ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΟΜΕΑΣ ΑΛΓΕΒΡΑΣ ΚΑΙ ΓΕΩΜΕΤΡΙΑΣ

ΠΛΙΑΤΣΙΚΑ ΑΓΓΕΛΙΚΗ

ΠΟΛΥΠΛΟΚΟΤΗΤΑ ΒΑΣΕΩΝ MARKOV ΚΑΙ GRAVER

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΙΩΑΝΝΙΝΑ, 2013

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΟΜΕΑΣ ΑΛΓΕΒΡΑΣ ΚΑΙ ΓΕΩΜΕΤΡΙΑΣ

ΠΛΙΑΤΣΙΚΑ ΑΓΓΕΛΙΚΗ

ΠΟΛΥΠΛΟΚΟΤΗΤΑ ΒΑΣΕΩΝ MARKOV ΚΑΙ GRAVER

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΙΩΑΝΝΙΝΑ, 2013

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών, για την απόκτηση του Μεταπτυχιακού Διπλώματος Ειδίκευσης στα ΜΑΘΗΜΑΤΙΚΑ (Ανάλυση-Άλγεβρα-Γεωμετρία), που απονέμει το Τμήμα Μαθηματικών του Πανεπιστημίου Ιωαννίνων, υπό την επίβλεψη του **Καθηγητή κ. Απόστολου Θωμά**.

Τριμελής Επιτροπη Κρισης

Θωμά Απόστολος, Καθηγητής του Τμήματος Μαθηματικών του Πανεπιστημίου Ιωαννίνων
(Επιβλέπων Καθηγητής)

Κεχαγιάς Επαμεινώνδας, Αναπληρωτής Καθηγητής του Τμήματος Μαθηματικών του Πανεπιστημίου Ιωαννίνων

Μπεληγιάννης Απόστολος, Αναπληρωτής Καθηγητής του Τμήματος Μαθηματικών του Πανεπιστημίου Ιωαννίνων

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ

Δηλώνω υπεύθυνα ότι η παρούσα διατριβή εκπονήθηκε κάτω από τους διεθνείς ηθικούς και ακαδημαϊκούς κανόνες δεοντολογίας και προστασίας της πνευματικής ιδιοκτησίας. Σύμφωνα με τους κανόνες αυτούς, δεν έχω προβεί σε ιδιοποίηση ξένου επιστημονικού έργου και έχω πλήρως αναφέρει τις πηγές που χρησιμοποίησα στην εργασία αυτή.

ΑΦΙΕΡΩΝΕΤΑΙ ΣΤΗΝ ΑΓΑΠΗΜΕΝΗ ΜΟΥ ΟΙΚΟΓΕΝΕΙΑ

Περιεχόμενα

Περιεχόμενα

Εισαγωγή **1**

1 Βάσεις Gröbner **5**
1.1 Πολυωνυμικοί δακτύλιοι και Ιδεώδη 6
1.2 Διατάξεις όρων και Λήμμα Dickson 12
1.3 Διαίρεση πολυωνύμων και Βάσεις Gröbner 19
1.4 S−πολυώνυμα και ανάγωγες βάσεις Gröbner 23
1.5 Καθολικές Βάσεις Gröbner 29

2 Τορικά Ιδεώδη και βάσεις Graver **39**
2.1 Τορικά Ιδεώδη 39
2.2 Καθολικές Βάσεις Gröbner για Τορικά Ιδεώδη 45
2.3 Πίνακας Lawrence $A^{(2)}$ 59

3 Βάσεις Markov **71**
3.1 Βάση Markov 71

4 Πολυπλοκότητα Graver και Markov **83**
4.1 Πίνακας Lawrence $A^{(r)}$ 83
4.2 Πολυπλοκότητα Graver 87
4.3 Η βάση Graver της βάσης Graver 99

Βιβλιογραφία **109**

Περιεχόμενα

Πρόλογος 1

1 Μοντέλο Cobham 5
1.1 Πολυπλοκότητα ... 5
1.2 Μοντέλο ... 12
1.3 ... 15
1.4 ... 19
1.5 ... 29

2 Τομικά θεωρήματα των μοντέλων Cobham 39
2.1 Τομικά θεωρήματα ... 39
2.2 ... 45
2.3 ... 59

3 Μοντέλο Μορλέυ 71
3.1 ... 71

4 Πεπερασμένα μοντέλα του Μορλέυ 83
4.1 ... 83
4.2 ... 87
4.3 ... 99

Βιβλιογραφία 109

Εισαγωγή

Η συνδυαστική μεταθετική άλγεβρα είναι τομέας της άλγεβρας και τα τελευταία χρόνια χρησιμοποιείται στην αλγεβρική στατιστική. Η αλγεβρική στατιστική ασχολείται με την ανάπτυξη τεχνικών της αλγεβρικής γεωμετρίας, και της συνδυαστικής μεταθετικής άλγεβρας για την αντιμετώπιση προβλημάτων στον τομέα της στατιστικής. Η άλγεβρα παρέχει ένα ισχυρό σύνολο εργαλείων για την αντιμετώπιση των προβλημάτων στατιστικής. Ωστόσο, είναι σπάνια η περίπτωση όπου οι αλγεβρικές τεχνικές είναι έτοιμες για την αντιμετώπιση των στατιστικών προκλήσεων, και συνήθως νέα αλγεβρικά αποτελέσματα πρέπει να αναπτυχθούν. Με αυτό τον τρόπο ο διάλογος μεταξύ άλγεβρας και στατιστικής οφελεί και τους δύο κλάδους. Η αλγεβρική στατιστική είναι ένα σχετικά νέο πεδίο που έχει εξελιχθεί μάλλον γρήγορα κατά τη διάρκεια των τελευταίων δεκαπέντε ετών. Μία από τις πρώτες εργασίες στον τομέα αυτό είναι το άρθρο των Diaconis-Sturmfels [5], στο οποίο εισήγαγαν την έννοια της βάσης Markov για λογαριθμικά-γραμμικά στατιστικά μοντέλα και έδειξαν τη σύνδεση της προς τη συνδυαστική μεταθετική άλγεβρα. Από εκεί και πέρα, η σύνδεση άλγεβρας και στατιστικής έχει εξαπλωθεί σε διάφορους τομείς με εκατοντάδες ερευνητικές δημοσιεύσεις και αρκετά βιβλία όπως [6], [14], [15].
Στην παρούσα διατριβή το ενδιαφέρον μας στρέφεται γύρω από τις βάσεις Markov και Graver με σκοπό την απόδειξη ενός θεωρήματος των F.Santos και B.Sturmfels που αφορά την πολυπλοκότητα των βάσεων αυτών και αποδεικνύει ότι η πολυπλοκότητα είναι πεπερασμένη. Για να επιτύχουμε όμως το σκοπό μας θα αντλήσουμε τις απαραίτητες πληροφορίες από διαφορετικά σύνολα όπως ενδεικτικά είναι οι βάσεις Gröbner και οι βάσεις Hilbert.
Στο πρώτο κεφάλαιο το ενδιαφέρον μας επικεντρώνεται στις βάσεις Gröbner και σε αποτελέσματα που σχετίζονται με αυτές. Οι βάσεις Gröbner είναι ένα σύνολο πολυωνύμων πολλών μεταβλητών με επιθυμητές αλγοριθμικές ιδιότητες. Η ιδέα αυτών έχει πρωτοεμφανιστεί σε άρθρα που γράφτηκαν το 1900 από τον διάσημο μαθηματικό Paul Gordan. Ωστόσο, ο Bruno Buchberger ήταν ο πρώτος που έδωσε έναν αλγόριθμο για τον υπολογισμό τους και ανέπτυξε τη θεωρία αυτού που το 1976 προς τιμήν του καθηγητή του ονόμασε βάσεις Gröbner. Ωστόσο το 1964 μία παρόμοια ιδέα για τους τοπικούς δακτυλίους αναπτύχθηκε από τον Heisuke Hironaka στα άρθρα του [9],[10], και τις ονόμασε κανονικές βάσεις (standard bases). Στο κεφάλαιο αυτό λοιπόν παρουσιάζουμε δύο γνωστά θεωρήματα το θεώρημα βάσης Hilbert, το οποίο αποδεικνύουμε με τη βοήθεια των βάσεων Gröbner, και το λήμμα του Dickson. Ορίζουμε τη διάταξη όρων του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$, τη διαίρεση πολυωνύμων και φτάνουμε στο επίκεντρο του πρώτου κεφαλαίου τις βάσεις Gröbner, τις οποίες υπολογίζουμε κάνοντας χρήση του αλγορίθμου Buchberger, βασικό εργαλείο του οποίου αποτελούν τα S−πολυώνυμα. Ολοκληρώνουμε το κεφάλαιο παρουσιάζοντας ένα πεπερασμένο υποσύνολο του

ιδεώδους I, τις καθολικές βάσεις Gröbner οι οποίες εισήχθηκαν από τον V. Weispfenning στο άρθρο [20] (1987) και τον Niels Schwartz στο άρθρο [18] (1988), και σημαντικά συμπεράσματα που σχετίζονται με αυτές.
Στο δεύτερο κεφάλαιο βασικό μας εργαλείο αποτελούν τα διωνυμικά ιδεώδη και κυρίως μια ειδική κατηγορία αυτών, τα τορικά ιδεώδη τα οποία είναι απαραίτητα για τον ορισμό πολύ σημαντικών εννοιών όπως οι βάσεις Graver. Οι βάσεις Graver είναι πολύ σημαντικές στα εφαρμοσμένα μαθηματικά και η σύνδεση τους με τη θεωρία των βάσεων Gröbner περιγράφεται στο βιβλίο [19] του B.Sturmfels. Η θεωρία αλγορίθμων των βάσεων Graver και η εφαρμογή τους στον ακέραιο προγραμματισμό περιγράφεται στα βιβλία [12] και [13] του Shmuel Onn. Ωστόσο οι βάσεις Graver είναι πολύ χρήσιμες όπως θα δούμε, εκτός από τον ακέραιο προγραμματισμό και στην άλγεβρα. Πολλά υποσύνολα διωνύμων του ιδεώδους όπως τα κυκλωμάτα, οι ανάγωγες βάσεις Gröbner, η καθολική βάση Gröbner, μια τουλάχιστον ελαχιστοτική βάση Markov, ανήκουν στη βάση Graver και την καθιστούν ιδιαίτερα σημαντική. Εισάγουμε μια έννοια που θα αναπτύξουμε αναλυτικά στο τέταρτο κεφάλαιο το Lawrence πίνακα $A^{(2)}$ αλλά συμβάλλει στο κεφάλαιο αυτό, στον υπολογισμό της βάσης Graver. Έπειτα αποδεικνύουμε ένα θεώρημα που εξασφαλίζει ότι η βάση Graver είναι πεπερασμένη ταυτίζοντας τη με τέσσερα σύνολα διωνύμων. Στη συνέχεια δίνουμε δύο διαφορετικούς αλγορίθμους υπολογισμού των βάσεων Graver. Ο πρώτος σχετίζεται με το θεώρημα που προαναφέραμε και ο δεύτερος με τις βάσεις Hilbert με τις οποίες ολοκληρώνουμε το κεφάλαιο.
Στο τρίτο κεφάλαιο αναπτύσσουμε τη θεωρία των βάσεων Markov. Στο κεφάλαιο αυτό παρουσιάζουμε το πολύ σημαντικό θεώρημα των P.Diakonis και B.Sturmfels το οποίο αποδεικνύει ότι οι βάσεις Markov είναι ισοδύναμες με ένα σύνολο γεννητόρων κάποιου τορικού ιδεώδους, [5]. Στη συνέχεια εισάγουμε την έννοια του ημισύμμορφου και του ισχυρά ημισύμμορφου αθροίσματος και παρατηρούμε πως το ισχυρά ημισύμμορφο άθροισμα σχετίζεται με την καθολική βάση Markov. Έπειτα παρουσιάζουμε ένα βασικό θεώρημα που θα μας χρειαστεί στην απόδειξη του θεωρήματος των F.Santos και B.Sturmfels στο τέταρτο κεφάλαιο, το οποίο συσχετίζει την $1-$νόρμα των συνόλων B και B^{σ}. Τέλος εισάγουμε την έννοια των αναντικατάστατων διωνύμων που προήλθαν από το ερώτημα της αλγεβρικής στατιστικής το οποίο ήταν η εύρεση μοναδικού ελαχιστοτικού συστήματος διωνυμικών γεννητόρων για ένα διωνυμικό ιδεώδες. Και βλέπουμε ποια σχέση συνδέει τα αναντικατάστατα διώνυμα των βάσεων Markov τόσο με το ημισύμμορφο άθροισμα διανυσμάτων του πυρήνα, όσο και με τα αναντικατάστατα διώνυμα των βάσεων Gröbner.
Φτάνουμε στο σημαντικότερο κεφάλαιο της διατριβής, το τέταρτο κεφάλαιο. Σκοπός μας είναι να παρουσιάσουμε το θεώρημα των F.Santos και B.Sturmfels, το οποίο σχετίζεται με τις πολυπλοκότητες Markov και Graver. Για το σκοπό αυτό ορίζουμε αρχικά το Lawrence πίνακα $A^{(r)}$, τις πολυπλοκότητες Markov και Graver και βλέπουμε ποια σχέση συνδέει τις δύο πολυπλοκότητες. Παρουσιάζουμε λήμματα και πορίσματα που συσχετίζουν στοιχεία της βάσης Graver του πίνακα $A^{(r)}$ με στοιχεία της βάσης Graver του πίνακα $A^{(s)}$, για $s > r$, και σύμμορφα αθροίσματα επί των διανυσμάτων τους. Ορίζουμε το διάνυσμα $\psi(\mathbf{u})$ και τη βάση Graver της βάσης Graver στην οποία ανήκει και παρουσιάζουμε ένα λήμμα που συνδέει τα στοιχεία της βάσης Graver με τα στοιχεία της βάσης Graver της βάσης Graver. Έτσι φτάνουμε στο σημαντικότερο θεώρημα της διατριβής, που αποδεικνύει ότι οι πολυπλοκότητες Markov και Graver είναι πεπερασμένες και ανεξάρτητες του r (που εμφανίζεται στον πίνακα $A^{(r)}$). Ολοκληρώνουμε το κεφάλαιο αποδεικνύοντας το θεώρημα το οποίο εξασφαλίζει ότι το άνω όριο της βάσης

Graver που βρήκαμε είναι το καλύτερο δυνατό.

Ευχαριστίες

Με μεγάλη μου χαρά θα ήθελα να ευχαριστήσω όλους αυτούς που με βοήθησαν για την εκπόνηση της μεταπτυχιακής μου διατριβής.
Αρχικά θα ήθελα να ευχαριστήσω την πολυαγαπημένη μου οικογένεια που από την αρχή ήταν στο πλευρό μου σε κάθε μου απόφαση. Η απέραντη στήριξη, η ανεξάντλητη αγάπη και η διαρκής συμπαράσταση σε όλες τις δυσκολίες με βοήθησαν ώστε να επιτύχω τους στόχους μου. Ένα μεγάλο λοιπόν ευχαριστώ στον μπαμπά μου Βαγγέλη, τη μαμά μου Αρετή την αδερφή μου Βασιλική και φυσικά στους παππούδες μου Φώτη και Βασιλική, Γεώργιο και Αγγελική και στην υπόλοιπη οικογένεια μου, που ήταν ανελλιπώς στο πλευρό μου.
Ένα μεγάλο ευχαριστώ και ευγνωμοσύνη οφείλω στον επιβλέποντα καθηγητή μου, Καθηγητή κ.Απόστολο Θωμά, του οποίου η συνεχής βοήθεια, συμπαράσταση, στήριξη και καθοδήγηση συνετέλεσαν στην ολοκλήρωση της μεταπτυχιακής μου διατριβής. Θα ήθελα ακόμη να τον ευχαριστήσω, διότι πέρα από πρότυπο καθηγητή αποτελεί και πρότυπο ανθρώπου.
Θα ήθελα επίσης να ευχαριστήσω τον υποψήφιο διδάκτορα Χρυσόστομο Ψαρουδάκη για την πολύτιμη βοήθεια του, τις συμβουλές και τη στήριξη του. Τον Χρήστο Όντι καθώς και όλα τα παιδιά που στάθηκαν στο πλευρό μου και με στήριξαν. Ακόμη, ευχαριστώ όλους τους καθηγητές που ο καθένας με το δικό του τρόπο ενθάρρυνε την προσπάθεια μου.
Τέλος οφείλω ένα μεγάλο ευχαριστώ στα άτομα που με την κατανόηση και την αγάπη τους με ενθάρρυναν και με στήριζαν κάθε στιγμή τον Κωνσταντίνο, τον Βαγγέλη, την Τάνια, τον Παύλο, τη Νάγια, και την Χριστίνα.

Κεφάλαιο 1

Βάσεις Gröbner

Σε αυτό το κεφάλαιο θα ασχοληθούμε με τις βάσεις Gröbner και τον υπολογισμό τους. Οι βάσεις Gröbner είναι ένα σύνολο πολυωνύμων πολλών μεταβλητών με επιθυμητές αλγοριθμικές ιδιότητες. Η ιδέα των βάσεων Gröbner έχει πρωτοεμφανιστεί σε άρθρα που γράφτηκαν το 1900 από τον διάσημο μαθηματικό Paul Gordan. Ωστόσο, ο Bruno Buchberger ήταν ο πρώτος που έδωσε έναν αλγόριθμο για τον υπολογισμό τους. Αφορμή στάθηκε ένα πρόβλημα που έθεσε το 1965 ο καθηγητής Wolfgang Gröbner στον τότε μαθητή του Bruno Buchberger. Θεωρούμε το δακτύλιο πολυωνύμων πάνω από ένα σώμα K, μόδιο ένα αυθαίρετο ιδεώδες. Το πρόβλημα ήταν η έρευση μιας βάσης για το δακτύλιο πηλίκο ως $K-$διανυσματικό χώρο. Στην προσπάθεια απάντησης σε αυτό το πρόβλημα, ο Bruno Buchberger ανέπτυξε τη θεωρία αυτού που αργότερα, το 1976, προς τιμήν του καθηγητή του ονόμασε βάσεις Gröbner. Ωστόσο μία παρόμοια ιδέα για τους τοπικούς δακτυλίους αναπτύχθηκε από τον Heisuke Hironaka το 1964 στα άρθρα του [9],[10], και τις ονόμασε κανονικές βάσεις (standard bases). Για τα άρθρα αυτά, του απονεμήθηκε το 1970 το Fields Medal η μεγαλύτερη διάκριση στα μαθηματικά.
Στις βάσεις Gröbner έγκειται η επίλυση προβλημάτων που ανακύπτουν τόσο στην Αλγεβρική Γεωμετρία όσο και στη Μεταθετική Άλγεβρα, όπως τα ακόλουθα:

- Το πρόβλημα απόφασης αν ένα πολυώνυμο ανήκει σε κάποιο ιδεώδες. Το τυχαίο πολυώνυμο $f \in K[x_1, ..., x_n]$ ανήκει στο ιδεώδες $I \subseteq K[x_1, ..., x_n]$;

- Το πρόβλημα εύρεσης πολυωνύμων $u_1, ..., u_s \in K[x_1, ..., x_n]$ ώστε όταν το πολυώνο f ανήκει στο ιδεώδες $I = \langle f_1, ..., f_s \rangle$ να γράφεται ως γραμμικός συνδυασμός των $f_1, ..., f_s$ με πολυωνυμικούς συντελεστές. Δηλαδή $f = u_1 f_1 + ... + u_s f_s$;

- Το πρόβλημα εύρεσης αντιπροσώπων για τα σύμπλοκα $f + I$ στο δακτύλιο πηλίκο $K[x_1, ..., x_n]/I$.

- Το πρόβλημα εύρεσης βάσης για τον $K-$διανυσματικό χώρο $K[x_1, ..., x_n]/I$.

- Το πρόβλημα απόφασης αν δύο ιδεώδη είναι ίσα ή διάφορα.

- Το πρόβλημα εύρεσης της τομής δύο ιδεωδών.

Στην αλγεβρική γεωμετρία και στην υπολογιστική μεταθετική άλγεβρα, οι βάσεις Gröbner είναι ένα ιδιαίτερο σύνολο γεννητόρων ενός ιδεώδους I σε έναν πολυωνυμικό δακτύλιο. Μπορούν να θεωρηθούν ως γενίκευση:

- του αλγορίθμου του Ευκλείδη για τον υπολογισμό του μέγιστου κοινού διαιρέτη πολλών μεταβλητών.

- της μεθόδου της απαλοιφής του Gauss για την επίλυση γραμμικών συστημάτων και

- διαφόρων μεθόδων του ακέραιου προγραμματισμού.

Ο αλγόριθμος του Buchberger είναι η πιο παλιά και η πιο γνωστή μέθοδος για τον υπολογισμό τους. Μάλιστα χάρη στο λήμμα του Dickson γνωρίζουμε πως ο αλγόριθμος του Buchberger τερματίζει. Επιπρόσθετα οι βάσεις Gröbner έχουν χρησιμοποιηθεί από ερευνητές στη ρομποτική, κωδικοποίηση, θεωρία ελέγχου, στατιστική, μοριακή βιολογία, κρυπτογραφία, υπεργεωμετρικές συναρτήσεις κ.α.

1.1 Πολυωνυμικοί δακτύλιοι και Ιδεώδη

Η ενότητα αυτή περιλαμβάνει βασικούς ορισμούς και βασικά θεωρήματα σχετικά με τη θεωρία των πολυωνυμικών δακτυλίων και τα ιδεώδη. Θεωρούμε το μεταθετικό δακτύλιο πολυωνύμων $K[x_1, \ldots, x_n]$ με συντελεστές από κάποιο σώμα K. Έστω $f(x_1, \ldots, x_n)$ ένα πολυώνυμο σε n μεταβλητές με συντελεστές από το σώμα K. Το πολυώνυμο f γράφεται ως πεπερασμένο άθροισμα όρων της μορφής $ax_1{}^{\alpha_1} \ldots x_n{}^{\alpha_n}$, όπου $a \in K$, $\alpha_i \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$, για κάθε $i = 1, \ldots, n$. Τα απλούστερα πολυώνυμα στον $K[x_1, \ldots, x_n]$ είναι τα μονώνυμα.

Ορισμός 1.1.1. ***Μονώνυμο*** *(monomial) M καλείται ένα πολυώνυμο του $K[x_1, \ldots, x_n]$ της μορφής $M = x_1{}^{\alpha_1} \ldots x_n{}^{\alpha_n}$, όπου $\alpha_1, \ldots, \alpha_n \in \mathbb{N}_0$ και συμβολίζεται με $x^{\mathbf{a}}$, όπου $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$.*

Το σύνολο των μονωνύμων του $K[x_1, \ldots, x_n]$ συμβολίζεται με $\mathbb{T}^n$. Δηλαδή,

$$\mathbb{T}^n = \{x_1{}^{\alpha_1} \ldots x_n{}^{\alpha_n}, \text{ όπου } \alpha_i \in \mathbb{N}_0, \text{ για κάθε } i = 1, \ldots, n\}.$$

Ο μεταθετικός δακτύλιος των πολυωνύμων $K[x_1, \ldots, x_n]$ είναι ένας K-διανυσματικός χώρος με βάση το σύνολο $\mathbb{T}^n$.

Ορισμός 1.1.2. *Ο φυσικός αριθμός $\alpha_1 + \ldots + \alpha_n$ καλείται* ***βαθμός μονωνύμου*** *(degree of the monomial) M και συμβολίζεται με $deg(M)$.*

Για παράδειγμα, ο βαθμός του μονωνύμου $x_1{}^3 x_2{}^7 x_3{}^2 x_4{}^5$ είναι

$$deg(x_1{}^3 x_2{}^7 x_3{}^2 x_4{}^5) = 3 + 7 + 2 + 5 = 17.$$

Ορισμός 1.1.3. *Ορίζουμε το* ***συσχετικό $n-$χώρο*** *(affine $n-$space)*

$$K^n = \{(a_1, \ldots, a_n) : \text{όπου } a_i \in K, \text{ για κάθε } i = 1, \ldots, n\}.$$

Για παράδειγμα αν $K = \mathbb{R}$, ο $K^n = \mathbb{R}^n$ είναι ο συνήθης Ευκλείδειος χώρος.

Ορισμός 1.1.4. *Ορίζουμε τη* ***συνάρτηση εκτίμησης*** *(evaluation function)*

$$f : K^n \to K$$

που καθορίζεται από ένα πολυώνυμο $f \in K[x_1, ..., x_n]$ *ως εξής:*

$$(a_1, ..., a_n) \mapsto f(a_1, ..., a_n), \text{ για κάθε } (a_1, ..., a_n) \in K^n.$$

Έχουμε λοιπόν δύο τρόπους να βλέπουμε ένα πολυώνυμο $f \in K[x_1, ..., x_n]$. Ο πρώτος, ως ένα τυπικό άθροισμα μονωνύμων του μεταθετικού δακτυλίου $K[x_1, ..., x_n]$, ο δεύτερος ως μια συνάρτηση από το K^n στο K. Η διπλή ιδιότητα των πολυωνύμων αποτελεί τη γέφυρα μεταξύ της άλγεβρας και της γεωμετρίας.

Ορισμός 1.1.5. *Έστω ένα πολυώνυμο* $f \in K[x_1, \ldots, x_n]$. *Το σύνολο των λύσεων της εξίσωσης* $f = 0$,

$$V(f) = \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0\} \subseteq K^n$$

καλείται ***ποικιλότητα*** *που ορίζεται από το πολυώνυμο* f *(variety of* f*).*

Γενικά,

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in K^n : f_i(a_1, \ldots, a_n) = 0, \text{ για κάθε } i = 1, \ldots, s\},$$

όπου $f_i \in K[x_1, \ldots, x_n]$, για κάθε $i = 1, \ldots, s$, παριστάνει το σύνολο των λύσεων του συστήματος $\{f_1 = 0, \ldots, f_s = 0\}$. Παρατηρούμε ότι

$$V(f_1, \ldots, f_s) = \bigcap_{i=1}^{s} V(f_i).$$

Για παράδειγμα, η ποικιλότητα $V(x^2 + y^2 - 1, x - 1) \subseteq \mathbb{R}^2$ είναι η τομή του κύκλου με εξίσωση $x^2 + y^2 = 1$ και της ευθείας με εξίσωση $x = 1$ που είναι το σημείο (1,0).

Επιπλέον, για ένα υποσύνολο S του $K[x_1, \ldots, x_n]$ έχουμε

$$V(S) = \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0, \text{ για κάθε } f \in S\}.$$

Ακολουθεί ο ορισμός ενός ιδεώδους του μεταθετικού δακτυλίου $K[x_1, \ldots, x_n]$.

Ορισμός 1.1.6. *Ένα μη κενό υποσύνολο* I *του μεταθετικού δακτυλίου* $K[x_1, \ldots, x_n]$ *καλείται* ***ιδεώδες*** *(ideal) του* $K[x_1, \ldots, x_n]$ *αν:*

- *Για κάθε* $f, g \in I$ *συνεπάγεται ότι* $f - g \in I$ *και*
- *Για κάθε* $f \in I$ *και* $h \in K[x_1, \ldots, x_n]$ *συνεπάγεται ότι* $hf \in I$

Ορισμός 1.1.7. *Ένα ιδεώδες* M *του* $K[x_1, \ldots, x_n]$ *καλείται* ***μεγιστοτικό ιδεώδες*** *αν* $M \neq K[x_1, \ldots, x_n]$ *και η σχέση* $M \subseteq I \subseteq K[x_1, \ldots, x_n]$ *συνεπάγεται πως* $M = I$ *ή* $I = K[x_1, \ldots, x_n]$.

Στη συνέχεια θα δώσουμε τον ορισμό του πεπερασμένα παραγόμενου ιδεώδους.

Ορισμός 1.1.8. *Ένα ιδεώδες I του $K[x_1,\dots,x_n]$ καλείται* ***πεπερασμένα παραγόμενο ιδεώδες*** *(finitely generated) αν υπάρχει υποσύνολο $\{f_1,\dots,f_s\}$ του I τέτοιο ώστε*

$$I=\{\sum_{i=1}^{s}u_if_i : u_i\in K[x_1,\dots,x_n],\ \text{για κάθε } i=1,\dots,s\}.$$

Τότε γράφουμε $I=\langle f_1,\dots,f_s\rangle$ και το σύνολο $\{f_1,\dots,f_s\}$ καλείται σύνολο γεννητόρων (generating set) του ιδεώδους I.

Στην ακόλουθη παρατήρηση, θα δούμε ποια σχέση συνδέει ένα πεπερασμένα παραγόμενο ιδεώδες με την ποικιλότητα του.

Παρατήρηση 1.1.9. Αν το ιδεώδες I είναι πεπερασμένα παραγόμενο, δηλαδή $I=\langle f_1,\dots,f_s\rangle$, τότε για την ποικιλότητα του ισχύει $V(I)=V(f_1,\dots,f_s)$.
Όπου $V(I)=\{(a_1,\dots,a_n)\in K^n : f(a_1,\dots,a_n)=0,\ \text{για κάθε } f\in I\}$.

Απόδειξη. Μια λύση του συστήματος πολυωνυμικών εξισώσεων

$$f=0, f\in I$$

είναι προφανώς λύση του συστήματος

$$f_1=0,\dots,f_s=0$$

αφού τα πολυώνυμα f_i ανήκουν στο ιδεώδες I για $i=1,\dots,s$. Άρα

$$V(I)\subseteq V(f_1,\dots,f_s).$$

Αντίστροφα έστω το πολυώνυμο f ανήκει στο ιδεώδες $I=\langle f_1,\dots,f_s\rangle$. Τότε υπάρχουν $u_i\in K[x_1,\dots,x_n]$ τέτοια ώστε $f=\sum_{i=1}^{s}u_if_i$. Αν λοιπόν $(a_1,\dots,a_n)$ είναι μια λύση του συστήματος

$$f_1=0,\dots,f_s=0$$

τότε είναι λύση και του συστήματος

$$f=0, f\in I$$

αφού $f=\sum_{i=1}^{s}u_if_i$. Άρα $V(f_1,\dots,f_s)\subseteq V(I)$. Συνεπώς $V(I)=V(f_1,\dots,f_s)$. □

Παρατήρηση 1.1.10. Ένα ιδεώδες μπορεί να έχει διαφορετικά σύνολα γεννητόρων με διαφορετικό πλήθος στοιχείων.

Για παράδειγμα στον πολυωνυμικό δακτύλιο $K[x,y]$ το ιδεώδες

$$\langle x+y,y\rangle=\langle x,y\rangle=\langle x+xy,x^2,y^2,y+xy\rangle.$$

Η επόμενη παρατήρηση, συνδέει ένα πεπερασμένα παραγόμενο ιδεώδες που παράγεται από δύο διαφορετικά σύνολα γεννητόρων, με την ποικιλότητα του.

Παρατήρηση 1.1.11. Έστω ότι έχουμε το ιδεώδες $I=\langle f_1,\dots,f_s\rangle=\langle f'_1,\dots,f'_t\rangle$ τότε ισχύει $V(f_1,\dots,f_s)=V(I)=V(f'_1,\dots,f'_t)$. Άρα το σύστημα πολυωνύμων

$$f_1=0,\dots,f_s=0$$

έχει τις ίδιες λύσεις με το σύστημα πολυωνύμων

$$f_1' = 0, \ldots, f_t' = 0.$$

Συνεπώς η ποικιλότητα καθορίζεται από το ιδεώδες κι όχι από το εκάστοτε σύνολο πολυωνυμικών εξισώσεων. Οπότε όταν έχουμε ένα "καλύτερο" σύνολο γεννητόρων για το ιδεώδες $I = \langle f_1, \ldots, f_s \rangle$, έχουμε και μια "καλύτερη" έκφραση για την ποικιλότητα $V(f_1, \ldots, f_s)$. Καλύτερο με την έννοια ότι το σύνολο γεννητόρων μας επιτρέπει να κατανοήσουμε την αλγεβρική δομή του ιδεώδους και τη γεωμετρική δομή της ποικιλότητας καλύτερα. Ένα τέτοιο λοιπόν "καλύτερο" σύνολο γεννητόρων για το ιδεώδες I, είναι και βάση Gröbner του ιδεώδους την οποία θα ορίσουμε και θα μελετήσουμε στη συνέχεια.

Ο Γερμανός μαθηματικός Hilbert (Καινιξβέργη(Πρωσία) 23 Ιανουαρίου 1862 - Γκέτινγκεν(Γερμανία) 14 Φεβρουαρίου 1943) αναγνωρίζεται ως ένας από τους πιο ισχυρούς μαθηματικούς όλου του κόσμου. Από αρκετούς θεωρείται ο σημαντικότερος μαθηματικός του 19ου και 20ου αιώνα. Η πιο γνωστή εργασία του περιλαμβάνει τα *Αξιώματα Χίλμπερτ* για τη γεωμετρία καθώς και την περιγραφή των *χώρων Χίλμπερτ* με εφαρμογές στην Κβαντομηχανική και στη Θεωρία Σχετικότητας. Η πρώτη δουλειά του Hilbert στις αναλλοίωτες συναρτήσεις τον οδήγησε το 1888 στο θεώρημα που σήμερα είναι γνωστό ως το θεώρημα βάσης του Hilbert. Το 1868 ο Paul Gordan απέδειξε το θεώρημα αυτό για διωνυμικές μορφές, χρησιμοποιώντας πολύπλοκη υπολογιστική προσέγγιση. Όσες προσπάθειες έγιναν για να γενικεύσουν τη μέθοδό του σε συναρτήσεις με περισσότερες από δύο μεταβλητές απέτυχαν λόγω του τεράστιου βαθμού δυσκολίας των υπολογισμών. Ο Hilbert κατάλαβε ότι ήταν απαραίτητο να ακολουθήσει άλλη πορεία. Έτσι οδηγήθηκε στο θεώρημα βάσης του Hilbert (Hilbert's basis theorem).

Θεώρημα 1.1.12. *(Θεώρημα Βάσης του Hilbert) Κάθε ιδεώδες I του $K[x_1, \ldots, x_n]$ είναι πεπερασμένα παραγόμενο. Δηλαδή, υπάρχουν πολυώνυμα $g_1, \ldots, g_t \in I$ τέτοια ώστε $I = \langle g_1, \ldots, g_t \rangle$.*

Την απόδειξη του Θεωρήματος Βάσης του Hilbert θα τη δούμε παρακάτω, όπου θα γίνει χρήση των βάσεων Gröbner.
Την ιδιότητα αυτή του δακτυλίου $K[x_1, \ldots, x_n]$, δηλαδή κάθε ιδεώδες του είναι πεπερασμένα παραγόμενο, την έχουν κι άλλοι δακτύλιοι. Οι δακτύλιοι αυτοί ονομάζονται δακτύλιοι Noether, τους οποίους ορίζουμε αμέσως μετά το θεώρημα που ακολουθεί.

Θεώρημα 1.1.13. *Έστω R ένας δακτύλιος. Οι ακόλουθες προτάσεις είναι ισοδύναμες:*
1) Κάθε μη κενό σύνολο ιδεωδών του R έχει μεγιστοτικό στοιχείο.
2) Κάθε αύξουσα ακολουθία ιδεωδών του R γίνεται τελικά σταθερή:

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset I_{n+1} \subset \ldots \subset I_N = I_{N+1} = \ldots = I_{N+l} = \ldots$$

3) Κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο.

Η απόδειξη του θεωρήματος αυτού βρίσκεται στο βιβλίο [3] των M.F. Atiyah και I.G. MacDonald.

Ορισμός 1.1.14. *Ένας δακτύλιος R λέγεται* ***δακτύλιος Noether*** *αν ισχύει μια από τις ακόλουθες ισοδύναμες προτάσεις:*
1) Κάθε μη κενό σύνολο ιδεωδών του R έχει μεγιστοτικό στοιχείο.
2) Κάθε αύξουσα ακολουθία ιδεωδών του R γίνεται τελικά σταθερή:

$$I_1 \subset I_2 \subset ... \subset I_n \subset I_{n+1} \subset ... \subset I_N = I_{N+1} = ... = I_{N+l} = ...$$

3) Κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο.

Οι δακτύλιοι αυτοί λέγονται δακτύλιοι Noether προς τιμή της μαθηματικού Emmy Noether.

Η Emmy Noether (Γερμανία(Ερλάνγκεν)23 Μαρτίου 1882-Μπριν Μορ 14 Απριλίου 1935) χαρακτηρίστηκε ως η σημαντικότερη γυναίκα στην ιστορία των μαθηματικών από πολλούς όπως P.Alexandrov, Hermann Weyl, Norbert Wiener. Οι επαναστατικές τεχνικές της Noether στην αφηρημένη άλγεβρα οδηγούν στην τέλεια μαθηματική διατύπωση της "θεωρίας της σχετικότητας", πρόσθεσε ο A.Einstein. Η Emmy σπούδασε μαθηματικά στο πανεπιστήμιο του Ερλάνγκεν όπου δίδασκε ο πατέρας της Max Noether, που ήταν κι αυτός μαθηματικός. Το 1907 δούλεψε υπό την επίβλεψη του P.Gordan, ενώ το 1915 προσκλήθηκε από τους D.Hilbert και F.Klein να συμμετάσχει στο μαθηματικό τμήμα στο πανεπιστήμιο του Γκέτινγκεν, ένα παγκοσμίως γνωστό ινστιτούτο μαθηματικής έρευνας. Το 1933 βρίσκεται στο Κολέγιο Μπριν Μορ, στην Πενσιλβάνια της Αμερικής. Το Ίδρυμα Ροκφέλερ χρηματοδοτεί τη συνεργασία της με το Ινστιτούτο Ανωτέρων Μελετών του Πρίνστον. Το 1935, βρίσκεται στο νοσοκομείο του Μπριν Μορ. Μετά από εγχείρηση, η Emmy πέφτει σε κώμα και πεθαίνει. Έφυγε αναπάντεχα, στο απόγειο της δημιουργικής της δύναμης. Ήταν πρωτοπόρος σε ένα πεδίο που θα αποτελούσε το μέλλον των μαθηματικών, στο εξής η άλγεβρα δεν θα ήταν ποτέ πια η ίδια. Η Emmy Noether είναι η μητέρα της σύγχρονης αφηρημένης άλγεβρας.

Σε αυτό το σημείο θα παρουσιάσουμε και θα αποδείξουμε το λήμμα του Dickson, το οποίο θα μας χρειαστεί για να αποδείξουμε ένα σημαντικό θεώρημα για τις διατάξεις όρων, τις οποίες θα δούμε αμέσως μετά. Ωστόσο πρέπει να τονίσουμε πως το λήμμα του Dickson αποτελεί το βασικό εργαλείο για την απόδειξη του θεωρήματος βάσης Hilbert η οποία βρίσκεται παρακάτω.
Θέτουμε $S = K[x_1, ..., x_n]$ ο πολυωνυμικός δακτύλιος πάνω από το σώμα K. Ένα μονωνυμικό ιδεώδες του S, είναι ένα ιδεώδες που γεννάται από μονώνυμα. Αυτή η κλάση ιδεωδών μας ενδιαφέρει, επειδή η θεωρία των βάσεων Gröbner ανάγει δύσκολους αλγεβρικούς υπολογισμούς, σε υπολογισμούς με μονωνυμικά ιδεώδη.

Ορισμός 1.1.15. *Ένα ιδεώδες I του $K[x_1, ..., x_n]$ λέγεται* ***μονωνυμικό ιδεώδες*** *αν υπάρχει υποσύνολο A του $\mathbb{N}^n$ τέτοιο ώστε το I να αποτελείται από όλα τα πολυώνυμα τα οποία είναι πεπερασμένα αθροίσματα της μορφής $\sum_{\mathbf{a}\in A} h_{\mathbf{a}} x^{\mathbf{a}}$, όπου $h_{\mathbf{a}} \in K[x_1, ..., x_n]$. Τότε γράφουμε $I = \langle x^{\mathbf{a}} : \mathbf{a} \in A \rangle$.*

Για παράδειγμα το $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle$ είναι μονωνυμικό ιδεώδες του $K[x, y]$, με $B = \{\mathbf{b}_1 = (4, 2), \mathbf{b}_2 = (3, 4), \mathbf{b}_3 = (2, 5)\} \subseteq \mathbb{N}^2$ και

$$I = \langle x^{\mathbf{b}_1}, x^{\mathbf{b}_2}, x^{\mathbf{b}_3} \rangle = \langle x^4y^2, x^3y^4, x^2y^5 \rangle.$$

Δίνονται δύο μονώνυμα $u = x_1^{a_1}...x_n^{a_n}$ και $v = x_1^{b_1}...x_n^{b_n}$ που ανήκουν στο S. Τότε το u διαιρεί το v αν ισχύει $a_i \leq b_i$ για κάθε $i = 1, ..., n$, στην περίπτωση αυτή

γράφουμε $u \setminus v$. Αφού το S είναι Περιοχή Μονοσήμαντης Ανάλυσης για κάθε δύο πολυώνυμα f και g του S, υπάρχει ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο των f, g. Έτσι έχουμε:

$$\text{μκδ}(u,v) = x_1^{min(a_1,b_1)} \ldots x_n^{min(a_n,b_n)}$$

$$\text{ΕΚΠ}(u,v) = x_1^{max(a_1,b_1)} \ldots x_n^{max(a_n,b_n)}$$

Ορισμός 1.1.16. *Έστω f ένα πολυώυυμο του S, τότε ορίζουμε το **στήριγμα του** f ως το σύνολο των μονωνύμων που εμφανίζονται στο πολυώνυμο f.*

Ο ακόλουθος χαρακτηρισμός μονωνυμικών ιδεωδών είναι πρωταρχικής σημασίας.

Θεώρημα 1.1.17. *Έστω $I \subset S$ ένα ιδεώδες. Τα ακόλουθα είναι ισοδύναμα:*

1. *Το I είναι μονωνυμικό ιδεώδες.*
2. *Για κάθε πολυώνυμο f που ανήκει στο I, το στήριγμα $supp(f)$ είναι υποσύνολο του ιδεώδους I.*

Απόδειξη. Έστω M το σύνολο των μονωνυμικών γεννητόρων του I κι έστω f ανήκει στο I. Τότε υπάρχουν μονώνυμα $u_1, ..., u_m$ που ανήκουν στο M και πολυώνυμα $f_1, ..., f_m$ που ανήκουν στο S, τέτοια ώστε $f = \sum_{i=1}^m f_i u_i$.
Συνεπώς $supp(f) \subseteq \bigcup_{i=1}^m supp(f_i u_i)$. Οπότε αν $u \in supp(f)$, τότε υπάρχει ένα $i = 1, ..., m$ τέτοιο ώστε $u \in supp(f_i u_i)$. Κάθε u που ανήκει στο $supp(f_i u_i)$ είναι της μορφής wu_i, συνεπώς $u = wu_i$ για κάποιο $i = 1, ..., m$ και για κάποιο μονώνυμο w του πολυωνύμου f_i, άρα το u ανήκει στο I.
Αντίστροφα έστω G το σύστημα γεννητόρων του I. Τότε το σύνολο $\bigcup_{f \in G} supp(f)$ περιέχεται στο I και είναι σύνολο μονωνυμικών γεννητόρων του I, δηλαδή $I = \langle \bigcup_{f \in G} supp(f) \rangle$. Αρχικά παρατηρούμε ότι $\langle \bigcup_{f \in G} supp(f) \rangle \subseteq I$, εφόσον $\{\bigcup_{f \in G} supp(f)\} \subseteq I$. Αρκεί να δείξουμε ότι $I \subseteq \langle \bigcup_{f \in G} supp(f) \rangle$. Έστω ένα πολυώνυμο $f \in I$. Το f γράφεται στη μορφή $f = \sum h_i f_i$, όπου τα πολυώνυμα $h_i \in K[x_1, \ldots, x_n]$, και $f_i \in G$.
Συνεπώς $supp(f) \subseteq \bigcup supp(f_i h_i) \subseteq \langle \bigcup_{f \in G} supp(f) \rangle$, άρα $f \in \langle \bigcup_{f \in G} supp(f) \rangle$ εφόσον το f γράφεται ως άθροισμα όρων των οποίων τα μονώνυμα ανήκουν στο ιδεώδες $\langle \bigcup_{f \in G} supp(f) \rangle$. Οπότε $I = \langle \bigcup_{f \in G} supp(f) \rangle$. □

Πόρισμα 1.1.18. *Έστω $I \subset S$ ένα μονωνυμικό ιδεώδες και M ένα σύνολο μονωνύμων του I. Τότε το M είναι ένα σύνολο γεννητόρων του I αν και μόνο αν για κάθε μονώνυμο $v \in I$ υπάρχει ένα μονώνυμο $u \in M$ τέτοιο ώστε $u \setminus v$.*

Απόδειξη. Υποθέτουμε ότι το M είναι σύνολο γεννητόρων του I. Έστω $v \in I$ ένα μονώνυμο. Τότε υπάρχουν μονώνυμα $u_1, ..., u_m$ που ανήκουν στο M και πολυώνυμα $f_1, ..., f_m$ που ανήκουν στο S, τέτοια ώστε $v = \sum_{i=1}^m f_i u_i$. Τότε το μονώνυμο $v \in \bigcup_{i=1}^m supp(f_i u_i)$ κι άρα $v \in supp(f_i u_i)$ για κάποιο $i = 1, ..., m$. Κάθε v που ανήκει στο $supp(f_i u_i)$ είναι της μορφής wu_i, συνεπώς $v = wu_i$ για κάποιο $i = 1, ..., m$ και για κάποιο μονώνυμο w του πολυωνύμου f_i. Άρα το $u_i \setminus v$.
Αντίστροφα έστω ότι για κάθε μονώνυμο $v \in I$, υπάρχει ένα μονώνυμο $u \in M$ τέτοιο ώστε $u \setminus v$. Έστω $f \in I$ ένα αυθαίρετο πολυώνυμο. Αφού το I είναι μονωνυμικό ιδεώδες από το θεώρημα 1.1.17 έχουμε ότι $supp(f) \subseteq I$. Έστω $supp(f) = \{v_1, ..., v_m\}$ και $f = \sum_{i=1}^m c_i v_i$, με $c_i \in K$. Από την υπόθεση λοιπόν έχουμε $v_i = w_i u_i$, με $u_i \in$ M και w_i μονώνυμα στο S. Άρα $f = \sum_{i=1}^m c_i w_i u_i$, δηλαδή το M γεννά το I. □

Δηλαδή το μονώνυμο $x^{\mathbf{b}}$ ανήκει στο μονωνυμικό ιδεώδες $I = \langle x^{\mathbf{a}} : \mathbf{a} \in A \rangle$ αν και μόνο αν το $x^{\mathbf{b}}$ διαιρείται από το $x^{\mathbf{a}}$ για κάποιο $\mathbf{a} \in A$.

1.2 Διατάξεις όρων και Λήμμα Dickson

Πλέον είμαστε έτοιμοι να ορίσουμε τις διατάξεις όρων στον πολυωνυμικό δακτύλιο $K[x_1, \ldots, x_n]$ και να αποδείξουμε το βασικό θεώρημα που σχετίζεται με αυτές.

Ορισμός 1.2.1. ***Μερική διάταξη*** *(partial order) σε ένα σύνολο S καλείται μία σχέση $\prec$ με τις εξής ιδιότητες:*

- *δεν ισχύει η σχέση $a \prec a$ για οποιοδήποτε $a \in S$ και*
- *αν $a_1 \prec a_2, a_2 \prec a_3$ τότε $a_1 \prec a_3$ για οποιαδήποτε $a_1, a_2, a_3 \in S$.*

Ορισμός 1.2.2. ***Ολική διάταξη*** *(total order) σε ένα σύνολο S καλείται μια μερική διάταξη $\prec$ όπου για οποιαδήποτε $a_1, a_2 \in S$ ισχύει ακριβώς μία από τις παρακάτω σχέσεις:*

$$a_1 \prec a_2 \text{ ή } a_1 = a_2 \text{ ή } a_1 \succ a_2.$$

Ορισμός 1.2.3. ***Διάταξη όρων*** *(term order) στον $K[x_1, \ldots, x_n]$ καλείται μία ολική διάταξη $\prec$ στο $\mathbb{T}^n$ με τις εξής ιδιότητες:*

1. *$1 \prec x^{\mathbf{b}}$ για κάθε μονώνυμο $x^{\mathbf{b}} \in T^n$ και $x^{\mathbf{b}} \neq 1$ και*
2. *αν $x^{\mathbf{b}_1} \prec x^{\mathbf{b}_2}$ τότε $x^{\mathbf{c}}x^{\mathbf{b}_1} \prec x^{\mathbf{c}}x^{\mathbf{b}_2}$ για κάθε μονώνυμο $x^{\mathbf{c}} \in \mathbb{T}^n$.*

Ακολουθεί μια πολύ χρήσιμη πρόταση σχετικά με τις διατάξεις όρων στον $K[x_1, \ldots, x_n]$.

Πρόταση 1.2.4. *Θεωρούμε μια διάταξη όρων $\prec$. Για μονώνυμα $x^{\mathbf{a}}, x^{\mathbf{b}} \in \mathbb{T}^n$, αν το $x^{\mathbf{a}}$ διαιρεί το $x^{\mathbf{b}}$ τότε ισχύει $x^{\mathbf{a}} < x^{\mathbf{b}}$ ή $x^{\mathbf{a}} = x^{\mathbf{b}}$.*

Απόδειξη. Υπάρχει ένα μονώνυμο $x^{\mathbf{c}} \in \mathbb{T}^n$ τέτοιο ώστε $x^{\mathbf{b}} = x^{\mathbf{a}}x^{\mathbf{c}}$, αφού $x^{\mathbf{a}} \backslash x^{\mathbf{b}}$. Από την πρώτη συνθήκη του ορισμού 1.2.3 έχουμε $x^{\mathbf{c}} \geq 1$ συνεπώς από τη δεύτερη συνθήκη του ίδιου ορισμού έχουμε $x^{\mathbf{a}}x^{\mathbf{c}} \geq x^{\mathbf{a}}$, άρα $x^{\mathbf{b}} \geq x^{\mathbf{a}}$, δηλαδή $x^{\mathbf{a}} < x^{\mathbf{b}}$ ή $x^{\mathbf{a}} = x^{\mathbf{b}}$. □

Στο δακτύλιο των πολυωνύμων $K[x_1, \ldots, x_n]$ για $n > 1$ υπάρχουν άπειρες διατάξεις όρων. Στη συνέχεια αναφέρουμε τέσσερις από αυτές.

Ορισμός 1.2.5. *Η **λεξικογραφική διάταξη** (lexicographic order) $\succ_{lex}$ στον $K[x_1, \ldots, x_n]$ με $x_1 > x_2 > \ldots > x_n$ ορίζεται ως εξής:*
Για $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{N}^n$, ισχύει $x^{\mathbf{a}} \succ_{lex} x^{\mathbf{b}}$ αν και μόνο αν η πρώτη μη μηδενική συντεταγμένη του $\mathbf{a} - \mathbf{b}$ είναι θετική.

Παράδειγμα 1.2.6. Στον $K[x, y]$ θεωρούμε τη λεξικογραφική διάταξη όρων $\succ_{lex}$, με $x > y$ έτσι έχουμε:
$1 < y < y^2 < y^3 < \ldots < y^k < \ldots$
$x < xy < xy^2 < xy^3 < \ldots < xy^k < \ldots$
$x^2 < x^2y < x^2y^2 < x^2y^3 < \ldots < x^2y^k < \ldots$
$x^m < x^my < x^my^2 < x^my^3 < \ldots < x^my^k < \ldots$

Παράδειγμα 1.2.7. Στον $K[x,y,z]$ θεωρούμε τη λεξικογραφική διάταξη όρων $\succ_{lex}$, με $z > y > x$ έχουμε:
$1 < x < x^2 < x^3 < ...$
$y < yx < yx^2 < ...$
$y^2 < y^2x < y^2x^2 < ...$
$y^3 < y^3x < y^3x^2 < ...$
...
$z < zyx < zyx^2 < ...$
$z^2 < z^2yx < z^2yx^2 < ...$

Ορισμός 1.2.8. *Η **βαθμωτή λεξικογραφική διάταξη** (degree lexicographic order) $\succ_{deglex}$ στον $K[x_1,\ldots,x_n]$ με $x_1 > x_2 > \ldots > x_n$ ορίζεται ως εξής:*
Για $\mathbf{a} = (a_1,\ldots,a_n), \mathbf{b} = (b_1,\ldots,b_n) \in \mathbb{N}^n$, ισχύει $x^{\mathbf{a}} \succ_{deglex} x^{\mathbf{b}}$ αν και μόνο αν $deg(x^{\mathbf{a}}) > deg(x^{\mathbf{b}})$ ή $deg(x^{\mathbf{a}}) = deg(x^{\mathbf{b}})$ και $x^{\mathbf{a}} \succ_{lex} x^{\mathbf{b}}$, δηλαδή η πρώτη μη μηδενική συντεταγμένη του $\mathbf{a} - \mathbf{b}$ είναι θετική.

Παράδειγμα 1.2.9. Στον $K[x,y]$ θεωρούμε τη λεξικογραφική διάταξη όρων $\succ_{deglex}$, με $x > y$ έχουμε:
$1 <$
$y < x <$
$y^2 < xy < x^2$
$y^3 < xy^2 < x^2y < x^3 <$
$y^m < xy^{m-1} < ... < x^{m-1}y < x^{m-1} <$

Παράδειγμα 1.2.10. Στον $K[x,y,z]$ θεωρούμε τη βαθμωτή λεξικογραφική διάταξη $\succ_{degrevlex}$, με $x > y > z$ έχουμε:
$1 < z < y < x < z^2 < yz < xz < y^2 < xy < x^2 <$
$z^3 < yz^2 < y^2z < y^3 <$
$xz^2 < xyz < xy^2 <$
$x^2z < x^2y < x^3 < ...$

Ορισμός 1.2.11. *Η **αντίστροφη βαθμωτή λεξικογραφική διάταξη** (degree reverse lexicographic order) $\succ_{degrevlex}$ στον $K[x_1,\ldots,x_n]$ με $x_1 > x_2 > \ldots > x_n$ ορίζεται ως εξής:*
Για $\mathbf{a} = (a_1,\ldots,a_n), \mathbf{b} = (b_1,\ldots,b_n) \in \mathbb{N}^n$, ισχύει $x^{\mathbf{a}} \succ_{degrevlex} x^{\mathbf{b}}$ αν και μόνο αν $deg(x^{\mathbf{a}}) > deg(x^{\mathbf{b}})$ ή $deg(x^{\mathbf{a}}) = deg(x^{\mathbf{b}})$ και η τελευταία μη μηδενική συντεταγμένη του $\mathbf{a} - \mathbf{b}$ είναι αρνητική.

Παράδειγμα 1.2.12. Στον $K[x,y,z]$ θεωρούμε την αντίστροφη βαθμωτή λεξικογραφική διάταξη $\succ_{degrevlex}$, με $x > y > z$ έχουμε:
$1 < z < y < x < z^2 < yz < xz < y^2 < xy < x^2 <$
$z^3 < yz^2 < xz^2 < y^2z < xyz < x^2z < y^3 <$
$xy^2 < x^2y < x^3 < ...$

Εύκολα προκύπτει ότι η βαθμωτή λεξικογραφική διάταξη και η αντίστροφη βαθμωτή λεξικογραφική διάταξη στον $K[x_1,x_2]$ ταυτίζονται. Αυτό δε συμβαίνει όμως για $n \geq 3$.

Παράδειγμα 1.2.13. Στον $K[x,y,z]$ θεωρούμε την αντίστροφη βαθμωτή λεξικογραφική διάταξη $\succ_{degrevlex}$, με $z > y > x$ έχουμε:
$z^4yx^4 \succ_{deglex} z^3y^3x^3$ ενώ $z^3y^3x^3 \succ_{degrevlex} z^4yx^4$.

Το πλήθος των τεσσάρων παραπάνω διατάξεων είναι $n!$ για κάθε μία από αυτές.

Υπάρχουν πολλών ειδών βαθμοί. Αλλάζοντας το βαθμό προκύπτουν άπειρες διατάξεις. Για παράδειγμα στον δακτύλιο $K[x,y]$ με κάθε διάνυσμα $\mathbf{c} = (c_1, c_2)$ ορίζουμε ένα βαθμό για το μονώνυμο $x^a y^b$. Δηλαδή $deg_{\mathbf{c}}(x^a y^b) = (c_1, c_2)(a, b) = c_1 a + c_2 b$.

Αν $\mathbf{c} = (1,1)$ τότε έχουμε το συνήθη βαθμό.

Αν $\mathbf{c_1} = (100\sqrt{7}, 1204)$ τότε ο βαθμός του μονωνύμου $x^a y^b$ είναι ο εξής:
$deg_{\mathbf{c_1}}(x^a y^b) = 100\sqrt{7}a + 1204b$.

Παρατηρούμε ότι με το βαθμό που ορίζεται από το διάνυσμα $\mathbf{c_1} = (100\sqrt{7}, 1204)$, κάθε μονώνυμο έχει διαφορετικό βαθμό. Πράγματι έστω τα μονώνυμα $x^a y^b, x^{a'} y^{b'}$ με $a, a', b, b' \in \mathbb{N}$.

Έστω

$$deg_{\mathbf{c_1}}(x^a y^b) = deg_{\mathbf{c_1}}(x^{a'} y^{b'})$$

τότε έχουμε

$$100\sqrt{7}a + 1204b = 100\sqrt{7}a' + 1204b'$$

άρα

$$100\sqrt{7}(a - a') = 1204(b' - b).$$

Διακρίνουμε περιπτώσεις:

1. Αν $a = a'$ τότε $b = b'$ άρα $(a, b) = (a', b')$.
2. Αν $a \neq a'$ τότε $\sqrt{7} = \frac{1204(b'-b)}{100(a-a')} \in \mathbb{Q}$ αφού $1204(b' - b) \in \mathbb{Z}, 100(a - a') \in \mathbf{Z}$.

Άρα $\sqrt{7} \in \mathbb{Q}$ άτοπο. Συνεπώς $a = a'$ και $b = b'$.

Το ίδιο συμβαίνει και με το βαθμό που ορίζεται από το διάνυσμα $\mathbf{c_2} = (37, \sqrt{2})$, δηλαδή δεν υπάρχουν διαφορετικά μονώνυμα που να έχουν τον ίδιο βαθμό. Ωστόσο οι δύο διατάξεις είναι διαφορετικές.

Θεωρούμε τα μονώνυμα $x^{10}y, y^5$. Είναι

$$deg_{\mathbf{c_1}}(x^{10}y) < deg_{\mathbf{c_1}}(y^5)$$

και

$$deg_{\mathbf{c_2}}(x^{10}y) > deg_{\mathbf{c_2}}(y^5).$$

Ορισμός 1.2.14. *Έστω X_1, X_2 μονώνυμα του πολυωνυμικού δακτύλιου $K[x_1, ..., x_n]$ και $\prec_x$ μία διάταξη όρων στις x μεταβλητές. Έστω Y_1, Y_2 μονώνυμα του πολυωνυμικού δακτύλιου $K[y_1, ..., y_m]$ και $\prec_y$ μία διαταξη όρων στις y μεταβλητές. Στον πολυωνυμικό δακτύλιο $K[x_1, ..., x_n, y_1, ..., y_m]$ ορίζουμε μια διάταξη όρων $\prec$ ως εξής:*

$$X_1 Y_1 \prec X_2 Y_2 \text{ αν και μόνο αν } X_1 \prec_x X_2 \text{ ή } X_1 = X_2 \text{ και } Y_1 \prec_y Y_2.$$

Η διαταξη αυτή καλείται ***διαταξη απαλοιφής*** *(elimination order) με τις x μεταβλητές μεγαλύτερες από τις y μεταβλητές.*

Παρατηρούμε πως η λεξικογραφική διάταξη είναι μια ειδική κατηγορία της διάταξης απαλοιφής. Στο σημείο αυτό είμαστε σε θέση να αποδείξουμε το πολύ σηματικό λήμμα του Dickson. Να θυμίσουμε ότι η μερική διάταξη που ορίζεται από τη διαιρετότητα είναι αυτή για την οποία ισχύει $x^{\mathbf{a}} \leq x^{\mathbf{b}}$ αν το $x^{\mathbf{a}}$ διαιρεί το $x^{\mathbf{b}}$.

Θεώρημα 1.2.15. *(Λήμμα του Dickson) Έστω M ένα μη κενό σύνολο μονωνύμων στο S. Το σύνολο M έχει μόνο ένα πεπερασμένο αριθμό ελαχιστοτικών στοιχείων ως προς τη μερική διάταξη που ορίζεται από τη διαιρετότητα.*

Απόδειξη. Θα αποδείξουμε το θεώρημα μέσω της επαγωγής στο n, τον αριθμό των μεταβλητών του S.
Αν $n = 1$, τότε το σύνολο M αποτελείται από κάποιες δυνάμεις του x_1 και το σύνολο των ελαχιστοτικών στοιχείων του M είναι το $\{x_1^a\}$, όπου a ο μικρότερος αριθμός για τον οποίο το μονώνυμο x_1^a ανήκει στο M. Τα υπόλοιπα στοιχεία του M, είναι πολλαπλάσια του x_1^a.
Αν $n > 1$, τότε ορίζουμε N το σύνολο των μονωνύμων $x^{\mathbf{c}}$ του πολυωνυμικού δακτυλίου $K[x_1, ..., x_{n-1}]$, τέτοια ώστε $x^{\mathbf{c}}x_n^d \in \mathbf{M}$, για $d \geq 0$. Δηλαδή
$N = \{x^{\mathbf{c}} \in K[x_1, ..., x_{n-1}] / x^{\mathbf{c}}x_n^d \in \mathbf{M}$, για κάποιο $d \geq 0\}$. Λόγω της υπόθεσης επαγωγής, γνωρίζουμε ότι το σύνολο N^{min} των ελαχιστοτικών στοιχείων του N, είναι πεπερασμένο. Έστω $N^{min} = \{x^{\mathbf{c}_1}, ..., x^{\mathbf{c}_r}\}$ για κάθε $x^{\mathbf{c}_i} \in N^{min}$, υπάρχει $a_i \geq 0$ τέτοιο ώστε $x^{\mathbf{c}_i}x_n^{a_i}$ να ανήκει στο M. Έστω $a = max\{a_1, ..., a_r\}$ και $0 \leq b < a$. Ορίζουμε το σύνολο $N_b = \{x^{\mathbf{c}} \in K[x_1, ..., x_{n-1}] / x^{\mathbf{c}}x_n^b \in \mathbf{M}\}$. Λόγω της υπόθεσης επαγωγής, γνωρίζουμε ότι το σύνολο N_b^{min} των ελαχιστοτικών στοιχείων του N_b, είναι πεπερασμένο.
Θα δείξουμε ότι $\mathbf{M}^{min} \subseteq \{x^{\mathbf{c}_1}x_n^{a_1}, ..., x^{\mathbf{c}_r}x_n^{a_r}\} \bigcup (\bigcup_{b=0}^{a-1} N_b^{min}x_n^b)$.
Έστω $x^{\mathbf{u}}$ ανήκει στο $\mathbf{M}^{min}$ και $x^{\mathbf{u}} = x^{\mathbf{c}}x_n^l$, με $l \geq 0$. Διακρίνουμε περιπτώσεις για το l.

