάση (basis)* του *I*. Ένα ιδώδες μπορεί να έχει πολλές βάσεις, αλλά η πιο χρήσιμη από αυτές είναι η Groebner που θα δούμε στο Κεφάλαιο 2.

Τα ιδεώδη συνδέονται με τη γραμμική άλγεβρα, καθώς μοιάζουν πολύ με τους υποχώρους, με μόνη διαφορά ότι στους υποχώρους πολλαπλασιάζουμε με αριθμούς, ενώ στα ιδεώδη με πολυώνυμα. Επίσης, το παραγόμενο ιδεώδες από τα $f_1,...,f_s$, μοιάζει με το ανάπτυγμα πεπερασμένων διανυσμάτων $\upsilon_1,...,\upsilon_s$. Και στις δύο περιπτώσεις παίρνουμε

γραμμικούς συνδυασμούς, απλά για το ανάπτυγμα χρησιμοποιούμε συντελεστές από το σώμα *K,* ενώ για το ιδεώδες χρησιμοποιούμε πολυωνυμικούς συντελεστές.

Πρόταση 1.4.4 [1]

Αν $f_1,...,f_s$ και $g_1,...,g_t$ είναι βάσεις του ίδιου ιδεώδους στο $K[x_1,...,x_n]$, τέτοιες ώστε $\langle f_1,...,f_s\rangle = \langle g_1,...,g_t\rangle$. Τότε ισχύει $\mathrm{V}(f_1,...,f_s) = \mathrm{V}(g_1,...,g_t)$

Απόδειξη

Από την $\langle f_1,...,f_s\rangle = \langle g_1,...,g_t\rangle$ συνεπάγεται ότι $h_1f_1 + ... + h_sf_s = \varphi_1 g_1 + ... + \varphi_t g_t$ για .

Η $\mathrm{V}(f_1,...,f_s)$ περιγράφει τις λύσεις $(a_1,...,a_n)$ του συστήματος $f_1 = ... = f_s = 0$. Άρα $\sum h_i f_i(a_1,...,a_n) = 0$ $h_i, \varphi_j \in K[x_1,...,x_n]$ και συνεπώς

$$h_1f_1(a_1,...,a_n) + ... + h_sf_s(a_1,...,a_n) = \varphi_1 g_1(a_1,...,a_n) + ... + \varphi_t g_t(a_1,...,a_n) = 0 .$$

Επομένως, τα $(a_1,...,a_n)$ είναι επίσης λύσεις των εξισώσεων $g_1 = ... = g_t = 0$ και τελικά ισχύει $\mathrm{V}(f_1,...,f_s) = \mathrm{V}(g_1,...,g_t)$. ∆

Σύμφωνα με την παραπάνω πρόταση, μπορούμε να αλλάζουμε τη βάση ενός ιδεώδους, για να προσδιορίζουμε μια πολλαπλότητα ευκολότερα. Για παράδειγμα, θεωρούμε την πολλαπλότητα $\mathrm{V}(3x^2 - 2y^2 - 7, x^2 - y^2 - 1)$. Ισχύει ότι:

$$\langle 3x^2 - 2y^2 - 7, x^2 - y^2 - 1\rangle = \langle x^2 - 6, y^2 - 4\rangle .$$

Άρα $\mathrm{V}(3x^2 - 2y^2 - 7, x^2 - y^2 - 1) = \left\{\left(\pm\sqrt{6}, \pm 2\right)\right\}$.

Επομένως, αλλάζοντας τη βάση, προσδιορίσαμε την πολλαπλότητα ευκολότερα.

Γενικά, οι αφινικές πολλαπλότητες καθορίζονται από ιδεώδη και όχι από εξισώσεις. Όμως στη στριμμένη κυβική καμπύλη, είδαμε ότι έπειτα από την παραμετροποίηση (t,t^2,t^3) , εκτός από τα πολυώνυμα $y-x^2, z-x^3$ μηδενίστηκαν και τα πολυώνυμα $z-xy, y^2-xz$. Για να δούμε πώς βρίσκουμε όλα τα πολυώνυμα που μηδενίζονται σε μια πολλαπλότητα *V*, εισάγουμε τον παρακάτω ορισμό:

Ορισμός 1.4.5 [1]

Έστω $V \subset K^n$ μια αφινική πολλαπλότητα .Τότε ορίζεται το σύνολο

$$\mathrm{I}(V) = \{ f \in K[x_1,...,x_n] : f(a_1,...,a_n) = 0, \forall (a_1,...,a_n) \in V \}$$

Λήμμα 1.4.6 [1]

Αν $V \subset K^n$ είναι μια αφινική πολλαπλότητα, τότε το $\mathrm{I}(V) \subset K[x_1,...,x_n]$ είναι ιδεώδες και ονομάζεται ιδεώδες της *V.*

Απόδειξη

Είναι προφανές ότι ισχύει ότι $0 \in \mathrm{I}(V)$, καθώς το μηδενικό πολυώνυμο μηδενίζεται σε όλα τα σώματα K^n, και άρα μηδενίζεται και στη *V.* Έπειτα, υποθέτουμε ότι $f, g \in \mathrm{I}(V)$ και $h \in K[x_1,...,x_n]$. Έστω $(a_1,...,a_n)$, ένα τυχαίο σημείο της *V.* Τότε

$$f(a_1,...,a_n) + g(a_1,...,a_n) = 0 + 0 = 0$$
$$h(a_1,...,a_n) f(a_1,...,a_n) = h(a_1,...,a_n) \cdot 0 = 0$$

και έπεται ότι $\mathrm{I}(V)$ είναι ιδεώδες. ∆

Εφαρμογή [1]

Έστω η στριμμένη κυβική καμπύλη $V = \mathrm{V}(y - x^2, z - x^3) \subset \mathrm{R}^3$. Θέλουμε να δείξουμε ότι

$$\mathrm{I}(V) = \langle y - x^2, z - x^3 \rangle .$$

Αρχικά ,θα δείξουμε ότι κάποιο πολυώνυμο $f \in \mathrm{R}[x.y, z]$, μπορεί να γραφεί στη μορφή

$$(1.4.1) \qquad f = h_1(y - x^2) + h_2(z - x^3) + r ,$$

όπου $h_1, h_2 \in \mathrm{R}[x, y, z]$, ενώ το *r* είναι πολυώνυμο που αποτελείται μόνο από *x*.

Για την περίπτωση όπου *f* είναι ένα μονώνυμο $x^a y^\beta z^\gamma$, από το θεώρημα των διωνύμων παίρνουμε:

$$x^a y^\beta z^\gamma = x^a (x^2 + (y - x^2))^\beta (x^3 + (z - x^3))^\gamma$$
$$= x^a (x^{2\beta} + \text{όροι που περιέχουν το } \ y - x^2) \ (x^{3\gamma} + \text{όροι που περιέχουν το } \ z - x^3)$$

και με επιμεριστική παίρνουμε:

$$x^\alpha y^\beta z^\gamma = h_1(y - x^2) + h_2(z - x^3) + x^{\alpha+2\beta+3\gamma}, h_1, h_2 \in \mathrm{R}[x, y, z].$$

Επομένως ιχύει η (1.4.1). Και δεδομένου ότι για ένα τυχαίο $f \in \mathrm{R}[x, y, z]$, δείξαμε ότι είναι
γραμμικός συνδυασμός μονωνύμων, έπεται ότι η (1.4.1) ισχύει γενικά.

Πλέον μπορούμε να δείξουμε ότι $\mathrm{I}(V) = \langle y - x^2, z - x^3 \rangle$. Από τον ορισμό της στριμμένης κυβικής καμπύλης, ξέρουμε ότι $y - x^2, z - x^3 \in \mathrm{I}(V)$, και αφού το $\mathrm{I}(V)$ είναι ιδεώδες, συμπεραίνουμε ότι $h_1(y - x^2) + h_2(z - x^3) \in \mathrm{I}(V)$. Άρα $\langle y - x^2, z - x^3 \rangle \in \mathrm{I}(V)$. Για το αντίστροφο, θεωρούμε $f \in \mathrm{I}(V)$ και έστω ότι

$$f = h_1(y - x^2) + h_2(z - x^3) + r \, .$$

Για να δείξουμε ότι *r*=0, χρησιμοποιούμε την παραμετροποίηση (t, t^2, t^3) της στριμμένης κυβικής καμπύλης. Εφόσον το *f* μηδενίζεται στη *V,* παίρνουμε

$$0 = f(t, t^2, t^3) = 0 + 0 + r(t) \quad .$$

Υπενθυμίζουμε ότι το *r* είναι πολυώνυμο με μεταβλητή μόνο το *x*. Επειδή *t* είναι κάποιος πραγματικός αριθμός, συνεπάγεται ότι το $r \in \mathrm{R}[x]$ πρέπει να είναι το μηδενικό πολυώνυμο. Αλλά το ότι *r*=0, σημαίνει ότι η *f* έχει την επιθυμητή μορφή, και τελικά ισχύει $\mathrm{I}(V) = \langle y - x^2, z - x^3 \rangle$.

<u>Λήμμα 1.4.7</u> [1]

Αν $f_1, ..., f_s \in K[x_1, ..., x_n]$, τότε $\langle f_1, ..., f_s \rangle \subset \mathrm{I}(\mathrm{V}(f_1, ..., f_s))$. Το αντίστροφο δεν ισχύει πάντα.

<u>Απόδειξη</u>

Έστω $f \in \langle f_1, ..., f_s \rangle$, που σημαίνει ότι $f = \sum_{i=1}^{s} h_i f_i$, για κάποια πολυώνυμα $h_1, ..., h_s \in K[x_1, ..., x_n]$. Επειδή τα $f_1, ..., f_s$ μηδενίζονται στην $\mathrm{V}(f_1, ..., f_s)$, άρα μηδενίζεται και το $\sum_{i=1}^{s} h_i f_i$. Συνεπώς το *f* μηδενίζεται στην $\mathrm{V}(f_1, ..., f_s)$, που τελικά αποδεικνύει $f \in \mathrm{I}(\mathrm{V}(f_1, ..., f_s)$. Για να αποδείξουμε το αντίστροφο, χρειαζόμαστε ένα παράδειγμα στο οποίο το $\mathrm{I}(\mathrm{V}(f_1, ..., f_s)$ να είναι αυστηρά μεγαλύτερο του $\langle f_1, ..., f_s \rangle$. Θα δείξουμε ότι για τη σχέση

$$\langle x^2, y^2 \rangle \subset \mathrm{I}(\mathrm{V}(x^2, y^2))$$

Δεν ισχύει ο αντίστροφος εγκλεισμός. Αρχικά, υπολογίζουμε το $\mathrm{I}(\mathrm{V}(x^2, y^2))$. Από τις εξισώσεις $x^2 = y^2 = 0$, συνεπάγεται ότι $\mathrm{V}(x^2, y^2) = \{(0,0)\}$ αλλά το ιδεώδες της {(0,0)}

είναι το $\langle x, y\rangle$ και άρα $\mathrm{I}(\mathrm{V}(x^2, y^2)) = \langle x, y\rangle$. Οπότε, πρέπει να δείξουμε ότι αυτό είναι αυστηρά μεγαλύτερο του $\langle x^2, y^2\rangle$. Παρατηρούμε ότι $x \notin \langle x^2, y^2\rangle$, καθώς για τα πολυώνυμα της μορφής $h_1(x, y)x^2 + h_2(x, y)y^2$ κάθε μονώνυμο έχει συνολικό βαθμό τουλάχιστον δύο. ▵

§1.5 ΠΟΛΥΩΝΥΜΑ ΜΙΑΣ ΜΕΤΑΒΛΗΤΗΣ

Στο κεφάλαιο αυτό θα μελετήσουμε πολυώνυμα μιας μεταβλητής, καθώς επίσης και τον αλγόριθμο της διαίρεσης για τέτοια πολυώνυμα. Ο αλγόριθμος της διαίρεσης είναι βασικό εργαλείο για τον προσδιορισμό της δομής των ιδεωδών του $K[x]$. Επίσης,θα εμβαθύνουμε και στην έννοια του *μέγιστου κοινού διαιρέτη* και τη χρήση του στο να επιλύουμε διάφορα προβλήματα, όπως αυτο της συμμετοχής των ιδεωδών, δηλαδή αν υπάρχει αλγόριθμος που να καθορίζει αν κάποιο $f \in K[x_1,...,x_n]$ ανήκει στο $\langle f_1,...,f_s \rangle$.

Ορισμός 1.5.1 [1]
Έστω ένα μη-μηδενικό πολυώνυμο $f \in K[x]$, και έστω

$$f = a_0 x^m + a_1 x^{m-1} + ... + a_m ,$$

όπου $a_i \in K, a_0 \neq 0$, (άρα $m = \deg(f)$). Τότε ο $a_0 x^m$ θα ονομάζεται **μεγιστοβάθμιος όρος (leading term)** της *f,* και θα συμβολίζεται με $\mathrm{LT}(f) = a_0 x^m$.

Γενικά, για δύο μη-μηδενικά πολυώνυμα *f,g* θα ισχύει

(1.5.1) $$\deg(f) \leq \deg(g) \Leftrightarrow \mathrm{LT}(f) \big| \mathrm{LT}(g) .$$

Πρόταση 1.5.2 (Ο Αλγόριθμος της Διαίρεσης) [1]
Έστω *K* ένα σώμα και *g* ένα μη-μηδενικό πολυώνυμο στο *K*[*x*]. Τότε κάθε $f \in K[x]$ μπορεί να γραφτεί ως

$$f = qg + r$$

όπου $q, r \in K[x]$ και ισχύει είτε *r*=0, είτε $\deg(f) < \deg(g)$. Επιπλέον, τα *q,r* είναι μοναδικά και υπάρχει αλγόριθμος για την εύρεσή τους.

Απόδειξη

Ακολουθεί αλγόριθμος σε μορφή ψευδοκώδικα που δείχνει πώς βρίσκουμε τα q και r.

Είσοδοι: g,f

Έξοδοι: q,r

$q:=0;\ r:=f$

ΟΣΟ ($r \neq 0$ AND LT(g) διαιρεί τον LT(r)) ΕΚΤΕΛΕΣΕ

$$q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$$
$$r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$$

Η εντολή ΟΣΟ...ΕΚΤΕΛΕΣΕ εκτελείται όσο η έκφραση ανάμεσά τους είναι αληθής. Οι εντολές $q:=...,\ r:=...$ δείχνουν ότι ορίζουμε και επανορίζουμε τις τιμές των q,r. Και το q και το r είναι *μεταβλητές* του αλγορίθμου και αλλάζουν τιμές σε κάθε βήμα. Πρέπει να δείξουμε ότι ο αλγόριθμος τερματίζει και οι τελικές τιμές των q,r έχουν τις επιθυμητές ιδιότητες.

Αρχικα, παρατηρούμε ότι η σχέση $f = qg + r$ ισχύει για τις αρχικές τιμές των q,r και καθώς επαναορίζονται η παραπάνω ισότητα παραμένει αληθής. Αυτό συμβαίνει διότι ισχύει η ισότητα

$$f = qg + r = (q + \mathrm{LT}(r)/\mathrm{LT}(g))g + (r - (\mathrm{LT}(r)/\mathrm{LT}(g))g .$$

Επειτα, παρατηρούμε ότι η εντολή ΟΣΟ...ΕΚΤΕΛΕΣΕ παύει να εκτελείται όταν η πρόταση "$r\neq 0$ και LT(g) διαιρεί τον LT(r)" γίνει ψευδής, δηλαδή παύει να εκτελείται όταν r=0 ή όταν ο LT(g) δε διαιρεί πλέον τον LT(r). Σύμφωνα με την (1.5.1), αυτό σημαίνει ότι $\deg(r) < \deg(g)$. Έτσι όταν ο αλγόριθμος τερματίζει, τα q,r έχουν τις επιθυμητές ιδιότητες.

Απομένει όμως να δείξουμε ότι όντως ο αλγόριθμος τερματίζει, δηλαδή ότι η έκφραση μεταξύ του ΟΣΟ και ΕΚΤΕΛΕΣΕ κάποια στιγμή γίναται ψευδής. Αρκεί να δείξουμε λοιπόν ότι το $(r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$ είτε είναι 0, είτε έχει βαθμό μικρότερο του r. Έστω λοιπόν

$$r = a_0x^m + ... + a_m, \mathrm{LT}(r) = a_0x^m$$
$$g = b_0x^k + ... + b_k, \mathrm{LT}(g) = b_0x^k$$

Και έστω ότι $m \geq k$. Τότε:

$$(r - (\mathrm{LT}(r)/\mathrm{LT}(g))g = (a_0x^m + ...) - (a_0/b_0)x^{m-k}(b_0x^k + ...)$$

και έπεται ότι ο βαθμός του *r* πρέπει να μειωθεί, (ή όλη η έκφραση να μηδενιστεί). Καθώς ο βαθμός είναι πεπερασμένος, σημαίνει ότι μπορεί να πέσει πεπεραμένες τι πλήθος φορές, πράγμα που αποδεικνύει ότι ο αλγόριθμος τελικά τερματίζει.

Για να δούμε πώς εφαρμόζεται στην πράξη ο παραπάνω αλγόριθμος, ας δούμε ένα παράδειγμα όπου $f = x^3 + 2x^2 + x + 1$ και $g = 2x + 1$. Σύμφωνα με τη διαίρεση, έτσι όπως την έχουμε μάθει από το σχολείο, παίρνουμε:

$$\begin{array}{l|l} x^3 + 2x^2 + x + 1 & 2x + 1 \\ \hline -x^3 + 1/2 \cdot x^2 & \overline{1/2 \cdot x^2} \\ \hline 3/2 \cdot x^2 + x + 1 & \end{array}$$

Σε αυτήν τη φάση του αλγορίθμου, ισχύει ότι $q = \frac{1}{2}x^2$ και $r = \frac{3}{2}x^2 + x + 1$. Αυτές οι τιμές όμως δεν είναι οι τελικές. Έπειτα εκτελούνται οι εντολές

$$q := q + \mathrm{LT}(r)/\mathrm{LT}(g)$$
$$r := r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$$

Όπου μας δίνουν τις τελικές τιμές των *q,r.* Απομένει να δειξουμε ότι αυτές οι τιμές είναι μοναδικές. θεωρούμε ότι ισχύει ότι $f = qg + r = q'g + r'$, όπου τα r, r' έχουν βαθμό μικρότερο του *g*. Εάν $r \neq r'$, τότε $\deg(r' - r) < \deg(g)$. Επιπλέον όμως ισχύει

(1.5.2) $(q-q')g = r'-r$

που σημαίνει ότι $q-q' \neq 0$, και συνεπώς,

$$\deg(r'-r) = \deg((q-q')g) = \deg(q-q') + \deg(g) \geq \deg(g),$$

Άτοπο. Άρα συνεπάγεται ότι $r = r'$, και από τη (5.2) παίρνουμε $q = q'$. △

Πόρισμα 1.5.3 [1]

Εάν *K* είναι ένα σώμα, τότε κάθε ιδεώδες του $K[x]$ μπορεί να γραφτεί ως $\langle f \rangle$ για κάποιο $f \in K[x]$. Επιπλέον το *f* είναι μοναδικό και απλά μπορεί να πολλαπλασιάζεται με μια μη-μηδενική σταθερά του *K*.

Γενικά, ένα ιδεώδες που παράγεται από ένα στοιχείο, θα λέγεται *βασικό ιδεώδες* (*principal ideal*) και το $K[x]$ θα λέγεται *βασικός χώρος ιδεωδών* (*principal ideal domain* (PID)).

Ορισμός 1.5.4 [1]

Μέγιστος κοινός διαιρέτης (Greatest Common Divisor) των πολυωνύμων $f, g \in K[x]$, είναι ένα πολυώνυμο *h* για το οποίο ισχύει:

i. Το *h* διαιρεί τα *f* και *g*
ii. Εάν *p* είναι κάποιο άλλο πολυώνυμο που διαιρεί τα *f* και *g,* τότε το *p* διαιρεί και το *h.*

Τότε θα συμβολίζουμε $h = \text{GCD}(f, g) = \text{ΜΚΔ}(f, g)$.

Πρόταση 1.5.5 [1]

Έστω $f, g \in K[x]$. Τότε:

i. Υπάρχει ο $\text{ΜΚΔ}(f, g)$ και είναι μοναδικός, απλά μπορεί να πολλαπλασιάζεται με μια μη-μηδενική σταθερά.
ii. Ο $\text{ΜΚΔ}(f, g)$ είναι γεννήτορας του ιδεωδούς $\langle f, g \rangle$.
iii. Υπάρχει αλγόριθμος για την εύρεση του $\text{ΜΚΔ}(f, g)$

Απόδειξη

Έστω ένα ιδεώδες $\langle f, g\rangle$. Συμφωνα με το Πόρισμα 1.5.3, επειδή κάθε ιδεώδες του $K[x]$ είναι βασικό, υπάρχει $h \in K[x]$, τέτοιο ώστε $\langle f, g\rangle = \langle h\rangle$. Εμεις, θέλουμε να δείξουμε ότι $h = \text{ΜΚ}\Delta(f, g)$. Αρχικά, παρατηρούμε ότι το h διαιρεί τα f,g εφόσον $f, g \in \langle h\rangle$. Συνεπώς ικανοποιείται η πρώτη προϋπόθεση του Ορισμού 1.5.4. Έπειτα, υποθέτουμε ότι το $p \in K[x]$, διαιρεί τα *f,g*. Αυτό σημαίνει ότι υπάρχουν $C, D \in K[x]$ τέτοια ώστε $f = Cp, g = Dp$. Δεδομένου ότι $h \in \langle f, g\rangle$, υπάρχουν *A,B* για τα οποία ισχύει *Af+Bg=h.* Αντικαθιστώντας παίρνουμε

$$h = Af + Bg = ACp + BDp = (AC + BD)p$$

που σημαίνει ότι το *p* διαιρεί το *h* και άρα $h = \text{ΜΚ}\Delta(f, g)$.

Άρα δείξαμε ότι υπάρχει ο ΜΚΔ και τώρα πρέπει να δείξουμε ότι είναι μοναδικός. Έστω *h'* ένας ακόμη ΜΚΔ των *f,g.* Από τη δεύτερη προϋπόθεση του Ορισμού 1.5.4, τα *h,h'* διαιρούν το ένα το άλλο. Αυτό σημαίνει ότι το *h* είναι μια μη-μηδενική σταθερά, πολλαπλάσια του *h'*. Άρα ως στιγμής έχουμε δείξει το πρώτο μέρος της Πρότασης 1.5.5 και το δεύτερο μέρος ισχύει από τον τρόπο που βρήκαμε το *h.*

Στην πραγματικότητα, η παραπάνω απόδειξη για την ύπαρξη ΜΚΔ δεν είναι εύχρηστη, καθώς χρειάζεται να βρούμε γεννήτορα του $\langle f, g\rangle$. Όπως διαπιστώσαμε και παραπάνω, αυτό σημαίνει πως πρέπει να βρούμε τους βαθμούς όλων των πολυωνύμων, τα οποία όμως είναι άπειρα. Το τρίτο μέρος της Πρότασης 5.5, μας δείχνει ότι υπάρχει αλγόριθμος για τον υπολογισμό του ΜΚΔ δύο πολυωνύμων του $K[x]$. Ο αλγόριθμος αυτός είναι γνωστός ως *Ευκλείδειος Αλγόριθμος.*

Έστω $f, g \in K[x]$, όπου $g \neq 0$, και $f = qg + r$, όπου τα *q,r* υπολογίζονται σύμφωνα με την Πρόταση 1.5.2. Ορίζουμε $r = remainder(f, g) = \upsilon\pi\acute{o}\lambda o\iota\pi o(f, g)$. Ο ευκλείδειος αλγόριθμος είναι ο εξής:

Είσοδοι: *f,g*

Έξοδοι: *h*

h:=f

s:=g

ΟΣΟ $s \neq 0$ ΕΚΤΕΛΕΣΕ

rem:=remainder(*h,s*)

h:=s

s:=rem

Για να διαπιστώσουμε ότι όντως αυτός ο αλγόριθμος λειτουργεί, σύμφωνα με την Πρόταση 1.5.2, γράφουμε την *f* ως *f=qg+r.* Θέλουμε να δείξουμε ότι

$$(1.5.3) \qquad \text{ΜΚ}\Delta(f,g) = \text{ΜΚ}\Delta(f-qg,g) = \text{ΜΚ}\Delta(r,g).$$

Από το (ii) συνεπάγεται ότι αρκεί να δείξουμε ότι τα ιδεώδη $\langle f,g\rangle, \langle f-qg,g\rangle$ είναι ισοδύναμα. Είναι προφανές ότι $\langle f-qg,g\rangle \in \langle f,g\rangle$. Επίσης,

$$\langle f-qg,g\rangle = h_1(f-qg)+h_2 g = h_1 f - h_1 qg + h_2 g = \langle f,g\rangle - h_1 qg$$

και άρα $\langle f,g\rangle = \langle f-qg,g\rangle + h_1 qg \Rightarrow \langle f,g\rangle \in \langle f-qg,g\rangle$.

