ΥΠΟΛΟΓΙΣΤΙΚΗ ΑΛΓΕΒΡΙΚΗ ΓΕΩΜΕΤΡΙΑ

ΣΥΣΤΗΜΑΤΑ ΠΟΛΥΩΝΥΜΙΚΩΝ ΕΞΙΣΩΣΕΩΝ

Διδάσκων: Αλέξης Κουβιδάκης

Περίληψη

Στις διαλέξεις θα μελετήσουμε συστήματα πολυωνυμικών εξισώσεων σε πολλές μεταβλητές και τρόπους εύρεσης των λύσεών τους. Η μελέτη θα επικεντρωθεί στα εξής:

1. Κριτίριο ύπαρξης λύσεων.
2. Μέχρι ποιό βαθμό καθορίζουν οι λύσεις το σύστημα των εξισώσεων;
3. Αλγόριθμοι γιά την εύρεση των λύσεων του συστήματος.

Η ύλη περιλαμβάνει στοιχεία από την θεωρία των ιδεωδών στον δακτύλιο των πολυωνύμων, το Θεώρημα Βάσης του Hilbert, την Nullstellensatz, Βάσεις Groebner και αλγόριθμος του Buchberger. Στις παραγράφους 1.2 - 1.5 έχουμε ακολουθήσει πιστά το βιβλίο των D. Cox, J. Little, D. O'Shea: *"Ideals, Varieties and Algorithms"*, Springer-Verlag 1997, απ' όπου είναι και όλα τα παραδείγματα.

1.1 Εισαγωγή

Εστω K σώμα (συνήθως $K = \mathbb{C}$) και συμβολίζουμε με $K[X_1, \ldots, X_n]$ τον δακτύλιο των πολυωνύμων n μεταβλητών $X_1, \ldots, X_n$, με συντελεστές στο K. Τα στοιχεία του $K[X_1, \ldots, X_n]$ έχουν την μορφή $f(X_1, \ldots, X_n) = \sum_\alpha c_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, όπου $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. Θα μελετήσουμε συστήματα πολυωνυμικών εξισώσεων

$$\begin{aligned} f_1(X_1, \ldots, X_n) &= 0 \\ &\cdots \\ f_s(X_1, \ldots, X_n) &= 0, \end{aligned} \tag{1}$$

όπου $f_i \in K[X_1, \ldots, X_n],\ i = 1, \ldots, s$. Το κύριο ερώτημα με το οποίο θα ασχοληθούμε είναι το τι μπορούμε να πούμε για τις λύσεις του παραπάνω συστήματος (1). Για να ανπτύξουμε μια καλή θεωρία θα πρέπει, για λόγους πληρότητας, να πάρουμε $K = \mathbb{C}$. Θα μελετήσουμε λοιπόν το σύνολο

$$\mathbb{V}(f_1, \ldots, f_s) := \{(a_1, \ldots a_n),\ \text{όπου}\ f_i(a_1, \ldots, a_n) = 0,\ \forall i = 1, \ldots, s\} \subseteq \mathbb{C}^n.$$

1^o **Ερώτημα:** Πότε το σύστημα έχει λύση;
Ας εξετάσουμε πρώτα την περίπτωση της μιας μεταβλητής, δηλ. $n = 1$. Το σύστημα είναι της μορφής

$$\begin{aligned} f_1(X) &= 0 \\ &\cdots \\ f_s(X) &= 0, \end{aligned} \tag{2}$$

Από την γνωστή θεωρία των πολυωνύμων μιας μεταβλητής, έχουμε ότι το σύστημα (2) είναι ισοδύναμο (δηλ. έχει τις ίδιες λύσεις) με το σύστημα της μιάς εξίσωσης $d(X) = 0$, όπου $d(x) = \text{ΜΚΔ}(f_1, \ldots, f_s)$. Πράγματι, αν $d(a) = 0$ τότε $f_i(a) = 0, \forall i = 1, \ldots, s$ διότι $f_i(X) = g_i(X)d(X)$. Από την άλλη μεριά, έστω $a \in \mathbb{V}(f_1, \ldots, f_s)$, δηλαδή $f_i(a) = 0, \forall i = 1, \ldots, s$. Γνωρίζουμε ότι ο ΜΚΔ εκφράζεται ως

$$d(X) = g_1(X)f_1(X) + \cdots + g_s(X)f_s(X). \tag{3}$$

Επομένως $d(a) = 0$. Συνεπώς οι λύσεις του συστήματος (2) είναι οι λύσεις της πολυωνυμικής εξίσωσης $d(X) = 0$. Αρα έχουμε το εξής κριτίριο

$$\begin{aligned} \mathbb{V}(f_1, \ldots, f_s) \neq \emptyset &\iff d(X) = 0 \text{ έχει λύση} \iff \deg d(X) \geq 1 \\ &\iff d(X) \neq 1 \iff f_1, \ldots, f_s \text{ όχι πρώτα μεταξύ τους.} \end{aligned}$$

Σημειώνουμε ότι το κύριο συστατικό για την διατύπωση του παραπάνω κριτιρίου είναι η σχέση (3) η οποία στηρίζεται ουσιαστικά στην ύπαρξη Ευκλείδειας διαίρεσης στον δακτύλιο $\mathbb{C}[X]$ των πολυωνύμων μιάς μεταβλητής.

Περνάμε τώρα στην περίπτωση των πολλών μεταβλητών, δηλ. $n \geq 2$. Κάθε πολυώνυμο του $\mathbb{C}[X_1, \ldots, X_n]$ γράφεται με μοναδικό τρόπο ως γινόμενο αναγώγων πολυωνύμων, δηλ. ο δακτύλιος $\mathbb{C}[X_1, \ldots, X_n]$ είναι δακτύλιος μονοσήμαντης ανάλυσης. Επομένως μπορούμε να ορίσουμε τον ΜΚΔ ενός συνόλου πολυωνύμων παίρνοντας τις ελάχιστες δυνάμεις της ανάλυσής τους σε ανάγωγα. Η δυσκολία όμως στις πολλές μεταβλητές είναι ότι δεν έχουμε μια καλή γενίκευση της Ευκλείδειας διαίρεσης και κατά συνέπεια δεν έχουμε για τον ΜΚΔ το ανάλογο της σχέσης (3). Για παράδειγμα, αν $f(x, y) = x^2(y + 1)$, $g(x, y) = xy^2$ δύο πολυώνυμα που δίδονται με τις αναλύσεις τους σε ανάγωγα, τότε $\text{ΜΚΔ}(f, g) = x$. Ομως το x δεν μπορεί να γραφεί στην μορφή $a(x, y)x^2(y + 1) + b(x, y)xy^2$, όπου $a(x, y), b(x, y)$ πολυώνυμα (αποδείξτε το!). Κατά συνέπεια για το σύστημα (1) έχουμε ότι αν $d(X_1, \ldots, X_n) = \text{ΜΚΔ}(f_1, \ldots, f_s)$ τότε $d(a_1, \ldots, a_n) = 0 \implies (a_1, \ldots, a_n) \in \mathbb{V}(f_1, \ldots, f_s)$, όχι όμως το αντίστροφο. Για παράδειγμα, αν θεωρήσουμε το σύστημα

$$\begin{aligned} f_1(x, y) = x &= 0 \\ f_2(x, y) = y &= 0, \end{aligned}$$

τότε $d(x, y) = \text{ΜΚΔ}(x, y) = 1$. Ομως το παραπάνω σύστημα έχει το $(0, 0)$ ως λύση δηλ. $\mathbb{V}(x, y) = \{(0, 0)\}$, ενώ $\mathbb{V}(d(x)) = \emptyset$. Τίθεται επομένως το ερώτημα, τί μπορούμε να πούμε στην περίπτωση των πολλών μεταβλητών.