1. Έστω ότι $l \geq a$. Τότε το $x^{\mathbf{u}} = x^{\mathbf{c}}x_n^l$, όπου $x^{\mathbf{c}} \in N$. Συνεπώς υπάρχει ένα $\mathbf{c_i} \in \{\mathbf{c_1}, ..., \mathbf{c_r}\}$, τέτοιο ώστε $\mathbf{c} \geq \mathbf{c_i}$. Άρα από τη μερική διάταξη που δίνεται από τη διαιρετότητα, έχουμε ότι $x^{\mathbf{c}_i} \setminus x^{\mathbf{c}}$. Ακόμη, εφόσον $l \geq a \geq a_i$, δηλαδή $l \geq a_i$ για κάθε $i = 1, ..., r$, από τη μερική διάταξη που δίνεται από τη διαιρετότητα, έχουμε ότι $x_n^{a_i} \setminus x_n^l$. Συνεπώς $x^{\mathbf{c}_i}x_n^{a_i} \setminus x^{\mathbf{c}}x_n^l = x^{\mathbf{u}}$. Δηλαδή $x^{\mathbf{c}_i}x_n^{a_i} \setminus x^{\mathbf{u}}$ και $x^{\mathbf{c}_i}x_n^{a_i}$ ανήκει στο M. Αφού το $x^{\mathbf{u}}$ ανήκει στο $\mathbf{M}^{min}$ είναι ελαχιστοτικό στοιχείο του M, τίποτα δεν μπορεί να το διαιρεί εκτός από τον ευατό του. Άρα $x^{\mathbf{u}} = x^{\mathbf{c}_i}x_n^{a_i} \in \{x^{\mathbf{c}_1}x_n^{a_1}, ..., x^{\mathbf{c}_r}x_n^{a_r}\}$.

2. Έστω ότι $l < a$. Τότε το $x^{\mathbf{u}} = x^{\mathbf{c}}x_n^l$, όπου $x^{\mathbf{c}} \in N_l = \{x^{\mathbf{c}} \in K[x_1, ..., x_{n-1}] / x^{\mathbf{c}}x_n^l \in \mathbf{M}\}$. Λόγω της υπόθεσης επαγωγής, γνωρίζουμε ότι το σύνολο N_l^{min} των ελαχιστοτικών στοιχείων του N_l, είναι πεπερασμένο. Έστω $N_l^{min} = \{x^{\mathbf{c}_{l_1}}, ..., x^{\mathbf{c}_{l_{r_l}}}\}$. Τότε το $x^{\mathbf{u}} = x^{\mathbf{c}}x_n^l$, όπου $x^{\mathbf{c}} \in N_l$. Συνεπώς υπάρχει ένα $\mathbf{c}_{l_i} \in \{\mathbf{c}_{l_1}, ..., \mathbf{c}_{l_{r_l}}\}$, τέτοιο ώστε $\mathbf{c} \geq \mathbf{c}_{l_i}$. Άρα από τη μερική διάταξη που δίνεται από τη διαιρετότητα έχουμε ότι $x^{\mathbf{c}_{l_i}} \setminus x^{\mathbf{c}}$. Συνεπώς $x^{\mathbf{c}_{l_i}}x_n^l \setminus x^{\mathbf{c}}x_n^l = x^{\mathbf{u}}$. Δηλαδή $x^{\mathbf{c}_{l_i}}x_n^l \setminus x^{\mathbf{u}}$ και $x^{\mathbf{c}_{l_i}}x_n^l$ ανήκει στο M. Αφού το $x^{\mathbf{u}}$ ανήκει στο $\mathbf{M}^{min}$ είναι ελαχιστοτικό στοιχείο του M, τίποτα δεν μπορεί να το διαιρεί εκτός από τον ευατό του. Άρα $x^{\mathbf{u}} = x^{\mathbf{c}_{l_i}}x_n^l \in \bigcup_{b=0}^{a-1} N_b^{min}x_n^b$.

Πράγματι λοιπόν το $\mathbf{M}^{min} \subseteq \{x^{\mathbf{c}_1}x_n^{a_1}, ..., x^{\mathbf{c}_r}x_n^{a_r}\} \bigcup (\bigcup_{b=0}^{a-1} N_b^{min}x_n^b)$. □

Ένα βασικό συμπέρασμα από το λήμμα του Dickson περιγράφεται στο ακόλουθο πόρισμα.

Πόρισμα 1.2.16. *Έστω I ένα μονωνυμικό ιδεώδες. Τότε κάθε σύνολο μονωνυμικών γεννητόρων του I, περιέχει ένα πεπερασμένο σύνολο το οποίο γεννά το I.*

Απόδειξη. Έστω M ένα σύνολο μονωνυμικών γεννητόρων του I. Από το λήμμα του Dickson, το σύνολο των ελαχιστοτικών στοιχείων του M είναι πεπερασμένο. Αυτό το πεπερασμένο σύνολο μονωνύμων γεννά το I. □

Έστω I ένα μονωνυμικό ιδεώδες. Ένα σύνολο μονωνυμικών γεννητόρων του I καλείται ελαχιστοτικό αν κάθε γνήσιο υποσύνολο του δεν αποτελεί σύνολο γεννητόρων του I. Από την πόρισμα 1.2.16, έχουμε ότι κάθε ελαχιστοτικό σύνολο μονωνυμικών γεννητόρων του I είναι πεπερασμένο.

Πρόταση 1.2.17. *Έστω I ένα μονωνυμικό ιδεώδες. Τότε υπάρχει μοναδικό ελαχιστοτικό σύνολο από μονωνυμικούς γεννήτορες του I.*

Απόδειξη. Η ύπαρξη συνεπάγεται από το πόρισμα 1.2.16.
Έστω $\{u_1, ..., u_r\}$ και $\{v_1, ..., v_s\}$ δύο ελαχιστοτικά μονωνυμικά σύνολα γεννητόρων του I. Αφού $I = \langle v_1, ..., v_s \rangle$ και το μονώνυμο u_i ανήκει στο I, συνεπάγεται από την πόρισμα 1.1.18 ότι $v_j \setminus u_i$ για κάποιο j. Όμοια $u_k \setminus v_j$ για κάποιο k, συνεπώς $u_k \setminus u_i$. Αφού το $\{u_1, ..., u_r\}$ είναι ελαχιστοτικό μονωνυμικό σύνολο γεννητόρων του I, παρατηρούμε ότι $i = k$ κι άρα $u_i = v_j$. Συνεπώς $\{u_1, ..., u_r\} \subseteq \{v_1, ..., v_s\}$. Όμοια έχουμε $\{v_1, ..., v_s\} \subseteq \{u_1, ..., u_r\}$. Άρα το ελαχιστοτικό μονωνυμικό σύνολο γεννητόρων του I είναι μοναδικό. □

Ορισμός 1.2.18. *Μια διάταξη όρων ονομάζεται* ***καλά διατεταγμένη διάταξη όρων*** *αν και μόνο αν κάθε μη κενό σύνολο $S \subseteq \mathbb{T}^n$ περιέχει ελάχιστο στοιχείο. Αν δηλαδή υπάρχει ένα μονώνυμο $x^{\mathbf{s}}$ στο S τέτοιο ώστε για κάθε μονώνυμο $x^{\mathbf{t}}$ στο S έχουμε $x^{\mathbf{s}} \leq x^{\mathbf{t}}$.*

Πρόταση 1.2.19. *Μια διάταξη όρων είναι καλά διατεταγμένη αν και μόνο αν δεν υπάρχει άπειρη αλυσίδα μονωνύμων τέτοια ώστε:*

$$x^{\mathbf{a}_1} > x^{\mathbf{a}_2} > x^{\mathbf{a}_3} > ...$$

στο $\mathbb{T}^n$.

Απόδειξη. Θεωρούμε μια διάταξη όρων $\succ$, η οποία είναι καλά διατεταγμένη. Έστω S ένα μη κενό σύνολο μονωνύμων του $\mathbb{T}^n$. Υποθέτουμε άτι υπάρχει αλυσίδα μονωνύμων του S τέτοια ώστε:

$$x^{\mathbf{a}_1} > x^{\mathbf{a}_2} > x^{\mathbf{a}_3} > ...$$

Θα καταλήξουμε σε άτοπο. Το S περιέχει ελάχιστο στοιχείο, έστω το $x^{\mathbf{a}_k}$ τέτοιο ώστε $x^{\mathbf{a}_i} \geq x^{\mathbf{a}_k}$ για κάθε i. Συνεπώς ισχύει $x^{\mathbf{a}_{k+1}} \geq x^{\mathbf{a}_k} > x^{\mathbf{a}_{k+1}}$, άρα $x^{\mathbf{a}_{k+1}} > x^{\mathbf{a}_{k+1}}$, άτοπο.
Αντίστροφα υποθέτουμε ότι δεν υπάρχει αλυσίδα μονωνύμων τέτοια ώστε:

$$x^{\mathbf{a}_1} > x^{\mathbf{a}_2} > x^{\mathbf{a}_3} > ...$$

Ισχυριζόμαστε ότι η διάταξη όρων $\succ$ είναι καλά διατεταγμένη. Έστω όχι, θα καταλήξουμε σε άτοπο. Αφού η διάταξη όρων $\succ$, δεν είναι καλά διατεταγμένη συνεπάγεται πως υπάρχει ένα μη κενό σύνολο $S \subseteq \mathbb{T}^n$, το οποίο δεν περιέχει ελάχιστο στοιχείο. Το S είναι μη κενό, άρα υπάρχει $x^{\mathbf{a}_1} \in S$, το οποίο δεν είναι ελάχιστο στοιχείο του S. Συνεπώς υπάρχει $x^{\mathbf{a}_2} \in S$, με $x^{\mathbf{a}_1} > x^{\mathbf{a}_2}$. Το $x^{\mathbf{a}_2}$ δεν είναι ελάχιστο στοιχείο του S. Συνεπώς υπάρχει $x^{\mathbf{a}_3} \in S$, με $x^{\mathbf{a}_2} > x^{\mathbf{a}_3}$. Συνεχίζουμε κατά αυτόν τον τρόπο και παρατηρούμε πως σχηματίζεται μια αλυσίδα μονωνύμων:

$$x^{\mathbf{a}_1} > x^{\mathbf{a}_2} > x^{\mathbf{a}_3} > ...$$

Άτοπο, εφόσον υποθέσαμε ότι δεν υπάρχει τέτοια αλυσίδα μονωνύμων. □

Ένα πολύ σημαντικό θεώρημα για τις διατάξεις όρων είναι το ακόλουθο:

Θεώρημα 1.2.20. *Κάθε διάταξη όρων είναι καλά διατεταγμένη, δηλαδή για κάθε* $A \neq \emptyset$, $A \subseteq \mathbb{T}^n$ *υπάρχει* $x^{\mathbf{a}} \in A$ *έτσι ώστε για κάθε* $x^{\mathbf{b}} \in A$ *να ισχύει* $x^{\mathbf{a}} \leq x^{\mathbf{b}}$.

Απόδειξη. Υποθέτουμε ότι η δοθείσα διάταξη όρων δεν είναι καλά διατεταγμένη θα καταλήξουμε σε άτοπο. Τότε σύμφωνα με την πρόταση 1.2.19 γνωρίζουμε πως υπάρχουν μονώνυμα $x^{\mathbf{a}_i} \in \mathbb{T}^n, i = 1, 2, ...$ τέτοια ώστε:

$$x^{\mathbf{a}_1} > x^{\mathbf{a}_2} > x^{\mathbf{a}_3} > \cdots .$$

Αυτό ορίζει μια αλυσίδα ιδεωδών στον πολυωνυμικό δακτύλιο $K[x_1, ..., x_n]$ την εξής:
$\langle x^{\mathbf{a}_1} \rangle \subseteq \langle x^{\mathbf{a}_1}, x^{\mathbf{a}_2} \rangle \subseteq \langle x^{\mathbf{a}_1}, x^{\mathbf{a}_2}, x^{\mathbf{a}_3} \rangle \subseteq \cdots$.
Αρχικά παρατηρούμε ότι $\langle x^{\mathbf{a}_1}, ..., x^{\mathbf{a}_i} \rangle \neq \langle x^{\mathbf{a}_1}, ..., x^{\mathbf{a}_i}, x^{\mathbf{a}_{i+1}} \rangle$. Υποθέτουμε ότι ισχύει η ισότητα, θα καταλήξουμε σε άτοπο. Εφόσον ισχύει η ισότητα το μονώνυμο $x^{\mathbf{a}_{i+1}}$ ανήκει στο ιδεώδες $\langle x^{\mathbf{a}_1}, ..., x^{\mathbf{a}_i} \rangle$. Υπάρχουν δηλαδή $u_j \in K[x_1, ..., x_n]$ για $j = 1, ..., i$, τέτοια ώστε

$$x^{\mathbf{a}_{j+1}} = \sum_{j=1}^{i} u_j x^{\mathbf{a}_j}.$$

Αν αναπτύξουμε κάθε u_j σαν γραμμικό συνδυασμό μονωνύμων, παρατηρούμε ότι κάθε όρος του $u_j x^{\mathbf{a}_j}$ είναι πολλαπλάσιο του $x^{\mathbf{a}_j}$. Άρα κάθε όρος στη δεξιά πλευρά της εξίσωσης διαιρείται από κάποιο $x^{\mathbf{a}_j}, 1 \leq j \leq i$. Όμοια και στην αριστερή πλευρά της εξίσωσης. Συνεπώς το μονώνυμο $x^{\mathbf{a}_{i+1}}$ διαιρείται από κάποιο $x^{\mathbf{a}_j}, 1 \leq j \leq i$. Οπότε σύμφωνα με την πρόταση 1.2.4 έχουμε $x^{\mathbf{a}_{i+1}} \geq x^{\mathbf{a}_j}$ για κάποιο $1 \leq j \leq i$. Συνεπώς ισχύει $x^{\mathbf{a}_{i+1}} \geq x^{\mathbf{a}_j} > x^{\mathbf{a}_{i+1}}$, άρα $x^{\mathbf{a}_{i+1}} > x^{\mathbf{a}_{i+1}}$, άτοπο. Άρα για την αλυσίδα ιδεωδών έχουμε

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset ... \subset \bigcup_{i=1}^{\infty} I_i$$

όπου $I_j = \langle x^{\mathbf{a}_1}, x^{\mathbf{a}_2}, ..., x^{\mathbf{a}_j} \rangle$. Το ιδεώδες $\bigcup_{i=1}^{\infty} I_i$ είναι μονωνυμικό ιδεώδες, σύμφωνα το πόρισμα 1.2.16 του λήμματος Dickson, γνωρίζουμε πως έχει πεπερασμένο σύνολο γεννητόρων. Έστω:

$$\bigcup_{i=1}^{\infty} I_i = \langle m_1, ..., m_t \rangle.$$

Το μονώνυμο $m_1 \in \bigcup_{i=1}^{\infty} I_i$, συνεπώς ανήκει σε κάποιο ιδεώδες I_{j1}, για κάποιο $j1$.
Το μονώνυμο $m_2 \in \bigcup_{i=1}^{\infty} I_i$, συνεπώς ανήκει σε κάποιο ιδεώδες I_{j2}, για κάποιο $j2$.
...
Το μονώνυμο $m_t \in \bigcup_{i=1}^{\infty} I_i$, συνεπώς ανήκει σε κάποιο ιδεώδες I_{jt}, για κάποιο jt.
Θέτουμε $M = max\{j1, ..., jt\}$, οπότε έχουμε:
Το μονώνυμο $m_1 \in \bigcup_{i=1}^{\infty} I_i$, το οποίο είναι υποσύνολο του ιδεώδους I_M.
Το μονώνυμο $m_2 \in \bigcup_{i=1}^{\infty} I_i$, το οποίο είναι υποσύνολο του ιδεώδους I_M.
...
Το μονώνυμο $m_t \in \bigcup_{i=1}^{\infty} I_i$, το οποίο είναι υποσύνολο του ιδεώδους I_M.

Άρα, το μονωνυμικό ιδεώδες $\langle m_1, ..., m_t \rangle$ είναι υποσύνολο του ιδεώδους I_M. Αν κοιτάξουμε την αλυσίδα ιδεωδών παρατηρούμε ότι

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_M \subset \cdots \subset \bigcup_{i=1}^{\infty} I_i \subset I_M$$

άρα $I_M = \bigcup_{i=1}^{\infty} I_i$, δηλαδή

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_M = I_{M+1} = \cdots = \bigcup_{i=1}^{\infty} I_i$$

το οποίο είναι άτοπο, διότι η αλυσίδα

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_M \subset \cdots \subset \bigcup_{i=1}^{\infty} I_i$$

είναι μια αυστηρά αύξουσα αλυσίδα ιδεωδών. □

Θα ορίσουμε τώρα τα βασικά μέρη ενός πολυωνύμου του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$, τα οποία διαφοροποιούνται ανάλογα με τη διάταξη όρων που επιλέγουμε κάθε φορά.

Ορισμός 1.2.21. *Έστω ένα μη μηδενικό πολυώνυμο $f \in K[x_1, \ldots, x_n]$. Αυτό γράφεται στη μορφή $f = c_1 x^{\mathbf{a}_1} + \ldots + c_s x^{\mathbf{a}_s}$, όπου $x^{\mathbf{a}_1} > \ldots > x^{\mathbf{a}_s}$ και $c_i \neq 0$, για κάθε $i = 1, \ldots, s$, ως προς κάποια διάταξη $\prec$. Τότε:*

1. *Το $x^{\mathbf{a}_1}$ ονομάζεται **αρχικό μονώνυμο του** f (leading power product ή leading monomial) και συμβολίζεται με $lm(f)$.*

2. *Ο c_1 ονομάζεται **αρχικός συντελεστής του** f (leading coefficient) και συμβολίζεται με $lc(f)$.*

3. *Ο $c_1 x^{\mathbf{a}_1}$ ονομάζεται **αρχικός όρος του** f (leading term) και συμβολίζεται με $lt(f)$.*

Ορισμός 1.2.22. *Έστω $S \subset K[x_1, \ldots, x_n]$. Το ιδεώδες*

$$Lt(S) = \langle lt(s) : s \in S \rangle$$

*καλείται **αρχικό ιδεώδες** (leading ideal) του S, ως προς κάποια διάταξη όρων $\prec$.*

Κάθε αρχικός όρος $lt(s)$ είναι της μορφής $lc(s)lm(s)$, όπου οι αρχικοί συντελεστές είναι μη μηδενικά στοιχεία του σώματος K κι επομένως διαθέτουν αντίστροφο. Συνεπώς $Lt(S) = \langle lm(s) : s \in S \rangle$, δηλαδή το αρχικό ιδεώδες $Lt(S)$ παράγεται και από τα αρχικά μονώνυμα $lm(s)$, ένα συμπέρασμα του οποίου η χρησιμότητα θα φανεί παρακάτω.

Παρατήρηση 1.2.23. Όταν αλλάζει η διάταξη όρων, μπορεί να αλλάζει και το αρχικό ιδεώδες.

Στη συνέχεια ακολουθεί ένα παράδειγμα στο οποίο γίνεται η εφαρμογή των παραπάνω ορισμών.

Παράδειγμα 1.2.24. Θεωρούμε το πολυώνυμο $f = 3x^4z - 2x^3y^4 + 7x^2y^2z^3 - 8xy^3z^3$ του $\mathbb{Q}[x,y,z]$ και το ιδεώδες $I = \langle f \rangle$.
Θα υπολογίσουμε τον αρχικό όρο, τον αρχικό συντελεστή, το αρχικό μονώνυμο του f και το αρχικό ιδεώδες του I ως προς τις διατάξεις όρων $\prec_{lex}$, $\prec_{deglex}$, $\prec_{degrevlex}$ με $x > y > z$.

- Στη λεξικογραφική διάταξη είναι $lt_{\prec_{lex}}(f) = 3x^4z, lc_{\prec_{lex}}(f) = 3, lm_{\prec_{lex}}(f) = x^4z$ και $Lt_{\prec_{lex}}(I) = \langle x^4z \rangle$.
- Στη βαθμωτή λεξικογραφική διάταξη είναι $lt_{\prec_{deglex}}(f) = -2x^3y^4, lc_{\prec_{deglex}}(f) = -2, lm_{\prec_{deglex}}(f) = x^3y^4$ και $Lt_{\prec_{deglex}}(I) = \langle x^3y^4 \rangle$.
- Στην αντίστροφη βαθμωτή λεξικογραφική διάταξη είναι $lt_{degrevlex}(f) = -2x^3y^4, lc_{degrevlex}(f) = -2, lm_{degrevlex}(f) = x^3y^4$ και $Lt_{\prec_{degrevlex}}(I) = \langle x^3y^4 \rangle$.

Παρατηρούμε ότι το αρχικό ιδεώδες του I αλλάζει ως προς τη λεξικογραφική διάταξη και τη βαθμωτή λεξικογραφική διάταξη. Ενώ μένει το ίδιο ως προς τη βαθμωτή λεξικογραφική διάταξη και την αντίστροφη βαθμωτή λεξικογραφική διάταξη.

1.3 Διαίρεση πολυωνύμων και Βάσεις Gröbner

Ορισμός 1.3.1. *Έστω f, g, h πολυώνυμα του $K[x_1, \ldots, x_n]$, με $g \neq 0$. Θα λέμε ότι το f **ανάγεται στο** h **μόδιο** g σε ένα βήμα (f reduces to h modulo g) και θα το συμβολίζουμε με $f \xrightarrow{g} h$ αν και μόνο αν:*

- *το αρχικό μονώνυμο του g διαιρεί ένα μη μηδενικό όρο X του f και*
- *$h = f - \frac{X}{lt(g)}g$.*

Σε αυτόν τον ορισμό πρέπει να γίνει κατανοητό ότι αφαιρούμε από το f ολόκληρο τον όρο X και τον αντικαθιστούμε με όρους αυστηρά μικρότερους του. Σκεφτόμαστε τον όρο h ως το υπόλοιπο της διαίρεσης του πολυωνύμου f με το πολυώνυμο g, διαίρεση παρόμοια με τη διαίρεση που ξέρουμε στην περίπτωση πολυωνύμων της μιας μεταβλητής.

Παράδειγμα 1.3.2. Θεωρούμε το δακτύλιο $\mathbb{Q}[x,y]$ εφοδιασμένο με τη λεξικογραφική διάταξη με $x > y$. Έστω τα πολυώνυμα $f = x^2y + 1$, $g = xy + 1$ και $h = -x + 1$. Τότε το αρχικό μονώνυμο xy του g διαιρεί ένα μη μηδενικό όρο $X = x^2y$ του f, έτσι έχουμε $h = f - \frac{x^2y}{xy}g$. Δηλαδή $f \xrightarrow{g} h$.

Ορισμός 1.3.3. *Έστω $f, h, f_1, \ldots, f_s$ πολυώνυμα του $K[x_1, \ldots, x_n]$, με $f_i \neq 0, i = 1, \ldots, s$ και $F = \{f_1, \ldots, f_s\}$. Θα λέμε ότι το f **ανάγεται στο** h **μόδιο** F και θα το συμβολίζουμε με $f \xrightarrow{F}_+ h$ αν και μόνο αν υπάρχει ακολουθία δεικτών $\{i_1, \ldots, i_t\} \subset \{1, \ldots, s\}$ και ακολουθία πολυωνύμων $\{h_1, \ldots, h_{t-1}\}$ του $K[x_1, \ldots, x_n]$ έτσι ώστε*

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \ldots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Παράδειγμα 1.3.4. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y, z]$ εφοδιασμένο με τη βαθμωτή λεξικογραφική διάταξη με $x > y > z$. Έστω τα πολυώνυμα $f = -xz^2 + 2y^2z$, $h = -xz^2 - \frac{3}{7}xz + z$ και $F = \{f_1 = 7y^2 + yz - 4, f_2 = 2yz - 3x - 1\}$ ένα σύνολο πολυωνύμων. Τότε είναι:

$$f \xrightarrow{f_1} h_1 = -xz^2 - \frac{2}{7}yz^2 + \frac{8}{7}z \xrightarrow{f_2} h.$$

Δηλαδή $f \xrightarrow{F}_+ h$. Παρατηρούμε ότι η διαδικασία της αναγωγής δεν μπορεί να συνεχιστεί αφού τόσο το αρχικό μονώνυμο y^2 του f_1, όσο και το αρχικό μονώνυμο yz του f_2 δεν διαιρεί κανένα όρο του h.

Ορισμός 1.3.5. *Ένα πολυώνυμο r καλείται* ***ανάγωγο πολυώνυμο*** *(reduced) ως προς ένα σύνολο μη μηδενικών πολυωνύμων $F = \{f_1, \ldots, f_s\}$ αν $r = 0$ ή αν δεν υπάρχει όρος του που να διαιρείται από το αρχικό μονώνυμο κάποιου f_i, για $i = 1, \ldots, s$.*

Στο παράδειγμα 1.3.4, το πολυώνυμο h είναι ανάγωγο.

Ορισμός 1.3.6. *Έστω f, r πολυώνυμα του $K[x_1, \ldots, x_n]$ και $F = \{f_1, \ldots, f_s\}$ ένα σύνολο μη μηδενικών πολυωνύμων. Αν το f ανάγεται στο r μόδιο F και το r είναι ανάγωγο ως προς το F, τότε το r καλείται* ***υπόλοιπο*** *(remainder) του f μόδιο F και η διαδικασία της αναγωγής καλείται* ***διαίρεση*** *(division).*

Παράδειγμα 1.3.7. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y, z, w]$ εφοδιασμένο με τη λεξικογραφική διάταξη με $x > y > z > w$. Έστω το πολυώνυμο $f = xw^3 - y^2zw$ και το σύνολο των πολυωνύμων $F = \{f_1 = x - y^2w, f_2 = z - w^3\}$. Εκτελώντας τη διαίρεση του f με το σύνολο F έχουμε ότι

$$f \xrightarrow{f_1} h_1 = -y^2zw + y^2w^4 \xrightarrow{f_2} - y^2zw + y^2w^4 - \frac{-y^2zw}{z}(z - w^3) = 0 = r.$$

Άρα το 0 είναι το υπόλοιπο του f μόδιο F.

Θα δώσουμε ένα ακόμη παράδειγμα στο οποίο το ανάγωγο πολυώνυμο είναι μη μηδενικό, ώστε να γίνει πλήρως κατανοητή η έννοια του ανάγωγου πολυωνύμου ως προς ένα σύνολο μη μηδενικών πολυωνύμων.

Παράδειγμα 1.3.8. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y, z, w]$ εφοδιασμένο με τη λεξικογραφική διάταξη με $x > y > z > w$. Έστω το πολυώνυμο $g = 2xw^3 + y^2zw$ και το σύνολο των πολυωνύμων $F = \{f_1 = x - y^2w, f_2 = z - w^3\}$. Εκτελώντας τη διαίρεση του g με το σύνολο F έχουμε ότι

$$g \xrightarrow{f_1} h_1 = y^2zw + 2y^2w^4 \xrightarrow{f_2} y^2zw + 2y^2w^4 - \frac{y^2zw}{z}(z - w^3) = 2y^2w^4 + y^2w^4 = 3y^2w^4 = r.$$

Το $3y^2w^4$ είναι ανάγωγο μόδιο F, αφού δε διαιρείται από το x ή το z και είναι το υπόλοιπο του f μόδιο F.

Είμαστε πλέον έτοιμοι να ορίσουμε τις βάσεις Gröbner. Θα δούμε πως οι βάσεις Gröbner αποτελούν γενίκευση της διαίρεσης των πολυωνύμων σε μία μεταβλητή. Από την σκοπιά της γραμμικής άλγεβρας, αποτελούν γενίκευση της διαδικασίας μετατροπής ενός πίνακα σε κλιμακωτή μορφή.

Ορισμός 1.3.9. *Ένα σύνολο μη μηδενικών πολυωνύμων $G = \{g_1, \ldots, g_t\}$ που περιέχεται σε ένα ιδεώδες I καλείται* ***βάση Gröbner του ιδεώδους*** *I (Gröbner basis) αν και μόνο αν για κάθε μη μηδενικό πολυώνυμο $f \in I$ υπάρχει $i \in \{1, \ldots, t\}$ έτσι ώστε το αρχικό μονώνυμο του g_i να διαιρεί το αρχικό μονώνυμο του f.*

Η ύπαρξη των βάσεων Gröbner έπεται από το λήμμα του Dickson, αφού αυτό συνεπάγεται ότι μπορούμε να βρούμε ένα πεπερασμένο σύνολο γεννητόρων για το αρχικό ιδεώδες του I.

Πρόταση 1.3.10. *Έστω I ιδεώδες του $K[x_1, ..., x_n]$, τότε ισχύουν τα ακόλουθα:*
(1) Το $Lt(I)$ είναι μονωνυμικό ιδεώδες.
(2) Υπάρχουν $g_1, ..., g_t \in I$ τέτοια ώστε $Lt(I) = \langle lt(g_1), ..., lt(g_t)\rangle$.

Απόδειξη. 1. Τα αρχικά μονώνυμα $lm(g)$ των μη μηδενικών πολυωνύμων g που ανήκουν στο ιδεώδες I, παράγουν το μονωνυμικό ιδεώδες

$$\langle lm(g) : g \in I\rangle.$$

Επειδή τα $lm(g)$ και τα $lt(g)$ διαφέρουν μόνο κατά μια μη-μηδενική σταθερά η οποία είναι στοιχείο του σώματος Κ, έχει δηλαδή αντίστροφο, έχουμε ότι

$$\langle lm(g) : g \in I\rangle = \langle lt(g) : g \in I\rangle.$$

Άρα $Lt(I) = \langle lt(g) : g \in I\rangle = \langle lm(g) : g \in I\rangle$.
Δηλαδή, $Lt(I) = \langle lm(g) : g \in I\rangle$. Επομένως το $Lt(I)$ είναι μονωνυμικό ιδεώδες.

2. Επειδή $Lt(I)$ παράγεται από τα μη μηδενικά μονώνυμα $lm(g)$ για $g \in I$, το πόρισμα 1.2.16 μας λεει ότι $Lt(I) = \langle lm(g_1), ..., lm(g_t)\rangle$ για πεπερασμένα σε πλήθος πολυώνυμα $g_1, ..., g_t \in I$. Επειδή τα $lm(g_i)$ διαφέρουν από τα $lt(g_i)$ κατά μια μη-μηδενική σταθερά η οποία είναι στοιχείο του σώματος Κ, έχει δηλαδή αντίστροφο, έπεται ότι:

$$Lt(I) = \langle lt(g_1), ..., lt(g_t)\rangle$$

το οποίο ολοκληρώνει την απόδειξη.

□

Σε αυτό το σημείο είμαστε έτοιμοι να παραθέσουμε την απόδειξη του θεωρήματος Βάσης Hilbert. Έχοντας ήδη δει ένα πολύ σημαντικό κομμάτι προς αυτή την κατεύθυνση, τα μονωνυμικά ιδεώδη και το λήμμα του Dickson.

Θεώρημα 1.3.11. *(Θεώρημα Βάσης του Hilbert) Κάθε ιδεώδες I του $K[x_1, \ldots, x_n]$ είναι πεπερασμένα παραγόμενο. Δηλαδή, υπάρχουν πολυώνυμα $g_1, ..., g_t \in I$ τέτοια ώστε $I = \langle g_1, ..., g_t\rangle$.*

Απόδειξη. Αν $I = 0$, τότε το θεώρημα ισχύει αφού $I = \langle 0\rangle$ είναι δηλαδή πεπερασμένα παραγόμενο.
Αν $I \neq 0$, τότε περιέχει κάποιο μη-μηδενικό πολυώνυμο. Ένα σύνολο λοιπόν πολυωνύμων του ιδεώδους I που να το παράγει, μπορεί να δημιουργηθεί ως εξής: από την πρόταση 1.3.10 (2), γνωρίζουμε ότι υπάρχουν πολυώνυμα $g_1, ..., g_t \in I$ τέτοια ώστε $Lt(I) = \langle lt(g_1), ..., lt(g_t)\rangle$. Ισχυριζόμαστε ότι $I = \langle g_1, ..., g_t\rangle$. Αρχικά παρατηρούμε ότι $\langle g_1, ..., g_t\rangle \subseteq I$, αφού $g_1, ..., g_t \in I$. Αρκεί να δείξουμε ότι

$I \subseteq \langle g_1, ..., g_t \rangle$. Έστω ένα μη μηδενικό πολυώνυμο $f \in I$. Εφαρμόζουμε τον αλγόριθμο διαίρεσης διαιρώντας το f με τα πολυώνυμα $g_1, ..., g_t$ και παίρνουμε μια έκφραση της μορφής $f = a_1 g_1 + ... + a_t g_t + r$, όπου το r ανάγωγο ως προς το σύνολο $\{g_1, ..., g_t\}$. Αν δείξουμε ότι $r = 0$, έχουμε τελειώσει. Παρατηρούμε ότι $r = f - (a_1 g_1 + ... + a_t g_t) \in I$. Αν $r \neq 0$ τότε $lt(r) \in Lt(I) = (lt(g_1), ..., lt(g_t))$ από το λήμμα 1.1.18, έπεται ότι το $lt(r)$ διαιρείται από κάποιο $lt(g_i)$. Άτοπο αφού το r είναι ανάγωγο. Επομένως, $r = 0$. Οπότε $f = a_1 g_1 + ... + a_t g_t \in \langle g_1, ..., g_t \rangle$. Συνεπώς $I = \langle g_1, ..., g_t \rangle$. □

Ακολουθεί μια σειρά ισοδύναμων προτάσεων που σχετίζονται με τις βάσεις Gröbner ενός ιδεώδους I.

Θεώρημα 1.3.12. *Έστω I ένα μη μηδενικό ιδεώδες του $K[x_1, \ldots, x_n]$, θεωρούμε τη διάταξη όρων $\prec$. Οι ακόλουθες προτάσεις είναι ισοδύναμες για ένα σύνολο μη μηδενικών πολυωνύμων $G = \{g_1, \ldots, g_t\} \subset I$:*

1. *Το G είναι βάση Gröbner του I.*
2. *$f \in I$ αν και μόνο αν f ανάγεται στο 0 μόδιο G.*
3. *$f \in I$ αν και μόνο αν $f = \sum_{i=1}^{t} h_i g_i$ με $lm(f) = max_{1 \leq i \leq t}(lm(h_i)lm(g_i))$.*
4. *Το αρχικό ιδεώδες του G ισούται με το αρχικό ιδεώδες του I, δηλαδή $Lt(G) = Lt(I)$.*

Ένα υποσύνολο S ενός ιδεώδους I του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$ με την ιδιότητα να παράγει το ιδεώδες I, ονομάζεται βάση του I. Με αυτή την έννοια λοιπόν, όταν λέμε βάση Gröbner εννοούμε ένα σύνολο γεννητόρων του ιδεώδους I του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$.

Πόρισμα 1.3.13. *Αν το σύνολο $G = \{g_1, \ldots, g_t\} \subseteq I$ αποτελεί βάση Gröbner του ιδεώδους I, τότε $I = \langle g_1, \ldots, g_t \rangle$.*

Απόδειξη. Παρατηρούμε πως $\langle g_1, \ldots, g_t \rangle \subseteq I$, εφόσον $\{g_1, \ldots, g_t\} \subseteq I$.
Αντίστροφα υποθέτουμε ότι το πολυώνυμο $f \in I$. Τότε από το θεώρημα 1.3.12, το f ανάγεται στο 0 μόδιο G δηλαδή $f = h_1 g_1 + ... + h_t g_t$ όπου $h_1, ..., h_t$ ανήκουν στον πολυωνυμικό δακτύλιο $K[x_1, \ldots, x_n]$, άρα ανήκει στο ιδεώδες που παράγεται από τα $g_1, ..., g_t$. Άρα $I \subseteq \langle g_1, \ldots, g_t \rangle$. Συνεπώς $I = \langle g_1, \ldots, g_t \rangle$. □

Παρατήρηση 1.3.14. Δηλαδή μια βάση Gröbner είναι πάντα βάση του ιδεώδους.

Πόρισμα 1.3.15. *Κάθε μη μηδενικό ιδεώδες I του $K[x_1, \ldots, x_n]$ έχει βάση Gröbner.*

Απόδειξη. Το αρχικό ιδεώδες του $Lt(I)$ έχει ένα πεπερασμένο σύνολο γεννητόρων το οποίο, σύμφωνα με την πρόταση 1.3.10, είναι της μορφής $\{lt(g_1), ..., lt(g_t)\}$ με $g_1, \ldots, g_t \in I$. Έστω ότι $G = \{g_1, ..., g_t\}$, τότε έχουμε $Lt(G) = Lt(I)$ άρα από το θεώρημα 1.3.12 (4), το σύνολο G είναι βάση Gröbner του ιδεώδους I. □

Ορισμός 1.3.16. *Ένα υποσύνολο $G = \{g_1, \ldots, g_t\}$ του $K[x_1, \ldots, x_n]$ καλείται βάση Gröbner αν και μόνο αν είναι **βάση Gröbner του ιδεώδους** $\langle G \rangle$ που γεννάει.*

Θεώρημα 1.3.17. *Έστω $G = \{g_1, \ldots, g_t\}$ ένα σύνολο μη μηδενικών πολυωνύμων του $K[x_1, ..., x_n]$. Τότε το G είναι βάση Gröbner αν και μόνο αν για κάθε πολυώνυμο f του $K[x_1, \ldots, x_n]$, το υπόλοιπο της διαίρεσης του f με το G είναι μοναδικό.*

Ορισμός 1.3.18. *Το υπόλοιπο της διαίρεσης κάθε πολυωνύμου f του $K[x_1, \ldots, x_n]$ με τη βάση Gröbner G είναι μοναδικό και καλείται* ***κανονική μορφή*** *(normal form) του f. Συμβολίζεται με $N_G(f)$. Δηλαδή,*

$$f \xrightarrow{G} r = N_G(f).$$

Παρατηρούμε ότι αν έχουμε μια βάση Gröbner $G = \{g_1, \ldots, g_t\}$ για το ιδεώδες I τότε μπορούμε να απαντήσουμε σε κάποια από τα ερωτήματα που θέσαμε στην αρχή. Για να αποφασίσουμε λοιπόν πότε ένα πολυώνυμο f ανήκει στο ιδεώδες I, χρησιμοποιούμε τον αλγόριθμο διαίρεσης και διαιρούμε το f με το G. Το υπόλοιπο της διαίρεσης καθορίζει την απάντηση. Δηλαδή το πολυώνυμο f ανήκει στο I αν και μόνο αν το υπόλοιπο ισούται με το μηδέν. Επίσης από το θεώρημα 1.3.17 έχουμε πως ο αντιπρόσωπος του στοιχείου $f + I$ στο δακτύλιο πηλίκο $K[x_1, ..., x_n]/I$ είναι ο $r + I$, όπου r το υπόλοιπο της διαίρεσης του f από το G. Επιπλέον μια βάση για τον $K-$ διανυσματικό χώρο $K[x_1, ..., x_n]/I$ είναι το σύνολο των συμπλόκων που προέρχονται από μονώνυμα τα οποία δεν διαιρούνται από κανένα αρχικό όρο $lt(g_i)$ για $i = 1, ..., t$, τα κανονικά μονώνυμα, κάτι το οποίο θα αποδείξουμε στην τελευταία ενότητα αυτού του κεφαλαίου στην οποία μάλιστα θα δώσουμε και δύο παραδείγματα ωστε να γίνει πλήρως κατανοητό.

1.4 ΄S−πολυώνυμα και ανάγωγες βάσεις Gröbner

Είμαστε πλέον έτοιμοι αφού παρουσιάσαμε τη σχετική θεωρία των βάσεων Gröbner να περάσουμε σε ένα εξίσου σημαντικό κομμάτι, των υπολογισμό τους. Γι' αυτό θα ορίσουμε τα S-πολυώνυμα η χρήση των οποίων θα μας βοηθήσει στον υπολογισμό των βάσεων Gröbner.

Ορισμός 1.4.1. *Έστω δύο μη μηδενικά πολυώνυμα $f, g \in K[x_1, \ldots, x_n]$ και L το ελάχιστο κοινό πολλαπλάσιο των αρχικών μονωνύμων των f και g. Το πολυώνυμο*

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

καλείται ***S−πολυώνυμο*** *($S-$polynomial) των πολυωνύμων f και g.*

Από τον τρόπο που ορίσαμε τα S-πολυώνυμα παρατηρούμε ότι το ελάχιστο κοινό πολλαπλάσιο των αρχικών μονωνύμων των δύο πολυωνύμων f και g απαλοίφεται αμοιβαία. Έτσι ο βαθμός του πολυωνύμου που προκύπτει είναι μικρότερος από το βαθμό του ελάχιστου κοινού πολλαπλάσιου L των αρχικών πολυωνύμων των f και g.

Παράδειγμα 1.4.2. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y, z]$ εφοδιασμένο με την αντίστροφη βαθμωτή λεξικογραφική διάταξη με $x > y > z$. Έστω τα πολυώνυμα $f = 3x^2yz - yz$ και $g = z^4 + xy^2$. Τα αρχικά τους μονώνυμα έχουν ελάχιστο κοινό πολλαπλάσιο το $L = x^2yz^4$. Το S-πολυώνυμο των f και g είναι

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

Θα παρουσιάσουμε τώρα τον αλγόριθμο υπολογισμού των βάσεων Gröbner, δηλαδή τον αλγόριθμο του Buchberger. Αφού προηγουμένως παραθέσουμε το θεώρημα στο οποίο βρίσκεται η βασική ιδέα του αλγορίθμου του Buchberger.

Θεώρημα 1.4.3. *(Buchberger) Έστω $G = \{g_1, \ldots, g_t\}$ ένα σύνολο μη μηδενικών πολυωνύμων του $K[x_1, \ldots, x_n]$. Τότε το σύνολο G είναι βάση Gröbner του ιδεώδους $I = \langle g_1, \ldots, g_t \rangle$ αν και μόνο αν για κάθε $i \neq j$, $S(g_i, g_j) \xrightarrow{G}_+ 0$.*

Παράδειγμα 1.4.4. 1. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y, z]$ εφοδιασμένο με τη βαθμωτή λεξικογραφική διάταξη με $x > y > z$. Τότε το σύνολο $G = \{g_1 = x^2y + z, g_2 = xz + y, g_3 = -x^2y + z^2, g_4 = y^3 + z^3\}$ είναι βάση Gröbner του ιδεώδους $I = \langle g_1, g_2 \rangle$, αφού τα αντίστοιχα S-πολυώνυμα που σχηματίζονται, $S(g_1, g_2), S(g_1, g_3), S(g_1, g_4), S(g_2, g_3), S(g_2, g_4), S(g_3, g_4)$, ανάγονται στο 0 μόδιο G.

2. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y]$ εφοδιασμένο με τη λεξικογραφική διάταξη με $y > x$. Το σύνολο $G = \{g_1 = xy - x, g_2 = -y + x^2\}$ δεν αποτελεί βάση Gröbner του ιδεώδους $I = \langle g_1, g_2 \rangle$, αφού το μοναδικό S-πολυώνυμο $S(g_1, g_2) = x^3 - x$ είναι ανάγωγο μόδιο G και διαφορετικό του μηδενός.

Αλγόριθμος 1.4.5. (Αλγόριθμος του Buchberger) Είσοδος: Ένα σύνολο μη μηδενικών πολυωνύμων $F = \{f_1, ..., f_s\}$ του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$.
Έξοδος: Η βάση Gröbner G $= \{g_1, ..., g_t\}$ του ιδεώδους $I = \langle f_1, ..., f_s \rangle$.
Τα βήματα είναι τα εξής:

1. Έστω G $= F$ και G$' = \{\{f_i, f_j\} : f_i, f_j \in$ G και $f_i \neq f_j\}$.

2. Όσο το σύνολο G$'$ είναι μη κενό:
   (α') Επιλέγουμε οποιοδήποτε δισύνολο πολυωνύμων $\{f, g\} \in$ G.
   (β') Τότε G$'$ = G$' -$ $\{\{f, g\}\}$.
   (γ') Το $S -$ πολυώνυμο $S(f, g)$ ανάγεται στο h μόδιο G,
   όπου το πολυώνυμο h είναι ανάγωγο μόδιο G.

3. Αν το πολυώνυμο h είναι μη μηδενικό, τότε:
   (α')G$'$ = G$' \bigcup \{\{$u, h$\} :$ για κάθε u $\in$ G$\}$.
   (β')G = G$\bigcup\{$h$\}$.

Θεώρημα 1.4.6. *Έστω ένα σύνολο πολυωνύμων $F = \{f_1, \ldots, f_s\}$ με $f_i \neq 0$, για $i = 1, \ldots, s$. Ο αλγόριθμος του Buchberger παράγει μία βάση Gröbner για το ιδεώδες $I = \langle f_1, \ldots, f_s \rangle$.*

Παράδειγμα 1.4.7. Στο παράδειγμα 1.4.4 (2) εκτελώντας τον αλγόριθμο του Buchberger βρίσκουμε ότι το σύνολο $G = \{g_1 = xy - x, g_2 = -y + x^2, g_3 = x^3 - x\}$, αποτελεί βάση Gröbner του ιδεώδους $I = \langle g_1, g_2 \rangle$.

Αλλάζοντας λοιπόν τη διάταξη όρων πιθανών αλλάζει και η βάση Gröbner. Ωστόσο δύναται να βρούμε βάσεις Gröbner του ίδιου ιδεώδους με διαφορετικό πλήθος στοιχείων. Ενώ πρέπει να τονίσουμε πως μπορεί να βρούμε διαφορετικές βάσεις Gröbner ως προς την ίδια διάταξη όρων, με λίγα λόγια η βάση Gröbner δεν είναι μοναδική. Σε αυτό το σημείο θα παραθέσουμε ένα πολύ σημαντικό λήμμα το οποίο βοηθά στον γρήγορο υπολογισμό των βάσεων Gröbner. Θα το χρησιμοποιήσουμε στο τέταρτο κεφάλαιο και συγκεκριμένα σε ένα παράδειγμα του τέταρτου κεφαλαίου στο οποίο διευκολύνει κατά πολύ τους υπολογισμούς για την εύρεση μιας βάσης Gröbner.

Λήμμα 1.4.8. *Έστω δύο μη μηδενικά πολυώνυμα $f, g \in K[x_1, ..., x_n]$, και έστω $d = μκδ(f, g)$. Οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. *Τα* $lm(\frac{f}{d})$ *και* $lm(\frac{g}{d})$ *έχουν μέγιστο κοινό διαιρέτη το 1.*

2. *Το* $S(f,g) \xrightarrow{f,g}_{+} 0$

Συνοψίζοντας το σύνολο $\{f,g\}$ είναι βάση Gröbner αν και μόνο αν τα $lm(\frac{f}{d})$ και $lm(\frac{g}{d})$ έχουν μέγιστο κοινό διαιρέτη το 1.
Σε αυτό το σημείο θα ορίσουμε την ελαχιστική βάση Gröbner.

Ορισμός 1.4.9. *Μία βάση Gröbner* $G = \{g_1, \ldots, g_t\}$ *καλείται* ***ελαχιστική βάση Gröbner*** *(minimal) αν για κάθε* i*, ο αρχικός συντελεστής του πολυωνύμου* g_i *είναι μονάδα και για κάθε* $i \neq j$ *το αρχικό μονώνυμο του* g_i *δεν διαιρεί το αρχικό μονώνυμο του* g_j*.*

Παράδειγμα 1.4.10. Θεωρούμε το δακτύλιο εφοδιασμένο με τη λεξικογραφική διάταξη $y > x$. Το σύνολο $G = \{g_1 = y^2x + yx + x^2, g_2 = y + x, g_3 = y, g_4 = x^2, g_5 = x\}$ είναι βάση Gröbner δεν είναι όμως ελαχιστική, αφού το αρχικό μονώνυμο του g_3 διαιρεί το αρχικό μονώνυμο του g_2 και το αρχικό μονώνυμο του g_5 διαιρεί το αρχικό μονώνυμο του g_4.

Παράδειγμα 1.4.11. Από την άσκηση 1.4.4 (1), γνωρίζουμε ότι μια βάση Gröbner του I είναι η ακόλουθη:

$$G = \{g_1 = x^2y + z, g_2 = xz + y, g_3 = -x^2y + z^2, g_4 = y^3 + z^3\}.$$

Παρατηρούμε ότι οι συντελεστές των πολυωνύμων g_1, g_2, g_4 είναι μονάδες σε αντίθεση με το συντελεστή του g_3 που είναι (-1). Άρα η βάση αυτή δεν είναι ελαχιστική.

Αντίστοιχη έννοια στη γραμμική άλγεβρα της ελαχιστικής βάσης Gröbner είναι ο κλιμακωτός πίνακας.
Έχοντας μία βάση Gröbner βρίσκουμε μία ελαχιστική βάση Gröbner. Το ακόλουθο πόρισμα παρέχει ένα τρόπο κατασκευής μιας ελαχιστικής βάσης Gröbner ενός ιδεώδους I.

Πόρισμα 1.4.12. *Έστω* $G = \{g_1, \ldots, g_t\}$ *βάση Gröbner του ιδεώδους* I*. Για να βρούμε μία ελαχιστική βάση Gröbner από τη* G*, διαγράφουμε όλα τα* g_i *για τα οποία υπάρχει* $j \neq i$ *τέτοιο ώστε το αρχικό μονώνυμο του* g_j *να διαιρεί το αρχικό μονώνυμο του* g_i *και διαιρούμε κάθε όρο των* g_j *που απομένουν με τον αρχικό συντελεστή τους.*

Παράδειγμα 1.4.13. Συνεχίζοντας το παράδειγμα 1.4.11 θα κάνουμε τη βάση Gröbner ελαχιστική. Αρκεί να πολλαπλασιάσουμε το πολυώνυμο g_3 με (-1), συνεπώς:

$$G' = \{g_1 = x^2y + z, g_2 = xz + y, g_3 = x^2y - z^2, g_4 = y^3 + z^3\}.$$

Στη συνέχεια διαγράφουμε το πολυώνυμο g_1 αφού το αρχικό μονώνυμο του g_3 διαιρεί το αρχικό μονώνυμο του g_1, και παρατηρούμε ότι δεν υπάρχει αρχικό μονώνυμο κάποιου από τα g_2, g_3, g_4 που να διαιρεί αρχικό μονώνυμο άλλου πολυωνύμου της βάσης G' και οι συντελεστές τους είναι μονάδες. Άρα η $\{g_2 = xz + y, g_3 = x^2y - z^2, g_4 = y^3 + z^3\}$ είναι ελαχιστική βάση Gröbner.

Παράδειγμα 1.4.14. Συνεχίζοντας το παράδειγμα 1.4.10, από τη βάση Gröbner G μπορούμε να βρούμε δύο διακεκριμένες ελαχιστικές βάσεις Gröbner, τις $G_0 = \{x, y\}$ και $G_1 = \{x, y + x\}$. Παρατηρούμε ότι οι δύο αυτές βάσεις έχουν το ίδιο πλήθος στοιχείων και ότι τα πολυώνυμα τους έχουν τους ίδιους αρχικούς όρους x και y. Στην πραγματικότητα, υπάρχουν άπειρες σε πλήθος διακεκριμένες ελαχιστικές βάσεις Gröbner. Για παράδειγμα τέτοιες βάσεις είναι οι

$$G_n = \{x, y + x^n\} \text{ για } n \geq 1.$$

Για όλες αυτές τις βάσεις ισχύει ότι

$$Lt(G_1) = Lt(G_n)$$

για $n \geq 1$, έχουν δηλαδή το ίδιο αρχικό ιδεώδες.

Η παρατήρηση λοιπόν αυτή γενικεύεται στην ακόλουθη πρόταση.

Πρόταση 1.4.15. *Αν $G = \{g_1, \ldots, g_t\}$ και $F = \{f_1, \ldots, f_s\}$ είναι ελαχιστικές βάσεις Gröbner ενός ιδεώδους I, τότε $s = t$ και μπορούμε να διατάξουμε ξανά έτσι ώστε ο αρχικός όρος ως προς τη διάταξη $\prec$ του πολυωνύμου f_i, $lt(f_i)$, να ισούται με τον αρχικό όρο του πολυωνύμου g_i ως προς την ίδια διάταξη, $lt(g_i)$, για κάθε $i = 1, \ldots, t$.*

Σε αυτό το σημείο θα ορίσουμε την ανάγωγη βάση Gröbner.

Ορισμός 1.4.16. *Μία βάση Gröbner $G = \{g_1, \ldots, g_t\}$ καλείται* ***ανάγωγη βάση Gröbner*** *(reduced) αν για κάθε i ο αρχικός συντελεστής του g_i είναι μονάδα και κάθε πολυώνυμο g_i είναι ανάγωγο ως προς το σύνολο $G - \{g_i\}$. Ισοδύναμα, αν δε υπάρχει μη μηδενικός όρος του g_i ο οποίος να διαιρείται από κάποιο αρχικό μονώνυμο του g_j, για κάθε $j \neq i$ με $i, j \in \{1, ..., t\}$.*

Από τον ορισμό φαίνεται ότι μία ανάγωγη βάση Gröbner είναι πάντα ελαχιστική. Αντίστοιχη έννοια στη γραμμική άλγεβρα της ανάγωγης βάσης Gröbner είναι ο ισχυρά κλιμακωτός πίνακας.

Παράδειγμα 1.4.17. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y]$ εφοδιασμένο με τη λεξικογραφική διάταξη με $x > y$ και έστω το ιδεώδες $I = \langle f_1 = xy - x, f_2 = x^2 - y \rangle$. Έχουμε:
$S(f_1, f_2) = \frac{x^2y}{xy} f_1 - \frac{x^2y}{x^2} f_2 = -x^2 + y^2 \to^{f_2} y^2 - y = f_3$. Καθώς το f_3 είναι ανάγωγο ως προς το $\{f_1, f_2\}$, το προσθέτουμε στη ζητούμενη βάση Gröbner και συνεχίζουμε τον αλγόριθμο με τα νέα $S-$πολυώνυμα που προκύπτουν. Άρα

$$G' = \{f_1 = xy - x, f_2 = x^2 - y, f_3 = y^2 - y\}.$$

Παρατηρούμε ότι $S(f_1, f_2) \to^{G'} 0$.
Ακόμη:

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

Τέλος,

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

Το σύνολο

$$G' = \{f_1 = xy - x, f_2 = x^2 - y, f_3 = y^2 - y\},$$

παρατηρούμε ότι είναι ελαχιστική βάση Gröbner του I, καθώς οι συντελεστές των πολυωνύμων είναι μονάδες και δεν υπάρχει αρχικό μονώνυμο των πολυωνύμων f_1, f_2, f_3 που να διαιρεί αρχικό μονώνυμο πολυωνύμου της G'. Ωστόσο παρατηρούμε ότι τα αρχικά μονώνυμα των πολυωνύμων της G' δε διαιρούν κανένα όρο των πολυωνύμων της G' εκτός από τον ευατό τους, άρα η βάση G' είναι και ανάγωγη βάση Gröbner του I.

Το ακόλουθο πόρισμα παρέχει ένα τρόπο κατασκευής μιας ανάγωγης βάσης Gröbner ενός ιδεώδους I, γνωρίζοντας μια ελαχιστική βάση Gröbner του I.

Πόρισμα 1.4.18. *Έστω $G = \{g_1, \ldots, g_t\}$ μία ελαχιστική βάση Gröbner του ιδεώδους I. Θεωρούμε την ακόλουθη διαδικασία αναγωγής:*
$g_1 \xrightarrow{H_1}_+ h_1$, *όπου h_1 ανάγωγο μόδιο $H_1 = \{g_2, \ldots, g_t\}$*
$g_2 \xrightarrow{H_2}_+ h_2$, *όπου h_2 ανάγωγο μόδιο $H_2 = \{h_1, g_3, \ldots, g_t\}$*
$g_3 \xrightarrow{H_3}_+ h_3$, *όπου h_3 ανάγωγο μόδιο $H_3 = \{h_1, h_2, g_4, \ldots, g_t\}$*
$\vdots$
$g_t \xrightarrow{H_t}_+ h_t$, *όπου h_t ανάγωγο μόδιο $H_t = \{h_1, h_2, \ldots, h_{t-1}\}$*
Τότε το σύνολο $H = \{h_1, \ldots, h_t\}$ αποτελεί ανάγωγη βάση Gröbner του ιδεώδους I.

Απόδειξη. Καθώς η $G = \{g_1, \ldots, g_t\}$ είναι μια ελαχιστική βάση Gröbner του ιδεώδους I, παίρνουμε ότι $lm(g_i) = lm(h_i)$ για κάθε i, αφού $lm(g_i)$ δεν διαιρεί $lm(g_j)$ για οποιοδήποτε $i \neq j$. Έτσι σε καθεμία από τις παραπάνω διαιρέσεις το αρχικό μονώνυμο $lm(g_i)$ απομένει αναγκαστικά στο υπόλοιπο h_i. Άρα $H = \{h_1, \ldots, h_t\}$ είναι μια βάση Gröbner του ιδεώδους I, σύμφωνα με το πόρισμα 1.3.12 (4) εφόσον $Lt(G) = Lt(H)$. Μάλιστα η βάση αυτή είναι ανάγωγη, αφού δεν υπάρχει όρος του h_i που να διαιρείται από κάποιο $lm(h_j)$, για κάθε $i \neq j$ με $i, j \in \{1, ..., t\}$. □

Παράδειγμα 1.4.19. Θεωρούμε το δακτύλιο $\mathbb{Z}_5[x, y]$ εφοδιασμένο με τη λεξικογραφική διάταξη με $x > y$ και έστω το ιδεώδες $I = \langle x^2 + y^2 + 1, x^2y + 2xy + x \rangle$. Το σύνολο

$$G = \{x^2 + y^2 + 1, x^2y + 2xy + x, 3xy + 4x + y^3 + y, 4y^5 + 3y^4 + y^2 + y + 3\}$$

είναι βάση Gröbner του I. Το σύνολο

$$G' = \{x^2 + y^2 + 1, xy + 3x + 2y^3 + 2y, y^5 + 2y^4 + 4y^2 + 4y + 2\}$$

είναι ελαχιστική βάση Gröbner του I, η οποία είναι και ανάγωγη.

Παράδειγμα 1.4.20. Από τις άπειρες ελαχιστικές βάσεις Gröbner του παραδείγματος 1.4.14, μοναδική ανάγωγη είναι η $G_0 = \{x, y\}$.

Γίνεται λοιπόν κατανοητό πως υπάρχουν άπειρες ελαχιστικές βάσεις Gröbner αλλά μοναδική ανάγωγη βάση Gröbner ως προς συγκεκριμένη διάταξη όρων. Το ακόλουθο θεώρημα του Buchberger περιλαμβάνει το συμπέρασμα αυτό.

Θεώρημα 1.4.21. *(Buchberger) Κάθε μη μηδενικό ιδεώδες I στον δακτύλιο πολυωνύμων $K[x_1,\ldots,x_n]$ ο οποίος είναι εφοδιασμένος με συγκεκριμένη διάταξη όρων $\prec$ έχει μοναδική ανάγωγη βάση ως προς τη διάταξη $\prec$.*

Απόδειξη. Έστω $G=\{g_1,\ldots,g_t\}$ και $H=\{h_1,\ldots,h_t\}$ ανάγωγες βάσεις Gröbner του I. Τότε από το πόρισμα 1.4.18 έχουμε ότι $lm(g_i)=lm(h_i)$ για κάθε $i=1,...,t$. Ισχυριζόμαστε ότι $g_i-h_i=0$. Έστω όχι. Θα καταλήξουμε σε άτοπο. Είναι $g_i,h_i\in I$ συνεπώς $g_i-h_i\in I$. Καθώς τα σύνολα $\{g_1,\ldots,g_t\},\{h_1,\ldots,h_t\}$ είναι βάσεις Gröbner του I συνεπάγεται πως υπάρχει ένα $j\in\{1,...,t\}$ ούτως ώστε $lm(g_j)=lm(h_j)\setminus lm(g_i-h_i)$. Προφανώς $i\neq j$, αφού $lm(g_i-h_i)<lm(g_i)=lm(h_i)$. Συνεπώς $lm(g_j)=lm(h_j)$ διαιρεί το αρχικό μονώνυμο του g_i-h_i. Το αρχικό μονώνυμο του g_i-h_i μπορεί να είναι μονώνυμο του g_i ή μονώνυμο του h_i ή και των δύο. Θεωρούμε τις ακόλουθες περιπτώσεις:

1. Αν το αρχικό μονώνυμο του g_i-h_i είναι μονώνυμο του g_i, τότε έχουμε ότι το $lm(g_j)\setminus lm(g_i-h_i)$. Άτοπο εφόσον η βάση $G=\{g_1,\ldots,g_t\}$ είναι ανάγωγη βάση Gröbner του I.

2. Αν το αρχικό μονώνυμο του g_i-h_i είναι μονώνυμο του h_i, τότε έχουμε ότι το $lm(g_j)=lm(h_j)\setminus lm(g_i-h_i)$. Άτοπο εφόσον η βάση $H=\{h_1,\ldots,h_t\}$ είναι ανάγωγη βάση Gröbner του I.

Άρα $g_i-h_i=0$ για κάθε $i=1,...,t$. □

Τέλος ακολουθεί μια σύνοψη των βασικότερων συμπερασμάτων της θεωρίας των βάσεων Gröbner στο επόμενο θεώρημα.