Η (1.5.3) μπορεί να γραφεί ως

$$\text{ΜΚ}\Delta(f,g) = \text{ΜΚ}\Delta(g,r).$$

Παρατηρούμε ότι $\deg(g) > \deg(\text{r})$ ή $r = 0$. Αν $r \neq 0$, μπορούμε να απλοποιήσουμε κι άλλο την παραπάνω σχέση, γράφοντας $g = q'r + r'$, όπως στην Πρόταση 1.5.2, και σύμφωνα με την παραπάνω διαδικασία παίρνουμε

$$\text{ΜΚ}\Delta(g,r) = \text{ΜΚ}\Delta(r,r'),$$

όπου $\deg(r) > \deg(\text{r}')$ ή $r = 0$. Συνεχίζοντας την ίδια διαδικασία παίρνουμε

(1.5.4) $\quad \text{ΜΚ}\,\Delta(f,g) = \text{ΜΚ}\,\Delta(g,r) = \text{ΜΚ}\,\Delta(r,r') = \text{ΜΚ}\,\Delta(r',r'') = \ldots,$

όπου είτε μειώνεται ο βαθμός, δηλαδή ισχύει

$$\deg(g) > \deg(r) > \deg(r') > \deg(r'') > \ldots.,$$

είτε τερματίζει η διαδικασία, όταν κάποιο από τα $r, r', r'', \ldots.$ μηδενιστεί.

Ο Ευκλείδειος Αλγόριθμος λειτουργεί ως εξής:

Έχει μεταβλητές *h* και *s,* τις οποίες συναντούμε στην (1.5.4). Οι τιμές του *h* είναι είναι το πρώτο πολυώνυμο σε κάθε ΜΚΔ και οι τιμές του *s* είναι το δεύτερο. Παρατηρούμε ότι στην (1.5.4), η μετάβαση από τον έναν ΜΚΔ στον επόμενο σημαίνει την εκτέλεση της εντολής ΟΣΟ...ΕΚΤΕΛΕΣΕ. Άρα, σε οποιοδήποτε στάδιο του αλγορίθμου ισχύει $\text{ΜΚΔ}(h,s) = \text{ΜΚΔ}(f,g)$.

Ο αλγόριθμος τερματίζει καθώς ο βαθμός του *s* συνεχώς μειώνεται και συνεπώς, κάποια στιγμή μηδενίζει. Όταν συμβεί αυτό, θα ισχύει $\text{ΜΚ}\,\Delta(h,0) = \text{ΜΚ}\,\Delta(f,g)$ και επειδή είναι προφανές ότι $\langle h,0\rangle = \langle h\rangle$, άρα τελικά ισχύει $\text{ΜΚ}\,\Delta(h,0) = h$. Άρα από αυτές τις δύο ισότητες έπεται ότι $\text{ΜΚ}\,\Delta(f,g) = h$, όταν *s*=0, και έτσι αποδείχτηκε η Πρόταση 1.5.5 Δ

<u>Ορισμός 1.5.6</u> [1]

Μέγιστος κοινός διαιρέτης των πολυωνύμων $f_1,\ldots,f_s \in K[x]$, είναι ένα πολυώνυμο *h* για το οποίο ισχύει:

i. Το *h* διαιρεί τα $f_1,\ldots,f_s$

ii. Αν *p* είναι ένα άλλο πολυώνυμο που διαιρεί τα $f_1,\ldots,f_s$, τότε το *p* διαιρεί και το *h.*

Σε αυτήν την περίπτωση θα συμβολίζουμε $h = \text{ΜΚΔ}(f_1,\ldots,f_s)$.

Πρόταση 1.5.7 [1]

Έστω $f_1,...,f_s \in K[x]$ με $s \geq 2$. Τότε:

i. Ο $\text{ΜΚΔ}(f_1,...,f_s)$ υπάρχει και είναι μοναδικός, απλά μπορεί να πολλαπλάσιαζεται με μια μη-μηδενική σταθερά.

ii. Ο $\text{ΜΚΔ}(f_1,...,f_s)$ ειναι γεννήτορας του ιδεώδους $\langle f_1,...,f_s \rangle$

iii. Εάν $s \geq 3$, τότε $\text{ΜΚΔ}(f_1,...,f_s) = \text{ΜΚΔ}(f_1, \text{ΜΚΔ}(f_2,...,f_s))$

iv. Υπάρχει αλγόριθμος για την εύρεση του $\text{ΜΚΔ}(f_1,...,f_s)$.

Παράδειγμα 1.5.8

Έστω το ιδεώδες

$$\langle 2x^3 - 3x^2 - 3x + 2, x^2 - 3x + 2, x^4 - 16 \rangle \subset K[x].$$

Γνωρίζουμε ότι ο $\text{ΜΚΔ}(2x^3 - 3x^2 - 3x + 2, x^2 - 3x + 2, x^4 - 16)$ είναι γεννήτορας. Επιπλέον ισχύει:

$$\begin{aligned} &\text{ΜΚΔ}(2x^3 - 3x^2 - 3x + 2, x^2 - 3x + 2, x^4 - 16) = \\ &\text{ΜΚΔ}(2x^3 - 3x^2 - 3x + 2, \text{ΜΚΔ}(x^2 - 3x + 2, x^4 - 16) = \\ &\text{ΜΚΔ}(2x^3 - 3x^2 - 3x + 2, x - 2) = x - 2 \end{aligned}$$

Έπεται λοιπόν ότι

$$\langle 2x^3 - 3x^2 - 3x + 2, x^2 - 3x + 2, x^4 - 16 \rangle = \langle x - 2 \rangle \qquad \triangle$$

Στην αρχή της παραγράφου, αναφέρθηκε το *πρόβλημα συμμετοχής των ιδεωδών*. Το συγκεκριμένο πρόβλημα, ελέγχει εάν κάποιο $f \in K[x]$, ανήκει στο $\langle f_1,...,f_s \rangle$, για κάποια $f_1,...,f_s \in K[x]$. Η απάντηση σε αυτό το ερώτημα είναι θετική.

Αρχικά, βρίσκω έναν γεννήτορα *h* του $\langle f_1,...,f_s \rangle$, μέσω του ΜΚΔ. Έπειτα, εφόσον το $f \in \langle f_1,...,f_s \rangle$ συνεπάγεται ότι $f \in \langle h \rangle$, αρκεί να γράψουμε το f ως $f = qh + r$ με $\deg(r) < \deg(h)$. Τότε, το *f* θα ανήκει στο ιδεώδες αν και μόνο αν *r*=0.

Παράδειγμα 1.5.9

Έστω ότι θέλουμε να ελέγξουμε εάν το x^3-2x^2+x-3 , ανήκει στο $\langle 2x^3-3x^2-3x+2, x^2-3x+2, x^4-16\rangle$. Είδαμε προηγουμένως ότι το x-2 είναι γεννήτορας αυτού του ιδεώδους, άρα τελικά αρκεί να ελέγξουμε εάν

$$x^3-2x^2+x-3 \in \langle x-2\rangle .$$

Διαιρώντας παίρνουμε:

$$x^3-2x^2+x-3=(x^2+1)(x-2)-1 \quad ,$$

που σημαίνει ότι τελικά το πολυώνυμο δεν ανήκει στο ιδεώδες $\langle 2x^3-3x^2-3x+2, x^2-3x+2, x^4-16\rangle$. $\triangle$

ΚΕΦΑΛΑΙΟ 2

ΒΑΣΗ GROEBNER

§2.1 ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο αρχικά περιγράφεται ο αλγόριθμος της διαίρεσης για πολυώνυμα πολλών μεταβλητών. Έπειτα γίνεται μελέτη της βάσης Groebner. Αυτή η βάση δίνει έναν αλγοριθμικό τρόπο για να επιλύουμε προβλήματα με ιδεώδη, όπως (α) *το πρόβλημα περιγραφής ιδεωδών*, δηλαδή αν ισχύει $I = \langle f_1, ..., f_s \rangle$, για κάποια $f_i \in K[x_1, ..., x_n]$, (β) *το πρόβλημα συμμετοχής ιδεωδών*, δηλαδή εάν κάποιο $f \in K[x_1, ..., x_n]$, ανήκει στο $I = \langle f_1, ..., f_s \rangle$, (γ) *το πρόβλημα επίλυσης πολυωνυμικών εξισώσεων*, δηλαδή η εύρεση όλων των λύσεων του συστήματος $f_1(x_1, ..., x_n) = ... = f_s(x_1, ..., x_n) = 0$. Τέλος παραθέτεται (δ) *το πρόβλημα πεπλεγμένης αναπαράστασης*, δηλαδή πώς βρίσκουμε τις αρχικές εξισώσεις ενός συστήματος όταν ξέρουμε τις παραμετρικές, που γεωμετρικά αυτό υποδεικνύει αν η V παριστάνει πολλαπλότητα ή μέρος της πολλαπλότητας.

Γενικός στόχος είναι λοιπόν να επεκτείνουμε τεχνικές που είδαμε στο προηγούμενο κεφάλαιο σε πολυώνυμα πολλών μεταβλητών, κάνοντας χρήση της βάσης Groebner, ώστε να απαντηθούν τα παραπάνω προβλήματα.

Σχετικά με το πρόβλημα πεπλεγμένης αναπαράστασης, έστω ότι έχουμε να λύσουμε το σύστημα πολυωνυμικών εξισώσεων:

$$\begin{array}{c} a_{11}x_1 + ... + a_{1n}x_n + b_1 = 0 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n + b_m = 0 \end{array}, \qquad (2.1.1)$$

όπου κάθε πολυώνυμο είναι γραμμικό, (δηλαδή έχει συνολικό βαθμό=1).

Κάνουμε πράξεις μεταξύ των γραμμών του πίνακα

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & -b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & -b_m \end{pmatrix}$$

μέχρις ότου να το φέρουμε στην κλιμακωτή μορφή μειωμένων γραμμών. Έπειτα βάζοντας τιμές στις ελεύθερες μεταβλητές, βρίσκουμε όλες τις λύσεις του αρχικού συστήματος. Υπάρχουν περιπτώσεις που είτε έχουμε μόνο μία λύση, είτε δεν έχουμε καμία λύση. Καμία λύση έχουμε όταν η κλιμακωτή μορφή μειωμένων γραμμών περιέχει γραμμή της μορφής (0,.....,0,1) που αντιστοιχεί στην εξίσωση 0=1, που είναι άτοπο.

<u>Παράδειγμα 2.1.1</u>

Έστω ότι έχουμε να λύσουμε το σύστημα

$$\begin{aligned} x_1 - x_2 - x_3 - 1 &= 0 \\ 2x_1 - 2x_2 + x_3 - 1 &= 0 \\ 5x_1 - 5x_2 - 2x_3 - 4 &= 0 \end{aligned} \qquad (2.1.2)$$

Εφαρμόζοντας την αναγωγή γραμμών στον πίνακα του συστήματος, προκύπτει η κλιμακωτή μορφή:

$$\begin{pmatrix} 1 & -1 & -1 & 1 \\ 2 & -2 & 1 & 1 \\ 5 & -5 & -2 & 4 \end{pmatrix} \xrightarrow{\gamma_2=\gamma_2-2\gamma_1} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 0 & 3 & -1 \\ 5 & -5 & -2 & 4 \end{pmatrix} \xrightarrow{\gamma_3=\gamma_3-5\gamma_1} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 3 & -1 \end{pmatrix} \xrightarrow{\gamma_3=\gamma_3-\gamma_2}$$

$$\begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\gamma_2=\gamma_2/3} \begin{pmatrix} 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & -1/3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\gamma_1=\gamma_1+\gamma_2} \begin{pmatrix} 1 & -1 & 0 & 2/3 \\ 0 & 0 & 1 & -1/3 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

Από τη μορφή του πίνακα συμπεραίνουμε ότι η x_2 είναι ελεύθερη μεταβλητή. Έτσι, θέτοντας $x_2 = t$, παίρνουμε:

$$\begin{aligned} x_1 &= t + 2/3 \\ x_2 &= t \\ x_3 &= -1/3 \end{aligned} \quad .$$

Αυτές είναι οι παραμετρικές εξισώσεις μιας ευθείας L στο K^3. Το αρχικό σύστημα των εξισώσεων (2.1.2), παριστάνει την L ως αφινική πολλαπλότητα.

Για το αντίστροφο, έστω ένα υποσύνολο V του K^n, που οι παραμετρικές του εξισώσεις είναι οι:

$$\begin{aligned} x_1 &= a_{11}t_1 + \ldots + a_{1m}t_m + b_1 \\ &\vdots \\ x_n &= a_{n1}t_1 + \ldots + a_{nm}t_m + b_n \end{aligned} \qquad (2.1.3)$$

Η V είναι γραμμικός αφινικός υποχώρος, εφόσον μπορεί να γραφτεί ως εικόνα της συνάρτησης $F : K^m \to K^n$ που ορίζεται από τον κανόνα

$$F(t_1, \ldots, t_m) = (a_{11}t_1 + \cdots + a_{1m}t_m + b_1, \ldots\ldots, a_{n1}t_1 + \cdots + a_{nm}t_m + b_n) .$$

Έστω λοιπόν ότι θέλουμε να λύσουμε το πρόβλημα πεπλεγμένης αναπαράστασης για αυτήν την περίπτωση. Στην ουσία δηλαδή, ψάχνουμε για ένα σύστημα γραμμικών εξισώσεων, των οποίων οι λύσεις είναι τα σημεία της V.

<u>Παράδειγμα 2.1.2</u> [1]

Έστω ο γραμμικός αφινικός υποχώρος $V \subset K^4$ που ορίζεται από τις εξισώσεις:

$$\begin{aligned} x_1 &= t_1 + t_2 + 1 \\ x_2 &= t_1 - t_2 + 3 \\ x_3 &= 2t_1 - 2 \\ x_4 &= t_1 + 2t_2 - 3 \end{aligned}$$

Ξαναγράφουμε τις παραπάνω εξισώσεις ως:

$$
\begin{aligned}
t_1 + t_2 - x_1 + 0x_2 + 0x_3 + 0x_4 &= -1 \\
t_1 - t_2 - 0x_1 - x_2 + 0x_3 + 0x_4 &= -3 \\
2t_1 + 0t_2 + 0x_1 + 0x_2 - x_3 + 0x_4 &= 2 \\
t_1 + 2t_2 + 0x_1 + 0x_2 + 0x_3 - x_4 &= 3
\end{aligned}
$$

και παίρνουμε τον πίνακα

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

Η κλιμακωτή μορφή μειωμένων γραμμών είναι η:

$$
\begin{pmatrix}
1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\
0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\
0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\
0 & 0 & 0 & 1 & -3/4 & 1/2 & 3
\end{pmatrix}
$$

Παρατηρούμε ότι στις δύο τευλευταίες γραμμές οι δύο πρώτες είσοδοι είναι μηδέν και άρα αυτές οι δύο γραμμές αντιστοιχούν στις εξισώσεις:

$$
\begin{aligned}
x_1 - 1/4\, x_3 - 1/2\, x_4 - 3 &= 0 \\
x_2 - 3/4\, x_3 + 1/2\, x_4 - 3 &= 0
\end{aligned}
$$

Οι παραπάνω εξισώσεις περιγράφουν τη V στο K^4.

§2.2 ΔΙΑΤΑΞΗ ΜΟΝΩΝΥΜΩΝ ΣΤΟ $K[x_1,...,x_n]$

Στον αλγόριθμο της διαίρεσης στον $K[x]$ του Κεφαλαίου 1, ή τον αλγόριθμο της κλιμακωτής μορφής μειωμένων γραμμών που χρησιμοποιήσαμε παραπάνω, σημαντικό ρόλο παίζει η ταξινόμηση των όρων των πολυωνύμων. Επομένως, για την επέκταση αυτών των αλγορίθμων για πολυώνυμα περισσότερων μεταβλητών, θα πρέπει να γίνει σωστή διάταξη των όρων των πολυωνύμων στο $K[x_1,...,x_n]$. Σε αυτήν την παράγραφο αναφέρονται διατάξεις που βοηθούν στη μελέτη των παραπάνω αλγορίθμων.

Δεδομένου ότι ένα μονώνυμο, κατασκευάζεται από μια n-αδα εκθετών $a=(a_1,...,a_n)\in Z_{\geq 0}^n$, υπάρχει μια ένα προς ένα αντιστοιχία μεταξύ των μονωνύμων του $K[x_1,...,x_n]$ και του $Z_{\geq 0}^n$. Επιπλέον, κάθε διάταξη > που ορίζουμε στον χώρο $Z_{\geq 0}^n$, μας δίνει μια διάταξη μονωνύμων. Ειδικότερα, αν $\alpha>\beta$ τότε και $x^a > x^\beta$. Οι τρόποι διάταξης είναι αρκετοί στο $Z_{\geq 0}^n$ αλλά προτιμάμε αυτόν που διευκολύνει περισσότερο τους υπολογισμούς .

<u>Ορισμός 2.2.1</u> [1]

Μια **διάταξη μονωνύμων** στο $K[x_1,...,x_n]$, είναι μια σχέση $>$ στο $Z_{\geq 0}^n$, ή ισοδύναμα, κάθε σχέση στο σύνολο των μονωνύμων x^a , που ικανοποιεί:

i. Η $>$ είναι σχέση ολικής (ή γραμμικής) διάταξης στο $Z_{\geq 0}^n$.

ii. Αν $\alpha>\beta$ και $\gamma\in Z_{\geq 0}^n$, τότε $\alpha+\gamma>\beta+\gamma$

iii. η $>$ είναι καλά διατεταγμένη στο $Z_{\geq 0}^n$. Δηλαδή για κάθε μη-κενό υποσύνολο του $Z_{\geq 0}^n$, υπάρχει μικρότερο στοιχείο σύμφωνα με τη σχέση >.

<u>Λήμμα 2.2.2</u> [1]

Μια σχέση διάταξης > στον $Z_{\geq 0}^n$, είναι καλά διατεταγμένη αν και μόνο αν κάθε αυστηρά φθίνουσα ακολουθία του $Z_{\geq 0}^n$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$ τελικά τερματίζει.

Ορισμός 2.2.3 (Λεξικογραφική Διάταξη-Lex Order) [1]

Έστω $\alpha = (\alpha_1, ..., \alpha_n), \beta = (\beta_1, ..., \beta_n) \in Z_{\geq 0}^n$. Θα λέμε ότι $\alpha >_{lex} \beta$, εάν στη διανυσματική διαφορά $\alpha - \beta \in Z_{\geq 0}^n$, η πρώτη από τα αριστερά μη-μηδενική είσοδος, είναι θετική. Επιπλέον θα γράφουμε $x^a >_{lex} x^\beta$ εάν $\alpha >_{lex} \beta$.

Παραδείγματα:

a. $(1,2,3) >_{lex} (1,1,1)$, αφού $\alpha - \beta = (0,1,2)$ και άρα η πρώτη μη-μηδενική είσοδος είναι θετική.

b. $(2,2,1) >_{lex} (0,2,9)$, αφού $\alpha - \beta = (2,0,-8)$ △

Για πολυώνυμα με δύο ή τρεις μεταβλητές θα χρησιμοποιούμε τον συμβολισμό x, y, z αντί για x_1, x_2, x_3.

Υπάρχουν πολλές λεξικογραφικές διατάξεις που αντιστοιχούν στον τρόπο που ταξινομούμε τις μεταβλητες. Συγκεκριμένα, για *n* μεταβλητές, υπάρχουν *n*! διαφορετικές λεξικογραφικές διατάξεις.

Ορισμός 2.2.4 (Μέγιστη Λεξικογραφική Διάταξη-Granded Lex Order) [1]

Έστω $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. Θα λέμε ότι $\alpha >_{grlex} \beta$ εάν

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \quad \text{ή} \quad |\alpha| = |\beta| \text{ και } \alpha >_{lex} \beta.$$

Παραδείγματα

a. $(1,1,3) >_{grlex} (0,2,0)$ αφού $|(1,1,3)| = 5 > |(0,2,0)| = 2$

b. $(1,2,4) >_{grlex} (1,1,5)$, αφού $|(1,2,4)| = |(1,1,5)|$ και επιπλέον $(1,2,4) >_{lex} (1,1,5)$ △

Όπως και στη λεξικογραφική διάταξη, έτσι και στη μέγιστη λεξικογραφική διάταξη όταν υπάρχουν *n* μεταβλητές, υπάρχουν *n*! διαφορετικες μέγιστες λεξικογραφικές διατάξεις.

<u>Ορισμός 2.2.5</u> (Μέγιστη Ανάστροφη Λεξικογραφική Διάταξη-Granded Reverse Lex Order) [1]

Έστω $\alpha, \beta \in Z_{\geq 0}^n$. Θα λέμε ότι $\alpha >_{grevlex} \beta$ αν

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \qquad \text{ή}$$

$|\alpha| = |\beta|$ και η δεξιότερη μη μηδενική είσοδος του $\alpha - \beta \in Z^n$ είναι αρνητική.

<u>Παραδείγματα</u>

a. $(4,7,1) >_{grevlex} (4,2,3)$ αφού $|(4,7,1)| = 12 > |(4,2,3)| = 9$

b. $(1,5,2) >_{grevlex} (4,1,3)$ αφού $|(1,5,2)| = |(4,1,3)|$ και $(1,5,2) - (4,1,3) = (-3,4,-1)$. ▵

Παρατηρούμε ότι και η μέγιστη λεξικογραφική αλλά και η μέγιστη ανάστροφη χρησιμοποιούν τον συνολικό βαθμό. Η πρώτη όταν συναντάει τον ίδιο συνολικό βαθμό, χρησιμοποιεί τη λεξικογραφική διάταξη και ελέγχει τις αριστερότερες μεταβλητές αναζητώντας τη μεγαλύτερη δύναμη. Αντιθέτως, η δεύτερη, όταν συναντάει τον ίδιο συνολικό βαθμό, ελέγχει τις δεξιότερες εισόδους και αναζητάει τη μικρότερη δύναμη.

Για παράδειγμα,

$$x^6 y^2 z^2 >_{grlex} x^4 yz^5,$$

αφού και τα δύο μονώνυμα έχουν συνολικό βαθμό 7 και επίσης $x^5 yz >_{lex} x^4 yz^2$.

Επιπλέον όμως ισχύει και

$$x^6y^2z^2 >_{grevlex} x^4yz^5,$$

αφού η μικρότερη μεταβλητή *z* έχει μικρότερο βαθμό στο πρώτο μονώνυμο.