Η ιδέα είναι να βάλουμε μια αλγεβρική δομή στο αρχικό σύστημα των εξισώσεων. Θεωρούμε το εξής σύνολο:

$$I := \mathbb{I}(f_1, \ldots, f_s) := \{g_1 f_1 + \cdots + g_s f_s, \ \text{όπου } g_i \in \mathbb{C}[X_1, \ldots, X_s]\} \subseteq \mathbb{C}[X_1, \ldots, X_s].$$

Ευκολα φαίνεται ότι το σύνολο I είναι ιδεώδες του δακτυλίου $\mathbb{C}[X_1, \ldots, X_s]$. Επίσης, παρατηρήστε ότι το αρχικό σύστημα (1) είναι ισοδύναμο με το άπειρο σύστημα εξισώσεων I, δηλ. $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(I)$. Το κριτίριο ύπαρξης λύσης που αναζητάμε μπορεί τώρα να διατυπωθεί σε σχέση με το ιδεώδες I.

Θεώρημα 1.1 $\mathbb{V}(I) \neq \emptyset \iff 1 \notin I (\iff I \neq \mathbb{C}[X_1, \ldots, X_s])$. *Επομένως το αρχικό σύστημα (1) δεν έχει λύση, αν και μόνον αν, υπάρχει συνδυασμός των $f_1, \ldots, f_s$ με συντελεστές πολυώνυμα που να ισούται με το σταθερό πολυώνυμο 1.*

Οπως θα δούμε στην συνέχεια, το παραπάνω Θεώρημα 1.1 είναι συνέπεια του Θεωρήματος 1.2 που παραθέτουμε στην συνέχεια. Επιβεβαιώνουμε τώρα το παραπάνω θεώρημα στην περίπτωση της μιάς μεταβλητής, δηλ. στην περίπτωση του συστήματος (2) Κατ' αρχάς, χρησημοποιώντας την σχέση (3), εύκολα φαίνεται ότι $I := \mathbb{I}(f_1(X), \ldots, f_s(X)) = \mathbb{I}(d(X))$. Οπως έχουμε πεί παραπάνω,

το σύστημα (2) δεν έχει λύση, αν και μόνον αν, $d(X) = 1$. Από την άλλη πλευρά, το Θεώρημα 1.1 λέγει ότι το σύστημα δεν έχει λύση, αν και μόνον αν, $1 \in I = \mathbb{I}(d(X)) \iff 1 = g(X)\, d(X) \iff d(X) =$ σταθερό πολυώνυμο. Ομως, εξ' ορισμού το $d(X)$ είναι μονικό πολυώνυμο, άρα είναι το σταθερό πολυώνυμο 1, αυτό ακριβώς που θέλαμε.

2^o **Ερώτημα:** Χαρακτηρίζουν οι λύσεις το σύστημα; Δηλ. αν (Σ) και (Σ') συστήματα πολυωνυμικών εξισώσεων με $\mathbb{V}(\Sigma) = \mathbb{V}(\Sigma')$, πώς σχετίζονται τα συστήματα (Σ) και (Σ'); Οπως θα δούμε, η έκφραση της συσχέτισης που αναζητάμε εμπεριέχει τα αντίστοιχα συστήματα ιδεωδών $\mathbb{I}(\Sigma)$ και $\mathbb{I}(\Sigma')$.

Παράδειγμα 1.1 Ας δούμε τι συμβαίνει στην περίπτωση της μιας μεταβλητής. Εστω δηλαδή, (Σ) και (Σ') συστήματα πολυωνύμων μιας μεταβλητής που έχουν το ίδιο σύνολο λύσεων. Οπως έχουμε δεί παραπάνω, $\mathbb{I}(\Sigma) = \mathbb{I}(d(X))$ και $\mathbb{I}(\Sigma') = \mathbb{I}(d'(X))$, όπου $d(X)$ και $d'(X)$ οι αντίστοιχοι ΜΚΔ των πολυωνύμων. Αν το κοινό σύνολο των λύσεων είναι το $V = \{a_1, \ldots, a_m\}$, αυτό ακριβώς θα είναι και το σύνολο λύσεων για κάθε μια από τις εξισώσεις $d(X) = 0$ και $d'(X) = 0$. Επομένως, υπενθυμίζοντας ότι έχουμε πάρει ως σώμα K τους μιγαδικούς αριθμούς $\mathbb{C}$, θα έχουμε ότι

$$\begin{aligned} d(X) &= (X - a_1)^{k_1} \cdots (X - a_m)^{k_m},\ k_i \geq 1, \\ d'(X) &= (X - a_1)^{t_1} \cdots (X - a_m)^{t_m},\ t_i \geq 1. \end{aligned}$$

Συνεπώς, συμπεραίνουμε ότι τα πολυώνυμα $d(X)$ και $d'(X)$ έχουν ως κοινό κομμάτι το γινόμενο $(X - a_1) \cdots (X - a_m)$. Για να το εκφράσουμε αυτό γενικότερα, με όρους που θα εφαρμόζονται και στην περίπτωση των πολλών μεταβλητών, δίδουμε τον παρακάτω ορισμό.

Ορισμός 1.1 (Ριζικό ενός ιδεώδους) *Εστω I ιδεώδες δακτυλίου R. Ορίζουμε ως ριζικό του I το ιδεώδες*

$$\mathrm{Rad}(I) := \{a \in R,\ \textit{όπου}\ a^k \in I,\ \textit{για κάποιον φυσικό αριθμό}\ k \geq 1\}.$$

Δηλαδή το $\mathrm{Rad}(I)$ περιλαμβάνει τα στοιχεία του I και τις ρίζες τους.