Θεώρημα 1.4.22. *Έστω ένα σύνολο μη μηδενικών πολυωνύμων $G=\{g_1,\ldots,g_t\}$ και $I=\langle G\rangle$ το ιδεώδες που γεννάται από αυτό. Τότε οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. *Για κάθε $f\in I$ υπάρχει i τέτοιο ώστε το αρχικό μονώνυμο του g_i να διαιρεί το αρχικό μονώνυμο του f, δηλαδή το σύνολο G είναι βάση Gröbner.*

2. *$Lt(G)=Lt(I)$.*

3. *$f\in I$ αν και μόνο αν $f\xrightarrow{G}_+0$.*

4. *Για κάθε πολυώνυμο f του $K[x_1,\ldots,x_n]$ αν $f\xrightarrow{G}_+r_1$, $f\xrightarrow{G}_+r_2$ και τα r_1,r_2 είναι ανάγωγα μόδιο G, τότε $r_1=r_2$.*

5. *Για κάθε $i\neq j$, $S(g_i,g_j)\xrightarrow{G}_+0$.*

6. *Για κάθε $f\in I$, υπάρχουν πολυώνυμα $h_1,...,h_t\in K[x_1,\ldots,x_n]$ τέτοια ώστε $f=h_1g_1+...+h_tg_t$ και $lm(f)=max_{1\leq v\leq t}(lm(h_v)lm(g_v))$.*

Παράδειγμα 1.4.23. Το 1983 ο Teo Mora βρήκε μια οικογένεια ιδεωδών

$$I_n=\langle x^{n+1}-yz^{n-1}w, xy^{n-1}-z^n, x^nz-y^nw\rangle\subset\mathbb{Q}[x,y,z,w], n\geq 1,$$

της οποίας κάθε στοιχείο I_n έχει τρείς γεννήτορες μολονότι η ανάγωγη βάση Gröbner του I_n, ως προς την αντίστροφη βαθμωτή λεξικογραφική διάταξη με $x>y>z>w$, αποτελείται από $n+3$ στοιχεία. Για παράδειγμα, το I_{2009} έχει τρείς γενήτορες ενώ η ανάγωγη βάση Gröbner αποτελείται από 2012 στοιχεία.

Καθένα από τα ιδεώδη I_n διαθέτει τρείς γεννήτορες, δύο βαθμού $n+1$ κι ένα βαθμού n. Η ανάγωγη βάση Gröbner του I_n, ως προς την αντίστροφη βαθμωτή λεξικογραφική διάταξη με $x > y > z > w$, έχει τα παρακάτω $n+3$ στοιχεία:
$G = \{x^{n+1} - yz^{n-1}w, xy^{n-1} - z^n, x^n z - y^n w, x^{n-1}z^{n+1} - y^{2n-1}w, x^{n-2}z^{2n+1} - y^{3n-2}w, ..., x^{n-j}z^{jn+1} - y^{(j+1)n-j}w, ..., xz^{n^2-n+1} - y^{n^2-n+1}w, z^{n^2+1} - y^{n^2}w\}$.

1.5 Καθολικές Βάσεις Gröbner

Μέχρι στιγμής έχουμε μιλήσει για τις βάσεις Gröbner και τον υπολογισμό τους. Πιο συγκεκριμένα, δοθέντος μίας διάταξης όρων $\prec$ κι ενός ιδεώδους I του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$ γνωρίζουμε πως να υπολογίσουμε μία βάση Gröbner του I. Η βάση αυτή εξαρτάται από τη διάταξη όρων $\prec$, καθώς αλλάζοντας τη διάταξη όρων πιθανόν αλλάζει το αρχικό ιδεώδες του I, ως συνέπεια της αλλαγής των αρχικών όρων των πολυωνύμων της βάσης. Συμπεραίνουμε λοιπόν ότι για κάθε διαφορετική διάταξη όρων βρίσκουμε πιθανόν διαφορετικές βάσεις Gröbner για το ιδεώδες I.

Σε αυτή την ενότητα θα ορίσουμε τις καθολικές βάσεις Gröbner τις οποίες ανέπτυξαν ο N.Schwartz στο άρθρο [18] και ο V.Weispfenning στο άρθρο [20]. Για το σκοπό αυτό θα διατυπώσουμε και θα αποδείξουμε μια σειρά ορισμάτων και προτάσεων, αφού δώσουμε πρώτα τον ακόλουθο ορισμό.

Ορισμός 1.5.1. *Έστω I ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$ και $Lt(I)$ αρχικό ιδεώδες του I ως προς κάποια διάταξη όρων $\prec$. Τα μονώνυμα M που δεν ανήκουν στο αρχικό ιδεώδες $Lt(I)$ καλούνται* **κανονικά μονώνυμα** *(standard).*

Λήμμα 1.5.2. *Έστω I ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$ και $Lt(I)$ αρχικό ιδεώδες του I ως προς κάποια διάταξη όρων $\prec$. Το σύνολο των συμπλόκων των μονωνύμων του $K[x_1, \ldots, x_n]$ που δεν ανήκουν στο $Lt(I)$ αποτελεί βάση για τον $K-$ διανυσματικό χώρο $K[x_1, \ldots, x_n]/I$.*

Απόδειξη. Έστω I ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$ και $Lt(I)$ αρχικό ιδεώδες του I ως προς κάποια διάταξη όρων $\prec$. Έστω $x^{\mathbf{u}}$ μονώνυμο του πολυωνυμικού δακτυλίου $K[x_1, \ldots, x_n]$. Θεωρούμε το σύνολο

$$S = \{x^{\mathbf{u}} + I : x^{\mathbf{u}} \notin Lt(I)\} = \{x^{\mathbf{u}} + I : x^{\mathbf{u}} \text{ κανονικό μονώνυμο}\}.$$

Θα δείξουμε ότι το σύνολο S αποτελεί βάση για τον $K-$ διανυσματικό χώρο $K[x_1, \ldots, x_n]/I$.

1. Έστω ένα πολυώνυμο $f \in K[x_1, \ldots, x_n]$. Τότε $f + I \in K[x_1, \ldots, x_n]/I$. Έστω $G = \{g_1, \ldots, g_t\}$ βάση Gröbner του ιδεώδους I, ως προς τη διάταξη όρων $\prec$. Το f ανάγεται στην κανονική μορφή $N_G(f)$ μόδιο G. Συνεπώς έχουμε ότι $f - N_G(f) \in I$ κι άρα $f + I = N_G(f) + I$, όπου $N_G(f)$ ανάγωγο μόδιο G. Δηλαδή, δεν υπάρχει όρος της κανονικής μορφής του f, που να διαιρείται από κάποιο αρχικό μονώνυμο $lm(g_i)$, για $i = 1, ..., n$. Συνεπώς τα μονώνυμα της κανονικής μορφής $N_G(f)$ δεν ανήκουν στο αρχικό ιδεώδες του I. Άρα είναι κανονικά. Επομένως γράφονται ως γραμμικός συνδυασμός των μονωνύμων του συνόλου S. Δηλαδή

$$N_G(f) = c_1 x^{\mathbf{u_1}} + \ldots + c_l x^{\mathbf{u_l}},$$

όπου $x^{u_j} \in S$, για κάθε $j = 1, \ldots, l$. Τότε,

$$f+I = N_G(f)+I = (c_1x^{u_1}+\ldots+c_lx^{u_l})+I = c_1(x^{u_1}+I)+\ldots+c_l(x^{u_l}+I)$$

γραμμικός συνδυασμός συμπλόκων κανονικών μονωνύμων. Άρα, το σύνολο S παράγει τον K-διανυσματικό χώρο $K[x_1, \ldots, x_n]/I$.

2. Έστω ότι το σύνολο S είναι γραμμικά εξαρτημένο και $G = \{g_1, \ldots, g_t\}$ η βάση Gröbner του ιδεώδους I, ως προς τη διάταξη όρων $\prec$. Τότε

$$c_1(x^{u_1} + I) + \ldots + c_l(x^{u_l} + I) = 0 + I, \text{ με } (c_1, ..., c_l) \neq (0, ..., 0)$$

ισοδύναμα

$$c_1x^{u_1} + \ldots + c_lx^{u_l} + I = 0 + I, \text{ με } (c_1, ..., c_l) \neq (0, ..., 0).$$

Τότε

$$c_1x^{u_1} + \ldots + c_lx^{u_l} \in I,$$

άρα από το θεώρημα 1.3.12 (5) έχουμε

$$c_1x^{u_1} + \ldots + c_lx^{u_l} \xrightarrow{G} 0.$$

Ακόμη τα μονώνυμα $x^{u_1} \ldots x^{u_l}$ είναι κανονικά, συνεπώς δεν ανήκουν στο αρχικό ιδεώδες του I. Κατά συνέπεια το πολυώνυμο $c_1x^{u_1} + \ldots + c_lx^{u_l}$ είναι ανάγωγο μόδιο G, αφού δεν υπάρχει μονώνυμο x^{u_j} για $j = 1, ..., l$ που να διαιρείται από κάποιο αρχικό μονώνυμο του g_i, για $i = 1, \ldots, t$. Συνεπώς

$$c_1x^{u_1} + \ldots + c_lx^{u_l} \xrightarrow{G} c_1x^{u_1} + \ldots + c_lx^{u_l}.$$

Διαιρέσαμε λοιπόν το πολυώνυμο $c_1x^{u_1} + \ldots + c_lx^{u_l}$ με το σύνολο $G = \{g_1, \ldots, g_t\}$ και βρήκαμε δύο υπόλοιπα $r_1 = 0, r_2 = c_1x^{u_1} + \ldots + c_lx^{u_l}$. Έτσι σύμφωνα με το θεώρημα 1.4.22 (4), έχουμε:

$$c_1x^{u_1} + \ldots + c_lx^{u_l} = 0.$$

Συνεπώς $c_1 = \ldots = c_l = 0$, άτοπο αφού υποθέσαμε ότι $(c_1, ..., c_l) \neq (0, ..., 0)$. Επομένως, το σύνολο S είναι γραμμικά ανεξάρτητο.

Εφόσον λοιπόν το σύνολο S παράγει τον K- διανυσματικό χώρο $K[x_1, \ldots, x_n]/I$ σύμφωνα με το (1), και είναι γραμμικά ανεξάρτητο σύμφωνα με το (2) προκύπτει ότι το σύνολο S αποτελεί βάση του K- διανυσματικό χώρο $K[x_1, \ldots, x_n]/I$. □

Για ένα συγκεκριμένο ιδεώδες τα κανονικά μονώνυμα μπορεί να είναι διαφορετικά αν αλλάξουμε τη διαταξη όρων, αλλά πάντα θα είναι ίδια σε πλήθος αφού το πλήθος τους είναι η διάσταση του K- διανυσματικού χώρου $K[x_1, \ldots, x_n]/I$, κάτι τα οποίο γίνεται αντιληπτό στα επόμενα παραδείγματα.

Παράδειγμα 1.5.3. Υποθέτουμε ότι $K = \mathbb{Q}$. Έστω $f_1 = yx^2 - y + x$, $f_2 = y^2x - x$, και $I = \langle f_1, f_2 \rangle$. Θα χρησιμοποιήσουμε βαθμωτή λεξικογραφική διάταξη όρων $\prec$, με $x < y$. Θα χρησιμοποιήσουμε τον αλγόριθμο 1.4.5.
Έστω $G_1 = \{f_1, f_2\}$, $G_1' = \{\{f_1, f_2\}\}$
Το σύνολο G_1' είναι μη κενό οπότε:

$$S(f_1, f_2) = yf_1 - xf_2 = -y^2 + xy + x^2$$

που είναι ανάγωγο ως προς το σύνολο G_1.
Θέτουμε $f_3 = -y^2 + yx + x^2$ και
$G_2 = \{f_1, f_2, f_3\}$ οπότε
$G_2' = \{\{f_1, f_3\}, \{f_2, f_3\}\}$.
Αφού τώρα $S(f_1, f_2) \xrightarrow{G_2} 0$.
Παρατηρούμε ότι:

$$S(f_1, f_3) = yf_1 + x^2 f_3 = x^3 y + x^4 + -y^2 + xy \xrightarrow{f_1} x^4 + -y^2 + 2xy - x^2 \xrightarrow{f_3} x^4 + yx - 2x^2$$

που είναι ανάγωγο ως προς το σύνολο G_2.
Θέτουμε $f_4 = x^4 + yx - 2x^2$ και
$G_3 = \{f_1, f_2, f_3, f_4\}$ οπότε
$G_3' = \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$.
Αφού τώρα $S(f_1, f_3) \xrightarrow{G_3} 0$.
Παρατηρούμε ότι:

$$S(f_2, f_3) = f_2 + xf_3 = x^2 y + x^3 - x \xrightarrow{f_1} x^3 + y - 2x$$

που είναι ανάγωγο ως προς το σύνολο G_3.
Θέτουμε $f_5 = x^3 + y - 2x$ και
$G_4 = \{f_1, f_2, f_3, f_4, f_5\}$ οπότε
$G_4' = \{\{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}, \{f_1, f_5\},$
$\{f_2, f_5\}, \{f_3, f_5\}, \{f_4, f_5\}\}$.

Παρατηρούμε ότι τα υπόλοιπα $S-$πολυώνυμα είναι όλα μηδενικά. Οπότε το σύνολο $G = \{f_1, f_2, f_3, f_4, f_5\}$ είναι βάση Gröbner του ιδεώδους I. Ωστόσο το σύνολο $G = \{f_1, -f_3, f_5\}$ είναι βάση Gröbner του ιδεώδους I, καθώς το αρχικό μονώνυμο $lm(f_2)$ διαιρείται από το αρχικό μονώνυμο $lm(f_3)$, και το αρχικό μονώνυμο $lm(f_4)$ διαιρείται από το αρχικό μονώνυμο $lm(f_5)$. Στην πραγματικότητα το σύνολο $G = \{f_1, -f_3, f_5\}$ είναι ανάγωγη βάση Gröbner του ιδεώδους I ως προς τη βαθμωτή λεξικογραφική διάταξη όρων $\prec$, με $x < y$, αφού δεν υπάρχει όρος των πολυωνύμων της βάσης, που να διαιρείται από κάποιο αρχικό μονώνυμο των πολυωνύμων αυτής. Άρα το αρχικό ιδεώδες είναι $Lt_{\prec}(I) = \langle x^2 y, y^2, x^3 \rangle$.
Συνεπώς τα κανονικά μονώνυμα είναι τα εξής $\{1, x, y, x^2, xy\}$. Σύμφωνα με το λήμμα 1.5.2, μια βάση για τον $\mathbb{Q}[x, y]/I$ αποτελείται από τα σύμπλοκα $\{1 + I$, $x + I, y + I, x^2 + I, xy + I\}$, συνεπώς η διάσταση του $\mathbb{Q}[x, y]/I$ είναι ίση με 5.

Στη συνέχεια θα δώσουμε και πάλι το ίδιο παράδειγμα στο οποίο θα αλλάξουμε όμως τη διάταξη όρων και θα δούμε ότι το πλήθος των κανονικών μονωνύμων είναι ίσο με 5.

Παράδειγμα 1.5.4. Υποθέτουμε ότι $K = \mathbb{Q}$. Έστω $f_1 = x^2 y + x - y$, $f_2 = xy^2 - x$, και $I = \langle f_1, f_2 \rangle$. Θα χρησιμοποιήσουμε λεξικογραφική διάταξη όρων $\prec$, με $x > y$. Θα χρησιμοποιήσουμε τον αλγόριθμο 1.4.5.
Έστω $G_1 = \{f_1, f_2\}$. $G_1' = \{\{f_1, f_2\}\}$
Το σύνολο G_1' είναι μη κενό οπότε:

$$S(f_1, f_2) = yf_1 - xf_2 = x^2 + xy - y^2$$

που είναι ανάγωγο ως προς το σύνολο G_1.
Θέτουμε $f_3 = x^2 + xy - y^2$ και

$G_2 = \{f_1, f_2, f_3\}$ οπότε
$G_2' = \{\{f_1, f_3\}, \{f_2, f_3\}\}$.
Αφού τώρα $S(f_1, f_2) \xrightarrow{G_2} 0$.
Παρατηρούμε ότι:

$$S(f_1, f_3) = 1f_1 - yf_3 = -xy^2 + x + y^3 - y \xrightarrow{f_2} y^3 - y$$

που είναι ανάγωγο ως προς το σύνολο G_2.
Θέτουμε $f_4 = y^3 - y$ και
$G_3 = \{f_1, f_2, f_3, f_4\}$ οπότε
$G_3' = \{\{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$.
Αφού τώρα $S(f_1, f_3) \xrightarrow{G_3} 0$.
Παρατηρούμε ότι:
$S(f_2, f_3) = xf_2 - y^2 f_3 = -x^2 - xy^3 + y^4$
$\xrightarrow{f_3} - xy^3 + xy + y^4 - y^2$
$\xrightarrow{f_2} y^4 - y^2$
$\xrightarrow{f_4} y^4 - y^2 - y^4 + y^2 = 0$
Άρα $S(f_2, f_3) \xrightarrow{G_3} 0$.
Παρατηρούμε ότι:
$S(f_1, f_4) = y^2 f_1 - x^2 f_4 = x^2 y + xy^2 - y^3$
$\xrightarrow{f_1} xy^2 - x - y^3 + y$
$\xrightarrow{f_2} - y^3 + y$
$\xrightarrow{f_4} - y^3 + y + y^3 - y = 0$
Άρα $S(f_1, f_4) \xrightarrow{G} 0$.
Παρατηρούμε ότι:

$$S(f_2, f_4) = yf_2 - xf_4 = xy^3 - xy - xy^3 + xy = 0$$

Άρα $S(f_2, f_4) \xrightarrow{G} 0$
Παρατηρούμε ότι:
$S(f_3, f_4) = y^3 f_3 - x^2 f_4 = x^2 y + xy^4 - y^5$
$\xrightarrow{f_1} xy^4 - x - y^5 + y$
$\xrightarrow{f_2} xy^2 - x - y^5 + y$
$\xrightarrow{f_2} - y^5 + y$
$\xrightarrow{f_4} - y^5 + y + y^5 - y = 0$
Άρα $S(f_3, f_4) \xrightarrow{G} 0$.
Άρα το σύνολο $G = \{f_1, f_2, f_3, f_4\}$ είναι βάση Gröbner του ιδεώδους I. Ωστόσο το σύνολο $G = \{f_2, f_3, f_4\}$ είναι βάση Gröbner του ιδεώδους I, καθώς το αρχικό μονώνυμο $lm(f_1)$ διαιρείται από το αρχικό μονώνυμο $lm(f_3)$. Στην πραγματικότητα το σύνολο $G = \{f_2, f_3, f_4\}$ είναι ανάγωγη βάση Gröbner του ιδεώδους I ως προς τη λεξικογραφική διάταξη όρων $\prec$, με $x > y$ αφού δεν υπάρχει όρος των πολυωνύμων της βάσης που να διαιρείται από κάποιο αρχικό μονώνυμο διαφορετικού πολυωνύμου αυτής. Άρα το αρχικό ιδεώδες είναι $Lt_{\prec}(I) = \langle xy^2, x^2, y^3 \rangle$. Συνεπώς τα κανονικά μονώνυμα είναι τα εξής $\{1, x, y, y^2, xy\}$. Σύμφωνα με το λήμμα 1.5.2, μια βάση για τον $\mathbb{Q}[x, y]/I$ αποτελείται από τα σύμπλοκα $\{1+I, x+I, y+I, y^2+I, xy+I\}$, συνεπώς η διάσταση του $\mathbb{Q}[x, y]/I$ είναι ίση με 5.

Πόρισμα 1.5.5. *Αν $L = Lt_{\prec}(I)$ και $M = Lt_{\prec'}(I)$ είναι δύο αρχικά ιδεώδη ενός ιδεώδους I του $K[x_1, ..., x_n]$ ως προς δύο διαφορετικές διατάξεις όρων $\prec$ και $\prec'$ αντίστοιχα, με $L \subseteq M$, τότε $L = M$.*

Απόδειξη. Έστω I ένα ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$ και $\prec$, $\prec'$ δύο διαφορετικές διατάξεις όρων του ιδεώδους. Έστω $L = Lt_{\prec}(I)$ το αρχικό ιδεώδες του I ως προς τη διάταξη $\prec$ και $M = Lt_{\prec'}(I)$ το αρχικό ιδεώδες του I ως προς τη διάταξη $\prec'$. Ισχυριζόμαστε ότι $M \subseteq L$, έστω όχι θα καταλήξουμε σε άτοπο. Εφόσον L και M είναι μονωνυμικά αρχικά ιδεώδη, και $M \subsetneq L$ συνεπάγεται πως υπάρχει ένα μονώνυμο $\mathbf{x}^{\mathbf{u}}$ τέτοιο ώστε $\mathbf{x}^{\mathbf{u}} \in M - L$. Το M είναι αρχικό ιδεώδες του I ως προς τη διάταξη $\prec'$ κι άρα ιδεώδες του $K[x_1, ..., x_n]$. Σύμφωνα λοιπόν με το λήμμα 1.5.2, το σύνολο των συμπλόκων των κανονικών μονωνύμων του $K[x_1, ..., x_n]$ αποτελεί βάση για τον K-διανυσματικό χώρο $K[x_1, ..., x_n]/I$. Έστω το σύνολο $\{x^{\mathbf{u}_1} + I, ..., x^{\mathbf{u}_t} + I\}$, η βάση του $K[x_1, ..., x_n]/I$, με $x^{\mathbf{u}_i} \notin M$ για κάθε $i = 1, ..., t$. Το μονώνυμο $\mathbf{x}^{\mathbf{u}} \in K[x_1, ..., x_n]$, συνεπώς το $\mathbf{x}^{\mathbf{u}} + I \in K[x_1, ..., x_n]/I$. Ωστόσο το μονώνυμο $\mathbf{x}^{\mathbf{u}} \in M$ δεν είναι κανονικό, συνεπώς δεν είναι στοιχείο της βάσης, άρα το $\mathbf{x}^{\mathbf{u}} + I$ μπορεί να γραφεί ως γραμμικός συνδυασμός των στοιχείων αυτής. Δηλαδή

$$\mathbf{x}^{\mathbf{u}} + I = c_1(\mathbf{x}^{\mathbf{u}_1} + I) + ... + c_t(\mathbf{x}^{\mathbf{u}_t} + I)$$

$$\mathbf{x}^{\mathbf{u}} + I = (c_1\mathbf{x}^{\mathbf{u}_1} + ... + c_t\mathbf{x}^{\mathbf{u}_t}) + I$$

$$\mathbf{x}^{\mathbf{u}} - (c_1\mathbf{x}^{\mathbf{u}_1} + ... + c_t\mathbf{x}^{\mathbf{u}_t}) = 0 + I$$

άρα

$$\mathbf{x}^{\mathbf{u}} - (c_1\mathbf{x}^{\mathbf{u}_1} + ... + c_t\mathbf{x}^{\mathbf{u}_t}) \in I.$$

Έστω $g = \mathbf{x}^{\mathbf{u}} - (c_1\mathbf{x}^{\mathbf{u}_1} + ... + c_t\mathbf{x}^{\mathbf{u}_t})$. Εξ' υποθέσεως $\mathbf{x}^{\mathbf{u}} \notin L$. Επιπλέον τα μονώνυμα $x^{\mathbf{u}_i} \notin M$, για κάθε $i = 1, ..., t$, κι αφού $L \subseteq M$ έχουμε ότι τα μονώνυμα $x^{\mathbf{u}_i} \notin L$ για κάθε $i = 1, ..., t$. Συνεπώς, βρήκαμε ένα πολυώνυμο g κανένας όρος του οποίου δεν ανήκει στο L ως προς τη διάταξη $\prec$, οπότε ούτε ο αρχικός όρος του g δεν ανήκει στο L, ενώ το πολυώνυμο g είναι στοιχείο του ιδεώδους I. Άτοπο, διότι από τον ορισμό του αρχικού ιδεώδους γνωρίζουμε ότι $L = Lt_{\prec}(I) = \langle lt(f) : f \in I \rangle$. Πράγματι λοιπόν ισχύει ότι $M \subseteq L$, επιπλέον από την υπόθεση έχουμε ότι $L \subseteq M$ άρα, $L = M$. □

Υπάρχουν άπειρες διατάξεις όρων στον πολυωνυμικό δακτύλιο $K[x_1, ..., x_n]$, για $n \geq 2$. Μπορούμε όμως να τις ομαδοποιήσουμε σε πεπερασμένες κλάσεις ισοδυναμίας σταθεροποιώντας ένα ιδεώδες I του $K[x_1, ..., x_n]$, κι έχοντας ως κριτήριο το αρχικό ιδεώδες του I. Δηλαδή, οι διατάξεις όρων του ιδεώδους I που βρίσκονται στην ίδια κλάση ισοδυναμίας, έχουν το ίδιο αρχικό ιδεώδες. Η ύπαρξη λοιπόν πεπερασμένου πλήθους αρχικών ιδεωδών του I, αποδεικνύεται στο ακόλουθο θεώρημα.

Πρόταση 1.5.6. *Έστω I ιδεώδες του $K[x_1, ..., x_n]$. Υπάρχει πεπερασμένο πλήθος διαφορετικών αρχικών ιδεωδών του I.*

Απόδειξη. Έστω I ένα ιδεώδες του $K[x_1, ..., x_n]$, το οποίο έχει άπειρο πλήθος αρχικών ιδεωδών. Έστω Σ_0 το σύνολο των αρχικών ιδεωδών του I. Αφού το Σ_0 είναι μη πεπερασμένο, το ιδεώδες I θα είναι μη μηδενικό. Πράγματι αν το ιδεώδες I ήταν μηδενικό, τότε θα έχει μόνο ένα αρχικό ιδεώδες το $\langle 0 \rangle$, άτοπο. Συνεπώς,

υπάρχει πολυώνυμο $f_1 \in I$ και $f_1 \neq 0$. Το f_1 έχει πεπερασμένο πλήθος όρων έστω $f_1 = a_0k_0 + ... + a_sk_s$ όπου k_i μονώνυμα του f_1, για $i = 1, ..., s$. Κάθε αρχικό ιδεώδες $Lt(I)$ του Σ_0 περιέχει κάποιον όρο του f_1. Το σύνολο Σ_0 είναι άπειρο έστω

$$\Sigma_0 = \Sigma_{01} \bigcup \Sigma_{02} \bigcup ... \bigcup \Sigma_{0s+1} \text{ όπου}$$

$\Sigma_{01} = \{Lt(I) \in \Sigma_0 : k_0 \in Lt(I)\}$
$\Sigma_{02} = \{Lt(I) \in \Sigma_0 : k_1 \in Lt(I)\}$
...
$\Sigma_{0s+1} = \{Lt(I) \in \Sigma_0 : k_s \in Lt(I)\}$.
Εφόσον το Σ_0 είναι άπειρο κάποιο από τα $\Sigma_{01}, ..., \Sigma_{0s+1}$ θα είναι άπειρο. Υποθέτουμε ότι το σύνολο $\Sigma_{01} = \{Lt(I) : k_0 \in Lt(I)\}$ είναι άπειρο και θέτουμε $\Sigma_{01} = \Sigma_1$. Έτσι υπάρχουν άπειρα αρχικά ιδεώδη που περιέχουν το ιδεώδες $\langle k_0 \rangle$ (όλα τα ιδεώδη του συνόλου Σ_1). Ακόμη υπάρχει μια διάταξη όρων $\prec_1$ τέτοια ώστε

$$Lt_{\prec_1}(I) \supsetneq \langle k_0 \rangle.$$

Διαφορετικά το τυχαίο αρχικό ιδεώδες $Lt_{\prec_1}(I)$ του Σ_1 θα ήταν το $\langle k_0 \rangle$ κατά συνέπεια το σύνολο Σ_1 θα ήταν πεπερασμένο. Τα ιδεώδη $\langle k_0 \rangle$ και $Lt_{\prec_1}(I)$ είναι μονωνυμικά ιδεώδη συνεπάγεται ότι υπάρχει μονώνυμο $m_0 \notin \langle k_0 \rangle$ και $m_0 \in Lt_{\prec_1}(I)$. Το m_0 δεν είναι κανονικό μονώνυμο ως προς τη διάταξη όρων $\prec_1$, οπότε σύμφωνα με το λήμμα 1.5.2, το σύμπλοκο του m_0 γράφεται ως γραμμικός συνδυασμός των συμπλόκων των κανονικών μονωνύμων ως προς τη διάταξη όρων $\prec_1$. Έστω τα σύμπλοκα αυτά είναι $m_1 + I, ..., m_t + I$. Δηλαδή,

$$m_0 + I = (b_1m_1 + ... + b_tm_t) + I.$$

Άρα υπάρχει πολυώνυμο

$$f_2 = m_0 - (b_1m_1 + ... + b_tm_t) \in I, f_2 \neq 0$$

και κανένα μονώνυμο του f_2 δεν ανήκει στο ιδεώδες $\langle k_0 \rangle$, αφού $m_0 \notin \langle k_0 \rangle$ και τα $m_1, ..., m_t$ είναι κανονικά ως προς το ιδεώδες I και τη διάταξη όρων $\prec_1$. Το πολυώνυμο f_2 έχει πεπερασμένο πλήθος όρων. Κάθε αρχικό ιδεώδες $Lt(I)$ του Σ_1 περιέχει κάποιον όρο του f_2. Το σύνολο Σ_1 είναι άπειρο έστω

$$\Sigma_1 = \Sigma_{11} \bigcup \Sigma_{12} \bigcup ... \bigcup \Sigma_{1(t+1)} \text{ όπου}$$

$\Sigma_{11} = \{Lt(I) \in \Sigma_1 : m_0 \in Lt(I)\}$
$\Sigma_{12} = \{Lt(I) \in \Sigma_1 : m_1 \in Lt(I)\}$
...
$\Sigma_{1(t+1)} = \{Lt(I) \in \Sigma_1 : m_t \in Lt(I)\}$.
Εφόσον το Σ_1 είναι άπειρο κάποιο από τα $\Sigma_{11}, ..., \Sigma_{1(t+1)}$ θα είναι άπειρο. Υποθέτουμε ότι το σύνολο $\Sigma_{11} = \{Lt(I) \in \Sigma_1 : m_0 \in Lt(I)\}$ είναι άπειρο και θέτουμε $\Sigma_{11} = \Sigma_2$. Αφού $m_0 \notin \langle k_0 \rangle$. Συνεπώς $\langle k_0 \rangle \subsetneq \langle k_0, m_0 \rangle$. Υπάρχουν άπειρα αρχικά ιδεώδη που περιέχουν το ιδεώδες $\langle k_0, m_0 \rangle$ (όλα τα ιδεώδη του συνόλου Σ_2). Ακόμη υπάρχει διάταξη όρων $\prec_2$ τέτοια ώστε

$$Lt_{\prec_2}(I) \supsetneq \langle k_0, m_0 \rangle.$$

Διαφορετικά το τυχαίο αρχικό ιδεώδες $Lt_{\prec_2}(I)$ θα ήταν το $\langle k_0, m_0 \rangle$ και κατά συνέπεια το σύνολο Σ_2 θα ήταν πεπερασμένο. Τα ιδεώδη $\langle k_0, m_0 \rangle$ και $Lt_{\prec_2}(I)$

είναι μονωνυμικά ιδεώδη συνεπάγεται ότι υπάρχει μονώνυμο $n_0 \notin \langle k_0, m_0\rangle$ και $n_0 \in Lt_{\prec_2}(I)$. Το n_0 δεν είναι κανονικό μονώνυμο ως προς τη διάταξη όρων $\prec_2$, οπότε σύμφωνα με το λήμμα 1.5.2, το σύμπλοκο του n_0 γράφεται ως γραμμικός συνδυασμός των συμπλόκων των κανονικών μονωνύμων ως προς τη διάταξη όρων $\prec_2$. Έστω τα σύμπλοκα αυτά είναι τα $n_1 + I, ..., n_l + I$. Δηλαδή,

$$n_0 + I = (c_1 n_1 + ... + c_l n_l) + I.$$

Άρα υπάρχει πολυώνυμο

$$f_3 = n_0 - (c_1 n_1 + ... + c_l n_l) \in I, f_3 \neq 0$$

και κανένα μονώνυμο του f_3 δεν ανήκει στο ιδεώδες $\langle k_0, m_0\rangle$, αφού $n_0 \notin \langle k_0, m_0\rangle$ και τα $n_1, ..., n_l$ είναι κανονικά μονώνυμα ως προς το ιδεώδες I και τη διάταξη όρων $\prec_2$. Το πολυώνυμο f_3 έχει πεπερασμένο πλήθος όρων. Κάθε αρχικό ιδεώδες $Lt(I)$ του Σ_2 περιέχει κάποιον όρο του f_3. Το σύνολο Σ_2 είναι άπειρο έστω

$$\Sigma_2 = \Sigma_{21} \bigcup \Sigma_{22} \bigcup ... \bigcup \Sigma_{2(l+1)} \text{ όπου}$$

$\Sigma_{21} = \{Lt(I) \in \Sigma_2 : n_0 \in Lt(I)\}$
$\Sigma_{22} = \{Lt(I) \in \Sigma_2 : n_1 \in Lt(I)\}$
...
$\Sigma_{2(l+1)} = \{Lt(I) \in \Sigma_2 : n_l \in Lt(I)\}$.
Εφόσον το Σ_2 είναι άπειρο κάποιο από τα $\Sigma_{21}, ..., \Sigma_{2(l+1)}$ θα είναι άπειρο. Υποθέτουμε ότι το σύνολο $\Sigma_{21} = \{Lt(I) \in \Sigma_2 : n_0 \in Lt(I)\}$ είναι άπειρο και θέτουμε $\Sigma_{21} = \Sigma_3$. Αφού $n_0 \notin \langle k_0, m_0\rangle$. Συνεπώς $\langle k_0, m_0\rangle \subsetneq \langle k_0, m_0, n_0\rangle$. Υπάρχουν άπειρα αρχικά ιδεώδη που περιέχουν το ιδεώδες $\langle k_0, m_0, n_0\rangle$ (όλα τα ιδεώδη του συνόλου Σ_3). Ακόμη υπάρχει διάταξη όρων $\prec_3$ τέτοια ώστε

$$Lt_{\prec_3}(I) \supsetneq \langle k_0, m_0, n_0\rangle.$$

Διαφορετικά το τυχαίο αρχικό ιδεώδες $Lt_{\prec_3}(I)$ θα ήταν το $\langle k_0, m_0, n_0\rangle$ κατά συνέπεια το σύνολο Σ_3 θα ήταν πεπερασμένο. Τα ιδεώδη $\langle k_0, m_0, n_0\rangle$ και $Lt_{\prec_3}(I)$ είναι μονωνυμικά ιδεώδη συνεπάγεται ότι υπάρχει μονώνυμο $q_0 \notin \langle k_0, m_0, n_0\rangle$ και $q_0 \in Lt_{\prec_3}(I)$. Το q_0 δεν είναι κανονικό μονώνυμο ως προς τη διάταξη όρων $\prec_3$, οπότε σύμφωνα με το λήμμα 1.5.2, το σύμπλοκο του q_0 γράφεται ως γραμμικός συνδυασμός των συμπλόκων των κανονικών μονωνύμων ως προς τη διάταξη όρων $\prec_3$. Έστω τα σύμπλοκα αυτά είναι τα $q_1 + I, ..., q_z + I$. Δηλαδή,

$$q_0 + I = (d_1 q_1 + ... + d_z q_z) + I.$$

Συνεχίζοντας με τον ίδιο τρόπο βρίσκουμε μία γνησίως αύξουσα ακολουθία ιδεωδών

$$\langle k_0\rangle \subset \langle k_0, m_0\rangle \subset \langle k_0, m_0, n_0\rangle \subset ... \subset \langle k_0, ..., r_0\rangle \subset \langle k_0, ..., r_0, s_0\rangle \subset ...$$

η οποία δε σταματάει ποτέ. Όμως ο πολυωνυμικός δακτύλιος $K[x_1, ..., x_n]$ είναι δακτύλιος της Noether, δηλαδή κάθε αύξουσα ακολουθία ιδεωδών του $K[x_1, ..., x_n]$ είναι τελικά σταθερή. Επομένως υπάρχει ένα σημείο στο οποίο η αύξουσα ακολουθία ιδεωδών σταθεροποιείται δηλαδή:

$$\langle k_0, ..., s_0\rangle = \langle k_0, ..., s_0, t_0\rangle = ...$$

Άρα, καταλήξαμε σε άτοπο αφού αποδείξαμε ότι έχουμε μια αυστηρά αύξουσα ακολουθία ιδεωδών . Συνεπώς, κάθε ιδεώδες I του $K[x_1, ..., x_n]$ έχει πεπερασμένο πλήθος διαφορετικών αρχικών ιδεωδών. □

Πρόταση 1.5.7. *Έστω I ένα ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$ και $\prec_1, \prec_2$ δύο διαφορετικές διατάξεις όρων. Αν τα αρχικά ιδεώδη του ιδεώδους I ως προς δύο διαφορετικές διατάξεις όρων $\prec_1$ και $\prec_2$ ταυτίζονται, τότε ταυτίζονται και οι αντίστοιχες ανάγωγες βάσεις Gröbner του I.*

Απόδειξη. Έστω I ένα ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$ και $\prec_1$, $\prec_2$ δύο διαφορετικές διατάξεις όρων.
Έστω $\{q_1, ..., q_s\}$ η ανάγωγη βάση Gröbner του I, ως προς τη διάταξη όρων $\prec_1$. Τότε έχουμε $lc(q_i) = 1$ για κάθε $i = 1, ..., s$, και κανένας όρος του q_j δεν διαιρείται από κάποιο αρχικό μονώνυμο $lm(q_i)$, για $j \neq i$ με $j = 1, ..., s$. Ενώ το σύνολο $\{q_1, ..., q_s\}$ είναι βάση Gröbner του I. Σύμφωνα με την πρόταση 1.3.10 το αρχικό ιδεώδες $Lt_{\prec_1}(I) = \langle lm_{\prec_1}(q_1), ..., lm_{\prec_1}(q_s)\rangle$, είναι ελαχιστοτικό σύνολο γεννητόρων, αφού η βάση $\{q_1, ..., q_s\}$ είναι ανάγωγη βάση Gröbner του I.
Έστω $\{p_1, ..., p_t\}$ η ανάγωγη βάση Gröbner του I, ως προς τη διάταξη όρων $\prec_2$. Τότε έχουμε $lc(p_j) = 1$ για κάθε $j = 1, ..., t$, και δεν υπάρχει όρος του p_k που να διαιρείται από κάποιο αρχικό μονώνυμο $lm(p_j)$, για $k \neq j$ με $k = 1, ..., t$. Ενώ το σύνολο $\{p_1, ..., p_t\}$ είναι βάση Gröbner του I. Σύμφωνα με την πρόταση 1.3.10 το αρχικό ιδεώδες $Lt_{\prec_2}(I) = \langle lm_{\prec_2}(p_1), ..., lm_{\prec_2}(p_t)\rangle$, το οποίο είναι ελαχιστοτικό σύνολο γεννητόρων αφού, αφού η βάση $\{p_1, ..., p_t\}$ είναι ανάγωγη βάση Gröbner του I.
Όμως έχουμε $Lt_{\prec_1}(I) = Lt_{\prec_2}(I)$, άρα

$$\langle lm_{\prec_1}(q_1), ..., lm_{\prec_1}(q_s)\rangle = \langle lm_{\prec_2}(p_1), ..., lm_{\prec_2}(p_t)\rangle.$$

Ωστόσο γνωρίζουμε ότι ένα μονωνυμικό ιδεώδες έχει μοναδικό ελαχιστοτικό σύνολο γεννητόρων. Άρα $\{lm_{\prec_1}(q_1), ..., lm_{\prec_1}(q_s)\} = \{lm_{\prec_2}(p_1), ..., lm_{\prec_2}(p_t)\}$. Συνεπώς το $s = t$ και τα διατάσσουμε ξανά έτσι ώστε:
$lm_{\prec_1}(q_i) = lm_{\prec_2}(p_i)$, για $i = 1, ..., s$.
Είναι $lm_{\prec_1}(q_1) = lm_{\prec_2}(p_1), lc_{\prec_1}(q_1) = lc_{\prec_2}(p_1)$, θα δείξουμε ότι $q_1 = p_1$.
Ισχυριζόμαστε ότι $q_1 - p_1 = 0$. Έστω όχι, θα καταλήξουμε σε άτοπο.
Έχουμε $q_1, p_1 \in I$ συνεπώς $q_1 - p_1 \in I$. Επιλέγουμε τη διάταξη όρων $\prec_1$. Τότε $lm_{\prec_1}(q_1 - p_1) \in Lt_{\prec_1}(I) = \langle lm_{\prec_1}(q_1), ..., lm_{\prec_1}(q_s)\rangle$ συνεπώς σύμφωνα με το πόρισμα 1.4.22 υπάρχει ένα $j \in \{1, ..., s\}$ τέτοιο ώστε το μονώνυμο $lm_{\prec_1}(q_j)$ να διαιρεί το μονώνυμο $lm_{\prec_1}(q_1 - p_1)$. Το $j \neq 1$, αφού $lm_{\prec_1}(q_1 - p_1) < lm_{\prec_1}(q_1) = lm_{\prec_2}(p_1)$. Ο όρος $lm_{\prec_1}(q_1 - p_1)$, είναι όρος του q_1 ή του p_1 ή και των δύο.
Έστω ότι ο $lm_{\prec_1}(q_1 - p_1)$ είναι όρος του q_1, τότε το μονώνυμο $lm_{\prec_1}(q_j)$ διαιρεί όρο του q_1, άτοπο αφού το σύνολο $\{q_1, ..., q_s\}$ είναι ανάγωγη βάση Gröbner του I.
Έστω ότι ο $lm_{\prec_1}(q_1 - p_1)$ είναι όρος του p_1, τότε το μονώνυμο $lm_{\prec_1}(q_j) = lm_{\prec_2}(p_j)$ διαιρεί όρο του p_1, άτοπο αφού το σύνολο $\{p_1, ..., p_t\}$ είναι ανάγωγη βάση Gröbner του I.
Άρα $q_1 - p_1 = 0$, συνεπώς $q_1 = p_1$. Όμοια $q_i = p_i$ για κάθε $i = 1, ..., s$. Άρα οι ανάγωγες βάσεις Gröbner του I ως προς τις διατάξεις όρων $\prec_1, \prec_2$, ταυτίζονται.
□

Πόρισμα 1.5.8. *Έστω I ιδεώδες του $K[x_1, ..., x_n]$. Υπάρχει πεπερασμένο σύνολο γενητόρων του I το οποίο αποτελεί βάση Gröbner του I ως προς οποιαδήποτε διάταξη όρων.*

Απόδειξη. Έστω I ένα ιδεώδες του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$. Αν τα αρχικά ιδεώδη του ιδεώδους I ως προς δύο διαφορετικές διατάξεις όρων $\prec_1$ και $\prec_2$ ταυτίζονται, τότε ταυτίζονται και οι αντίστοιχες ανάγωγες βάσεις Gröbner του

I σύμφωνα με την πρόταση 1.5.7. Από την πρόταση 1.5.6 γνωρίζουμε ότι υπάρχει πεπερασμένο πλήθος αρχικών ιδεωδών $\{J_1, ..., J_q\}$. Έστω $G_i = \{g_{i_1}, ..., g_{i_{s_i}}\}$, $1 \leq i \leq q$, η αντίστοιχη ανάγωγη βάση Gröbner για το αρχικό ιδεώδες J_i. Ισχυριζόμαστε ότι η ένωση των αντίστοιχων ανάγωγων βάσεων Gröbner $\bigcup_{i=1}^{q} G_i$, είναι το ζητούμενο πεπερασμένο σύνολο γεννητόρων για το I, το οποίο αποτελεί βάση Gröbner του I ως προς οποιαδήποτε διάταξη όρων. Πράγματι αν $\prec$ είναι μια τυχαία διάταξη όρων, τότε το αρχικό ιδεώδες $Lt_{\prec}(I)$ ισούται με το J_k, για κάποιο $1 \leq k \leq q$, σύμφωνα με τα παραπάνω. Άρα η ανάγωγη βάση Gröbner ως προς τη διάταξη όρων $\prec$ είναι η G_k. Είναι $G_k \subseteq \bigcup_{i=1}^{q} G_i$, δηλαδή η $\bigcup_{i=1}^{q} G_i$ περιέχει μια βάση Gröbner. Εφόσον τα υπόλοιπα στοιχεία της ανήκουν στο ιδεώδες I συμπεραίνουμε ότι η $\bigcup_{i=1}^{q} G_i$ είναι βάση Gröbner του I. □

Ορισμός 1.5.9. *Η* ***καθολική βάση Gröbner*** *ορίζεται ως η ένωση όλων των ανάγωγων βάσεων Gröbner ενός ιδεώδους I, ως προς οποιαδήποτε διάταξη όρων.*

Από το τελευταίο πόρισμα έπεται ότι για ένα ιδεώδες I πάντα υπάρχει μία καθολική βάση Gröbner. Η καθολική βάση Gröbner είναι ένα πεπερασμένο υποσύνολο του ιδεώδους I, το οποίο αποτελεί βάση Gröbner ως προς οποιαδήποτε διάταξη όρων. Οι καθολικές βάσεις Gröbner εισήχθηκαν από τον V. Weispfenning στο άρθρο [20] (1987) και τον Niels Schwartz στο άρθρο [18] (1988).

Κεφάλαιο 2

Τορικά Ιδεώδη και βάσεις Graver

Σε αυτό το κεφάλαιο το ενδιαφέρον μας θα επικεντρωθεί στα τορικά ιδεώδη και τις βάσεις Graver. Οι βάσεις Graver είναι πολύ σημαντικές στα εφαρμοσμένα μαθηματικά, καθώς επιτρέπουν επαναληπτικές λύσεις γραμμικών και ποικίλων μη γραμμικών προβλημάτων ακέραιου προγραμματισμού σε πολυωνυμικό χρόνο. Η σύνδεση τους με τη θεωρία των βάσεων Gröbner περιγράφεται στο βιβλίο [19] του B.Sturmfels. Η θεωρία αλγορίθμων των βάσεων Graver και η εφαρμογή τους στον ακέραιο προγραμματισμό περιγράφεται στα βιβλία [12] και [13] του Shmuel Onn. Ωστόσο οι βάσεις Graver είναι πολύ σημαντικές όπως θα δούμε, εκτός από τον ακέραιο προγραμματισμό και στην άλγεβρα. Στο κεφάλαιο αυτό, το βασικό μας εργαλείο θα είναι τα διώνυμα και πιο συγκεκριμένα τα διωνυμικά ιδεώδη, ιδεώδη που παράγονται από διωνυμικούς γεννήτορες. Με τον όρο διώνυμα εννοούμε πολυώνυμα του πολυωνυμικού δακτυλίου $K[x_1, ..., x_n]$, τα οποία προκύπτουν ως διαφορές μονωνύμων. Για παράδειγμα, το $x^4yz - yz^6$ είναι ένα διώνυμο του πολυωνυμικού δακτυλίου $K[x, y, z]$. Πολλά σημαντικά υποσύνολα διωνύμων του ιδεώδους ανήκουν στη βάση Graver τα οποία την καθιστούν ιδιαίτερα σημαντική. Τα υποσύνολα αυτά είναι το σύνολο των κυκλωμάτων, οι ανάγωγες βάσεις Gröbner, η καθολική βάση Gröbner. Όπως επίσης και μια τουλάχιστον ελαχιστοτική βάση Markov. Στην περίπτωση μάλιστα που $(\mathbb{N}A) \bigcap -(\mathbb{N}A) = \{0\}$ όλες οι ελαχιστοτικές βάσεις Markov βρίσκονται στη βάση Graver. Όπως γίνεται λοιπόν αντιληπτό η χρησιμότητα των βάσεων Graver είναι μεγάλη.
Τα διωνυμικά ιδεώδη βρίσκουν εφαρμογή σε διάφορους κλάδους των μαθηματικών, όπως στην άλγεβρα, στη στατιστική, στην αλγεβρική γεωμετρία, στη θεωρία γραφημάτων, στις διαφορικές εξισώσεις, αλλά και στη μαθηματική βιολογία, στη θεωρητική φυσική και στο γεωμετρικό σχεδιασμό με τη βοήθεια υπολογιστών. Μία ειδική κατηγορία διωνυμικών ιδεωδών είναι τα τορικά ιδεώδη, τα οποία θα μας απασχολήσουν κατά κύριο λόγο στο κεφάλαιο αυτό.

2.1 Τορικά Ιδεώδη

Σταθεροποιούμε ένα σύνολο μη μηδενικών διανυσμάτων $\mathbf{A} = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\} \subseteq \mathbb{Z}^m \subseteq \mathbb{Q}^m$. Θεωρούμε τον πολυωνυμικό δακτύλιο Laurent $K[t_1, \ldots, t_m, t_1^{-1}, \ldots, t_m^{-1}]$.

Θεωρούμε τον ακόλουθο ομομορφισμό ημιομάδων:

$$deg_{\mathbf{A}} : \mathbb{N}^n \longrightarrow \mathbb{Z}^m$$

$$\mathbf{u} \mapsto u_1\mathbf{a}_1 + \ldots + u_n\mathbf{a}_n,$$

όπου $\mathbf{u} = (u_1, \ldots, u_n)$. Η εικόνα δηλαδή του $\mathbf{u}$ ταυτίζεται με τον $\mathbf{A}-$βαθμό του μονωνύμου $x^{\mathbf{u}}$ που θα ορίσουμε στη συνέχεια. Η εικόνα της $deg_{\mathbf{A}}$ είναι η ημιομάδα:

$$\mathbb{N}\mathbf{A} = \{\lambda_1\mathbf{a}_1 + \ldots + \lambda_n\mathbf{a}_n : \lambda_1, \ldots, \lambda_n \in \mathbb{N}_0\}.$$

Επιπλέον υποθέτουμε ότι η ημιομάδα $\mathbb{N}\mathbf{A}$ είναι θετικό μονοειδές. Με τον όρο *θετικό μονοειδές* ορίζουμε την ημιομάδα όπου το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του στην ημιομάδα είναι το μηδενικό.

Η απεικόνιση $deg_{\mathbf{A}}$ επάγει τον ομομορφισμό δακτυλίων:

$$\Phi : K[x_1, ..., x_n] \longrightarrow K[t_1, \ldots, t_m, t_1^{-1}, \ldots, t_m^{-1}]$$

$$x_i \mapsto t^{\mathbf{a}_i}.$$

Σε αυτό το σημείο θα ορίσουμε μία βαθμολόγηση στον δακτύλιο πολυωνύμων $K[x_1, ..., x_n]$ θέτοντας $deg(x_i) = \mathbf{a}_i$, για $i = 1, \ldots, n$.

Ορισμός 2.1.1. (**A** – *βαθμός μονωνύμου* – **A** – *degree of a monomial*) *Ορίζουμε* **A**– ***βαθμό του μονωνύμου*** $\mathbf{x}^{\mathbf{u}} = x_1^{u_1} ... x_n^{u_n}$ *ως:*

$$deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}}) = u_1\mathbf{a}_1 + ... + u_n\mathbf{a}_n \in \mathbb{N}\mathbf{A},$$

όπου $\mathbf{u} = (u_1, ..., u_n) \in \mathbb{N}^n$.

Μια χαρακτηριστική ιδιότητα του $\mathbf{A}-$ βαθμού των μονωνύμων $x^{\mathbf{a}}, x^{\mathbf{b}}$ είναι η ακόλουθη:

$$deg_A(x^{\mathbf{a}} \cdot x^{\mathbf{b}}) = deg_A(x^{\mathbf{a}}) + deg_A(x^{\mathbf{b}}).$$

Η βαθμολόγηση αυτή προκύπτει από τον ομομορφισμό Φ. Το σύνολο των βαθμών των πολυωνύμων του $K[x_1, ..., x_n]$ είναι το μονοειδές $\mathbb{N}\mathbf{A}$. Ένα πολυώνυμο f του $K[x_1, ..., x_n]$ θα είναι $\mathbf{A}$-ομογενές, αν είναι ομογενές με την παραπάνω βαθμολόγηση. Δηλαδή, οποιαδήποτε δύο μονώνυμα $\mathbf{x}^{\mathbf{u}}$ και $\mathbf{x}^{\mathbf{v}}$ του πολυωνύμου f είναι $\mathbf{A}$-ομογενή:

$$deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}}).$$

Ορισμός 2.1.2. *Ο πυρήνας της απεικόνισης* Φ *καλείται* ***τορικό ιδεώδες*** *(toric ideal) του* $\mathbf{A}$ *και συμβολίζεται με* $I_{\mathbf{A}}$.

Παράδειγμα 2.1.3. Θεωρούμε το υποσύνολο $\mathbf{A} = \{\mathbf{a}_1 = (4, 0), \mathbf{a}_2 = (3, 1), \mathbf{a}_3 = (1, 3), \mathbf{a}_4 = (0, 4)\}$ του $\mathbb{Z}^2$ και τον ομομορφισμό ημιομάδων

$$deg_{\mathbf{A}} : \mathbb{N}^4 \longrightarrow \mathbb{Z}^2$$

$$\mathbf{u} = (u_1, u_2, u_3, u_4) \mapsto (4u_1 + 3u_2 + u_3, u_2 + 3u_3 + 4u_4),$$

Η $deg_{\mathbf{A}}$ επάγει τον ομομορφισμό δακτυλίων:

$$\Phi : \mathbf{C}[x, y, z, w] \longrightarrow \mathbf{C}[s^{\pm 1}, t^{\pm 1}]$$

$$x \mapsto s^4$$
$$y \mapsto s^3t$$
$$z \mapsto st^3$$
$$w \mapsto t^4$$

Ο πυρήνας της απεικόνισης Φ είναι το ιδεώδες:

$$\langle yz - xw, y^3 - x^2z, z^3 - yw^2, y^2w - z^2x\rangle.$$

Άρα, το τορικό ιδεώδες του $\mathbf{A}$ είναι το εξής:

$$I_{\mathbf{A}} = \langle yz - xw, y^3 - x^2z, z^3 - yw^2, y^2w - z^2x\rangle.$$

Παράδειγμα 2.1.4. Θεωρούμε το υποσύνολο
$\mathbf{A} = \{\mathbf{a}_1 = (2,1,0), \mathbf{a}_2 = (1,2,0), \mathbf{a}_3 = (0,2,1), \mathbf{a}_4 = (0,1,2), \mathbf{a}_5 = (1,0,2),$
$\mathbf{a}_6 = (2,0,1)\}$ του $\mathbb{Z}^3$ και τον ομομορφισμό ημιομάδων

$$deg_{\mathbf{A}} : \mathbb{N}^6 \longrightarrow \mathbb{Z}^3$$

$\mathbf{u} = (u_1,u_2,u_3,u_4,u_5,u_6) \mapsto (2u_1+u_2+u_5+2u_6, u_1+2u_2+2u_3+u_4, u_3+2u_4+2u_5+u_6),$

Η $deg_{\mathbf{A}}$ επάγει τον ομομορφισμό δακτυλίων:

$$\Phi : \mathbb{C}[x_1,x_2,x_3,x_4,x_5,x_6] \longrightarrow \mathbb{C}[t_1^{\pm 1}, t_2^{\pm 1}, t_3^{\pm 1}]$$

$$x_1 \mapsto t_1^2t_2$$
$$x_2 \mapsto t_1t_2^2$$
$$x_3 \mapsto t_2^2t_3$$
$$x_4 \mapsto t_2t_3^2$$
$$x_5 \mapsto t_1t_3^2$$
$$x_6 \mapsto t_1^2t_3$$

Ο πυρήνας της απεικόνισης Φ είναι το ιδεώδες:
$\langle x_2x_5 - x_3x_6, x_1x_4 - x_3x_6, x_1x_3^2 - x_2^2x_4, x_2^2x_4 - x_3^2x_5, x_1^2x_3 - x_2^2x_6, x_3x_5^2 - x_4^2x_6, x_1x_5^2 - x_4x_6^2, x_1x_3x_5 - x_2x_4x_6\rangle$.
Άρα, το τορικό ιδεώδες του $\mathbf{A}$ είναι το εξής:
$I_{\mathbf{A}} = \langle x_2x_5 - x_3x_6, x_1x_4 - x_3x_6, x_1x_3^2 - x_2^2x_4, x_2^2x_4 - x_3^2x_5, x_1^2x_3 - x_2^2x_6, x_3x_5^2 - x_4^2x_6, x_1x_5^2 - x_4x_6^2, x_1x_3x_5 - x_2x_4x_6\rangle$.

Ορισμός 2.1.5. *Το σύνολο*

$$deg_{\mathbf{A}}^{-1}(\mathbf{x}^{\mathbf{u}}) = \{\mathbf{x}^{\mathbf{v}} \in \mathbb{T}^n : deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}})\}$$

καλείται ***ίνα*** *(fiber) του μονωνύμου* $\mathbf{x}^{\mathbf{u}}$.

Στο μονοειδές $\mathbb{N}\mathbf{A}$ ορίζουμε μια μερική διάταξη η οποία είναι σημαντική για τη θεωρία μας:

Ορισμός 2.1.6. *Ισχύει* $\mathbf{c} \geq \mathbf{d}$ *αν και μόνο αν υπάρχει* $\mathbf{e} \in \mathbb{N}\mathbf{A}$ *τέτοιο ώστε:* $\mathbf{c} = \mathbf{d} + \mathbf{e}$.

Στη συνέχεια θα δούμε ορισμένες ιδιότητες των τορικών ιδεωδών που είναι πολύ βασικές.

Πρόταση 2.1.7. *Το τορικό ιδεώδες $I_{\mathbf{A}}$ είναι πρώτο ιδεώδες του $K[x_1, ..., x_n]$.*

Απόδειξη. Έχουμε:

$$K[x_1, ..., x_n]/\mathrm{Ker}(\Phi) \simeq \Phi(K[x_1, ..., x_n]) \subseteq K[t_1, \ldots, t_m, t_1^{-1}, \ldots, t_m^{-1}],$$

το οποίο είναι ακεραία περιοχή. Άρα, ο πυρήνας $\mathrm{Ker}(\Phi) = I_{\mathbf{A}}$ είναι πρώτο ιδεώδες. □

Μπορούμε να παρουσιάσουμε το τορικό ιδεώδες με ένα διαφορετικό, περισσότερο κατανοητό τρόπο ως ένα σύνολο που γεννάται από διώνυμα με μια χαρακτηριστική ιδιότητα, έχουν το ίδιο $\mathbf{A}-$βαθμό.

Πρόταση 2.1.8. *Το τορικό ιδεώδες $I_{\mathbf{A}}$ παράγεται από τα διώνυμα $\mathbf{x^u - x^v}$, ώστε $deg_{\mathbf{A}}(\mathbf{x^u}) = deg_{\mathbf{A}}(\mathbf{x^v})$, με $\mathbf{u}, \mathbf{v} \in \mathbb{N}^n$. Δηλαδή,*

$$I_{\mathbf{A}} = \langle \mathbf{x^u - x^v} : deg_{\mathbf{A}}(\mathbf{x^u}) = deg_{\mathbf{A}}(\mathbf{x^v}), \text{ όπου } \mathbf{u}, \mathbf{v} \in \mathbb{N}^n \rangle.$$

Απόδειξη. Καταρχήν, παρατηρούμε ότι ένα διώνυμο $\mathbf{x^u - x^v}$ ανήκει στο ιδεώδες $I_{\mathbf{A}}$ αν και μόνο αν είναι $\mathbf{A}$-ομογενές. Δηλαδή, αν και μόνο αν $deg_{\mathbf{A}}(\mathbf{x^u}) = deg_{\mathbf{A}}(\mathbf{x^v})$, όπου $\mathbf{u}, \mathbf{v} \in \mathbb{N}^n$. Αρκεί λοιπόν να δείξουμε ότι το ιδεώδες $I_{\mathbf{A}}$ παράγεται από $\mathbf{A}$-ομογενή διώνυμα. Ισχυριζόμαστε ότι κάθε πολυώνυμο f που ανήκει στο τορικό ιδεώδες $I_{\mathbf{A}}$, γράφεται ως K-γραμμικός συνδυασμός αυτών των διωνύμων. Έστω όχι, θα καταλήξουμε σε άτοπο. Σταθεροποιούμε μία διάταξη όρων $\prec$ στον $K[x_1, ..., x_n]$. Εφόσον το ιδεώδες $I_{\mathbf{A}}$ δεν παράγεται από $\mathbf{A}$-ομογενή διώνυμα υπάρχει κάποιο πολυώνυμο $f \in I_{\mathbf{A}}$, το οποίο δε μπορεί να γραφεί ως K-γραμμικός συνδυασμός των διωνύμων $\mathbf{x^u - x^v}$, με την ιδιότητα $deg_{\mathbf{A}}(\mathbf{x^u}) = deg_{\mathbf{A}}(\mathbf{x^v})$, όπου $\mathbf{u}, \mathbf{v} \in \mathbb{N}^n$. Από όλα αυτά τα πολυώνυμα f, επιλέγουμε ένα πολυώνυμο f, του οποίου ο αρχικός όρος, ως προς τη διάταξη όρων $\prec$, $lt(f) = \mathbf{x^{u_1}}$, είναι ελαχιστοτικός. Έστω $f = c_1\mathbf{x^{u_1}} + ... + c_s\mathbf{x^{u_s}}$. Αφού το f ανήκει στο ιδεώδες $I_{\mathbf{A}} = \mathrm{Ker}(\Phi)$, έπεται ότι $f(\mathbf{t^{a_1}}, \ldots, \mathbf{t^{a_n}}) = 0$. Συνεπώς $c_1\mathbf{t}^{deg_{\mathbf{A}}(\mathbf{x^{u_1}})} + ... + c_s\mathbf{t}^{deg_{\mathbf{A}}(\mathbf{x^{u_s}})} = 0$. Άρα, ο όρος $\mathbf{t}^{deg_{\mathbf{A}}(\mathbf{x^{u_1}})} = \Phi(\mathbf{x^{u_1}})$, πρέπει να απαλειφθεί από τουλάχιστον έναν άλλο όρο του πολυωνύμου f. Έστω ένας από αυτούς είναι ο $\Phi(\mathbf{x^{u_k}})$. Διαφορετικά θα είχαμε $\Phi(f) \neq 0$. Άρα, υπάρχει κάποιο μονώνυμο $\mathbf{x^{u_k}} \prec \mathbf{x^{u_1}}$ του f, τέτοιο ώστε $deg_{\mathbf{A}}(\mathbf{x^{u_k}}) = deg_{\mathbf{A}}(\mathbf{x^{u_1}})$, συνεπώς $\mathbf{x^{u_1}} - \mathbf{x^{u_k}} \in I_{\mathbf{A}}$. Τότε το πολυώνυμο $f' = f - c_1(\mathbf{x^{u_1}} - \mathbf{x^{u_k}}) = f - \mathbf{x^{u_1}} + \mathbf{x^{u_k}} \in I_{\mathbf{A}}$ αφού το πολυώνυμο f και το διώνυμο $\mathbf{x^{u_1}} - \mathbf{x^{u_k}}$ ανήκουν στο ιδεώδες $I_{\mathbf{A}}$ και δε μπορεί να γραφεί ως K-γραμμικός συνδυασμός διωνύμων του τορικού ιδεώδους $I_{\mathbf{A}}$. Παρατηρούμε όμως ότι $lt(f') \prec lt(f)$, το οποίο αντίκειται στην υπόθεση ότι ο αρχικός όρος του f, ως προς τη διάταξη όρων $\prec$, είναι ελαχιστοτικός. □

Θεωρούμε τον πίνακα A του οποίου οι στήλες του είναι τα διανύσματα $\mathbf{a_1}, ..., \mathbf{a_n}$, και τον βλέπουμε ως τη γραμμική απεικόνιση:

$$A : \mathbb{Z}^n \to \mathbb{Z}^d,$$

$$(u_1, \ldots, u_n) \mapsto u_1\mathbf{a_1} + \ldots + u_n\mathbf{a_n}.$$

Στο σημείο αυτό ορίζουμε τον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$.