Όπως στις lex και grlex διατάξεις, για *n* μεταβλητές, υπάρχουν *n*! διαφορετικές grevlex διατάξεις.

<u>Ορισμός 2.2.6</u> [1]

Έστω $f = \sum_a a_a x^a$ ένα μη-μηδενικό πολυώνυμο στο $K[x_1,...,x_n]$ και έστω $>$ μια διάταξη μονωνύμων.

i. Ο **πολλαπλός βαθμός (multidegree)** του *f* είναι

$$\text{multideg}(f) = \max\left(\alpha \in \mathbb{Z}_{\geq 0}^n : \alpha_\alpha \neq 0\right)$$

(βάλαμε max επειδή η διάταξη είναι η $>$)

ii. Ο **κύριος συντελεστής (leading coefficient)** του *f* είναι

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

iii. Το **κύριο μονώνυμο (leading monomial)** του *f* είναι

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

(ο συντελεστής του είναι 1)

iv. Ο **κύριος όρος (leading term)** του *f* είναι

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$$

Για παράδειγμα, έστω ότι έχουμε όπως και πριν το $f = -3xy^2z^3 + 2yz - x^4z + 4x^3y^4z^2$ και η > δηλώνει τη lex διάταξη Τότε:

$$\text{multideg}(f) = (4,0,1)$$
$$\text{LC}(f) = -1$$
$$\text{LM}(f) = x^4z$$
$$\text{LT}(f) = -x^4z$$

Λήμμα 2.2.7 [1]

Έστω $f, g \in K[x_1,...,x_n]$ δύο μη-μηδενικά πολυώνυμα. Τότε:

i. $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$

ii. Εάν $f + g \neq 0$, τότε $\text{multideg}(f+g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. Η ισότητα ισχύει όταν $\text{multideg}(f) \neq \text{multideg}(g)$.

Απόδειξη

Έστω $f = \sum_{\alpha} a_\alpha x^\alpha$, $g = \sum_{\beta} a_\beta x^\beta$.

i. Επειδή $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$, άρα $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.

Το (ii), είναι προφανές. ∆

§2.3 Ο ΑΛΓΟΡΙΘΜΟΣ ΤΗΣ ΔΙΑΙΡΕΣΗΣ ΣΤΟ $K[x_1,...,x_n]$

Στόχος αυτής της παραγράφου είναι η επέκταση του Αλγορίθμου της Διαίρεσης σε πολυώνυμα πολλαπλών μεταβλητών. Ειδικότερα, θα δούμε πώς διαιρείται το $f \in K[x_1,...,x_n]$, με τα $f_1,...,f_s \in K[x_1,...,x_n]$ και κατ΄επέκταση πώς λύνεται το πρόβλημα συμμετοχής των ιδεωδών για πολυώνυμα μιας μεταβλητής. Ουσιαστικά πρέπει να εκφραστεί το f ως

$$f = a_1 f_1 + ... + a_s f_s + r ,$$

όπου τα πηλίκα $\alpha_1,...,\alpha_s$ και το υπόλοιπο r ανήκουν στο $K[x_1,...,x_n]$. Για να προσδιορίσουμε το υπόλοιπο r θα χρησιμοποιήσουμε τις διατάξεις που είδαμε στην §2.2. Έπειτα θα δούμε πώς ο αλγόριθμος της διαίρεσης εφαρμόζεται στο πρόβλημα συμμετοχής των ιδεωδών.

Κεντρική ιδέα, όπως και στα πολυώνυμα μιας μεταβλητής, είναι να εξαλείψουμε τον μεγιστοβάθμιο όρο του f. Αυτό γίνεται πολλαπλασιάζοντας κάποια από τα f_i με κατάλληλα μονώνυμα και αφαιρώντας. Τότε αυτό το μονώνυμο, γίνεται όρος για το αντίστοιχο a_i.

Παράδειγμα 2.3.1

Έστω ότι θέλουμε να διαιρέσουμε το $f = x^2y^2 + 1$ με τα $f_1 = x^2y + 1$ και $f_2 = y + 1$ χρησιμοποιώντας τη λεξικογραφική διάταξη $x > y$. Όπως και στα πολυώνυμα μιας μεταβλητής θα χρησιμοποιήσουμε τον αλγόριθμο της διαίρεσης με μόνη διαφορά ότι τώρα υπάρχουν πολλοί διαιρέτες και πηλίκα.

Παρατηρούμε ότι και ο $\mathrm{LT}(f_1) = x^2y$ και ο $\mathrm{LT}(f_2) = y$ διαιρούν τον $\mathrm{LT}(f) = x^2y^2$. Εμείς θα ξεκινήσουμε διαιρώντας το x^2y^2 με το $\mathrm{LT}(f_1)$ και περισσεύει το y. Έπειτα αφαιρώ το $y \cdot f_1$ από το f και έχω:

$$\begin{array}{l|l} x^2y^2+1 & \underline{x^2y+1} \\ \underline{x^2y^2-y} & y \\ -y+1 & \end{array}$$

Ακολουθούμε την ίδια διαδικασία για το $-y+1$. Αυτήν τη φορά όμως διαιρούμε με το f_2, αφού ο $\mathrm{LT}(f_1)=x^2y$ δε διαιρεί το $\mathrm{LT}(-y+1)=-y$. Έτσι, παίρνουμε:

$$\begin{array}{l|l} -y+1 & \underline{y+1} \\ \underline{y+1} & -1 \\ 2 & \end{array}$$

εφόσον ούτε ο $\mathrm{LT}(f_1)=x^2y$ ούτε ο $\mathrm{LT}(f_2)=y$ δε διαιρούν το 2, συμπεραίνουμε ότι r=2 και άρα το $f=x^2y^2+1$ μπορεί να γραφεί ως

$$xy^2+1=y\cdot(x^2y+1)+(-1)\cdot(y+1)+2 \qquad \vartriangle$$

<u>Παράδειγμα 2.3.2</u>

Έστω ότι θέλουμε να διαιρέσουμε το $f=x^3y^2+x^2y^2+y^2$ με τα $f_1=x^2y-1, f_2=y^2-1$. Χρησιμοποιούμε τη λεξικογραφική διάταξη $x>y$. Τα δύο πρώτα βήματα του αλγορίθμου είναι όμοια με πριν, οπότε παίρνουμε

$$\begin{array}{l|l} x^3y^2+x^2y^2+y^2 & \underline{x^2y-1} \\ \underline{-x^3y+xy} & xy+y \\ x^2y^2+xy+y^2 & \\ \underline{-x^2y^2+y} & \\ xy+y^2+y & \end{array}$$

Παρατηρούμε ότι κανένα από τα $\mathrm{LT}(f_1)=x^2y, \mathrm{LT}(f_2)=y^2$ δε διαιρεί το

$\mathrm{LT}(xy + y^2 + y) = xy$. Όμως δε μπορούμε να ισχυριστούμε ότι $r = x + y^2 + y$, αφού το $\mathrm{LT}(f_2)$ διαιρεί τον δεύτερο όρο του *r*, που είναι ο y^2 .

Έτσι, αν μετακινήσουμε το *xy* στο *r* μπορούμε να συνεχίσουμε τη διαίρεση. (Αυτό το πρόβλημα δε θα το συναντούσαμε ποτέ σε πολυώνυμα μιας μεταβλητής).

Για να εφαρμόσουμε την παραπάνω ιδέα , χρησιμοποιούμε μια στήλη *r* όπου θα τοποθετούμε τους όρους του *r.* Το πολυώνυμο που θα προκύπτει από την αφαίρεση, θα το αποκαλούμε *ενδιάμεσος διαιρέτης (intermediate dividend).* Έτσι συνεχίζουμε τη διαίρεση μέχρις ότου ο ενδιάμεσος διαιρέτης γίνει μηδέν. Δηλαδή έχουμε:

$$\begin{array}{r|l} x^3y^2 + x^2y^2 + y^2 & x^2y - 1 \\ \underline{-x^3y + xy} & \\ x^2y^2 + xy + y^2 & xy + y \\ \underline{-x^2y^2 + y} & \\ xy + y^2 + y & \\ \underline{y^2 + y} & \\ 0 & \end{array} \quad , \; r = xy \, .$$

Τώρα συνεχίζουμε τη διαδικασία. Εάν μπορούμε να διαιρέσουμε με κάποιον από τα $\mathrm{LT}(f_1), \mathrm{LT}(f_2)$ συνεχίζουμε κανονικά, αλλιώς μετακινούμε τον μεγιστοβάθμιο όρο του ενδιάμεσου διαιρέτη στην στήλη *r.* Άρα παίρνουμε:

$$\begin{array}{r|l} y^2 + y & y^2 - 1 \\ \underline{-y^2 + 1} & 1 \\ y + 1 & \end{array} \quad , r = xy + y + 1 \, .$$

Άρα τελικά το υπόλοιπο είναι το $xy + y + 1$ και άρα ισχύει

(2.3.1) $\qquad x^3y^2 + x^2y^2 + y^2 = (xy + y)(x^2y - 1) + 1(y^2 - 1) + xy + y + 1 \, .$

Παρατηρούμε ότι κανένα από τα $\mathrm{LT}(f_1), \mathrm{LT}(f_2)$ δε διαιρεί κάποιον όρο του *r*. $\quad \Delta$

<u>Θεώρημα 2.3.3</u> (Ο Αλγόριθμος της Διαίρεσης στο $K[x_1,...,x_n]$) [1]

Έστω η διάταξη μονωνύμων $>$ στο $Z_{\geq 0}^n$ και έστω $F=(f_1,...,f_s)$ μια διατεταγμένη s-άδα πολυωνύμων στο $K[x_1,...,x_n]$**.** Τότε, κάθε $f \in K[x_1,...,x_n]$ μπορεί να γραφεί ως

$$f = a_1 f_1 + ... + a_s f_s + r,$$

όπου $a_i, r \in K[x_1,...,x_n]$ και το r είναι είτε μηδέν, είτε γραμμικός συνδυασμός των μονωνύμων με συντελεστές από το K ,όπου κανένα από τα μονώνυμα δε διαιρείται με κάποιο από τα $\mathrm{LT}(f_1),...,\mathrm{LT}(f_s)$. Το r θα το αποκαλούμε **υπόλοιπο (remainder)** της διαίρεσης του f από τα F. Επιπλέον, εάν $a_i f_i \neq 0$, τότε ισχύει

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i f_i).$$

<u>Απόδειξη</u>

Θα δώσουμε μια γενίκευση του αλγορίθμου που είδαμε στην Πρόταση 1.5.2, για πολυώνυμα μιας μεταβλητής. Θα αποδείξουμε λοιπόν μέσα από την κατασκευή αυτού του αλγόριθμου, την ύπαρξη των $a_1,...,a_s,r$ τα οποία έχουν τις επιθυμητές ιδιότητες και λειτουργούν για οποιαδήποτε είσοδο δώσουμε στον αλγόριθμο.

Είσοδοι: $f_1,...,f_s,f$

Έξοδοι: $a_1,...,a_s,r$

$a_1 := 0;....;a_s := 0; r := 0$

$p := f$

ΟΣΟ $p \neq 0$ ΕΚΤΕΛΕΣΕ

$i := 1$

div:=ψευδής

ΟΣΟ($i \leq s$ ΚΑΙ div:=ψευδής) ΕΚΤΕΛΕΣΕ

ΑΝ ($\mathrm{LT}(f_i)$ διαιρεί το (p)) ΤΟΤΕ

$a_i := a_i + \mathrm{LT}(p) / \mathrm{LT}(f_i)$

$p := p - (\mathrm{LT}(p) / \mathrm{LT}(f_i)) f_i$

div:=αληθής

ΑΛΛΙΩΣ

$i := i + 1$

ΑΝ div=αληθής ΤΟΤΕ

$r := r + \mathrm{LT}(p)$

$p := p - \mathrm{LT}(p)$

Μπορούμε να συσχετίσουμε τον παραπάνω αλγόριθμοι με αυτόν που είδαμε στο προηγούμενο παράδειγμα. Το p αντιπροσωπεύει τον ενδιάμεσο διαιρέτη, το r τη στήλη όπου δεξιά μετακινούσαμε τους όρους και οι μεταβλητές $a_1, \ldots a_s$ είναι τα πηλίκα. Τέλος, η λογική μεταβλητή div μας δείχνει πότε κάποιο από τα $\mathrm{LT}(f_i)$ διαιρεί κάποιον όρο του ενδιάμεσου διαιρέτη. Παρατηρούμε ότι κάθε φορά που εκτελείται η εντολή ΟΣΟ...ΕΚΤΕΛΕΣΕ συμβαίνει κάποιο από τα εξής:

- (το βήμα της διαίρεσης) εάν κάποιο από τα $\mathrm{LT}(f_i)$, διαιρεί το $\mathrm{LT}(p)$, τότε ο αλγόριθμος συνεχίζει κανονικά, όπως στην περίπτωση της μιας μεταβλητής.
- (το βήμα του υπολοίπου) εάν κανένα από τα $\mathrm{LT}(f_i)$ δε διαιρεί το $\mathrm{LT}(p)$, τότε ο αλγόριθμος προσθέτει το $\mathrm{LT}(p)$ στο υπόλοιπο.

Αυτά ακριβώς τα βήματα ακολουθήσαμε και στο Παράδειγμα 2.3.2.

Για να δείξουμε ότι ο αλγόριθμος είναι σωστός, αρχικά θα δείξουμε ότι η

$$f = a_1 f_1 + \ldots + a_s f_s + p + r, \tag{2.3.2}$$

ισχύει σε κάθε στάδιο του αλγορίθμου. Αυτό είναι προφανές για τις αρχικές τιμές των $a_1, \ldots a_s, p, r$. Έστω λοιπόν ότι η (2.3.2) ισχύει σε κάθε βήμα του αλγορίθμου. Εάν το επόμενο βήμα είναι βήμα διαίρεσης, τότε η ισότητα

$$a_i f_i + p = (a_i + \mathrm{LT}(p) / \mathrm{LT}(f_i)) f_i + (p - \mathrm{LT}(p) / \mathrm{LT}(f_i)) f_i)$$

Σημαίνει ότι το $a_i f_i + p$ δεν αλλάζει. Εφόσον λοιπόν καμιά μεταβλητή δεν επηρεάζεται, η (2.3.2) παραμένει αληθής. Στην περίπτωση λοιπόν που το επόμενο βήμα είναι βήμα υπολοίπου, τότε παρόλο που αλλάζουν τα p, r , το άθροισμα $p + r$, παραμένει αμετάβλητο καθώς ισχύει η ισότητα

$$p + r = (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p))$$

Άρα και πάλι η ισότητα (2.3.2) παραμένει αληθής.
Δεδομένου ότι προσθέτουμε στο *r* εκείνους τους όρους που δε διαιρούνται από κανένα από τα $\mathrm{LT}(f_i)$, έπεται ότι όταν ο αλγόριθμος τερματίζει, τα $a_1, \ldots a_s, r$ έχουν τις επιθυμητές ιδιότητες.

Τέλος, απομένει να δείξουμε ότι ο αλγόριθμος όντως τερματίζει. Όσο ο αλγόριθμος εκτελείται, και το *p* παίρνει νέες τιμές, ο πολλαπλός βαθμός είτε μειώνεται (ανάλογα με ποια διάταξη δουλεύουμε),είτε μηδενίζει. Για να το επιβεβαιώσουμε αυτό, υποθέτουμε ότι κατά τη διάρκεια του βήματος της διαίρεσης, το *p* παίρνει τη νέα τιμή

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i .$$

Από το Λήμμα 2.2.7, έχουμε

$$\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i \right) = \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \mathrm{LT}(f_i) = \mathrm{LT}(p)$$

που σημαίνει ότι τα p, $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$, έχουν τον ίδιο κύριο όρο. Ως εκ τούτου, η διάφορά τους, p' πρέπει να έχει αυστηρά μικρότερο πολλαπλό βαθμό όταν $p' \neq 0$. Έστω τώρα ότι εκτελείται το βήμα του υπολοίπου. Σε αυτήν την περίπτωση το *p* παίρνει τη νέα τιμή

$$p' = p - \mathrm{LT}(p)$$

Είναι προφανές ότι ισχύει ότι $\mathrm{multideg}(p') < \mathrm{multideg}(p)$ όταν $p' \neq 0$. Άρα σε κάθε περίπτωση, ο πολλαπλός βαθμός μειώνεται. Εάν ο αλγόριθμος δεν τερμάτιζε ποτέ, τότε θα είχαμε μια άπειρη, φθίνουσα ακολουθία των πολλαπλών βαθμών. Η καλά διατεταγμένη ιδιότητα > όπως είδαμε στο Λήμμα 2.2.7, δείχνει ότι αυτό είναι άτοπο. Άρα τελικά πρέπει να ισχύει ότι $p = 0$, ώστε ο αλγόριθμος να τερματίζει έπειτα από πεπερασμένα βήματα.

Απομένει να μελετήσουμε τη σχέση μεταξύ των $\mathrm{multideg}(f), \mathrm{multideg}(a_i, f_i)$. Κάθε όρος στο a_i είναι της μορφής $\mathrm{LT}(p)/\mathrm{LT}(f_i)$, για κάποια τιμή της μεταβλητής *p*. Ο αλγόριθμος ξεκινάει θέτωντας $p = f$ και έτσι δείξαμε ότι ο πολλαπλός βαθμός του *p* μειώνεται. Από αυτό συνεπάγεται ότι $\mathrm{LT}(p) < \mathrm{LT}(f)$ και συνεπώς, χρησιμοποιώντας τη συνθήκη (ii) του ορισμού της διάταξης μονωνύμων, έπεται ότι $\mathrm{multideg}(f) > \mathrm{multideg}(a_i, f_i)$, όταν $a_i f_i \neq 0$, και έτσι ολοκληρώνεται η απόδειξη του θεωρήματος. △

<u>Παράδειγμα 2.3.4</u>

Έστω ότι θέλουμε να διαιρέσουμε το $f = x^3y^2 + x^2y^2 + y^2$ με τα $f_1 = y^2 - 1, f_2 = x^2y - 1$. Θα χρησιμοποιήσουμε τη λεξικογραφική διάταξη $x > y$. Παρατηρούμε ότι είναι το ίδιο παράδειγμα με το Παράδειγμα 2.3.2, με διαφορά ότι αλλάζουμε τη σειρά των διαιρετών. Εκτελώντας τη διαίρεση παίρνουμε:

$$
\begin{array}{r|l}
x^3y^2 + x^2y^2 + y^2 & y^2 - 1 \\
\cline{2-2}
-x^3y^2 + x^3 & \\
\cline{1-1}
x^3 + x^2y^2 + y^2 & r = x^3 \\
x^2y^2 + y^2 & \\
-x^2y^2 + x^2 & \\
\cline{1-1}
x^2 + y^2 & r = x^3 + x^2 \\
y^2 & \\
-y^2 + 1 & \\
\cline{1-1}
1 &
\end{array}
$$

Άρα ισχύει η :

$$(2.3.3) \qquad x^3y^2 + x^2y^2 + y^2 = (x^3 + x^2 + 1)\cdot(y^2 - 1) + 0\cdot(xy - 1) + x^3 + x^2 + 1 .$$

Η παραπάνω σχέση μας δίνει διαφορετικό υπόλοιπο από τη σχέση (2.3.1). Αυτό σημαίνει ότι το *r* δεν είναι μοναδικά ορισμένο.

Για τα πολυώνυμα μιας μεταβλητής λοιπόν, ο αλγόριθμος της διαίρεσης δίνει μια άμεση λύση στο πρόβλημα συμμετοχής των ιδεωδών. Όμως, για πολυώνυμα πολλών μεταβλητών, από το Θεώρημα 2.3.3 πρόκυπτει η εξής παρατήρηση:

Εάν διαιρώντας το f με τα $F = (f_1, ..., f_s)$ καταλήγουμε ότι $r = 0$, τότε

$$f = a_1 f_1 + ... + a_s f_s$$

που σημαίνει ότι $f \in \langle f_1, ..., f_s \rangle$. Άρα το $r = 0$, είναι μια ικανή συνθήκη για το πρόβλημα συμμετοχής των ιδεωδών. Ωστόσο, αυτή η συνθήκη δεν είναι και αναγκαία, όπως διαπιστώνεται και από το επόμενο παράδειγμα.

Παράδειγμα 2.3.5

Έστω $f = x^3y^2 + x^2y - xy - y$ και θέλουμε να τη διαιρέσουμε με τα $F = (f_1, f_2)$, όπου $f_1 = xy + y,\ f_2 = x^2 + 1$. Εκτελώντας τη διαίρεση παίρνουμε

$$x^3y^2 + x^2y - xy - y = (x^2 - 1)(xy + y) + 0 \cdot (x^2 + 1) + 0 .$$

Διαιρώντας τώρα το f με τα $F = (f_2, f_1)$, παίρνουμε

$$x^3y^2 + x^2y - xy - y = (y - 1)(xy + y) + (xy^2 + y) \cdot (x^2 + 1) - y^2 - y .$$

Αν και από την πρώτη σχέση συνεπάγεται ότι $f \in \langle f_1, f_2 \rangle$, η δεύτερη σχέση δηλώνει ότι είναι πιθανόν το υπόλοιπο που θα λάβουμε να μην είναι μηδεν. ▵

Ο αλγόριθμος της διαίρεσης του Θεωρήματος 2.3.3, είναι μια γενίκευση αυτού της μιας μεταβλητής, αν και όχι τόσο αποδοτικός.

§2.4 ΙΔΕΩΔΗ ΜΟΝΩΝΥΜΩΝ ΚΑΙ ΤΟ ΛΗΜΜΑ ΤΟΥ DICKSON

Σε αυτήν την ενότητα εισάγεται η έννοια των ιδεωδών μονωνύμων. Διασαφηνίζεται λοιπόν, πώς χρησιμοποιούνται αυτά τα σύνολα και οι ιδιότητες τους στο πρόβλημα περιγραφής των μονωνύμων.

Ορισμός 2.4.1 [1]

Ένα ιδεώδες $I \subset K[x_1,...,x_n]$ θα είναι **ιδεώδες μονωνύμων** εάν υπάρχει ένα υποσύνολο $A \subset Z_{\geq 0}^n$, τέτοιο ώστε το I να αποτελείται από όλα τα πολυώνυμα που είναι πεπερασμένα αθροίσματα της μορφής $\sum_{\alpha \in A} h_\alpha x^\alpha$, όπου $h_\alpha \in K[x_1,...,x_n]$. Σε αυτήν την περίπτωση θα γράφουμε $I = \langle x^\alpha : \alpha \in A \rangle$.

Λήμμα 2.4.2 [1]

Έστω $I = \langle x^\alpha : \alpha \in A \rangle$ ένα ιδεώδες μονωνύμων. Τότε, ένα μονώνυμο της μορφής x^β, θα ανήκει στο I αν και μόνο αν το x^β διαιρείται από το x^α, για κάποιο $\alpha \in A$.

Απόδειξη

Εάν το x^β είναι πολλαπλάσιο του x^α, για κάποιο $\alpha \in A$, τότε $x^\beta \in I$, από τον ορισμό του ιδεωδούς. Αντίστροφα, αν $x^\beta \in I$, τότε $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, όπου $h_i \in K[x_1,...,x_n]$ και $\alpha(i) \in A$. Εάν αναλύσουμε το h_i ως γραμμικό συνδυασμό μονωνύμων, παρατηρούμε ότι κάθε όρος από το δεξί μέλος της παραπάνω εξίσωσης διαιρείται από κάποιο $x^{\alpha(i)}$. Επομένως, και το αριστερό μέλος x^β, πρέπει να έχει την ίδια ιδιότητα. Δ

Λήμμα 2.4.3 [1]

Έστω *I* ένα ιδεώδες μονωνύμων, και έστω $f \in K[x_1,...,x_n]$. Τότε οι παρακάτω προτάσεις είναι ισοδύναμες:

i. $f \in I$

ii. Κάθε όρος του *f* ανήκει στο *I*.

iii. Το *f* είναι γραμμικός συνδυασμός των μονωνύμων του *I*.