Παράδειγμα 1.2 Αν $I = \mathbb{I}(d(X))$, όπου $d(X) = (X - a_1)^{k_1} \cdots (X - a_m)^{k_m},\ k_i \geq 1$, τότε $\mathrm{Rad}(I) = \mathbb{I}((X - a_1) \cdots (X - a_m))$. Πράγματι, ας αποδείξουμε τους δύο εγκλεισμούς.
'$\supseteq$' Αρκεί να δείξω ότι $(X - a_1) \cdots (X - a_m) \in \mathrm{Rad}(I)$. Εστω $k = \max\{k_1, \ldots, k_m\}$. Τότε $[(X - a_1) \cdots (X - a_m)]^k = (X - a_1)^{k_1} \cdots (X - a_m)^{k_m} [(X - a_1)^{k-k_1} \cdots (X - a_m)^{k-k_m}] \in I$, και άρα $(X - a_1) \cdots (X - a_m) \in \mathrm{Rad}(I)$.
'$\subseteq$' Εστω $f \in \mathrm{Rad}(I)$, δηλ. $f^k \in I$, για κάποιον θετικό φυσικό k. Θα έχουμε επομένως $f^k(X) = g(X)\,(X - a_1)^{k_1} \cdots (X - a_m)^{k_m}$. Θέλουμε να δείξουμε ότι το $f(X)$ είναι πολλαπλάσιο του $(X - a_1) \cdots (X - a_m)$. Εχουμε ότι $(X - a_i)^{k_i} \mid f^k(X)$. Ομως, το $X - a_i$ είναι ανάγωγο άρα $X - a_i \mid f(X)$, $\forall i = 1, \ldots, m$ και αφού τα $X - a_i$, $i = 1, \ldots, m$ είναι πρώτα μεταξύ τους, έχουμε ότι και το γινόμενό τους διαιρεί το $f(X)$.

Το Θεώρημα που ισχύει γενικά, και δίδει απάντηση στο 2^o ερώτημα είναι το εξής.

Θεώρημα 1.2 *Δύο συστήματα πολυωνυμικών εξισώσεων* (Σ) *και* (Σ') *με μιγαδικούς συντελεστές έχουν τις ίδιες λύσεις, δηλ.* $\mathbb{V}(\Sigma) = \mathbb{V}(\Sigma')$*, αν και μόνον αν, για τα αντίστοιχα συστήματα ιδεωδών* $\mathbb{I}(\Sigma)$ *και* $\mathbb{I}(\Sigma')$ *ισχύει ότι* $\mathrm{Rad}(\mathbb{I}(\Sigma)) = \mathrm{Rad}(\mathbb{I}(\Sigma'))$.

Σημειώνουμε ότι η μία κατεύθυνση '$\Longleftarrow$' είναι εύκολη λόγω του ότι, όπως εύκολα φαίνεται, $\mathbb{V}(\Sigma) = \mathbb{V}(\mathbb{I}(\Sigma)) = \mathbb{V}(\mathrm{Rad}(\mathbb{I}(\Sigma)))$. Η άλλη κατεύθυνση είναι μη τετριμμένη και είναι συνέπεια του Θεωρήματος Nullstellensatz, βλ. Θεώρημα 1.4.

Παράδειγμα 1.3 Στην περίπτωση της μίας μεταβλητής, με βάση τα παραδείγματα 1.1 και 1.2, επιβεβαιώνεται το Θεώρημα 1.2.

Σημείωση 1.1 Οπως είπαμε παραπάνω, το Θεώρημα 1.1 είναι συνέπεια του Θεωρήματος 1.2. Πραγματι, δείχνουμε πρώτα ότι αν $1 \in I := \mathbb{I}(\Sigma)$ τότε $\mathbb{V}(\Sigma) = \emptyset$. Αυτό είναι φανερό από το ότι $\mathbb{V}(\Sigma) = \mathbb{V}(I)$ και αφού το I περιέχει το σταθερό πολυώνυμο 1, το αντίστοιχο σύστημα δεν έχει λύσεις. Αντίστροφα, έστω ότι $\mathbb{V}(\Sigma) = \emptyset$, τότε και $\mathbb{V}(I) = \emptyset$. Ομως, αν πάρουμε το ιδεώδες που παράγεται από το σταθερό πολυώνυμο 1, δηλ. το $< 1 >$, έχουμε επίσης ότι $\mathbb{V}(< 1 >) = \emptyset$. Συνεπώς, από το Θεώρημα 1.2 συνάγουμε ότι $\mathrm{Rad}(I) = \mathrm{Rad}(< 1 >)$. Ομως, $\mathrm{Rad}(< 1 >) =< 1 >$. Συνεπώς $1 \in \mathrm{Rad}(I)$, άρα $1 \in I := \mathbb{I}(\Sigma)$.

Κλείνουμε αυτή την εισαγωγή διατυπώνοντας δύο βασικά θεωρήματα για τον δακτύλιο των πολυωνύμων, το θεώρημα βάσης του Hilbert και το θεώρημα Nullstellensatz.

Θεώρημα 1.3 (Θεώρημα βάσης του Hilbert) *Κάθε ιδεώδες* I *του δακτυλίου των πολυωνύμων* $K[X_1, \ldots, X_n]$ *έχει ένα πεπερασμένο σύστημα γεννητόρων, δηλ. υπάρχουν* $g_1, \ldots, g_s \in I$ *τέτοια ώστε* $I =< g_1, \ldots, g_s >$.

Για να διατυπώσουμε το επόμενο θεώρημα χρειαζόμαστε έναν ορισμό.

Ορισμός 1.2 *Εστω* $A \subseteq \mathbb{C}^n$*. Τότε ορίζουμε*

$$\mathbb{I}(A) := \{f \in K[X_1, \ldots, X_n],\ \textit{όπου}\ f(a_1, \ldots, a_n) = 0,\ \forall (a_1, \ldots, a_n) \in A\}.$$

Θεώρημα 1.4 (Nullstellensatz) *Εστω* I *ιδεώδες του δακτυλίου* $\mathbb{C}[X_1, \ldots, X_n]$*. Τότε*

$$\mathbb{IV}(I) = \mathrm{Rad}(I).$$

Σημείωση 1.2 Δείχνουμε τώρα πώς το Θεώρημα 1.2 είναι συνέπεια του Θεωρήματος 1.4. Αφού $\mathbb{V}(\Sigma) = \mathbb{V}(\Sigma')$ θα έχουμε, επίσης, ότι $\mathbb{V}(\mathbb{I}(\Sigma)) = \mathbb{V}(\mathbb{I}(\Sigma'))$, διότι τα συστήματα (Σ) (αντιστ. (Σ')) και $\mathbb{I}(\Sigma)$ (αντιστ. $\mathbb{I}(\Sigma')$) είναι ισοδύναμα. Αρα $\mathbb{I}(\mathbb{V}(\mathbb{I}(\Sigma))) = \mathbb{I}(\mathbb{V}\mathbb{I}(\Sigma'))$. Από το Θεωρήματος 1.4 έχουμε ότι $\mathbb{I}(\mathbb{V}(\mathbb{I}(\Sigma))) = \mathrm{Rad}(\mathbb{I}(\Sigma))$ και, επίσης, $\mathbb{I}(\mathbb{V}(\mathbb{I}(\Sigma'))) = \mathrm{Rad}(\mathbb{I}(\Sigma'))$. Συνεπώς, $\mathrm{Rad}(\mathbb{I}(\Sigma)) = \mathrm{Rad}(\mathbb{I}(\Sigma'))$, αυτό που ζητούσαμε.

1.2 Διάταξη πολυωνύμων

Στον δακτύλιο $K[X]$ μπορούμε να διατάξουμε τα μονώνυμα ως προς τον βαθμό τους: $X^n > X^m \iff n > m$. Ανάλογες διατάξεις ορίζονται στην περίπτωση μονωνύμων σε πολλές μεταβλητές. Σε κάθε μονώνυμο του $K[X] = K[X_1, \ldots, X_n]$ αντιστοιχούμε μια διατεταγμένη ν-άδα του $\mathbb{Z}^n_{\geq 0}$ ως εξής: $X^a = X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} \longrightarrow a = (a_1, a_2, \cdots, a_n)$. Οταν χρησιμοποιούμε ως μεταβλητές τις x, y, z, w κλπ, υποθέτουμε ότι $x = X_1, y = X_2, z = X_3, w = X_4$ κλπ.