Ορισμός 2.1.9. *Ο πυρήνας* $\mathrm{Ker}_{\mathbb{Z}}A = \mathrm{Ker}A \bigcap \mathbb{Z}^n$ *είναι δηλαδή τα στοιχεία του πυρήνα* $\mathrm{Ker}A$ *που έχουν ακέραιες συντεταγμένες.*

Είναι:

$$\mathrm{Ker}_{\mathbb{Z}}A = \{(u_1, \ldots, u_n) \in \mathbb{Z}^n : u_1\mathbf{a}_1 + \ldots + u_n\mathbf{a}_n = \mathbf{0}\}.$$

Δοθέντος ενός διανύσματος $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ μπορούμε να το γράψουμε κατά μοναδικό τρόπο ως εξής:

$$\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-,$$

όπου

$$\mathbf{u}^+ = \{(u'_1, \ldots, u'_n) : u'_i = u_i \text{ αν } u_i > 0 \text{ ή } u'_i = 0 \text{ αν } u_i \leq 0\}$$

και

$$\mathbf{u}^- = \{(u'_1, \ldots, u'_n) : u'_i = -u_i \text{ αν } u_i < 0 \text{ ή } u'_i = 0 \text{ αν } u_i \geq 0\}.$$

Για παράδειγμα για το διάνυσμα $\mathbf{u} = (2, -4, 7, -3, 6)$, έχουμε ότι $\mathbf{u}^+ = (2, 0, 7, 0, 6)$ και $\mathbf{u}^- = (0, 4, 0, 3, 0)$.

Μπορούμε σε αυτό το σημείο να ορίσουμε το τορικό ιδεώδες $I_{\mathbf{A}}$ χρησιμοποιώντας το διάνυσμα $\mathbf{u}$ και τον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$.

Παρατήρηση 2.1.10.

$$I_{\mathbf{A}} = \langle \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} : \mathbf{u} \in \mathrm{Ker}_{\mathbb{Z}}A \rangle.$$

Πράγματι, αν $\mathbf{u} \in \mathrm{Ker}_{\mathbb{Z}}A \Leftrightarrow$

$$u_1\mathbf{a}_1 + \ldots + u_n\mathbf{a}_n = \mathbf{0} \Leftrightarrow$$

$$(u_1^+ - u_1^-)\mathbf{a}_1 + \ldots + (u_n^+ - u_n^-)\mathbf{a}_n = \mathbf{0} \Leftrightarrow$$

$$u_1^+\mathbf{a}_1 + \ldots + u_n^+\mathbf{a}_n = u_1^-\mathbf{a}_1 + \ldots + u_n^-\mathbf{a}_n \Leftrightarrow$$

$$deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^-}) \Leftrightarrow$$

$$\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_{\mathbf{A}}.$$

Έχουμε δηλαδή ότι $\mathbf{u} \in \mathrm{Ker}_{\mathbb{Z}}A \Leftrightarrow \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_{\mathbf{A}} \Leftrightarrow deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^-})$.

Ορίζουμε $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^-})$.

Συνεχίζοντας το προηγούμενο παράδειγμα, αν

$$2\mathbf{a}_1 - 4\mathbf{a}_2 + 7\mathbf{a}_3 - 3\mathbf{a}_4 + 6\mathbf{a}_5 = \mathbf{0}, \tag{1}$$

τότε

$$\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} = x_1^2x_3^7\mathbf{x}_5^6 - x_2^4x_4^3,$$

με

$$deg_{\mathbf{A}}(x_1^2x_3^7x_5^6) = 2\mathbf{a}_1 + 7\mathbf{a}_3 + 6\mathbf{a}_5$$

και

$$deg_{\mathbf{A}}(x_2^4x_4^3) = 4\mathbf{a}_2 + 3\mathbf{a}_4.$$

Από τη σχέση (1), έπεται ότι οι βαθμοί είναι ίσοι, κι άρα $x_1^2x_3^7x_5^6 - x_2^4x_4^3$ ανήκει στο τορικό ιδεώδες $I_{\mathbf{A}}$.

Πρόταση 2.1.11. *Για κάθε διάταξη όρων $\prec$, η ανάγωγη βάση Gröbner του τορικού ιδεώδους $I_{\mathbf{A}}$, ως προς τη $\prec$, αποτελείται από ένα πεπερασμένο σύνολο διωνύμων της μορφής $\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} \in I_{\mathbf{A}}$.*

Απόδειξη. Σύμφωνα με το Θεώρημα Βάσης του Hilbert 1.3.11 το τορικό ιδεώδες $I_{\mathbf{A}}$ είναι πεπερασμένα παραγόμενο. Επιπλέον σύμφωνα με την πρόταση 2.1.8, το τορικό ιδεώδες $I_{\mathbf{A}}$ παράγεται από $\mathbf{A}-$ ομογενή διώνυμα. Άρα το σύνολο γεννητόρων του τορικού ιδεώδους $I_{\mathbf{A}}$ είναι ένα πεπερασμένο σύνολο που αποτελείται από $\mathbf{A}-$ ομογενή διώνυμα. Το σύνολο αυτό είναι της μορφής:

$$\{\mathbf{x}^{\mathbf{u}_1} - \mathbf{x}^{\mathbf{v}_1}, \ldots, \mathbf{x}^{\mathbf{u}_s} - \mathbf{x}^{\mathbf{v}_s} / deg_{\mathbf{A}}(\mathbf{u}_i) = deg_{\mathbf{A}}(\mathbf{v}_i), \text{ όπου } \mathbf{u}_i, \mathbf{v}_i \in \mathbb{N}^n \text{ για } 1 \leq i \leq s\}.$$

Σε αυτό θα εφαρμόσουμε τον αλγόριθμο του Buchberger για να βρούμε μια βάση Gröbner. Οι διαδικασίες σχηματισμού S-πολυωνύμων και της αναγωγής διατηρούν τη διωνυμική δομή. Δηλαδή, κάθε S-πολυώνυμο που δημιουργείται από δύο $\mathbf{A}$-ομογενή διώνυμα, είναι και πάλι $\mathbf{A}$-ομογενές διώνυμο. Πράγματι κατά τη διαδικασία σχηματισμού ενός S-πολυωνύμου από δύο $\mathbf{A}$-ομογενή διώνυμα, απαλοίφεται ένας όρος από το ένα $\mathbf{A}$-ομογενές διώνυμο κι ένας όρος από το άλλο. Ο όρος αυτός είναι το ελάχιστο κοινό πολλαπλάσιο των αρχικών μονωνύμων, των δύο $\mathbf{A}$-ομογενών διωνύμων. Έτσι αυτό που μένει είναι είτε ένα $\mathbf{A}$-ομογενές διώνυμο το οποίο προκύπτει ως διαφορά των δυο μονωνύμων που απέμειναν, ένα από κάθε $\mathbf{A}$-ομογενές διώνυμο, είτε το μηδέν στην περίπτωση που τα εναπομείναντα μονώνυμα ταυτίζονται. Όμοια η κανονική μορφή ενός $\mathbf{A}$-ομογενούς διωνύμου, μόδιο ενός συνόλου $\mathbf{A}$-ομογενών διωνύμων, είναι και πάλι $\mathbf{A}$-ομογενές διώνυμο. Πράγματι, έχουμε πως το αρχικό μονώνυμο του $\mathbf{A}$-ομογενούς διωνύμου,g, διαιρεί ένα μονώνυμο,Q, του $\mathbf{A}$-ομογενούς διωνύμου f. Έτσι κατά τη διαδικασία διαίρεσης, αφαιρούμε από το $\mathbf{A}$-ομογενές διώνυμο f, το $\mathbf{A}$-ομογενές διώνυμο g, πολλαπλασιασμένο με ένα μονώνυμο. Με αποτέλεσμα ολόκληρο το μονώνυμο Q του f, να απαλειφθεί από ένα μονώνυμο του g. Άρα αυτό που μένει θα είναι είτε ένα $\mathbf{A}$-ομογενές διώνυμο το οποίο προκύπτει ως διαφορά των δυο μονωνύμων που απέμειναν, ένα από κάθε $\mathbf{A}$-ομογενές διώνυμο, είτε το μηδέν στην περίπτωση που τα εναπομείναντα μονώνυμα ταυτίζονται. Έτσι, μέσω του αλγορίθμου Buchberger η βάση Gröbner που δημιουργείται, αποτελείται από $\mathbf{A}$-ομογενή διώνυμα. Κάνουμε αυτή τη βάση ελαχιστική και στη συνέχεια ανάγωγη. Παρατηρούμε ότι κάθε ανάγωγη βάση Gröbner του τορικού ιδεώδους $I_{\mathbf{A}}$, ως προς οποιαδήποτε διάταξη όρων $\prec$, είναι ένα πεπερασμένο σύνολο $\mathbf{A}$-ομογενών διωνύμων. Διωνύμων δηλαδή, που ανήκουν στο σύνολο $\{\mathbf{x}^{\mathbf{u}} - \mathbf{x}^{\mathbf{v}} : deg_{\mathbf{A}}(\mathbf{u}) = deg_{\mathbf{A}}(\mathbf{v}), \text{ όπου } \mathbf{u}, \mathbf{v} \in \mathbb{N}^n\}$. □

Θα δώσουμε ένα παράδειγμα σχηματισμού ενός $\mathbf{A}-$ομογενούς $S-$πολυωνύμου από $\mathbf{A}-$ομογενή πολυώνυμα.

Παράδειγμα 2.1.12. Θεωρούμε το δακτύλιο $\mathbb{Q}[x, y, z]$ εφοδιασμένο με τη βαθμωτή λεξικογραφική διάταξη με $z > y > x$. Έστω $\mathbf{A} = \{\mathbf{a}_1 = 11, \mathbf{a}_2 = 14, \mathbf{a}_3 = 2\}$. Θεωρούμε τα $\mathbf{A}-$ομογενή διωνυμικά πολυώνυμα $f = z^4y - x^2$ και $g = zy^3 - x^4$ που έχουν ελάχιστο κοινό πολλαπλάσιο $L = z^4y^3$. Το $S-$πολυώνυμο των f και g είναι

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

Τα πολυώνυμα f και g είναι $\mathbf{A}-$ομογενή. Δηλαδή για το πολυώνυμο f έχουμε $deg_{\mathbf{A}}(x^2) = deg_{\mathbf{A}}(z^4y)$ συνεπώς $2\mathbf{a}_1 = \mathbf{a}_2 + 4\mathbf{a}_3$, ενώ για το πολυώνυμο g έχουμε $deg_{\mathbf{A}}(x^4) = deg_{\mathbf{A}}(zy^3)$ συνεπώς $4\mathbf{a}_1 = 3\mathbf{a}_2 + \mathbf{a}_3$. Για το $S-$πολυωνύμο παρατηρούμε ότι διατηρεί τη διωνυμική δομή ενώ εξακολουθεί να είναι $\mathbf{A}-$ομογενές

αφού $deg_{\mathbf{A}}(z^3x^4) = 4\mathbf{a}_1 + 3\mathbf{a}_3 = (3\mathbf{a}_2 + \mathbf{a}_3) + 3\mathbf{a}_3 = 3\mathbf{a}_2 + 4\mathbf{a}_3$ και $deg_{\mathbf{A}}(y^2x^2) = 2\mathbf{a}_1 + 2\mathbf{a}_2 = (\mathbf{a}_2 + 4\mathbf{a}_3) + 2\mathbf{a}_2 = 3\mathbf{a}_2 + 4\mathbf{a}_3$, άρα $deg_{\mathbf{A}}(z^3x^4) = deg_{\mathbf{A}}(y^2x^2)$.

Το ακόλουθο λήμμα είναι ιδιαίτερα σημαντικό, καθώς θα το χρησιμοποιήσουμε σε αρκετές αποδείξεις.

Λήμμα 2.1.13. *Έστω ότι* $deg_A(x^{\mathbf{b}}) = 0 \Rightarrow \mathbf{b} = \mathbf{0}$.

Απόδειξη. Έστω $A = \{\mathbf{a}_1, ..., \mathbf{a}_n\} \subseteq \mathbb{Z}^m \subseteq \mathbb{Q}^m$ ένα σύνολο μη μηδενικών διανυσμάτων. Έστω ότι $deg_A(x^{\mathbf{b}}) = 0$ και $\mathbf{b} = (b_1, ..., b_n) \in \mathbb{N}_0^n$, με $\mathbf{b} \neq 0$ τότε υπάρχει τουλάχιστον μια συνιστώσα του διανύσματος $\mathbf{b}$ μη μηδενική, και χωρίς βλάβη της γενικότητας υποθέτουμε ότι είναι η $b_1 \neq 0$ και μάλιστα $b_1 > 0$. Τότε ο βαθμός
$deg_A(x^{\mathbf{b}}) = 0 \Rightarrow$
$b_1\mathbf{a}_1 + ... + b_n\mathbf{a}_n = 0 \Rightarrow$
$-b_1\mathbf{a}_1 = b_2\mathbf{a}_2 + ... + b_n\mathbf{a}_n \in \mathbb{N}\mathbf{A}$, αφού $b_2, ..., b_n \in \mathbb{N}_0$ και $\mathbf{a}_2, ..., \mathbf{a}_n \in \mathbf{A}$. Δηλαδή έχουμε ότι $b_1\mathbf{a}_1 \in \mathbb{N}\mathbf{A}$ και $-b_1\mathbf{a}_1 \in \mathbb{N}\mathbf{A}$, όμως από τον ορισμό της $\mathbb{N}\mathbf{A}$ το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του είναι το $\mathbf{0}$ συνεπώς $b_1\mathbf{a}_1 = \mathbf{0}$. Εφόσον τα $\mathbf{a}_i \in \mathbf{A}$ είναι μη μηδενικά, έχουμε $b_1 = 0$. Άτοπο, άρα $\mathbf{b} = \mathbf{0}$. □

2.2 Καθολικές Βάσεις Gröbner για Τορικά Ιδεώδη

Στο τέλος του πρώτου κεφαλαίου ορίσαμε την καθολική βάση Gröbner ως την ένωση όλων των ανάγωγων βάσεων Gröbner του ιδεώδους $I_{\mathbf{A}}$ ως προς οποιαδήποτε διάταξη όρων. Τη συμβολίζουμε με $U_{\mathbf{A}}$ και τα κύρια χαρακτηριστικά της είναι πως είναι κι αυτή βάση Gröbner του ιδεώδους ως προς οποιαδήποτε διάταξη όρων και μάλιστα πεπερασμένη σύμφωνα με την πρόταση 1.5.6. Ενώ σύμφωνα με την πρόταση 2.1.11 η καθολική βάση Gröbner $\mathbf{A}$-ομογενών διωνύμων αποτελείται από $\mathbf{A}$-ομογενή διώνυμα. Κύριος στόχος στην ενότητα αυτή, είναι να βρούμε έναν πιο ακριβή τρόπο περιγραφής της καθολικής βάσης Gröbner του $I_{\mathbf{A}}$. Γι'αυτό ξεκινάμε δίνοντας τον ακόλουθο ορισμό.

Ορισμός 2.2.1. *Ένα διώνυμο* $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}}$ *του* $I_{\mathbf{A}}$ *καλείται* ***πρωταρχικό*** *(primitive) αν δεν υπάρχει διώνυμο* $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \neq \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ *του* $I_{\mathbf{A}}$, *τέτοιο ώστε το μονώνυμο* $\mathbf{x}^{\mathbf{v}^+}$ *να διαιρεί το μονώνυμο* $\mathbf{x}^{\mathbf{u}^+}$ *και το μονώνυμο* $\mathbf{x}^{\mathbf{v}^-}$ *να διαιρεί το μονώνυμο* $\mathbf{x}^{\mathbf{u}^-}$.

Παρατήρηση 2.2.2. Αν ένα διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ είναι πρωταρχικό τότε ο

$$\text{μ.κ.δ.}(u_1, ..., u_n) = 1,$$

δηλαδή το διώνυμο είναι ανάγωγο.

Ορισμός 2.2.3. *Το σύνολο των πρωταρχικών διωνύμων καλείται* ***βάση Graver*** *(Graver basis) του* $I_{\mathbf{A}}$ *και συμβολίζεται με* $Gr_{\mathbf{A}}$.

Το όνομα δόθηκε προς τιμή του Jack Graver και του έργου του στον ακέραιο προγραμματισμό.

Πρόταση 2.2.4. *Κάθε στοιχείο της καθολικής βάσης Gröbner του* $I_{\mathbf{A}}$ *είναι πρωταρχικό.*

Απόδειξη. Έστω $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ένα διώνυμο της καθολικής βάσης Gröbner $U_{\mathbf{A}}$, το οποίο δεν είναι πρωταρχικό. Από τον ορισμό της $U_{\mathbf{A}}$, θα υπάρχει μία διάταξη όρων $\prec$, τέτοια ώστε το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ να ανήκει στην ανάγωγη βάση Gröbner $\{f_1, \ldots, f_s\}$ του $I_{\mathbf{A}}$, ως προς αυτή τη διάταξη. Επίσης, το διώνυμο αυτό δεν είναι πρωταρχικό, που σημαίνει ότι θα υπάρχει διώνυμο $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \neq \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ του $I_{\mathbf{A}}$, τέτοιο ώστε το μονώνυμο $\mathbf{x}^{\mathbf{v}^+}$ να διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$ και το μονώνυμο $\mathbf{x}^{\mathbf{v}^-}$ να διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $\mathbf{x}^{\mathbf{u}^+} \succ \mathbf{x}^{\mathbf{u}^-}$. Διακρίνουμε δύο περιπτώσεις:

1. $\mathbf{x}^{\mathbf{v}^+} \succ \mathbf{x}^{\mathbf{v}^-}$.
   Καθώς το διώνυμο $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_{\mathbf{A}}$, υπάρχει $i \in \{1, \ldots, s\}$, τέτοιο ώστε το αρχικό μονώνυμο του f_i, να διαιρεί το αρχικό μονώνυμο του διωνύμου $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}$. Όμως $lm(\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}) = \mathbf{x}^{\mathbf{v}^+}$ και το μονώνυμο $\mathbf{x}^{\mathbf{v}^+}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$. Συνεπώς, το αρχικό μονώνυμο $lm(f_i)$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$, άρα το αρχικό μονώνυμο $lm(f_i)$ ταυτίζεται με το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$, αφού το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ανήκει στην ανάγωγη βάση Gröbner $\langle f_1, \ldots, f_s \rangle$ του $I_{\mathbf{A}}$, οπότε το $f_i = \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$. Γνωρίζουμε όμως ότι το αρχικό μονώνυμο του f_i το οποίο ισούται με το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{v}^+}$ κι αυτό με τη σειρά του διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$. Συνεπώς το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$ ισούται με το μονώνυμο $\mathbf{x}^{\mathbf{v}^+}$, $\mathbf{x}^{\mathbf{u}^+} = \mathbf{x}^{\mathbf{v}^+}$. Επιπλέον γνωρίζουμε ότι το μονώνυμο $\mathbf{x}^{\mathbf{v}^-}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$ απ' όπου έχουμε ότι το $\mathbf{x}^{\mathbf{u}^-} = \mathbf{x}^{\mathbf{b}} \cdot \mathbf{x}^{\mathbf{v}^-}$.
   Θα δείξουμε ότι $\mathbf{x}^{\mathbf{b}} = 1$, δηλαδή ότι $\mathbf{b} = 0$. Αφού $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_{\mathbf{A}}$ έχουμε ότι $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^-})$, ομοίως αφού $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_{\mathbf{A}}$ έχουμε ότι $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^-})$. Όμως ισχύει ότι $\mathbf{x}^{\mathbf{u}^+} = \mathbf{x}^{\mathbf{v}^+}$, οπότε $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^+})$. Άρα $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^-}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^-})$, συνεπώς $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{b}} \cdot \mathbf{x}^{\mathbf{v}^-}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^-}) \Rightarrow deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{b}}) + deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^-}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{v}^-})$ άρα $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{b}}) = 0$. Σύμφωνα με το λήμμα 2.1.13 έχουμε ότι $\mathbf{b} = \mathbf{0}$ άρα $\mathbf{x}^{\mathbf{b}} = 1$. Συνεπώς το μονώνυμο $\mathbf{x}^{\mathbf{u}}$ ισούται με το μονώνυμο $\mathbf{x}^{\mathbf{v}}$, οπότε $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} = \mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}$, άτοπο εξ' υποθέσεως.

2. $\mathbf{x}^{\mathbf{v}^-} \succ \mathbf{x}^{\mathbf{v}^+}$.
   Καθώς το διώνυμο $\mathbf{x}^{\mathbf{v}^-} - \mathbf{x}^{\mathbf{v}^+} \in I_{\mathbf{A}}$, υπάρχει $i \in \{1, \ldots, s\}$, τέτοιο ώστε το αρχικό μονώνυμο του f_i, να διαιρεί το αρχικό μονώνυμο $\mathbf{x}^{\mathbf{v}^-} - \mathbf{x}^{\mathbf{v}^+}$. Όμως $lm(\mathbf{x}^{\mathbf{v}^-} - \mathbf{x}^{\mathbf{v}^+}) = \mathbf{x}^{\mathbf{v}^-}$ και το μονώνυμο $\mathbf{x}^{\mathbf{v}^-}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$. Συνεπώς, το αρχικό μονώνυμο $lm(f_i)$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$, το οποίο είναι άτοπο εφόσον το διώνυμο $\mathbf{x}^{\mathbf{u}^-} - \mathbf{x}^{\mathbf{u}^+}$ ανήκει στην ανάγωγη βάση Gröbner $\langle f_1, \ldots, f_s \rangle$ του $I_{\mathbf{A}}$.

Επομένως, κάθε στοιχείο της $U_{\mathbf{A}}$ είναι πρωταρχικό.

Αποδείξαμε δηλαδή, ότι η καθολική βάση Gröbner είναι υποσύνολο της βάσης Graver του $\mathbf{A}$. Δηλαδή

$$U_{\mathbf{A}} \subseteq Gr_{\mathbf{A}}.$$

□

Ακολουθεί ένας χρήσιμος ορισμός με τη βοήθεια του οποίου θα ορίσουμε τα κυκλώματα, ο ορισμός του φορέα διανύσματος.

Ορισμός 2.2.5. *(φορέας διανύσματος – vector support)*
Ο ***φορέας διανύσματος*** $supp(\mathbf{u})$, *όπου* $\mathbf{u} = (u_1, ..., u_n) \in \mathbb{Z}^n \subset \mathbb{Q}^n$, *ορίζεται ως το σύνολο:*

$$\{i \in \{1, ..., n\} : u_i \neq 0\}.$$

Ορισμός 2.2.6. *Το σύνολο*

$$\{x_i : \text{ είτε } x_i \text{ διαιρεί το } \mathbf{x}^{\mathbf{u}^+} \text{ ή } x_i \text{ διαιρεί το } \mathbf{x}^{\mathbf{u}^-}\}$$

καλείται ***φορέας διωνύμου*** *(support) του διωνύμου* $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ *και συμβολίζεται με* $supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-})$.

Ισοδύναμα θα μπορούσαμε να ορίσουμε το φορέα ενός διωνύμου $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ως το σύνολο των μεταβλητών που εμφανίζονται στο διώνυμο αυτό. Ένα παράδειγμα στο οποίο μπορούμε να δούμε μια απλή εφαρμογή των παραπάνω ορισμών, είναι το ακόλουθο.

Παράδειγμα 2.2.7. Έστω ένα διάνυσμα $\mathbf{u} = (-5, 2, 0, -2, -1, 3)$. Σύμφωνα με τους παραπάνω ορισμούς, έχουμε ότι $\mathbf{u}^+ = (0, 2, 0, 0, 0, 3)$ και $\mathbf{u}^- = (5, 0, 0, 2, 1, 0)$. Ενώ

$$supp(\mathbf{u}) = \{1, 2, 4, 5, 6\},$$

και

$$supp(\mathbf{u}^+) = \{2, 6\} \text{ και } supp(\mathbf{u}^-) = \{1, 4, 5\}.$$

Ενώ παρατηρούμε ότι $supp(\mathbf{u}^+) \bigcap supp(\mathbf{u}^-) = \emptyset$.
Επιπλέον

$$\mathbf{x}^{\mathbf{u}^+} = x_2^2 x_6^3, \mathbf{x}^{\mathbf{u}^-} = x_1^5 x_4^2 x_5.$$

Ενώ

$$supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}) = supp(x_2^2 x_6^3 - x_1^5 x_4^2 x_5) = \{x_2, x_6, x_1, x_4, x_5\}.$$

Μια σημαντική κατηγορία διωνύμων του τορικού ιδεώδους $I_{\mathbf{A}}$ είναι τα κυκλώματα.

Ορισμός 2.2.8. *(κύκλωμα – circuit)*
Ένα ανάγωγο διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ *του τορικού ιδεώδους* $I_{\mathbf{A}}$ *καλείται* ***κύκλωμα*** *αν και μόνο αν έχει ελαχιστοτικό φορέα, ως προς τη σχέση υποσύνολου. Δηλαδή δεν υπάρχει κάποιο άλλο διώνυμο της μορφής* $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_{\mathbf{A}}$, *ο φορέας του οποίου να είναι γνήσιο υποσύνολο του φορέα του διωνύμου* $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$.

Το σύνολο όλων των κυκλωμάτων ενός τορικού ιδεώδους $I_{\mathbf{A}}$ υπεράνω ενός συνόλου $\mathbf{A}$, συμβολίζεται με $C_{\mathbf{A}}$.

Παρατήρηση 2.2.9. Έστω $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ένα κύκλωμα του ιδεώδους $I_{\mathbf{A}}$. Εφόσον το $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ανήκει στο $I_{\mathbf{A}}$ συνεπάγεται πως $deg_A(\mathbf{x}^{\mathbf{u}^+}) = deg_A(\mathbf{x}^{\mathbf{u}^-})$. Άρα $u_1\mathbf{a}_1 + ... + u_s\mathbf{a}_s = \mathbf{0}$. Απ' όπου συμπεραίνουμε πως το διάνυσμα $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$. Έχουμε δηλαδή μια σχέση εξάρτησης και μάλιστα ελαχιστική από τον ορισμό του κυκλώματος. Αυτό σημαίνει ότι από το σύνολο $\{\mathbf{a}_i / x_i \in supp(c)\}$, όπου $c = \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ το κύκλωμα του $I_{\mathbf{A}}$ αν αφαιρέσουμε οποιοδήποτε διάνυσμα $\mathbf{a}_j$ με x_j να ανήκει στο φορέα $supp(c)$ και $j \neq i$ τότε τα υπόλοιπα διανύσματα είναι γραμμικώς ανεξάρτητα.

Πρόταση 2.2.10. *Κάθε κύκλωμα ανήκει στην καθολική βάση Gröbner του* $I_{\mathbf{A}}$.

Απόδειξη. Έστω $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ένα κύκλωμα του $I_{\mathbf{A}}$. Για να αποδείξουμε το ζητούμενο, αρκεί να προσδιορίσουμε μία κατάλληλη διάταξη όρων, στην οποία το κύκλωμα $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ θα ανήκει στην ανάγωγη βάση Gröbner του $I_{\mathbf{A}}$, ως προς αυτή τη διάταξη. Θεωρούμε μία διάταξη απαλοιφής $\prec$ όπως αυτή ορίστηκε στο πρώτο κεφάλαιο, στο 1.2.14, τέτοια ώστε οι μεταβλητές που δεν ανήκουν στο φορέα $supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-})$, να είναι μεγαλύτερες από τις μεταβλητές που ανήκουν στο φορέα $supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-})$. Θα δείξουμε ότι το κύκλωμα $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ανήκει στην ανάγωγη βάση Gröbner $\{f_1, \ldots, f_s\}$, ως προς τη διάταξη $\prec$.

Έστω ότι δεν ανήκει, θα καταλήξουμε σε άτοπο. Αφού το κύκλωμα $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν ανήκει στην ανάγωγη βάση Gröbner $\{f_1, \ldots, f_s\}$ υπάρχει $i \in \{1, \ldots, s\}$, τέτοιο ώστε το αρχικό μονώνυμο του f_i, να διαιρεί είτε το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$ ή το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$. Θα αποδείξουμε το ζητούμενο, καταλήγοντας σε άτοπο, στην περίπτωση που το αρχικό μονώνυμο του f_i, διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$. Αν $lm(f_i)$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$, ανάλογα αποδεικνύουμε το ζητούμενο.

Έστω $f_i = \mathbf{x}^{\mathbf{u}_i^+} - \mathbf{x}^{\mathbf{u}_i^-}$, με $lm(f_i) = \mathbf{x}^{\mathbf{u}_i^+}$, τέτοιο ώστε το μονώνυμο $\mathbf{x}^{\mathbf{u}_i^+}$ να διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$. Τότε:

$$supp(\mathbf{x}^{\mathbf{u}_i^+}) \subseteq supp(\mathbf{x}^{\mathbf{u}^+}) \subseteq supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}).$$

Αφού $\mathbf{x}^{\mathbf{u}_i^+} \succ \mathbf{x}^{\mathbf{u}_i^-}$ λόγω της διάταξης απαλοιφής , έπεται ότι

$$supp(\mathbf{x}^{\mathbf{u}_i^-}) \subseteq supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}).$$

Άρα,

$$supp(\mathbf{x}^{\mathbf{u}_i^+} - \mathbf{x}^{\mathbf{u}_i^-}) \subseteq supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}).$$

Όμως το $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ είναι κύκλωμα, δηλαδή έχει ελαχιστοτικό φορέα. Επομένως,

$$supp(\mathbf{x}^{\mathbf{u}_i^+} - \mathbf{x}^{\mathbf{u}_i^-}) = supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}) = \{\mathbf{x}_{j_1}, \ldots, \mathbf{x}_{j_t}\}.$$

Αν $\mathbf{u} = (u_1, \ldots, u_n)$ και $\mathbf{u}_i = (u_{i_1}, \ldots, u_{i_n})$, τότε αφού $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in I_{\mathbf{A}}$ έχουμε $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}^-})$. Άρα $u_{j_1}^+ \mathbf{a}_{j_1} + \ldots + u_{j_t}^+ \mathbf{a}_{j_t} = u_{j_1}^- \mathbf{a}_{j_1} + \ldots + u_{j_t}^- \mathbf{a}_{j_t}$ οπότε

$$u_{j_1} \mathbf{a}_{j_1} + \ldots + u_{j_t} \mathbf{a}_{j_t} = \mathbf{0} \tag{1}$$

Όμοια $\mathbf{x}^{\mathbf{u}_i{}^+} - \mathbf{x}^{\mathbf{u}_i{}^-} \in I_{\mathbf{A}}$, άρα έχουμε $deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}_i{}^+}) = deg_{\mathbf{A}}(\mathbf{x}^{\mathbf{u}_i{}^-})$. Άρα

$$u_{i_{j_1}}^+ \mathbf{a}_{j_1} + \ldots + u_{i_{j_t}}^+ \mathbf{a}_{j_t} = u_{i_{j_1}}^- \mathbf{a}_{j_1} + \ldots + u_{i_{j_t}}^- \mathbf{a}_{j_t},$$

$$u_{i_{j_1}} \mathbf{a}_{j_1} + \ldots + u_{i_{j_t}} \mathbf{a}_{j_t} = \mathbf{0}. \tag{2}$$

Οι δείκτες $\{j_1, \ldots, j_t\}$ είναι οι δείκτες των μεταβλητών που εμφανίζονται στο φορέα $supp(\mathbf{x}^{\mathbf{u}_i^+} - \mathbf{x}^{\mathbf{u}_i^-}) = supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-})$, δηλαδή οι δείκτες των $\mathbf{x}_{j_1}, \ldots, \mathbf{x}_{j_t}$. Τα στοιχεία με τους υπόλοιπους δείκτες είναι μηδενικά. Δηλαδή αν είναι $u_k = 0$, τότε το x_k δεν ανήκει στο φορέα $supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-})$ και το k δεν ανήκει στο σύνολο $\{j_1, \ldots, j_t\}$. Αντίστοιχα αν είναι $u_k \neq 0$, τότε το x_k ανήκει στο φορέα $supp(\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-})$ και το k ανήκει στο σύνολο $\{j_1, \ldots, j_t\}$, όπου $k = 1, \ldots, n$.

Έστω $u_k \neq 0$ δηλαδή $k \in \{j_1, \ldots, j_t\}$. Θεωρούμε

$$\lambda = \frac{u_{j_1}}{u_{i_{j_1}}}.$$

Πολλαπλασιάζουμε τη σχέση (2) με λ και την αφαιρούμε από τη σχέση (1), οπότε προκύπτει η εξής σχέση:

$$u_{j_1}\mathbf{a}_{j_1} + \ldots + u_{j_t}\mathbf{a}_{j_t} - \lambda(u_{i_{j_1}}\mathbf{a}_{j_1} + \ldots + u_{i_{j_t}}\mathbf{a}_{j_t}) = 0\mathbf{a}_{j_1} + (u_{j_2} - \lambda u_{i_{j_2}})\mathbf{a}_{j_2} + \ldots$$
$$+(u_{j_t} - \lambda u_{i_{j_t}})\mathbf{a}_{j_t} = 0.$$

Επειδή το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ είναι κύκλωμα, έπεται ότι τα διανύσματα $\{\mathbf{a}_{j_2}, \ldots, \mathbf{a}_{j_t}\}$ είναι γραμμικώς ανεξάρτητα, δηλαδή

$$u_{j_2} - \lambda u_{i_{j_2}} = 0, \ldots, u_{j_t} - \lambda u_{i_{j_t}} = 0.$$

Διαφορετικά θα είχαμε ένα νέο διάνυσμα $\mathbf{v} = (0, u_{j_2} - \lambda u_{i_{j_2}}, \ldots, u_{j_t} - \lambda u_{i_{j_t}})$ με το φορέα του αντίστοιχου διωνύμου, $supp(\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}) = \{x_{j_2}, ..., x_{j_t}\}$ γνήσια μικρότερο του ελαχιστοτικού $\{x_{j_1}, x_{j_2}, ..., x_{j_t}\}$, άτοπο. Άρα,

$$\mathbf{u} = \lambda \mathbf{u_i} = \frac{u_{j_1}}{u_{i_{j_1}}}\mathbf{u}_i.$$

Διαιρώντας με το μέγιστο κοινό διαιρέτη των u_{j_1} και $u_{i_{j_1}}$, μπορούμε να υποθέσουμε ότι

$$\mathbf{u} = \frac{\kappa}{\mu}\mathbf{u}_i, \tag{3}$$

όπου κ, μ είναι πρώτοι μεταξύ τους. Τότε

$$(\mu u_{j_1}, \ldots, \mu u_{j_t}) = (\kappa u_{i_{j_1}}, \ldots, \kappa u_{i_{j_t}}).$$

Για κάθε $l = 1, ..., t$, έχουμε

$$\mu u_{j_l} = \kappa u_{i_{j_l}} \in \mathbb{Z}.$$

Από την τελευταία σχέση, έπεται ότι το κ διαιρεί το μu_{j_l}. Όμως ο μέγιστος κοινός διαιρέτης των κ και μ είναι μονάδα, αφού είναι πρώτοι μεταξύ τους, άρα το κ διαιρεί το u_{j_l}, για όλα τα $l = 1, ..., t$. Το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ είναι ανάγωγο, ως κύκλωμα, οπότε υποχρεωτικά είναι $\kappa = 1$, διαφορετικά θα ήταν

$$\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} = \mathbf{x}^{\kappa\mathbf{v}^+} - \mathbf{x}^{\kappa\mathbf{v}^-},$$

το οποίο διαιρείται από το διώνυμο $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}$ κι άρα το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δε θα ήταν ανάγωγο. Για $\kappa = 1$ η σχέση (3) γράφεται:

$$\mathbf{u} = \frac{1}{\mu}\mathbf{u}_i$$

και συνεπάγεται ότι

$$\mathbf{u}_i = \mu\mathbf{u}.$$

Αυτό σημαίνει ότι το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}_i^+}$ και το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}_i^-}$. Επίσης, υποθέσαμε ότι το μονώνυμο $\mathbf{x}^{\mathbf{u}_i^+}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$. Συνεπώς $\mathbf{x}^{\mathbf{u}^+} = \mathbf{x}^{\mathbf{u}_i^+}$. Άρα, θα είναι $\mu = 1$. Τελικά,

$$\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} = \mathbf{x}^{\mathbf{u}_i^+} - \mathbf{x}^{\mathbf{u}_i^-},$$

το οποίο είναι άτοπο, αφού υποθέσαμε ότι το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν ανήκει στην ανάγωγη βάση Gröbner $\{f_1, \ldots, f_s\}$, ως προς τη διάταξη $\prec$.

Αντίστοιχα, καταλήγουμε σε άτοπο και στην περίπτωση που το αρχικό μονώνυμο του f_i, $lm(f_i)$, διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$.

Τελικά, το κύκλωμα $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ανήκει στην ανάγωγη βάση Gröbner $\{f_1, \ldots, f_s\}$, ως προς τη διάταξη $\prec$, άρα ανήκει και στην ένωση όλων των ανάγωγων βάσεων Gröbner, ως προς οποιαδήποτε διάταξη όρων, δηλαδή ανήκει στην καθολική βάση Gröbner του $I_{\mathbf{A}}$.

Αποδείξαμε λοιπόν, ότι το σύνολο των κυκλωμάτων του τορικού ιδεώδους $I_{\mathbf{A}}$ είναι υποσύνολο της καθολικής βάσης Gröbner του $I_{\mathbf{A}}$. Δηλαδή

$$C_{\mathbf{A}} \subseteq U_{\mathbf{A}}.$$

□

Παρατήρηση 2.2.11. Στο τέλος της απόδειξης της ανωτέρω πρότασης είχαμε ότι το $\mathbf{u}_i = \mu\mathbf{u}$ και συμπεράναμε ότι το μονώνυμο $\mathbf{x}^{\mathbf{u}^+}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}_i^+}$ και το μονώνυμο $\mathbf{x}^{\mathbf{u}^-}$ διαιρεί το μονώνυμο $\mathbf{x}^{\mathbf{u}_i^-}$. Πράγματι, αφού το $\mathbf{u}_i \geq \mathbf{u}$ συνεπάγεται πως το $\mathbf{x}^{\mathbf{u}} \setminus \mathbf{x}^{\mathbf{u}_i}$. Άρα το μονώνυμο $\mathbf{x}^{\mathbf{u}^+} \setminus \mathbf{x}^{\mathbf{u}_i^+}$ και το μονώνυμο $\mathbf{x}^{\mathbf{u}^-} \setminus \mathbf{x}^{\mathbf{u}_i^-}$.

Στη συνέχεια θα δώσουμε ένα χαρακτηρισμό στα στοιχεία της βάσης Graver. Για το σκοπό αυτό θα δώσουμε τον ακόλουθο ορισμό.

Ορισμός 2.2.12. *Το διάνυσμα* $\mathbf{a} \in \mathbb{Z}^n$, $\mathbf{a} = (a_1, \ldots, a_n)$, *λέμε ότι είναι* ***σύμμορφο άθροισμα*** *(conformal sum) δύο μη μηδενικών διανυσμάτων* $\mathbf{b}, \mathbf{c} \in \mathbb{Z}^n$ *δηλαδή* $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$, *αν και μόνο αν* $\mathbf{a} = \mathbf{b} + \mathbf{c}$ *και* $|a_i| = |b_i| + |c_i|$ *για κάθε* $i = 1, \ldots, n$.

Ορισμός 2.2.13. *Έστω* $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$ *δύο διανύσματα, τότε λέμε ότι* $\mathbf{a} \geqslant \mathbf{b}$ *αν και μόνο αν* $\mathbf{a} - \mathbf{b} \in \mathbb{N}_0^n$ *δηλαδή αν κάθε συνιστώσα του διανύσματος* $\mathbf{a} - \mathbf{b}$ *είναι θετική ή μηδενική (μη αρνητική).*

Παρατήρηση 2.2.14. Από τον ορισμό προκύπτει πως το $a_i = b_i + c_i$ και τα a_i, b_i, c_i είναι ομόσημα, αφού $|a_i| = |b_i| + |c_i| \Rightarrow |b_i + c_i| = |b_i| + |c_i|$ για κάθε $i = 1, \ldots, n$. Πιο αναλυτικά διακρίνουμε τις ακόλουθες περιπτώσεις:
1) Αν $a_i > 0 \Rightarrow b_i \geqslant 0$ και $c_i \geqslant 0$.
2) Αν $a_i < 0 \Rightarrow b_i \leqslant 0$ και $c_i \leqslant 0$.
3) Αν $a_i = 0 \Rightarrow b_i = 0$ και $c_i = 0$.

Πρόταση 2.2.15. *Τα στοιχεία* $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ *της βάσης Graver του* I_A, *είναι ακριβώς εκείνα για τα οποία το* $\mathbf{u} \neq 0$, $\mathbf{u} \in \mathrm{Ker}_{\mathbf{Z}} A$, *και το* $\mathbf{u}$ *δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων* $\mathbf{v}_1, \mathbf{v}_2 \in \mathrm{Ker}_{\mathbf{Z}} A$.

Απόδειξη. Έστω $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ανήκει στη βάση Graver του I_A. Ισχυριζόμαστε ότι το $\mathbf{u}$ δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων $\mathbf{v}_1, \mathbf{v}_2 \in \mathrm{Ker}_{\mathbf{Z}} A$. Έστω ότι αυτό δεν ισχύει, θα καταλήξουμε σε άτοπο. Άρα το $\mathbf{u} = \mathbf{v}_1 +_c \mathbf{v}_2$ με $\mathbf{v}_1, \mathbf{v}_2 \in \mathrm{Ker}_{\mathbf{Z}} A$, γράφεται ως σύμμορφο άθροισμα. Τότε $|u_i| = |v_{1i}| + |v_{2i}|$ όπου $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{v_1} = (v_{11}, \ldots, v_{1n})$, $\mathbf{v_2} = (v_{21}, \ldots, v_{2n})$.

1η περίπτωση

Αν το $u_i > 0$, το $v_{1i} \geqslant 0$ και το $v_{2i} \geqslant 0$, για κάθε $i = 1, \ldots, n$ τότε έχουμε $u_i = v_{1i} + v_{2i} \Rightarrow u_i \geqslant v_{1i} \geqslant 0 \Rightarrow u_i \geqslant 0 \Rightarrow u_i = u_i^+$, όμοια $v_{1i} = v_{1i}^+$. Άρα

$u_i \geqslant v_{1i} \Rightarrow u_i^+ \geqslant v_{1i}^+$.

2η περίπτωση

Αν το $u_i < 0$, το $v_{1i} \leqslant 0$ και το $v_{2i} \leqslant 0$, για κάθε $i = 1, ..., n$ τότε έχουμε $u_i = v_{1i} + v_{2i} \Rightarrow u_i \leqslant v_{1i} \leqslant 0 \Rightarrow u_i \leqslant 0 \Rightarrow u_i = -u_i^-$, όμοια $v_{1i} = -v_{1i}^-$. Άρα $u_i \leqslant v_{1i} \Rightarrow -u_i^- \leqslant -v_{1i}^- \Rightarrow u_i^- \geqslant v_{1i}^-$.

3η περίπτωση

Αν το $u_i = 0 \Rightarrow$ το $v_{1i} = 0$ και το $v_{2i} = 0$.
Έχουμε δείξει λοιπόν ότι $u_i^+ \geqslant v_{1i}^+$ και $u_i^- \geqslant v_{1i}^-$ για κάθε $i = 1, ..., n$ συνεπώς $\mathbf{u}^+ \geqslant \mathbf{v}_1^+$ και $\mathbf{u}^- \geqslant \mathbf{v}_1^-$. Άρα έχουμε ότι $\mathbf{x}^{\mathbf{v}_1^+} \backslash \mathbf{x}^{\mathbf{u}^+}$ είναι $\mathbf{x}^{\mathbf{v}_1^-} \backslash \mathbf{x}^{\mathbf{u}^-}$, δηλαδή το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν είναι πρωταρχικό. Άτοπο εξ' υποθέσεως.

Αντίστροφα υποθέτουμε ότι $\mathbf{u} \neq 0, \mathbf{u} \in \mathrm{Ker}_{\mathbb{Z}} A$ και το $\mathbf{u}$ δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών διανυσμάτων $\mathbf{v}_1, \mathbf{v}_2 \in \mathrm{Ker}_{\mathbb{Z}} A$. Ισχυριζόμαστε ότι το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ είναι πρωταρχικό, δηλαδή ανήκει στη βάση Graver του ιδεώδους I_A. Έστω όχι, θα καταλήξουμε σε άτοπο. Αφού το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν είναι πρωταρχικό συνεπάγεται πως υπάρχει ένα άλλο διώνυμο $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_A$ τέτοιο ώστε $\mathbf{x}^{\mathbf{v}^+} \backslash \mathbf{x}^{\mathbf{u}^+}$ και $\mathbf{x}^{\mathbf{v}^-} \backslash \mathbf{x}^{\mathbf{u}^-}$. Τότε από τη μερική διάταξη που ορίζεται από τη διαιρετότητα έχουμε $\mathbf{u}^+ \geqslant \mathbf{v}^+$, $\mathbf{u}^- \geqslant \mathbf{v}^-$, δηλαδή $\mathbf{u}^+ - \mathbf{v}^+ \geqslant (0, ..., 0)$ και $\mathbf{u}^- - \mathbf{v}^- \geqslant (0, ..., 0)$ δηλαδή $\mathbf{u}^+ - \mathbf{v}^+ \in \mathbb{N}_0^n$ και $\mathbf{u}^- - \mathbf{v}^- \in \mathbb{N}_0^n$. Δηλαδή ${u_i}^+ - {v_i}^+ \in \mathbb{N}_0^n$ και ${u_i}^- - {v_i}^- \in \mathbb{N}_0^n$ για κάθε $i = 1, ..., n$. Συνεπώς ${u_i}^+ \geqslant {v_i}^+$ και ${u_i}^- \geqslant {v_i}^-$ για κάθε $i = 1, ..., n$. Τώρα λοιπόν γράφουμε το διάνυσμα $\mathbf{u}$ ως το άθροισμα των διανυσμάτων $\mathbf{v}, \mathbf{u} - \mathbf{v}$ τα οποία ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$. Έχουμε δηλαδή $\mathbf{u} = \mathbf{v} + (\mathbf{u} - \mathbf{v})$, θα αποδείξουμε ότι το άθροισμα αυτό είναι σύμμορφο. Για το σκοπό αυτό αρκεί να δείξουμε σύμφωνα με τον ορισμό του σύμμορφου αθροίσματος, ότι η απόλυτη τιμή του αθροίσματος ισούται με το άθροισμα των απολύτων τιμών. Δηλαδή για να έχουμε σύμμορφο άθροισμα θα δείξουμε ότι $|u_i| = |v_i + (u - v)_i| = |v_i| + |(u - v)_i|$. Από την τελευταία σχέση συμπεραίνουμε για τα $v_i, u_i, u_i - v_i$ ότι είναι ομόσημα.

1η περίπτωση

Αν το $v_i > 0, \Rightarrow v_i = v_i^+ \Rightarrow 0 < v_i = v_i^+ \leqslant u_i^+$. Άρα $u_i^+ > 0 \Rightarrow u_i > 0 \Rightarrow$
$u_i = u_i^+ \Rightarrow u_i^+ \geqslant v_i^+ \Rightarrow u_i \geqslant v_i \Rightarrow u_i - v_i \geqslant 0$. Άρα $v_i > 0, u_i > 0, u_i - v_i \geqslant 0$, δηλαδή είναι ομόσημα.

2η περίπτωση

Αν το $v_i < 0, \Rightarrow v_i = -v_i^- < 0 \Rightarrow v_i^- > 0 \Rightarrow u_i^- \geqslant v_i^- > 0 \Rightarrow u_i^- > 0 \Rightarrow$
$u_i < 0 \Rightarrow u_i = -u_i^-$. Άρα $u_i^- - v_i^- \geqslant 0 \Rightarrow -u_i + v_i \geqslant 0 \Rightarrow u_i - v_i \leqslant 0$. Άρα $v_i < 0, u_i < 0, u_i - v_i \leqslant 0$, δηλαδή είναι ομόσημα.

3η περίπτωση

Αν $v_i = 0$ τότε $u_i = u_i$ είναι ομόσημα αφού είναι ίσα.

Άρα πράγματι σε κάθε περίπτωση τα $u_i, v_i, u_i - v_i$ είναι ομόσημα συνεπώς το $|u_i| = |v_i| + |(u-v)_i| \Rightarrow |v_i + (u-v)_i| = |v_i| + |(u-v)_i|$ για κάθε $i = 1, ..., n$. Δηλαδή καταφέραμε και γράψαμε το $\mathbf{u}$ ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων των $\mathbf{v}, \mathbf{u}-\mathbf{v}$ με $\mathbf{v} \in \mathrm{Ker}_{\mathbf{Z}} A, \mathbf{u}-\mathbf{v} \in \mathrm{Ker}_{\mathbf{Z}} A$. Το οποίο είναι άτοπο. □

Παρατήρηση 2.2.16. Έχουμε ότι το διάνυσμα $\mathbf{u} \in \mathrm{Ker}_{\mathbf{Z}} A$, το διάνυσμα $\mathbf{v} \in \mathrm{Ker}_{\mathbf{Z}} A$ συνεπώς $\mathbf{u}-\mathbf{v} \in \mathrm{Ker}_{\mathbf{Z}} A$.

Θα ορίσουμε τώρα το ιδεώδες $I_{A,\mathbf{b}}$ και αμέσως μετά θα παραθέσουμε ένα λήμμα που σχετίζεται με το ιδεώδες αυτό.

Ορισμός 2.2.17. *Έστω A ένα σύνολο διανυσμάτων και $\mathbf{b} \in \mathbf{NA}$. Ορίζουμε το ιδεώδες $I_{A,\mathbf{b}} = \langle B/B \in I_{\mathbf{A}}$ με $deg_{\mathbf{A}}(B) < \mathbf{b} \rangle$.*

Παρατήρηση 2.2.18. Από τον ορισμό 2.2.17 παρατηρούμε ότι το ιδεώδες $I_{A,\mathbf{b}}$ είναι υποσύνολο του τορικού ιδεώδους I_A.

Λήμμα 2.2.19. *Αν το τορικό ιδεώδες $I_{\mathbf{A}}$ γεννάται από τα διώνυμα $B_1, ..., B_s$ τότε το ιδεώδες $I_{A,\mathbf{b}}$ γεννάται από εκείνα τα διώνυμα B_i με βαθμό αυστηρά μικρότερο του $\mathbf{b}$.*

Απόδειξη. Θα δείξουμε ότι το ιδεώδες $I_{A,\mathbf{b}}$ παράγεται από εκείνους τους γεννήτορες B_i του ιδεώδους I_A που έχουν βαθμό μικρότερο του $\mathbf{b}$. Αρκεί να δείξουμε ότι ισχύουν οι δύο σχέσεις υποσυνόλου. Υποθέτουμε ότι ο γεννήτορας $B_j = x^{u_j^+} - x^{u_j^-}$ ανήκει στο σύνολο $\langle B_i/1 \leq i \leq s$ με $deg_{\mathbf{A}}(B_i) < \mathbf{b} \rangle$ για κάποιο j, με $1 \leq j \leq s$. Συνεπώς έχουμε $deg_{\mathbf{A}}(B_j) < \mathbf{b}$. Άρα ο γεννήτορας B_i ανήκει στο ιδεώδες $I_{A,\mathbf{b}}$. Δηλαδή $\langle B_i/1 \leq i \leq s$ με $deg_{\mathbf{A}}(B_i) < \mathbf{b} \rangle \subseteq I_{A,\mathbf{b}}$.
Αντίστροφα, έστω το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ είναι γεννήτορας του ιδεώδους $I_{A,\mathbf{b}}$ τότε το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ ανήκει στο ιδεώδες I_A και ο βαθμός του είναι $deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) < \mathbf{b}$. Από την πρόταση 2.2.14 που βρίσκεται στη μεταπτυχιακή διατριβή του Χ.Τατάκη [22] γνωρίζουμε πως το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ μπορεί να γραφεί ως γραμμικός συνδυασμός διωνύμων $B_{i_1}, ..., B_{i_t}$ με μονωνυμικούς συντελεστές, δηλαδή $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} = x^{\mathbf{a}_1}(x^{\mathbf{u}_{i_1}^+} - x^{\mathbf{u}_{i_1}^-}) + ... + x^{\mathbf{a}_t}(x^{\mathbf{u}_{i_t}^+} - x^{\mathbf{u}_{i_t}^-})$, με $B_{i_1} = x^{\mathbf{u}_{i_1}^+} - x^{\mathbf{u}_{i_1}^-}, ..., B_{i_t} = x^{\mathbf{u}_{i_t}^+} - x^{\mathbf{u}_{i_t}^-}$. Όπου $\{i_1, ..., i_t\} \subseteq \{1, ..., s\}$ οι δείκτες των διωνύμων που χρησιμοποιήθηκαν για την περιγραφή του διωνύμου $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$. Έστω $\mathbf{b}_i = deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-})$ τότε είναι $\mathbf{b} > \mathbf{b}_1 = deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) \geq deg_{\mathbf{A}}(B_{i_1}), ..., \mathbf{b} > \mathbf{b}_i = deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) \geq deg_{\mathbf{A}}(B_{i_t})$. Άρα $deg_{\mathbf{A}}(B_{i_1}) < \mathbf{b}, ..., deg_{\mathbf{A}}(B_{i_t}) < \mathbf{b}$ για $1 \leq i_1, ..., i_t \leq s$.
Άρα οι γεννήτορες $B_{i_1}, ..., B_{i_t}$ ανήκουν στο σύνολο

$$\{B_i/1 \leq i \leq s \text{ με } deg_{\mathbf{A}}(B_i) < \mathbf{b}\} \Rightarrow$$

$x^{\mathbf{v}^+} - x^{\mathbf{v}^-} = x_1^{\mathbf{a}} B_{i_1} + ... + x_t^{\mathbf{a}} B_{i_t}$ ανήκει στο ιδεώδες

$$\langle B_i/1 \leq i \leq s \text{ με } deg_{\mathbf{A}}(B_i) < \mathbf{b} \rangle.$$

Συνεπώς το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}}$ ανήκει στο ιδεώδες

$$\langle B_i/1 \leq i \leq s \text{ με } deg_{\mathbf{A}}(B_i) < \mathbf{b} \rangle.$$

Οπότε $I_{A,\mathbf{b}} \subseteq \langle B_i / 1 \leq i \leq s \text{ με } deg_{\mathbf{A}}(B_i) < \mathbf{b} \rangle$. Αποδείξαμε δηλαδή ότι:

$$I_{A,\mathbf{b}} = \langle B_i / 1 \leq i \leq s \text{ με } deg_{\mathbf{A}}(B_i) < \mathbf{b} \rangle.$$

□

Στη συνέχεια ακολουθεί ένα σημαντικό θεώρημα που σχετίζεται με τις βάσεις Markov. Στο τρίτο κεφάλαιο θα ασχοληθούμε εκτενέστερα με τις βάσεις αυτές, σε αυτό το κεφάλαιο όμως είναι ιδιαίτερα χρήσιμες στις αποδείξεις σημαντικών θεωρημάτων και προτάσεων.
Ακολουθεί ο ορισμός των βάσεων Markov.

Ορισμός 2.2.20. *Ένα πεπερασμένο σύνολο γεννητόρων του ιδεώδους $I_{\mathbf{A}}$ καλείται* ***βάση Markov*** *του A. Ένα πεπερασμένο σύνολο ονομάζεται ελαχιστοτικό σύνολο γεννητόρων ή* ***ελαχιστοτική βάση Markov*** *του ιδεώδους $I_{\mathbf{A}}$ αν δεν υπάρχει γνήσιο υποσύνολο του που να είναι βάση Markov του ιδεώδους $I_{\mathbf{A}}$.*

Ορισμός 2.2.21. *Η ένωση των ελαχιστοτικών βάσεων Markov του A καλείται* ***καθολική βάση Markov*** *του A.*

Θεώρημα 2.2.22. *Έστω $\{B_1, ..., B_s\}$ ελαχιστοτικό σύστημα γεννητόρων του ιδεώδους $I_{\mathbf{A}}$ τότε το B_i ανήκει στη βάση Graver του ιδεώδους $I_{\mathbf{A}}$ για κάθε $i = 1, ..., s$. Δηλαδή η καθολική βάση Markov είναι υποσύνολο της βάσης Graver.*

Απόδειξη. Έστω ότι υπάρχει ένα διώνυμο $B_i = x^{\mathbf{u}_i^+} - x^{\mathbf{u}_i^-}$ που ανήκει στο σύνολο $\{B_1, ..., B_s\}$ και το B_i δεν ανήκει στη βάση Graver του ιδεώδους $I_{\mathbf{A}}$. Συνεπώς το B_i δεν είναι πρωταρχικό. Άρα υπάρχει ένα διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} \in I_{\mathbf{A}}$ με $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} \neq x^{\mathbf{u}_i^+} - x^{\mathbf{u}_i^-}$ τέτοιο ώστε $x^{\mathbf{v}^+} \setminus x^{\mathbf{u}_i^+}$ και $x^{\mathbf{v}^-} \setminus x^{\mathbf{u}_i^-}$. Αφού $x^{\mathbf{v}^+} \setminus x^{\mathbf{u}_i^+}$ συνεπάγεται ότι $x^{\mathbf{u}_i^+} = x^{\mathbf{a}} x^{\mathbf{v}^+}$ με $x^{\mathbf{a}} \neq 1$, δηλαδή $deg_{\mathbf{A}}(x^{\mathbf{a}}) \neq 0$ κι αφού $x^{\mathbf{v}^-} \setminus x^{\mathbf{u}_i^-}$ συνεπάγεται ότι $x^{\mathbf{u}_i^-} = x^{\mathbf{b}} x^{\mathbf{v}^-}$ με $x^{\mathbf{b}} \neq 1$, δηλαδή $deg_{\mathbf{A}}(x^{\mathbf{b}}) \neq 0$, σύμφωνα με την πρώτη περίπτωση της απόδειξης της πρότασης 2.2.4. Άρα το $B_i = x^{\mathbf{u}_i^+} - x^{\mathbf{u}_i^-} = x^{\mathbf{a}} x^{\mathbf{v}^+} - x^{\mathbf{b}} x^{\mathbf{v}^-} = x^{\mathbf{a}} x^{\mathbf{v}^+} - x^{\mathbf{a}} x^{\mathbf{v}^-} + x^{\mathbf{a}} x^{\mathbf{v}^-} - x^{\mathbf{b}} x^{\mathbf{v}^-} = x^{\mathbf{a}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) + x^{\mathbf{v}^-}(x^{\mathbf{a}} - x^{\mathbf{b}})$. Συνεπώς

$$B_i = x^{\mathbf{a}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) + x^{\mathbf{v}^-}(x^{\mathbf{a}} - x^{\mathbf{b}}).$$

Άρα $deg_{\mathbf{A}}(x^{\mathbf{u}_i^+}) = deg_{\mathbf{A}}(x^{\mathbf{u}_i^-}) \Rightarrow deg_{\mathbf{A}}(x^{\mathbf{a}}) + deg_{\mathbf{A}}(x^{\mathbf{v}^+}) = deg_{\mathbf{A}}(x^{\mathbf{b}}) + deg_{\mathbf{A}}(x^{\mathbf{v}^-}) \Rightarrow$ $deg_{\mathbf{A}}(x^{\mathbf{a}}) = deg_{\mathbf{A}}(x^{\mathbf{b}})$, αφού $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} \in I_{\mathbf{A}}$. Άρα τελικά το διώνυμο $x^{\mathbf{a}} - x^{\mathbf{b}}$ ανήκει στο ιδεώδες $I_{\mathbf{A}}$.
Το διώνυμο $B_i = x^{\mathbf{u}_i^+} - x^{\mathbf{u}_i^-}$ έχει βαθμό $deg_{\mathbf{A}}(B_i) = \mathbf{b}_i$. Είναι $B_i = x^{\mathbf{a}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) + x^{\mathbf{v}^-}(x^{\mathbf{a}} - x^{\mathbf{b}})$ άρα $deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) < deg_{\mathbf{A}}(B_i) = \mathbf{b}_i$ και $deg_{\mathbf{A}}(x^{\mathbf{a}} - x^{\mathbf{b}}) < deg_{\mathbf{A}}(B_i) = \mathbf{b}_i$. Το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ έχει βαθμό $\mathbf{b}$. Συνεπώς $\mathbf{b}_i = deg_{\mathbf{A}}(x^{\mathbf{u}_i^+} - x^{\mathbf{u}_i^-}) > deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) = \mathbf{b}$. Δηλαδή $\mathbf{b}_i > \mathbf{b}$. Το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ ανήκει στο ιδεώδες $I_{\mathbf{A}} = \langle B_1, ..., B_s \rangle$. συνεπώς από την πρόταση 2.2.14 που βρίσκεται στη μεταπτυχιακή διατριβή του Χ.Τατάκη [22] το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ γράφεται ως γραμμικός συνδυασμός διωνύμων με μονωνυμικούς συντελεστές δηλαδή

$$x^{\mathbf{v}^+} - x^{\mathbf{v}^-} = x^{\mathbf{a}_1}(x^{\mathbf{u}_{i_1}^+} - x^{\mathbf{u}_{i_1}^-}) + ... + x^{\mathbf{a}_t}(x^{\mathbf{u}_{i_t}^+} - x^{\mathbf{u}_{i_t}^-})$$

με $B_{i_1} = x^{\mathbf{u}_{i_1}^+} - x^{\mathbf{u}_{i_1}^-}, ..., B_{i_t} = x^{\mathbf{u}_{i_t}^+} - x^{\mathbf{u}_{i_t}^-}$. Όπου $\{i_1, ..., i_t\} \subseteq \{1, ..., s\}$ οι δείκτες των διωνύμων που χρησιμοποιήθηκαν για την περιγραφή του διωνύμου $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$. Το διώνυμο $x^{\mathbf{v}^+} - x^{\mathbf{v}^-}$ ανήκει στο ιδεώδες:

$$I_{A,\mathbf{b}_i} = \langle B_j / 1 \leq j \leq s \text{ με } deg_{\mathbf{A}}(B_j) < \mathbf{b}_i \rangle$$

αφού $deg_{\mathbf{A}}(B_{i_1}) < deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) = \mathbf{b} < \mathbf{b}_i, ..., deg_{\mathbf{A}}(B_{i_t}) < deg_{\mathbf{A}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) = \mathbf{b} < \mathbf{b}_i$. Όμοια το διώνυμο $x^{\mathbf{a}} - x^{\mathbf{b}}$ ανήκει στο ιδεώδες:

$$I_{A,\mathbf{b}_i} = \langle B_j / 1 \leq j \leq s \text{ με } deg_{\mathbf{A}}(B_j) < \mathbf{b}_i \rangle.$$

Θα δείξουμε ότι

$$\langle B_1, ..., B_i, ..., B_s \rangle = \langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle.$$

Η μια κατεύθυνση είναι προφανής, δηλαδή $\langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle \subseteq \langle B_1, ..., B_i, ..., B$ αφού το σύνολο $\{B_1, ..., B_{i-1}, B_{i+1}, ..., B_s\}$ είναι υποσύνολο του $\{B_1, ..., B_i, ..., B_s\}$. Μένει να δείξουμε ότι

$$\langle B_1, ..., B_i, ..., B_s \rangle \subseteq \langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle.$$

Αρκεί λοιπόν να δείξουμε ότι κάθε γεννήτορας του συνόλου

$$\{B_1, ..., B_i, ..., B_s\}$$

βρίσκεται στο σύνολο

$$\{B_1, ..., B_{i-1}, B_{i+1}, ..., B_s\}.$$

Προφανώς τα $B_1, ..., B_{i-1}, B_{i+1}, ..., B_s$ βρίσκονται και στα δύο σύνολα. Απομένει να δείξουμε ότι το B_i ανήκει στο $\{B_1, ..., B_{i-1}, B_{i+1}, ..., B_s\}$.
Έχουμε το διώνυμο $B_i = x^{\mathbf{u}_{i_t}^+} - x^{\mathbf{u}_{i_t}^-} = x^{\mathbf{a}}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) + x^{\mathbf{v}^-}(x^{\mathbf{a}} - x^{\mathbf{b}})$,
όπου $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} \in I_{A,\mathbf{b}_i}$ και $x^{\mathbf{a}} - x^{\mathbf{b}} \in I_{A,\mathbf{b}_i}$ συνεπώς και το B_i ανήκει στο ιδεώδες $I_{A,\mathbf{b}_i}$. Άρα σύμφωνα με το λήμμα 2.2.19 το B_i ανήκει στο σύνολο

$$\langle B_j / 1 \leq j \leq s \text{ με } deg_{\mathbf{A}}(B_j) < \mathbf{b}_i \rangle$$

το οποίο είναι υποσύνολο του $\langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle$, συνεπώς το B_i ανήκει στο σύνολο $\langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle$.
Άρα δείξαμε ότι το σύνολο $\langle B_1, ..., B_i, ..., B_s \rangle$ είναι ίσο με το $\langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle$.
Όμως το σύνολο $\langle B_1, ..., B_{i-1}, B_{i+1}, ..., B_s \rangle$ είναι σύνολο γεννητόρων του ιδεώδους $I_{\mathbf{A}}$ γνήσιο υποσύνολο του ελαχιστοτικού, δηλαδή του συνόλου $\langle B_1, ..., B_i, ..., B_s \rangle$, άτοπο. Οπότε το διώνυμο B_i ανήκει στη βάση Graver του ιδεώδους $I_{\mathbf{A}}$. Εφόσον μια τυχαία ελαχιστοτική βάση Markov είναι υποσύνολο της βάσης Graver του ιδεώδους $I_{\mathbf{A}}$, συνεπάγεται πως κάθε ελαχιστοτική βάση Markov είναι υποσύνολο της βάσης Graver. Άρα η καθολική βάση Markov είναι υποσύνολο της βάσης Graver του ιδεώδους $I_{\mathbf{A}}$. □

Παρατήρηση 2.2.23. Στην απόδειξη σημαντικό ρόλο έπαιξε η διάταξη των βαθμών στο $\mathbb{N}\mathbf{A}$. Για να ορίσουμε τη διάταξη έπρεπε $(\mathbb{N}\mathbf{A}) \bigcap -(\mathbb{N}\mathbf{A}) = \{0\}$. Στις περιπτώσεις που για κάποιο A δεν ισχύει αυτό, το θεώρημα 2.2.22 δεν ισχύει.