Πόρισμα 2.4.4 [1]

Δύο ιδεώδη μονωνύμων είναι όμοια αν και μόνο αν περιέχουν τα ίδια μονώνυμα.

Θεώρημα 2.4.5 (Το λήμμα του Dickson) [1]

Έστω $I = \left\langle x^\alpha : \alpha \in A \right\rangle \subseteq K[x_1,...,x_n]$ ένα ιδεώδες μονωνύμων. Τότε το *I* μπορεί να γραφεί στη μορφή $I = \left\langle x^{\alpha(1)},...,x^{\alpha(s)} \right\rangle$, όπου $\alpha(1),...,\alpha(s) \in A$. Συγκεκριμένα, το *I* έχει μια πεπερασμένη βάση.

Απόδειξη

Το θεώρημα αποδεικνύεται επαγωγικά για τις τιμές *n* που συμβολίζουν το πλήθος των μεταβλητών. Για *n*=1, το *I* παράγεται από τα μονώνυμα x_1^α, όπου $\alpha \in A \subset \mathrm{Z}_{\geq 0}$. Έστω $\beta \leq \alpha$, το μικρότερο στοιχείο του $A \subset \mathrm{Z}_{\geq 0}$. Τότε $\beta \leq \alpha$, για κάθε $\alpha \in A$, και άρα το x_1^β διαιρεί όλους τους γεννήτορες x_1^α. Επομένως, εύκολα συμπεραίνουμε ότι $I = \langle x_1^\beta \rangle$.

Για την περίπτωση όπου *n*>1 και έστω ότι το θεώρημα ισχύει για *n*-1. Θα συμβολίζουμε τις μεταβλητές με $x_1,...,x_{n-1},y$, έτσι ώστε τα μονώνυμα του $K[x_1,...,x_{n-1},y]$ να είναι της μορφής $x^\alpha y^m$, όπου $\alpha = (\alpha_1,...,\alpha_{n-1}) \in \mathrm{Z}_{\geq 0}^{n-1}, \quad m \in \mathrm{Z}_{\geq 0}$.

Υποθέτουμε ότι το $I \subset K[x_1,...,x_{n-1},y]$ είναι ένα ιδεώδες μονωνύμων. Για να βρούμε τους γεννήτορες για το *I,* θεωρούμε *J* το ιδεώδες του $K[x_1,...,x_{n-1}]$ που παράγεται από τα μονώνυμα x^α, για τα οποία ισχύει $x^\alpha y^m \in I$ για κάποιο $m \geq 0$. Δεδομένου ότι το *J* είναι ιδεώδες μονωνύμων στο $K[x_1,...,x_{n-1}]$, από την επαγωγική μας υπόθεση συνεπάγεται ότι πεπερασμένο πλήθος από τα x^α παράγουν το *J*, δηλαδή $J = \left\langle x^{\alpha(1)},...,x^{\alpha(s)} \right\rangle$. Γενικά, το

ιδεώδες J μπορεί να θεωρηθεί ως η προβολή του I στο $K[x_1,...,x_{n-1}]$.

Για κάθε $1 \le i \le s$, από τον ορισμό του J έχουμε $x^{a(i)}y^{m_i} \in I$ για κάποια $m_i \ge 0$. Έστω m το μεγαλύτερο από αυτά τα m_i. Τότε για κάθε $0 \le k \le m-1$, θεωρούμε το ιδεώδες $J_k \subset K[x_1,...,x_{n-1}]$ που παράγεται από τα μονώνυμα x^β, έτσι ώστε να ισχύει $x^\beta y^k \in I$. Το J_k μπορεί να θεωρηθεί ως ένα κομμάτι του I που παράγεται από τα μονώνυμα που περιέχουν το y^k. Χρησιμοποιώντας και πάλι την επαγωγική υπόθεση, το J_k έχει ένα πεπερασμένο παραγόμενο σύνολο μονωνύμων, δηλαδή $J_k = \langle x^{\alpha_k(1)},...,x^{\alpha_k(s)} \rangle$.

Έστω ότι το I παράγεται από τα παρακάτω μονώνυμα:

$$\begin{aligned} & J : x^{a(1)}y^m,...,x^{a(s)}y^m \\ & J_0 : x^{a_0(1)},...,x^{a_0(s_0)} \\ \text{Από τα:} \quad & J_1 : x^{a_1(1)}y,...,x^{a_1(s_1)}y \\ & \quad \vdots \\ & J_{m-1} : x^{a_{m-1}(1)}y^{m-1},...,x^{a_{m-1}(s_{m-1})}y^{m-1} \end{aligned}$$

Αρχικά, παρατηρούμε ότι κάθε μονώνυμο του I διαιρείται από κάποιο από τα παραπάνω μονώνυμα. Αυτό θα το διαπιστώσουμε θεωρώντας ότι $x^\alpha y^p \in I$. Εάν $p \ge m$, τότε από την κατασκευή του J συμπεραίνουμε ότι το $x^\alpha y^p$ διαιρείται από κάποιο από τα $x^{\alpha(i)}y^m$. Αντιθέτως, εάν $p \le m-1$, από την κατασκευή του J_p, συμπεραίνουμε ότι το $x^\alpha y^p$ διαιρείται από κάποιο από τα $x^{\alpha_p(i)}y^p$. Έπεται λοιπόν από το Λήμμα 2.4.2, ότι τα παραπάνω μονώνυμα παράγουν ένα ιδεώδες που περιέχει τα ίδια μονώνυμα με το *I*. Από το Πόρισμα 2.4.4, συνεπάγεται ότι τα δύο ιδεώδη είναι τα ίδια και έτσι αποδείχτηκε ο ισχυρισμός μας.

Για να τελειώσουμε την απόδειξη, απομένει να δείξουμε ότι το πεπερασμένο σύνολο των γεννητόρων μπορούμε να το επιλέξουμε από το σύνολο των γεννητόρων του ιδεώδους. Γράφοντας και πάλι τις μεταβλητές ως $x_1,...,x_n$, τότε το ιδεώδες μονωνύμων είναι το $I = \langle x^\alpha : \alpha \in A \rangle \subset K[x_1,...,x_n]$. Αρκεί να δείξουμε λοιπόν ότι το I παράγεται από πεπερασμένο

πλήθος των $x^{\alpha}, \alpha \in A$. Είδαμε παραπάνω ότι $I=\left\langle x^{\beta(1)},...,x^{\beta(s)}\right\rangle$, όπου τα $x^{\beta(i)}$ είναι μονώνυμα του *I*. Δεδομένου ότι $x^{\beta} \in I=\left\langle x^{\alpha} : \alpha \in A\right\rangle$, από το Λήμμα 4.2 έπεται ότι κάθε $x^{\beta(i)}$ διαιρείται από κάποιο $x^{\alpha(i)}, \alpha(i) \in A$.Από εδώ συμπεραίνουμε εύκολα ότι $I=\left\langle x^{\alpha(1)},...,x^{\alpha(s)}\right\rangle$.

△

Εφαρμογή [1]

Θεωρούμε το ιδεώδες $I=\left\langle x^4y^2, x^3y^4, x^2y^5\right\rangle$ που είδαμε και νωρίτερα. Από την εικόνα που σχηματίζουν οι εκθέτες, συνεπάγεται ότι η προβολή του *I* είναι το $J=\left\langle x^2\right\rangle \subset K[x]$. Εφόσον $x^2y^5 \in I$, έπεται ότι *m*=5. Έπειτα, παίρνουμε τα κομμάτια J_k, $0 \le k \le m-1$, τα οποία παράγονται από τα μονώνυμα που περιέχουν τα y^k:

$$J_0 = J_1 = \{0\}$$
$$J_2 = J_3 = \left\langle x^4\right\rangle$$
$$J_4 = \left\langle x^3\right\rangle$$

Σύμφωνα με την απόδειξη του παραπάνω θεωρήματος, από τα παραπάνω κομμάτια προκύπτει το ιδεώδες $I=\left\langle x^2y^5, x^4y^2, x^4y^3, x^3y^4\right\rangle$. △

Το Θεώρημα 2.4.5 επιλύει το πρόβλημα περιγραφής των ιδεωδών στην περίπτωση που τα ιδεώδη είναι ιδεώδη μονωνύμων, καθώς το ιδεώδες που προκύπτει έχει μια πεπερασμένη βάση. Συνεπώς, μπορούμε να προχωρήσουμε και στην επίλυση του προβλήματος συμμετοχής των ιδεωδών για ιδεώδη μονωνύμων. Ειδικότερα, εάν $I=\left\langle x^{\alpha(1)},...,x^{\alpha(s)}\right\rangle$, τότε εύκολα μπορούμε να εξετάσουμε αν κάποιο *f* ανήκει στο *I,* ελέγχοντας το υπόλοιπο της διαίρεσης του *f* με τα $x^{\alpha(1)},...,x^{\alpha(s)}$. Γενικά, το θα *f* ανήκει στο *I,* αν το υπόλοιπο της διαίρεσης του *f* με τα $x^{\alpha(1)},...,x^{\alpha(s)}$ είναι μηδέν και αντίστροφα.

§2.5 ΤΟ ΘΕΩΡΗΜΑ HILBERT ΚΑΙ Η ΒΑΣΗ GROEBNER

Σε αυτήν την παράγραφο δίνεται μια πλήρης λύση του προβλήματος περιγραφής των ιδεωδών. Επίσης, θα εστιάσουμε στη βάση Groebner και την κατασκευή της, καθώς αύτή η βάση διευκολύνει τους υπολογισμούς στα προβλήματα που έχουν αναφερθεί. Για να τα δούμε όλα αυτά, αρχικά ορίζουμε το *ιδεώδες μεγιστοβάθμιων όρων (ideal of leading terms)* ως εξής:

Ορισμός 2.5.1 [1]

Έστω $I \subset K[x_1,...,x_n]$ με $I \neq \{0\}$ ένα ιδεώδες.

i. Συμβολίζουμε με $\mathrm{LT}(I)$ το σύνολο που αποτελείται από από τους μεγιστοβάθμιους όρους των στοιχείων του I. Δηλαδή

$$\mathrm{LT}(I) = \{cx^a : \ \upsilon\pi\acute{a}\rho\chi\varepsilon\iota \ f \in I \ \mu\varepsilon \ \mathrm{LT}(f) = cx^a\}$$

ii. Συμβολίζουμε με $\langle \mathrm{LT}(I) \rangle$ το ιδεώδες που παράγεται από τα στοιχεία του $\mathrm{LT}(I)$.

Επειδή στον Αλγόριθμο της Διαίρεσης οι μεγιστοβάθμιοι όροι παίζουν σπουδαίο ρόλο, γεννάται το ερώτημα εάν για κάποιο πεπερασμένο παραγόμενο σύνολο του I, (δηλαδή αν για το $I = \langle f_1,..., f_s \rangle$) τα $\langle \mathrm{LT}(f_1),..., \mathrm{LT}(f_s) \rangle$ και $\langle \mathrm{LT}(I) \rangle$ είναι το ίδιο σύνολο. Εξ ορισμού ισχύει ότι $\mathrm{LT}(f_i) \in \mathrm{LT}(I) \subset \langle \mathrm{LT}(I) \rangle$ που συνεπάγεται ότι $\langle \mathrm{LT}(f_1),..., \mathrm{LT}(f_s) \rangle \subset \langle \mathrm{LT}(I) \rangle$. Ωστόσο, το παρακάτω παράδειγμα δείχνει ότι το $\langle \mathrm{LT}(I) \rangle$ μπορεί να είναι αυστηρά μεγαλύτερο.

Παράδειγμα 2.5.2

Έστω $I = \langle f_1, f_2 \rangle$ όπου $f_1 = xy^2 - y + x^2$, $f_2 = x^2 y - x$ και χρησιμοποιώντας τη μέγιστη λεξικογραφική διάταξη στα μονώνυμα του $K[x, y]$, έχουμε:

$$x \cdot (xy^2 + x^2 - y) - y \cdot (x^2 y - x) = x^3$$

Αφού $x^3 \in I$, άρα $x^3 = \mathrm{LT}(x^3) \in \langle \mathrm{LT}(I) \rangle$. Ωστόσο, το x^3 δε διαιρείται ούτε από το $\mathrm{LT}(f_1) = xy^2$, ούτε από το $\mathrm{LT}(f_2) = x^2 y$ και τελικά, σύμφωνα με το Λήμμα 2.4.2 $x^3 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. ▵

Πρόταση 2.5.3 [1]

Έστω $I \subset K[x_1, ..., x_n]$ ένα ιδεώδες. Τότε:

i. Το $\langle \mathrm{LT}(I) \rangle$ είναι ιδεώδες μονωνύμων.

ii. Υπάρχουν $g_1, ..., g_t \in I$ τέτοια ώστε $\langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

Απόδειξη

Για την απόδειξη του (i), παρατηρούμε ότι το κύριο μονώνυμο $\mathrm{LM}(g)$ των στοιχείων $g \in I - \{0\}$, παράγουν το ιδεώδες μονωνύμων $\langle \mathrm{LM}(g) : g \in I - \{0\} \rangle$. Εφόσον τα $\mathrm{LM}(g)$ και $\mathrm{LT}(g)$ διαφέρουν κατά μια μη μηδενική σταθερά, τότε ισχύει $\langle \mathrm{LM}(g) : g \in I - \{0\} \rangle = \langle \mathrm{LT}(I) \rangle$. Άρα το $\langle \mathrm{LT}(I) \rangle$ είναι ιδεώδες μονωνύμων.

Για την απόδειξη του (ii), δεδομένου ότι το $\langle \mathrm{LT}(I) \rangle$ παράγεται από τα μονώνυμα $\mathrm{LM}(g)$, όπου $g \in I - \{0\}$. Από το λήμμα του Dickson παίρνουμε ότι $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LM}(g_1), ..., \mathrm{LM}(g_t) \rangle$ για πεπερασμένου πλήθους $g_1, ..., g_t \in I$. Εφόσον τα $\mathrm{LM}(g_i)$ διαφέρουν από τα $\mathrm{LT}(g_i)$ κατά μια μη-μηδενική σταθερά, έπεται ότι $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$. ▵

Χρησιμοποιώντας την παραπάνω πρόταση και τον αλγόριθμο της διαίρεσης, θα αποδείξουμε ότι υπάρχει ένα πεπερασμένο σύνολο που παράγεται από κάθε πολυωνυμικό ιδεώδες, πράγμα που επιβεβαιώνει ότι έχει επίλυση το πρόβλημα περιγραφής των ιδεωδών.

<u>Θεώρημα 2.5.4</u> (Το Θεώρημα Hilbert) [1]

Κάθε ιδεώδες $I \subset K[x_1,...,x_n]$ έχει ένα πεπερασμένο παραγόμενο σύνολο.

Δηλαδή $I = \langle g_1,...,g_t \rangle$ για κάποια $g_1,...,g_t \in I$

<u>Απόδειξη</u>

Εάν $I = \{0\}$, τότε το παραγόμενο σύνολο είναι το $\{0\}$, το οποίο είναι πράγματι πεπερασμένο. Στην περίπτωση που το I περιέχει κάποια μη-μηδενικά πολυώνυμα, τότε το παραγόμενο σύνολο $g_1,...,g_t$ μπορεί να κατασκευαστεί ως εξής:

Από την Πρόταση 2.5.3, υπάρχουν $g_1,...,g_t \in I$, τέτοια ώστε $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1),...,\mathrm{LT}(g_t) \rangle$ και θέλουμε να δείξουμε ότι $I = \langle g_1,...,g_t \rangle$.

Είναι προφανές ότι $\langle g_1,...,g_t \rangle \subset I$ καθώς $g_i \in I$. Αντιθέτως, έστω το πολυώνυμο $f \in I$. Εφαρμόζουμε τον αλγόριθμο της διαίρεσης για να διαιρέσουμε το f με το $\langle g_1,...,g_t \rangle$ και παίρνουμε

$$f = a_1 g_1 + ... + a_t g_t + r \quad ,$$

όπου κανένας όρος του r δε διαιρείται με κάποιο από τα $\mathrm{LT}(g_1),...,\mathrm{LT}(g_t)$. Θέλουμε να δείξουμε ότι $r = 0$. Αρχικά παρατηρούμε ότι

$$r = f - a_1 g_1 + ... + a_t g_t \in I \, .$$

Εάν $r \neq 0$, τότε $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1),...,\mathrm{LT}(g_t) \rangle$ και από το Λήμμα 2.4.2, έπεται ότι ο $\mathrm{LT}(r)$ διαιρείται απο κάποιον από τα $\mathrm{LT}(g_i)$, πράγμα που είναι άτοπο, καθώς αντικρούει στον ορισμό του υπολοίπου. Άρα τελικά $r = 0$. Συνεπώς, $f = a_1 g_1 + ... + a_t g_t + 0 \in \langle g_1,...,g_t \rangle$, από όπου προκύπτει $I \subset \langle g_1,...,g_t \rangle$.

Δ

Ορισμός 2.5.5 [1]

Έστω μια συγκεκριμένη διάταξη μονωνύμων. Ένα πεπερασμένο υποσύνολο $G = \{g_1, ..., g_t\}$ ενός ιδεωδούς I θα ονομάζεται **Groebner βάση** ή **standard basis** εάν

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle .$$

Ισοδύναμα, ένα σύνολο $\{g_1, ..., g_t\} \subset I$, το οποίο κατασκευάστηκε όπως στην απόδειξη του Θεωρήματος 2.5.4, είναι Groebner βάση, αν και μόνο αν ο μεγιστοβάθμιος όρος κάθε στοιχείου του I, διαιρείται από κάποιον από τους $\mathrm{LT}(g_i)$.

Επίσης, από την απόδειξη του Θεωρήματος 2.5.4 προκύπτει και το παρακάτω πόρισμα.

Πόρισμα 2.5.6 [1]

Έστω κάποια συγκεκριμένη διάταξη μονωνύμων. Τότε, κάθε ιδεώδες $I \subset K[x_1, ..., x_n]$, με $I \neq \{0\}$ έχει μια Groebner βάση. Επιπλέον, κάθε Groebner βάση, είναι και βάση του ιδεωδούς I.

Η βάση Groebner για τη λεξικογραφική διάταξη, καθορίζεται από αυτήν την κλιμακωτή μορφή του πίνακα που σχηματίζεται από τους συντελεστές των γεννήτορων.

Μια εφαρμογή του θεωρήματος Hilbert αφορά την **Αύξουσα Αλυσίδα (ascending chain)** ιδεωδών, η οποία είναι η αύξουσα ακολουθία

$$I_1 \subset I_2 \subset ....$$

Θεώρημα 2.5.7 (Η συνθήκη της Αύξουσας Αλυσίδας-Ascending Chain Condition (ACC)) [1]Εστω

$$I_1 \subset I_2 \subset .... ,$$

μια αύξουσα αλυσίδα των ιδεωδών στο $K[x_1, ..., x_n]$. Τότε υπάρχει $N \geq 1$, τέτοιο ώστε

$$I_N = I_{N+1} = I_{N+2} = ...$$

Απόδειξη

Έστω η αύξουσα αλυσίδα $I_1 \subset I_2 \subset ....$ και θεωρούμε το σύνολο $I = \bigcup_{i=1}^{\infty} I_i$. Θα ξεκινήσουμε δείχνοντας ότι το *I* είναι ιδεώδες στο $K[x_1,...,x_n]$. Παρατηρούμε ότι $0 \in I_i$ για κάθε *i*. Επίσης, εάν $f, g \in I$, τότε εξορισμού, $f \in I_i$ και $g \in I_j$, για κάποια i, j . Όμως, εφόσον τα I_i σχηματίζουν μια αύξουσα αλυσίδα, μπορούμε αλλάζοντας την ονομασία να πάρουμε $i \le j$. Τότε και το *f* και το *g* ανήκουν στο I_j , το οποίο είναι ιδεώδες. Συνεπώς, $f + g \in I_j$ και άρα $f + g \in I$. Ομοίως, αν $f \in I$ και $r \in k[x_1,...,x_n]$, τότε $f \in I_i$ για κάποιο *i* και $r \cdot f \in I_i \subset I$. Επομένως, το *I* είναι ιδεώδες.

Από το θεώρημα Hilbert έπεται ότι το ιδεώδες *I*, έχει ένα πεπερασμένο παραγόμενο σύνολο $I = \langle f_1,..., f_s \rangle$.

Κάθε γεννήτορας όμως, περιέχεται σε κάποιο από τα I_j , δηλαδή ισχύει $f \in I_{ji}$, για κάποιο j_i, $i = 1, 2, ..., s$. Παίρνουμε ως *N* το μέγιστο από τα j_i . Τότε από τον ορισμό της αύξουσας αλυσίδας $f_i \in I_N$ για όλα τα *i*. Ως εκ τούτου,

$$I = \langle f_1,..., f_s \rangle \subset I_N \subset I_{N+1} \subset ... \subset I$$

και τελικά, η αύξουσα αλυσίδα σταθεροποιείται στο I_N , ενώ όλα τα επόμενα ιδεώδη είναι ισοδύναμα. ∆

Την ιδιότητα που έχουν οι αύξουσες αλυσίδες των ιδεωδών του $K[x_1,...,x_n]$ να σταθεροποιούνται, την αποκαλούμε **Συνθήκη της Αύξουσας Αλυσίδας (ascending chain condition-ACC)** και είναι ισοδύναμη με το συμπέρασμα του Θεωρήματος Hilbert.

Ορισμός 2.5.8 [1]

Έστω $I \subset K[x_1,...,x_n]$ ένα ιδεώδες. Θα συμβολίζουμε με $\mathrm{V}(I)$ το σύνολο

$$\mathrm{V}(I) = \left\{(a_1,...,a_n) \in K^n : f_i(a_1,...,a_n) = 0 \ \textit{για κάθε} \ f \in I\right\}.$$

Ένα μη-μηδενικό ιδεώδες, πάντα περιέχει άπειρα διαφορετικά πολυώνυμα. Ωστόσο, το σύνολο $\mathrm{V}(I)$ μπορεί να οριστεί από ένα πεπερασμένο σύνολο πολυωνυμικών εξισώσεων.

Πρόταση 2.5.9 [1]

Το $\mathrm{V}(I)$ είναι μια αφινική πολλαπλότητα. Ειδικότερα, αν $I = \langle f_1, ..., f_s \rangle$, τότε

$$\mathrm{V}(I) = \mathrm{V}(f_1, ..., f_s) .$$

Απόδειξη

Από το θεώρημα Hilbert, $I = \langle f_1, ..., f_s \rangle$ για κάποιο πεπερασμένο παραγόμενο σύνολο. Αρχικά, εφόσον $f_i \in \mathrm{I}$, αν $f(a_1, ..., a_n) = 0$ για κάθε $f \in \mathrm{I}$, τότε $f_i(a_1, ..., a_n) = 0$ και έτσι $\mathrm{V}(I) \subset \mathrm{V}(f_1, ..., f_s)$. Αντίστροφα, έστω $(a_1, ..., a_n) \in \mathrm{V}(f_1, ..., f_s)$ και έστω $f \in \mathrm{I}$. Δεδομένου ότι $I = \langle f_1, ..., f_s \rangle$, ισχύει

$$f = \sum_{i=1}^{s} h_i f_i ,$$

για κάποιο $h_i \in K[x_1, ..., x_n]$. Όμως τότε,

$$f(a_1, ..., a_n) = \sum_{i=1}^{s} h_i(a_1, ..., a_n) f_i(a_1, ..., a_n) = \sum_{i=1}^{s} h_i(a_1, ..., a_n) \cdot 0 = 0 .$$

Επομένως, $\mathrm{V}(f_1, ..., f_s) \subset \mathrm{V}(I)$. Άρα τελικά $\mathrm{V}(I) = \mathrm{V}(f_1, ..., f_s)$. ∎

Το σημαντικότερο αποτέλεσμα της παραπάνω πρότασης, είναι ότι οι πολλαπλότητες προσδιορίζονται από ιδεώδη. Στο Κεφάλαιο 1, δείξαμε ότι $\mathrm{V}(f_1, ..., f_s) = \mathrm{V}(g_1, ..., g_s)$, όταν $\langle f_1, ..., f_s \rangle = \langle g_1, ..., g_s \rangle$. Αυτό είναι άμεση συνέπεια αυτής της πρότασης.