Ορισμός 1.3 (Μονωνυμική διάταξη) *Μια μονωνυμική διάταξη του $K[X_1, \ldots, X_n]$ είναι μια σχέση $>$ στο $\mathbb{Z}^n_{\geq 0}$ η οποία ικανοποιεί τα εξής:*

1. *$H >$ είναι ολική διάταξη του $\mathbb{Z}^n_{\geq 0}$. Δηλαδή αν $a, b \in \mathbb{Z}^n_{\geq 0}$ ισχύει ακριβώς ένα από τα εξής: $a > b$ ή $b > a$ ή $a = b$.*
2. *Αν $a, b, c \in \mathbb{Z}^n_{\geq 0}$ με $a > b$ τότε $a + c > b + c$.*
3. *$H >$ είναι μια καλή διάταξη, δηλαδή κάθε μη κενό υποσύνολο του $\mathbb{Z}^n_{\geq 0}$ έχει ελάχιστο στοιχείο ως προς την σχέση $>$.*

Συμβολισμός: Γράφουμε $X_1^{a_1} \cdots X_n^{a_n} > X_1^{b_1} \cdots X_n^{b_n}$ αν $a = (a_1, \ldots, a_n) > b = (b_1, \ldots, b_n)$.

Θα αναφέρουμε δύο παραδείγματα μονωνυμικών διατάξεων του $K[X_1, \ldots, X_n]$.

Ορισμός 1.4 (Λεξικογραφική διάταξη) *Εστω $a = (a_1, \ldots, a_n)$ και $b = (b_1, \ldots, b_n)$ στοιχεία του $\mathbb{Z}^n_{\geq 0}$. Τότε ορίζουμε $a >_{\text{lex}} b$ αν στο διάνυσμα $a - b \in \mathbb{Z}^n$ το πρώτο από τα αριστερά μη-μηδενικό στοιχείο είναι θετικό. Γράφουμε $X^a >_{\text{lex}} X^b$ αν $a >_{\text{lex}} b$.*

Παράδειγμα 1.4 $(3, 1, 2) >_{\text{lex}} (1, 8, 9)$.
$X_1^4 X_2^3 X_3^5 >_{\text{lex}} X_1^4 X_2^2 X_3^7$.
$X_1 >_{\text{lex}} X_2 >_{\text{lex}} \cdots >_{\text{lex}} X_n$.

Ορισμός 1.5 (Βαθμωτή λεξικογραφική διάταξη) *Εστω $a = (a_1, \ldots, a_n)$ και $b = (b_1, \ldots, b_n)$ στοιχεία του $\mathbb{Z}^n_{\geq 0}$. Τότε ορίζουμε $a >_{\text{grlex}} b$ αν $|a| := \sum_{i=1}^n a_i > |b| := \sum i = 1^n b_i$, είτε, $|a| = |b|$ και $a >_{\text{lex}} b$. Γράφουμε $X^a >_{\text{grlex}} X^b$ αν $a >_{\text{grlex}} b$.*

Παράδειγμα 1.5 $(3, 2, 3) >_{\text{grlex}} (4, 2, 1)$.
$X_1^4 X_2^3 X_3^5 >_{\text{grlex}} X_1^4 X_2^1 X_3^7$.
$X_1 >_{\text{grlex}} X_2 >_{\text{grlex}} \cdots >_{\text{grlex}} X_n$.

Ορισμός 1.6 *Έστω $f = \sum_a \alpha_a X_1^{a_1} \cdots X_n^{a_n}$, όπου $a = (a_1, \ldots, a_n)$ ένα μη-μηδενικό πολυώνυμο του $K[X_1, \ldots, X_n]$ και έστω $>$ μια μονωνυμική διάταξη.*

1. *Ο πολυβαθμός (multidegree) του f ορίζεται ως $\text{multideg}(f) = \max\{a = (a_1, \ldots, a_n) \in \mathbb{Z}^n_{\geq 0}, \ \alpha_a \neq 0\}$.*
2. *Ο οδηγός συντελεστής (leading coefficient) του f ορίζεται ως $\text{LC}(f) = \alpha_{\text{multideg}(f)} \in K$.*

3. *Το οδηγό μονώνυμο (leading monomial) του f ορίζεται ως* $\mathrm{LM}(f) = X_1^{c_1} \cdots X_n^{c_n}$, *όπου* $(c_1, \ldots, c_n) = \mathrm{multideg}(f)$.

4. *Ο οδηγός όρος (leading term) του f ορίζεται ως* $\mathrm{LT}(f) = \mathrm{LC}(f)\,\mathrm{LM}(f)$.

Για παράδειγμα, αν $f(x, y, z) = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ και με $>$ συμβολίσουμε την λεξικογραφική διάταξη τότε
$\mathrm{multideg}(f) = (3, 0, 0)$, $\mathrm{LC}(f) = -5$, $\mathrm{LM}(f) = x^3$ και $\mathrm{LT}(f) = -5x^3$.

1.3 Αλγόριθμος διαίρεσης στο $K[X_1, \ldots, X_n]$

Θα εξετάσουμε σε αυτήν την παράγραφο πώς ο αλγόριθμος διαίρεσης πολυωνύμων μιας μεταβλητής μπορεί να γενικευτεί σε πολλές μεταβλητές. Ισχύει το παρακάτω θεώρημα, το οποίο εφαρμόζουμε σε παραδείγματα

Θεώρημα 1.5 (Αλγόριθμος διαίρεσης σε πολλές μεταβλητές) *Διαλέγουμε μια μονωνυμική διάταξη στο $\mathbb{Z}^n_{\geq 0}$. Εστω $(f_1, \ldots, f_s)$ μια διατεταγμένη s-άδα πολυωνύμων του $K[X_1, \ldots, X_n]$. Τότε κάθε $f \in K[X_1, \ldots, X_n]$ μπορεί να γραφεί ως*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

όπου $a_1, \ldots, a_s, r \in K[X_1, \ldots, X_n]$ και είτε $r = 0$ είτε το r είναι γραμμικός συνδυασμός με συντελεστές στο K από μονώνυμα, κανένα από τα οποία δεν διαιρείται από τα $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. Επίσης, $\mathrm{multdeg}(f) \geq \mathrm{multdeg}(a_i f_i)$, για κάθε $i = 1, \ldots, s$.