Παράδειγμα 2.2.24. Θεωρούμε το σύνολο διανυσμάτων $A = \{\mathbf{a}_1 = (1,0), \mathbf{a}_2 = (-1,0), \mathbf{a}_3 = (0,1), \mathbf{a}_4 = (0,-1)\}$ και τον πολυωνυμικό δακτύλιο $K[x,y,z,w]$. Τότε το τορικό ιδεώδες $I_{\mathbf{A}}$ είναι το εξής:

$$I_{\mathbf{A}} = \langle xy - 1, zw - 1 \rangle.$$

Θεωρούμε το διώνυμο $B = x^{u_1}y^{u_2}z^{u_3}w^{u_4} - x^{v_1}y^{v_2}z^{v_3}w^{v_4}$ με $B \neq 0, B \neq xy - 1, B \neq zw - 1$ που ανήκει στο ιδεώδες $I_{\mathbf{A}}$. Τότε έχουμε ότι:

$$deg_{\mathbf{A}}(x^{u_1}y^{u_2}z^{u_3}w^{u_4}) = deg_{\mathbf{A}}(x^{v_1}y^{v_2}z^{v_3}w^{v_4})$$

δηλαδή

$$(u_1 - u_2, u_3 - u_4) = (v_1 - v_2, v_3 - v_4)$$

άρα

$$u_1 - u_2 = v_1 - v_2, u_3 - u_4 = v_3 - v_4$$

Εφόσον το διώνυμο είναι $B \neq 0$ συνεπάγεται πως $(u_1, u_2, u_3, u_4) \neq (v_1, v_2, v_3, v_4)$. Διακρίνουμε τις ακόλουθες περιπτώσεις:

1. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $u_1 > v_1$, τότε αφού $v_1 \geq 0$ συνεπάγεται πως το $u_1 \neq 0$ και μάλιστα $u_1 > 0$. Ισχυριζόμαστε ότι $u_2 \neq 0$. Έστω όχι, θα καταλήξουμε σε άτοπο. Αφού $u_2 = 0$ τότε το $u_1 = u_1 - u_2 = v_1 - v_2$ συνεπώς $u_1 = v_1 - v_2$ κι από τη σχέση $u_1 > v_1$ έχουμε τελικά $v_2 < 0$, άτοπο. Συνεπώς $u_2 \neq 0$. Για το διώνυμο $xy - 1$ παρατηρούμε ότι:

   $$xy \backslash x^{u_1} y^{u_2} z^{u_3} w^{u_4}$$

   και

   $$1 \backslash x^{v_1} y^{v_2} z^{v_3} w^{v_4}.$$

   Το διώνυμο B είναι διάφορο του $xy - 1$, άρα το B δεν είναι πρωταρχικό, δηλαδή δεν ανήκει στη βάση Graver του ιδεώδους $I_{\mathbf{A}}$.

2. Υποθέτουμε ότι $u_1 = v_1$ συνεπώς $u_2 = v_2$. Τότε εφόσον το διώνυμο είναι $B' \neq 0$ συνεπάγεται πως $u_3 \neq v_3$ ή $u_4 \neq v_4$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $u_3 > v_3$, τότε αφού $v_3 \geq 0$ συνεπάγεται πως το $u_3 \neq 0$, και μάλιστα $u_3 > 0$. Ισχυριζόμαστε ότι $u_4 \neq 0$. Έστω όχι, θα καταλήξουμε σε άτοπο. Αφού $u_4 = 0$ τότε το $u_3 = u_3 - u_4 = v_3 - v_4$ συνεπώς $u_3 = v_3 - v_4$ κι από τη σχέση $u_3 > v_3$ έχουμε τελικά $v_4 < 0$, άτοπο. Συνεπώς $u_4 \neq 0$. Για το διώνυμο $zw - 1$ παρατηρούμε ότι:

   $$zw \backslash x^{u_1} y^{u_2} z^{u_3} w^{u_4}$$

   και

   $$1 \backslash x^{v_1} y^{v_2} z^{v_3} w^{v_4}.$$

   Το διώνυμο B είναι διάφορο του $zw - 1$, άρα το το B δεν είναι πρωταρχικό, δηλαδή δεν ανήκει στη βάση Graver του ιδεώδους $I_{\mathbf{A}}$.

Συνεπώς τα μοναδικά στοιχεία της βάσης Graver του ιδεώδους $I_{\mathbf{A}}$ είναι τα διώνυμα $xy - 1, zw - 1$. Δηλαδή

$$Gr_A = \{xy - 1, zw - 1\}.$$

Θεωρούμε το ιδεώδες $M = \langle 1 - (xy)^{2012}(zw)^{2013}, 1 - (xy)^{2011}(zw)^{2012} \rangle$. Παρατηρούμε ότι:

1. Το διώνυμο $1-(xy)(zw) = 1-(xy)^{2012}(zw)^{2013}-(xy)(zw)(1-(xy)^{2011}(zw)^{2012})$, συνεπώς διώνυμο $1 - (xy)(zw)$ ανήκει στο M.

2. Το διώνυμο $1 - xy = (1 - (xy)^{2013}(zw)^{2013}) - xy(1 - (xy)^{2012}(zw)^{2013})$, όπου $1 - (xy)^{2013}(zw)^{2013} = 1^{2013} - (xy)^{2013}(zw)^{2013} = (1 - (xy)(zw))$ $(1 + (xy)(zw) + ... + (xy)^{2012}(zw)^{2012})$.
   Δηλαδή:
   $1 - xy = (1 - (xy)(zw))(1 + (xy)(zw) + ... + (xy)^{2012}(zw)^{2012}) -$ $xy(1-(xy)^{2012}(zw)^{2013})$, κι αφού τα διώνυμα $1-(xy)(zw), 1-(xy)^{2012}(zw)^{2013}$ ανήκουν στο M συνεπάγεται πως $1 - xy$ ανήκει στο M.

3. Το διώνυμο $1 - zw = 1 - (xy)(zw) - zw(1 - xy)$, κι αφού τα διώνυμα $1 - (xy)(zw), 1 - xy$ ανήκουν στο M συνεπάγεται πως το διώνυμο $1 - zw$ ανήκει στο M.

Προφανώς και τα διώνυμα $xy - 1, zw - 1$ ανήκουν στο M, δηλαδή το ιδεώδες $I_{\mathbf{A}}$ είναι υποσύνολο του M.
Ωστόσο τα διώνυμα $1-(xy)^{2012}(zw)^{2013}, 1-(xy)^{2011}(zw)^{2012}$ ανήκουν στο ιδεώδες $I_{\mathbf{A}}$, δηλαδή το M είναι υποσύνολο του ιδεώδους $I_{\mathbf{A}}$. Άρα τελικά είναι ίσα δηλαδή

$$M = \langle 1 - (xy)^{2012}(zw)^{2013}, 1 - (xy)^{2011}(zw)^{2012} \rangle = \langle xy - 1, zw - 1 \rangle = I_{\mathbf{A}}.$$

Βρήκαμε ένα ακόμη σύνολο γεννητόρων του ιδεώδους $I_{\mathbf{A}}$, δηλαδή μια ακόμη βάση Markov πέραν της

$$\{xy - 1, zw - 1\}$$

η οποία είναι η

$$\{1 - (xy)^{2012}(zw)^{2013}, 1 - (xy)^{2011}(zw)^{2012}\}$$

που είναι ελαχιστοτική βάση Markov, αφού το ιδεώδες $I_{\mathbf{A}}$ δεν είναι κύριο κάτι το οποίο αποδεικνύουμε στη συνέχεια. Ωστόσο παρατηρούμε πως υπάρχουν άπειρες ελαχιστοτικές βάσεις Markov. Κάποιες από αυτές είναι της μορφής:

$$\{1 - (xy)^k(zw)^{k+1}, 1 - (xy)^{k-1}(zw)^k\}$$

όπου $k \in \mathbb{N}_0$. Άρα η καθολική βάση Markov, ως ένωση των ελαχιστοτικών βάσεων Markov έχει άπειρα στοιχεία, κατά συνέπεια δεν είναι υποσύνολο της βάσης Graver που έχει μονάχα δύο.
Τώρα θα αποδείξουμε αυτό που αναφέραμε παραπάνω. Δηλαδή πως η βάση Markov είναι ελαχιστοτική, αφού το ιδεώδες $I_{\mathbf{A}}$ δεν είναι κύριο.
Αρχικά ισχυριζόμαστε ότι τα διώνυμα $xy - 1, zw - 1$ είναι ανάγωγα. Θα το αποδείξουμε για το διώνυμο $xy - 1$, όμοια αποδεικνύεται και για το διώνυμο $zw - 1$. Θεωρούμε τη βαθμωτή λεξικογραφική διάταξη $\succ_{deglex}$ με $x > y$. Έστω ότι $xy - 1 = f(x, y)g(x, y)$, με

$$xy = lt_{\prec_{deglex}}(f)lt_{\prec_{deglex}}(g),$$

αφού ισχύει ότι $lt_{\prec}(fg) = lt_{\prec}(f)lt_{\prec}(g)$. Διακρίνουμε περιπτώσεις:

1. Ο αρχικός όρος $lt_{\prec_{deglex}}(f) = xy$. Τότε ο αρχικός όρος $lt_{\prec_{deglex}}(g) = 1$, δηλαδή το πολυώνυμο g είναι μονάδα.

2. Ο αρχικός όρος $lt_{\prec_{deglex}}(f) = x$. Τότε ο αρχικός όρος $lt_{\prec_{deglex}}(g) = y$. Εφόσον ο αρχικός όρος $lt_{\prec_{deglex}}(f) = x$, τότε το πολυώνυμο f ισούται με $ax + by + c$. Εφόσον ο αρχικός όρος $lt_{\prec_{deglex}}(g) = y$, τότε το πολυώνυμο g ισούται με $= dy + e$. Άρα για το διώνυμο $xy - 1$ έχουμε:

$$xy - 1 = (ax + by + c)(dy + e)$$

   το σύστημα αυτό είναι αδύνατο.

3. Ο αρχικός όρος $lt_{\prec_{deglex}}(f) = y$. Τότε ο αρχικός όρος $lt_{\prec_{deglex}}(g) = x$, όμοια με την δεύτερη περίπτωση.

4. Ο αρχικός όρος $lt_{\prec_{deglex}}(f) = 1$. Τότε ο αρχικός όρος $lt_{\prec_{deglex}}(g) = xy$, δηλαδή το πολυώνυμο f είναι μονάδα.

Οπότε το διώνυμο $xy - 1$ είναι ανάγωγο όμοια το διώνυμο $zw - 1$ είναι ανάγωγα. Τώρα υποθέτουμε ότι το ιδεώδες I_A είναι κύριο, θα καταλήξουμε σε άτοπο. Είναι:

$$\langle 1 - xy, 1 - zw \rangle = \langle f \rangle$$

Άρα $1 - xy = g_1 f, 1 - zw = g_2 f$. Όμως το διώνυμο $1 - xy$ είναι ανάγωγο και ο πολυωνυμικός δακτύλιος $K[x, y, z, w]$ είναι Π.Μ.Α, άρα είναι:

$$f = a(1 - xy), a \in K$$

ή

$$f = b, b \in K.$$

Αντίστοιχα το διώνυμο $1 - zw$ είναι ανάγωγο και ο πολυωνυμικός δακτύλιος $K[x, y, z, w]$ είναι Π.Μ.Α, άρα είναι:

$$f = c(1 - zw), c \in K$$

ή

$$f = d, d \in K$$

Άρα αναγκαστικά το πολυώνυμο f είναι μονάδα. Αν το πολυώνυμο f ήταν μονάδα, τότε $\langle f \rangle = K[x, y, z, w]$. Δηλαδή, $\langle 1 - xy, 1 - zw \rangle = K[x, y, z, w]$. Τότε το 1 ανήκει στον πολυωνυμικό δακτύλιο $K[x, y, z, w] = \langle 1 - xy, 1 - zw \rangle$, άρα

$$1 = F(x, y, z, w)(1 - xy) + G(x, y, z, w)(1 - zw)$$

όμως για $x = y = z = w = 1$ έχουμε ότι $1 = 0$, άτοπο.

Πρόταση 2.2.25. *Η βάση Graver του ιδεώδους I_A είναι σύνολο γεννητόρων του ιδεώδους I_A και μια βάση Gröbner ως προς οποιαδήποτε διάταξη όρων.*

Απόδειξη. Η καθολική βάση Gröbner του ιδεώδους I_A, είναι υποσύνολο της βάσης Graver του ιδεώδους I_A, σύμφωνα με την πρόταση 2.2.4. Ωστόσο η καθολική βάση Gröbner είναι η ένωση όλων των ανάγωγων βάσεων Gröbner ως προς οποιαδήποτε διάταξη όρων. Άρα περιέχει τουλάχιστον μια ανάγωγη βάση Gröbner. Έτσι η βάση Graver του A περιέχει μια βάση Gröbner του ιδεώδους I_A. Εφόσον τα υπόλοιπα στοιχεία της, ανήκουν στο ιδεώδες I_A συμπεραίνουμε πως η βάση Graver του A είναι βάση Gröbner του I_A. Αν επιλέξουμε μια οποιαδήποτε διάταξη όρων τότε η ανάγωγη βάση Gröbner ως προς τη διάταξη αυτή ανήκει στην καθολική βάση Gröbner, η οποία είναι υποσύνολο της βάσης Graver. Άρα η βάση Graver είναι μια βάση Gröbner ως προς οποιαδήποτε διάταξη. Μια ανάγωγη βάση Gröbner, ως βάση Gröbner αποτελεί σύνολο γεννητόρων του ιδεώδους. Έτσι η βάση Graver του A περιέχει ένα σύνολο γεννητόρων του ιδεώδους I_A. Εφόσον τα υπόλοιπα στοιχεία της, πέραν των γεννητόρων του ιδεώδους, ανήκουν στο ιδεώδες I_A συμπεραίνουμε πως η βάση Graver του A είναι σύνολο γεννητόρων του ιδεώδους I_A. □

Τέλος θα δούμε μια σχέση που συνδέει τις ανάγωγες βάσεις Gröbner και τις βάσεις Markov του ιδεώδους I_A. Μάλιστα στο παράδειγμα που ακολουθεί θα γίνει χρήση ενός πολύ σημαντικού λήμματος του πρώτου κεφαλαίου σχετικά με τον υπολογισμό των βάσεων Gröbner στο οποίο είχαμε κάνει μια ιδιαίτερη αναφορά, του λήμματος 1.4.8.

Παρατήρηση 2.2.26. Σε κάθε ανάγωγη βάση Gröbner περιέχεται τουλάχιστον μια ελαχιστική βάση Markov αλλά κάθε βάση Markov δεν περιέχεται αναγκαστικά σε μια ανάγωγη βάση Gröbner. Δηλαδή υπάρχουν βάσεις Markov που δεν περιέχονται σε καμία ανάγωγη βάση Gröbner.

Παράδειγμα 2.2.27. Στο παράδειγμα αυτό θα δείξουμε ότι υπάρχουν βάσεις Markov που δεν περιέχονται σε καμία ανάγωγη βάση Gröbner. Έστω το σύνολο $A = \{(2,4,4,2,2),(2,0,0,2,2),(2,4,0,2,2),(2,0,4,2,2),(3,3,3,6,6),(3,3,3,0,0),(3,3,3,6,0),(3,3,3,0,6)\}$. Για το τορικό ιδεώδες I_A μια βάση Markov δίνεται από τα διώνυμα $x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8$. Πιο συγκεκριμένα υπάρχουν ακριβώς 12 ελαχιστοτικές βάσεις Markov και είναι οι ακόλουθες:

$A_1 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^3x_2^3 - x_5^2x_6^2\}$
$A_2 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^3x_2^3 - x_5x_6x_7x_8\}$
$A_3 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^3x_2^3 - x_7^2x_8^2\}$
$A_4 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_5^2x_6^2\}$
$A_5 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8\}$
$A_6 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_7^2x_8^2\}$
$A_7 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1x_2x_3^2x_4^2 - x_5^2x_6^2\}$
$A_8 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1x_2x_3^2x_4^2 - x_5x_6x_7x_8\}$
$A_9 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1x_2x_3^2x_4^2 - x_7^2x_8^2\}$
$A_{10} = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_3^3x_4^3 - x_5^2x_6^2\}$
$A_{11} = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_3^3x_4^3 - x_5x_6x_7x_8\}$
$A_{12} = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_3^3x_4^3 - x_7^2x_8^2\}$.

Η καθολική βάση Markov του ιδεώδους I_A είναι η εξής:

$$A_1 \bigcup \ldots \bigcup A_{12} =$$

$\{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^3x_2^3 - x_5^2x_6^2, x_1^3x_2^3 - x_5x_6x_7x_8, x_1^3x_2^3 - x_7^2x_8^2,$
$x_1^2x_2^2x_3x_4 - x_5^2x_6^2, x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8, x_1^2x_2^2x_3x_4 - x_7^2x_8^2, x_1x_2x_3^2x_4^2 - x_5^2x_6^2,$
$x_1x_2x_3^2x_4^2 - x_5x_6x_7x_8, x_1x_2x_3^2x_4^2 - x_7^2x_8^2, x_3^3x_4^3 - x_5^2x_6^2, x_3^3x_4^3 - x_5x_6x_7x_8,$
$x_3^3x_4^3 - x_7^2x_8^2\}$.

Θα δείξουμε ότι η Markov βάση A_5 δεν περιέχεται σε καμία ανάγωγη βάση Gröbner, όπου δε μας ενδιαφέρει το πρόσημο. Με τον ίδιο τρόπο αποδεικνύεται ότι οι βάσεις $A_2, A_4, A_6, A_7, A_8, A_9, A_{11}$ δεν περιέχονται σε καμία ανάγωγη βάση Gröbner. Έστω ότι η Markov βάση $A_5 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8\}$ περιέχεται σε μια ανάγωγη βάση Gröbner ως προς κάποια διάταξη όρων $\prec$. Θέτουμε $f = x_1x_2 - x_3x_4, g = x_5x_6 - x_7x_8, h = x_1^2x_2^2x_3x_4 - x_5x_6x_7x_8$. Τότε η ανάγωγη βάση θα είναι της μορφής $\{f, g, h, \ldots\}$. Παρατηρούμε ότι αυτό είναι άτοπο, καθώς το $lm(g) \setminus x_5x_6x_7x_8$ όποιο κι αν είναι το αρχικό μονώνυμο του g, άρα η βάση δεν είναι ανάγωγη. Συνεπώς βρήκαμε ένα στοιχείο που ανήκει στην καθολική βάση Markov και δεν ανήκει στην καθολική βάση Gröbner. Μονάχα τα διώνυμα $x_1^3x_2^3 - x_5^2x_6^2, x_1^3x_2^3 - x_7^2x_8^2, x_3^3x_4^3 - x_5^2x_6^2, x_3^3x_4^3 - x_7^2x_8^2$ ανήκουν σε κάποια ανάγωγη βάση Gröbner με την κατάλληλη διάταξη όρων, τα υπόλοιπα όχι. Άρα μονάχα οι βάσεις A_1, A_3, A_{10}, A_{12} είναι υποσύνολα κάποιας ανάγωγης βάσης Gröbner με την κατάλληλη διάταξη όρων. Θα δείξουμε ότι η βάση A_1 περιέχεται σε μια ανάγωγη βάση Gröbner. Με τον ίδιο τρόπο αποδεικνύουμε ότι και οι βάσεις A_3, A_{10}, A_{12} περιέχονται σε κάποια ανάγωγη βάση Gröbner με την κατάλληλη διάταξη. Έστω η βάση $A_1 = \{x_1x_2 - x_3x_4, x_5x_6 - x_7x_8, x_1^3x_2^3 - x_5^2x_6^2\}$. Ορίζουμε λεξικογραφική διάταξη όρων τέτοια ώστε $x_3 > x_4 > x_7 > x_8 > x_5 > x_6 > x_1 > x_2$. Ισχυριζόμαστε ότι η βάση A_1 είναι βάση Gröbner. Θέτουμε $f = -x_3x_4 + x_1x_2, g = -x_7x_8 + x_5x_6, h =$

$-x_5^2x_6^2+x_1^3x_2^3$. Πράγματι παρατηρώντας ότι μκδ(f,g) =μκδ(f,h) =μκδ$(h,g)=1$, και μκδ$(lt(f),lt(g))$ =μκδ$(lt(f),lt(h))$ =μκδ$(lt(h),lt(g))=1$ σύμφωνα με το λήμμα 1.4.8 του πρώτου κεφαλαίου, καταλήγουμε στο συμπέρασμα πως η βάση A_1 είναι βάση Gröbner. Παρατηρούμε μάλιστα πως η $\{-f,-g,-h\}$ είναι μια ανάγωγη βάση Gröbner ως προς τη διάταξη όρων που ορίσαμε. Συνεπώς δείξαμε πως η βάση A_1 περιέχεται στην καθολική βάση Gröbner.

2.3 Πίνακας Lawrence $A^{(2)}$

Σε αυτό το σημείο θα παραθέσουμε κάποιες έννοιες οι οποίες θα μας απασχολήσουν κατά κύριο λόγο στο τρίτο και τέταρτο κεφάλαιο. Ωστόσο είναι απαραίτητες σε μας γιατί μας βοηθάνε για τον υπολογισμό της βάσης Graver του ιδεώδους I_A.

Ορισμός 2.3.1. *Θεωρούμε L μια υποομάδα του $\mathbb{Z}^n=\{(u_1,...,u_n): u_i\in\mathbb{Z}\}$. Οι υποομάδες του $\mathbb{Z}^n$ ονομάζονται* **κιγκλιδώματα.**

Σταθεροποιούμε ένα σύνολο διανυσμάτων $A=\{\mathbf{a}_1,...,\mathbf{a}_n\}\subseteq\mathbb{Z}^d\subseteq\mathbb{Q}^d$ που παράγουν τον $\mathbb{Q}^d$ κι έστω $\mathrm{Ker}_{\mathbb{Z}}A$ το κιγκλίδωμα των γραμμικών συνδυασμών του A. Το σύνολο διανυσμάτων A μπορούμε να το παραστήσουμε και στη μορφή ενός $d\times n$ πίνακα οι στήλες του οποίου είναι τα διανύσματα του συνόλου A. Δηλαδή

$$\mathcal{A}=\begin{pmatrix} a_{11} & a_{21} & . & . & . & a_{n1} \\ a_{12} & a_{22} & . & . & . & a_{n2} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{1d} & a_{2d} & . & . & . & a_{nd} \end{pmatrix}$$

όπου $\mathbf{a}_1=(a_{11},...,a_{1d}),...,\mathbf{a}_n=(a_{n1},...,a_{nd})$.
Το A λοιπόν το βλέπουμε με δύο τρόπους, πρώτον ως σύνολο διανυσμάτων και δεύτερον στη μορφή πίνακα.
Ορίζουμε τη δεύτερη άρση του πίνακα A, $A^{(2)}$, ως εξής:

$$A^{(2)}=\begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & A \\ \mathrm{I} & \mathrm{I} \end{pmatrix}$$

Όπου I ο μοναδιαίος $n\times n$ πίνακας. Το $I_{\mathbf{A}}$ είναι το ιδεώδες:

$$I_{\mathbf{A}}=\langle x^{\mathbf{u}^+}-x^{\mathbf{u}^-}/deg_A(x^{\mathbf{u}^+})=deg_A(x^{\mathbf{u}^-})\rangle$$

όπου $\mathbf{u}=(u_1,...,u_n)$. Από την παρατήρηση 2.1.10 έχουμε ότι:

$$deg_A(x^{\mathbf{u}^+})=deg_A(x^{\mathbf{u}^-})\Leftrightarrow u_1\mathbf{a}_1+...+u_n\mathbf{a}_n=0.$$

Δηλαδή
$$\begin{pmatrix} a_{11} & a_{21} & . & . & . & a_{n1} \\ a_{12} & a_{22} & . & . & . & a_{n2} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{1d} & a_{2d} & . & . & . & a_{nd} \end{pmatrix}\begin{pmatrix} u_1 \\ . \\ . \\ . \\ u_n \end{pmatrix}=\begin{pmatrix} 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}.$$

Συνεπώς

$$a_{11}u_1+...+a_{n1}u_n=0$$

...

$$a_{1d}u_1 + ... + a_{nd}u_n = 0$$

δηλαδή $Au^\tau = 0 \Leftrightarrow u^\tau \in \mathrm{Ker}_{\mathbb{Z}} A$. Θα επαναλάβουμε τη διαδικασία για τον πίνακα $A^{(2)}$.

Είναι $A^{(2)} = \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0} & A \\ \mathrm{I} & \mathrm{I} \end{pmatrix} =$

$$\begin{pmatrix}
a_{11} & . & . & . & a_{n1} & 0 & . & . & . & 0 \\
a_{12} & . & . & . & a_{n2} & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
a_{1d} & . & . & . & a_{nd} & 0 & . & . & . & 0 \\
0 & . & . & . & 0 & a_{11} & . & . & . & a_{n1} \\
. & . & . & . & . & a_{12} & . & . & . & a_{n2} \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & 0 & a_{1d} & . & . & . & a_{nd} \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

άρα

$$\begin{pmatrix}
a_{11} & . & . & . & a_{n1} & 0 & . & . & . & 0 \\
a_{12} & . & . & . & a_{n2} & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
a_{1d} & . & . & . & a_{nd} & 0 & . & . & . & 0 \\
0 & . & . & . & 0 & a_{11} & . & . & . & a_{n1} \\
. & . & . & . & . & a_{12} & . & . & . & a_{n2} \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
0 & . & . & . & 0 & a_{1d} & . & . & . & a_{nd} \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\begin{pmatrix} u_1 \\ . \\ . \\ . \\ . \\ . \\ u_n \\ v_1 \\ . \\ . \\ . \\ . \\ . \\ . \\ v_n \end{pmatrix}
=
\begin{pmatrix} 0 \\ . \\ . \\ . \\ 0 \\ 0 \\ . \\ . \\ . \\ 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}.$$

Συνεπώς

$$a_{11}u_1 + ... + a_{n1}u_n = 0$$

$$a_{12}u_1 + ... + a_{n2}u_n = 0$$

...

$$a_{1d}u_1 + ... + a_{nd}u_n = 0$$

και

$$a_{11}v_1 + ... + a_{n1}v_n = 0$$

$$a_{12}v_1 + ... + a_{n2}v_n = 0$$

...

$$a_{1d}v_1 + ... + a_{nd}v_n = 0.$$

Είναι $A\mathbf{u}^\tau = 0 \Leftrightarrow \mathbf{u}^\tau \in \mathrm{Ker}_{\mathbb{Z}}A$ και $A\mathbf{v}^\tau = 0 \Leftrightarrow \mathbf{v}^\tau \in \mathrm{Ker}_{\mathbb{Z}}A$. Ακόμη από τις τελευταίες γραμμές του πίνακα $A^{(2)}$, έχουμε $u_1 + v_1 = 0, ..., u_n + v_n = 0$, δηλαδή $\mathbf{u}^\tau + \mathbf{v}^\tau = 0 \Rightarrow \mathbf{v}^\tau = -\mathbf{u}^\tau$. Τα διανύσματα λοιπόν $\mathbf{u}^\tau, \mathbf{v}^\tau$ είναι αντίθετα συνεπώς $\mathbf{v}^+ = \mathbf{u}^-$ και $\mathbf{v}^- = \mathbf{u}^+$.
Είμαστε στο δακτύλιο πολυωνύμων $K[x_1^{(1)}, ..., x_n^{(1)}, x_1^{(2)}, ..., x_n^{(2)}]$, το τορικό ιδεώδες στο $A^{(2)}$ είναι το εξής:

$$I_{A^{(2)}} = \langle x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}} - x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}} / \mathbf{u}^\tau \in \mathrm{Ker}_{\mathbb{Z}}A \rangle.$$

Πρόταση 2.3.2. *Η βάση Graver του $A^{(2)}$ είναι το σύνολο:*

$$\{x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}} - x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}} / \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in Gr_A\}.$$

Απόδειξη. Έστω ότι το διώνυμο $x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}} - x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}}$ ανήκει στη βάση Graver του $I_{A^{(2)}}$, υποθέτουμε ότι το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν ανήκει στη βάση Graver του I_A, θα καταλήξουμε σε άτοπο. Αφού το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν ανήκει στη βάση Graver του I_A συνεπάγεται πως υπάρχει ένα διώνυμο $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \in I_A$ με $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-} \neq \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ τέτοιο ώστε $\mathbf{x}^{\mathbf{v}^+} \setminus \mathbf{x}^{\mathbf{u}^+}$ και $\mathbf{x}^{\mathbf{v}^-} \setminus \mathbf{x}^{\mathbf{u}^-}$. Συνεπώς:

$$x^{(1)^{\mathbf{v}^+}} \setminus x^{(1)^{\mathbf{u}^+}}, x^{(2)^{\mathbf{v}^-}} \setminus x^{(2)^{\mathbf{u}^-}} \quad (1)$$

$$\text{και } x^{(2)^{\mathbf{v}^+}} \setminus x^{(2)^{\mathbf{u}^+}}, x^{(1)^{\mathbf{v}^-}} \setminus x^{(1)^{\mathbf{u}^-}} \quad (2).$$

Τότε από τη σχέση (1) συνεπάγεται πως το $x^{(1)^{\mathbf{v}^+}} x^{(2)^{\mathbf{v}^-}} \setminus x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}}$ ενώ από τη σχέση (2) συνεπάγεται πως το $x^{(1)^{\mathbf{v}^-}} x^{(2)^{\mathbf{v}^+}} \setminus x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}}$ και $x^{(1)^{\mathbf{v}^+}} x^{(2)^{\mathbf{v}^-}} - x^{(1)^{\mathbf{v}^-}} x^{(2)^{\mathbf{v}^+}}$ ανήκει στο ιδεώδες $I_{A^{(2)}}$. Άρα το διώνυμο $x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}} - x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}}$ δεν είναι πρωταρχικό, άτοπο.
Αντίστροφα έστω ότι το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ ανήκει στη βάση Graver του I_A, υποθέτουμε ότι το διώνυμο $x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}} - x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}}$ δεν ανήκει στη βάση Graver του $I_{A^{(2)}}$, θα καταλήξουμε σε άτοπο.
Αφού το διώνυμο $x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}}} - x^{(1)^{\mathbf{u}}} x^{(2)^{\mathbf{u}^+}}$ δεν ανήκει στη βάση Graver του $I_{A^{(2)}}$ συνεπάγεται πως υπάρχει ένα διώνυμο $x^{(1)^{\mathbf{v}^+}} x^{(2)^{\mathbf{v}^-}} - x^{(1)^{\mathbf{v}^-}} x^{(2)^{\mathbf{v}^+}} \in I_{A^{(2)}}$ με $x^{(1)^{\mathbf{v}^+}} x^{(2)^{\mathbf{v}}} - x^{(1)^{\mathbf{v}}} x^{(2)^{\mathbf{v}^+}} \neq x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}}} - x^{(1)^{\mathbf{u}}} x^{(2)^{\mathbf{u}^+}}$, τέτοιο ώστε $x^{(1)^{\mathbf{v}^+}} x^{(2)^{\mathbf{v}^-}} \setminus x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}}$ και $x^{(1)^{\mathbf{v}^-}} x^{(2)^{\mathbf{v}^+}} \setminus x^{(1)^{\mathbf{u}^-}} x^{(2)^{\mathbf{u}^+}}$. Από τη σχέση

$x^{(1)^{\mathbf{v}^+}} x^{(2)^{\mathbf{v}^-}} \setminus x^{(1)^{\mathbf{u}^+}} x^{(2)^{\mathbf{u}^-}}$, έχουμε ότι το $x^{(1)^{\mathbf{v}^+}} \setminus x^{(1)^{\mathbf{u}^+}}$ και το $x^{(2)^{\mathbf{v}^-}} \setminus x^{(2)^{\mathbf{u}^-}}$. Άρα $\mathbf{u}^+ \geq \mathbf{v}^+ \Rightarrow \mathbf{u}^+ - \mathbf{v}^+ \geq (0,...,0)$ και $\mathbf{u}^- \geq \mathbf{v}^- \Rightarrow \mathbf{u}^- - \mathbf{v}^- \geq (0,...,0)$ σύμφωνα με τον ορισμό 2.2.13. Από τη μερική διάταξη που ορίζεται από τη διαιρετότητα έχουμε ότι $\mathbf{x}^{\mathbf{v}^+} \geq \mathbf{x}^{\mathbf{u}^+} \Rightarrow \mathbf{x}^{\mathbf{v}^+} \setminus \mathbf{x}^{\mathbf{u}^+}$ και $\mathbf{x}^{\mathbf{v}} \geq \mathbf{x}^{\mathbf{u}} \Rightarrow \mathbf{x}^{\mathbf{v}} \setminus \mathbf{x}^{\mathbf{u}}$ και το διώνυμο $\mathbf{x}^{\mathbf{v}^+} - \mathbf{x}^{\mathbf{v}^-}$ ανήκει στο ιδεώδες I_A. Άρα το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν είναι πρωταρχικό, άτοπο. □

Πρόταση 2.3.3. *Όταν ισχύει* $(\mathbb{N}\mathbf{A}) \bigcap -(\mathbb{N}\mathbf{A}) = \{0\}$ *τότε έχουμε* $(\mathbb{N}A^{(2)}) \bigcap -(\mathbb{N}A^{(2)}) = \{0\}$.

Απόδειξη. Έστω το σύνολο διανυσμάτων $\Lambda = \{\mathbf{a}_1,...,\mathbf{a}_n\}$. Τότε ο αντίστοιχος πίνακας A είναι ο εξής

$$A = \begin{pmatrix} a_{11} & a_{21} & . & . & . & a_{n1} \\ a_{12} & a_{22} & . & . & . & a_{n2} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{1d} & a_{2d} & . & . & . & a_{nd} \end{pmatrix}.$$

Οι στήλες του πίνακα A καθορίζουν την ημιομάδα

$$\mathbb{N}\mathbf{A} = \{c_1\mathbf{a}_1 + ... + c_n\mathbf{a}_n / c_i \in \mathbb{N}_0\}.$$

Θεωρούμε τον πίνακα $A^{(2)}$,

$$A^{(2)} = \begin{pmatrix} a_{11} & . & . & . & a_{n1} & 0 & . & . & . & 0 \\ a_{12} & . & . & . & a_{n2} & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ a_{1d} & . & . & . & a_{nd} & 0 & . & . & . & 0 \\ 0 & . & . & . & 0 & a_{11} & . & . & . & a_{n1} \\ . & . & . & . & . & a_{12} & . & . & . & a_{n2} \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & 0 & a_{1d} & . & . & . & a_{nd} \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Έστω το σύνολο διανυσμάτων $\mathbf{B} = \{\mathbf{b}_1,...,\mathbf{b}_n,...,\mathbf{b}_{2n}\}$ του οποίου τα διανύσματα είναι οι στήλες του πίνακα $A^{(2)}$. Οι στήλες του πίνακα $A^{(2)}$ καθορίζουν την ημιομάδα $\mathbb{N}\mathbf{B} = \{k_1\mathbf{b}_1 + ... + k_{2n}\mathbf{b}_{2n} / k_i \in \mathbb{N}_0\}$.
Ισχυριζόμαστε ότι το μοναδικό στοιχείο που και το αντίθετο του ανήκει στην ημιομάδα $\mathbb{N}\mathbf{B}$ είναι το μηδενικό. Έστω όχι, θα καταλήξουμε σε άτοπο. Υποθέτουμε λοιπόν ότι $\mathbf{b}, -\mathbf{b}$ ανήκουν στην ημιομάδα $\mathbb{N}\mathbf{B}$ και το $\mathbf{b}$ είναι μη μηδενικό. Είναι:
$\mathbf{b}_1 = (a_{11},...,a_{1d},0,...,0,1,...,0)$,...,$\mathbf{b}_n = (a_{n1},...,a_{nd},0,...,0,0,...,1)$
$\mathbf{b}_{n+1} = (0,...,0,a_{11},...,a_{1d},1,...,0)$,...,$\mathbf{b}_{2n} = (0,...,0,a_{n1},...,a_{nd},0,...,1)$.
Έτσι για τα διανύσματα $\mathbf{b}, -\mathbf{b}$ έχουμε:
$\mathbf{b} = l_1\mathbf{b}_1 + ... + l_n\mathbf{b}_n + l_{n+1}\mathbf{b}_{n+1} + ... + l_{2n}\mathbf{b}_{2n}$
$-\mathbf{b} = m_1\mathbf{b}_1 + ... + m_n\mathbf{b}_n + m_{n+1}\mathbf{b}_{n+1} + ... + m_{2n}\mathbf{b}_{2n}$, όπου $l_1,...,l_{2n}, m_1...,m_{2n} \geq$

0.
Θεωρούμε την απεικόνιση $\pi_1 : \mathbb{Z}^{2d+n} \to \mathbb{Z}^d$, η οποία είναι η προβολή του διανύσματος στις πρώτες d συντεταγμένες. Η προβολή π_1 είναι γραμμικός μετασχηματισμός οπότε έχουμε:
$\pi_1(\mathbf{b}) = l_1\pi_1(\mathbf{b}_1) + ... + l_n\pi_1(\mathbf{b}_n) + l_{n+1}\pi_1(\mathbf{b}_{n+1}) + ... + l_{2n}\pi_1(\mathbf{b}_{2n})$. Όμως για $1 \leq i \leq n$ ισχύει $\pi_1(\mathbf{b}_i) = \mathbf{a}_i$, ενώ $n+1 \leq i \leq 2n$ ισχύει $\pi_1(\mathbf{b}_i) = 0$. Άρα τελικά:
$\pi_1(\mathbf{b}) = l_1\mathbf{a}_1 + ... + l_n\mathbf{a}_n$ και $-\pi_1(\mathbf{b}) = m_1\mathbf{a}_1 + ... + m_n\mathbf{a}_n$.
Οπότε $\pi_1(\mathbf{b}), -\pi_1(\mathbf{b})$ ανήκουν στην ημιομάδα $\mathbb{N}\mathbf{A}$. Συνεπώς από τον ορισμό της $\mathbb{N}\mathbf{A}$ εφόσον το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του στην ημιομάδα είναι το μηδενικό, συνεπάγεται πως $\pi_1(\mathbf{b}) = 0$, δηλαδή $l_1\mathbf{a}_1 + ... + l_n\mathbf{a}_n = 0$. Παρατηρούμε ότι $l_1 = ... = l_n = 0$. Έστω όχι, θα καταλήξουμε σε άτοπο. Υποθέτουμε λοιπόν ότι υπάρχει ένα $l_i \neq 0$ τότε έχουμε:
$-l_i\mathbf{a}_i = l_1\mathbf{a}_1 + ... + l_{i-1}\mathbf{a}_{i-1} + l_{i+1}\mathbf{a}_{i+1} + ... + l_n\mathbf{a}_n \in \mathbb{N}\mathbf{A}$,
αφού τα $l_1, ..., l_{i-1}, l_{i+1}, ..., l_n$ ανήκουν στο $\mathbb{N}_0$ και $\mathbf{a}_1, ..., \mathbf{a}_{i-1}, \mathbf{a}_{i+1}, ..., \mathbf{a}_n$ ανήκουν στο A.
Το $l_i\mathbf{a}_i$ ανήκει στην ημιομάδα $\mathbb{N}\mathbf{A}$, δηλαδή έχουμε ότι $l_i\mathbf{a}_i \in \mathbb{N}\mathbf{A}$ και $-l_i\mathbf{a}_i \in \mathbb{N}\mathbf{A}$, όμως από τον ορισμό της $\mathbb{N}\mathbf{A}$ το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του στην ημιομάδα είναι το μηδενικό, συνεπώς $l_i\mathbf{a}_i = \mathbf{0}$, άρα εφόσον το διάνυσμα $\mathbf{a}_i$ είναι μη μηδενικό, έχουμε $l_i = 0$. Άτοπο, άρα τελικά $l_1 = ... = l_n = 0$.
Θεωρούμε την απεικόνιση $\pi_2 : \mathbb{Z}^{2d+n} \to \mathbb{Z}^d$, η οποία είναι η προβολή του διανύσματος στις δεύτερες d συντεταγμένες. Η προβολή π_2 είναι γραμμικός μετασχηματισμός οπότε έχουμε:
$\pi_2(\mathbf{b}) = l_1\pi_2(\mathbf{b}_1) + ... + l_n\pi_2(\mathbf{b}_n) + l_{n+1}\pi_2(\mathbf{b}_{n+1}) + ... + l_{2n}\pi_2(\mathbf{b}_{2n})$. Όμως για $1 \leq i \leq n$ ισχύει $\pi_2(\mathbf{b}_i) = 0$, ενώ $n+1 \leq i \leq 2n$ ισχύει $\pi_2(\mathbf{b}_i) = a_{i-n}$. Άρα τελικά:
$\pi_2(\mathbf{b}) = l_{n+1}\mathbf{a}_1 + ... + l_{2n}\mathbf{a}_n$ και $-\pi_2(\mathbf{b}) = m_{n+1}\mathbf{a}_1 + ... + m_{2n}\mathbf{a}_n$.
Οπότε $\pi_2(\mathbf{b}), -\pi_2(\mathbf{b})$ ανήκουν στην ημιομάδα $\mathbb{N}\mathbf{A}$. Συνεπώς από τον ορισμό της $\mathbb{N}\mathbf{A}$ εφόσον το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του στην ημιομάδα είναι το μηδενικό, συνεπάγεται πως $\pi_2(\mathbf{b}) = 0$, δηλαδή $l_{n+1}\mathbf{a}_1 + ... + l_{2n}\mathbf{a}_n = 0$. Παρατηρούμε ότι $l_{n+1} = ... = l_{2n} = 0$. Έστω όχι, θα καταλήξουμε σε άτοπο. Υποθέτουμε λοιπόν ότι υπάρχει ένα $l_j \neq 0$ τότε έχουμε:
$-l_j\mathbf{a}_{j-n} = l_{n+1}\mathbf{a}_1 + ... + l_{j-1}\mathbf{a}_{(j-1)-n} + l_{(j+1)-n}\mathbf{a}_{j+1} + ... + l_{2n}\mathbf{a}_n \in \mathbb{N}\mathbf{A}$, αφού $l_1, ..., l_{j-1}, l_{j+1}, ..., l_n \in \mathbb{N}_0$ και $\mathbf{a}_1, ..., \mathbf{a}_{(j-1)-n}, \mathbf{a}_{(i+1)-n}, ..., \mathbf{a}_n \in A$.
Το $l_j\mathbf{a}_j$ ανήκει στην ημιομάδα $\mathbb{N}\mathbf{A}$, δηλαδή έχουμε ότι $l_j\mathbf{a}_j \in \mathbb{N}\mathbf{A}$ και $-l_j\mathbf{a}_j \in \mathbb{N}\mathbf{A}$, άρα από τον ορισμό της $\mathbb{N}\mathbf{A}$ το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του στην ημιομάδα είναι το μηδενικό, συνεπώς $l_j\mathbf{a}_j = 0$, άρα εφόσον τα διανύσματα $\mathbf{a}_j$ είναι μη μηδενικά, έχουμε $l_j = 0$. Άτοπο, άρα τελικά $l_{n+1} = ... = l_{2n} = 0$.
Συνεπώς το διάνυσμα $\mathbf{b}$ είναι το μηδενικό διάνυσμα αφού

$$\mathbf{b} = l_1\mathbf{b}_1 + ... + l_n\mathbf{b}_n + l_{n+1}\mathbf{b}_{n+1} + ... + l_{2n}\mathbf{b}_{2n}$$

και αποδείξαμε ότι $l_1 = ... = l_n = l_{n+1} = ... = l_{2n} = 0$, άτοπο αφού υποθέσαμε ότι το διάνυσμα $\mathbf{b}$ είναι μη μηδενικό. Άρα τελικά το μοναδικό στοιχείο το οποίο έχει και το αντίθετο του στην ημιομάδα $\mathbb{N}\mathbf{B}$ είναι το μηδενικό. □

Πρόταση 2.3.4. *Για το τορικό ιδεώδες του δεύτερου πίνακα Lawrence $A^{(2)}$, τα ακόλουθα σύνολα διωνύμων ταυτίζονται:*
1) Η βάση Graver του $I_{A^{(2)}}$.
2) Κάθε ανάγωγη βάση Gröbner.
3) Η καθολική βάση Gröbner του $I_{A^{(2)}}$.

4) Κάθε ελαχιστοτική βάση Markov.
5) Η καθολική βάση Markov.

Απόδειξη. Έστω S μια ελαχιστοτική βάση Markov του $I_{A^{(2)}}$, δηλαδή ένα ελαχιστοτικό σύνολο γεννητόρων του ιδεώδους $I_{A^{(2)}}$. Θα δείξουμε ότι η βάση Graver του $I_{A^{(2)}}$, είναι ίση με την S. Σύμφωνα με την πρόταση 2.2.22 , γνωρίζουμε ότι η ελαχιστοτική βάση Markov S είναι υποσύνολο της βάσης Graver του $I_{A^{(2)}}$. Για να δείξουμε την ισότητα, αρκεί να δείξουμε ότι η βάση Graver του $I_{A^{(2)}}$ είναι υποσύνολο της βάσης Markov S. Έστω όχι, θα καταλήξουμε σε άτοπο.
Αφού η βάση Graver του $I_{A^{(2)}}$ δεν είναι υποσύνολο της ελαχιστοτικής βάσης Markov S, υπάρχει ένα στοιχείο $g = x^{(1)^{u^+}} x^{(2)^{u^-}} - x^{(1)^{u^-}} x^{(2)^{u^+}}$ το οποίο ανήκει στη βάση Graver του $I_{A^{(2)}}$ το οποίο δεν ανήκει στην S. Έστω B το σύνολο όλων των διωνύμων $x^{(1)^{v^+}} x^{(2)^{v^-}} - x^{(1)^{v^-}} x^{(2)^{v^+}}$, που ανήκουν στη βάση Graver του $I_{A^{(2)}}$ εκτός του g. Υποθέτουμε ότι το σύνολο B γεννά το ιδεώδες $I_{A^{(2)}}$. Γνωρίζουμε ότι ένα διάνυσμα $\mathbf{u} \in \mathrm{Ker}_{\mathbf{Z}} A$ είναι πρωταρχικό αν και μόνο αν το αντίστοιχο διάνυσμα $(\mathbf{u}, -\mathbf{u}) \in \mathrm{Ker}_{\mathbf{Z}} A^{(2)}$ είναι πρωταρχικό από την πρόταση 2.3.2, αφού η βάση Graver είναι ίση με:

$$\mathrm{Gr}_{A^{(2)}} = \{x^{(1)^{u^+}} x^{(2)^{u^-}} - x^{(1)^{u^-}} x^{(2)^{u^+}} : \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} \in \mathrm{Gr}_A\}.$$

Έχουμε λοιπόν ότι το g ανήκει στο ιδεώδες $I_{A^{(2)}}$, αλλά δεν είναι γεννήτορας του. Άρα το g σύμφωνα με την πρόταση 2.2.14 που βρίσκεται στη μεταπτυχιακή διατριβή του Χ.Τατάκη [22] γράφεται ως γραμμικός συνδυασμός διωνύμων του B, με μονωνυμικούς συντελεστές. Δηλαδή

$g = x^{(1)^{u^+}} x^{(2)^{u^-}} - x^{(1)^{u^-}} x^{(2)^{u^+}} =$
$x^{(1)^{a_{11}}} x^{(2)^{a_{12}}} (x^{(1)^{v_1{}^+}} x^{(2)^{v_1{}^-}} - x^{(1)^{v_1{}^-}} x^{(2)^{v_1{}^+}}) + \ldots +$
$x^{(1)^{a_{n1}}} x^{(2)^{a_{n2}}} (x^{(1)^{v_n{}^+}} x^{(2)^{v_n{}^-}} - x^{(1)^{v_n{}^-}} x^{(2)^{v_n{}^+}})$.
Όπου $x^{(1)^{v_1{}^+}} x^{(2)^{v_1{}^-}} - x^{(1)^{v_1{}^-}} x^{(2)^{v_1{}^+}}, \ldots, x^{(1)^{v_n{}^+}} x^{(2)^{v_n{}^-}} - x^{(1)^{v_n{}^-}} x^{(2)^{v_n{}^+}} \in B$.
Κάποιος από τους όρους του διωνύμου $x^{(1)^{v_1{}^+}} x^{(2)^{v_1{}^-}} - x^{(1)^{v_1{}^-}} x^{(2)^{v_1{}^+}} \in B$, διαιρεί το $x^{(1)^{u^+}} x^{(2)^{u^-}}$. Έστω ο όρος $x^{(1)^{v_1{}^+}} x^{(2)^{v_1{}^-}}$.
Δηλαδή $x^{(1)^{u^+}} x^{(2)^{u^-}} = x^{(1)^{a_{11}}} x^{(2)^{a_{12}}} x^{(1)^{v_1{}^+}} x^{(2)^{v_1{}^-}} \Rightarrow x^{(1)^{v_1{}^+}} x^{(2)^{v_1{}^-}} \backslash x^{(1)^{u^+}} x^{(2)^{u^-}}$
συνεπώς $x^{(1)^{v_1{}^+}} \backslash x^{(1)^{u^+}}$ και $x^{(2)^{v_1{}^-}} \backslash x^{(2)^{u^-}}$, οπότε $\mathbf{u}^+ \geq \mathbf{v}_1{}^+$, $\mathbf{u}^- \geq \mathbf{v}_1{}^-$. Άρα από τη μερική διάταξη που ορίζεται από τη διαιρετότητα έχουμε $x^{\mathbf{v}_1{}^+} \backslash \mathbf{x}^{\mathbf{u}^+}$ και $x^{\mathbf{v}_1{}^-} \backslash \mathbf{x}^{\mathbf{u}^-}$. Άρα το διώνυμο $\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ δεν ανήκει στη βάση Graver κι άρα δεν είναι πρωταρχικό, άτοπο αφού εξ' υποθέσεως $g \in Gr_{A^{(2)}}$. Άρα η βάση Graver του $I_{A^{(2)}}$ είναι υποσύνολο της ελαχιστοτικής βάσης S. Άρα τελικά η βάση Graver του $I_{A^{(2)}}$ είναι ίση με την τυχαία ελαχιστοτική βάση Markov S, κατά συνέπεια είναι ίση με κάθε ελαχιστοτική βάση Markov. Συνεπώς η βάση Graver ισούται με την καθολική βάση Markov.
Μια ανάγωγη βάση Gröbner ως προς κάποια διάταξη όρων $\prec$, $G_\prec$ είναι σύνολο γεννητόρων του ιδεώδους, δηλαδή είναι μια βάση Markov. Άρα περιέχει μια ελαχιστοτική βάση Markov. Στην περίπτωση μας όμως, αποδείξαμε ότι κάθε ελαχιστοτική βάση Markov είναι ίση με τη βάση Graver του $I_{A^{(2)}}$. Άρα η βάση Graver περιέχεται στην ανάγωγη βάση Gröbner $G_\prec$, ως προς τη διάταξη όρων $\prec$, που περιέχεται στην καθολική βάση Gröbner, που περιέχεται στη βάση Graver. Άρα όλες ταυτίζονται. Τουτέστιν η βάση Graver του $I_{A^{(2)}}$ ισούται με την καθολική βάση Gröbner του $I_{A^{(2)}}$ ισούται με κάθε ανάγωγη βάση Gröbner του $I_{A^{(2)}}$ ισούται με κάθε βάση Markov του $I_{A^{(2)}}$ ισούται με την καθολική βάση Markov του $I_{A^{(2)}}$. □

Οι προτάσεις 2.3.4 και 2.3.2, μας δίνουν ένα τρόπο υπολογισμού μιας βάσης Graver του I_A. Αρχικά υπολογίζουμε μια ανάγωγη βάση Gröbner του $A^{(2)}$ η οποία σύμφωνα με την πρόταση 2.3.4 γνωρίζουμε πως είναι βάση Graver του $A^{(2)}$. Στη συνέχεια στην ανάγωγη βάση Gröbner αυτή, αντικαθιστούμε τα $y_1, ..., y_n$ με μονάδες, και το σύνολο πολυωνύμων που δημιουργείται είναι μια βάση Graver του I_A.

Αλγόριθμος 2.3.5. (Αλγόριθμος υπολογισμού βάσης Graver) Τα βήματα είναι τα εξής:

1. Επιλέγουμε οποιαδήποτε διάταξη όρων $\prec$ στον πολυωνυμικό δακτύλιο

$$K[x_1, ..., x_n, y_1, ..., y_n].$$

Υπολογίζουμε την ανάγωγη βάση Gröbner G του $I_{A^{(2)}}$ ως προς τη διάταξη όρων $\prec$.

2. Αντικαθιστούμε τα $y_1, ..., y_n \mapsto 1$ στα διώνυμα του συνόλου G. Το υποσύνολο του $K[x_1, ..., x_n]$ που προκύπτει, είναι η βάση Graver του I_A.

Παράδειγμα 2.3.6. Θεωρούμε το δακτύλιο $\mathbb{K}[x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4]$. Έστω το σύνολο διανυσμάτων $A = \{\mathbf{a}_1 = (4,0), \mathbf{a}_2 = (3,1), \mathbf{a}_3 = (2,2), \mathbf{a}_4 = (1,3), \mathbf{a}_5 = (0,4)\}$. Ο αντίστοιχος πίνακας A είναι ο ακόλουθος:

$$\mathcal{A} = \begin{pmatrix} 4 & 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

τότε ο πίνακας $A^{(2)}$ είναι ο ακόλουθος:

$$\mathcal{A}^{(2)} = \begin{pmatrix} 4 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Υπολογίζουμε την ανάγωγη βάση Gröbner του $I_{A^{(2)}}$ μέσω του υπολογιστικού προγράμματος $4ti2$ [21]. Η ανάγωγη βάση Gröbner του $I_{A^{(2)}}$ είναι η εξής:
$\{x_3x_5y_4^2 - x_4^2y_3y_5, x_2x_4y_3^2 - x_3^2y_2y_4, x_2x_5y_3y_4 - x_3x_4y_2y_5, x_2x_5^2y_4^3 - x_4^3y_2y_5^2,$
$x_2^2x_5y_3^3 - x_3^3y_2^2y_5, x_1x_4^2y_2^2y_5 - x_2^2x_5y_1y_4^2, x_1x_3y_2^2 - x_2^2y_1y_3, x_1x_4y_2y_3 - x_2x_3y_1y_4,$
$x_1x_5y_3y_4 - x_2x_4y_1y_5, x_1x_4^2y_3^3 - x_3^3y_1y_4^2, x_1x_5y_3^2 - x_3^2y_1y_5, x_1x_5^2y_3y_4^2 - x_3x_4^2y_1y_5^2,$
$x_1x_5^3y_4^4 - x_4^4y_1y_5^3, x_1^2x_4y_2^3 - x_2^3y_1^2y_4, x_1^2x_5y_2^2y_3 - x_2^2x_3y_1^2y_5, x_1^3x_5y_2^4 - x_2^4y_1^3y_5\}.$
Σύμφωνα με τον αλγόριθμο 2.3.5 αντικαθιστούμε τα y_1, y_2, y_3, y_4 με μονάδες και παίρνουμε τη βάση Graver του I_A. Άρα η βάση Graver του I_A είναι:
$A = \{x_3x_5 - x_4^2, x_2x_4 - x_3^2, x_2x_5 - x_3x_4, x_2x_5^2 - x_4^3, x_2^2x_5 - x_3^3, x_1x_4^2 - x_2^2x_5,$
$x_1x_3 - x_2^2, x_1x_4 - x_2x_3, x_1x_5 - x_2x_4, x_1x_4^2 - x_3^3, x_1x_5 - x_3^2, x_1x_5^2 - x_3x_4^2,$
$x_1x_5^3 - x_4^4, x_1^2x_4 - x_2^3, x_1^2x_5 - x_2^2x_3, x_1^3x_5 - x_2^4\}.$

Στη συνέχεια θα δούμε την έννοια των βάσεων Hilbert. Χρησιμοποιώντας τις βάσεις Hilbert, μπορούμε να δώσουμε έναν άλλο αλγόριθμο για τον υπολογισμό των βάσεων Gröbner.

Ορισμός 2.3.7. ***Ρητός πολυεδρικός κώνος*** C *καλείται το σύνολο*

$$C = pos_{\mathbf{Q}}(\mathbf{c}_1, ..., \mathbf{c}_s) = \{\sum l_i \mathbf{c}_i / l_i \in \mathbb{Q}_0^+\}.$$

Ορισμός 2.3.8. *Ένα σύνολο διανυσμάτων* $B = \{\mathbf{b}_1, ..., \mathbf{b}_t\} \subseteq \mathbb{Z}^n \subseteq \mathbb{Q}^n$ *λέγεται* ***βάση Hilbert*** *αν κάθε διάνυσμα* $\mathbf{b} \in \mathbb{Z}^n$ *και* $\mathbf{b} \in pos_{\mathbf{Q}}(B)$ *μπορεί να γραφεί στη μορφή* $\mathbf{b} = \sum n_i \mathbf{b}_i$, *με* $n_i \in \mathbb{Z}_0^+$.

Παρατήρηση 2.3.9. Η βάση Hilbert από τον τρόπο που ορίστηκε είναι πεπερασμένη.

Παράδειγμα 2.3.10. Έστω το σύνολο διανυσμάτων

$$B = \{\mathbf{b}_1 = (-1, 2), \mathbf{b}_2 = (2, 2)\},$$

αυτό δεν αποτελεί βάση Hilbert.
Πράγματι θεωρούμε το διάνυσμα $(1, 1) \in \mathbb{Z}^2 \subseteq \mathbb{Q}^2$ του κώνου $pos_{\mathbf{Q}}(B)$. Παρατηρούμε ότι δεν μπορεί να γραφεί ως γραμμικός συνδυασμός των διανυσμάτων $\mathbf{b}_1, \mathbf{b}_2$ με ακέραιους μη αρνητικούς συντελεστές. Αφού:

$$(1, 1) = 0(-1, 2) + \frac{1}{2}(2, 2).$$

Τα διανύσματα $\mathbf{b}_1, \mathbf{b}_2$ είναι γραμμικά ανεξάρτητα, άρα αποτελούν βάση του $\mathbb{Q}^2$. Άρα ο τρόπος γραφής του διανύσματος $(1, 1)$ ως γραμμικός συνδυασμός των διανυσμάτων $\mathbf{b}_1, \mathbf{b}_2$ είναι μοναδικός. Άρα το B δεν είναι βάση Hilbert.
Ωστόσο μπορούμε να βρούμε μια βάση Hilbert B', τέτοια ώστε ο κώνος $pos_{\mathbf{Q}}(B')$ να είναι ίσος με τον κώνο $pos_{\mathbf{Q}}(B)$. Η βάση

$$B' = \{\mathbf{b}'_1 = (-1, 2), \mathbf{b}'_2 = (0, 1), \mathbf{b}'_3 = (1, 1)\}$$

αποτελεί βάση Hilbert. Στη συνέχεια θα δούμε τον τρόπο με τον οποίο βρήκαμε τη βάση Hilbert B'.