§2.6 ΙΔΙΟΤΗΤΕΣ ΤΗΣ ΒΑΣΗΣ GROEBNER

Μέχρι στιγμής έχουμε δει πως κάθε μη-μηδενικό ιδεώδες I έχει μια βάση Groebner. Σε αυτήν την παράγραφο, παραθέτονται οι ιδιότητες μιας τέτοιας βάσης, αλλά και ο τρόπος για να ελέγχουμε εάν μια βάση είναι βάση Groebner. Όταν διαιρεθεί ένα πολυωνύμο με μια βάση Groebner, τότε το υπόλοιπο της διαίρεσης είναι μηδενικό. Επομένως, η ανεπιθύμητη συμπεριφορά του αλγορίθμου της διαίρεσης στο $K[x_1,...,x_n]$ εξαλείφεται κάνοντας χρήση αυτής της βάσης.

Πρόταση 2.6.1 [1]

Έστω $G=\{g_1,...,g_s\}$ μια βάση Groebner για κάποιο ιδεώδες $I \subset K[x_1,...,x_n]$ και έστω $f \in K[x_1,...,x_n]$. Τότε, υπάρχει μοναδικό $r \in K[x_1,...,x_n]$, με τις παρακάτω ιδιότητες:

i. Κανένας όρος του r δε διαιρείται με κάποιο από τα $\mathrm{LT}(g_1),...,\mathrm{LT}(g_t)$.

ii. Υπάρχει $g \in I$, τέτοιο ώστε $f=g+r$

Συγκεκριμένα, το r είναι το υπόλοιπο της διαίρεσης του f με το G, ασχέτως με τη σειρά που έχουν ταξινομηθεί τα στοιχεία του G.

Απόδειξη

Από τον αλγόριθμο της διαίρεσης έχουμε $f=a_1g_1+\cdots+a_tg_t+r$, όπου το r πληρεί την (i). Θέτοντας $g=a_1g_1+\cdots+a_tg_t \in I$, ικανοποιείται και η συνθήκη (ii). Για να αποδείξουμε και τη μοναδικότητα, θεωρούμε $f=g+r=g'+r'$ τέτοια ώστε να ικανοποιούνται τα (i) και (ii). Τότε, $r-r'=g'-g \in I$, και αν $r \neq r'$, θα ισχύει $\mathrm{LT}(r-r') \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1),...,\mathrm{LT}(g_t) \rangle$. Από το Λήμμα 2.4.2, έπεται ότι το $\mathrm{LT}(r-r')$ διαιρείται από κάποιο από τα $\mathrm{LT}(g_i)$. Αυτό είναι άτοπο, καθώς κανένας όρος των r,r' δε διαιρείται από κάποιο από τα $\mathrm{LT}(g_1),...,\mathrm{LT}(g_t)$. Επομένως το $r-r'$ πρέπει να είναι μηδέν και συνεπώς αποδείχτηκε ότι $r=r'$. ∆

Το *r* θα το αποκαλούμε ***κανονική μορφή (normal form)*** *της f*. Στην πραγματικότητα, **η μοναδικότητα του υπολοίπου** χαρακτηρίζει μια βάση Groebner.

Παρόλο που το *r* είναι μοναδικό, οι συντελεστές a_i , όπου προκύπτουν από τον αλγόριθμο της διαίρεσης όταν το *f* παίρνει τη μορφή $f = a_1 g_1 + \cdots + a_t g_t + r$, μπορούν να αλλάξουν εάν αλλάξουμε τη σειρά των γεννητόρων.

Πόρισμα 2.6.2 [1]

Έστω $G = \{g_1, ..., g_s\}$ μια βάση Groebner για κάποιο ιδεώδες $I \subset K[x_1, ..., x_n]$ και έστω $f \in K[x_1, ..., x_n]$. Τότε $f \in I$ αν και μόνο αν κατά τη διαίρεση του *f* με το *G* το υπόλοιπο είναι μηδέν.

Απόδειξη

Αν *r*=0, τότε είναι προφανές ότι $f \in I$. Αντίστροφα, έστω ότι $f \in I$. Τότε γράφοντας $f = f + 0$, ικανοποιούνται και οι δύο συνθήκες της Πρότασης 2.6.1, από όπου έπεται ότι 0 είναι το υπόλοιπο του *f* με το *G*. ▵

Το παραπάνω πόρισμα, χρησιμοποιείται και ως ορισμός της Groebner, αφού ισχύει αν και μόνο αν $\langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

Χρησιμοποιώντας το, παίρνουμε έναν αλγόριθμο για τη λύση του προβλήματος συμμετοχής των ιδεωδών. Για να προσδιορίσουμε εάν $f \in I$, πρέπει μόνο με βάση το *G* να υπολογίσουμε το *r*.

Ορισμός 2.6 3 [1]

Θα συμβολίζουμε με $\overline{f}^F$ το υπόλοιπο της διαίρεσης του *f* με τη διατεταγμένη *s*-άδα $F = (f_1, ..., f_s)$. Αν η *F* είναι βάση Groebner για το $(f_1, ..., f_s)$, τότε μπορούμε να θεωρούμε το *F* ως ένα σύνολο, που δεν εξαρτάται από τη διάταξη που θα χρησιμοποιήσουμε.

Εφαρμογή

Έστω το μονώνυμο x^3y^2 και $F=(x^4y^2+x^2y^2-x^2y, x^5y-x^2)\subset K[x,y]$. Χρησιμοποιώντας τον αλγόριθμο της διαίρεσης και τη λεξικογραφική διάταξη παίρνουμε:

$$x^3y^2 = x\cdot(x^4y^2+x^2y^2-x^2y)-y\cdot(x^5y-x^2)+xy^2,$$

από όπου προκύπτει ότι $\overline{x^3y^2}^F = xy^2$. △

Ορισμός 2.6.4

Έστω $f,g\in K[x_1,...,x_n]$ δύο μη-μηδενικά πολυώνυμα.

i. Εάν $\text{multideg}(f)=\alpha$ και $\text{multideg}(g)=\beta$, τότε θεωρούμε $\gamma=(\gamma_1,...,\gamma_n)$, όπου $\gamma_i=\max(\alpha_i,\beta_i),\ \gamma\iota\alpha\ \kappa\acute{\alpha}\theta\varepsilon\ i$. Το x^γ αποτελεί **ελάχιστο κοινό πολλαπλάσιο-ΕΚΠ--(Least Common Multiple- LCM)** των $\text{LM}(f),\text{LM}(g)$ και θα γράφουμε $x^\gamma=\text{LCM}(\text{LM}(f),\text{LM}(g))$.

ii. Το **S-polynomial (S-πολυώνυμο)** των f,g είναι ο συνδυασμός

$$S(f,g)=\frac{x^\gamma}{\text{LT}(f)}\cdot f-\frac{x^\gamma}{\text{LT}(g)}\cdot g\,.$$

Ένα *S*-πολυώνυμο $S(f,g)$ σχεδιάζεται με σκοπό να παράγει ακύρωση των μεγιστοβάθμιων όρων. Στην πραγματικότητα, το επόμενο λήμμα δείχνει ότι κάθε ακύρωση των μεγιστοβάθμιων όρων μεταξύ των πολυωνύμων που έχουν το ίδιο πολλαπλό βαθμό, προκύπτει από μια τέτοια διαδικασία.

Λήμμα 2.6.5 [1]

Έστω ότι έχουμε το άθροισμα $\sum_{i=1}^{s} c_i f_i$, όπου $c_i \in K$ και $\text{multideg}(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$, για κάθε *i*. Εάν $\text{multideg}\left(\sum_{i=1}^{s} c_i f_i\right) \prec \delta$, τότε $\sum_{i=1}^{s} c_i f_i$ είναι γραμμικός συνδυασμός με συντελεστές από το *K*, των *s*-πολυωνύμων $S(f_j, f_k),\ για\ 1 \leq j,\ k \leq s$. Επιπλέον, κάθε $S(f_i, f_k)$ έχει multidegree<δ.

Απόδειξη

Έστω $d_i = \text{LC}(f_i)$ και $c_i d_i$ είναι ο κύριος συντελεστής του $c_i f_i$. Δεδομένου ότι όλα τα $c_i f_i$ έχουν πολλαπλό βαθμό δ και το άθροισμά τους έχει αυστηρά μικρότερο πολλαπλό βαθμό, έπεται ότι $\sum_{i=1}^{s} c_i d_i = 0$.

Ορίζουμε $p_i = f_i / d_i$ και παρατηρούμε ότι $\text{LC}(p_i) = 1$. Τώρα θεωρούμε το άθροισμα

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i =$$

$$c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s$$

Από υπόθεση, $\text{LT}(f_i) = d_i x^{\delta}$, από όπου συνεπάγεται ότι $\text{LCM}(\text{LM}(f_j), \text{LM}(f_k)) = x^{\delta}$. Άρα,

$$(2.6.1) \quad S(f_i, f_k) = \frac{x^{\delta}}{\text{LT}(f_j)} f_j - \frac{x^{\delta}}{\text{LT}(f_k)} f_k = \frac{x^{\delta}}{d_j x^{\delta}} f_j - \frac{x^{\delta}}{d_k x^{\delta}} f_k = p_j - p_k$$

Χρησιμοποιώντας αυτήν την εξίσωση και την $\sum_{i=1}^{s} c_i d_i = 0$ το πιο πάνω ανάπτυγμα γίνεται

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s)$$

Το οποίο έχει την επιθυμητή μορφή. Αφού τα p_j, p_k έχουν πολλαπλό βαθμό δ και κύριο συντελεστή 1, το $p_j - p_k$ έχει πολλαπλό βαθμό μικρότερο από δ . Από την (6.1) έπεται ότι ισχύει το ίδιο και για το $S(f_i, f_k)$ και έτσι αποδείχτηκε το λήμμα. $\triangle$

<u>Θεώρημα 2.6.6</u> (Το κριτήριο του Buchberger) [1]

Έστω *I* ένα ιδεώδες πολυώνυμων. Τότε, η $G = \{g_1, ..., g_t\}$ είναι βάση Groebner για το *I* αν και μόνο αν για όλα τα ζευγάρια $i \neq j$, το υπόλοιπο της διαίρεσης του $S(g_i, g_j)$ με το G είναι μηδέν.

<u>Απόδειξη</u>

$\Rightarrow$: αν G είναι βάση Groebner, τότε, από το Πόρισμα 2.6.2, το υπόλοιπο της διαίρεσης του $S(g_i, g_j)$ με τη G , είναι μηδέν, αφού ισχύει $S(g_i, g_j) \in I$.

$\Leftarrow$: έστω $f \in I$ ένα μη-μηδενικό πολυώνυμο. Θελουμε να δείξουμε ότι αν το υπόλοιπο της διαίρεσης των *s*-πολυωνύμων με τη *G* είναι μηδέν, τότε $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$. Αρχικά, ας δώσουμε ένα συνοπτικό διάγραμμα για το πώς θα κινηθούμε στην απόδειξη.

Για κάποιο πολυώνυμο $f \in I = (g_1, ..., g_t)$, υπάρχουν τα πολυώνυμα $h_i \in K[x_1, ..., x_n]$, τέτοια ώστε να ισχύει

$$\sum_{i=1}^{t} h_i g_i = 0 \qquad (2.6.2)$$

Από το Λήμμα 2.2.8 έπεται ότι

$$\mathrm{multideg}(f) \leq \max(\mathrm{multideg}(h_i g_i)). \qquad (2.6.3)$$

Εάν δεν ισχύει η ισότητα, τότε πρέπει κάποιοι μεγιστοβάθμιοι όροι της (2.6.2) να ακυρώνονται. Σύμφωνα με το Λήμμα 2.2.5, μπορούμε να προσαρμόσουμε αυτήν τη σχέση για *s*-πολυώνυμα. Τότε όμως, από την υπόθεση των *s*-πολυώνυμων ότι έχουν μηδενικό

υπόλοιπο, μπορούμε να αντικαταστήσουμε τα *s*-πολυώνυμα με εκφράσεις που περιλαμβάνουν μικρότερη ακύρωση. Έτσι, εκφάζουμε το f με μικρότερες ακυρώσεις των μεγιστοβάθμιων όρων. Συνεχίζοντας κατ'αυτόν τον τρόπο, τελικά βρίσκουμε μια έκφραση για το f όπου τελικά ισχύει η ισότητα στην (2.6.3). Άρα τότε θα έχουμε $\text{multideg}(f) \le \text{multideg}(h_i g_i)$ για κάποιο i, από όπου συμπαιρένουμε ότι το $\text{LT}(f)$ διαιρείται από το $\text{LT}(g_i)$. Αυτό σημαίνει ότι $\text{LT}(f) \in \langle \text{LT}(g_1), ..., \text{LT}(g_t) \rangle$ και τελικά αποδεικνύεται το θεώημα.

Ας δούμε τώρα και την απόδειξη αναλυτικά. Έστω ότι εκφράζουμε το f με τη (2.6.2) και $m(i) = \text{multideg}(h_i g_i)$. Επίσης, ορίζουμε $\delta = \max(m(1), ..., m(t))$. Τότε, η ανισότητα (2.6.3) γίνεται

$$\text{multideg}(f) \le \delta .$$

Τώρα, θεωρούμε όλες τις πιθανές μορφές που παίρνει το f σύμφωνα με την (2.6.2). Ενδεχομένως, για κάθε τέτοια έκφραση, παίρνουμε ένα διαφορετικό δ. Εφόσον η διάταξη μονωνύμων είναι καλά ορισμένη, μπορούμε να επιλέξουμε την έκφραση για το f που δίνει το ελάχιστο δ.

Εμείς θα δείξουμε ότι αν επιλεχθεί το ελάχιστο δ, τότε $\text{multideg}(f) = \delta$. Επομένως, ισχύει η ισότητα στην (2.6.3) και έπεται ότι $\text{LT}(f) \in \langle \text{LT}(g_1), ..., \text{LT}(g_t) \rangle$, που αποδεικνύει και το θεώρημα.

Αρκεί να δείξουμε λοιπόν ότι $\text{multideg}(f) = \delta$. Θεωρούμε λοιπόν ότι δεν ισχύει η ισότητα και άρα $\text{multideg}(f) < \delta$. Απομονώνουμε τους όρους με multidegree δ, γράφοντας το f στη μορφή

$$(2.6.4) \qquad \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} \text{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \text{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i .$$

Όλα τα μονώνυμα που εμφανίζονται στο δεύτερο και τρίτο άθροισμα, έχουν $\text{multideg}(f) < \delta$. Επομένως, από την υπόθεση ότι $\text{multideg}(f) < \delta$ έπεται ότι και το

πρώτο άθροισμα, έχει κι αυτό $\text{multideg}(f) < \delta$.

Έστω $\text{LT}(h_i) = c_i x^{\alpha(i)}$. Τότε, το άθροισμα $\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ έχει τη μορφή που περιγράψαμε στο Λήμμα 2.2.5 με $f_i = x^{\alpha(i)} g_i$. Άρα, από το Λήμμα 2.2.5 συνεπάγεται ότι αυτό το άθροισμα είναι ένας γραμμικός συνδυασμός των *s*-πολυωνύμων $S(x^{\alpha(i)} g_j, x^{\alpha(k)} g_k)$. Όμως,

$$S(x^{\alpha(i)} g_j, x^{\alpha(k)} g_k) = \frac{x^{\delta}}{x^{\alpha(j)} \text{LT}(g_j)} x^{\alpha(i)} g_j - \frac{x^{\delta}}{x^{\alpha(k)} \text{LT}(g_k)} = x^{\delta - \gamma_{jk}} S(g_j, g_k),$$

όπου $x^{\gamma_{jk}} = \text{LCM}(\text{LM}(g_j), \text{LM}(g_k))$. Συνεπώς, υπάρχουν σταθερές $c_{jk} \in k$, τέτοιες ώστε

$$\text{(2.6.5)} \qquad \sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_{j,k} c_j x^{\delta - \gamma_{jk}} S(g_j, g_k)$$

Το επόμενο βήμα είναι να χρησιμοποιήσουμε την υπόθεση ότι το υπόλοιπο της διαίρεσης του $S(g_j, g_k)$ με τα $g_1, ..., g_t$ είναι μηδέν. Αυτό σημαίνει ότι κάνοντας χρήση του αλγορίθμου της διαίρεσης μπορούμε κάθε *s*-πολυώνυμο μπορεί να γραφεί στη μορφή

$$\text{(2.6.6)} \qquad S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i,$$

όπου $a_{ijk} \in K[x_1, ..., x_n]$. Επίσης, από τον αλγόριθμο της διαίρεσης παίρνουμε

$$\text{(2.6.7)} \qquad \text{multideg}(a_{ijk} g_i) \leq \text{multi deg}(S(g_j, g_k)),$$

για κάθε i, j, k. Αυτό ουσιαστικά μας μας οδηγεί στην παραδοχή ότι όταν το υπόλοιπο είναι μηδέν, μπορούμε να εκφράσουμε το $S(g_j, g_k)$ συναρτήσει του G με τέτοιον τρόπο, ώστε να μην ακυρώνονται όλοι οι μεγιστοβάθμιοι όροι.

Για να κάνουμε την καλύτερη δυνατή χρήση αυτής της διαπίστωσης, πολλαπλασιάζουμε το $S(g_j, g_k)$ με $x^{\delta-\gamma_{ij}}$ και τότε παίρνουμε

$$x^{\delta-\gamma_{ij}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

όπου $b_{ijk} = x^{\delta-\gamma_{ij}} a_{ijk}$. Από την (2.6.7) και το Λήμμα 2.6.5 συνεπάγεται

(2.6.8) $$\text{multideg}(b_{ijk} g_i) \le \text{multideg}(x^{\delta-\gamma_{ij}} S(g_j, g_k)) < \delta.$$

Αντικαθιστώντας την $x^{\delta-\gamma_{ij}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i$, στην (2.6.5), παίρνουμε την εξίσωση

$$\sum_{m(i)} \text{LT}(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{ij}} S(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_{i=1}^{t} b_{ijk} g_i \right) = \sum_i \tilde{h}_i g_i .$$

Από την (2.6.8), ισχύει

$$\text{multideg}(\tilde{h}_i g_i) < \delta, \qquad \text{για κάθε } i.$$

Για να ολοκληρωθεί η απόδειξη, αντικαθιστούμε τη $\sum_{m(i)} \text{LT}(h_i) g_i = \sum_i \tilde{h}_i g_i$ στην (2.6.4). Με αυτόν τον τρόπο, εκφράζουμε το f ως γραμμικό συνδυασμό των g_i, όπου όλοι οι όροι έχουν $\text{multidegree} < \delta$. Αυτό είναι άτοπο όμως, γιατί αρχικά υποθέσαμε ότι το δ είναι το ελάχιστο. Δ

Εφαρμογή [1]

Έστω το ιδεώδες $I = \langle y - x^2, z - x^3 \rangle$ της στριμμένης κυβικής καμπύλης στον R^3. Θα δείξουμε ότι το σύνολο $G = \{y - x^2, z - x^3\}$, αποτελεί βάση Groebner με τη λεξικογραφική διάταξη $y > z > x$. Θεωρούμε λοιπόν το *S*-πολυώνυμο

$$S(y - x^2, z - x^3) = \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) = -zx^2 + yx^3 .$$

Χρησιμοποιώντας τον αλγόριθμο της διαίρεσης, παίρνουμε

$$-zx^2 + yx^3 = x^3 \cdot (y - x^2) + (-x^2) \cdot (z - x^3) + 0 .$$

Συνεπώς, $\overline{S(y-x^2, z-x^3)}^{G} = 0$. Άρα, από το Θεώρημα 2.6.6, η *G* είναι βάση Groebner για το *I*.

Ακολουθώντας την ίδια διαδικασία, μπορούμε να δείξουμε ότι η $G = \{y - x^2, z - x^3\}$, δεν αποτελεί βάση Groebner με τη λεξικογραφική διάταξη $x > y > z$. ▵

§2.7 Ο ΑΛΓΟΡΙΘΜΟΣ BUCHBERGER

Σε αυτήν την παράγραφο θα μελετήσουμε πώς να κατασκευάσουμε μια βάση Groebner για το ιδεώδες I του $K[x_1,...,x_n]$.

<u>Παράδειγμα 2.7.1</u> [3]

Έστω $K[x,y]$ και η λεξικογραφική διάταξη και έστω $I=\langle f_1,f_2\rangle=\langle x^2-2xy^2, xy-2y^3-1\rangle$.

Υπενθυμίζουμε ότι $\{f_1,f_2\}$ δεν είναι Groebner, αφού $\mathrm{LT}(S(f_1,f_2))=x\notin\langle \mathrm{LT}(f_1),\mathrm{LT}(f_2)\rangle$.

Για την κατασκευή μιας Groebner, η πρώτη ιδέα είναι να επεκτείνουμε το αρχικό παραγόμενο σύνολο σε μια Groebner, προσθέτοντας περισσότερα πολυώνυμα στο I. Η προσθήκη ή η αφαίρεση ενός περιττού στοιχείου δεν προκαλεί κάποια αλλαγή, στο ιδεώδες. Για να εντοπίσουμε ποιους γεννήτορες θα πρέπει να εισάγουμε, χρησιμοποιούμε τις πληροφορίες της §2.6 για τα S-πολυώνυμα και έχουμε:

$$S(f_1,f_2)=\frac{x^2y}{x^2}(x^2-2xy^2)-\frac{x^2y}{xy}(xy-2y^3-1)=x$$

και το υπόλοιπο της διαίρεσης με το $F=(f_1,f_2)$ είναι το $x\neq 0$, αφού $x=0\cdot f_1+0\cdot f_2+x$. Επομένως, θα πρέπει να συμπεριλάβουμε αυτό το υπόλοιπο στο παραγόμενο σύνολο, ως έναν νέο γεννήτορα $f_3=x$. Εάν ορίσουμε $F=(f_1,f_2,f_3)$, μπορούμε να χρησιμοποιήσουμε το Θεώρημα 2.6.6 για να ελέγξουμε εάν το νέο σύνολο είναι Groebner για το I. Έχουμε:

$$S(f_1,f_2)=f_3$$
$$S(f_2,f_3)=\frac{xy}{xy}(xy-2y^3-1)-\frac{xy}{x}x=-2y^3-1$$

Συνεπώς, πρέπει να προσθέσουμε το $f_4=-2y^3-1$ στο παραγόμενο σύνολο. Άρα $F=(f_1,f_2,f_3,f_4)$ και έτσι έχουμε:

$$S(f_1,f_3)=\frac{x^2}{x^2}(x^2-2xy^2)-\frac{x^2}{x}x=-2xy^2=-2y^2f_3$$

$$S(f_1,f_4)=\frac{x^2y^3}{x^2}(x^2-2xy^2)-\frac{x^2y^3}{-2y^3}(-2y^3-1)=-\frac{x^2}{2}-2xy^5=-\tfrac{1}{2}f_3+xy^2f_4$$

$$S(f_2,f_4)=\frac{xy^3}{xy}(xy-2y^3-1)-\frac{xy^3}{-2y^3}(-2y^3-1)=-\tfrac{1}{2}x+y^2(-2y^3-1)=\tfrac{1}{2}f_1+xy^2f_4$$

$$S(f_3,f_4)=\frac{xy^3}{x}x-\frac{xy^3}{-2y^3}(-2y^3-1)=-\frac{x}{2}=-\tfrac{1}{2}f_3$$

Άρα $\overline{S(f_i,f_j)}^F=0,\ \gamma\iota\alpha\ \kappa\acute{\alpha}\theta\varepsilon\ 1\le i\le j\le 4.$

από όπου έπεται ότι το $F=\{f_1,f_2,f_3,f_4\}$ αποτελεί βάση Groebner για το I η οποία δίνεται από το

$$\{f_1,f_2,f_3,f_4\}=\left\{x^2+2xy^2,xy+2y^3-1,\ x\ ,2y^3-1\right\}.\qquad\qquad\Delta$$

Από το παραπάνω παράδειγμα, γίνεται μετατροπή μιας βάσης F σε βάση Groebner, επεκτείνοντάς την, προσθέτοντας διαδοχικά μη-μηδενικά υπόλοιπα $\overline{S(f_i,f_j)}^F$. Αυτή η ιδέα είναι άμεση συνέπεια του κριτηρίου *s*-ζευγαριών και βασισμένοι σε αυτό προκύπτει ο αλγόριθμος Buchberger για τον υπολογισμό μιας βάσης Groebner.