Παράδειγμα 1.6 Εστω $f_1 = xy - 1$, $f_2 = y^2 - 1$ και $f = x^2y + xy^2 + y^2$. Διαλέγουμε την λεξικογραφική διάταξη με $x = X_1$, $y = X_2$. Το αποτέλεσμα της διαίρεσης δίδει:
$a_1 = x + y$,
$a_2 = 1$,
$r = x + y + 1$,
τα οποία βρίσκονται ως εξής: $\mathrm{LT}(f_1) = xy$, $\mathrm{LT}(f_2) = y^2$, $\mathrm{LT}(f) = x^2y$. Το $\mathrm{LT}(f_1) = xy$ διαιρεί το $\mathrm{LT}(f) = x^2y$ και κάνουμε την διαίρεση του f με το f_1 ως συνήθως. Βρίσκουμε πηλίκο x, το οποίο συνεισφέρει στο a_1, και το υπόλοιπο είναι $g_1 = xy^2 + x + y^2$. Εχουμε $\mathrm{LT}(g_1) = xy^2$, το οποίο διαιρείται από τον $\mathrm{LT}(f_1) = xy$ και κάνουμε την διαίρεση του g_1 με το f_1. Βρίσκουμε πηλίκο y, το οποίο συνεισφέρει στο a_1, και υπόλοιπο $g_2 = x + y^2 + y$. Είναι $\mathrm{LT}(g_2) = x$ που δεν διαιρείται από τον $\mathrm{LT}(f_1) = xy$ ούτε, επίσης, από τον $\mathrm{LT}(f_2) = y^2$. Μεταφέρουμε τον $\mathrm{LT}(g_2) = x$ στο υπόλοιπο και συνεχίζουμε με το $g_3 = y^2 + y$. Είναι $\mathrm{LT}(g_3) = y^2$ το οποίο δεν διαιρείται από το $\mathrm{LT}(f_1) = xy$, διαιρείται όμως από τον $\mathrm{LT}(f_2) = y^2$. Κάνουμε την διαίρεση και βρίσκουμε πηλίκο x, το οποίο συνεισφέρει στο a_2, και υπόλοιπο $g_4 = y + 1$. Είναι $\mathrm{LT}(g_4) = y$ που δεν το διαιρεί ούτε το $\mathrm{LT}(f_1) = xy$ ούτε το $\mathrm{LT}(f_2) = y^2$. Μεταφέρεται επομένως στο υπόλοιπο και μένει $g_5 = 1$ το οποίο, ομοίως, μεταφέρεται στο υπόλοιπο. Εχουμε τελικώς

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

Σημείωση 1.3 Τα κύρια μειονεκτήματα του παραπάνω αλγορίθμου είναι τα εξής.

1. Ο αλγόριθμος εξαρτάται από την διάταξη των στοιχείων $f_1, \ldots, f_s$, πράγμα μη φυσιολογικό. Στο παραπάνω παράδειγμα, αν αλλάξουμε την διάταξη των $f_1,\ f_2$ και διατάξουμε το f_2 ως πρώτο στοιχείο, τότε το αποτέλεσμα της διαίρεσης δίδει:
$a_1 = x + 1$,
$a_2 = x$,
$r = 2x + 1$.

2. Είναι δύσκολο να αναγνωρίσουμε με διαίρεση πότε ένα πολυώνυμο f πολλών μεταβλητών ανήκει σε ένα ιδεώδες I. Στην μία μεταβλητή, όπως γνωρίζουμε, κάθε ιδεώδες I του $K[X]$ παράγεται από ένα - ουσιαστικά μοναδικο - στοιχείο, δηλ. $I =< g >$. Οταν μας δώσουν $f \in K[X]$, τότε $f \in I$, εάν και μόνον εάν, το υπόλοιπο της διαίρεσης του f με το g είναι μηδεν. Στις πολλές μεταβλητές όμως τα πράγματα δεν είναι ακριβώς έτσι. Σε αυτήν την περίπτωση τα ιδεώδη παράγονται από πεπερασμένα το πλήθος στοιχεία, βλ. Θεώρημα βάσης του Hilbert 1.3, όχι όμως μοναδικά επιλεγμένα. Επίσης, για να κάνουμε διαίρεση πρέπει να να διατάξουμε αυθαίρετα τους γεννήτορες του ιδεώδους. Για παράδειγμα, ας πάρουμε το ιδεώδες I του $K[x, y]$ που παράγεται από τα στοιχεία $f_1 = xy+1,\ f_2 = y^2-1$ και ας ρωτήσουμε αν το πολυώνυμο $f = xy^2 - x$ ανήκει στο I. Προσπαθούμε να λύσουμε το πρόβλημα με διαίρεση. Διαλέγουμε την λεξικογραφική διάταξη και διαιρούμε με $f_1,\ f_2$. Τότε βρίσκουμε πηλίκα $a_1 = y,\ a_2 = 0$ και υπόλοιπο $r = -x-y$, δηλ. $xy^2-x = y(xy+1)+0(y^2-1)-x-y$. Αρα η παραπάνω διαίρεση δεν μας εκφράζει το f ως συνδυασμό των $f_1,\ f_2$. Αυτό όμως δεν αποκλείει το f να γράφεται ως συνδυασμός των $f_1,\ f_2$!. Αν για παράδειγμα αλλάξουμε στην διαίρεση την διάταξη των $f_1,\ f_2$, τότε παίρνουμε ως πηλίκα τα $a_1 = x,\ a_2 = 0$ και υπόλοιπο $r = 0$ δηλ. $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$ (το οποίο βέβαια μπορούσαμε να το βρούμε και χωρίς να κάνουμε την διαίρεση!).

Τελικά όμως τα πράγματα δεν είναι και τόσο άσκημα. Στην παρακάτω παράγραφο θα δούμε ότι για κάθε ιδεώδες I του δακτυλίου $K[X_1, \ldots, X_n]$ μπορούμε να διαλέξουμε ένα ειδικό σύστημα γεννητόρων, την λεγόμενη βάση Groebner, με την χρήση της οποίας αίρονται οι παραπάνω δυσκολίες.

1.4 Βάσεις Groebner

Ορισμός 1.7 *Εστω I ένα μη μηδενικό ιδεώδες του $K[X_1, \ldots, X_n]$.*

1. *Συμβολίζουμε με $\mathrm{LT}(I)$ το σύνολο των οδηγών όρων (leading terms) των στοιχείων του I, δηλ.*

$$\mathrm{LT}(I) = \{cX_1^{a_1} \cdots X_n^{a_n},\ \ \text{υπάρχει } f \in I \text{ με } \mathrm{LT}(f) = cX_1^{a_1} \cdots X_n^{a_n}\}.$$

2. *Συμβολίζουμε με $< \mathrm{LT}(I) >$ το ιδεώδες που παράγεται από τα στοιχεία του συνόλου $\mathrm{LT}(I)$.*

Σημείωση 1.4 Αν $I =< f_1, \ldots, f_s >$, τότε το ιδεώδες $< \mathrm{LT}(I) >$ είναι, εν γένει, μεγαλύτερο από το ιδεώδες $< \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) >$. Για παράδειγμα, αν $I =< f_1, f_2 >$, όπου $f_1 = x^3 - 2xy$ και $f_2 = x^2y - 2y^2 + x$ και έστω ότι χρησιμοποιούμε την grlex διάταξη, τότε έχουμε $\mathrm{LT}(f_1) = x^3,\ \mathrm{LT}(f_2) = x^2y$. Το $x^2 \in I$ διότι $x^2 = xf_2 - yf_1$. Αρα $\mathrm{LT}(x^2) = x^2 \in < \mathrm{LT}(I) >$. Ομως, $x^2 \notin < x^3, x^2y >$ (αποδείξτε το!).