Ορισμός 2.3.11. *Μια βάση Hilbert* B *καλείται* ***ελαχιστοτική βάση Hilbert****, αν δεν υπάρχει γνήσιο υποσύνολο του* B *που να παράγει τον ίδιο κώνο και να είναι βάση Hilbert.*

Παράδειγμα 2.3.12. Η βάση Hilbert

$$B' = \{\mathbf{b}'_1 = (-1, 2), \mathbf{b}'_2 = (0, 1), \mathbf{b}'_3 = (1, 1)\}$$

είναι ελαχιστοτική βάση Hilbert.
Πράγματι, το σύνολο $\{(-1, 2), (1, 1)\} \subset B'$ δεν αποτελεί βάση Hilbert, καθώς παρατηρούμε πως το διάνυσμα $(0, 1)$ του κώνου δεν μπορεί να γραφεί ως γραμμικός συνδυασμός των διανυσμάτων $\mathbf{b}_1, \mathbf{b}_2$ με ακέραιους μη αρνητικούς συντελεστές. Αφού:

$$(0, 1) = \frac{1}{3}(-1, 2) + \frac{1}{3}(1, 1)$$

και τα διανύσματα $(-1, 2), (1, 1)$ είναι βάση του $\mathbb{Q}^2$. Ενώ τα σύνολα $\{(-1, 2), (0, 1)\} \subset B'$, $\{(0, 1), (1, 1)\} \subset B'$ είναι βάσεις Hilbert, παράγουν όμως διαφορετικούς κώνους.

Ακολουθεί ένα παράδειγμα στο οποίο ο κώνος έχει άπειρες βάσεις Hilbert.

Παράδειγμα 2.3.13. Έστω ότι έχουμε την ευθεία $\mathbb{Q}$, τότε ο κώνος $pos_{\mathbb{Q}}(-1,1) = \mathbb{Q}$ και το σύνολο $\{-1,1\}$ είναι βάση Hilbert. Θα δείξουμε πως η εύθεία $\mathbb{Q}$, έχει άπειρες βάσεις Hilbert, και θα βρούμε κάποιες από αυτές.
Θεωρούμε $m,n \in \mathbb{N}$ με μκδ$(m,n) = 1$. Τότε το σύνολο $\{m,-n\}$ είναι βάση Hilbert της ευθείας $\mathbb{Q}$.
Θεωρούμε $m,n \in \mathbb{N}$, τότε έχουμε $1 = \kappa m + \lambda n$. Χωρίς βλάβη της γενικότητας θεωρούμε πως το $\kappa > 0$ και το $\lambda < 0$.
Ισχυριζόμαστε ότι το σύνολο $\{m,-n\}$ είναι ελαχιστοτική βάση Hilbert της ευθείας $\mathbb{Q}$.
Θεωρούμε ένα $l \in \mathbb{Z}$, διακρίνουμε περιπτώσεις.
1η περίπτωση
Αν $l \geq 0$, τότε από τη σχέση

$$1 = \kappa m + \lambda n$$

έχουμε

$$l = (l\kappa)m + (l(-\lambda))(-n),$$

όπου $l\kappa > 0$ και $l(-\lambda) > 0$, αφού $\lambda < 0$, άρα γράψαμε το l ως ακέραιο μη αρνητικό γραμμικό συνδυασμό των $m,-n$.
2η περίπτωση
Αν $l < 0$, τότε βλέπουμε τη σχέση $1 = \kappa m + \lambda n$ ως διοφαντική εξίσωση $1 = xm + yn$ κι αφού γνωρίζουμε τη λύση κ, λ, γνωρίζουμε άπειρες λύσεις της.
Έτσι έχουμε

$$1 = (\kappa + tn)m + (\lambda - tm)n \Rightarrow$$

$$l = l(\kappa + tn)m + l(\lambda - tm)n \Rightarrow$$

$$l = (l(\kappa + tn))m + (l(tm - \lambda))(-n).$$

Θέλουμε $l(\kappa + tn) \geq 0$, συνεπώς $\kappa + tn \leq 0$, άρα $t \leq \frac{-\kappa}{n}$.
Θέλουμε $l(lm - \lambda) \geq 0$, συνεπώς $lm - \lambda \leq 0$, άρα $t \leq \frac{\lambda}{m}$.
Οπότε για $t \leq min(\frac{-\kappa}{n}, \frac{\lambda}{m})$ και $t \in \mathbb{Z}$ έχουμε το ζητούμενο, δηλαδή καταφέραμε και γράψαμε το l ως ακέραιο μη αρνητικό γραμμικό συνδυασμό των $m,-n$. Ακόμη είναι $\mathbb{Z} \neq \mathbb{N}_0 m$ και $\mathbb{Z} \neq \mathbb{N}_0(-n)$ άρα το σύνολο $\{m,-n\}$ είναι ελαχιστική βάση Hilbert, συνεπώς υπάρχουν άπειρα ζεύγη $m,-n$ τα οποία αποτελούν ελαχιστικές βάσεις Hilbert της ευθείας $\mathbb{Q}$.

Ορισμός 2.3.14. *Ορίζουμε το* ***πολύτοπο*** P *ως το σύνολο*

$$P = \{l_1\mathbf{b}_1 + ... + l_s\mathbf{b}_s / 0 \leq l_i \leq 1, l_i \in \mathbb{Q}_0^+, 1 \leq i \leq s\}.$$

Ορισμός 2.3.15. ***Ο κώνος*** C ***έχει κορυφή*** *αν το μοναδικό διάνυσμα του κώνου που και το αντίθετο του ανήκει στον κώνο, είναι το μηδενικό.*

Θεώρημα 2.3.16. *Για κάθε ρητό πολυεδρικό κώνο C, υπάρχει τουλάχιστον μια βάση Hilbert. Αν ο κώνος C έχει κορυφή, τότε υπάρχει μοναδική ελαχιστοτική βάση Hilbert.*

Απόδειξη. Έστω $C = pos_{\mathbb{Q}}(\mathbf{c}_1, ..., \mathbf{c}_s)$ ένας ρητός πολυεδρικός κώνος, με $\mathbf{c}_i \in \mathbb{Q}^n$. Είναι $\mathbf{c}_i = (\frac{p_{i_1}}{q_{i_1}}, ..., \frac{p_{i_n}}{q_{i_n}})$, όπου $p_{i_j}, q_{i_j} \in \mathbb{Z}$, για $1 \leq i \leq s$, $1 \leq j \leq n$. Θεωρούμε τα διανύσματα $\mathbf{b}_i = \text{ΕΚΠ}(q_{i_1}, ..., q_{i_n}) \cdot \mathbf{c}_i$. Άρα τα $\mathbf{b}_i \in \mathbb{Z}^n$ και $C = pos_{\mathbb{Q}}(\mathbf{b}_1, ..., \mathbf{b}_s)$. Έστω $\mathbf{a}_1, ..., \mathbf{a}_t$ όλα τα μη μηδενικά διανύσματα με ακέραιες συντεταγμένες του πολυτόπου $P = \{l_1\mathbf{b}_1 + ... + l_s\mathbf{b}_s / 0 \leq l_i \leq 1, l_i \in \mathbb{Q}_0^+, 1 \leq i \leq$

$s\}$. Τα διανύσματα αυτά είναι πεπερασμένα, γιατί υπάρχουν πεπερασμένα σημεία με ακέραιες συντεταγμένες σε ένα πολύτοπο. Πράγματι, θεωρούμε το διάνυσμα $\mathbf{a}_j = (x_1, ..., x_i, ..., x_n)$ το οποίο είναι ένα εκ των διανυσμάτων $\mathbf{a}_1, ..., \mathbf{a}_t$, κι έχουμε

$$\begin{aligned} |\, x_i \,| &= |\, l_1 b_{1_i} + ... + l_s b_{s_i} \,| \\ &\leq |\, l_1 b_{1_i} \,| + ... + |\, l_s b_{s_i} \,| \\ &\leq |\, l_1 \,|\, |\, b_{1_i} \,| + ... + |\, l_s \,|\, |\, b_{s_i} \,| \\ &\leq |\, b_{1_i} \,| + ... + |\, b_{s_i} \,| = d_i. \end{aligned}$$

Έτσι το x_i παίρνει τιμές μεταξύ του d_i και του $-d_i$. Όμως στο διάστημα $-d_i \leq x_i \leq d_i$ υπάρχουν $2d_i + 1$ ακέραιες τιμές, συμπεριλαμβανομένου και του 0. Συνεπώς συνολικά υπάρχουν το πολύ $\prod_{i=1}^{n}(2d_i + 1)$ ακέραια σημεία στο πολύτοπο P. Παρατηρούμε ότι:

1. Έχουμε ότι $\{\mathbf{b}_1, ..., \mathbf{b}_s\} \subseteq \{\mathbf{a}_1, ..., \mathbf{a}_t\}$ εφόσον τα διανύσματα $\mathbf{b}_1, ..., \mathbf{b}_s \in \mathbb{Z}^n$ και $\mathbf{b}_i = 0\mathbf{b}_1 + ... + 1\mathbf{b}_i + ...0\mathbf{b}_s$, για $1 \leq i \leq s$.
   Άρα κάθε $\mathbf{b}_i$ ανήκει στο πολύτοπο P .

2. Έχουμε ότι $\{\mathbf{a}_1, ..., \mathbf{a}_t\} \subseteq pos_{\mathbf{Q}}(\mathbf{b}_1, ..., \mathbf{b}_s)$ εφόσον τα διανύσματα $\mathbf{a}_i$ γράφονται γραμμικοί συνδυασμοί των $\mathbf{b}_i$, με τους συντελεστές l_i να ανήκουν στο $\mathbb{Q}_0^+$, από τον ορισμό του πολυτόπου.

Από την πρώτη παρατήρηση συμπεραίνουμε πως $pos_{\mathbf{Q}}(\mathbf{b}_1, ..., \mathbf{b}_s) \subseteq pos_{\mathbf{Q}}(\mathbf{a}_1, ..., \mathbf{a}_t)$, ενώ από τη δεύτερη συμπεραίνουμε πως $pos_{\mathbf{Q}}(\mathbf{a}_1, ..., \mathbf{a}_t) \subseteq pos_{\mathbf{Q}}(\mathbf{b}_1, ..., \mathbf{b}_s)$. Συνεπώς έχουμε

$$pos_{\mathbf{Q}}(\mathbf{b}_1, ..., \mathbf{b}_s) = pos_{\mathbf{Q}}(\mathbf{a}_1, ..., \mathbf{a}_t).$$

Έστω ένα διάνυσμα $\mathbf{b} \in \mathbb{Z}^n$ και $\mathbf{b} \in pos_{\mathbf{Q}}(\mathbf{a}_1, ..., \mathbf{a}_t)$. Θα δείξουμε ότι το σύνολο διανυσμάτων $\{\mathbf{a}_1, ..., \mathbf{a}_t\}$ αποτελεί βάση Hilbert. Αρκεί να δείξουμε ότι το διάνυσμα $\mathbf{b}$ γράφεται ως γραμμικός συνδυασμός των διανυσμάτων της βάσης, με ακέραιες μη αρνητικές συντεταγμένες.
Έχουμε $\mathbf{b} \in pos_{\mathbf{Q}}(\mathbf{a}_1, ..., \mathbf{a}_t) = pos_{\mathbf{Q}}(\mathbf{b}_1, ..., \mathbf{b}_s)$, συνεπώς $\mathbf{b} = \sum l_i \mathbf{b}_i$ όπου $l_i \in \mathbb{Q}_0^+$. Δηλαδή
$\mathbf{b} = l_1\mathbf{b}_1 + ... + l_s\mathbf{b}_s =$
$\lfloor l_1 \rfloor \mathbf{b}_1 + (l_1 - \lfloor l_1 \rfloor)\mathbf{b}_1 + ... + \lfloor l_s \rfloor \mathbf{b}_s + (l_s - \lfloor l_s \rfloor)\mathbf{b}_s =$
$\lfloor l_1 \rfloor \mathbf{b}_1 + ... + \lfloor l_s \rfloor \mathbf{b}_s + (l_1 - \lfloor l_1 \rfloor)\mathbf{b}_1 + ... + (l_s - \lfloor l_s \rfloor)\mathbf{b}_s.$
Έχουμε $\mathbf{b} \in \mathbb{Z}^n$ και $\lfloor l_1 \rfloor \mathbf{b}_1 + ... + \lfloor l_s \rfloor \mathbf{b}_s \in \mathbb{Z}^n$ αφού πήραμε το ακέραιο μέρος των l_i, για $i = 1, ..., s$, συνεπώς $(l_1 - \lfloor l_1 \rfloor)\mathbf{b}_1 + ... + (l_s - \lfloor l_s \rfloor)\mathbf{b}_s \in \mathbb{Z}^n$.
Θέτουμε $\mathbf{b}' = (l_1 - \lfloor l_1 \rfloor)\mathbf{b}_1 + ... + (l_s - \lfloor l_s \rfloor)\mathbf{b}_s$ και παρατηρούμε ότι $0 \leq l_i - \lfloor l_i \rfloor \leq 1$, άρα το $\mathbf{b}'$ ανήκει στο πολύτοπο P, συνεπώς ισούται με κάποιο $\mathbf{a}_i$ για κάποιο από τα $i = 1, ..., t$. Οπότε έχουμε $\mathbf{b} = \lfloor l_1 \rfloor \mathbf{b}_1 + ... + \lfloor l_s \rfloor \mathbf{b}_s + \mathbf{a}_i$.
Παρατηρήσαμε όμως ότι $\{\mathbf{b}_1, ..., \mathbf{b}_s\} \subseteq \{\mathbf{a}_1, ..., \mathbf{a}_t\}$, άρα τελικά γράψαμε το διάνυσμα $\mathbf{b}$ γραμμικό συνδυασμό των διανυσμάτων $\mathbf{a}_1, ..., \mathbf{a}_t$ με ακέραιους μη αρνητικούς συντελεστές. Οπότε πράγματι το σύνολο $\{\mathbf{a}_1, ..., \mathbf{a}_t\}$ είναι βάση Hilbert.
Έστω ότι ο κώνος C έχει κορυφή, τότε από το βιβλίο του A.Schrijrer [17], γνωρίζουμε ότι υπάρχει ένα διάνυσμα $\mathbf{x} \in \mathbb{Q}^n$, τέτοιο ώστε το εσωτερικό γινόμενο να είναι θετικό, δηλαδή $\mathbf{x} \cdot \mathbf{y} > 0$ για κάθε μη μηδενικό $\mathbf{y}$ που ανήκει στον κώνο C.
Αποδείξαμε πως το σύνολο $\{\mathbf{a}_1, ..., \mathbf{a}_t\}$ είναι βάση Hilbert. Θεωρούμε το σύνολο $H \subseteq \{\mathbf{a}_1, ..., \mathbf{a}_t\}$ που αποτελείται από στοιχεία της βάσης Hilbert τα οποία δεν

μπορούν να γραφούν ως άθροισμα άλλων στοιχείων της βάσης. Το Η από τον τρόπο που ορίστηκε είναι μοναδικό επειδή ο κώνος C έχει κορυφή.
Ισχυριζόμαστε ότι κάθε $\mathbf{a}_i$, για $i = 1, ..., t$, είναι ακέραιος μη αρνητικός γραμμικός συνδυασμός των στοιχείων του συνόλου Η, δηλαδή ότι το Η είναι βάση Hilbert. Έστω όχι, θα καταλήξουμε σε άτοπο.
Εφόσον δεν ισχύει ο ισχυρισμός μας, συνεπάγεται πως υπάρχουν κάποια $\mathbf{a}_i$, τα οποία δεν γράφονται ως ακέραιος μη αρνητικός γραμμικός συνδυασμός των στοιχείων του συνόλου Η. Από αυτά διαλέγουμε ένα $\mathbf{a}_i$ τέτοιο ώστε το το εσωτερικό γινόμενο $\mathbf{x} \cdot \mathbf{a}_i$ να είναι το μικρότερο δυνατό. Το $\mathbf{a}_i$ δεν ανήκει στο σύνολο Η άρα μπορεί να γραφεί στη μορφή:

$$\mathbf{a_i} = \mathbf{a_{j_1}} + ... + \mathbf{a_{j_k}}.$$

Κάποιο διάνυσμα εκ των $\mathbf{a_{j_1}}, ..., \mathbf{a_{j_k}} \in \{\mathbf{a_1}, ..., \mathbf{a_t}\}$ μπορεί να επαναληφθεί περισσότερες φορές.
Είναι $\mathbf{x} \cdot \mathbf{a}_i = \mathbf{x} \cdot \mathbf{a}_{j_1} + ... + \mathbf{x} \cdot \mathbf{a}_{j_k} > 0$ και $\mathbf{x} \cdot \mathbf{a}_i > 0$ άρα $\mathbf{x} \cdot \mathbf{a}_i > \mathbf{x} \cdot \mathbf{a_{j_l}}$ για κάθε $1 \leq l \leq k$ και $k \geq 2$. Από τη σχέση $\mathbf{x} \cdot \mathbf{a}_i > \mathbf{x} \cdot \mathbf{a_{j_l}}$ και την υπόθεση μας, ότι το $\mathbf{x} \cdot \mathbf{a}_i$ να είναι το μικρότερο δυνατό εσωτερικό γινόμενο, συνεπάγεται πως τα διανύσματα $\mathbf{a_{j_l}}$, για κάθε $1 \leq l \leq k$, μπορούμε να τα γράψουμε σαν ακέραιο μη αρνητικό γραμμικό συνδυασμό στοιχείων του συνόλου Η. Κατά συνέπεια και το διάνυσμα $\mathbf{a_i} = \mathbf{a_{j_1}} + ... + \mathbf{a_{j_k}}$ μπορεί να γραφεί ως ακέραιος μη αρνητικός γραμμικός σύνδυασμός των στοιχείων του συνόλου H, άτοπο. Άρα το σύνολο Η είναι βάση Hilbert και μάλιστα ελαχιστική. Αν δεν ήταν ελαχιστική βάση Hilbert, τότε θα υπήρχε γνήσιο υποσύνολο της $\mathrm{H}' = \mathrm{H} - \{\mathbf{a_j}\}$ το οποίο θα ήταν βάση Hilbert. Δηλαδή θα υπήρχε ένα διάνυσμα $\mathbf{a_j}$ στο σύνολο Η το οποίο θα μπορούσαμε να το αφαιρέσουμε. Τότε όμως το $\mathbf{a_j}$ θα γραφόταν ως ακέραιος μη αρνητικός γραμμικός συνδυασμός στοιχείων του συνόλου H', αφού το H' υποθέσαμε ότι είναι βάση Hilbert. Αυτό όμως είναι άτοπο, εφόσον ορίσαμε το Η έτσι ώστε τα στοιχεία του να μην μπορούν να γραφούν ως άθροισμα άλλων στοιχείων της βάσης. Έτσι για τον κώνο C που υποθέσαμε ότι έχει κορυφή, βρήκαμε μοναδική ελαχιστοτική βάση Hilbert, κι αυτή είναι το σύνολο Η. □

Παράδειγμα 2.3.17. Επιστρέφουμε στο παράδειγμα 2.3.10.
Έχουμε τον κώνο $pos_{\mathbb{Q}}(B)$, όπου $B = \{\mathbf{b}_1 = (-1, 2), \mathbf{b_2} = (2, 2)\}$. Θα βρούμε μια βάση Hilbert για τον B. Θεωρούμε το πολύτοπο

$$P = \{l_1\mathbf{b}_1 + l_2\mathbf{b}_2 / 0 \leq l_i \leq 1, l_i \in \mathbb{Q}_0^+, 1 \leq i \leq 2\}.$$

Τα σημεία του πολυτόπου με ακέραιες συντεταγμένες αποδείξαμε ότι είναι πεπερασμένα, και είναι τα ακόλουθα:
$\mathbf{a}_1 = (-1, 2), \mathbf{a}_2 = (0, 1), \mathbf{a}_3 = (0, 2), \mathbf{a}_4 = (0, 3),$
$\mathbf{a}_5 = (1, 1), \mathbf{a}_6 = (1, 2), \mathbf{a}_7 = (1, 3), \mathbf{a}_8 = (1, 4), \mathbf{a}_9 = (2, 2).$
Σύμφωνα με το θεώρημα 2.3.16 έχουμε ότι το σύνολο $\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4, \mathbf{a}_5, \mathbf{a}_6, \mathbf{a}_7, \mathbf{a}_8, \mathbf{a}_9\}$ είναι μια βάση Hilbert του κώνου $pos_{\mathbb{Q}}(B)$, και παρατηρούμε πως ο κώνος B είναι κώνος με κορυφή άρα έχει μοναδική ελαχιστοτική βάση Hilbert Η, τα στοιχεία της οποίας δεν μπορούν να γραφούν ως άθροισμα άλλων στοιχείων της βάσης. Τα μοναδικά στοιχεία που πληρούν αυτή την ιδιότητα είναι $\mathbf{a}_1 = (-1, 2), \mathbf{a}_3 = (0, 1), \mathbf{a}_6 = (1, 1)$ δηλαδή η ελαχιστοτική βάση είναι η Hilbert $\mathrm{H} = \{\mathbf{a}_1 = (-1, 2), \mathbf{a}_3 = (0, 1), \mathbf{a}_6 = (1, 1)\}$. Καθώς τα υπόλοιπα στοιχεία γράφονται ως άθροισμα άλλων στοιχείων της βάσης. Για παράδειγμα το:

$$\mathbf{a}_7 = (1, 3) = \mathbf{a}_3 + \mathbf{a}_5,$$

όμοια και τα στοιχεία $\mathbf{a}_3 = (0,2), \mathbf{a}_4 = (0,3), \mathbf{a}_6 = (1,2), \mathbf{a}_8 = (1,4), \mathbf{a}_9 = (2,2)$.

Ορίζουμε $\sigma = (\sigma_{(1)}, ..., \sigma_{(n)}) \in \{+,-\}^n$ μια διάταξη προσήμων. Συμβολίζουμε με

$$\mathbb{Q}^n_\sigma = \mathbb{Q}_{\sigma_{(1)}} \times ... \times \mathbb{Q}_{\sigma_{(n)}}$$

όπου

$$\mathbb{Q}_+ = \{q \in Q / q \geq 0\}$$

$$\mathbb{Q}_- = \{q \in Q / q \leq 0\}$$

Θέτουμε $C_\sigma = KerA \bigcap \mathbb{Q}^n_\sigma$, τον κώνο αυτόν ο οποίος έχει κορυφή το $(0, ..., 0)$. Έστω H_σ η μοναδική ελαχιστοτική βάση Hilbert του κώνου C_σ. Το παρακάτω θεώρημα μας δίνει έναν ακόμη τρόπο υπολογισμού της βάσης Graver του A.

Θεώρημα 2.3.18. *Το σύνολο* $\{\mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-} / \mathbf{u} \in \bigcup H_\sigma - 0\}$, *είναι η βάση Graver του ιδεώδους* $I_\mathbf{A}$.

Απόδειξη. Έστω ένα μη μηδενικό διάνυσμα $\mathbf{u}$ ανήκει στην ένωση $\bigcup H_\sigma$, συνεπώς το $\mathbf{u}$ ανήκει στο H_σ για κάποιο σ. Υποθέτουμε ότι το διάνυσμα $\mathbf{u}$ δεν ανήκει στη βάση Graver του ιδεώδους $I_\mathbf{A}$, θα καταλήξουμε σε άτοπο. Εφόσον το διάνυσμα $\mathbf{u}$ δεν ανήκει στη βάση Graver του ιδεώδους $I_\mathbf{A}$, σύμφωνα με την πρόταση 2.2.15, γράφεται ως σύμμορφο άθροισμα:

$$\mathbf{u} = \mathbf{u}_1 +_c \mathbf{u}_2$$

με τα διανύσματα $\mathbf{u}_1, \mathbf{u}_2 \in KerA$ και $\mathbf{u}_1 \neq 0, \mathbf{u}_2 \neq 0$. Από το σύμμορφο άθροισμα συνεπάγεται ότι το $\mathbf{u}_1$ ανήκει στον κώνο C_σ και το $\mathbf{u}_2$ ανήκει στον κώνο C_σ. Άτοπο, αφού από το θεώρημα 2.3.16 η βάση Hilbert H έχει οριστεί έτσι ώστε τα στοιχεία της να μην γράφονται ως άθροισμα άλλων στοιχείων. Άρα το διάνυσμα $\mathbf{u}$ ανήκει στη βάση Graver του ιδεώδους I_A.
Αντίστροφα υποθέτουμε ότι το μη μηδενικό διάνυσμα $\mathbf{u}$ ανήκει στη βάση Graver του ιδεώδους I_A. Τότε υπάρχει ένα σ τέτοιο ώστε το $\mathbf{u}$ ανήκει στον κώνο C_σ. Συνεπώς το διάνυσμα $\mathbf{u}$ ανήκει στη βάση H_σ. Διαφορετικά, θα είχαμε

$$\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$$

με τα διανύσματα $\mathbf{u}_1, \mathbf{u}_2 \in KerA$ και $\mathbf{u}_1, \mathbf{u}_2$ ανήκουν στον κώνο C_σ. Άρα τα διανύσματα $\mathbf{u}_1, \mathbf{u}_2$ έχουν ομόσημες συντεταγμένες, δηλαδή το άθροισμα είναι σύμμορφο. Άτοπο σύμφωνα με την πρόταση 2.2.15. Άρα το διάνυσμα $\mathbf{u}$ ανήκει στη βάση $H_\sigma \subseteq \bigcup H_\sigma$. Δηλαδή το $\mathbf{u}$ ανήκει στην ένωση $\bigcup H_\sigma$.

□

Normaliz είναι ένας αλγόριθμος υπολογισμού των βάσεων Hilbert, κατασκευαστές του οποίου είναι οι W.Bruns, B.Ichim, Ch.Söger. Ο αλγόριθμος Normaliz χρησιμοποιεί το θεώρημα 2.3.18 για τον υπολογισμό των βάσεων Graver χρησιμοποιώντας τις βάσεις Hilbert. Ο αλγόριθμος αυτός χρησιμοποιείται και στην επίλυση διοφαντικών γραμμικών συστημάτων. Συστημάτων εξισώσεων ή και ανισώσεων των οποίων οι ακέραιες λύσεις μας ενδιαφέρουν μόνο.

Κεφάλαιο 3

Βάσεις Markov

Οι βάσεις Markov είναι πολύ χρήσιμες στην αλγεβρική στατιστική. Από τη σκοπιά της στατιστικής μπορούν να χρησιμοποιηθούν για να εκτιμήσουν πόσο καλά ταιριάζουν τα εμπειρικά δεδομένα σε ένα στατιστικό μοντέλο. Στην αλγεβρική γεωμετρία οι βάσεις Markov είναι ισοδύναμες με ένα σύνολο γεννητόρων κάποιου τορικού ιδεώδους. Αυτές οι ιδέες αναλύθηκαν για πρώτη φορά στο άρθρο [5] των P.Diakoŋis και B.Sturmfels το 1988.
Η αλγεβρική στατιστική χρησιμοποιεί την άλγεβρα για να κατανοήσει προβλήματα στατιστικής. Η άλγεβρα ήταν χρήσιμη για τον πειραματικό σχεδιασμό, την εκτίμηση παραμέτρων και τον έλεγχο υποθέσεων. Παραδοσιακά η αλγεβρική στατιστική έχει συνδεθεί με το σχεδιασμό πειραμάτων και την πολυπαραγοντική ανάλυση. Τα τελευταία χρόνια έχει περιοριστεί κάπως ο όρος αλγεβρική στατιστική και σημαίνει τη χρήση της αλγεβρικής γεωμετρίας και της μεταθετικής άλγεβρας στη στατιστική.

3.1 Βάση Markov

Έστω ένα σύνολο μη μηδενικών διανυσμάτων A.

Ορισμός 3.1.1. *Ένα πεπερασμένο υποσύνολο M του πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ λέγεται* ***βάση Markov*** *του A, αν για κάθε $\mathbf{t}, \mathbf{u} \in \mathbb{N}_0^n$ με $A\mathbf{t} = A\mathbf{u}$ υπάρχει μια ακολουθία $\{\mathbf{v}_i\}$ για $i = 1, ..., s$ από στοιχεία του M τέτοια ώστε το $\mathbf{t} + \sum_{i=1}^{\rho} \mathbf{v}_i \geq \mathbf{0}$ για κάθε $\rho = 1, ..., s$ και $\mathbf{t} + \sum_{i=1}^{s} \mathbf{v}_i = \mathbf{u}$. Ένα πεπερασμένο υποσύνολο M του πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ λέγεται* ***ελαχιστοτική βάση Markov*** *του A, αν δεν υπάρχει γνήσιο υποσύνολο του που να είναι βάση Markov του A.*

Ακολουθεί ένα πολύ σημαντικό θεώρημα των Diaconis και Sturmfels που βρίσκεται στο άρθρο [5] που δημοσιεύτηκε το 1998.

Θεώρημα 3.1.2. *Diaconis–Sturmfels*
Το πεπερασμένο υποσύνολο $M = \{\mathbf{u}_1, ..., \mathbf{u}_l\}$ του πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ είναι βάση Markov του A αν και μόνο αν το σύνολο $\{x^{\mathbf{u}_1^+} - x^{\mathbf{u}_1^-}, ..., x^{\mathbf{u}_l^+} - x^{\mathbf{u}_l^-}\}$ είναι σύνολο γεννητόρων του ιδεώδους I_A.

Απόδειξη. Έστω ότι το σύνολο $\{x^{\mathbf{u}_1^+} - x^{\mathbf{u}_1^-}, ..., x^{\mathbf{u}_l^+} - x^{\mathbf{u}_l^-}\}$ είναι σύνολο γεννητόρων του ιδεώδους I_A. Θα δείξουμε ότι το σύνολο $M = \{\mathbf{u}_1, ..., \mathbf{u}_l\}$ είναι βάση Markov του A. Έστω $\mathbf{t}, \mathbf{u} \in \mathbb{N}_0^n$ με $A\mathbf{t} = A\mathbf{u}$. Από τη σχέση $A\mathbf{t} = A\mathbf{u}$ συνεπάγεται πως το

$\mathbf{u}-\mathbf{t}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$, οπότε σύμφωνα με την παρατήρηση 2.1.10 το διώνυμο $x^{\mathbf{u}}-x^{\mathbf{t}}$ ανήκει στο ιδεώδες I_A. Συνεπώς σύμφωνα με την πρόταση 2.2.14 της μεταπτυχιακής διατριβής του Χ.Τατάκη [22] το διώνυμο $x^{\mathbf{u}}-x^{\mathbf{t}}$ γράφεται ως γραμμικός συνδυασμός διωνύμων του συνόλου γεννητόρων με μονωνυμικούς συντελεστές. Είναι:
$x^{\mathbf{u}}-x^{\mathbf{t}}=x^{\mathbf{a}_s}(x^{\mathbf{v}_s^+}-x^{\mathbf{v}_s^-})+x^{\mathbf{a}_{s-1}}(x^{\mathbf{v}_{s-1}^+}-x^{\mathbf{v}_{s-1}^-})+\ldots+x^{\mathbf{a}_1}(x^{\mathbf{v}_1^+}-x^{\mathbf{v}_1^-})$, με
$x^{\mathbf{u}}=x^{\mathbf{a}_s}x^{\mathbf{v}_s^+}, x^{\mathbf{a}_s}x^{\mathbf{v}_s^-}=x^{\mathbf{a}_{s-1}}x^{\mathbf{v}_{s-1}^+},\ldots,x^{\mathbf{a}_1}x^{\mathbf{v}_1^-}=x^{\mathbf{t}}$ και $\mathbf{a}_i\in\mathbb{N}_0^n$, με
$\{\mathbf{v}_1,\ldots,\mathbf{v}_s\}\subseteq\{\mathbf{u}_1,\ldots,\mathbf{u}_l\}$. Όπου $\{1,\ldots,s\}\subseteq\{1,\ldots,l\}$ οι δείκτες των διωνύμων που χρησιμοποιούνται για την περιγραφή του διωνύμου $x^{\mathbf{u}}-x^{\mathbf{t}}$. Άρα
$\mathbf{u}=\mathbf{a}_s+\mathbf{v}_s^+$
$\mathbf{a}_s+\mathbf{v}_s^-=\mathbf{a}_{s-1}+\mathbf{v}_{s-1}^+$
...
$\mathbf{a}_2+\mathbf{v}_2^-=\mathbf{a}_1+\mathbf{v}_1^+$
$\mathbf{a}_1+\mathbf{v}_1^-=\mathbf{t}$
προσθέτουμε κατά μέλη κι έχουμε:
$\mathbf{u}+\mathbf{a}_s+\mathbf{v}_s^-+\ldots+\mathbf{a}_2+\mathbf{v}_2^-+\mathbf{a}_1+\mathbf{v}_1^-=\mathbf{a}_s+\mathbf{v}_s^++\mathbf{a}_{s-1}+\mathbf{v}_{s-1}^++\ldots+\mathbf{a}_1+\mathbf{v}_1^++\mathbf{t}\Rightarrow$
$\mathbf{u}+\mathbf{v}_s^-+\ldots+\mathbf{v}_1^-=\mathbf{v}_s^++\mathbf{v}_{s-1}^++\ldots+\mathbf{v}_1^++\mathbf{t}\Rightarrow$
$$\mathbf{u}=\mathbf{t}+\mathbf{v}_s^+-\mathbf{v}_s^-+\ldots+\mathbf{v}_1^+-\mathbf{v}_1^-\Rightarrow\mathbf{u}=\mathbf{t}+\sum_{i=1}^{s}\mathbf{v}_i.$$
Θα δείξουμε ότι $\mathbf{t}+\mathbf{v}_1\geq\mathbf{0}$.
Είναι $\mathbf{t}+\mathbf{v}_1=\mathbf{t}+\mathbf{v}_1^+-\mathbf{v}_1-=\mathbf{v}_1^++\mathbf{t}-\mathbf{v}_1^-=\mathbf{v}_1^++\mathbf{a}_1\geq\mathbf{0}$, αφού $\mathbf{a}_1\in\mathbb{N}_0^n$.
Θα δείξουμε ότι $\mathbf{t}+\mathbf{v}_1+\mathbf{v}_2\geq\mathbf{0}$.
Είναι $\mathbf{t}+\mathbf{v}_1+\mathbf{v}_2=\mathbf{a}_1+\mathbf{v}_1^++\mathbf{v}_2^+-\mathbf{v}_2-=\mathbf{a}_2+\mathbf{v}_2^-+\mathbf{v}_2^+-\mathbf{v}_2^-=\mathbf{a}_2+\mathbf{v}_2^+\geq\mathbf{0}$, αφού $\mathbf{a}_2\in\mathbb{N}_0^n$.
Όμοια θα δείξουμε ότι $\mathbf{t}+\mathbf{v}_1+\mathbf{v}_2+\ldots+\mathbf{v}_\rho\geq\mathbf{0}$.
Είναι $\mathbf{t}+\mathbf{v}_1+\mathbf{v}_2+\ldots+\mathbf{v}_\rho=\mathbf{a}_\rho+\mathbf{v}_\rho^+\geq\mathbf{0}$, άρα $\mathbf{t}+\sum_{i=1}^{\rho}\mathbf{v}_i\geq\mathbf{0}$. Άρα για τα διανύσματα $\mathbf{t},\mathbf{u}\in\mathbb{N}_0^n$ με $A\mathbf{t}=A\mathbf{u}$, αποδείξαμε ότι υπάρχει μια ακολουθία $\{\mathbf{v}_i\}$ για $i=1,\ldots,s$ από στοιχεία του M τέτοια ώστε το $\mathbf{t}+\sum_{i=1}^{\rho}\mathbf{v}_i\geq\mathbf{0}$ για κάθε $\rho=1,\ldots,s$ και $\mathbf{t}+\sum_{i=1}^{s}\mathbf{v}_i=\mathbf{u}$. Συνεπώς το σύνολο $M=\{\mathbf{u}_1,\ldots,\mathbf{u}_l\}$ είναι βάση Markov του A.
Αντίστροφα έστω ότι το σύνολο $M=\{\mathbf{u}_1,\ldots,\mathbf{u}_l\}$ είναι βάση Markov του A. Θα δείξουμε ότι το σύνολο $\{x^{\mathbf{u}_1^+}-x^{\mathbf{u}_1^-},\ldots,x^{\mathbf{u}_l^+}-x^{\mathbf{u}_l^-}\}$ είναι σύνολο γεννητόρων του ιδεώδους I_A. Από τον ορισμό της βάσης Markov του A έχουμε ότι για κάθε $\mathbf{t},\mathbf{u}\in\mathbb{N}_0^n$ με $A\mathbf{t}=A\mathbf{u}$ υπάρχει μια ακολουθία $\{\mathbf{v}_i\}$ για $i=1,\ldots,s$ από στοιχεία του M τέτοια ώστε το $\mathbf{t}+\sum_{i=1}^{\rho}\mathbf{v}_i\geq0$ για κάθε $\rho=1,\ldots,s$ και $\mathbf{t}+\sum_{i=1}^{s}\mathbf{v}_i=\mathbf{u}$.
Θεωρούμε δύο τυχαία διανύσματα $\mathbf{t},\mathbf{u}$ με $A\mathbf{t}=A\mathbf{u}$ συνεπάγεται πως το $\mathbf{u}-\mathbf{t}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$, οπότε σύμφωνα με την παρατήρηση 2.1.10 το διώνυμο $x^{\mathbf{u}}-x^{\mathbf{t}}$ ανήκει στο ιδεώδες I_A.
Θέτουμε $\mathbf{a}_\rho=\mathbf{t}+\mathbf{v}_1+\ldots+\mathbf{v}_{\rho-1}-\mathbf{v}_\rho^-$ για $\rho>1$,
$\mathbf{a}_1=\mathbf{t}-\mathbf{v}_1^-$ για $\rho=1$. Είναι:
$x^{\mathbf{a}_1}(x^{\mathbf{v}_1^+}-x^{\mathbf{v}_1^-})+x^{\mathbf{a}_2}(x^{\mathbf{v}_2^+}-x^{\mathbf{v}_2^-})+\ldots+x^{\mathbf{a}_s}(x^{\mathbf{v}_s^+}-x^{\mathbf{v}_s^-})=$
$x^{\mathbf{t}-\mathbf{v}_1^-}(x^{\mathbf{v}_1^+}-x^{\mathbf{v}_1^-})+x^{\mathbf{t}+\mathbf{v}_1-\mathbf{v}_2^-}(x^{\mathbf{v}_2^+}-x^{\mathbf{v}_2^-})+\ldots+x^{\mathbf{t}+\mathbf{v}_1+\ldots+\mathbf{v}_{s-1}-\mathbf{v}_s^-}(x^{\mathbf{v}_s^+}-x^{\mathbf{v}_s^-})=$
$x^{\mathbf{t}+\mathbf{v}_1}-x^{\mathbf{t}}+x^{\mathbf{t}+\mathbf{v}_1+\mathbf{v}_2}-x^{\mathbf{t}+\mathbf{v}_1}+\ldots+x^{\mathbf{t}+\mathbf{v}_1+\ldots+\mathbf{v}_s}-x^{\mathbf{t}+\mathbf{v}_1+\ldots+\mathbf{v}_{s-1}}=$
$$x^{\mathbf{t}+\mathbf{v}_1+\ldots+\mathbf{v}_s}-x^{\mathbf{t}}=x^{\mathbf{t}+\sum_{i=1}^{s}\mathbf{v}_i}-x^{\mathbf{t}}=x^{\mathbf{u}}-x^{\mathbf{t}},$$
με $\{\mathbf{v}_1,\ldots,\mathbf{v}_s\}\subseteq\{\mathbf{u}_1,\ldots,\mathbf{u}_l\}$ και $\mathbf{t}-\mathbf{v}_1^-,\mathbf{t}+\mathbf{v}_1-\mathbf{v}_2^-,\ldots,\mathbf{t}+\mathbf{v}_1+\ldots+\mathbf{v}_{s-1}-\mathbf{v}_s^-\geq0$. Άρα το διώνυμο $x^{\mathbf{u}}-x^{\mathbf{t}}$ ανήκει

στο ιδεώδες $\langle x^{\mathbf{v}_1^+} - x^{\mathbf{v}_1^-}, ..., x^{\mathbf{v}_s^+} - x^{\mathbf{v}_s^-} \rangle$, όπου $\{\mathbf{v}_1, ..., \mathbf{v}_s\} \subseteq \{\mathbf{u}_1, ..., \mathbf{u}_l\}$. Δηλαδή το σύνολο $\{x^{\mathbf{u}_1^+} - x^{\mathbf{u}_1^-}, ..., x^{\mathbf{u}_l^+} - x^{\mathbf{u}_l^-}\}$ είναι σύνολο γεννητόρων του ιδεώδους $I_{\mathbf{A}}$. □

Εξαιτίας του θεωρήματος Diaconis–Sturmfels ακολουθεί ο ορισμός της βάσης Markov του ιδεώδους I_A, ο οποίος συνδέει ένα σύνολο γεννητόρων ενός ιδεώδους με τη βάση Markov του ιδεώδους. Για πρώτη φορά τον ορισμό αυτό τον είδαμε στο δεύτερο κεφάλαιο.

Ορισμός 3.1.3. *Ένα πεπερασμένο σύνολο γεννητόρων του ιδεώδους I_A καλείται* ***βάση Markov*** *του I_A. Ένα πεπερασμένο σύνολο γεννητόρων του ιδεώδους I_A ονομάζεται ελαχιστοτικό σύνολο γεννητόρων του ιδεώδους I_A ή* ***ελαχιστοτική βάση Markov*** *του ιδεώδους I_A αν δεν υπάρχει γνήσιο υποσύνολο του που να είναι βάση Markov του ιδεώδους I_A.*

Ορισμός 3.1.4. *Η ένωση των ελαχιστοτικών βάσεων Markov του ιδεώδους I_A καλείται καθολική βάση Markov του I_A.*

Ορισμός 3.1.5. *Το διάνυσμα του πυρήνα $\mathbf{a} \in \mathrm{Ker}_{\mathbb{Z}} A$, $\mathbf{a} = (a_1, ..., a_n)$ λέμε ότι είναι* ***ημισύμμορφο άθροισμα*** *(semiconformal sum) δύο μη μηδενικών διανυσμάτων του πυρήνα $\mathbf{b}, \mathbf{c} \in \mathrm{Ker}_{\mathbb{Z}} A$, δηλαδή $\mathbf{a} = \mathbf{b} +_{sc} \mathbf{c}$ αν και μόνο αν ισχύει $\mathbf{a} = \mathbf{b} + \mathbf{c}$ και αν ,*

$$b_i > 0 \Rightarrow a_i \geqslant b_i$$

ενώ αν

$$c_i < 0 \Rightarrow a_i \leqslant c_i$$

για κάθε $1 \leq i \leq n$.

Παρατήρηση 3.1.6. Από τον ορισμό προκύπτει πως αν $\mathbf{a} = \mathbf{b} +_{sc} \mathbf{c}$ τότε ισχύει $\mathbf{a}^+ \geqslant \mathbf{b}^+$ και $\mathbf{a}^- \geqslant \mathbf{c}^-$.
Πράγματι αν $b_i > 0 \Rightarrow b_i = b_i^+ \Rightarrow a_i \geqslant b_i^+ > 0 \Rightarrow a_i > 0 \Rightarrow a_i = a_i^+ \Rightarrow a_i^+ \geqslant b_i^+$, για κάθε $i = 1, ..., n$. Άρα $\mathbf{a}^+ \geqslant \mathbf{b}^+$.
Επιπλέον αν $c_i < 0 \Rightarrow c_i = -c_i^- \Rightarrow a_i \leqslant c_i < 0 \Rightarrow a_i < 0 \Rightarrow a_i = -a_i^- \Rightarrow -a_i^- \leqslant -c_i^- \Rightarrow a_i^- \geqslant c_i^-$, για κάθε $i = 1, ..., n$. Άρα $\mathbf{a}^- \geqslant \mathbf{c}^-$.

Παρατήρηση 3.1.7. Στο σύμμορφο άθροισμα ισχύει η μεταθετική ιδιότητα. Δηλαδή:

$$\mathbf{a} = \mathbf{b} +_c \mathbf{c} = \mathbf{c} +_c \mathbf{b}.$$

Στο ημισύμμορφο άθροισμα δεν ισχύει. Αν το $\mathbf{a}$ είναι το ημισύμμορφο άθροισμα $\mathbf{b} +_{sc} \mathbf{c}$, τότε συνήθως το άθροισμα $\mathbf{c} + \mathbf{b}$ δεν είναι ημισύμμορφο.

Θεώρημα 3.1.8. *Τα αθροίσματα $\mathbf{b} + \mathbf{c}$ και $\mathbf{c} + \mathbf{b}$ είναι ημισύμμορφα αθροίσματα αν και μόνο αν το άθροισμα $\mathbf{b} + \mathbf{c}$ είναι σύμμορφο άθροισμα.*

Απόδειξη. Έστω ότι $\mathbf{a} = \mathbf{b} +_{sc} \mathbf{c}$ και $\mathbf{a} = \mathbf{c} +_{sc} \mathbf{b}$. Τότε από το πρώτο ημισύμμορφο άθροισμα έχουμε ότι $\mathbf{a}^+ \geqslant \mathbf{b}^+$ και $\mathbf{a}^- \geqslant \mathbf{c}^-$ κι από το δεύτερο έχουμε ότι $\mathbf{a}^+ \geqslant \mathbf{c}^+$ και $\mathbf{a}^- \geqslant \mathbf{b}^-$.
Έστω η i–συντεταγμένη του $\mathbf{b}$ είναι μη αρνητική, δηλαδή $b_i \geqslant 0$ συνεπώς $0 \leqslant b_i = b_i^+$. Άρα από τη σχέση $\mathbf{a}^+ \geqslant \mathbf{b}^+$ έχουμε $a_i^+ \geqslant b_i^+ \geqslant 0 \Rightarrow a_i^+ \geqslant 0 \Rightarrow a_i = a_i^+ \Rightarrow a_i \geqslant b_i \geqslant 0$. Άρα από τη σχέση $a_i = b_i + c_i \geqslant b_i$ συνεπάγεται $b_i + c_i \geqslant b_i \Rightarrow c_i \geqslant 0 \Rightarrow c_i = c_i^+$. Άρα είναι $a_i = a_i^+, b_i = b_i^+, c_i = c_i^+$ κι από $a_i = b_i + c_i$ συνεπάγεται πως $a_i^+ = b_i^+ + c_i^+$ για κάθε $i = 1, ..., n$, δηλαδή

$\mathbf{a}^+ = \mathbf{b}^+ + \mathbf{c}^+$.
Έστω η $i-$συντεταγμένη του $\mathbf{b}$ είναι αρνητική, δηλαδή $b_i < 0$ συνεπώς $0 > b_i = -b_i^- \Rightarrow b_i^- > 0$. Άρα από τη σχέση $\mathbf{a}^- \geqslant \mathbf{b}^-$ έχουμε $a_i^- \geqslant b_i^- > 0 \Rightarrow a_i^- > 0 \Rightarrow -a_i^- < 0 \Rightarrow 0 > a_i = -a_i^- \Rightarrow a_i^- \geqslant b_i^-$. Άρα από τη σχέση $a_i^- \geqslant b_i^-$ συνεπάγεται $-a_i^- \leqslant -b_i^- \Rightarrow a_i \leqslant b_i \Rightarrow a_i = b_i + c_i \leqslant b_i \Rightarrow c_i \leqslant 0 \Rightarrow c_i = -c_i^-$. Άρα είναι $a_i = -a_i^-, b_i = -b_i^-, c_i = -c_i^-$ κι από $a_i = b_i + c_i$ συνεπάγεται πως $-a_i^- = -b_i^- + (-c_i^-) \Rightarrow -a_i^- = -b_i^- - c_i^- \Rightarrow a_i^- = b_i^- + c_i^-$ για κάθε $i = 1, ..., n$, δηλαδή $\mathbf{a}^- = \mathbf{b}^- + \mathbf{c}^-$. Συνεπώς έχουμε $\mathbf{a}^+ = \mathbf{b}^+ + \mathbf{c}^+$ και $\mathbf{a}^- = \mathbf{b}^- + \mathbf{c}^-$. Δηλαδή το άθροισμα $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$ είναι σύμμορφο.
Αντίστροφα έστω ότι το άθροισμα $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$ είναι σύμμορφο. Θα δείξουμε ότι τα αθροίσματα $\mathbf{b} + \mathbf{c}$ και $\mathbf{c} + \mathbf{b}$ είναι ημισύμμορφα. Από το σύμμορφο άθροισμα έχουμε ότι $\mathbf{a}^+ = \mathbf{b}^+ + \mathbf{c}^+$ και $\mathbf{a}^- = \mathbf{b}^- + \mathbf{c}^-$. Συνεπώς $\mathbf{a}^+ \geqslant \mathbf{b}^+$ και $\mathbf{a}^- \geqslant \mathbf{c}^-$, ομοίως $\mathbf{a}^+ \geqslant \mathbf{c}^+$ και $\mathbf{a}^- \geqslant \mathbf{b}^-$. Οπότε τα αθροίσματα $\mathbf{b} + \mathbf{c}$ και $\mathbf{c} + \mathbf{b}$ είναι ημισύμμορφα δηλαδή $\mathbf{a} = \mathbf{b} +_{sc} \mathbf{c}$ και $\mathbf{a} = \mathbf{c} +_{sc} \mathbf{b}$.

□

Παρατήρηση 3.1.9. Αν έχουμε $\mathbf{a} = \mathbf{b} +_{sc} \mathbf{c}$ τότε ισχύει $(-\mathbf{a}) = (-\mathbf{c}) +_{sc} (-\mathbf{b})$.

Απόδειξη. Έχουμε $\mathbf{a} = \mathbf{b} +_{sc} \mathbf{c}$ συνεπώς $\mathbf{a}^+ \geqslant \mathbf{b}^+$ και $\mathbf{a}^- \geqslant \mathbf{c}^-$.
Όμως παρατηρούμε ότι $\mathbf{a}^- = (-\mathbf{a})^+$ και $\mathbf{a}^+ = (-\mathbf{a})^-$. Άρα είναι $(-\mathbf{a})^- \geqslant (-\mathbf{b})^-$ και $(-\mathbf{a})^+ \geqslant (-\mathbf{c})^+$, συνεπώς $(-\mathbf{a}) = (-\mathbf{c}) +_{sc} (-\mathbf{b})$. □

Ορισμός 3.1.10. *Το διάνυσμα του πυρήνα* $\mathbf{a} \in \mathrm{Ker}_{\mathbb{Z}} A$, $\mathbf{a} = (a_1, ..., a_n)$ *λέμε ότι είναι* ***ισχυρά ημισύμμορφο άθροισμα*** *(strongly semiconformal sum) δύο μη μηδενικών διανυσμάτων του πυρήνα* $\mathbf{b}, \mathbf{c} \in \mathrm{Ker}_{\mathbb{Z}} A$ *δηλαδή* $\mathbf{a} = \mathbf{b} +_{ssc} \mathbf{c}$, *αν και μόνο αν* $\mathbf{a} = \mathbf{b} + \mathbf{c}$ *και αν*

$$b_i > 0 \Rightarrow a_i > b_i$$

ενώ αν

$$c_i < 0 \Rightarrow a_i < c_i.$$

Παρατήρηση 3.1.11. Από τον ορισμό προκύπτει πως ισχύει $\mathbf{a}^+ > \mathbf{b}^+$ και $\mathbf{a}^- > \mathbf{c}^-$. Πράγματι αν είναι $b_i > 0 \Rightarrow b_i = b_i^+ \Rightarrow a_i > b_i > 0 \Rightarrow a_i > 0 \Rightarrow a_i = a_i^+ \Rightarrow a_i^+ > b_i^+$ για κάθε $i = 1, ..., n$. Άρα $\mathbf{a}^+ > \mathbf{b}^+$.
Επιπλέον αν είναι $c_i < 0 \Rightarrow c_i = -c_i^- \Rightarrow a_i < c_i < 0 \Rightarrow a_i < 0 \Rightarrow a_i = -a_i^- \Rightarrow -a_i^- < -c_i^- \Rightarrow a_i^- > c_i^-$ για κάθε $i = 1, ..., n$. Άρα $\mathbf{a}^- > \mathbf{c}^-$.

Θεώρημα 3.1.12. *Αν είναι* $\mathbf{a} = \mathbf{b} +_{ssc} \mathbf{c}$ *τότε το διώνυμο* $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$ *δεν ανήκει στην καθολική βάση Markov του* $I_{\mathbf{A}}$, *όπου* $\mathbf{a}, \mathbf{b}, \mathbf{c}$ *ανήκουν στον πυρήνα* $\mathrm{Ker}_{\mathbb{Z}} A$.

Απόδειξη. Έστω ότι είναι $\mathbf{a} = \mathbf{b} +_{ssc} \mathbf{c}$, όπου $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathrm{Ker}_{\mathbb{Z}} A$. Υποθέτουμε ότι το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$ ανήκει στην καθολική βάση Markov, θα καταλήξουμε σε άτοπο. Εφόσον το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$ ανήκει στην καθολική βάση Markov, που είναι η ένωση όλων των ελαχιστοτικών βάσεων Markov, υπάρχει μια ελαχιστοτική βάση Markov στην οποία ανήκει. Έστω $\langle x^{\mathbf{a}^+} - x^{\mathbf{a}^-}, B_2, ..., B_t \rangle$ η ελαχιστοτική βάση Markov στην οποία ανήκει το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}}$. Τότε για το $\mathbf{a}$ έχουμε $\mathbf{a} = \mathbf{b} +_{ssc} \mathbf{c}$. Συνεπώς $x^{\mathbf{a}^+} - x^{\mathbf{a}^-} = x^{\mathbf{a}^+ - \mathbf{b}^+}(x^{\mathbf{b}^+} - x^{\mathbf{b}^-}) + x^{\mathbf{a}^+ - \mathbf{b}^+ + \mathbf{b}^-} - x^{\mathbf{a}^-}$.
Όμως από τη σχέση $\mathbf{a} = \mathbf{b} + \mathbf{c}$ συνεπάγεται ότι $\mathbf{a}^+ - \mathbf{a}^- = \mathbf{b}^+ - \mathbf{b}^- + \mathbf{c}^+ - \mathbf{c}^- \Rightarrow \mathbf{a}^+ - \mathbf{b}^+ + \mathbf{b}^- = \mathbf{a}^- + \mathbf{c}^+ - \mathbf{c}^-$. Άρα $x^{\mathbf{a}^+} - x^{\mathbf{a}^-} = x^{\mathbf{a}^+ - \mathbf{b}^+}(x^{\mathbf{b}^+} - x^{\mathbf{b}^-}) + x^{\mathbf{a}^+ + \mathbf{c}^+ - \mathbf{c}^-} - x^{\mathbf{a}^-} = x^{\mathbf{a}^+ - \mathbf{b}^+}(x^{\mathbf{b}^+} - x^{\mathbf{b}^-}) + x^{\mathbf{a}^- - \mathbf{c}^-}(x^{\mathbf{c}^+} - x^{\mathbf{c}^-})$. Το διάνυσμα $\mathbf{b}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ οπότε σύμφωνα με την παρατήρηση 2.1.10 το διώνυμο $x^{\mathbf{b}^+} - x^{\mathbf{b}^-}$ ανήκει στο ιδεώδες I_A, συνεπώς σύμφωνα με την πρόταση 2.2.14 της

μεταπτυχιακής διατριβής του Χ.Τατάκη [22] γράφεται ως γραμμικός συνδυασμός διωνύμων της βάσης Markov με μονωνυμικούς συντελεστές. Δηλαδή

$$x^{\mathbf{b}^+} - x^{\mathbf{b}^-} = x^{\mathbf{u}_1} B_{i_1} + ... + x^{\mathbf{u}_t} B_{i_t},$$

όπου $\{i_1, ..., i_t\}$ οι δείκτες των διωνύμων που χρησιμοποιούνται για την περιγραφή του διωνύμου $x^{\mathbf{b}^+} - x^{\mathbf{b}^-}$. Άρα έχουμε:
$deg_{\mathbf{A}}(x^{\mathbf{b}^+} - x^{\mathbf{b}^-}) \geqslant deg_{\mathbf{A}}(B_{i_k})$, για κάθε $k = 1, ..., t$. Συνεπώς το διώνυμο $x^{\mathbf{b}^+} - x^{\mathbf{b}^-}$ ανήκει στο σύνολο $\langle B_2, ..., B_t \rangle$. Από τα διώνυμα που χρησιμοποιούνται για την περιγραφή του διωνύμου $x^{\mathbf{b}^+} - x^{\mathbf{b}^-}$, απουσιάζει το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$. Πράγματι αφού $\mathbf{a} = \mathbf{b} +_{ssc} \mathbf{c}$ συνεπάγεται πως $\mathbf{a}^+ > \mathbf{b}^+$, δηλαδή έχουμε ότι $x^{\mathbf{b}^+} \backslash x^{\mathbf{a}^+}$. Άρα $deg_{\mathbf{A}}(x^{\mathbf{a}^+}) > deg_{\mathbf{A}}(x^{\mathbf{b}^+})$. Οπότε $deg_{\mathbf{A}}(x^{\mathbf{a}^+} - x^{\mathbf{a}^-}) = deg_{\mathbf{A}}(x^{\mathbf{a}^+}) > deg_{\mathbf{A}}(x^{\mathbf{b}^+}) = deg_{\mathbf{A}}(x^{\mathbf{b}^+} - x^{\mathbf{b}^-})$.
Το διάνυσμα $\mathbf{c}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ οπότε σύμφωνα με την παρατήρηση 2.1.10 το διώνυμο $x^{\mathbf{c}^+} - x^{\mathbf{c}^-}$ ανήκει στο ιδεώδες I_A συνεπώς γράφεται ως γραμμικός συνδυασμός διωνύμων της βάσης Markov με μονωνυμικούς συντελεστές. Δηλαδή

$$x^{\mathbf{c}^+} - x^{\mathbf{c}^-} = x^{\mathbf{u}_1} B_{j_1} + ... + x^{\mathbf{u}_t} B_{j_m},$$

όπου $\{j_1, ..., j_m\}$ οι δείκτες των διωνύμων που χρησιμοποιούνται για την περιγραφή του διωνύμου $x^{\mathbf{c}^+} - x^{\mathbf{c}^-}$. Άρα έχουμε:
$deg_{\mathbf{A}}(x^{\mathbf{c}^+} - x^{\mathbf{c}^-}) \geqslant deg_{\mathbf{A}}(B_{j_l})$, για κάθε $l = 1, ..., m$. Συνεπώς το διώνυμο $x^{\mathbf{c}^+} - x^{\mathbf{c}^-}$ ανήκει στο σύνολο $\langle B_2, ..., B_t \rangle$. Από τα διώνυμα που χρησιμοποιούνται για την περιγραφή του διωνύμου $x^{\mathbf{c}^+} - x^{\mathbf{c}^-}$, απουσιάζει το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$. Πράγματι αφού $\mathbf{a} = \mathbf{b} +_{ssc} \mathbf{c}$ συνεπάγεται πως $\mathbf{a}^- > \mathbf{c}^-$, δηλαδή έχουμε ότι $x^{\mathbf{a}^-} \setminus x^{\mathbf{c}^-}$. Άρα $deg_{\mathbf{A}}(x^{\mathbf{a}^-}) > deg_{\mathbf{A}}(x^{\mathbf{c}^-})$. Δηλαδή $deg_{\mathbf{A}}(x^{\mathbf{a}^+} - x^{\mathbf{a}^-}) = deg_{\mathbf{A}}(x^{\mathbf{a}^-}) > deg_{\mathbf{A}}(x^{\mathbf{c}^-}) = deg_{\mathbf{A}}(x^{\mathbf{c}^+} - x^{\mathbf{c}^-})$.
Αποδείξαμε δηλαδή ότι τα διώνυμα $x^{\mathbf{b}^+} - x^{\mathbf{b}^-}, x^{\mathbf{c}^+} - x^{\mathbf{c}^-}$ ανήκουν στο σύνολο $\langle B_2, ..., B_t \rangle$. Όμως έχουμε ότι:

$$x^{\mathbf{a}^+} - x^{\mathbf{a}^-} = x^{\mathbf{a}^+ - \mathbf{b}^+}(x^{\mathbf{b}^+} - x^{\mathbf{b}^-}) + x^{\mathbf{a}^- - \mathbf{c}^-}(x^{\mathbf{c}^+} - x^{\mathbf{c}^-}).$$

Άρα και το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$ ανήκει στο σύνολο $\langle B_2, ..., B_t \rangle$. Δηλαδή είναι:

$$\langle x^{\mathbf{a}^+} - x^{\mathbf{a}^-}, B_2, ..., B_t \rangle \subseteq \langle B_2, ..., B_t \rangle.$$

Η άλλη κατεύθυνση είναι προφανής, δηλαδή $\langle B_2, ..., B_t \rangle \subseteq \langle x^{\mathbf{a}^+} - x^{\mathbf{a}^-}, B_2, ..., B_t \rangle$. Οπότε δείξαμε ότι το ιδεώδες $\langle x^{\mathbf{a}^+} - x^{\mathbf{a}^-}, B_2, ..., B_t \rangle$ είναι ίσο με το ιδεώδες $\langle B_2, ..., B_t \rangle$. Όμως το σύνολο $\{B_2, ..., B_t\}$ είναι σύνολο γεννητόρων γνήσιο υποσύνολο του ελαχιστοτικού, δηλαδή του συνόλου $\{x^{\mathbf{a}^+} - x^{\mathbf{a}^-}, B_2, ..., B_t\}$, άτοπο. Συνεπώς το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$ δεν ανήκει στην καθολική βάση Markov του $I_{\mathbf{A}}$. □

Ορισμός 3.1.13. *Έστω $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ τότε ορίζουμε ως $B^\sigma = \{\mathbf{b}_1^\sigma, ..., \mathbf{b}_s^\sigma\}$ όπου $\mathbf{b}_i^\sigma = \mathbf{b}_i$ όταν το i ανήκει στο σ ή $\mathbf{b}_i^\sigma = -\mathbf{b}_i$ όταν το i δεν ανήκει στο σ, με $\sigma \subseteq \{1, ..., s\}$.*

Παρατήρηση 3.1.14. Υπάρχουν 2^s διαφορετικά υποσύνολα σ.