<u>Θεώρημα 2.7.2</u> (Ο Αλγόριθμος Buchberger) [1]

Έστω $I=\langle f_1,...,f_s\rangle\neq\{0\}$ ένα πολυωνυμικό ιδεώδες. Μια βάση Groebner μπορεί να κατασκευαστεί για το *I,* σε πεπερασμένο αριθμό βημάτων, ως εξής:

Είσοδοι: $F = (f_1, ..., f_s)$

Έξοδοι: η βάση Groebner $G = (g_1, ..., g_t)$, με $F \subset G$

$G := F$

ΕΠΑΝΕΛΑΒΕ

$G' := G$

ΓΙΑ κάθε ζευγάρι $\{p, q\}$, $p \neq q$ στο G' ΕΚΤΕΛΕΣΕ

$S := \overline{S(p,q)}^{G'}$

ΑΝ $S \neq 0$ ΤΟΤΕ $G := G \cup \{S\}$

ΜΕΧΡΙ $G = G'$

<u>Απόδειξη</u>

Σε προηγούμενη ενότητα είδαμε πως για μια δοθείσα βάση $G = \{g_1, ..., g_t\}$, τα παραγόμενα σύνολα

$$\langle G \rangle = \langle g_1, ..., g_t \rangle$$
$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_t) \rangle$$

αποτελούν ιδεώδη.

Αρχικά θα δείξουμε ότι η υπόθεση $G \subset I$ παραμένει αληθής καθόλη τη διάρκεια εκτέλεσης του αλγορίθμου. Δεδομένου ότι ισχύει κατά την εκκίνηση του αλγορίθμου και στη συνέχεια επεκτείνουμε το G προσθέτοντας το υπόλοιπο $S = \overline{S(p,q)}^{G'}$ για κάθε $p, q \in G$. Άρα, εάν $G \subset I$, τότε τα p, q και συνεπώς και το $S(p,q)$ ανήκουν στο I. Εφόσον λοιπόν διαιρούμε με το $G' \subset I$, συνεπάγεται ότι $G \cup \{S\} \subset I$. Επίσης, παρατηρούμε ότι το σύνολο G περιέχει τη βάση F του I και άρα τελικά το G είναι πράγματι βάση του I.

Ο αλγόριθμος τερματίζει όταν $G = G'$, πράγμα που σημαίνει ότι $S = \overline{S(p,q)}^{G'} = 0$, για κάθε $p, q \in G$. Ως εκ τούτου, (από το Θεώρημα 6) η G αποτελεί βάση Groebner του $\langle G \rangle = I$.

Τώρα απομένει να δείξουμε ότι ο αλγόριθμος τερματίζει. Ας ελέγξουμε τι συμβαίνει κάθε φορά που εκτελείται ο κύριος βρόχος. Το σύνολο G αποτελείται από ένα σύνολο

G' , (που είναι το παλιό G), καθώς επίσης και από τα μη-μηδενικά υπόλοιπα των S-πολυωνύμων των στοιχείων του G'. Τότε, αφού ισχύει η $G' \subset G$, θα ισχύει και η

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(G') \rangle . \qquad (2.7.1)$$

Επιπλέον, αν $G' \neq G$, θα δείξουμε ότι το $\langle \mathrm{LT}(G') \rangle$ είναι αυστηρά μικρότερο από το $\langle \mathrm{LT}(G) \rangle$. Θεωρούμε λοιπόν, ότι κάποιο μη-μηδενικό υπόλοιπο r ενός S-πολυωνύμου, έχει προστεθεί στο G. Εφόσον το r είναι το υπόλοιπο της διαίρεσης με το G', τότε το $\mathrm{LT}(r)$ δε διαιρείται από τους μεγιστοβάθμιους όρους των στοιχείων του G' και συνεπώς, $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$. Έπεται λοιπόν ότι $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$.

Από την (2.7.1), τα ιδεώδη $\langle \mathrm{LT}(G') \rangle$, έπειτα από διαδοχικές επαναλήψεις, σχηματίζουν μια αύξουσα αλυσίδα των ιδεωδών του $K[x_1, ..., x_n]$. Επομένως, από τη συνθήκη αύξουσας αλυσίδας συνεπάγεται ότι μετά από πεπερασμένα βήματα η αλυσίδα σταθεροποιείται και έτσι προκύπτει $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(G') \rangle$. Αυτό, σύμφωνα με την προηγούμενη παράγραφο, σημαίνει ότι $G' = G$ και άρα τελικά ο αλγόριθμος τερματίζει. $\triangle$

Ο παραπάνω αλγόριθμος είναι μια απλή εκδοχή για να μας διασαφηνίσει πώς κατασκευάζεται μια βάση Groebner. Ωστόσο, δεν είναι πολύ αποδοτικός και επιδέχεται βελτιώσεις. Σαν μια πρώτη βελτίωση, παρατηρούμε ότι ότι εάν κάποιο υπόλοιπο $\overline{S(p,q)}^{G'} = 0$, αυτό το υπόλοιπο θα παραμένει μηδέν, ακόμη και αν προσθέσουμε επιπλέον στοιχεία στο G' . Άρα, μπορούμε να παραλείπουμε τα υπόλοιπα αυτά στις επόμενες επαναλήψεις του κεντρικού βρόχου. Πράγματι, εάν προσθέσουμε τους γεννήτορες f_j , τα μόνα υπόλοιπα που θα πρέπει να ελέγξουμε είναι τα $\overline{S(f_i, f_j)}^{G'}$, $i \leq j-1$. Χρησιμοποιώντας τον αλγόριθμο Buchberger, η βάση Groebner που βρίσκουμε, περιέχει συχνά επιπλέον στοιχεία από αυτά που μας είναι πραγματικά απαραίτητα. Για την εξάλειψη των περιττών γεννητόρων, χρησιμοποιούμε το επόμενο λήμμα.

Λήμμα 2.7.3 [1]

Έστω G μια βάση Groebner. Έστω $p \in G$ ένα πολυώνυμο τέτοιο ώστε $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. Τότε το $G - \{p\}$ είναι κι αυτό βάση Groebner.

Απόδειξη

Γνωρίζουμε ότι $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. Εάν $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$, τότε θα ισχύει $\langle \mathrm{LT}(G - \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. Άρα, εξ'ορισμού συνεπάγεται ότι $G - \{p\}$ είναι επίσης βάση Groebner για το *I*. ▵

Ορισμός 2.7.4 [1]

Μια **ελάχιστη (minimal) βάση Groebner** για κάποιο πολυωνυμικό ιδεώδες *I,* είναι μια βάση Groebner *G* τέτοια ώστε:

i. $\mathrm{LC}(p) = 1, \ \textit{για κάθε} \ p \in G$

ii. Για κάθε $p \in G, \ \mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\}) \rangle$

Εφαρμογή

Χρησιμοποιώντας το Παράδειγμα 2.7.1 και τη λεξικογραφική διάταξη, έχουμε τη βάση Groebner:

$$\begin{aligned} f_1 &= x^2 + 2xy^2 \\ f_2 &= xy + 2y^3 - 1 \\ f_3 &= x \\ f_4 &= -2y^3 - 1 \end{aligned} \ .$$

Παρατηρούμε ότι $\mathrm{LT}(f_1) = x^2 = x \cdot \mathrm{LT}(f_3)$. Επίσης $\mathrm{LT}(f_2) = xy = x \cdot \mathrm{LT}(f_3)$ και δεν υπάρχουν άλλες περιπτώσεις που ο μεγιστοβάθμιος όρος κάποιου γεννήτορα να διαιρεί τον μεγιστοβάθμιο όρο ενός άλλου γεννήτορα. Από το Λήμμα 2.7.3, έπεται λοιπόν ότι τα f_1, f_2 μπορούν να παραλειφθούν. Όμως για να πετύχουμε μια ελάχιστη βάση Groebner, πρέπει να πολλαπλασιάσουμε τους κύριους συντελεστές με κατάλληλες σταθερές, ώστε να γίνουν όλοι μονάδες και άρα η ελάχιστη βάση τελικά αποτελείται από τα:

$$\tilde{f}_3 = x, \qquad \tilde{f}_4 = y^3 + 1/2 \quad .$$

Ένα ιδεώδες μπορεί να έχει πολλές ελάχιστες Groebner βάσεις. Σκοπός είναι να επιλέγουμε την ελάχιστη βάση που μας διευκολύνει περισσότερο. △

Ορισμός 2.7.5 [1]

Μια **μειωμένη Groebner** για ένα πολυωνυμικό ιδώδες I είναι η βάση Groebner G για το I για την οποία ισχύει:

i. $\mathrm{LC}(p) = 1, \ \textit{για κάθε} \ p \in G$

ii. Για κάθε $p \in G$, κανένα μονώνυμο του p δεν ανήκει στο $\langle \mathrm{LT}(G - \{p\}) \rangle$.

Γενικά, μια μειωμένη βάση διακρίνεται από την εξής επιθυμητή ιδιότητα:

Πρόταση 2.7.6 [1]

Έστω $I \neq \{0\}$ ένα πολυωνυμικό ιδεώδες. Τότε για κάποια διάταξη μονωνύμων, το I έχει μοναδική μειωμένη βάση Groebner.

Μια συνέπεια της μοναδικότητας της παραπάνω πρότασης, είναι ότι προκύπτει ένας **Αλγόριθμος Ισοδυναμίας Ιδεωδών (ideal equality algorithm)** από τον οποίο μπορούμε να ελέγξουμε πότε δυο βάσεις $\{f_1, ..., f_s\}, \{g_1, ..., g_t\}$ παράγουν το ίδιο σύνολο. Συγκεκριμένα τα ιδεώδη θα είναι ισοδύναμα αν και μόνον αν οι μειωμένες βάσεις Groebner για τα $\langle f_1, ..., f_s \rangle, \langle g_1, ..., g_t \rangle$ είναι το ίδιο σύνολο.

Για το τέλος, αφήσαμε να δείξουμε πώς συνδέεται ο αλγόριθμος Buchberger με τον αλγόριθμο μείωσης γραμμών (απαλοιφή του Gauss), για τα συστήματα γραμμικών εξισώσεων. Παρατηρούμε όμως ότι ο αλγόριθμος της μείωσης γραμμών είναι ειδική περίπτωση του αλγορίθμου που μελετήσαμε. Ας δούμε λοιπόν μια εφαρμογή για να το διασαφηνίσουμε.

Εφαρμογή

Έστω το σύστημα γραμμικών εξισώσεων

$$\begin{aligned} x+3y+\ z+\ 9w&=0\\ x+2y\quad\ +\ 5w&=0\\ y+\ z+\ 4w&=0 \end{aligned}.$$

Στον πίνακα των παραπάνω συντελεστών, αφαιρούμε την πρώτη γραμμή από τη δεύτερη και έπειτα προσθέτουμε τις δυο τελευταίες γραμμές και λαμβάνουμε σε κλιμακωτή μορφή μειωμένων γραμμών, παίρνουμε

$$\begin{pmatrix} 1 & 3 & 1 & 9\\ 1 & 2 & 0 & 5\\ 0 & 1 & 1 & 4 \end{pmatrix} \xrightarrow{\gamma_2=\gamma_2-\gamma_1} \begin{pmatrix} 1 & 3 & 1 & 9\\ 0 & -1 & -1 & -4\\ 0 & 1 & 1 & 4 \end{pmatrix} \xrightarrow{\gamma_2=-\gamma_2} \begin{pmatrix} 1 & 3 & 1 & 9\\ 0 & 1 & 1 & 4\\ 0 & 1 & 1 & 4 \end{pmatrix} \longrightarrow .$$

$$\text{(2.7.3)} \qquad \xrightarrow{\gamma_2=\gamma_2-\gamma_3} \begin{pmatrix} 1 & 3 & 1 & 9\\ 0 & 1 & 1 & 4\\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Αυτός ο πίνακας αντιστοιχεί σε μια ελάχιστη βάση Groebner. Συνεχίζοντας τις πράξεις και αφαιρώντας από την πρώτη γραμμή το τριπλάσιο της τρίτης, παίρνουμε τον πίνακα της μειωμένης κλιμακωτής μορφής, που αντιστοιχεί στη μειωμένη βάση Groebner:

$$\text{(2.7.4)} \qquad \begin{pmatrix} 1 & 0 & -2 & -3\\ 0 & 1 & 1 & 4\\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Για να δούμε αλγεβρικά τους παραπάνω υπολογισμούς, έστω I το ιδεώδες

$$I=\langle x+3y+z+9w,\ x+2y+5w,\ y+z+4w\rangle \subset K[x,y,z,w].$$

που αντιστοιχεί στο αρχικό σύστημα. Θα χρησιμοποιήσουμε τη λεξικογραφική διάταξη $x > y > z > w$. Η γραμμική μορφή που καθορίζεται από τον πίνακα (2.7.3), δίνει την ελάχιστη βάση Groebner

$$I = \langle x + 3y + z + 9w,\ \ y + z + 4w \rangle,$$

ενώ ο πίνακας (2.7.4) δίνει τη μειωμένη βάση Groebner

$$I = \langle x - 2z - 3w,\ \ y + z + 4w \rangle.$$

Υπενθυμίζουμε ότι κάθε πίνακας έχει μοναδική κλιμακωτή μορφή μειωμένων γραμμών. Αυτό λοιπόν μπορεί να θεωρηθεί ως ειδική περίπτωση της μοναδικότητας της μειωμένης βάσης Groebner. △

ΚΕΦΑΛΑΙΟ 3

ΕΦΑΡΜΟΓΕΣ ΤΩΝ ΙΔΕΩΔΩΝ ΚΑΙ ΤΗΣ ΒΑΣΗΣ GROEBNER

§3.1 ΕΙΣΑΓΩΓΗ

Έχουμε δει μέχρι στιγμής τη χρήση της βάσης Groebner στη μελέτη των πολυωνυμικών ιδεωδών και πολλαπλοτήτων. Η βάση αυτή είναι σημαντικό εργαλείο στην επίλυση μαθηματικών προβλημάτων, φυσικής και μηχανικής, όπου απαιτείται η χρήση πινάκων με πολυώνυμα πολλών μεταβλητών. Βασικό της πλεονέκτημα είναι ότι μετασχηματίζει ένα σύνολο πολυωνύμων και κατ΄επέκταση ένα σύστημα, σε ένα άλλο που έχει ίδιοτητες που διευκολύνουν τη μελέτη των προβλημάτων. Μια πρώτη εφαρμογή αυτής της βάσης, είναι στα προβλήματα συμμετοχής και περιγραφής των ιδεωδών που αναφέρθηκαν στα προηγούμενα κεφάλαια. Παρακάτω δίνεται μια εκτενής πριγραφή από τις εφαρμογές της βάσης Groebner σε προβλήματα που σχετίζονται με την παραγοντοποίση των *n*-διάστατων πολυωνυμικών πινάκων και σε προβλήματα μετασχηματισμού πολυωνυμικών πινάκων πολλών μεταβλητών σε άλλες ισοδύναμες δομές. Επιπλέον, γίνεται αναφορά σε εντολές του Mathematica για τον υπολογισμό της ενώ, καταγράφονται συνοπτικά οι εφαρμογές αυτής της βάσης στον τομέα των κυκλωμάτων, του ελέγχου, στη θεωρία συστημάτων και κατ’επέκταση στην κωδικοποίηση, αποκωδικοποίηση και ρομποτική.

§3.2 ΟΙ ΠΡΩΤΕΣ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΒΑΣΗΣ GROEBNER

Στην §2.1 είδαμε πώς μπορούμε να επιλύσουμε το πρόβλημα περιγραφής ιδεωδών χρησιμοποιώντας το θεώρημα Hilbert. Τώρα θα μελετήσουμε πώς βοηθάει η βάση Groebner στην επίλυση των προβλημάτων που τέθηκαν στο προηγούμενο κεφάλαιο.

Το Πρόβλημα Συμμετοχής των Ιδεωδών [1]

Συνδυάζοντας τη βάση Groebner με τον αλγόριθμο της διαίρεσης παίρνουμε τον **αλγόριθμο για τη συμμετοχή των ιδεωδών.** Για κάποιο ιδεώδες, αρχικά χρησιποποιούμε το Θεώρημα 2.7.2 και βρίσκουμε μια βάση Groebner $G = \{g_1, ..., g_t\}$ για το *I*. Από το Πόρισμα 2.6.2 συνεπάγεται ότι $f \in I$ *αν και μόνον αν* $\overline{f}^G = 0$.

Παράδειγμα 3.2.1 [4]

Έστω $I = \langle f_1, f_2 \rangle = \langle x^3 + xy + x + 3, xy^2 + 4xy \rangle$ και θα χρησιμοποιήσουμε την grlex διάταξη. Έστω $f = x^3y^2 + 3x^2y + 2xy$ και θέλουμε να ελέγξουμε αν $f \in I$.

Το αρχικό παραγόμενο σύνολο δεν είναι βάση Groebner για το *I*, αφού $f = y^2(x^3 + xy + x + 3) + (-y + 3)(xy^2 + 4xy) + 3x^2y + 10xy - 3y^2$ και άρα $\overline{f}^{\{f_1, f_2\}} = 3x^2y + 10xy - 3y^2 \neq 0$. Συνεχίζουμε λοιπόν με τον υπολογισμό μιας βάσης Groebner.

$$S(f_1, f_2) = \frac{x^3y^2}{x^3}(x^3 + xy + x + 3) - \frac{x^3y^2}{xy^2}(xy^2 + 4xy) = -4x^3y + xy^3 + xy^2 + 3y^2.$$

Εκτελώντας τον αλγόριθμο της διαίρεσης παίρνουμε:

$$-4x^3y + xy^3 + xy^2 + 3y^2 = -4y(x^3 + xy + x + 3) + (y + 1)(xy^2 + 4xy) + 3y^2 + 12y.$$

Έστω $f_3 = y^2 + 4y$.

$$S(f_1,f_3)=\frac{x^3y^2}{x^3}(x^3+xy+x+3)-\frac{x^3y^2}{y^2}(y^2+4y)=-4x^3y+xy^3+xy^2+3y^2=S(f_1,f_2)$$
$$S(f_2,f_3)=\frac{xy^2}{xy^2}(xy^2+4xy)-\frac{xy^2}{y^2}(y^2+4y)=xy^2+4xy-xy^2-4xy=0$$

Από τον αλγόριθμο της διαίρεσης παίρνουμε:

$$S(f_1,f_2)=S(f_2,f_3)=-4y\cdot f_1+(y+1)\cdot f_2+3\cdot f_3$$

και άρα $\overline{S(f_1,f_2)}^{\{f_1,f_2,f_3\}}=\overline{S(f_1,f_3)}^{\{f_1,f_2,f_3\}}=0$.

Επίσης είναι προφανές ότι $\overline{S(f_2,f_3)}^{\{f_1,f_2,f_3\}}=0$ και άρα η βάση Groebner είναι το σύνολο:

$$G=\{f_1,f_2,f_3\}=\{x^3+xy+x+3,xy^2+4xy,y^2+4y\}.$$

Η μειωμένη βάση Groebner είναι η $G=\{f_1,f_3\}=\{x^3+xy+x+3,y^2+4y\}$.

Τώρα απομένει να ελέγξουμε εάν τα πολυώνυμα ανήκουν στο *I*. Διαιρώντας με το *f* την παραπάνω μειωμένη βάση παίρνουμε:

$$f=(2y^2+4y)\cdot f_1+(-xy-x-3)\cdot f_3=0.$$

Αφού λοιπόν το υπόλοιπο είναι μηδέν, συμπεραίνουμε ότι $f\in I$.

Ομοίως, αν θέλουμε να ελέγξουμε αν το $f=xy^3-6yz$ ανήκει στο *I*, χωρίς να χρειαστεί να υπολογίσουμε το υπόλοιπο της διαίρεσης με το *G*, παρατηρούμε ότι $\mathrm{LT}(f)=xy^3\notin\langle\mathrm{LT}(G)\rangle=\langle x^3,xy^2,y^2\rangle$. Ως εκ τούτου, $\overline{f}^G\neq 0$ και άρα $f\notin I$.

Με αυτήν την τελευταία παρατήρηση διασαφηνίζεται πώς τα στοιχεία μιας βάσης Groebner μας δίνουν πληροφορίες για τις ιδιότητες των ιδεωδών.

Το προβλημα επίλυσης πολυωνυμικών εξισώσεων [1]

Σε αυτό το σημείο θα μελετήσουμε πώς μέσα από τη βάση Groebner μπορούμε να λύσουμε πολυωνυμικές εξισώσεις.