Θεώρημα 1.6 *Εστω I ένα ιδεώδες του $K[X_1, \ldots, X_n]$ και έστω ότι διαλέγουμε μια μονωνυμική διάταξη.*

1. *Τότε υπάρχουν $g_1, \ldots, g_s \in I$ τέτοια ώστε $< \mathrm{LT}(I) >=< \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) >$.*
2. *Αν διαλέξουμε πολυώνυμα $g_1, \ldots, g_s \in I$ με την ιδιότητα $< \mathrm{LT}(I) >=< \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) >$ τότε αυτά παράγουν το ιδεώδες I, δηλ. $I =< g_1, \ldots, g_s >$.*

Η απόδειξη του Θεωρήματος 1.6 στηρίζεται στο Θεώρημα βάσης του Hilbert 1.3.

Ορισμός 1.8 (Βάση Groebner) *Εστω I ένα ιδεώδες του $K[X_1, \ldots, X_n]$ και έστω ότι διαλέγουμε μια μονωνυμική διάταξη. Ενα σύνολο πολυωνύμων $\{g_1, \ldots, g_s\}$ όπως στο παραπάνω Θεώρημα 1.6 λέγεται βάση Groebner του ιδεώδους I.*

Σημειώνουμε ότι το σύνολο $\{f_1, f_2\}$ του παραδείγματος της Σημείωσης 1.4 δεν είναι βάση Groebner του αντίστοιχου ιδεώδους. Εστω I ένα ιδεώδες του $K[X_1, \ldots, X_n]$, διαλέγουμε μια μονωνυμική διάταξη, και έστω $\{g_1, \ldots, g_s\}$ μια βάση Groebner του I. Εστω $f \in K[X_1, \ldots, X_n]$. Οι βασικές ιδιότητες της βάσης Groebner είναι οι εξής:

1. Το υπόλοιπο της διαίρεσης του f με τα $g_1, \ldots, g_s$ δεν εξαρτάται από την διάταξη των $\{g_1, \ldots, g_s\}$, δηλ. είναι ουσιαστικά μοναδικό.
2. Το $f \in I$, αν και μόνον αν, το παραπάνω υπόλοιπο είναι μηδέν.

Επομένως έχοντας διαλέξει μια βάση Groebner για το ιδεώδες I μπορούμε να κάνουμε φυσιολογικά διαίρεση και επίσης να αποφασίσομε πότε ενα πολυώνυμο ανήκει στο I. Από το Θεώρημα 1.6 γνωρίζουμε ότι κάθε ιδεώδες του $K[X_1, \ldots, X_n]$ έχει μια βάση Groebner. Ενα πρώτο ερώτημα που φυσιολογικά τίθεται είναι πώς μπορούμε να αναγνωρίσουμε αν ένα δοσμένο σύνολο γεννητόρων του ιδεώδους είναι βάση Groebner. Ενα δεύτερο ερώτημα ειναι να κατασκευάσουμε μια βάση Groebner για ένα δοσμένο ιδεώδες. Το Θεώρημα 1.7 παρακάτω δίδει ένα κριτίριο που απαντάει στο πρώτο ερώτημα. Απάντηση στο δεύτερο ερώτημα δίδει ο αλγόριθμος του Buchberger.

Θα δώσουμε πρώτα έναν ορισμό.

Ορισμός 1.9 *Εστω $f, g \in K[X_1, \ldots, X_n]$ μη μηδενικά πολυώνυμα.*

1. *Αν $\mathrm{multideg}(f) = a = (a_1, \ldots, a_n)$ και $\mathrm{multideg}(g) = b = (b_1, \ldots, b_n)$, τότε έστω $c = (c_1, \ldots, c_n)$, όπου $c_i = \max(a_i, b_i)$. Καλούμε το $X_1^{c_1} \cdots X_n^{c_n}$ το ελάχιστο κοινό πολλαπλάσιο των $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ και το συμβολίζουμε με $\mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$.*
2. *Το S-πολυώνυμο των f και g ορίζεται ως*

$$S(f,g) := \frac{X_1^{c_1} \cdots X_n^{c_n}}{\mathrm{LT}(f)}\, f - \frac{X_1^{c_1} \cdots X_n^{c_n}}{\mathrm{LT}(g)}\, g.$$

Παράδειγμα 1.7 Εστω $f = x^3y^2 - x^2y^3$ και $g = 3x^4y + y^2$ με την grlex διάταξη. Τότε $\mathrm{multideg}(f) = (3,2)$, $\mathrm{multideg}(g) = (4,1)$ άρα $c = (4,2)$ και επομένως $X^c = x^4y^2$. Επίσης, $\mathrm{LT}(f) = x^3y^2$, $\mathrm{LT}(g) = 3x^4y$ και παίρνουμε

$$S(f,g) = \frac{x^4y^2}{x^3y^2}\,(x^3y^2 - x^2y^3) - \frac{x^4y^2}{3x^4y}\,(3x^4y + y^2) = -x^3y^3 + x^2 - \frac{1}{3}y^3.$$

Θεώρημα 1.7 (Κριτίριο για βάση Groebner) *Εστω I ένα ιδεώδες του $K[X_1, \ldots, X_n]$ και διαλέγουμε μια μονωνυμική διάταξη. Τότε ένα σύστημα γεννητόρων $G = \{g_1, \ldots, g_s\}$του I είναι βάση Groebner του I, αν και μόνον αν, για όλα τα $i \neq j$ το υπόλοιπο της διαίρεσης του $S(g_i, g_j)$ με τα πολυώνυμα του G (ως προς κάποια διάταξη) είναι μηδέν.*

Παράδειγμα 1.8 Αν $I =< y - x^2, z - x^3 >$ το σύστημα γεννητόρων $G = \{y - x^2, z - x^3\}$ του I είναι βάση Groebner με την λεξικογραφική διάταξη διότι $S = S(y - x^2, z - x^3) = -zx^2 + yx^3$ και η διαίρεση του S με τα $f_1 = y - x^2,\ f_2 = z - x^3$ δίδει υπόλοιπο μηδέν.

Παράδειγμα 1.9 Αναφερόμενοι στο παράδειγμα της Σημείωσης 1.4 γνωρίζουμε ότι το σύστημα γεννητόρων $f_1 = x^3 - 2xy$ και $f_2 = x^2y - 2y^2 + x$ του ιδεώδους $I =< f_1, f_2 >$ δεν είναι βάση Groebner του I διότι $x^2 \notin < x^3, x^2y >$ και $x^2 \in I$ με $\mathrm{LT}(x^2) = x^2$. Αυτό επιβεβαιώνεται από το παραπάνω κριτίριο διότι $S(f_1, f_2) = -x^2$ και η διαίρεση του $-x^2$ με τα f_1, f_2 (με οποιαδήποτε διάταξη) δεν δίδει υπόλοιπο μηδέν.