Θεώρημα 3.1.15. *Έστω $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$. Τότε το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ ανήκει στη βάση Graver του I_B αν και μόνο αν το διώνυμο $x^{\mathbf{u}^{\sigma +}} - x^{\mathbf{u}^{\sigma -}}$ ανήκει στη βάση Graver του I_{B^σ}, όπου $u_i^\sigma = u_i$ όταν το i ανήκει στο σ ή $u_i^\sigma = -u_i$ όταν το i δεν ανήκει στο σ, με $\sigma \subseteq \{1, ..., s\}$.*

Απόδειξη. Έστω το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ ανήκει στη βάση Graver του I_B. Σύμφωνα με την πρόταση 2.2.15 το διάνυσμα $\mathbf{u} = (u_1, ..., u_s) \neq \mathbf{0}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$ και το u δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$. Θα δείξουμε ότι το διώνυμο $x^{\mathbf{u}^{\sigma +}} - x^{\mathbf{u}^{\sigma -}}$ ανήκει στη βάση Graver του I_{B^σ}. Εφόσον το διάνυσμα $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$ συνεπάγεται πως $u_1\mathbf{b}_1 + ... + u_s\mathbf{b}_s = \mathbf{0}$. Διακρίνουμε περιπτώσεις:
1η περίπτωση

Το i ανήκει στο $\sigma \Rightarrow u_i = u_i^\sigma, \mathbf{b}_i = \mathbf{b}_i{}^\sigma \Rightarrow u_i\mathbf{b}_i = u_i^\sigma \mathbf{b}_i^\sigma$.

2η περίπτωση

Το i δεν ανήκει στο $\sigma \Rightarrow u_i = -u_i^\sigma, \mathbf{b}_i = -\mathbf{b}_i^\sigma \Rightarrow u_i\mathbf{b}_i = (-u_i^\sigma)(-\mathbf{b}_i^\sigma) = u_i^\sigma \mathbf{b}_i^\sigma$.

Και στις δύο περιπτώσεις ισχύει $u_i\mathbf{b}_i = u_i^\sigma \mathbf{b}_i^\sigma$.
Οπότε η σχέση $u_1\mathbf{b}_1 + ... + u_s\mathbf{b}_s = \mathbf{0}$ συνεπάγεται ότι $u_1^\sigma \mathbf{b}_1^\sigma + ... + u_s^\sigma \mathbf{b}_s^\sigma = \mathbf{0}$.
Δηλαδή το διάνυσμα $\mathbf{u}^\sigma = (u_1^\sigma, ..., u_s^\sigma)$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$.
Επιπλέον αφού το u δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$ συνεπάγεται πως και το $\mathbf{u}^\sigma$ δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$.
Έστω όχι, θα καταλήξουμε σε άτοπο. Είναι $\mathbf{u}^\sigma = \mathbf{a}^\sigma +_c \mathbf{b}^\sigma$ με $\mathbf{a}^\sigma, \mathbf{b}^\sigma \in \mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$.
Δηλαδή $\mathbf{u}^\sigma = \mathbf{a}^\sigma + \mathbf{b}^\sigma$ και $\mid u^\sigma{}_i \mid = \mid a_i^\sigma \mid + \mid b_i^\sigma \mid$ με $u_i^\sigma = a_i^\sigma + b_i^\sigma$.
Αν το i ανήκει στο σ συνεπάγεται πως $u_i^\sigma = u_i \Rightarrow \mid u_i^\sigma \mid = \mid a_i^\sigma \mid + \mid b_i^\sigma \mid \Leftrightarrow$
$\mid u_i \mid = \mid a_i \mid + \mid b_i \mid$, και $\mathbf{u} = \mathbf{a} + \mathbf{b}$ με $\mathbf{a}, \mathbf{b} \in \mathrm{Ker}_{\mathbf{Z}} B$ άρα $\mathbf{u} = \mathbf{a} +_c \mathbf{b}$ άτοπο.
Αν το i δεν ανήκει στο σ συνεπάγεται πως $u_i^\sigma = -u_i \Rightarrow \mid u_i^\sigma \mid = \mid a_i^\sigma \mid +$
$\mid b_i^\sigma \mid \Leftrightarrow \mid -u_i \mid = \mid -a_i \mid + \mid -b_i \mid \Rightarrow \mid u_i \mid = \mid a_i \mid + \mid b_i \mid$, και $\mathbf{u} = \mathbf{a} + \mathbf{b}$ με $\mathbf{a}, \mathbf{b} \in \mathrm{Ker}_{\mathbf{Z}} B$ άρα $\mathbf{u} = \mathbf{a} +_c \mathbf{b}$ άτοπο. Άρα $\mathbf{u}^\sigma \neq \mathbf{a}^\sigma +_c \mathbf{b}^\sigma$ με $\mathbf{a}^\sigma, \mathbf{b}^\sigma \in \mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$.
Συνεπώς έχουμε ότι το μη μηδενικό διάνυσμα $\mathbf{u}^\sigma$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$ και δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$, συνεπώς το $\mathbf{u}^\sigma$ ανήκει στη βάση Graver του I_{B^σ}.

Αντίστροφα υποθέτουμε ότι το διώνυμο $x^{\mathbf{u}^{\sigma +}} - x^{\mathbf{u}^\sigma}$ ανήκει στη βάση Graver του I_{B^σ} θα δείξουμε ότι το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ ανήκει στη βάση Graver του I_B.
Σύμφωνα με την πρόταση 2.2.15 το διάνυσμα $\mathbf{u}^\sigma = (u_1^\sigma, ..., u_s^\sigma) \neq \mathbf{0}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$ και δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$. Εφόσον το διάνυσμα $\mathbf{u}^\sigma$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}(B^\sigma)$ συνεπάγεται πως $u_1^\sigma \mathbf{b}_1^\sigma + ... + u_s^\sigma \mathbf{b}_s^\sigma = \mathbf{0}$. Διακρίνουμε περιπτώσεις:
1η περίπτωση

Το i ανήκει στο $\sigma \Rightarrow u_i^\sigma = u_i, \mathbf{b}_i^\sigma = \mathbf{b}_i \Rightarrow u_i^\sigma \mathbf{b}_i^\sigma = u_i\mathbf{b}_i$.

2η περίπτωση

Το i δεν ανήκει στο $\sigma \Rightarrow u_i^\sigma = -u_i, \mathbf{b}_i^\sigma = -\mathbf{b}_i \Rightarrow u_i^\sigma \mathbf{b}_i^\sigma = (-u_i)(-\mathbf{b}_i) = u_i\mathbf{b}_i$.

Και στις δύο περιπτώσεις ισχύει $u_i^\sigma \mathbf{b}_i^\sigma = u_i\mathbf{b}_i$.
Οπότε έχουμε $u_1^\sigma \mathbf{b}_1^\sigma + ... + u_s^\sigma \mathbf{b}_s^\sigma = \mathbf{0} \Rightarrow u_1\mathbf{b}_1 + ... + u_s\mathbf{b}_s = \mathbf{0}$. Δηλαδή το διάνυσμα $\mathbf{u} = (u_1, ..., u_s)$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$.

Ακόμη αφού το $\mathbf{u}^\sigma$ δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbb{Z}}(B^\sigma)$ συνεπάγεται πως και το $\mathbf{u}$ δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$.
Έστω όχι, θα καταλήξουμε σε άτοπο.
Είναι $\mathbf{u} = \mathbf{a} +_c \mathbf{b}$ με $\mathbf{a}, \mathbf{b} \in \mathrm{Ker}_{\mathbb{Z}}B$. Δηλαδή $\mathbf{u} = \mathbf{a} + \mathbf{b}$ και $\mid u_i \mid = \mid a_i \mid + \mid b_i \mid$ με $u_i = a_i + b_i$.
Αν το i ανήκει στο σ συνεπάγεται πως $u_i = u_i^\sigma, a_i = a_i^\sigma, b_i = b_i^\sigma \Rightarrow \mid u_i \mid = \mid a_i \mid + \mid b_i \mid \Leftrightarrow \mid u_i^\sigma \mid = \mid a_i^\sigma \mid + \mid b_i^\sigma \mid \Rightarrow \mathbf{u}^\sigma = \mathbf{a}^\sigma +_c \mathbf{b}^\sigma$, με $\mathbf{a}^\sigma, \mathbf{b}^\sigma \in \mathrm{Ker}_{\mathbb{Z}}(B^\sigma)$, άτοπο.
Αν το i δεν ανήκει στο σ συνεπάγεται πως $u_i = -u_i^\sigma, a_i = -a_i^\sigma, b_i = -b_i^\sigma \Rightarrow \mid u_i \mid = \mid a_i \mid + \mid b_i \mid \Leftrightarrow \mid -u_i^\sigma \mid = \mid -a_i^\sigma \mid + \mid -b_i^\sigma \mid \Leftrightarrow \mid u_i^\sigma \mid = \mid a_i^\sigma \mid + \mid b_i^\sigma \mid \Rightarrow \mathbf{u}^\sigma = \mathbf{a}^\sigma +_c \mathbf{b}^\sigma$, με $\mathbf{a}^\sigma, \mathbf{b}^\sigma \in \mathrm{Ker}_{\mathbb{Z}}(B^\sigma)$, άτοπο.
Άρα πράγματι το $\mathbf{u}$ ανήκει στη βάση Graver του I_B.

□

Παρατήρηση 3.1.16. Το $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$ αν και μόνο αν $\mathbf{a}^\sigma = \mathbf{b}^\sigma +_c \mathbf{c}^\sigma$ με $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathrm{Ker}_{\mathbb{Z}}B$ και $\mathbf{a}^\sigma, \mathbf{b}^\sigma, \mathbf{c}^\sigma \in \mathrm{Ker}_{\mathbb{Z}}(B^\sigma)$.

Απόδειξη. Έστω είναι $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$ τότε $\mathbf{a} = \mathbf{b} + \mathbf{c}$ και $\mid a_i \mid = \mid b_i \mid + \mid c_i \mid$, με $a_i = b_i + c_i$ όπου τα διανύσματα $\mathbf{a}, \mathbf{b}, \mathbf{c}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$.
Διακρίνουμε περιπτώσεις:
1η περίπτωση

Αν το i ανήκει στο σ συνεπάγεται πως $a_i = a_i^\sigma, b_i = b_i^\sigma, c_i = c_i^\sigma$. Συνεπώς $\mid a_i^\sigma \mid = \mid b_i^\sigma \mid + \mid c_i^\sigma \mid$ με $a_i^\sigma = b_i^\sigma + c_i^\sigma$ και $\mathbf{a}^\sigma = \mathbf{b}^\sigma + \mathbf{c}^\sigma$. Οπότε ισχύει $\mathbf{a}^\sigma = \mathbf{b}^\sigma +_c \mathbf{c}^\sigma$, όπου τα διανύσματα $\mathbf{b}^\sigma, \mathbf{c}^\sigma$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}(B^\sigma)$.
2η περίπτωση

Αν το i δεν ανήκει στο σ συνεπάγεται πως $a_i = -a_i^\sigma, b_i = -b_i^\sigma, c_i = -c_i^\sigma$. Συνεπώς $\mid -a_i^\sigma \mid = \mid -b_i^\sigma \mid + \mid -c_i^\sigma \mid$ με $(-a_i^\sigma) = (-b_i^\sigma) + (-c_i^\sigma) \Rightarrow \mid a_i^\sigma \mid = \mid b_i^\sigma \mid + \mid c_i^\sigma \mid$ με $a_i^\sigma = b_i^\sigma + c_i^\sigma$ και $\mathbf{a}^\sigma = \mathbf{b}^\sigma + \mathbf{c}^\sigma$. Οπότε ισχύει $\mathbf{a}^\sigma = \mathbf{b}^\sigma +_c \mathbf{c}^\sigma$, όπου τα διανύσματα $\mathbf{b}^\sigma, \mathbf{c}^\sigma$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}(B^\sigma)$.

Αντίστροφα έστω ότι είναι $\mathbf{a}^\sigma = \mathbf{b}^\sigma +_c \mathbf{c}^\sigma \Rightarrow \mid a_i^\sigma \mid = \mid b_i^\sigma \mid + \mid c_i^\sigma \mid$.
Διακρίνουμε περιπτώσεις:
1η περίπτωση

Αν το i ανήκει στο σ συνεπάγεται πως $a_i^\sigma = a_i, b_i^\sigma = b_i, c_i^\sigma = c_i$. Συνεπώς $\mid a_i \mid = \mid b_i \mid + \mid c_i \mid$ με $a_i = b_i + c_i$ και $\mathbf{a} = \mathbf{b} + \mathbf{c}$. Οπότε ισχύει $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$, όπου τα διανύσματα $\mathbf{b}, \mathbf{c}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$.
2η περίπτωση

Αν το i δεν ανήκει στο σ συνεπάγεται πως $a_i^\sigma = -a_i, b_i^\sigma = -b_i, c_i^\sigma = -c_i$. Συνεπώς $\mid -a_i \mid = \mid -b_i \mid + \mid -c_i \mid$ με $(-a_i) = (-b_i) + (-c_i) \Rightarrow \mid a_i \mid = \mid b_i \mid + \mid c_i \mid$ με $a_i = b_i + c_i$ και $\mathbf{a} = \mathbf{b} + \mathbf{c}$. Οπότε ισχύει $\mathbf{a} = \mathbf{b} +_c \mathbf{c}$, όπου τα διανύσματα $\mathbf{b}, \mathbf{c}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$. □

Παρατήρηση 3.1.17. Έστω το διάνυσμα $\mathbf{u} = (u_1, ..., u_s)$. Τότε ισχύει:

$$\| \mathbf{u} \|_1 = \| \mathbf{u}^\sigma \|_1 .$$

Απόδειξη. Διακρίνουμε περιπτώσεις:
1η περίπτωση

Αν το i ανήκει στο σ συνεπάγεται πως $u_i^\sigma = u_i$.
Τότε ισχύει $\mid u_i \mid = \mid u_i^\sigma \mid$.
2η περίπτωση

Αν το i δεν ανήκει στο σ συνεπάγεται πως $u_i^\sigma = -u_i$.
Τότε ισχύει $\mid u_i \mid = \mid -u_i^\sigma \mid = \mid u_i^\sigma \mid$.
Οπότε και στις δύο περιπτώσεις ισχύει:

$$\mid u_i \mid = \mid u_i^\sigma \mid .$$

Συνεπώς $\| \mathbf{u} \|_1 = \mid u_1 \mid + \ldots + \mid u_s \mid = \mid u_1^\sigma \mid + \ldots + \mid u_s^\sigma \mid = \| \mathbf{u}^\sigma \|_1$.
Δηλαδή τα σύνολα $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}, B^\sigma = \{\mathbf{b}_1^\sigma, \ldots, \mathbf{b}_s^\sigma\}$ δεν έχουν την ίδια βάση Graver αλλά οι δυο βάσεις έχουν την ίδια $max(1 - norm)$. □

Ορισμός 3.1.18. *Το σύνολο των στοιχείων* $\mathbf{a}$ *του πυρήνα* $\mathrm{Ker}_{\mathbf{Z}} A$ *τα οποία δεν μπορούν να γραφούν ως ημισύμμορφο άθροισμα συμβολίζεται με* $S(A)$.

Ορισμός 3.1.19. *Το σύνολο των στοιχείων* $\mathbf{a}$ *του πυρήνα* $\mathrm{Ker}_{\mathbf{Z}} A$ *τα οποία είναι τέτοια ώστε:*
το διώνυμο $x^{\mathbf{a}^+} - x^{\mathbf{a}^-}$ *ή, το διώνυμο* $x^{\mathbf{a}^-} - x^{\mathbf{a}^+}$ *ανήκει σε κάθε ελαχιστοτική βάση Markou του ιδεώδους* $I_{\mathbf{A}}$,
συμβολίζεται με $Ind(A)$.

Ορισμός 3.1.20. *Το διώνυμο* $B = x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ *καλείται* ***αναντικατάστατο των ελαχιστοτικών βάσεων Markou*** *του ιδεώδους* $I_{\mathbf{A}}$ *αν και μόνο αν κάθε ελαχιστοτικό σύστημα γεννητόρων του* $I_{\mathbf{A}}$ *περιέχει το* B *ή το* $-B$.

Ορισμός 3.1.21. *Το διώνυμο* $B = x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ *καλείται* ***αναντικατάστατο των ανάγωγων βάσεων Gröbner*** *του ιδεώδους* $I_{\mathbf{A}}$ *αν και μόνο αν κάθε ανάγωγη βάση Gröbner του* $I_{\mathbf{A}}$ *περιέχει το* B *ή το* $-B$.

Παρατήρηση 3.1.22. Η ένωση των ελαχιστοτικών βάσεων Markov του ιδεώδους $I_{\mathbf{A}}$ αποτελεί την καθολική βάση Markov του $I_{\mathbf{A}}$, ενώ η τομή των ελαχιστοτικών βάσεων Markov του $I_{\mathbf{A}}$ αποτελεί το σύνολο των αναντικατάστατων διωνύμων των ελαχιστοτικών βάσεων Markov.
Η ένωση των ανάγωγων βάσεων Gröbner του ιδεώδους $I_{\mathbf{A}}$ αποτελεί την καθολική βάση Gröbner του $I_{\mathbf{A}}$, ενώ η τομή των ανάγωγων βάσεων Gröbner του $I_{\mathbf{A}}$ αποτελεί το σύνολο των αναντικατάστατων διωνύμων των ανάγωγων βάσεων Gröbner.

Πρόταση 3.1.23. *Για το διάνυσμα* $\mathbf{t} \in \mathbb{N}_0^n$ *και το διάνυσμα* $\mathbf{v} \in \mathrm{Ker}_{\mathbf{Z}} A$ *έχουμε* $\mathbf{t} + \mathbf{v} \geq 0$ *αν και μόνο αν* $\mathbf{t} \geq \mathbf{v}^-$.

Απόδειξη. Έστω το διάνυσμα $\mathbf{t} = (t_1, \ldots, t_n)$ και το διάνυσμα $\mathbf{v} = (v_1, \ldots, v_n)$.
Υποθέτουμε ότι $\mathbf{t} + \mathbf{v} \geq \mathbf{0}$ τότε $(t_1, \ldots, t_n) + (v_1, \ldots, v_n) \geq \mathbf{0} \Rightarrow$
$(t_1 + v_1, \ldots, t_n + v_n) \geq \mathbf{0}$. Θεωρούμε ένα $i \in \{1, \ldots n\}$ και διακρίνουμε περιπτώσεις για το v_i.
Αν $v_i \leq 0 \Rightarrow v_i = -v_i^- \Rightarrow v_i^- = -v_i$. Τότε είναι $t_i + v_i \geq 0 \Rightarrow t_i \geq -v_i = v_i^- \Rightarrow$ $t_i \geq v_i^-$.
Αν $v_i > 0 \Rightarrow v_i^- = 0$. Τότε είναι $t_i \geq 0 = v_i^- \Rightarrow t_i \geq v_i^-$. Αφού ισχύει για το τυχαίο $i \in \{1, \ldots n\}$, θα ισχύει και για κάθε $i \in \{1, \ldots n\}$ άρα $\mathbf{t} \geq \mathbf{v}^-$.

Αντίστροφα έστω ότι $\mathbf{t} \geq \mathbf{v}^-$. Θα δείξουμε ότι $\mathbf{t}+\mathbf{v} \geq \mathbf{0}$. Είναι $\mathbf{t} \geq \mathbf{v}^- \geq \mathbf{0} \Rightarrow \mathbf{t}-\mathbf{v}^- \geq \mathbf{0}$. Έχουμε $\mathbf{t}+\mathbf{v} = \mathbf{t}+\mathbf{v}^+-\mathbf{v}^- = (\mathbf{t}-\mathbf{v}^-)+\mathbf{v}^+ \geq \mathbf{0}$. Αφού $(\mathbf{t}-\mathbf{v}^-) \geq \mathbf{0}$ και $\mathbf{v}^+ \geq \mathbf{0}$. Άρα $\mathbf{t}+\mathbf{v} \geq \mathbf{0}$. □

Ορισμός 3.1.24. *Το ελάχιστο μεταξύ δύο μη αρνητικών διανυσμάτων* $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^n$ *ορίζεται ως εξής:*

$$min(\mathbf{a}, \mathbf{b}) = (min(a_i, b_i)/1 \leq i \leq n).$$

Θεώρημα 3.1.25. *Το σύνολο των στοιχείων* $\mathbf{a}$ *του πυρήνα* $\mathrm{Ker}_{\mathbb{Z}}A$ *τα οποία δεν μπορούν να γραφούν ως ημισύμμορφο άθροισμα είναι ίσο με το σύνολο των αναντικατάστατων διωνύμων των βάσεων Markov, δηλαδή* $S(A) = Ind(A)$.

Απόδειξη. Έστω ένα διάνυσμα $\mathbf{u}$ ανήκει στο σύνολο $Ind(A)$, θα δείξουμε ότι το $\mathbf{u}$ ανήκει στο σύνολο $S(A)$. Έστω όχι, θα καταλήξουμε σε άτοπο. Το $\mathbf{u}$ ανήκει στο σύνολο $Ind(A)$ άρα το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ ανήκει σε κάθε ελαχιστοτικό σύνολο γεννητόρων του ιδεώδους $I_{\mathbf{A}}$. Έστω $\{x^{\mathbf{u}^+} - x^{\mathbf{u}^-}, B_2, ..., B_s\}$ μια ελαχιστοτική βάση Markov του A, δηλαδή

$$I_{\mathbf{A}} = \langle x^{\mathbf{u}^+} - x^{\mathbf{u}^-}, B_2, ..., B_s \rangle.$$

Το διάνυσμα u δεν ανήκει στο σύνολο $S(A)$ συνεπώς γράφεται ως ημισύμμορφο άθροισμά των διανυσμάτων του πυρήνα $\mathbf{v}, \mathbf{w} \in \mathrm{Ker}_{\mathbb{Z}}A$, $\mathbf{u} = \mathbf{v} +_{sc} \mathbf{w} \Rightarrow$
$\mathbf{u} = \mathbf{v} + \mathbf{w}, \mathbf{u}^+ \geq \mathbf{v}^+, \mathbf{u}^- \geq \mathbf{w}^-$. Αφού λοιπόν ισχύει $\mathbf{u} = \mathbf{v} + \mathbf{w}$ συνεπάγεται πως $\mathbf{u}^+ - \mathbf{u}^- = \mathbf{v} + \mathbf{w} \Rightarrow \mathbf{u}^+ - \mathbf{v} = \mathbf{u}^- + \mathbf{w}$.
Ισχυριζόμαστε ότι το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ είναι ίσο με $x^{\mathbf{u}^+} - x^{\mathbf{u}^-} = x^{\mathbf{u}^+-\mathbf{v}^+}(x^{\mathbf{v}^+} - x^{\mathbf{v}^-}) + x^{\mathbf{u}^--\mathbf{w}^-}(x^{\mathbf{w}^+} - x^{\mathbf{w}^-})$, κι αφού $\mathbf{u}^+ - \mathbf{v} = \mathbf{u}^- + \mathbf{w} \Rightarrow x^{\mathbf{u}^+-\mathbf{v}} = x^{\mathbf{u}^-+\mathbf{w}}$, ισχύει η ισότητα.
Θέτουμε $B_{\mathbf{u}} = x^{\mathbf{u}^+} - x^{\mathbf{u}^-}, B_{\mathbf{v}} = x^{\mathbf{v}^+} - x^{\mathbf{v}^-}, B_{\mathbf{w}} = x^{\mathbf{w}^+} - x^{\mathbf{w}^-}$.
Έχουμε $B_{\mathbf{u}} = x^{\mathbf{u}^+-\mathbf{v}^+}B_{\mathbf{v}} + x^{\mathbf{u}^--\mathbf{w}^-}B_{\mathbf{w}}$. Δηλαδή για το ιδεώδες $I_{\mathbf{A}}$ ισχύει:

$$I_{\mathbf{A}} = \langle B_{\mathbf{u}}, B_2, ..., B_s \rangle \subseteq \langle B_{\mathbf{v}}, B_{\mathbf{w}}, B_2, ..., B_s \rangle.$$

Ακόμη $\mathbf{v}, \mathbf{w} \in \mathrm{Ker}_{\mathbb{Z}}A$ από την παρατήρηση 2.1.10 συνεπάγεται πως $x^{\mathbf{v}^+} - x^{\mathbf{v}^-} = B_{\mathbf{v}}, x^{\mathbf{w}^+} - x^{\mathbf{w}^-} = B_{\mathbf{w}} \in I_{\mathbf{A}}$, οπότε

$$\langle B_{\mathbf{u}}, B_2, ..., B_s \rangle \supseteq \langle B_{\mathbf{v}}, B_{\mathbf{w}}, B_2, ..., B_s \rangle.$$

Άρα είναι

$$\langle B_{\mathbf{u}}, B_2, ..., B_s \rangle = \langle B_{\mathbf{v}}, B_{\mathbf{w}}, B_2, ..., B_s \rangle.$$

Δηλαδή το σύνολο $\{B_{\mathbf{v}}, B_{\mathbf{w}}, B_2, ..., B_s\}$ είναι σύνολο γεννητόρων του ιδεώδους $I_{\mathbf{A}}$.
Συνεπώς υπάρχει ένα ελαχιστοτικό σύνολο γεννητόρων υποσύνολο του $\{B_{\mathbf{v}}, B_{\mathbf{w}}, B_2, ..., B_s\}$ που δεν περιέχει το αναντικατάστατο διώνυμο $B_{\mathbf{u}} = x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$, άτοπο.
Αντίστροφα έστω το διάνυσμα $\mathbf{u}$ ανήκει στο σύνολο $S(A)$ και το $\mathbf{u}$ δεν ανήκει στο σύνολο $Ind(A)$ θα καταλήξουμε σε άτοπο. Αφού το $\mathbf{u}$ δεν ανήκει στο σύνολο $Ind(A)$ σύμφωνα με το άρθρο [4] των Α.Θωμά, Α.Κατσαμπέκη και της Χ.Χαραλάμπους, στην ίνα $deg_{\mathbf{A}}^{-1}(x^{\mathbf{u}^+})$ που περιέχει τα μονώνυμα $x^{\mathbf{u}^+}, x^{\mathbf{u}}$ περιέχεται τουλάχιστον ένα ακόμη μονώνυμο, έστω το μονώνυμο $x^{\mathbf{a}}$, όπου $\mathbf{a} \in \mathbb{N}_0^n$.
Είναι $x^{\mathbf{u}^+} - x^{\mathbf{u}^-} = x^{\mathbf{s}}(x^{\mathbf{u}^+-\mathbf{s}} - x^{\mathbf{a}-\mathbf{s}}) + x^{\mathbf{t}}(x^{\mathbf{a}-\mathbf{t}} - x^{\mathbf{u}^--\mathbf{t}})$, με $\mathbf{s} = min(\mathbf{u}^+, \mathbf{a}), \mathbf{t} = min(\mathbf{u}^-, \mathbf{a})$.
Θέτουμε $\mathbf{u}^+ - \mathbf{a} = \mathbf{v} = (\mathbf{u}^+ - \mathbf{s}) - (\mathbf{a} - \mathbf{s})$. Ισχυριζόμαστε ότι $\mathbf{v}^+ = \mathbf{u}^+ - \mathbf{s}, \mathbf{v}^- =$

$\mathbf{a}-\mathbf{s}$.
Πράγματι:
Όταν το $v_i^+ = (u^+ - s)_i > 0$, τότε ισχύει $(a-s)_i = 0$. Πράγματι είναι $(u^+ - s)_i > 0 \Rightarrow u_i^+ - s_i > 0$ συνεπώς $u_i^+ > s_i \Rightarrow s_i = a_i \Rightarrow (a-s)_i = 0$, εφόσον το $\mathbf{s}$ είναι το ελάχιστο εκ των $\mathbf{u}^+, \mathbf{a}$. Δηλαδή το s_i είναι το ελάχιστο εκ των u_i^+, a_i κι από τη σχέση $u_i^+ > s_i$, έχουμε ότι το s_i ισούται με το a_i, για κάθε $i = 1, ...n$.
Όταν το $v_i^- = (a-s)_i > 0$, τότε ισχύει $(u^+ - s)_i = 0$. Πράγματι είναι $(a-s)_i > 0$ συνεπώς $a_i - s_i > 0 \Rightarrow a_i > s_i \Rightarrow s_i = u_i^+ \Rightarrow (u^+ - s)_i = 0$, εφόσον το $\mathbf{s}$ είναι το ελάχιστο εκ των $\mathbf{u}^+, \mathbf{a}$. Δηλαδή το s_i είναι το ελάχιστο εκ των u_i^+, a_i κι από τη σχέση $a_i > s_i$, έχουμε ότι το s_i ισούται με το u_i^+, για κάθε $i = 1, ...n$.
Θέτουμε $\mathbf{a} - \mathbf{u}^- = \mathbf{w} = (\mathbf{a} - \mathbf{t}) - (\mathbf{u}^- - \mathbf{t})$. Ισχυριζόμαστε ότι $\mathbf{w}^+ = \mathbf{a} - \mathbf{t}, \mathbf{w}^- = \mathbf{u}^- - \mathbf{t}$.
Πράγματι:
Όταν το $w_i^+ = (a-t)_i > 0$, τότε ισχύει $(u^- - t)_i = 0$. Πράγματι είναι $(a-t)_i > 0$ συνεπώς $a_i - t_i > 0 \Rightarrow a_i > t_i \Rightarrow t_i = u_i^- \Rightarrow (u^- - t)_i = 0$, εφόσον το $\mathbf{t}$ είναι το ελάχιστο εκ των $\mathbf{u}^-, \mathbf{a}$. Δηλαδή το t_i είναι το ελάχιστο εκ των u_i^-, a_i κι από $a_i > t_i$, έχουμε ότι το t_i ισούται με το u_i^-, για κάθε $i = 1, ...n$.
Όταν το $w_i^- = (u^- - t)_i > 0$, τότε ισχύει $(a-t)_i = 0$. Πράγματι είναι $(u^- - t)_i > 0$ συνεπώς $u_i^- - t_i > 0 \Rightarrow u_i^- > t_i \Rightarrow t_i = a_i \Rightarrow (a-t)_i = 0$, εφόσον το $\mathbf{t}$ είναι το ελάχιστο εκ των $\mathbf{u}^-, \mathbf{a}$. Δηλαδή το t_i είναι το ελάχιστο εκ των u_i^-, a_i κι από $u_i^- > t_i$, έχουμε ότι το t_i ισούται με το a_i, για κάθε $i = 1, ...n$.
Άρα $\mathbf{v} = \mathbf{u}^+ - \mathbf{a}, \mathbf{w} = \mathbf{a} - \mathbf{u}^-$ συνεπώς $\mathbf{u}^+ - \mathbf{a} + \mathbf{a} - \mathbf{u}^- = \mathbf{v} + \mathbf{w} \Rightarrow \mathbf{u} = \mathbf{v} + \mathbf{w}$.
Θα δείξουμε ότι $\mathbf{u}^+ \geq \mathbf{v}^+$ και $\mathbf{u}^- \geq \mathbf{w}^-$. Δηλαδή θα δείξουμε ότι το $\mathbf{u}^+ \geq \mathbf{u}^+ - \mathbf{s} \Rightarrow \mathbf{s} \geq 0$. Όμως το $\mathbf{s}$ εξ' ορισμού είναι το ελάχιστο μεταξύ δύο μη αρνητικών διανυσμάτων συνεπώς θα είναι κι αυτό μη αρνητικό διάνυσμα. Δηλαδή $\mathbf{s} \geq 0$. Θα δείξουμε ότι $\mathbf{u}^- \geq \mathbf{w}^-$ δηλαδή $\mathbf{u}^- \geq \mathbf{u}^- - \mathbf{t} \Rightarrow \mathbf{t} \geq 0$. Όμως το $\mathbf{t}$ εξ' ορισμού είναι το ελάχιστο μεταξύ δύο μη αρνητικών διανυσμάτων συνεπώς θα είναι κι αυτό μη αρνητικό διάνυσμα. Δηλαδή $\mathbf{t} \geq 0$. Άρα σύμφωνα με την παρατήρηση 3.1.6 ισχύει $\mathbf{u} = \mathbf{v} +_{sc} \mathbf{w}$ άτοπο, εφόσον υποθέσαμε ότι το διάνυσμα $\mathbf{u}$ ανήκει στο σύνολο $S(A)$. □

Πρόταση 3.1.26. *Το διώνυμο B ανήκει σε κάθε ελαχιστοτικό σύστημα γεννητόρων του $I_{\mathbf{A}}$ αν και μόνο αν το B ανήκει σε κάθε σύστημα γεννητόρων.*

Απόδειξη. Έστω ότι το B ανήκει σε κάθε ελαχιστοτικό σύστημα γεννητόρων του $I_{\mathbf{A}}$ θα δείξουμε ότι ανήκει σε κάθε σύστημα γεννητόρων. Έστω ένα τυχαίο σύστημα γεννητόρων, αυτό περιέχει ένα ελαχιστοτικό σύστημα γεννητόρων στο οποίο όπως υποθέσαμε ανήκει το B. Άρα το διώνυμο B ανήκει σε κάθε σύστημα γεννητόρων. Αντίστροφα έστω ότι το B ανήκει σε κάθε σύστημα γεννητόρων συνεπώς ανήκει και σε κάθε ελαχιστοτικό σύστημα γεννητόρων. □

Πρόταση 3.1.27. *Το διώνυμο B ανήκει σε κάθε ανάγωγη βάση Gröbner του $I_{\mathbf{A}}$ αν και μόνο αν το B ανήκει σε κάθε βάση Gröbner.*

Απόδειξη. Έστω ότι το B ανήκει σε κάθε ανάγωγη βάση Gröbner του $I_{\mathbf{A}}$ θα δείξουμε ότι ανήκει σε κάθε βάση Gröbner. Έστω μια τυχαία βάση Gröbner, αυτή περιέχει μια ανάγωγη βάση Gröbner στην οποία όπως υποθέσαμε ανήκει το B. Άρα το διώνυμο B ανήκει στην τυχαία βάση Gröbner, συνεπώς και σε κάθε βάση Gröbner.
Αντίστροφα έστω ότι το B ανήκει σε κάθε βάση Gröbner συνεπώς ανήκει και σε κάθε ανάγωγη βάση Gröbner. □

Θεώρημα 3.1.28. *Το σύνολο των αναντικατάστατων διωνύμων των βάσεων Markov είναι ίσο με το σύνολο των αναντικατάστατων διωνύμων των βάσεων Gröbner.*

Απόδειξη. Έστω $x^{\mathbf{u}^+} - x^{\mathbf{u}}$ ένα αναντικατάστατο διώνυμο των βάσεων Markov. Θα δείξουμε ότι το $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ ανήκει σε κάθε βάση Gröbner. Θεωρούμε μια τυχαία βάση Gröbner G, αυτή σύμφωνα με το πόρισμα 1.3.13 είναι βάση Markov, αποτελεί δηλαδή σύστημα γεννητόρων του ιδεώδους $I_{\mathbf{A}}$. Όπως υποθέσαμε σε αυτό ανήκει το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$, άρα το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ ανήκει και στην τυχαία βάση Gröbner G. Συνεπώς ανήκει σε κάθε βάση Gröbner. Οπότε το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ είναι αναντικατάστατο των βάσεων Gröbner.
Αντίστροφα θα δείξουμε ότι το σύνολο των αναντικατάστατων διωνύμων των βάσεων Gröbner είναι υποσύνολο του συνόλου των αναντικατάστατων διωνύμων των βάσεων Markov. Έστω ότι το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ δεν ανήκει στο σύνολο των αναντικατάστατων διωνύμων των βάσεων Markov. Θα δείξουμε ότι το $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ δεν ανήκει στο σύνολο των αναντικατάστατων διωνύμων των βάσεων Gröbner. Αρκεί να δείξουμε ότι υπάρχει μια διάταξη όρων ως προς την οποία το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}}$ δεν ανήκει, σύμφωνα με την πρόταση 3.1.27, στο σύνολο των αναντικατάστατων διωνύμων των ανάγωγων βάσεων Gröbner. Αφού το $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ δεν ανήκει στο σύνολο των αναντικατάστατων διωνύμων των βάσεων Markov σύμφωνα με την πρόταση 3.1.26 δεν ανήκει στο σύνολο των αναντικατάστατων διωνύμων των ελαχιστότικών βάσεων Markov, άρα το διάνυσμα $\mathbf{u}$ δεν ανήκει στο σύνολο $Ind(A)$. Συνεπώς υπάρχουν κι άλλα μονώνυμα στην ίνα $deg_{\mathbf{A}}^{-1}(x^{\mathbf{u}^+})$ εκτός των $x^{\mathbf{u}^+}, x^{\mathbf{u}^-}$ σύμφωνα με το άρθρο [4] των Α.Θωμά, Α.Κατσαμπέκη και της Χ.Χαραλάμπους. Διακρίνουμε περιπτώσεις:
1η περίπτωση
Υπάρχει ένα μονώνυμο $x^{\mathbf{a}}$ τέτοιο ώστε μκδ$(x^{\mathbf{u}^+}, x^{\mathbf{a}}) = x^{\mathbf{g}} \neq 1$, όπου μκδ$(x^{\mathbf{u}^+}, x^{\mathbf{a}}) = x^{min(\mathbf{u}^+, \mathbf{a})}$. Τα μονώνυμα $x^{\mathbf{u}^+}, x^{\mathbf{a}}$ ανήκουν στην ίδια ίνα συνεπώς $deg_{\mathbf{A}}(x^{\mathbf{u}^+}) = deg_{\mathbf{A}}(x^{\mathbf{a}}) \Rightarrow deg_{\mathbf{A}}(x^{\mathbf{u}^+ - \mathbf{g}}) = deg_{\mathbf{A}}(x^{\mathbf{a}-\mathbf{g}})$, με $\mathbf{u}^+ - \mathbf{g} \geq \mathbf{0}$ και $\mathbf{a} - \mathbf{g} \geq \mathbf{0}$ αφού $\mathbf{g} = min(\mathbf{u}^+, \mathbf{a})$. Άρα τα μονώνυμα $x^{\mathbf{u}^+ - \mathbf{g}}, x^{\mathbf{a}-\mathbf{g}}$ έχουν τον ίδιο $A-$βαθμό συνεπώς το διώνυμο $x^{\mathbf{u}^+ - \mathbf{g}} - x^{\mathbf{a}-\mathbf{g}}$ ανήκει στο ιδεώδες $I_{\mathbf{A}}$. Θεωρώ μια διάταξη απαλοιφής $\succ$ με τις μεταβλητές που ανήκουν στο φορέα $supp(x^{\mathbf{u}^+ - \mathbf{g}})$ μεγαλύτερες απ' όλες τις άλλες και $G_{\succ}$ η αντίστοιχη ανάγωγη βάση Gröbner. Τότε το αρχικό μονώνυμο του διωνύμου $x^{\mathbf{u}^+ - \mathbf{g}} - x^{\mathbf{a}-\mathbf{g}}$ είναι το $x^{\mathbf{u}^+ - \mathbf{g}}$. Η $G_{\succ}$ είναι βάση Gröbner, άρα από τον ορισμό της υπάρχει ένα διώνυμο $g_i \in G_{\succ}$ τέτοιο ώστε $lm(g_i) \setminus x^{\mathbf{u}^+ - \mathbf{g}}$. Όμως ισχύει $x^{\mathbf{u}^+ - \mathbf{g}} \neq x^{\mathbf{u}^+}$ αφού $x^{\mathbf{g}} \neq 1$, δηλαδή $\mathbf{g} \neq \mathbf{0}$, άρα είναι $\mathbf{u}^+ > \mathbf{u}^+ - \mathbf{g}$. Σύμφωνα με τη μερική διάταξη που δίνεται από τη διαιρετότητα έχουμε ότι το μονώνυμο $x^{\mathbf{u}^+ - \mathbf{g}}$ διαιρεί το μονώνυμο $x^{\mathbf{u}^+}$ και μάλιστα το διαιρεί γνήσια. Άρα τελικά $lm(g_i) \setminus x^{\mathbf{u}^+} \Rightarrow x^{\mathbf{u}^+} - x^{\mathbf{u}^-} \notin G_{\succ}$. Δηλαδή το διώνυμο $x^{\mathbf{u}^+} - x^{\mathbf{u}^-}$ δεν ανήκει στην ανάγωγη βάση Gröbner $G_{\succ}$ ως προς τη διάταξη που ορίσαμε.
2η περίπτωση
Υπάρχει ένα μονώνυμο $x^{\mathbf{a}}$ τέτοιο ώστε μκδ$(x^{\mathbf{u}^-}, x^{\mathbf{a}}) = x^{g} \neq 1$ όπου μκδ$(x^{\mathbf{u}^-}, x^{\mathbf{a}}) = x^{min(u^-, \mathbf{a})}$, η απόδειξη είναι όμοια με την πρώτη περίπτωση.
3η περίπτωση
Για κάθε $x^{\mathbf{a}}$ που ανήκει στην ίνα $deg_{\mathbf{A}}^{-1}(x^{\mathbf{u}^+})$ των $x^{\mathbf{u}^+}, x^{\mathbf{u}}$ ο μκδ$(x^{\mathbf{u}^+}, x^{\mathbf{a}}) = 1$ και μκδ$(x^{\mathbf{u}}, x^{\mathbf{a}}) = 1$, άρα οι τρεις φορείς $supp(x^{\mathbf{u}^+}), supp(x^{\mathbf{u}^+}), supp(x^{\mathbf{a}})$ είναι ξένοι μεταξύ τους. Έστω $x^{\mathbf{a}'}$ ανήκει στην ίνα $deg_{\mathbf{A}}^{-1}(x^{\mathbf{u}^+})$. Ορίζουμε διάταξη απαλοιφής $\prec$ με τις μεταβλητές που ανήκουν στο φορέα $supp(x^{\mathbf{u}^+})$, μεγαλύτερες από τις μεταβλητές που ανήκουν στο φορέα $supp(x^{\mathbf{u}^-})$, μεγαλύτερες από τις με-

ταβλητές που ανήκουν στο φορέα $supp(x^{a'})$ και $G_{\prec}$ η αντίστοιχη ανάγωγη βάση Gröbner. Παρατηρούμε ότι το αρχικό μονώνυμο του διωνύμου $x^{u^+} - x^u$ είναι το x^{u^+}, ενώ το αρχικό μονώνυμο του διωνύμου $x^{u^-} - x^{a'}$ είναι το x^{u^-}. Όμως το διώνυμο $x^{u^-} - x^{a'}$ ανήκει στο ιδεώδες I_A, άρα από τον ορισμό της βάσης Gröbner υπάρχει ένα διώνυμο $g_i \in G_{\prec}$ τέτοιο ώστε $lm(g_i) \setminus x^{u^-} \Rightarrow x^{u^+} - x^{u^-} \notin G_{\prec}$. Δηλαδή το διώνυμο $x^{u^+} - x^{u^-}$ δεν ανήκει στην ανάγωγη βάση Gröbner $G_{\succ}$ ως προς τη διάταξη που ορίσαμε. □

Κεφάλαιο 4

Πολυπλοκότητα Graver και Markov

Κάθε σύνολο διανυσμάτων με ακέραιες συντεταγμένες εγείρει μια ιεραρχία από συνθέσεις υψηλότερων διαστάσεων οι οποίες γενικεύουν την Lawrence κατασκευή που είδαμε στο κεφάλαιο δύο. Το 2002 οι στατιστικοί S.Aoki και A.Takemura [2] παρατήρησαν μελετώντας βάσεις Markov για πίνακες της μορφής $A^{(r)}$, που προερχόταν από προβλήματα στατιστικής, ότι γράφοντας τα στοιχεία της βάσης Markov $A^{(r)}$ σαν πίνακες $r \times n$, είχαν το πολύ πέντε μη μηδενικές γραμμές για οποιοδήποτε r. Το εντυπωσιακό αυτό γεγονός οδήγησε τους F.Santos και B.Sturmfels να ασχοληθούν με το θέμα και να ορίσουν ως τύπο ενός πίνακα το πλήθος των μη μηδενικών γραμμών του. Επίσης την έννοια της Markov και Graver πολυπλοκότητας ενός πίνακα A, σαν τον μέγιστο τύπο των στοιχείων των βάσεων Markov και Graver του $A^{(r)}$ αντίστοιχα, όταν γράψουμε τα στοιχεία τους ως πίνακες $r \times n$. Ακόμη απέδειξαν ότι η Markov και η Graver πολυπλοκότητα είναι πάντα πεπερασμένη. Στόχος αυτού του κεφαλαίου είναι να δούμε την απόδειξη των F.Santos και B.Sturmfels.

4.1 Πίνακας Lawrence $A^{(r)}$

Σταθεροποιούμε ένα σύνολο διανυσμάτων $A = \{\mathbf{a_1}, ..., \mathbf{a_n}\} \subseteq \mathbb{Z}^{\mathbf{d}} \subseteq \mathbb{Q}^{\mathbf{d}}$ που παράγουν τον $\mathbb{Q}^d$ κι έστω $\mathrm{Ker}_{\mathbb{Z}} A$ το κιγκλίδωμα γραμμικών συνδυασμών στο A. Εισάγουμε την ακολουθία πινάκων $A^{(2)}$, $A^{(3)}$, $A^{(4)}$,..., $A^{(k)}$,...:

$$A^{(2)} = \begin{pmatrix} A & 0 \\ 0 & A \\ I & I \end{pmatrix}$$

$$A^{(3)} = \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \\ I & I & I \end{pmatrix}$$

$$A^{(4)} = \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & A \\ I & I & I & I \end{pmatrix}$$

...

$$A^{(k)} = \begin{pmatrix} A & 0 & . & . & . & . & . & . & . & . & 0 & 0 \\ 0 & A & . & . & . & . & . & . & . & . & 0 & 0 \\ 0 & 0 & A & . & . & . & . & . & . & . & 0 & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & . & . & . & . & . & . & . & 0 & A \\ I & I & I & . & . & . & . & . & . & . & I & I \end{pmatrix}.$$

Όπου I ο μοναδιαίος $n \times n$ πίνακας και A ο $d \times n$ πίνακας οι στήλες του οποίου είναι τα διανύσματα του συνόλου A. Εφόσον ο πίνακας A είναι ένας $d \times n$ πίνακας τότε ο πίνακας $A^{(2)}$ είναι ένας $(2d + n) \times 2n$ πίνακας, ο πίνακας $A^{(3)}$ είναι ένας $(3d + n) \times 3n$ πίνακας κι αντίστοιχα ο πίνακας $A^{(k)}$ είναι ένας $(kd + n) \times kn$ πίνακας.
Το ιδεώδες I_A είναι το εξής

$$I_A = \langle x^{\mathbf{u}^+} - x^{\mathbf{u}^-} / deg_A(x^{\mathbf{u}^+}) = deg_A(x^{\mathbf{u}^-}) \rangle,$$

όπου $\mathbf{u} = (u_1, ..., u_n)$.
Από τη σχέση $deg_A(x^{\mathbf{u}^+}) = deg_A(x^{\mathbf{u}^-})$ έχουμε ότι
$u_1^+ \mathbf{a}_1 + ... + u_n^+ \mathbf{a}_n = u_1^- \mathbf{a}_1 + ... + u_n^- \mathbf{a}_n \Rightarrow$
$(u_1^+ - u_1^-)\mathbf{a}_1 + ... + (u_n^+ - u_n^-)\mathbf{a}_n = 0 \Rightarrow$
$u_1 \mathbf{a}_1 + ... + u_n \mathbf{a}_n = 0$. Όπου $\mathbf{a}_i = (a_{i_1}, ..., a_{i_d})$ για $1 \leq i \leq n$.
Είναι $\begin{pmatrix} a_{11} & a_{21} & . & . & . & a_{n1} \\ a_{12} & a_{22} & . & . & . & a_{n2} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{1d} & a_{2d} & . & . & . & a_{nd} \end{pmatrix} \begin{pmatrix} u_1 \\ . \\ . \\ . \\ u_n \end{pmatrix} = \begin{pmatrix} 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}$.
Συνεπώς

$$a_{11}u_1 + ... + a_{n1}u_n = 0$$

...

$$a_{1d}u_1 + ... + a_{nd}u_n = 0.$$

Είναι $A\mathbf{u}^\tau = 0 \Leftrightarrow$ το διάνυσμα $\mathbf{u}^\tau$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} A$. Θα επαναλάβουμε τη διαδικασία για τον πίνακα $A^{(2)}$.

Είναι $A^{(2)} = \begin{pmatrix} A & 0 \\ 0 & A \\ I & I \end{pmatrix} =$

$$\begin{pmatrix}
a_{11} & \cdot & \cdot & \cdot & a_{n1} & 0 & \cdot & \cdot & \cdot & 0 \\
a_{12} & \cdot & \cdot & \cdot & a_{n2} & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a_{1d} & \cdot & \cdot & \cdot & a_{nd} & 0 & \cdot & \cdot & \cdot & 0 \\
0 & \cdot & \cdot & \cdot & 0 & a_{11} & \cdot & \cdot & \cdot & a_{n1} \\
\cdot & \cdot & \cdot & \cdot & \cdot & a_{12} & \cdot & \cdot & \cdot & a_{n2} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & 0 & a_{1d} & \cdot & \cdot & \cdot & a_{nd} \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

άρα

$$\begin{pmatrix}
a_{11} & \cdot & \cdot & \cdot & a_{n1} & 0 & \cdot & \cdot & \cdot & 0 \\
a_{12} & \cdot & \cdot & \cdot & a_{n2} & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a_{1d} & \cdot & \cdot & \cdot & a_{nd} & 0 & \cdot & \cdot & \cdot & 0 \\
0 & \cdot & \cdot & \cdot & 0 & a_{11} & \cdot & \cdot & \cdot & a_{n1} \\
\cdot & \cdot & \cdot & \cdot & \cdot & a_{12} & \cdot & \cdot & \cdot & a_{n2} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & 0 & a_{1d} & \cdot & \cdot & \cdot & a_{nd} \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}
\begin{pmatrix} u_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ u_n \\ v_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ v_n \end{pmatrix} =
\begin{pmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}.$$

Συνεπώς

$$a_{11}u_1 + \ldots + a_{n1}u_n = 0$$

$$a_{12}u_1 + \ldots + a_{n2}u_n = 0$$

$$\ldots$$

$$a_{1d}u_1 + \ldots + a_{nd}u_n = 0$$

και

$$a_{11}v_1 + \ldots + a_{n1}v_n = 0$$

$$a_{12}v_1 + \ldots + a_{n2}v_n = 0$$

$$\ldots$$

$$a_{1d}v_1 + \ldots + a_{nd}v_n = 0.$$

Είναι $A\mathbf{u}^\tau = 0 \Leftrightarrow \mathbf{u}^\tau \in \mathrm{Ker}_{\mathbf{Z}}A$ και $A\mathbf{v}^\tau = 0 \Leftrightarrow \mathbf{v}^\tau \in \mathrm{Ker}_{\mathbf{Z}}A$. Ακόμη έχουμε $u_1 + v_1 = 0, \ldots, u_n + v_n = 0$, δηλαδή $\mathbf{u}^\tau + \mathbf{v}^\tau = 0$ συνεπώς $\mathbf{v}^\tau = -\mathbf{u}^\tau$. Τα διανύσματα λοιπόν $\mathbf{u}^\tau, \mathbf{v}^\tau$ είναι αντίθετα.
Στην περίπτωση όπου έχουμε τον πίνακα $A^{(k)}$ είναι

$$\begin{pmatrix} A & 0 & \cdots & 0 & 0 \\ 0 & A & \cdots & 0 & 0 \\ 0 & 0 & A & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & A \\ I & I & I & I & I \end{pmatrix} \begin{pmatrix} u_{11} \\ \vdots \\ u_{1n} \\ u_{21} \\ \vdots \\ u_{2n} \\ \vdots \\ u_{k1} \\ \vdots \\ u_{kn} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Είναι $A\mathbf{u}^{(1)\tau} = 0, A\mathbf{u}^{(2)\tau} = 0, \ldots, A\mathbf{u}^{(k)\tau} = 0$. Συνεπώς τα διανύσματα $\mathbf{u}^{(1)\tau}, \mathbf{u}^{(2)\tau}, \ldots, \mathbf{u}^{(k)\tau}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}A$ και είναι $\mathbf{u}^{(1)\tau} + \ldots + \mathbf{u}^{(k)\tau} = 0$, όπου $\mathbf{u}^{(1)} = (u_{11}, \ldots, u_{1n}), \ldots, \mathbf{u}^{(k)} = (u_{k1}, \ldots, u_{kn})$.
Η διάσταση του πυρήνα του $A^{(r)}$ ισούται με $(r-1)(n-d)$ και ο πυρήνας του $A^{(r)}$ είναι ο εξής:

$$\mathrm{Ker}_{\mathbf{Z}}A^{(r)} = \{(\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(r)}) \in (\mathbf{Z}^n)^r : \mathbf{u}^{(i)} \in \mathrm{Ker}_{\mathbf{Z}}A \ \forall i \ , \sum \mathbf{u}^{(i)} = 0\}.$$

Ορισμός 4.1.1. *Ο πίνακας* $M(\mathbf{u})$ *που προέρχεται από το διάνυσμα* $\mathbf{u} \in (\mathbf{Z}^n)^r \subseteq (\mathbf{Q}^n)^r$ *είναι ο ακόλουθος:*

$$M(\mathbf{u}) = M(u_{11}, \ldots, u_{1n}, \ldots, u_{r1}, \ldots, u_{rn}) = \begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & \vdots & \vdots \\ u_{r1} & \cdots & u_{rn} \end{pmatrix},$$

όπου $\mathbf{u} = (\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(r)})$ *με* $\mathbf{u}^{(1)} = (u_{11}, \ldots, u_{1n}), \ldots, \mathbf{u}^{(r)} = (u_{r1}, \ldots, u_{rn})$.

Αν το διάνυσμα $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}A^{(r)}$ τότε ο πίνακας $M(\mathbf{u})$ είναι ο ακέραιος πίνακας του οποίου οι στήλες αθροίζουν στο μηδέν και οι γραμμές του ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}A$.

Θα δώσουμε ένα παράδειγμα ώστε να μας βοηθήσει να κατανοήσουμε καλύτερα την παραπάνω διαδικασία.

Παράδειγμα 4.1.2. Έστω ο πίνακας A :

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

Τότε ο πίνακας $A^{(3)}$ είναι ο 10×12 πίνακας :

$$A^{(3)} = \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \\ I & I & I \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Τότε ένα στοιχείο του πυρήνα είναι το εξής:

$$\begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \\ 1 \\ -2 \\ 1 \\ 0 \\ -1 \\ 1 \\ 1 \\ -1 \end{pmatrix}.$$

Ο αντίστοιχος πίνακας $M(\mathbf{u})$ είναι ο πίνακας:

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

Ακόμη παρατηρούμε πως οι στήλες του αθροίζουν στο μηδέν και οι γραμμές του ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$.

4.2 Πολυπλοκότητα Graver

Ορισμός 4.2.1. *Καλούμε* ***τύπο*** *ενός διανύσματος* $\mathbf{u} \in (\mathbb{Z}^n)^r \subseteq (\mathbb{Q}^n)^r$ *τον αριθμό των μη μηδενικών γραμμών του πίνακα* $M(\mathbf{u})$.

Ορισμός 4.2.2. *Η* ***πολυπλοκότητα Markov*** $m(A)$ *του* A *είναι ο μέγιστος τύπος των πινάκων της Markov βάσης του* $A^{(r)}$ *για οποιοδήποτε* r.

Ορισμός 4.2.3. *Η πολυπλοκότητα Graver $g(A)$ του A είναι ο μέγιστος τύπος των πινάκων της βάσης Graver του $A^{(r)}$ για οποιοδήποτε r.*

Παρατήρηση 4.2.4. Ισχύει $m(A) \leq g(A)$, αφού έχουμε αποδείξει ότι η καθολική βάση Markov είναι υποσύνολο της βάσης Graver όταν $(\mathbb{N}A^{(r)}) \bigcap -(\mathbb{N}A^{(r)}) = \{0\}$, για $r > 2$.

Παρατήρηση 4.2.5. Στη συνέχεια θα δούμε ένα πολύ σημαντικό θεώρημα στο οποίο θα αποδείξουμε ότι ο τύπος των πινάκων $M(u)$ σταθεροποιείται καθώς η r Lawrence άρση του A, $A^{(r)}$, αυξάνει για $r \geq 2$. Δηλαδή η πολυπλοκότητα Markov και Graver είναι ένας φυσικός αριθμός.

Παράδειγμα 4.2.6. Έστω $A = \{\mathbf{a}_1 = (3,0), \mathbf{a}_2 = (2,1), \mathbf{a}_3 = (1,2), \mathbf{a}_4 = (0,3)\} \subseteq \mathbb{Z}^2$. Ο πίνακας του A είναι ο εξής:

$$A = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

Θεωρούμε τον ομομορφισμό Φ,

$$\Phi : K[x_1, x_2, x_3, x_4] \to K[t_1, t_2], \text{ με } x_1 \to {t_1}^3, x_2 \to {t_1}^2 t_2, x_3 \to t_1 {t_2}^2, x_4 \to {t_2}^3$$

όπως αυτός ορίστηκε στο δεύτερο κεφάλαιο. Έτσι έχουμε :
$I_A = \mathrm{Ker}(\Phi) = \langle x_1x_3 - x_2^2, x_1x_4 - x_2x_3, x_2x_4 - x_3^2 \rangle$.
Η Markov βάση του A είναι το σύνολο των τριών διανυσμάτων

$$\{(1,-2,1,0), (1,-1,-1,1), (0,1,-2,1)\}$$

που αντιστοιχούν στους ελαχιστοτικούς γεννήτορες

$$\{x_1x_3 - x_2^2, x_1x_4 - x_2x_3, x_2x_4 - x_3^2\}$$

του ιδεώδους I_A.
Η Graver βάση του A είναι το σύνολο των πέντε διανυσμάτων

$$\{(1,-2,1,0), (1,-1,-1,1), (0,1,-2,1), (1,0,-3,2), (2,-3,0,1)\}.$$

Ο πίνακας $A^{(2)} = \begin{pmatrix} 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$ είναι ένας 8×8 πίνακας με βαθμίδα 6. Η διάσταση του πυρήνα του πίνακα $A^{(2)}$ ισούται με 2. Ενώ για τα στοιχεία του πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(2)}$ έχουμε ότι οι στήλες του αθροίζουν στο μηδέν και οι γραμμές του ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$.
Από το θεώρημα 2.3.4 η βάση Markov του $A^{(2)}$ είναι ίση με τη βάση Graver του $A^{(2)}$. Αποτελείται από πέντε πίνακες που προήλθαν από τη βάση Graver του A. Δηλαδή:

$$\mathrm{Markov}(A^{(2)}) = Gr_{A^{(2)}} = \{\begin{pmatrix} 1 & -2 & 1 & 0 \\ -1 & 2 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{pmatrix},$$

$$\left(\begin{array}{cccc} 0 & 1 & -2 & 1 \\ 0 & -1 & 2 & -1 \end{array}\right), \left(\begin{array}{cccc} 1 & 0 & -3 & 2 \\ -1 & 0 & 3 & -2 \end{array}\right), \left(\begin{array}{cccc} 2 & -3 & 0 & 1 \\ -2 & 3 & 0 & -1 \end{array}\right)\}.$$

Η τρίτη Lawrence άρση του πίνακα A είναι ο 10×12 πίνακας με βαθμίδα 8:

$$A^{(3)} = \left(\begin{array}{ccc} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \\ I & I & I \end{array}\right) = \left(\begin{array}{cccccccccccc} 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 3 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right).$$

Η διάσταση του πυρήνα του πίνακα $A^{(3)}$ ισούται με 4. Ενώ για τα στοιχεία του πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(3)}$ έχουμε ότι οι στήλες του αθροίζουν στο μηδέν και οι γραμμές του ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$.

Η βάση Markov του $A^{(3)}$ αποτελείται από 21 πίνακες:

$$\{\left(\begin{array}{cccc} 1 & -2 & 1 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right), \left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 \\ -1 & 2 & -1 & 0 \end{array}\right), \left(\begin{array}{cccc} -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 \end{array}\right),$$

$$\left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{array}\right), \left(\begin{array}{cccc} 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ -1 & 1 & 1 & -1 \end{array}\right), \left(\begin{array}{cccc} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

$$\left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 1 \\ 0 & -1 & 2 & -1 \end{array}\right), \left(\begin{array}{cccc} 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 \end{array}\right), \left(\begin{array}{cccc} 0 & 1 & -2 & 1 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 1 & 0 & -3 & 2 \\ -1 & 0 & 3 & -2 \end{array}\right), \left(\begin{array}{cccc} 1 & 0 & -3 & 2 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 3 & -2 \end{array}\right), \left(\begin{array}{cccc} 1 & 0 & -3 & 2 \\ -1 & 0 & 3 & -2 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\left(\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 2 & -3 & 0 & 1 \\ -2 & 3 & 0 & -1 \end{array}\right), \left(\begin{array}{cccc} 2 & -3 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ -2 & 3 & 0 & -1 \end{array}\right), \left(\begin{array}{cccc} 2 & -3 & 0 & 1 \\ -2 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

$$\left(\begin{array}{cccc} 0 & 1 & -2 & 1 \\ 1 & -2 & 1 & 0 \\ -1 & 1 & 1 & -1 \end{array}\right), \left(\begin{array}{cccc} 0 & 1 & -2 & 1 \\ -1 & 1 & 1 & -1 \\ 1 & -2 & 1 & 0 \end{array}\right), \left(\begin{array}{cccc} 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \\ -1 & 1 & 1 & -1 \end{array}\right)$$

$$\left(\begin{array}{cccc} 1 & -2 & 1 & 0 \\ -1 & 1 & 1 & -1 \\ 0 & 1 & -2 & 1 \end{array}\right), \left(\begin{array}{cccc} -1 & 1 & 1 & -1 \\ 0 & 1 & -2 & 1 \\ 1 & -2 & 1 & 0 \end{array}\right), \left(\begin{array}{cccc} -1 & 1 & 1 & -1 \\ 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{array}\right)\}.$$

Μπορεί να ελεγχθεί ότι δεν προστίθενται νέα στοιχεία στη βάση Markov του $A^{(r)}$ για $r \geq 4$, παρά μόνο μηδενικές γραμμές. Δηλαδή τα στοιχεία της βάσης Markov του $A^{(r)}$ για $r \geq 4$, σχηματίζονται με την προσθήκη μηδενικών γραμμών στα

στοιχεία της βάσης Markov του $A^{(3)}$. Για παράδειγμα ένα στοιχείο της βάσης Markov του $A^{(7)}$ είναι το εξής:

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

Παρατήρηση 4.2.7. Η συνεστραμμένη κυβική καμπύλη A έχει πολυπλοκότητα Markov $\mathrm{m}(A) = 3$. Η βάση Graver του $A^{(3)}$ αποτελείται από 87 πίνακες. Εικοσιένα από αυτούς είναι οι πίνακες που ανήκουν στη βάση Markov και τους έχουμε γράψει προηγουμένως. Οι υπόλοιποι 66 προέρχονται από μεταθέσεις γραμμών των παρακάτω 11 πινάκων:

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

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

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

$$\begin{pmatrix} -4 & 6 & 0 & -2 \\ 3 & -6 & 3 & 0 \\ 1 & 0 & -3 & 2 \end{pmatrix}, \begin{pmatrix} -2 & 0 & 6 & -4 \\ 0 & 3 & -6 & 3 \\ 2 & -3 & 0 & 1 \end{pmatrix}.$$

Μπορεί να υπολογίσει κανείς χρησιμοποιώντας το πρόγραμμα 4ti2 τις βάσεις Graver του $A^{(r)}$ για μεγαλύτερα r. Αυτό που παρατηρούμε είναι πρώτον ότι στον $A^{(6)}$ υπάρχει ένα στοιχείο με τύπο 6 το ακόλουθο:

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

Δεύτερον για $r > 6$ τα στοιχεία της βάσης Graver προέρχονται από στοιχεία της βάσης Graver του $A^{(6)}$ με την προσθήκη $r-6$ μηδενικών γραμμών. Παρατηρούμε λοιπόν ότι η πολυπλοκότητα Graver $g(A)$ είναι ίση με 6. Το λόγο που συμβαίνει αυτό θα τον καταλάβουμε στο θεώρημα 4.3.4.