Παράδειγμα 3.2.2 [1]

Σε αυτό το παράδειγμα αναζητούμε μέγιστη και ελάχιστη τιμή του $x^3 + 2xyz - z^2$, υπό τον περιορισμό $x^2 + y^2 + z^2 = 1$. Έστω λοιπόν οι εξισώσεις:

$$\begin{aligned} 3x^2 + 2yz - 2x\lambda &= 0 \\ 2xz - 2y\lambda &= 0 \\ 2x^2 - 2z - 2z\lambda &= 0 \\ x^2 + y^2 + z^2 - 1 &= 0 \end{aligned} .$$

Αρχικά, υπολογίζουμε μια βάση Groebner για το ιδεώδες στο $\mathrm{R}[x, y, z, \lambda]$ που παράγεται από τα αριστερά μέλη των εξισώσεων, χρησιμοποιώντας τη λεξικογραφική διάταξη $\lambda > x > y > z$. Χρησιμοποιώντας το Mathematica έχουμε:

```
GroebnerBasis[{3x^2+2y*z-2x*λ,2x*z-2y*λ,2x^2-2z-2z*λ,x^2+y^2+z^2-1},{λ,
x,y,z}]
```

και παίρνουμε:

$$\begin{aligned} &\lambda - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 + \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ &x^2 + y^2 + z^2 - 1, \\ &xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ &xz + yz^2 - \frac{1152}{3835}z^5 + \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ &y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ &y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ &yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2, \\ &z^7 - \frac{1763}{1152}z^5 + \frac{655}{1152}z^3 - \frac{11}{288}z. \end{aligned} \qquad (3.2.1)$$

Με μια πρώτη ματιά, τα παραπάνω πολυώνυμα δείχνουν πολύπλοκα, καθώς οι συντελεστές των στοιχείων της Groebner βάσης είναι πιο σύνθετοι από αυτούς του αρχικού παραγόμενου συνόλου. Ωστόσο, αν παρατηρήσουμε καλύτερα, θα δούμε ότι το τελευταίο πολυώνυμο εξαρτάται μόνο από z. Οι υπόλοιπες μεταβλητές εξαφανίστηκαν κατά τη διαδικασία δημιουργίας της βάσης. Θέτωντας τις παραπάνω εξισώσεις ίσες με μηδέν, παίρνουμε τις ρίζες:

$$z = 0,\ \pm 1,\ \pm\frac{2}{3},\ \pm\frac{\sqrt{11}}{8\sqrt{2}}.$$

Αν αντικαταστήσουμε αυτές τις τιμές του z στις εξισώσεις (3.2.1), οι εξισώσεις που προκύπτουν μπορούν να λυθούν ως προς x ή y ή λ. Αυτές με το λ δεν μας εξυπηρετούν σε κάποιο σκοπό, οπότε τελικά έχουμε τις εξής λύσεις:

$$\begin{aligned}
&z = 0; \quad y = 0; \quad x = \pm 1\\
&z = 0; \quad y = \pm 1, \quad x = \pm 1\\
&z = \pm 1, \quad y = 0, \quad x = 0\\
&z = 2/3; \quad y = 1/3; \quad x = -2/3\\
&z = -2/3; \quad y = -1/3; \quad x = -2/3\\
&z = \sqrt{11}/\sqrt{2}; \quad y = -3\sqrt{11}/8\sqrt{2}; \quad x = -3/8\\
&z = -\sqrt{11}/\sqrt{2}; \quad y = 3\sqrt{11}/8\sqrt{2}; \quad x = -3/8
\end{aligned}$$

Από αυτές τις λύσεις μπορούμε εύκολα να βρούμε πιθανή μέγιστη και ελάχιστη τιμή. △

Παρατηρούμε ότι με τη χρήση της βάσης Groebner και τη λεξικογραφική διάταξη απλοποιούνται πολύ οι εξισώσεις μας, Συγκεκριμένα, χρησιμοποιούμε εξισώσεις όπου οι μεταβλητές εξαφανίζονται διαδοχικά με σειρά που αντιστοιχεί στη διάταξή τους.

Το Πρόβλημα της Πεπλεγμένης Αναπαράστασης

Έστω οι παραμετρικές εξισώσεις

$$\begin{array}{l} x_1 = f_1(t_1,...,t_m) \\ \quad\vdots \\ x_n = f_n(t_1,...,t_m) \end{array} \quad , \tag{3.2.2}$$

οι οποίες ορίζουν ένα υποσύνολο μιας πολλαπλότητας V στο K^n. Χρησιμοποιώντας τη βάση Groebner, μπορούμε να βρούμε πολυωνυμικές εξισώσεις με τα $x_1,...,x_n$ που ορίζουν τη V. Έστω ότι τα f_i είναι πολυώνυμα και θα μελετήσουμε την αφινική πολλαπλότητα στο K^{n+m} που δίνεται από τις εξισώσεις:

$$\begin{array}{l} x_1 - f_1(t_1,...,t_m) = 0 \\ \quad\vdots \\ x_n - f_n(t_1,...,t_m) = 0 \end{array} \quad . \tag{3.2.3}$$

Βασική ιδέα, όπως και στο προηγούμενο παράδειγμα είναι ότι εξαλείφοντας τις μεταβλητές $t_1,...,t_m$, παίρνουμε τις εξισώσεις του V.

Έστω λοιπόν η λεξικογραφική διάταξη $t_1 > ... > t_m > x_1 > ... > x_n$ στο $K[t_1,...,t_m,x_1,...,x_n]$ και το ιδεώδες $\tilde{I} = \langle x_1 - f_1,...,x_n - f_n \rangle$. Η βάση Groebner του παραπάνω ιδεωδούς περιέχει κάποια πολυώνυμα που εξαλείφουν τις μεταβλητές. Οι πρώτες που θα εξαφανιστούν είναι οι $t_1,...,t_m$. Έτσι, η Groebner για το $\tilde{I}$ θα αποτελείται από πολυώνυμα που θα περιέχουν μόνο τα $x_1,...,x_n$.

Παράδειγμα 3.2.3 [1]

Έστω η παραμετρική καμπύλη V στο C^3:

$$x = t^4$$
$$y = t^3$$
$$z = t^2$$

Κάνοντας χρήση του Mathematica, υπολογίζουμε μια βάση Groebner G για το $I = \langle t^4 - x, t^3 - y, t^2 - z \rangle$ και χρησιμοποιώντας τη λεξικογραφική διάταξη στο $C[x, y, z, \lambda]$, παίρνουμε:

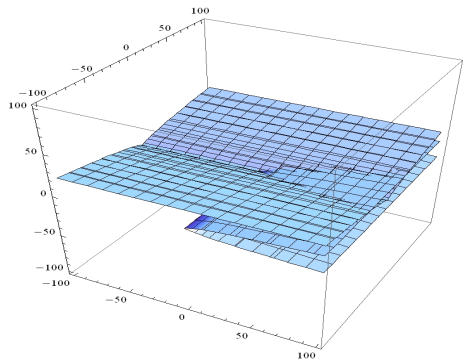
```
In[1]:= GroebnerBasis[{t^4 - x, t^3 - y, t^2 - z}, {t, x, y, z}]
Out[1]= {y^2 - z^3, x - z^2, -y + t z, t y - z^2, t^2 - z}
```

$$G = \{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}.$$

Παρατηρούμε ότι τα τελευταία δύο πολυώνυμα αποτελούνται μόνο από τα x, y, z και άρα ορίζουν μια αφινική πολλαπλότητα στο C^3, που περιέχει την καμπύλη μας. Σύμφωνα με όσα είδαμε στο Κεφάλαιο 1, δύο εξισώσεις στο C^3 , δίνουν μια 3-2=μονοδιάστατη πολλαπλότητα, δηλαδή καμπύλη. Για να σχεδιάσουμε αυτήν την πολλαπλότητα, χρησιμοποιούμε στο Mathematica την εντολή:

```
ContourPlot3D[{x-z^2,y^2-z^3},{x,-100,100},{y,-100,100},{z,-100,100}]
```

και παίρνουμε:



§3.3 ΜΗΔΕΝΙΚΕΣ ΔΟΜΕΣ ΠΟΛΥΩΝΥΜΙΚΩΝ ΠΙΝΑΚΩΝ

Σκοπός αυτής της παραγράφου είναι να βρούμε ισοδυναμίες πολυωνυμικών πινάκων πολλών μεταβλητών, που διατηρούν αναλλοίωτα συγκεκριμένα χαρακτηριστικά τους. Όπως θα δούμε η γνώση των ιδεωδών και των αφινικών πολλαπλοτήτων αποτελεί σημαντικό εργαλείο στη μελάτη αυτή.

Στα πολυώνυμα μιας μεταβλητής, οι κοινές ρίζες τους αντιστοιχούν στους κοινούς διαιρέτες τους και αντίστροφα. Ωστόσο, για τα *n*-διάστατα πολυώνυμα, υπάρχει περίπτωση δύο πολυώνυμα να είναι πρώτα μεταξύ τους, δηλαδή να μην έχουν κοινό διαιρέτη (παραγοντικά πρώτα πολυώνυμα - factor coprime), αλλά παρόλα αυτά να έχουν κοινή λύση (δηλαδή δεν είναι μηδενικά πρώτα - zero coprime).

Για παράδειγμα, τα πολυώνυμα $f(x,y)=xy^2$, $f(x,y)=x+y$, είναι παραγοντικά πρώτα, αλλά όχι μηδενικά πρώτα, καθώς έχουν κοινή λύση την $(x,y)=(0,0)$.

<u>Ορισμός 3.3.1</u> [4]

Ο διαιρέτης $d_i(x),\ i=1,...,r$ των οριζουσών *i*-τάξης, του πίνακα P(x), είναι ο ΜΚΔ των υποοριζουσών *i*-τάξης του P(x). Οι ρίζες του $d_i(x)$ ονομάζονται ρίζες *i*-τάξης του P(x).

Αυτός ο ορισμός είναι επέκταση αυτού της μονοδιάστατης περίπτωσης, αλλα δεν είναι πολύ σαφής, καθώς υπάρχουν περιπτώσεις, όπως για παράδειγμα τα πολυώνυμα που είδαμε παραπάνω, όπου για τον πίνακα $\mathrm{P}(x)=(xy^2 \quad x+y)$ ισχύει ότι $d_1(x)=1$ και άρα δεν υπάρχουν ρίζες οριζουσών 1x1, όμως, η τάξη του πίνακα μειώνεται για $x=y=0$.

Με $m_{(i,j)}$ θα συμβολίζουμε την $i\times i$ υποορίζουσα του $p\times q$ πίνακα P(x) , όπου $j=1,...,k_i=\dfrac{p!}{i!(p-i)!}\cdot\dfrac{q!}{i!(q-i)!}$. Επίσης, με $I_i^{[\mathrm{P}]}$ θα συμβολίζεται το σύνολο των πολυωνύμων που παράγεται από τις $i\times i$ υποορίζουσες του P(x) και έστω ότι $I_i^{[\mathrm{P}]}=d_iJ_i^{[\mathrm{P}]}$. Δηλαδή, το $J_i^{[\mathrm{P}]}$ είναι το σύνολο που παράγεται από τις $i\times i$ υποορίζουσες του P(x) , χωρίς να περιέχει τον διαιρέτη των οριζουσών *i*-τάξης. Τα στοιχεία του $J_i^{[\mathrm{P}]}$ είναι παραγοντικά πρώτα μεταξύ του, αλλά ενδέχεται να μην είναι και μηδενικά πρώτα.

Ορισμός 3.3.2 [4]

Οι αναλλοίωτες ρίζες *i*-τάξης, *i*=1,...,*r* , ενός πολυωνυμικού πίνακα $\mathrm{P}(x)$, είναι τα στοιχεία της πολλαπλότητας $V(I_i^{[\mathrm{P}]})$.

Ορισμός 3.3.3 [4]

Η αλγεβρική διάταξη μιας αναλλοίωτης ρίζας $a=(a_1,...,a_n)\in \mathrm{C}^n$, είναι ο θετικός ακέραιος $n(a)=r-\mathrm{rank}\mathrm{P}(a)$. Ο γεωμετρικός βαθμός *i*-οστής τάξης, $\delta_i(a),\ i=1,...,r$ μιας αναλλοίωτης ρίζας $a\in \mathrm{C}^n$, είναι ο αριθμός των φορών που το α εμφανίζεται στην πολλαπλότητα $V(I_i^{[\mathrm{P}]})$.

Θεώρημα 3.3.4 [4]

Αν $\mathrm{P}(x)$ είναι ένας $p\times q$ πίνακας, τότε θα ισχύει:

$$I_r^{[\mathrm{P}]}\subseteq ...\subseteq I_1^{[\mathrm{P}]}$$
$$V(I_r^{[\mathrm{P}]})\supseteq ...\supseteq V(I_1^{[\mathrm{P}]})$$

Απόδειξη

Κάθε $i\times i$ υποορίζουσα $m_{(i,j)}$, μπορεί να εκφραστεί ως γραμμικός συνδυασμός $(i-1)\times(i-1)$ υποοριζουσών. Συνεπώς, $m_{(i,j)}\in I_{i-1}^{[\mathrm{P}]}$ και άρα $I_i^{[\mathrm{P}]}\in I_{i-1}^{[\mathrm{P}]}$. Αν τώρα $a\in V(I_{i-1}^{[\mathrm{P}]})$ άρα θα ισχύει και ότι $a\in V(I_i^{[\mathrm{P}]})$. ▵

Πόρισμα 3.3.5 [4]

Αν $d_i(x)$ είναι ο διαιρέτης *i*-τάξης των οριζουσών του $\mathrm{P}(x)$, τότε $d_1\big|d_2\big|\cdots\big|d_r$ και άρα

$$\langle d_r\rangle\subseteq\cdots\subseteq\langle d_1\rangle$$
$$V\left(\langle d_r\rangle\right)\supseteq\cdots\supseteq V\left(\langle d_1\rangle\right)$$

Ιδιαίτερο ενδιαφέρον στα προβλήματα που επιλύονται με τη χρήση πολυωνυμικών

πινάκων, παρουσιάζουν οι ρίζες που ορίσαμε νωρίτερα ως αναλλοίωτες, καθώς διευκολύνουν τη μελέτη της ελεγξιμότητας και παρατηρησιμότητας n-διάστατων συστημάτων.

Ορισμός 3.3.6 [5]

Ένας πολυωνυμικός πίνακας πίνακας $\mathrm{P}(x)$ θα λέγεται **μηδενικά αριστερά πρώτος (zero left prime-zlp)** αν και μόνο αν όλες οι $i \times i$ υποορίζουσές του παράγουν το μοναδιαίο ιδεώδες.

Για να δούμε πώς εφαρμόζεται η βάση Groebner στους n-διάστατους πολυωνυμικούς πίνακες, έστω ότι $a_1,...,a_\beta$, όλες οι $i \times i$ υποορίζουσες του $p \times q$ πίνακα P, όπου $\beta = \binom{p}{q} = \frac{p!}{(p-q)!q!}$. Σύμφωνα με τον παραπάνω ορισμό, για να είναι ο P zlp, αρκεί να υπάρχουν $e_1,...,e_\beta$, τέτοια ώστε:

$$\sum_{i=1}^{\beta} e_i a_i = 1.$$

Άρα, εάν η βάση Groebner του ιδεωδούς που σχηματίζεται από τα $a_1,...,a_\beta$ περιέχει το 1, τότε ο πίνακας είναι zlp.

Ορισμός 3.3.7 [6]

Δύο $p \times q,\ q \times l$ n-διάστατοι πολυωνυμικοί πίνακες $T(x),\ U(x)$ με $p \le q + l$ θα λέγονται **μηδενικά αριστερά πρώτοι (zero left coprime-zlc)** εάν ισχύει η:

$$\text{(3.3.1)} \qquad \operatorname{rank}(T(x) \quad U(x)) = p, \quad \forall x \in \mathbb{C}^n .$$

Αντίστοιχα, οι πίνακες $T(x),\ V(x)$ θα λέγονται **μηδενικά δεξιά πρώτοι (zero right coprime -zrc)** εάν ισχύει η:

$$\operatorname{rank}(T^T(x) \quad V^T(x))^T = q, \quad \forall x \in \mathbb{C}^n .$$

Θεώρημα 3.3.8 [4]

Οι $p\times q,\ p\times l\ X(x),\ Y(x)$ πίνακες $T(x),\ U(x)$, με $p\le q+1$ θα είναι zlc εάν ισχύει κάποια από τις παρακάτω ισοδύναμες προτάσεις.

i. Υπάρχουν $q\times p,\ l\times p$ πολυωνυμικοί πίνακες , τέτοιοι ώστε:

$$T(x)X(x)+U(x)Y(x)=I_p\,.$$

ii. Ο $(T(x)\quad U(x))$ δεν περιλαμβάνει αναλλοίωτες ρίζες.

Ορισμός 3.3.9 [4]

Έστω $\mathcal{P}(x,y)$ η κλάση όλων των $(s+p)\times(s+q)$ n-διάστατων πολυωνυμικών πινάκων, όπου $s>-\min(p,q)$. Οι $P_1(x),P_2(x)\in\mathcal{P}(x,y)$, θα λέγονται **μηδενικά πρώτοι ισοδύναμοι (zero coprime equivalent- ZC-E)** αν υπάρχουν πίνακες κατάλληλων διαστάσεων $M(x),\ N(x)$, τέτοιοι ώστε:

$$M(x)P_2(x)=P_1(x)N(x)\,, \tag{3.3.3}$$

όπου M,P_1 zlc, P_2,N zrc .

Θεώρημα 3.3.10 [4]

Έστω οι ZC-E πίνακες $P_1(x),P_2(x)\in\mathcal{P}(x,y)$, τάξεων r_1,r_2 και διαστάσεων $p_1\times q_1,p_2\times q_2$, όπου $p_1-q_1=p_2-q_2=p-q$, για τους οποίους ισχύει η

$$M(x)P_2(x)=P_1(x)N(x)\,. \tag{3.3.4}$$

Τότε θα ισχύει:

$$I_{r_1-i}^{[P_1]}=I_{r_2-i}^{[P_2]},\ i=0,...,r-1\,, \tag{3.3.5}$$

όπου $r = \min(r_1, r_2)$. Για κάθε $i \geq r$, $I_{r_1 - i}^{[P_1]} = \langle 1 \rangle$, όταν $r_1 - i \geq 0$, ή $I_{r_2 - i}^{[P_2]} = \langle 1 \rangle$, όταν $r_2 - i \geq 0$.

<u>Απόδειξη</u>

Έστω ότι $h_1 = \min(p_1, q_1),\ h_2 = \min(p_2, q_2)$ και έστω $i \in \{1, 2\}$, όπου για το συμπλήρωμα του i' ισχύει $h_i \leq h_{i'}$.

Έστω

$$P_i^{'}(x) = \begin{pmatrix} I_{h_{i'} - h_i} & 0 \\ 0 & P_i(x) \end{pmatrix}.$$

Για τα ιδεώδη που παράγονται από τις υποορίζουσες των $P_i(x), P_i^{'}(x)$, ισχύει:

(3.3.6)
$$\left.\begin{array}{rcl} I_{h_{i'}}^{[P_i^{'}]} & = & I_{h_i}^{[P_i]} \\ \vdots & = & \vdots \\ I_{h_{i'} - h_i + 1}^{[P_i^{'}]} & = & I_1^{[P_i]} \\ I_{h_{i'} - h_i}^{[P_i^{'}]} & = & \langle 1 \rangle \\ \vdots & = & \vdots \\ I_1^{[P_i^{'}]} & = & \langle 1 \rangle \end{array}\right\}.$$

Οι $P_i(x), P_i^{'}(x)$ είναι ZC-E , αφού ισχύουν οι:

$$\begin{array}{c} \begin{pmatrix} 0 & I_{p_i} \end{pmatrix} P_i^{'}(x) = P_i(x) \begin{pmatrix} 0 & I_{q_i} \end{pmatrix} \\ \begin{pmatrix} 0 \\ I_{p_i} \end{pmatrix} P_i(x) = P_i^{'}(x) \begin{pmatrix} 0 \\ I_{q_i} \end{pmatrix} \end{array} .$$

Από τη μεταβατική ιδιότητα της σχέσης ισοδυναμίας ZC-E, έπεται ότι τα $P_1^{'}(x), P_2^{'}(x)$ είναι κι αυτά ZC-E, με ίδιες διαστάσεις $p' \times q'$. Εφαρμόζοντας το ίδιο θεώρημα , έστω $h = \min(p', q')$. Από τις ιδιότητες των ZC-E, υπάρχουν πολυωνυμικοί πίνακες $X(x), Y(x), W(x), Z(x)$ με κατάλληλες διαστάσεις, ώστε να ισχύει

$$\left.\begin{matrix} MX + P_1^{'}Y = I_{p^{'}} \\ WP_2^{'} + ZN = I_{q^{'}} \end{matrix}\right\}. \qquad (3.3.7)$$

Από τις (3.3.4) και (3.3.7) έπεται ότι:

$$\begin{pmatrix} W & -Z \\ M & P_1^{'} \end{pmatrix}\begin{pmatrix} P_2^{'} & X \\ -N & Y \end{pmatrix} = \begin{pmatrix} I_{q^{'}} & J \\ 0 & I_{p^{'}} \end{pmatrix}, \qquad (3.3.8)$$

όπου $J=WX-ZY$.

Για κάθε πίνακα Q θα συμβολίζουμε με $Q^{i_1,\ldots,i_k}_{j_1,\ldots,j_k}$ τον $k\times k$ υποπίνακα που σχηματίζεται από τις γραμμές $i_1,\ldots,i_k$ και τις στήλες $j_1,\ldots,j_k$. Άρα η (3.8) γίνεται:

$$\underbrace{\begin{pmatrix} E^{i_1,..,i_k} & 0 \\ M & P_1^{'} \end{pmatrix}}_{A}\underbrace{\begin{pmatrix} P^{'}_{2_{j1,\ldots,jk}} & X \\ -N_{j_1,\ldots,j_k} & Y \end{pmatrix}}_{B} = \begin{pmatrix} P_{2_{j1,\ldots,jk}}^{'i_1,..,i_k} & X^{i_1,..,i_k} \\ 0 & I_{p^{'}} \end{pmatrix}, \qquad (3.3.9)$$

όπου $1\le k\le h$ και $E^{i_1,..,i_k}$ είναι ο πίνακας όπου παίρνει την τιμή 1, αν για το στοιχείο t που υπάρχει στη θέση s, ισχύει $s=i_t$, αλλιώς παίρνει την τιμή 0.

Παίρνοντας τις ορίζουσες των πινάκων και των δυο μελών και εφαρμόζοντας το θεώρημα Cauchy-Binet έχουμε:

$$\sum_m \left|A^{1,\ldots,p'+k}_{m_1,\ldots,m_{p'+k}}\right|\left|B^{m_1,\ldots,m_{p'+k}}_{1,\ldots,p'+k}\right| = \left|P_{2_{j1,\ldots,jk}}^{'i_1,..,i_k}\right|. \qquad (3.3.10)$$

Από τη μορφή του πίνακα A,φαίνεται ότι κάθε παράγοντας του A που βρίσκεται στο αριστερό μέλος της (3.3.10), για τον οποίο το $\{i_1,\ldots,i_k\}$ δεν είναι υποσύνολο του $\{m_1,\ldots,m_{p+k}\}$ είναι μηδενικός. Επομένως, όλες οι υποορίζουσες του A που εμφανίζοται στο αριστερό μέλος της (3.3.10) περιέχουν τις στήλες $\{i_1,\ldots,i_k\}$. Ένας τέτοιος παράγοντας

μπορεί να εκφραστεί με το ανάπτυγμα Laplace, ως προς τις υποορίζουσες των M και $P_1^{'}$. Η μικρότερη υποορίζουσα που εμφανίζεται στο ανάπτυγμα Laplace, είναι τάξης k. Άρα, το $\left|P_{2_{j_1,\ldots,j_k}}^{'i_1,\ldots,i_k}\right|$ μπορεί να εκφραστεί ως γραμμικός συνδυασμός των υποοριζουσών του $P_1^{'}$, που είναι τάξης μεγαλύτερης ή ίσης του k. Εφόσον κάθε υποορίζουσα είναι ανάπτυγμα υποοριζουσών μικρότερης τάξης, έπεται ότι το $\left|P_{2_{j1,\ldots,jk}}^{'i_1,\ldots,i_k}\right|$ μπορεί να γραφτεί ως γραμμικός συνδυασμός των οριζουσών τάξης k του $P_1^{'}$. Οπότε ισχύει:

$$I_k^{[P_2^{'}]} \subset I_k^{[P_1^{'}]},\ k=1,\ldots,h=\min(p',q'). \tag{3.3.11}$$

Από τη συμμετρική ιδιότητα της ισοδυναμίας ZC-E, υπάρχουν πολυωνυμικοί πίνακες $M'(x), N'(x)$, τέτοιοι ώστε:

$$M' P_1^{'} = P_2^{'} N',$$

όπου οι $M'(x), P_2'(x)$ είναι zlc και οι $P_1'(x), N'(x)$ είναι zrc. Ομοίως με την προηγούμενη διαδικασία καταλήγουμε ότι:

$$I_k^{[P_1^{'}]} \subset I_k^{[P_2^{'}]}$$

και άρα τελικά $I_k^{[P_1^{'}]} = I_k^{[P_2^{'}]},\ k=1,\ldots,h$.