Ο αλγόριθμος του Buchberger: Δοσμένου ιδεώδους I του $K[X_1, \ldots, X_n]$ και μιας μονωνυμικής διάταξης, ο αλγόριθμος του Buchberger παράγει μιά βάση Groebner του ιδεώδους I. Η ιδέα είναι να αρχίσουμε από ένα σύστημα γεννητόρων του I και να προσθέτουμε διαδοχικά όλα τα S-πολυώνυμα των στοιχείων του συστήματος γεννητόρων, ελέγχοντας αν το υπόλοιπο της διαίρεσης είναι μηδέν, οπότε τελικα στηριζόμενοι στο Θεώρημα 1.7 να παράγουμε μια βάση Groebner.

Παράδειγμα 1.10 Θα εφαρμόσουμε τον παραπάνω αλγόριθμο στο ιδεώδες του παραδείγματος 1.9 διαλέγοντας την grlex διάταξη. Αρχίζουμε από το δοσμένο σύστημα γεννητόρων $G = \{f_1 = x^3 - 2xy,\ f_2 = x^2y - 2y^2 + x\}$. Το $f_3 := S(f_1, f_2) = -x^2$ το οποίο δεν αφήνει υπόλοιπο μηδεν με τα πολυώνυμα του G, άρα διευρύνουμε το G σε $G_1 = \{f_1, f_2, f_3\}$. Το $S(f_1, f_2) = f_3$ αφήνει υπόλοιπο μηδεν με το G_1 όμως το $f_4 := S(f_1, f_3) = -2xy$ δεν αφήνει υπόλοιπο μηδεν με τα πολυώνυμα G_1. Επομένως διευρύνουμε σε $G_2 = \{f_1, f_2, f_3, f_4\}$. Τα $S(f_1, f_2) = f_3,\ S(f_1, f_3) = f_4$ όπως, επίσης, και το $S(f_1, f_4) = -2xy^2 = yf_4$ αφήνουν υπόλοιπο μηδεν με τα πολυώνυμα του G_2. Ομως το $f_5 := S(f_2, f_3) = -2y^2 + x$ δεν αφήνει υπόλοιπο μηδεν με τα πολυώνυμα του G_2. Διευρύνουμε πάλι σε $G_3 = \{f_1, f_2, f_3, f_4, f_5\}$ το οποίο ικανοποιεί το κριτίριο του Θεωρήματος 1.7 και επομένως το σύστημα γεννητόρων

$$\{x^3 - 2xy,\ x^2y - 2y^2 + x,\ -x^2,\ -2xy,\ -2y^2 + x\}$$

είναι βάση Groebner του I.

Ενα ιδεώδες επιδέχεται πολλές βάσεις Groebner. Για να επιτύχουμε μοναδικότητα, τις κανονικοποιούμε ως εξής.

Ορισμός 1.10 (reduced βάση Groebner) *Μια reduced βάση Groebner για ένα ιδεώδες πολυωνύμων I είναι μια βάση Groebner G του I που ικανοποιεί τις παρακάτω ιδιότητες.*
1. $LC(f) = 1$, για κάθε $f \in G$.
2. Για κάθε $f \in G$, κανένα από τα μονώνυμα του f δεν ανήκει στο ιδεώδες $< \mathrm{LT}(G - \{f\}) >$.

Ισχύει το παρακάτω θεώρημα.

Θεώρημα 1.8 *Εστω $I \neq 0$ ένα ιδεώδες πολυωνύμων. Τότε για κάθε μονωνυμική διάταξη υπάρχει μοναδική reduced βάση Groebner.*

Εχοντας μιά βάση Groebner για ένα ιδέωδες I μπορούμε να κατασκευάσουμε μια reduced βάση Groebner στηριζόμενοι στην παρακάτω πρόταση, που είναι απλό πόρισμα του Θεωρήματος 1.6.

Πρόταση 1.1 *Εστω G μια βάση Groebner ενός ιδεώδους I. Εστω $f \in G$ ένα στοιχείο της βάσης τέτοιο ώστε $\mathrm{LT}(f) \in < \mathrm{LT}(G - \{f\}) >$. Τότε το $G - \{f\}$ είναι μια βάση Groebner του ιδεώδους I.*

Παράδειγμα 1.11 Αναφερόμενοι στο παράδειγμα 1.10, για να παράξουμε μια reduced βάση Groebner πολλαπλασιάζουμε πρώτα κάθε εξίσωση με κατάλληλη σταθερά ώστε ο οδηγός συντελεστής να γίνει 1. Κατόπιν εφαρμόζουμε την παραπάνω Πρόταση 1.1 και παρατηρούμε ότι οι δύο πρώτες εξισώσεις μπορεί να παραλειφθούν και έτσι παίρνουμε ως reduced βάση Groebner την

$$\{x^2,\ xy,\ y^2 - \frac{1}{2}x\}.$$

Παρατηρήστε, επίσης, ότι χρησιμοποιώντας την παραπάνω βάση βλέπουμε ότι το αρχικό πολυωνυμικό σύστημα

$$\begin{aligned} x^3 - 2xy &= 0 \\ x^2y - 2y^2 + x &= 0, \end{aligned}$$

που αντιστοιχεί στο Παράδειγμα 1.9 είναι ισοδύναμο με το σύστημα

$$\begin{aligned} x^2 &= 0 \\ xy &= 0 \\ y^2 - \frac{1}{2}x &= 0, \end{aligned}$$

το οποίο πολύ εύκολα φαίνεται ότι έχει ως σύνολο λύσεων το $\{(0,0)\}$.

1.5 Επίλυση συστήματος πολυωνυμικών εξισώσεων

Η τελευταία παρατήρηση της προηγούμενης παραγράφου ουσιαστικά γενικεύεται και δίδει μια απάντηση στο πρόβλημα της επίλυσης συστημάτων πολυωνυμικών εξισώσεων. Ας πάρουμε πρώτα την γνωστή περίπτωση των γραμμικών πολυωνύμων. Γνωρίζουμε ότι για να επιλύσουμε το αντίστοιχο σύστημα πρέπει να εφαρμόσουμε την απαλλοιφή του Gauss και να πάρουμε την ανηγμένη μορφή του συστήματος η οποία λύνεται εύκολα με αντικατάσταση. Η παρατήρηση εδώ είναι ότι η διαδικασία της απαλλοιφής του Gauss συμπίπτει με την διαδικασία εύρεσης από μία δοσμένη βάση Groebner, ως προς την λεξικογραφική διάταξη, της αντίστοιχης reduced βάσης Groebner.