Έστω $i \in \{1,2\}$, όπου για το συμπλήρωμα του i' ισχύει $h_i \le h_{i'}$. Από τα παραπάνω και τις σχέσεις (3.3.6) παίρνουμε

$$
\left.
\begin{array}{rcl}
I_{h_{i'}}^{[P_i']} & = & I_{h_i}^{[P_i]} \\
\vdots & = & \vdots \\
I_{h_{i'}-h_i+1}^{[P_i']} & = & I_1^{[P_i]} \\
I_{h_{i'}-h_i}^{[P_i']} & = & \langle 1 \rangle \\
\vdots & = & \vdots \\
I_1^{[P_i']} & = & \langle 1 \rangle
\end{array}
\right\}. \tag{3.3.12}
$$

Για $r_{i'} = \mathrm{rank}\mathrm{P}_{i'}$ έχουμε:

$$I_{h_{i'}}^{[P_{i'}]} = \cdots = I_{r_{i'}+1}^{[P_{i'}]} = \{0\} \neq I_{r_{i'}}^{[P_{i'}]}.$$

Από τις (3.3.12) συνεπάγεται ότι:

$$I_{h_{i'}}^{[P_i]} = \cdots = I_{h_i-h_{i'}+r_{i'}+1}^{[P_i]} = \{0\} \neq I_{h_i-h_{i'}+r_{i'}}^{[P_i]}.$$

Ως εκ τούτου, $r_i = h_i - h_{i'} + r_{i'}$

και άρα οι σχέσεις (3.3.12) ανάγονται στις:

$$
\left.
\begin{array}{rcl}
I_{r_{i'}}^{[P_{i'}]} & = & I_{r_i}^{[P_i]} \\
\vdots & = & \vdots \\
I_{r_{i'}-r_i+1}^{[P_{i'}]} & = & I_1^{[P_i]} \\
I_{r_{i'}-r_i}^{[P_i]} & = & \langle 1 \rangle \\
\vdots & = & \vdots \\
I_1^{[P_i']} & = & \langle 1 \rangle
\end{array}
\right\}. \tag{3.3.13}
$$

Πόρισμα 3.3.11 [4]

Αν $V(I)$ είναι η πολλαπλότητα που παράγεται από το ιδεώδες I και ισχύουν οι συνθήκες του Θεωρήματος 3.3.9, τότε:

$$V\left(I_{r_1-i}^{[P_1]}\right)=V\left(I_{r_2-i}^{[P_2]}\right),\ i=0,1,...,r-1, \tag{3.3.14}$$

Πόρισμα 3.3.12 [4]

Αν $a\in \mathrm{C}$ είναι μια αναλλοίωτη ρίζα του P_1 με αλγεβρική διάταξη $n(a)$ και μη-μηδενικούς γεωμετρικούς βαθμούς $\delta_{r_1-n(a)+1}(a),...,\delta_{r_1(a)}(a)$, τότε το a ειναι ρίζα και για το P_2, με την ίδια αλγεβρική διάταξη και τους ίδιους γεωμετρικούς βαθμούς.

Πόρισμα 3.3.13 [4]

Έστω $d_i^{[P_1]}, d_i^{[P_2]}$, οι διαιρέτες των οριζουσών i-τάξης, των πινάκων P_1, P_2 αντίστοιχα, για τους οποίους ισχύουν οι συνθήκες του Θεωρήματος 3.3.9. Έστω $V\left(\left\langle d_i^{[P_1]}\right\rangle\right), V\left(\left\langle d_i^{[P_2]}\right\rangle\right)$, οι πολλαπλότητες που ορίζονται από τα ιδεώδη που παράγονται από τα $d_i^{[P_1]}, d_i^{[P_2]}$. Τότε:

$$\begin{aligned} d_{r_1-i}^{P_1} &= c_i d_{r_2-i}^{P_2} \\ V\left(\left\langle d_i^{[P_1]}\right\rangle\right) &= V\left(\left\langle d_i^{[P_2]}\right\rangle\right), \end{aligned}$$

όπου $i=0,1,...,r-1$ και $c_i\in \mathrm{C}\{0\}$. Για κάθε, $i\geq r$, $d_{r_1-i}^{[P_1]}=c_i(\neq 0)$ (και άρα $V\left(I_{r_1-i}^{[P_1]}\right)=\varnothing$), όταν $r_1-i\geq 0$, ενώ $d_{r_2-i}^{[P_2]}=c_i(\neq 0)$ (και άρα $V\left(I_{r_2-i}^{[P_2]}\right)=\varnothing$), όταν $r_2-i\geq 0$.

Πόρισμα 3.3.14 [4]

Έστω οι πίνακες P_1, P_2 για τους οποίους ισχύουν οι συνθήκες του Θεωρήματος 3.3.9. Για τα ιδεώδη $J_i^{P_1}, J_i^{P_2}$ θα ισχύει:

$$J_{r_1-i}^{[P_1]} = J_{r_1-i}^{[P_2]}$$
$$V\left(J_{r_1-i}^{[P_1]}\right) = V\left(J_{r_2-i}^{[P_1]}\right)'$$

όπου $i = 0,1,...,r-1$.

Για κάθε $i \geq r$, $J_{r_1-i}^{[P_1]} = \langle 1 \rangle$ (και αρα $V\left(I_{r_1-i}^{[P_1]}\right) = \varnothing$), όταν $r_1 - i \geq 0$, ενώ $J_{r_2-i}^{[P_2]} = \langle 1 \rangle$ (και άρα $V\left(I_{r_2-i}^{[P_2]}\right) = \varnothing$), όταν $r_2 - i \geq 0$.

Ας δούμε λοιπόν μια εφαρμογή του παραπάνω θεωρήματος και των πορισμάτων του.

Παράδειγμα 3.3.15 [4]

Έστω οι πίνακες

$$P_1(x,y,z) = \begin{bmatrix} x^2 & 0 & xy \\ 0 & z^2 & xz \end{bmatrix}, P_2(x,y,z) = \begin{bmatrix} 1 & 0 & y & 0 \\ z & x^2 & yz & xy \\ 0 & 0 & z^2 & xz \end{bmatrix},$$

οι οποίοι είναι ZC-E, καθώς ισχύει:

$$\underbrace{\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}}_{M} \underbrace{\begin{bmatrix} x^2 & 0 & xy \\ 0 & z^2 & xz \end{bmatrix}}_{P_1} = \underbrace{\begin{bmatrix} 1 & 0 & y & 0 \\ z & x^2 & yz & xy \\ 0 & 0 & z^2 & xz \end{bmatrix}}_{P_2} \underbrace{\begin{bmatrix} 0 & -y & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}_{N}$$

και οι πίνακες $\begin{bmatrix} M & P_2 \end{bmatrix}, \begin{bmatrix} P_1 \\ -N \end{bmatrix}$ έχουν τάξη 3, αφού υπάρχουν 3×3 υποορίζουσες με

$$\det\begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & z \\ 0 & 1 & 0 \end{vmatrix} = 1 \neq 0, \ \det\begin{vmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{vmatrix} = -1 \neq 0.$$ Δηλαδή M, P_2 zlc, P_1, N zrc.

Βρίσκουμε τα ιδεώδη που παράγονται από τις υποορίζουσες του P_1 και έχουμε:

$$\begin{aligned} I_2^{[P_1]} &= \left\langle x^3 z, x^2 z^2, -xyz^2 \right\rangle \\ I_1^{[P_1]} &= \left\langle x^2, xy, xz, z^2 \right\rangle \end{aligned} ,$$

ενώ για τα ιδεώδη του P_2 έχουμε:

$$\begin{aligned} I_3^{[P_2]} &= \left\langle x^2 z^2, x^3 z, -xyz^2, x^3 yz^2 \right\rangle \\ I_2^{[P_2]} &= \left\langle x^2, xy, x^2 y, xy^2, z^2, xz, xyz, z^3, xz^2, x^2 z^2, x^3 z \right\rangle \\ I_1^{[P_2]} &= \left\langle 1, y, z, x^2, yz, xy, z^2, xz \right\rangle \end{aligned} .$$

Είναι προφανές ότι:

$$\begin{aligned} I_2^{[P_1]} &= I_3^{[P_2]} \\ I_1^{[P_1]} &= I_2^{[P_2]} \\ I_1^{[P_2]} &= \left\langle 1 \right\rangle \end{aligned}$$

και

$$\begin{aligned} d_3^{[P_2]} &= d_2^{[P_1]} = xz \\ d_2^{[P_2]} &= d_1^{[P_1]} = 1 \\ d_1^{[P_2]} &= 1 \end{aligned} .$$

Δ

Παρακάτω θα δούμε μια επέκταση του Θεωρήματος 3.3.9, στην ισοδυναμία περιγραφών πολυωνυμικών συστημάτων .

Σύμφωνα με τον Rosenbrock (1970), ένα *n*-διάστατο σύστημα πινάκων, περιγράφει ένα *n*-διάστατο σύστημα γραμμικών εξισώσεων με *l* εισόδους και *m* εξόδους, όταν είναι της μορφής:

$$(3.3.15) \qquad P(x) = \begin{pmatrix} T(x) & U(x) \\ -V(x) & W(x) \end{pmatrix} ,$$

όπου $T(x),U(x),V(x),W(x)$, είναι πολυωνυμικοί πίνακες *n*-μεταβλητών, διαστάσεων $r\times r, r\times l, m\times r, m\times l$, αντίστοιχα και με $\mathcal{P}_S(m,l)$ συμβολίζεται το *n*-διάστατο πολυωνυμικό σύστημα πινάκων, διαστάσεων $(r+m)\times(r+l), r>0$.

Ορισμός 3.3.16 [4]

Δύο πολυωνυμικές περιγραφές συστημάτων $P_1(x), P_2(x)\in\mathcal{P}_S(m,l)$, με διαστάσεις $(r_1+m)\times(r_1+l)$,$(r_2+m)\times(r_2+l)$, για τις οποίες ισχύει:

$$\underbrace{\begin{pmatrix} Q_1(x) & 0 \\ R_1(x) & I_m \end{pmatrix}}_{S_1(x)}\underbrace{\begin{pmatrix} T_2(x) & U_2(x) \\ -V_2(x) & W_2(x) \end{pmatrix}}_{P_2(x)}=\underbrace{\begin{pmatrix} T_1(x) & U_1(x) \\ -V_1(x) & W_1(x) \end{pmatrix}}_{P_1(x)}\underbrace{\begin{pmatrix} Q_2(x) & R_1(x) \\ 0 & I_l \end{pmatrix}}_{S_2(x)}, \tag{3.3.16}$$

θα αποκαλούνται **μηδενικά πρώτα ισοδύναμες (zero coprime system equivalent-(ZC-SE))** αν S_1, P_1 είναι zlc και S_2, P_2 είναι zrc.

Γενικά, η σχέση ZC-SE είναι μια σχέση ισοδυναμίας όπου χρησιμοποιώντας αναγωγή στο αρχικό γραμμικό σύστημα μπορούμε να μεταβούμε σε μια απλή μορφή πίνακα.

Λήμμα 3.3.17 [4]

Έστω δύο πολυωνυμικές περιγραφές συστημάτων $P_1(x), P_2(x)\in\mathcal{P}_S(m,l)$ για τις οποίες ισχύει η (3.3.16). Τα S_1, P_1 θα είναι zlc, αν και μόνο αν τα Q_1, T_1 είναι zlc. Αντίστοιχα θα είναι και τα S_2, P_2 zrc.

Λήμμα 3.3.18 [4]

Δύο πολυωνυμικές περιγραφές συστημάτων $P_1(x), P_2(x)\in\mathcal{P}_S(m,l)$ για τις οποίες ισχύει η (3.3.16), θα είναι ZC-SE αν και μόνο αν τα Q_1, T_1 είναι zlc και τα T_2, Q_2 είναι zrc.

Λήμμα 3.3.19 [4]

Έστω δύο πολυωνυμικές περιγραφές συστημάτων $P_1(x), P_2(x) \in \mathcal{P}_S(m,l)$ για τις οποίες ισχύει η (3.3.16). Τότε να παρακάτω ζευγάρια πινάκων είναι ZC-E:

i. $P_1(x), P_2(x)$

ii. $T_1(x), T_2(x)$

iii. $T_i(x), U_i(x),\ i=1,2$

iv. $T_i(x), -V_i(x),\ i=1,2$

Θεώρημα 3.3.20 [4]

Δύο n-διάστατες πολυωνυμικές περιγραφές συστημάτων $P_1(x), P_2(x) \in \mathcal{P}_S(m,l)$, με διαστάσεις $(r_1+m)\times(r_1+l)$, $(r_2+m)\times(r_2+l)$ για τα οποία ισχύει η (3.16). Τότε:

i. Για $h=\min(h_1,h_2),\ h_i=\min(r_i+m, r_i+l),\ i=1,2$,

$$I_{h_1-i}^{[P_1]} = I_{h_2-i}^{[P_2]}$$
$$V\left(I_{h_1-i}^{[P_1]}\right) = V\left(I_{h_2-i}^{[P_2]}\right),\ i=0,\ldots,h-1$$

ii. Για $r=\min(r_1,r_2)$,

$$I_{r_1-i}^{[T_1]} = I_{r_2-i}^{[T_2]}$$
$$V\left(I_{r_1-i}^{[T_1]}\right) = V\left(I_{r_2-i}^{[T_2]}\right),\ i=0,\ldots,r-1$$

iii. Για $r=\min(r_1,r_2)$,

$$I_{r_1-i}^{[T_1\ \ U_1]} = I_{r_2-i}^{[T_2\ \ U_2]}$$
$$V\left(I_{r_1-i}^{[T_1\ \ U_1]}\right) = V\left(I_{r_2-i}^{[T_2\ \ U_2]}\right)\ i=0,\ldots,r-1$$

iv. Για $r = \min(r_1, r_2)$,

$$I_{r_1-i}^{[T_1 \quad -V_1]} = I_{r_2-i}^{[T_2 \quad -V_2]}$$
$$V\left(I_{r_1-i}^{[T_1 \quad -V_1]}\right) = V\left(I_{r_2-i}^{[T_2 \quad -V_2]}\right) \quad i = 0,...,r-1$$

όπου για κάθε $i \geq h$, $I_{h_1-i}^{[P_1]} = \langle 1 \rangle$, $V\left(I_{h_1-i}^{[P_1]}\right) = \varnothing$, για $h_1 - i \geq 0$, ή $I_{h_2-i}^{[P_2]} = \langle 1 \rangle$, $V\left(I_{h_2-i}^{[P_2]}\right) = \varnothing$, για $h_2 - i \geq 0$. Επίσης, για κάθε $i \geq r$, $I_{r_1-i}^{[T_1]} = I_{r_1-i}^{[T_1 \quad U_1]} = I_{r_1-i}^{[T_1 \quad -V_1]} = \langle 1 \rangle$, όταν $r_1 - i \geq 0$, ή $I_{r_2-i}^{[T_2]} = I_{r_2-i}^{[T \quad U_2]} = I_{r_2-i}^{[T_2 \quad -V_2]} = \langle 1 \rangle$, όταν $r_2 - i \geq 0$.

<u>Πόρισμα 3.3.21</u> [4]

Αν

$$P(x) = \begin{pmatrix} T(x) & U(x) \\ -V(x) & W(x) \end{pmatrix}$$

είναι μια πολυωνυμική περιγραφή συστήματος, τότε οι αναλλοίωτες ρίζες των $P(x), T(x), (T(x)\ U(x)), (T(x)^T\ -V(x)^T)^T$, παραμένουν αναλλοίωτες με τη σχέση ισοδυναμίας ZC-SE και διατηρούν την αλγεβρική διάταξή τους και τον γεωμετρικό βαθμό τους.

§3.4 ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΒΑΣΗΣ GROEBNER ΣΕ ΑΛΛΑ ΠΕΔΙΑ ΤΩΝ ΠΟΛΥΔΙΑΣΤΑΤΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σε αυτήν την παράγραφο, δίνεται μια συνοπτική περιγραφή από άλλα πεδία της θεωρίας συστημάτων, όπου εφαρμόζεται η βάση Groebner. Οι παρακάτω εφαρμογές καταγράφονται στο [5].

1) n-διάστατα συστήματα ανάλυσης, σύνθεσης και πραγμάτωσης:

Βασική εφαρμογή της βάσης Groebner υπάρχει στην σταθεροποιησιμότητα της ανατροφοδότησης σε δισδιάστατα συστήματα, καθώς επιτρέπει να ανάγουμε ένα πρόβλημα στην επίλυση μιας διοφαντικής εξίσωσης. Για τα *n*-διάστατα συστήματα, η βάση Groebner χρησιμοποιείται για την ανάκτηση της κανονικής αναπαράστασης στον χώρο των καταστάσεων, καθώς επίσης και για την ελάχιστη πραγμάτωσής τους. Είναι αποδοτική στο να επιλύει συστήματα με αρκετές μεταβλητές και χρησιμοποιήται για την διατήρηση του ελέγχου, για την αποφυγή σφαλμάτων και για τον σχεδιασμό παρατηρητών.[7]

2) n-διάστατες ταλαντώσεις και φίλτρα:

Η βάση Groebner διευκολύνει την επεξεργασία *n*-διάστατων ταλαντώσεων και την εύρεση φίλτρων όπου διαχωρίζουν την είσοδο ενός σήματος σε επιμέρους συνθετικά, αφού κάτι τέτοιο επιτυγχάνεται με τη δημιουργία πολυδιάστατων πολυωνυμικών ή ρητών πινάκων. Επίσης, στα *n*-διάστατα ψηφιακά φίλτρα, ο έλεγχος σταθερότητας μπορεί να αναχθεί στην επίλυση $n+1$ πολυωνυμικών εξισώσεων, με $n+1$ αγνώστους, όπου η λύση ενός τέτοιου συστήματος προσεγγίζεται επιτυχώς με τη χρήση αυτής της βάσης.[8]

3) n-διάστατη κωδικοποίηση και αποσυνέλιξη:

Για να γίνει *n*-διάστατη κωδικοποίηση, απαιτούνται *n*-διάστατοι πίνακες και η εύκολη διαχείριση αυτών γίνεται με τη βάση Groebner. Επιπλέον, πολλές εφαρμογές έχει *n*-διάστατη πολυκάναλη αποσυνέλιξη, όπως για παράδειγμα στην ισότητα καναλιών για πολλές κεραίες, στην αποσυνέλιξη της εικόνας και τη βαθμονόμηση των ραντάρ. Αρχικά, η αποσυνέλιξη λυνόταν με τη χρήση γραμμικής άλγεβρας αλλά τα τελευταία χρόνια εφαρμόζεται η βάση Groebner καθώς είναι πιο εύχρηστη.[9]

Σ Υ Μ Π Ε Ρ Α Σ Μ Α Τ Α

Για τη συσχέτιση της άλγεβρας με τη γεωμετρία, μελετάμε πολυώνυμα πάνω σε ένα σώμα. Η γεωμετρική έννοια της αφινικής πολλαπλότητας είναι το σύνολο που περιέχει τις λύσεις του συστήματος $f_1(x_1,...,x_n)=0$,..., $f_s(x_1,...,x_n)=0$. Για να βρούμε όλα τα σημεία μιας πολλαπλότητας, πρέπει να βρούμε όλες τις λύσεις αυτού του συστήματος. Αν το σύστημα έχει άπειρες λύσεις, τότε παραμετροποιούμε. Για τον καλύτερο υπολογισμό των πολλαπλοτήτων, χρησιμοποιούμε τα ιδεώδη, τα οποία είναι σύνολα με συγκεκριμένες ιδιότητες. Κάθε ιδεώδες έχει πολλές βάσεις, αλλά η πιο χρήσιμη από αυτές είναι η βάση Groebner. Μια αφινική πολλαπλότητα εξαρτάται μόνο από το ιδεώδη που παράγεται από τις εξισώσεις που ορίζουν την πολλαπλότητα. Ο αλγόριθμος της διαίρεσης για πολυώνυμα πολλών μεταβλητών βοηθά στην επίλυση του προβλήματος συμμετοχής των ιδεωδών· δηλαδή βοηθά στο να προσδιορίσουμε εάν κάποιο f ανήκει σε συγκεκριμένο ιδεώδες $\langle f_1,...,f_s\rangle$. Όταν η διαίρεση γίνεται με βάση Groebner, τότε το υπόλοιπο είναι μοναδικά ορισμένο.

Το κριτήριο Buchberger εισάγει τα S-πολυώνυμα και βοηθάει να ελέγξουμε εάν μια βάση είναι Groebner. Επίσης ο αλγόριθμος Buchberger χρησιμοποιείται για την κατασκευή μιας τέτοιας βάσης. Η βάση Groebner έχει πολλές εφαρμογές. Αρχικά, εφαρμόζεται για την επίλυση του προβλήματος συμμετοχής των ιδεωδών. Βρίσκουμε μια βάση από τον αλγόριθμο Buchberger και έπειτα ελέγχουμε αν το υπόλοιπο της διαίρεσης του δοθέντος πολυωνύμου με αυτή τη βάση είναι μηδενικό. Μια δεύτερη εφαρμογή είναι στην επίλυση πολυωνυμικών εξισώσεων με πολλαπλές μεταβλητές. Σε αυτήν την περίπτωση βρίσκουμε με τη βοήθεια του αλγορίθμου Buchberger μια βάση Groebner και έπειτα οι μεταβλητές τείνουν να εξαφανίζονται σταδιακά, με αποτέλεσμα να απλοποιούνται οι εξισώσεις μας. Επιπλέον, αυτή η βάση χρησιμοποιείται στο να βρούμε τις αρχικές εξισώσεις ενός παραμετροποιημένου συστήματος. Όπως ήδη αναφέραμε, βρίσκοντας μια βάση Groebner οι μεταβλητές σταδιακά εξαλείφονται. Συνεπώς απαλλαγόμαστε από τις παραμέτρους και απομένουν οι αρχικές μεταβλητές.

Τέλος, τα ιδεώδη και οι πολλαπλότητες συνδέονται με τις ισοδυναμίες πολυωνυμικών

πινάκων και συστημάτων. Για την ακρίβεια, τα ιδεώδη που παράγονται από τον ΜΚΔ των οριζουσών ισοδύναμων πινάκων είναι ίσα και όπως επίσης, ίσες είναι και οι πολλαπλότητες που παράγονται από αυτά τα ιδεώδη. Το ίδιο συμπέρασμα προκύπτει εάν επεκτείνουμε τους πίνακες σε πολυωνυμικές περιγραφές συστημάτων.

Β Ι Β Λ Ι Ο Γ Ρ Α Φ Ι Α

[1] David Cox, John Little, Donal O'Shea, 2007, Ideals, Varieties and Algorithms- An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer ,3rd ed., pp 1-114

[2] A Fryant and V L N Sarma, Gauss' first proof of the fundamental theorem of algebra, *Math. Student*

[3] http://lall.stanford.edu/data/engr210b_0405/more_groebner_bases_2003_10_20_02.pdf

[4] A.C.Pugh, S.J.McInerney, E.M.O. EL-Nabrawy, 2005, International Journal of Control, vol 78

[5] Zhiping Lin, Li Xu, Nirmal K. Bose, 2008, A Tutorial on Groebner Bases with Applications in Signals and Systems, IEEE Transactions on circuits and systems-I, pp 445-457, vol.55

[6] A.C. Pugh, G.E. Hayton, E.M.O. EL-Nabrawy and N.P.Karampetakis, Numerator -Denominator Structures of *n*-D MFDs

[7]U.Oberst, 2006, Canonical state representations and Hilbert functions of multidimensional systems, *Acta Appl Math*, pp. 83-135, vol 94

[8] C.Charoenlarpnopparut and N.K.Bose, 2001, Groebner bases for problem solving in multidimensional systems, Multidimensional Syst. Signal Process, pp. 365-376, vol. 12

[9] J.Zhou and M.N.Do, 2006, Multidimensional multichannel FIR deconvolution using Groebner bases, IEEE Trans. Image Process, pp. 2998-3007, vol.11