Παράδειγμα 1.12 Ας θεωρήσουμε το γραμμικό σύστημα

$$\begin{aligned} f_1 = 3x - 6y - 2z &= 0 \\ f_2 = 2x - 4y + 4w &= 0 \\ f_3 = x - 2y - z - w &= 0 \end{aligned}$$

Εφαρμόζουμε πρώτα τον αλγόριθμο του Buchberger για να βρούμε μια βάση Groebner του ιδεώδους $I =< f_1, f_2, f_3 >$ ως προς την λεξικογραφική διάταξη. Εχουμε

$$S(f_1, f_2) = \frac{x}{3x} f_1 - \frac{x}{2x} f_2 = -\frac{2}{3}z - 2w.$$

Το υπόλοιπο της διαίρεσης του $S(f_1, f_2)$ με τα πολυώνυμα $\{f_1, f_2, f_3\}$ είναι διάφορο του μηδενός, άρα θα πρέπει να διευρύνομε το σύνολο γεννητόρων με το $f_4 = -\frac{2}{3}z - 2w$. Συνεχίζουμε την διαδικασία.

$$\begin{aligned}
S(f_1, f_3) &= \frac{x}{3x} f_1 - \frac{x}{x} f_3 = \frac{1}{3}z + w = -\frac{1}{2} f_4, \text{ υπόλοιπο μηδέν .} \\
S(f_2, f_3) &= \frac{x}{2x} f_2 - \frac{x}{x} f_3 = z + 3w = -\frac{3}{2} f_4, \text{ υπόλοιπο μηδέν .} \\
S(f_1, f_4) &= \frac{xz}{3x} f_1 - \frac{xz}{-\frac{2}{3}z} f_4 = -3xw - 2yz - \frac{2}{3}z^2 = 3(y + \frac{1}{3}z) f_4 - w f_1, \text{ υπόλοιπο μηδέν .} \\
S(f_2, f_4) &= \frac{xz}{2x} f_2 - \frac{xz}{-\frac{2}{3}z} f_4 = -3xw - 2yz + 2wz = S(f_1, f_4) - z f_4, \text{ υπόλοιπο μηδέν .} \\
S(f_3, f_4) &= \frac{xz}{x} f_3 - \frac{xz}{-\frac{2}{3}z} f_4 = -3xw - 2yz - z^2 - wz = S(f_2, f_4) + \frac{3}{2} z f_4, \text{ υπόλοιπο μηδέν .}
\end{aligned}$$

Συνεπώς η βάση Groebner που παίρνουμε είναι η

$$\{f_1 = 3x - 6y - 2z, \;\; f_2 = 2x - 4y + 4w, \;\; f_3 = x - 2y - z - w, \;\; f_4 = \frac{-2}{3}z - 2w\}.$$

Εφαρμόζουμε τώρα την διαδικασία για την εύρεση της reduced βάσης Groebner. Πρώτα απ΄ όλα πολλαπλασιάζουμε κάθε όρο με κατάλληλη σταθερά ώστε ο οδηγός συντελεστής να είναι 1. Παίρνουμε ως νέα βάση Groebner την

$$\{g_1 = x - 2y - \frac{2}{3}z, \;\; g_2 = x - 2y + 2w, \;\; g_3 = x - 2y - z - w, \;\; g_4 = z + 3w\}.$$

Εχουμε $\mathrm{LT}(g_1) = x \in < \mathrm{LT}(g_2) = x, \;\; \mathrm{LT}(g_3) = x, \;\; \mathrm{LT}(g_4) = z >$ συνεπώς, από την Πρόταση 1.1, το βγάζουμε από την βάση. Επίσης, $\mathrm{LT}(g_2) = x \in < \mathrm{LT}(g_3) = x, \;\; \mathrm{LT}(g_4) = z >$, άρα το βγάζουμε και αυτό από την βάση. Επομένως έχουμε ως νέα βάση την

$$\{g_3 = x - 2y - z - w, \;\; g_4 = z + 3w\}.$$

Ο όρος $-z$ του g_3 ανήκει στο $< \mathrm{LT}(g_4) = z >$ και επομένως αντικαθιστούμε το g_3 με το $g_5 = g_3 + g_4 = x - 2y + 2w$ και έχουμε ως νέα βάση την

$$\{g_5 = x - 2y + 2w, g_4 = z + 3w\},$$

η οποία μπορούμε να δούμε ότι εναι μια reduced βάση Groebner. Επομένως το αρχικό σύστημα είναι ισοδύναμο με το

$$\begin{aligned} x - 2y + 2w &= 0 \\ z + 3w &= 0, \end{aligned}$$

το οποίο συμπίπτει με το σύστημα που προκύπτει από την απαλλοιφή του Gauss.

Τελειώνουμε παραθέτοντας ένα παράδειγμα επίλυσης ενός (μη γραμμικού) συστήματος πολυωνυμικών εξισώσεων.

Παράδειγμα 1.13 Θεωρούμε το σύστημα

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

Η reduced βάση Groebner που αντιστοιχεί στο παραπάνω σύστημα είναι η

$$\begin{aligned} f_1 &= w - \frac{3}{2}x - \frac{3}{2}yz - \frac{167616}{3835}z^6 - \frac{36717}{590}z^4 - \frac{134419}{7670}z^2, \\ f_2 &= x^2 + y^2 + z^2 - 1, \\ f_3 &= xy - \frac{19584}{3835}z^5 + \frac{1999}{295}z^3 - \frac{6403}{3835}z, \\ f_4 &= xz + yz^2 - \frac{1152}{3835}z^5 - \frac{108}{295}z^3 + \frac{2556}{3835}z, \\ f_5 &= y^3 + yz^2 - y - \frac{9216}{3835}z^5 + \frac{906}{295}z^3 - \frac{2562}{3835}z, \\ f_6 &= y^2z - \frac{6912}{3835}z^5 + \frac{827}{295}z^3 - \frac{3839}{3835}z, \\ f_7 &= yz^3 - yz - \frac{576}{59}z^6 + \frac{1605}{118}z^4 - \frac{453}{118}z^2, \\ f_8 &= z^7 - \frac{1763}{1152}z^5 + \frac{665}{1152}z^3 - \frac{11}{288}z. \end{aligned}$$

Αν και το αντίστοιχο σύστημα εξισώσεων είναι πολύ μεγαλύτερο από το αρχικό, παρατηρήστε όμως ότι είναι σε 'διαγώνιο' μορφη. Το λύνουμε αρχίζοντας από την τελευταία εξίσωση $f_8 = 0$, που περιλαμβάνει μία μόνο μεταβλητή, και προχωράμε προς τα πάνω με αντικατάσταση. Η εξίσωση $f_8 = 0$ έχει ως λύσεις τις

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

Αντικαθιστώντας, βρίσκουμε τις λύσεις του συστήματος (γράφουμε μόνον τις τιμές για τις μεταβλητές x, y, z διότι η τιμή της μεταβλητής w καθορίζεται μοναδικά από την

πρώτη εξίσωση $f_1 = 0$).

$$
\begin{array}{lll}
z = 0\,, & y = 0\,, & x = 1 \\
z = 0\,, & y = \pm 1\,, & x = 0 \\
z = \pm 1\,, & y = 0\,, & x = 0 \\
z = \frac{2}{3}\,, & y = \frac{1}{3}\,, & x = -\frac{2}{3} \\
z = -\frac{2}{3}\,, & y = -\frac{1}{3}\,, & x = -\frac{2}{3} \\
z = \frac{\sqrt{11}}{8\sqrt{2}}\,, & y = -\frac{3\sqrt{11}}{8\sqrt{2}}\,, & x = -\frac{3}{8} \\
z = -\frac{\sqrt{11}}{8\sqrt{2}}\,, & y = \frac{3\sqrt{11}}{8\sqrt{2}}\,, & x = -\frac{3}{8}\,.
\end{array}
$$