Λήμμα 4.2.8. *Έστω το διάνυσμα* $\mathbf{u}$ *ανήκει στη βάση Graver του* $A^{(r)}$. *Υποθέτουμε ότι μια από τις γραμμές του* $r \times n$ *πίνακα* $M(\mathbf{u})$, *έστω η* $\mathbf{u}^{(i)}$, *έχει σύμμορφη παράσταση δηλαδή* $\mathbf{u}^{(i)} = \mathbf{u}_1^{(i)} +_c \ldots +_c \mathbf{u}_k^{(i)}$, *όπου* $\mathbf{u}_1^{(i)}, \ldots, \mathbf{u}_k^{(i)}$ *ανήκουν στον πυρήνα* $\mathrm{Ker}_{\mathbb{Z}} A$. *Τότε ο* $(r+k-1) \times n$ *πίνακας* $M(\mathbf{u}')$, *ο οποίος προέρχεται από την αντικατάσταση της γραμμής* $\mathbf{u}^{(i)}$ *από τις γραμμές* $\mathbf{u}_1^{(i)}, \ldots, \mathbf{u}_k^{(i)}$ *ανήκει στη βάση Graver του* $A^{(r+k-1)}$.

Απόδειξη. Υποθέτουμε ότι ο πίνακας $M(\mathbf{u}')$ δεν ανήκει στη βάση Graver του $A^{(r+k-1)}$, θα καταλήξουμε σε άτοπο. Αφού ο $M(\mathbf{u}')$ δεν ανήκει στη βάση Graver του $A^{(r+k-1)}$ συνεπάγεται σύμφωνα με την πρόταση 2.2.15 πως το διάνυσμα $\mathbf{u}'$ μπορεί να γραφεί ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων $\mathbf{v}', \mathbf{t}'$ του πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r+k-1)}$. Δηλαδή $\mathbf{u}' = \mathbf{v}' +_c \mathbf{t}'$ συνεπώς $\mathbf{u}' = \mathbf{v}' + \mathbf{t}'$ και $|u_{lm}| = |v'_{lm}| + |t'_{lm}|$ για $l = 1, ..., i_1, ..., i_k, ..., r$ και $m = 1, ..., n$, όπου $\mathbf{u}' = (\mathbf{u}^{(1)}, ..., \mathbf{u}_1^{(i)}, ..., \mathbf{u}_k^{(i)}, ..., \mathbf{u}^{(r)}), \mathbf{v}' = (\mathbf{v}'^{(1)}, ..., \mathbf{v}'^{(i)}_1, ..., \mathbf{v}'^{(i)}_k, ..., \mathbf{v}'^{(r)}), \mathbf{t}' = (\mathbf{t}'^{(1)}, ..., \mathbf{t}'^{(i)}_1, ..., \mathbf{t}'^{(i)}_k, ..., \mathbf{t}'^{(r)})$ με $\mathbf{u}^{(j)} = (u_{j1}, ..., u_{jn}), \mathbf{v}'^{(j)} = (v'_{j1}, ..., v'_{jn}), \mathbf{t}'^{(j)} = (t'_{j1}, ..., t'_{jn})$ για $j = 1, ..., i-1, i+1, ..., r$ και $\mathbf{u}_m^{(i)} = (u_{i_{m1}}, ..., u_{i_{mn}})$, $\mathbf{v}'^{(i)}_m = (v'_{i_{m1}}, ..., v'_{i_{mn}})$, $\mathbf{t}'^{(i)}_m = (t'_{i_{m1}}, ..., t'_{i_{mn}})$ για $m = 1, ..., k$.

Γνωρίζουμε ότι το διάνυσμα $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. Θα δείξουμε ότι το διάνυσμα $\mathbf{u}'$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r+k-1)}$.

Εφόσον το διάνυσμα $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$, έχουμε ότι τα διανύσματα $\mathbf{u}^{(1)}, ..., \mathbf{u}^{(i)}, ..., \mathbf{u}^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ και είναι $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(i)} + ... + \mathbf{u}^{(r)} = 0$.

Ισχύει ότι $\mathbf{u}^{(i)} = \mathbf{u}_1^{(i)} +_c ... +_c \mathbf{u}_k^{(i)}$ με $\mathbf{u}_1^{(i)}, ..., \mathbf{u}_k^{(i)} \in \mathrm{Ker}_{\mathbb{Z}}A$. Τότε είναι $\mathbf{u}^{(1)}, ..., \mathbf{u}^{(i-1)}, \mathbf{u}_1^{(i)}, \mathbf{u}_2^{(i)}, ..., \mathbf{u}_k^{(i)}, \mathbf{u}^{(i+1)}, ..., \mathbf{u}^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ και $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(i)} + ... + \mathbf{u}^{(r)} = 0$.

Συνεπώς τα διανύσματα $\mathbf{u}^{(1)}, ..., \mathbf{u}^{(i-1)}, \mathbf{u}_1^{(i)}, \mathbf{u}_2^{(i)}, ..., \mathbf{u}_k^{(i)}, \mathbf{u}^{(i+1)}, ..., \mathbf{u}^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ και $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(i-1)} + (\mathbf{u}_1^{(i)} + ... + \mathbf{u}_k^{(i)}) + \mathbf{u}^{(i+1)} + ... + \mathbf{u}^{(r)} = 0$.

Άρα πράγματι το διάνυσμα $\mathbf{u}' = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(i-1)}, \mathbf{u}_1^{(i)}, \mathbf{u}_2^{(i)}, ..., \mathbf{u}_k^{(i)}, \mathbf{u}^{(i+1)}, ..., \mathbf{u}^{(r)})$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r+k-1)}$.

Έχουμε ότι το διάνυσμα $\mathbf{u}^{(i)} = \mathbf{u}_1^{(i)} +_c ... +_c \mathbf{u}_k^{(i)}$ είναι σύμμορφο άθροισμα, δηλαδή ισχύει $\mathbf{u}^{(i)} = \mathbf{u}_1^{(i)} + ... + \mathbf{u}_k^{(i)}$ και $|u_{ij}| = |u_{i_{1j}}| + ... + |u_{i_{kj}}|$, όπου $i = 1, ..., k$ και $j = 1, ..., n$. Δηλαδή στον πίνακα $M(\mathbf{u}')$, τα στοιχεία $u_{i_{1j}}, ..., u_{i_{kj}}$ είναι ομόσημα. Από το σύμμορφο άθροισμα $\mathbf{u}' = \mathbf{v}' +_c \mathbf{t}'$, συνεπάγεται πως τα αντίστοιχα στοιχεία των πινάκων $M(\mathbf{v}'), M(\mathbf{t}')$ είναι ομόσημα. Συνεπώς έχουμε:

$|u_{im}| = |u_{i_{1m}} + ... + u_{i_{km}}| = |u_{i_{1m}}| + ... + |u_{i_{km}}| =$
$|v_{i_{1m}} + t_{i_{1m}}| + ... + |v_{i_{km}} + t_{i_{km}}| =$
$|v_{i_{1m}}| + |t_{i_{1m}}| + ... + |v_{i_{km}}| + |t_{i_{km}}|.$

Δηλαδή είναι $|u_{im}| = |v_{i_{1m}}| + ... + |v_{i_{km}}| + ... + |t_{i_{1m}}| + ... + |t_{i_{km}}|$.

Παρατηρούμε για το διάνυσμα $\mathbf{u}$ ότι ισχύει:

$$\mathbf{u} = \mathbf{v} + \mathbf{t},$$

όπου $\mathbf{v} = (\mathbf{v}'^{(1)}, ..., \mathbf{v}'^{(i)}, ..., \mathbf{v}'^{(r)})$ και $\mathbf{t} = (\mathbf{t}'^{(1)}, ..., \mathbf{t}'^{(i)}, ..., \mathbf{t}'^{(r)})$ θέτοντας $\mathbf{v}'^{(i)} = \mathbf{v}'^{(i)}_1 + ... + \mathbf{v}'^{(i)}_k$ και $\mathbf{t}'^{(i)} = \mathbf{t}'^{(i)}_1 + ... + \mathbf{t}'^{(i)}_k$. Ακόμη παρατηρούμε πως ισχύει $|u_{lm}| = |v'_{lm}| + |t'_{lm}|$ για $l = 1, ..., i_1, ..., i_k, ..., r$ και $m = 1, ..., n$. Απομένει να δείξουμε ότι τα διανύσματα $\mathbf{v}, \mathbf{t}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$.

Υποθέσαμε ότι τα διανύσματα $\mathbf{v}', \mathbf{t}'$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r+k-1)}$. Θα δείξουμε ότι τα διανύσματα $\mathbf{v}, \mathbf{t}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. Αρκεί να το δείξουμε για το διάνυσμα $\mathbf{v}$ όμοια αποδεικνύεται και για το διάνυσμα $\mathbf{t}$.

Εφόσον το διάνυσμα $\mathbf{v}'$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r+k-1)}$, έχουμε ότι τα διανύσματα $\mathbf{v}'^{(1)}, ..., \mathbf{v}'^{(i)}_1, \mathbf{v}'^{(i)}_2, ..., \mathbf{v}'^{(i)}_k, ..., \mathbf{v}'^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ και είναι $\mathbf{v}'^{(1)} + ... + \mathbf{v}'^{(i)}_1 + \mathbf{v}'^{(i)}_2 + ... + \mathbf{v}'^{(i)}_k, + ... + \mathbf{v}'^{(r)} = 0$.

Θέσαμε $\mathbf{v}'^{(i)} = \mathbf{v}'^{(i)}_1 + ... + \mathbf{v}'^{(i)}_k$ με το διάνυσμα $(\mathbf{v}'^{(i)}_1 + ... + \mathbf{v}'^{(i)}_k)$ να ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ αφού τα διανύσματα $\mathbf{v}'^{(i)}_1, ..., \mathbf{v}'^{(i)}_k$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$. Τότε είναι $\mathbf{v}'^{(1)}, ..., \mathbf{v}'^{(i)}, ..., \mathbf{v}'^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ και

$\mathbf{v}'^{(1)} + \ldots + \mathbf{v}'^{(i)} + \ldots + \mathbf{v}'^{(r)} = 0.$

Συνεπώς τα διανύσματα $\mathbf{v}'^{(1)}, \ldots, \mathbf{v}'^{(i)}, \ldots, \mathbf{v}'^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ και $\mathbf{v}'^{(1)}+\ldots+\mathbf{v}'^{(i)}+\ldots+\mathbf{v}'^{(r)} = 0$. Άρα πράγματι το διάνυσμα $\mathbf{v} = (\mathbf{v}'^{(1)}, \ldots, \mathbf{v}'^{(i)}, \ldots, \mathbf{v}'^{(r)})$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(r)}$. Όμοια και το διάνυσμα $\mathbf{t}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(r)}$.

Άρα αποδείξαμε ότι είναι $\mathbf{u} = \mathbf{v} +_c \mathbf{t}$ σύμμορφο άθροισμα με τα διανύσματα $\mathbf{v}, \mathbf{t}$ να ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(r)}$, άτοπο σύμφωνα με την πρόταση 2.2.15 αφού το διάνυσμα $\mathbf{u}$ ανήκει στη βάση Graver του $A^{(r)}$.

Για να γίνει περισσότερο κατανοητή η απόδειξη θα την παρουσιάσουμε με τη βοήθεια πινάκων. Είναι:

$$M(\mathbf{u}) = \begin{pmatrix} \mathbf{u}^{(1)} \\ \mathbf{u}^{(2)} \\ \cdot \\ \cdot \\ \mathbf{u}^{(i)} = \mathbf{u}_1^{(i)} + \ldots + \mathbf{u}_k^{(i)} \\ \cdot \\ \cdot \\ \mathbf{u}^{(r)} \end{pmatrix} = \begin{pmatrix} u_{11} & \cdot & \cdot & \cdot & u_{1n} \\ u_{21} & \cdot & \cdot & \cdot & u_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{i1} & \cdot & \cdot & \cdot & u_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{r1} & \cdot & \cdot & \cdot & u_{rn} \end{pmatrix}$$

$$= \begin{pmatrix} u_{11} & \cdot & \cdot & \cdot & u_{1n} \\ u_{21} & \cdot & \cdot & \cdot & u_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{i_{11}} + \ldots + u_{i_{k1}} & \cdot & \cdot & \cdot & u_{i_{1n}} + \ldots + u_{i_{kn}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{r1} & \cdot & \cdot & \cdot & u_{rn} \end{pmatrix}$$

λόγω του σύμμορφου αθροίσματος της γραμμής $\mathbf{u}^{(i)}$ του πίνακα $M(\mathbf{u})$.

Ο πίνακας $M(\mathbf{u}')$ είναι ο εξής:

$$M(\mathbf{u}') = \begin{pmatrix} \mathbf{u}^{(1)} \\ \mathbf{u}^{(2)} \\ \cdot \\ \cdot \\ \mathbf{u}^{(i-1)} \\ \mathbf{u}_1^{(i)} \\ \cdot \\ \cdot \\ \cdot \\ \mathbf{u}_k^{(i)} \\ \mathbf{u}^{(i+1)} \\ \cdot \\ \cdot \\ \mathbf{u}^{(r)} \end{pmatrix} = \begin{pmatrix} u_{11} & \cdot & \cdot & \cdot & u_{1n} \\ u_{21} & \cdot & \cdot & \cdot & u_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{i_{11}} & \cdot & \cdot & \cdot & u_{i_{1n}} \\ u_{i_{21}} & \cdot & \cdot & \cdot & u_{i_{2n}} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{i_{k1}} & \cdot & \cdot & \cdot & u_{i_{kn}} \\ u_{i+11} & \cdot & \cdot & \cdot & u_{i+1n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{r1} & \cdot & \cdot & \cdot & u_{rn} \end{pmatrix}$$

Όμως το $\mathbf{u}'$ είναι σύμμορφο άθροισμα των $\mathbf{v}'$ και $\mathbf{t}'$ άρα:

$$M(\mathbf{u}') = \begin{pmatrix} \mathbf{u}^{(1)} \\ \mathbf{u}^{(2)} \\ . \\ . \\ \mathbf{u}^{(i-1)} \\ \mathbf{u}_1^{(i)} \\ . \\ . \\ . \\ \mathbf{u}_k^{(i)} \\ \mathbf{u}^{(i+1)} \\ . \\ . \\ \mathbf{u}^{(r)} \end{pmatrix} = \begin{pmatrix} \mathbf{v}'^{(1)} \\ \mathbf{v}'^{(2)} \\ . \\ . \\ \mathbf{v}'^{(i-1)} \\ \mathbf{v}'_1{}^{(i)} \\ . \\ . \\ . \\ \mathbf{v}'_k{}^{(i)} \\ \mathbf{v}'^{(i+1)} \\ . \\ . \\ \mathbf{v}'^{(r)} \end{pmatrix} + \begin{pmatrix} \mathbf{t}'^{(1)} \\ \mathbf{t}'^{(2)} \\ . \\ . \\ \mathbf{t}'^{(i-1)} \\ \mathbf{t}'_1{}^{(i)} \\ . \\ . \\ . \\ \mathbf{t}'_k{}^{(i)} \\ \mathbf{t}'^{(i+1)} \\ . \\ . \\ \mathbf{t}'^{(r)} \end{pmatrix}$$

Άρα είναι:

$$M(\mathbf{u}') = \begin{pmatrix} u_{11} & . & . & . & u_{1n} \\ u_{21} & . & . & . & u_{2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{i_11} & . & . & . & u_{i_1n} \\ u_{i_21} & . & . & . & u_{i_2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{i_k1} & . & . & . & u_{i_kn} \\ u_{i+11} & . & . & . & u_{i+1n} \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{r1} & . & . & . & u_{rn} \end{pmatrix} = \begin{pmatrix} v_{11} & . & . & . & v_{1n} \\ v_{21} & . & . & . & v_{2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ v_{i_11} & . & . & . & v_{i_1n} \\ v_{i_21} & . & . & . & v_{i_2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ v_{i_k1} & . & . & . & v_{i_kn} \\ v_{i+11} & . & . & . & v_{i+1n} \\ . & . & . & . & . \\ . & . & . & . & . \\ v_{r1} & . & . & . & v_{rn} \end{pmatrix} + \begin{pmatrix} t_{11} & . & . & . & t_{1n} \\ t_{21} & . & . & . & t_{2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ t_{i_11} & . & . & . & t_{i_1n} \\ t_{i_21} & . & . & . & t_{i_2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ t_{i_k1} & . & . & . & t_{i_kn} \\ t_{i+11} & . & . & . & t_{i+1n} \\ . & . & . & . & . \\ . & . & . & . & . \\ t_{r1} & . & . & . & t_{rn} \end{pmatrix}$$

Όμως δείξαμε ότι:

$$M(\mathbf{u}) = \begin{pmatrix} u_{11} & . & . & . & u_{1n} \\ u_{21} & . & . & . & u_{2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{i_11} + \ldots + u_{i_k1} & . & . & . & u_{i_1n} + \ldots + u_{i_kn} \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{r1} & . & . & . & u_{rn} \end{pmatrix} =$$

$$\begin{pmatrix} u_{11} & . & . & . & u_{1n} \\ u_{21} & . & . & . & u_{2n} \\ . & . & . & . & . \\ . & . & . & . & . \\ (v_{i_11} + t_{i_11}) + \ldots + (v_{i_k1} + t_{i_k1}) & . & . & . & (v_{i_1n} + t_{i_1n}) + \ldots + (v_{i_kn} + t_{i_kn}) \\ . & . & . & . & . \\ . & . & . & . & . \\ u_{r1} & . & . & . & u_{rn} \end{pmatrix}$$

η συνέπεια του σύμμορφου αθροίσματος $\mathbf{u}' = \mathbf{v}' +_c \mathbf{t}'$ στη γραμμή $\mathbf{u}^{(i)}$ του πίνακα $M(\mathbf{u})$.

$$M(\mathbf{u}) = \begin{pmatrix} (v_{11}+t_{11}) & \cdots & (v_{1n}+t_{1n}) \\ (u_{21}+t_{21}) & \cdots & (u_{2n}+t_{1n}) \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ (v_{i_{11}}+t_{i_{11}})+\ldots+(v_{i_{k1}}+t_{i_{k1}}) & \cdots & (v_{i_{1n}}+t_{i_{1n}})+\ldots+(v_{i_{kn}}+t_{i_{kn}}) \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ (v_{r1}+t_{r1}) & \cdots & (v_{rn}+t_{rn}) \end{pmatrix}$$

η συνέπεια του σύμμορφου αθροίσματος $\mathbf{u}' = \mathbf{v}' +_c \mathbf{t}'$ στις υπόλοιπες γραμμές του πίνακα $M(\mathbf{u})$. Άρα τελικά έχουμε: $M(\mathbf{u}) =$

$$\begin{pmatrix} v_{11} & \cdots & v_{1n} \\ v_{21} & \cdots & v_{2n} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ v_{i_{11}}+\ldots+v_{i_{k1}} & \cdots & v_{i_{1n}}+\ldots+v_{i_{kn}} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ v_{r1} & \cdots & v_{rn} \end{pmatrix} + \begin{pmatrix} t_{11} & \cdots & t_{1} \\ t_{21} & \cdots & t_{2} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ t_{i_{11}}+\ldots+t_{i_{k1}} & \cdots & t_{i_{1n}}+\ldots \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ t_{r1} & \cdots & t_{rn} \end{pmatrix}$$

δηλαδή $\mathbf{u} = \mathbf{v} +_c \mathbf{t}$, όπου

$$M(\mathbf{v}) = \begin{pmatrix} v_{11} & \cdots & v_{1n} \\ v_{21} & \cdots & v_{2n} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ v_{i_{11}}+\ldots+v_{i_{k1}} & \cdots & v_{i_{1n}}+\ldots+v_{i_{kn}} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ v_{r1} & \cdots & v_{rn} \end{pmatrix},$$

$$M(\mathbf{t}) = \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ t_{21} & \cdots & t_{2n} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ t_{i_{11}}+\ldots+t_{i_{k1}} & \cdots & t_{i_{1n}}+\ldots+t_{i_{kn}} \\ \vdots & \cdots & \vdots \\ \vdots & \cdots & \vdots \\ t_{r1} & \cdots & t_{rn} \end{pmatrix}$$

□

Ορισμός 4.2.9. *Έστω $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ βάση Graver κάποιου συνόλου διανυσμάτων A. Θα ορίσουμε το B^r, $r \geq s$, ως εξής:*

$$B^r = \{(\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(r)}) / \mathbf{u}^{(i)} \in B \text{ ή } -\mathbf{u}^{(i)} \in B \text{ ή } \mathbf{u}^{(i)} = 0 \text{ για } i = 1, \ldots, r\}.$$

Πόρισμα 4.2.10. *Κάθε στοιχείο $\mathbf{u}$ της βάσης Graver του $A^{(r)}$ μπορεί να δοθεί μέσω σύμμορφης πρόσθεσης γραμμών ενός στοιχείου $\mathbf{u}'$ της βάσης Graver του $A^{(s)}$, με $s > r$, με την ιδιότητα κάθε μη μηδενική γραμμή του $\mathbf{u}'$ να ανήκει στη βάση Graver του A.*

Απόδειξη. Έστω $\mathbf{u}$ ένα στοιχείο της βάσης Graver του $A^{(r)}$. Έστω $\mathbf{u}^{(1)}$ η πρώτη γραμμή του πίνακα $M(\mathbf{u})$. Η $\mathbf{u}^{(1)}$ μπορεί να ανήκει στη βάση Graver του A, μπορεί και όχι.
Έστω ότι η $\mathbf{u}^{(1)}$ δεν ανήκει στη βάση Graver του A. Τότε σύμφωνα με την πρόταση

2.2.15, το $\mathbf{u}^{(1)}$ μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών διανυσμάτων $\mathbf{a}, \mathbf{b}$, δηλαδή $\mathbf{u}^{(1)} = \mathbf{a} +_c \mathbf{b}$ με τα διανύσματα $\mathbf{a}, \mathbf{b}$ να ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ και $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$. Ο πίνακας που προέρχεται από την αντικατάσταση του διανύσματος $\mathbf{u}^{(1)}$ από τα διανύσματα $\mathbf{a}, \mathbf{b}$ ανήκει στη βάση Graver του $A^{(r+1)}$, σύμφωνα με το λήμμα 4.2.8.
Συνεχίζουμε με το διάνυσμα $\mathbf{a}$. Το διάνυσμα $\mathbf{a}$ είτε ανήκει στη βάση Graver του A, είτε όχι. Έστω ότι το $\mathbf{a}$ δεν ανήκει στη βάση Graver του A. Τότε σύμφωνα με την πρόταση 2.2.15 το $\mathbf{a}$ μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών διανυσμάτων $\mathbf{d}, \mathbf{e}$ δηλαδή $\mathbf{a} = \mathbf{d} +_c \mathbf{e}$ με τα διανύσματα $\mathbf{d}, \mathbf{e}$ να ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ και $\mathbf{d}, \mathbf{e} \in \mathbb{Z}^n$. Ο πίνακας που προέρχεται από την αντικατάσταση του διανύσματος $\mathbf{a}$ από τα διανύσματα $\mathbf{d}, \mathbf{e}$ ανήκει στη βάση Graver του $A^{(r+2)}$.
Συνεχίζουμε με το διάνυσμα $\mathbf{b}$. Το διάνυσμα $\mathbf{b}$ είτε ανήκει στη βάση Graver του A, είτε όχι. Έστω ότι το $\mathbf{b}$ δεν ανήκει στη βάση Graver του A. Τότε σύμφωνα με την πρόταση 2.2.15 το $\mathbf{b}$ μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών διανυσμάτων $\mathbf{m}, \mathbf{n}$ δηλαδή $\mathbf{b} = \mathbf{m} +_c \mathbf{n}$ με τα διανύσματα $\mathbf{m}, \mathbf{n}$ να ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ και $\mathbf{m}, \mathbf{n} \in \mathbb{Z}^n$. Ο πίνακας που προέρχεται από την αντικατάσταση του διανύσματος $\mathbf{b}$ από τα διανύσματα $\mathbf{m}, \mathbf{n}$ ανήκει στη βάση Graver του $A^{(r+3)}$.
Συνεχίζουμε κατά αυτόν τον τρόπο αντικαθιστώντας τα στοιχεία εκείνα που δεν ανήκουν στη βάση Graver του A, με τα σύμμορφα αθροίσματα τους. Η διαδικασία αυτή τερματίζει κάποια στιγμή. Πράγματι θεωρούμε το σύμμορφο άθροισμα

$$\mathbf{u} = \mathbf{u}_1 +_c \mathbf{u}_2.$$

Τότε έχουμε $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$ και $\mid u_i \mid = \mid u_{1i} \mid + \mid u_{2i} \mid$, όπου $\mathbf{u} = (u_1, ..., u_n), \mathbf{u}_1 = (u_{11}, ..., u_{1n}), \mathbf{u}_2 = (u_{21}, ..., u_{2n})$. Αν κοιτάξουμε την $1-$νόρμα του διανύσματος $\mathbf{u}$ παρατηρούμε ότι είναι:

$$\| \mathbf{u} \|_1 = \| \mathbf{u}_1 \|_1 + \| \mathbf{u}_2 \|_1$$

αφού $\| \mathbf{u} \|_1 = \mid u_1 \mid + ... + \mid u_n \mid = \mid u_{11} \mid + \mid u_{21} \mid ... + \mid u_{1n} \mid + \mid u_{2n} \mid$. Όπου ισχύει $\| \mathbf{u} \|_1 > \| \mathbf{u}_1 \|_1$. Το διάνυσμα $\mathbf{u}_1$ μπορεί να ανήκει στη βάση Graver του A, μπορεί και όχι. Έστω ότι το $\mathbf{u}_1$ δεν ανήκει στη βάση Graver του A. Τότε σύμφωνα με την πρόταση 2.2.15, το $\mathbf{u}_1$ μπορεί να γραφεί ως σύμμορφο άθροισμα δύο μη μηδενικών διανυσμάτων $\mathbf{u}_{11}, \mathbf{u}_{12}$, δηλαδή $\mathbf{u}_1 = \mathbf{u}_{11} +_c \mathbf{u}_{12}$ με τα διανύσματα $\mathbf{u}_{11}, \mathbf{u}_{12}$ να ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$ και $\mathbf{u}_{11}, \mathbf{u}_{12} \in \mathbb{Z}^n$. Όπου ισχύει $\| \mathbf{u}_1 \|_1 > \| \mathbf{u}_{11} \|_1$. Οπότε συνολικά έχουμε

$$\| \mathbf{u} \|_1 > \| \mathbf{u}_1 \|_1 > \| \mathbf{u}_{11} \|_1 > ...$$

Όμως δεν υπάρχει φθίνουσα ακολουθία φυσικών αριθμών, συνεπώς κάποια στιγμή θα έχουμε

$$\| \mathbf{u}_{km} \|_1 = \| \mathbf{u}_{km} \|_1 + 0,$$

για κάποιους φυσικούς αριθμούς k, m. Έτσι το διάνυσμα $\mathbf{u}_{km}$ δεν αναλύεται σε περαιτέρω σύμμορφο άθροισμα, άρα ανήκει στη βάση Graver του A. Έτσι καταλήγουμε σε κάποιο πίνακα $M(\mathbf{u}')$ ο οποίος ανήκει στη βάση Graver του $A^{(s)}$, σύμφωνα με το λήμμα 4.2.8 με $s > r$. Είμαστε βέβαιοι ότι κάθε γραμμή του $M(\mathbf{u}')$ ανήκει στη βάση Graver του A, διότι διαφορετικά θα συνεχιζόταν η διαδικασία ανάλυσης των γραμμών που δεν ανήκουν, σε σύμμορφα αθροίσματα έως ότου κάθε γραμμή να μην μπορεί να σπάσει σε περαιτέρω σύμμορφα αθροίσματα, με συνέπεια κάθε γραμμή του $M(\mathbf{u}')$ να ανήκει στη βάση Graver του A. □

Παρατήρηση 4.2.11. Αν το διάνυσμα $\mathbf{u}$ ανήκει στη βάση Graver του $A^{(r)}$, τότε υπάρχει ένα διάνυσμα $\mathbf{u}'$ το οποίο ανήκει στη βάση Graver του $A^{(s)}$, με $r < s$, τέτοιο ώστε το διάνυσμα $\mathbf{u}$ να δίνεται ως σύμμορφη πρόσθεση γραμμών του πίνακα $M(\mathbf{u}')$ το αντίστροφο δεν ισχύει, όπως φαίνεται και στο παρακάτω παράδειγμα.

Παράδειγμα 4.2.12. Έστω το σύνολο διανυσμάτων $A = \{1, 2, 1\}$, τότε ο αντίστοιχος πίνακας είναι ο εξής:

$$A = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix}.$$

Ο πίνακας

$$M(\mathbf{u}') = \begin{pmatrix} 0 & -1 & 2 \\ 2 & -1 & 0 \\ -1 & 1 & -1 \\ -1 & 1 & -1 \end{pmatrix}$$

ανήκει στη βάση Graver $Gr_{A^{(4)}}$. Ο πίνακας που προέρχεται από το σύμμορφο άθροισμα των γραμμών $\mathbf{u}'^{(3)}$ και $\mathbf{u}'^{(4)}$ είναι ο εξής:

$$M(\mathbf{u}) = \begin{pmatrix} 0 & -1 & 2 \\ 2 & -1 & 0 \\ -2 & 2 & -2 \end{pmatrix}.$$

Ο οποίος δεν ανήκει στη βάση $Gr_{A^{(3)}}$.
Θα δείξουμε ότι το διάνυσμα $\mathbf{u} = ((0,-1,2),(2,-1,0),(-2,2,-2))$ γράφεται ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων $\mathbf{a}, \mathbf{b}$, δηλαδή είναι $\mathbf{u} = \mathbf{a} +_c \mathbf{b}$ όπου τα διανύσματα $\mathbf{a}, \mathbf{b}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(3)}$. Έστω:

$$\mathbf{a} = ((0,-1,2),(0,0,0),(0,1,-2))$$

$$\mathbf{b} = ((0,0,0),(2,-1,0),(-2,1,0)).$$

Οπότε έχουμε:

$$\begin{pmatrix} 0 & -1 & 2 \\ 2 & -1 & 0 \\ -2 & 2 & -2 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 2 \\ 0 & 0 & 0 \\ 0 & 1 & -2 \end{pmatrix} +_c \begin{pmatrix} 0 & 0 & 0 \\ 2 & -1 & 0 \\ -2 & 1 & 0 \end{pmatrix}$$

Δηλαδή είναι $\mathbf{u} = \mathbf{a} + \mathbf{b}$ και τα στοιχεία u_{ij}, a_{ij}, b_{ij}, $1 \le i, j \le 3$ είναι ομόσημα.
Άρα ισχύει $\mathbf{u} = \mathbf{a} +_c \mathbf{b}$, μένει να δείξουμε ότι τα διανύσματα $\mathbf{a}, \mathbf{b}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(3)}$.

Παρατηρούμε ότι $A(\mathbf{a}^{(1)})^\tau = \begin{pmatrix} 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ -1 \\ 2 \end{pmatrix} = 0$ όμοια,

$$A(\mathbf{a}^{(2)})^\tau = 0, A(\mathbf{a}^{(3)})^\tau = 0.$$

Δηλαδή τα διανύσματα $\mathbf{a}^{(1)^\tau}, \mathbf{a}^{(2)^\tau}, \mathbf{a}^{(3)^\tau}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$.
Ακόμη είναι $\mathbf{a}^{(1)^\tau} + \mathbf{a}^{(2)^\tau} + \mathbf{a}^{(3)^\tau} = (0,0,0)$. Άρα το διάνυσμα $\mathbf{a}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A^{(3)}$.
Παρατηρούμε ότι:

$$A(\mathbf{b}^{(1)})^\tau = 0, A(\mathbf{b}^{(2)})^\tau = 0, A(\mathbf{b}^{(3)})^\tau = 0.$$

Δηλαδή τα διανύσματα $\mathbf{b}^{(1)^\tau}, \mathbf{b}^{(2)^\tau}, \mathbf{b}^{(3)^\tau}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}} A$.
Ακόμη είναι $\mathbf{b}^{(1)^\tau} + \mathbf{b}^{(2)^\tau} + \mathbf{b}^{(3)^\tau} = (0,0,0)$. Άρα το διάνυσμα $\mathbf{b}$ ανήκει στον

πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(3)}$.
Συνεπώς τα διανύσματα $\mathbf{a}, \mathbf{b}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(3)}$, οπότε έχουμε σύμμορφο άθροισμα. Άρα το διάνυσμα $\mathbf{u}$ σύμφωνα με την πρόταση 2.2.15, δεν ανήκει στη βάση Graver του $A^{(3)}$, παρόλο που το διάνυσμα $\mathbf{u}'$ ανήκει στη βάση Graver $Gr_{A^{(4)}}$.

Λήμμα 4.2.13. *Έστω το σύνολο διανυσμάτων $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ είναι η βάση Graver του A. Αν το διάνυσμα $\mathbf{u} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)})$ είναι στοιχείο της βάσης Graver του $A^{(r)}$ και $\mathbf{u} \in B^r$, τότε ισχύει $\mathbf{u}^{(i)} \neq -\mathbf{u}^{(j)}$ για κάθε $i, j = 1, ..., s$ και $r > 2$.*

Απόδειξη. Υποθέτουμε ότι ισχύει $\mathbf{u}^{(i)} = -\mathbf{u}^{(j)}$ για κάποια i, j, θα καταλήξουμε σε άτοπο. Διακρίνουμε περιπτώσεις για τα i, j.
1η περίπτωση
Αν $i = j$ τότε $\mathbf{u}^{(i)} = -\mathbf{u}^{(i)} \Rightarrow 2\mathbf{u}^{(i)} = \mathbf{0} \Rightarrow \mathbf{u}^{(i)} = \mathbf{0}$, άτοπο αφού το $\mathbf{u}^{(i)} \in B$.
2η περίπτωση
Αν $i \neq j$ τότε έχουμε
$\mathbf{u} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(i-1)}, \mathbf{0}, \mathbf{u}^{(i+1)}, ..., \mathbf{u}^{(j-1)}, \mathbf{0}, \mathbf{u}^{(j+1)}, ..., \mathbf{u}^{(r)}) +_c$
$(\mathbf{0}, ..., \mathbf{0}, \mathbf{u}^{(i)}, \mathbf{0}, ..., \mathbf{0}, \mathbf{u}^{(j)}, \mathbf{0}, ..., \mathbf{0})$.
Το άθροισμα αυτό είναι σύμμορφο. Πράγματι, παρατηρούμε πως

$$| u_{km} | = | u_{km} + 0 | = | u_{km} | + 0,$$

για κάθε $1 \leq k \leq r$ και $1 \leq m \leq n$. Πιο αναλυτικά, χρησιμοποιώντας τους συμβολισμούς του ορισμού του σύμμορφου αθροίσματος, θέτουμε

$$\mathbf{a} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(i-1)}, \mathbf{0}, \mathbf{u}^{(i+1)}, ..., \mathbf{u}^{(j-1)}, \mathbf{0}, \mathbf{u}^{(j+1)}, ..., \mathbf{u}^{(r)})$$

και

$$\mathbf{b} = (\mathbf{0}, ..., \mathbf{0}, \mathbf{u}^{(i)}, \mathbf{0}, ..., \mathbf{0}, \mathbf{u}^{(j)}, \mathbf{0}, ..., \mathbf{0}).$$

Παρατηρούμε ότι είναι $\mathbf{a}^{(i)} = \mathbf{0}$ και $\mathbf{b}^{(i)} = \mathbf{u}^{(i)}$ και $\mathbf{a}^{(j)} = \mathbf{0}$ και $\mathbf{b}^{(j)} = \mathbf{u}^{(j)}$. Ενώ για τα υπόλοιπα $k = 1, ..., r - \{i, j\}$ ισχύει ότι $\mathbf{a}^{(k)} = \mathbf{u}^{(k)}$ και $\mathbf{b}^{(k)} = \mathbf{0}$. Άρα πληρείται η συνθήκη του ορισμού του σύμμορφου αθροίσματος, μένει τώρα να δείξουμε ότι τα $\mathbf{a}, \mathbf{b}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$.
Αφού το διάνυσμα $\mathbf{u} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)})$ ανήκει στη βάση Graver του $A^{(r)}$ έχουμε ότι το $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. Συνεπώς τα διανύσματα $\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ και $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(i)} + ... + \mathbf{u}^{(j)} + ...\mathbf{u}^{(r)} = \mathbf{0}$.
Συνεπώς για το διάνυσμα $\mathbf{a}$ έχουμε:
$\mathbf{u}^{(1)}, ...\mathbf{u}^{(i-1)}, \mathbf{u}^{(i+1)}, ..., \mathbf{u}^{(j-1)}, \mathbf{u}^{(j+1)}, ...\mathbf{u}^{(r)} \in \mathrm{Ker}_{\mathbb{Z}}A$ και
$\mathbf{u}^{(1)} + ... + \mathbf{u}^{(i-1)} + \mathbf{u}^{(i+1)} + ... + \mathbf{u}^{(j-1)} + \mathbf{u}^{(j+1)} + .. + \mathbf{u}^{(r)} = -\mathbf{u}^{(i)} - \mathbf{u}^{(j)}$ άρα
$\mathbf{u}^{(1)} + ... + \mathbf{u}^{(i-1)} + \mathbf{u}^{(i+1)} + ... + \mathbf{u}^{(j-1)} + \mathbf{u}^{(j+1)} + .. + \mathbf{u}^{(r)} = -\mathbf{u}^{(i)} - (-\mathbf{u}^{(i)}) = \mathbf{0}$.
Συνεπώς το διάνυσμα $\mathbf{a}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$.
Για το διάνυσμα $\mathbf{b}$ έχουμε:
$\mathbf{u}^{(i)}, \mathbf{u}^{(j)} \in \mathrm{Ker}_{\mathbb{Z}}A$ και
$\mathbf{0} + ...\mathbf{0} + \mathbf{u}^{(i)} + \mathbf{0} + ... + \mathbf{0} + \mathbf{u}^{(j)} + \mathbf{0} + ... + \mathbf{0} = \mathbf{u}^{(i)} + \mathbf{u}^{(j)} = \mathbf{u}^{(i)} + (-\mathbf{u}^{(i)}) = \mathbf{0}$.
Συνεπώς το $\mathbf{b}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. Άρα το διάνυσμα $\mathbf{u}$ το γράψαμε ως σύμμορφο άθροισμα διανυσμάτων που ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. Άτοπο αφού εξ' υποθέσεως το διάνυσμα $\mathbf{u}$ ανήκει στη βάση Graver του $A^{(r)}$, δηλαδή δεν μπορεί να γραφεί ως σύμμορφο άθροισμα διανυσμάτων που ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. □

Παρατήρηση 4.2.14. Κάθε σώμα έχει χαρακτηριστική, το μηδέν ή πρώτο αριθμό. Επειδή το σώμα $\mathbb{Q}$ έχει χαρακτηριστική μηδέν γι' αυτό στην απόδειξη του

λήμματος 4.2.13 συμπεραίνουμε από τη σχέση $2\mathbf{u}^{(i)} = 0$ πως το διάνυσμα είναι $\mathbf{u}^{(i)} = 0$.

Παρατήρηση 4.2.15. Το λήμμα 4.2.13 συνεπάγεται πως αν $\mathbf{u}^{(i)} = \mathbf{b}_j$ για κάποια i, j τότε δεν υπάρχει $k \neq i$ τέτοιο ώστε $\mathbf{u}^{(k)} = -\mathbf{b}_j$, για $1 \leqslant k \leqslant r$, κι αντίστοιχα αν $\mathbf{u}^{(i)} = -\mathbf{b}_j$ τότε δεν υπάρχει $k \neq i$ τέτοιο ώστε $\mathbf{u}^{(k)} = \mathbf{b}_j$, για $1 \leqslant k \leqslant r$. Συνεπώς αν το διάνυσμα $\mathbf{u}$ ανήκει στη βάση Graver και $\mathbf{u} \in B^r$ και μια γραμμή του πίνακα $M(\mathbf{u})$ είναι ίση με το $\mathbf{b}_j$ τότε καμία άλλη γραμμή του πίνακα $M(\mathbf{u})$ δεν μπορεί να είναι ίση με το $-\mathbf{b}_j$, για $r > 2$.

Ορισμός 4.2.16. *Έστω το διάνυσμα $\mathbf{u}$ ανήκει στο σύνολο B^r, όπου το σύνολο $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ είναι η βάση Graver κάποιου συνόλου διανυσμάτων A. Έστω $\psi(\mathbf{u}) = (\psi(\mathbf{u})_1, ..., \psi(\mathbf{u})_s)$. Θα ορίσουμε το $\psi(\mathbf{u})_j$, για $1 \leq j \leq s$, ως εξής:*
Το $\psi(\mathbf{u})_j$ ισούται με λ, αν το $\mathbf{b}_j$ εμφανίζεται λ φορές στον πίνακα $M(\mathbf{u})$. Ενώ το $\psi(\mathbf{u})_j$ ισούται με $-\lambda$, αν το $-\mathbf{b}_j$ εμφανίζεται λ φορές στον πίνακα $M(\mathbf{u})$.

Παράδειγμα 4.2.17. Έστω το σύνολο $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4, \mathbf{b}_5, \mathbf{b}_6\}$ αποτελεί βάση Graver κάποιου συνόλου διανυσμάτων A. Τότε αν ο πίνακας κάποιου διανύσματος $\mathbf{u}$ είναι ο ακόλουθος

$$M(\mathbf{u}) = \begin{pmatrix} \mathbf{b}_2 \\ \mathbf{b}_3 \\ -\mathbf{b}_1 \\ -\mathbf{b}_1 \\ \mathbf{b}_2 \\ \mathbf{b}_6 \\ -\mathbf{b}_4 \end{pmatrix}$$

έχουμε $\psi(\mathbf{u}) = (\psi(\mathbf{u})_1, \psi(\mathbf{u})_2, \psi(\mathbf{u})_3, \psi(\mathbf{u})_4, \psi(\mathbf{u})_5, \psi(\mathbf{u})_6) = (-2, 2, 1, -1, 0, 1)$. Το $-\mathbf{b}_1$ εμφανίζεται 2 φορές στον πίνακα $M(\mathbf{u})$, συνεπώς είναι $\psi(\mathbf{u})_1 = -2$. Ενώ το $\mathbf{b}_2$ εμφανίζεται 2 φορές στον $M(\mathbf{u})$ συνεπώς είναι $\psi(\mathbf{u})_2 = 2$. Το $\mathbf{b}_3$ εμφανίζεται 1 φορά συνεπώς είναι $\psi(\mathbf{u})_3 = 1$, το $-\mathbf{b}_4$ εμφανίζεται επίσης 1 φορά άρα είναι $\psi(\mathbf{u})_4 = -1$. Καμία φορά το $\mathbf{b}_5$, άρα $\psi(\mathbf{u})_5 = 0$. Τέλος το $\mathbf{b}_6$ εμφανίζεται 1 φορά στον πίνακα $M(\mathbf{u})$, συνεπώς $\psi(\mathbf{u})_6 = 1$.

Πρόταση 4.2.18. *Έστω $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ η βάση Graver κάποιου συνόλου διανυσμάτων A. Το διάνυσμα $\mathbf{u} \in B^r$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} A^{(r)}$ αν και μόνο αν το διάνυσμα $\psi(\mathbf{u})$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$.*

Απόδειξη. Έστω ότι το $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} A^{(r)}$ και $\mathbf{u}$ ανήκει στο B^r θα δείξουμε ότι το $\psi(\mathbf{u})$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} B$. Δηλαδή

$$\mathbf{b}_1\psi(\mathbf{u})_1 + ... + \mathbf{b}_s\psi(\mathbf{u})_s = 0.$$

Είναι $\mathbf{u} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)})$ με:

$M(\mathbf{u}) = \begin{pmatrix} \mathbf{u}^{(1)} \\ . \\ . \\ . \\ \mathbf{u}^{(r)} \end{pmatrix}$. Όπου το διάνυσμα $\mathbf{u}$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} A^{(r)}$. Συνεπώς έχουμε ότι τα διανύσματα $\mathbf{u}^{(1)^T}, ..., \mathbf{u}^{(r)^T}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}} A$ και $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(r)} = 0$. Ακόμη αφού το διάνυσμα $\mathbf{u}$ ανήκει στο σύνολο B^r συνεπάγεται ότι $\mathbf{u}^{(i)} \in B$ ή $-\mathbf{u}^{(i)} \in B$ ή $\mathbf{u}^{(i)} = 0$. Άρα καθένα από τα μη μηδενικά

$\mathbf{u}^{(i)}$ του πίνακα $M(\mathbf{u})$ ισούται το ίδιο ή το αντίθετο του, με κάποιο στοιχείο του B. Αυτό σημαίνει ότι κάποια $\mathbf{b}_k$ μπορεί να εμφανίζονται περισσότερες φορές από μία. Από τη σχέση $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(r)} = 0$ συνεπάγεται ότι το άθροισμα των $\mathbf{u}^{(i)}$ για $i = 1, ..., r$ ισούται με το μηδέν δηλαδή το άθροισμα των $\mathbf{b}_1, ..., \mathbf{b}_s$ επί την πολλαπλότητα εμφάνισης των, ισούται με το μηδέν. Άρα από τον ορισμό του $\psi(\mathbf{u})_j$ έχουμε:
$\mathbf{u}^{(1)} + ... + \mathbf{u}^{(r)} = 0 \Rightarrow \mathbf{b}_1\psi(\mathbf{u})_1 + ... + \mathbf{b}_s\psi(\mathbf{u})_s = 0$. Άρα το διάνυσμα $\psi(\mathbf{u}) = (\psi(\mathbf{u})_1, ..., \psi(\mathbf{u})_s)$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$.
Αντίστροφα έστω ότι $\psi(\mathbf{u})$ ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$ συνεπώς
$\mathbf{b}_1\psi(\mathbf{u})_1 + ... + \mathbf{b}_s\psi(\mathbf{u})_s = 0$.
Δηλαδή $\psi(\mathbf{u})_1$ φορές το $\mathbf{b}_1$ και $\psi(\mathbf{u})_2$ φορές το $\mathbf{b}_2$ και $\psi(\mathbf{u})_s$ φορές το $\mathbf{b}_s$ ισούται με μηδέν. Άρα $\mathbf{u}^{(1)} + ... + \mathbf{u}^{(r)} = 0$, όπου τα μη μηδενικά $\mathbf{u}^{(j)}$ ή τα αντίθετα τους ταυτίζονται με κάποιο στοιχείο του B, για $j = 1, ..., r$. Ωστόσο υπάρχει η πιθανότητα ταύτισης δυο ή και περισσότερων διανυσμάτων $\mathbf{u}^{(j)}$ με το ίδιο $\mathbf{b}_k$, για $1 \leqslant k \leqslant s$. Ενώ από το $\psi(\mathbf{u})_j$ παίρνουμε την πληροφορία ότι αν είναι $\psi(\mathbf{u})_j > 0$ τότε έχουμε ότι $\psi(\mathbf{u})_j$ σε πλήθος εκ των $\mathbf{u}^{(r)}$ είναι ίσα με το $\mathbf{b}_j$, ενώ αν είναι $\psi(\mathbf{u})_j < 0$ τότε έχουμε ότι $\psi(\mathbf{u})_j$ σε πλήθος εκ των $\mathbf{u}^{(r)}$ είναι ίσα με το $-\mathbf{b}_j$. Προφανώς τα μη μηδενικά $\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ αφού ταυτίζονται με στοιχεία της βάσης Graver του A. Άρα συνολικά έχουμε ότι το διάνυσμα $\mathbf{u} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)})$ του B^r ανήκει στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(r)}$. □

4.3 Η βάση Graver της βάσης Graver

Έστω $A = \{\mathbf{a}_1, ..., \mathbf{a}_n\}$ ένα σύνολο διανυσμάτων. Για κάθε σύνολο διανυσμάτων έχουμε ένα τορικό ιδεώδες, σε αυτή την περίπτωση έχουμε το τορικό ιδεώδες I_A. Το τορικό ιδεώδες I_A έχει μια βάση Graver. Τα διανύσματα που αντιστοιχούν στους εκθέτες των διωνύμων της βάσης Graver του A καθορίζουν το σύνολο B. Είναι $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ η βάση Graver του A. Το σύνολο $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ ως σύνολο διανυσμάτων ορίζει ένα τορικό ιδεώδες, το τορικό ιδεώδες I_B. Το τορικό ιδεώδες I_B έχει μια βάση Graver, σε αυτή την περίπτωση λοιπόν μιλάμε για τη βάση Graver της βάσης Graver.

Ακολουθεί ένα παράδειγμα που θα μας βοηθήσει να κατανοήσουμε καλύτερα την παραπάνω διαδικασία.

Παράδειγμα 4.3.1. Έστω το σύνολο διανυσμάτων $A = \{\mathbf{a}_1 = (3, 0), \mathbf{a}_2 = (2, 1), \mathbf{a}_3 = (1, 2), \mathbf{a}_4 = (0, 3)\} \subseteq \mathbb{Z}^2$. Ο πίνακας του A είναι ο εξής:

$$\mathcal{A} = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

Τότε η βάση Graver του A είναι η εξής:

$$Gr_A = \{(1, -2, 1, 0), (1, -1, -1, 1), (0, 1, -2, 1), (1, 0, -3, 2), (2, -3, 0, 1)\} = B.$$

Ο πίνακας του συνόλου διανυσμάτων B που ορίζει το τορικό ιδεώδες I_B είναι ο εξής:

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

Λήμμα 4.3.2. *Έστω το σύνολο διανυσμάτων $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ η βάση Graver κάποιου συνόλου διανυσμάτων A. Το διάνυσμα $\mathbf{u} = (\mathbf{u}^{(1)}, ..., \mathbf{u}^{(r)}) \in B^r$ είναι στοιχείο της βάσης Graver του $A^{(r)}$ αν και μόνο αν το $\psi(\mathbf{u})$ ανήκει στη βάση Graver του B.*

Απόδειξη. Υποθέτουμε ότι το $\psi(\mathbf{u})$ δεν ανήκει στη βάση Graver του B θα καταλήξουμε σε άτοπο. Αφού λοιπόν το $\psi(\mathbf{u})$ δεν ανήκει στη βάση Graver του B συνεπάγεται πως γράφεται ως σύμμορφο άθροισμα δύο μη μηδενικών διανυσμάτων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}}B$, δηλαδή $\psi(\mathbf{u}) = \mathbf{v}_1 +_c \mathbf{v}_2$.
Θα κατασκευάσουμε τα $\mathbf{u}_1$, $\mathbf{u}_2$ έτσι ώστε:
$\psi(\mathbf{u}_1) = \mathbf{v}_1 \in \mathrm{Ker}_{\mathbf{Z}}B$, δηλαδή $\psi(\mathbf{u}_1) = (\psi(u_1)_1, ..., \psi(u_1)_s) = (v_{11}, ..., v_{1s}) = \mathbf{v}_1$
και
$\psi(\mathbf{u}_2) = \mathbf{v}_2 \in \mathrm{Ker}_{\mathbf{Z}}B$, δηλαδή $\psi(\mathbf{u}_2) = (\psi(u_2)_1, ..., \psi(u_2)_s) = (v_{21}, ..., v_{2s}) = \mathbf{v}_2$.

Έχουμε τον πίνακα $M(\mathbf{u}) = \begin{pmatrix} \mathbf{u}^{(1)} \\ . \\ . \\ . \\ \mathbf{u}^{(r)} \end{pmatrix}$.

Ορίζουμε το διάνυσμα ${\mathbf{u}_1}^{(i)}$.

1. ${\mathbf{u}_1}^{(i)} = \mathbf{u}^{(i)} = \mathbf{b}_k$ και το πλήθος των $j \leqslant i$ τέτοιο ώστε $\mathbf{u}^{(j)} = \mathbf{b}_k$ είναι μικρότερο ή ίσο από το $\mid v_{1k} \mid$

ή

2. ${\mathbf{u}_1}^{(i)} = \mathbf{u}^{(i)} = -\mathbf{b}_k$ και το πλήθος των $j \leqslant i$ τέτοιο ώστε $\mathbf{u}^{(j)} = -\mathbf{b}_k$ είναι μικρότερο ή ίσο από το $\mid v_{1k} \mid$.

Διαφορετικά το ${\mathbf{u}_1}^{(i)}$ είναι ίσο με το μηδέν.
Ορίζουμε το ${\mathbf{u}_2}^{(i)}$. Όταν το ${\mathbf{u}_1}^{(i)}$ ισούται με το $\mathbf{u}^{(i)}$ τότε το αντίστοιχο ${\mathbf{u}_2}^{(i)}$ ισούται με το μηδέν. Αντίστροφα όταν το ${\mathbf{u}_1}^{(i)}$ ισούται με το μηδέν τότε το αντίστοιχο ${\mathbf{u}_2}^{(i)}$ ισούται με το $\mathbf{u}^{(i)}$. Δηλαδή σε αυτό το άθροισμα η μια εκ των δύο, συνιστώσα είναι η μηδενική για κάθε $i = 1, ..., r$ αφού $\mathbf{u}_2 = \mathbf{u} - \mathbf{u}_1$. Άρα το άθροισμα $\mathbf{u} = \mathbf{u}_1 +_c \mathbf{u}_2$ είναι σύμμορφο δηλαδή οι συντεταγμένες των διανυσμάτων $\mathbf{u}, \mathbf{u}_1, \mathbf{u}_2$ είναι ομόσημες. Δείξαμε ότι $\psi(\mathbf{u}_1) = \mathbf{v}_1, \psi(\mathbf{u}_2) = \mathbf{v}_2$ όπου τα διανύσματα $\mathbf{v}_1, \mathbf{v}_2$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}B$. Κατά συνέπεια σύμφωνα με την πρόταση 4.2.18 τα διανύσματα $\mathbf{u}_1, \mathbf{u}_2$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}A^{(r)}$. Άτοπο αφού το $\mathbf{u}$ ανήκει στη βάση Graver του $A^{(r)}$ και σύμφωνα με την πρόταση 2.2.15 δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}}A^{(r)}$.
Αντίστροφα υποθέτουμε ότι το $\mathbf{u}$ δεν ανήκει στη βάση Graver του $A^{(r)}$ θα καταλήξουμε σε άτοπο. Αφού το $\mathbf{u}$ δεν ανήκει στη βάση Graver του $A^{(r)}$ συνεπάγεται πως γράφεται ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων του πυρήνα $\mathrm{Ker}_{\mathbf{Z}}A^{(r)}$, δηλαδή $\mathbf{u} = \mathbf{u}_1 +_c \mathbf{u}_2$ με $\mathbf{u}_1, \mathbf{u}_2 \in \mathrm{Ker}_{\mathbf{Z}}A^{(r)}$. Τότε από την πρόταση 4.2.18 έχουμε ότι τα διανύσματα $\psi(\mathbf{u}_1), \psi(\mathbf{u}_2)$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbf{Z}}B$. Θα δείξουμε ότι το άθροισμα $\psi(\mathbf{u}) = \psi(\mathbf{u}_1) + \psi(\mathbf{u}_2)$ είναι σύμμορφο άθροισμα.

Είναι $M(\mathbf{u}) = \begin{pmatrix} \mathbf{u}^{(1)} \\ . \\ . \\ . \\ \mathbf{u}^{(r)} \end{pmatrix} = \begin{pmatrix} \mathbf{u}_1^{(1)} \\ . \\ \mathbf{u}_1^{(i)} \\ . \\ \mathbf{u}_1^{(r)} \end{pmatrix} +_c \begin{pmatrix} \mathbf{u}_2^{(1)} \\ . \\ \mathbf{u}_2^{(i)} \\ . \\ \mathbf{u}_2^{(r)} \end{pmatrix}$ όπου $M(\mathbf{u}_1) = \begin{pmatrix} \mathbf{u}_1^{(1)} \\ . \\ \mathbf{u}_1^{(i)} \\ . \\ \mathbf{u}_1^{(r)} \end{pmatrix}$

και $M(\mathbf{u}_2) = \begin{pmatrix} \mathbf{u}_2^{(1)} \\ . \\ \mathbf{u}_2^{(i)} \\ . \\ \mathbf{u}_2^{(r)} \end{pmatrix}$ με $\mathbf{u}_1 \neq \mathbf{0}, \mathbf{u}_2 \neq \mathbf{0}$.

Έχουμε λοιπόν $\mathbf{u}^{(i)} = \mathbf{u}_1^{(i)} +_c \mathbf{u}_2^{(i)}$. Υποθέτουμε ότι $\mathbf{u}^{(i)} \in B$ ή $-\mathbf{u}^{(i)} \in B$ συνεπώς $\mathbf{u}_1^{(i)} = \mathbf{0}$ ή $\mathbf{u}_2^{(i)} = \mathbf{0}$ κι αυτό γιατί εφόσον το $\mathbf{u}^{(i)}$ ανήκει στη βάση Graver του A σύμφωνα με την πρόταση 2.2.15 δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων του πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A$ οπότε κάποιο εκ των δύο θα είναι το μηδενικό διάνυσμα.
Άρα $\psi(\mathbf{u})_j = \psi(\mathbf{u}_1)_j + \psi(\mathbf{u}_2)_j$ όλα έχουν το ίδιο πρόσημο από τον τρόπο κατασκευής των διανυσμάτων $\mathbf{u}_1, \mathbf{u}_2$. Οπότε είναι ομόσημα κι άρα το άθροισμα $\psi(\mathbf{u}) = \psi(\mathbf{u}_1) +_c \psi(\mathbf{u}_2)$ είναι σύμμορφο. Άτοπο αφού το διάνυσμα $\psi(\mathbf{u})$ ανήκει στη βάση Graver του B και σύμφωνα με την πρόταση 2.2.15 δεν μπορεί να γραφεί ως σύμμορφο άθροισμα δυο μη μηδενικών διανυσμάτων του πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$. □

Παράδειγμα 4.3.3. Συνεχίζοντας το παράδειγμα 4.2.17 υποθέτουμε ότι το διάνυσμα $\psi(\mathbf{u})$ γράφεται ως σύμμορφο άθροισμα δυο μη μηδενικών στοιχείων του πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$ ως εξής:
$\psi(\mathbf{u}) = (-2,2,1,-1,0,1) = (-1,0,1,-1,0,1) +_c (-1,2,0,0,0,0)$, όπου τα διανύσματα $\psi(\mathbf{a}) = (-1,0,1,-1,0,1)$ και $\psi(\mathbf{b}) = (-1,2,0,0,0,0)$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}B$. Συνεπώς τα διανύσματα $\mathbf{a}, \mathbf{b}$ ανήκουν στον πυρήνα $\mathrm{Ker}_{\mathbb{Z}}A^{(7)}$ σύμφωνα με την πρόταση 4.2.18.
Είναι:

$$\begin{pmatrix} b_2 \\ b_3 \\ -b_1 \\ -b_1 \\ b_2 \\ b_6 \\ -b_4 \end{pmatrix} = \begin{pmatrix} 0 \\ b_3 \\ -b_1 \\ 0 \\ 0 \\ b_6 \\ -b_4 \end{pmatrix} +_c \begin{pmatrix} b_2 \\ 0 \\ 0 \\ -b_1 \\ b_2 \\ 0 \\ 0 \end{pmatrix}$$

με $M(\mathbf{u}) = \begin{pmatrix} b_2 \\ b_3 \\ -b_1 \\ -b_1 \\ b_2 \\ b_6 \\ -b_4 \end{pmatrix}$, $M(\mathbf{a}) = \begin{pmatrix} 0 \\ b_3 \\ -b_1 \\ 0 \\ 0 \\ b_6 \\ -b_4 \end{pmatrix}$, $M(\mathbf{b}) = \begin{pmatrix} b_2 \\ 0 \\ 0 \\ -b_1 \\ b_2 \\ 0 \\ 0 \end{pmatrix}$.

Άρα έχουμε

$$\mathbf{u} = \mathbf{a} +_c \mathbf{b}$$

δηλαδή το διάνυσμα $\mathbf{u}$ δεν ανήκει στη βάση Graver του $A^{(7)}$.

Το παρακάτω θεώρημα είναι το σημαντικότερο θεώρημα της διατριβής, που αποδεικνύει ότι η πολυπλοκότητα Graver κι άρα και η πολυπλοκότητα Markov, είναι πεπερασμένη και δεν εξαρτάται από το r.

Θεώρημα 4.3.4. *Η πολυπλοκότητα Graver ενός τορικού ιδεώδους I_A είναι μικρότερη ή ίση από το μέγιστο των $1-$νορμών των στοιχείων της βάσης Graver της βάσης Graver.*

Απόδειξη. Έστω $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ η βάση Graver του A και $\mathbf{u}$ το διάνυσμα που ανήκει στη βάση Graver του $A^{(r)}$ με τύπο κ. Σύμφωνα με το πόρισμα 4.2.10 μπορούμε να βρούμε ένα στοιχείο $\mathbf{u}' \in B^{r'}$ και $\mathbf{u}'$ να ανήκει στη βάση Graver του $A^{(r')}$, με $r \leq r'$, το οποίο να έχει τύπο λ με $\kappa \leqslant \lambda$. Όμως το λ ισούται με το άθροισμα $\mid \psi(u_1) \mid + ... + \mid \psi(u_s) \mid = \parallel \psi(\mathbf{u}') \parallel_1$ άρα

$$\kappa \leqslant \parallel \psi(\mathbf{u}') \parallel_1 = \parallel \mathbf{c}_i \parallel_1 \leqslant max_{1 \leqslant j \leqslant w}(\parallel \mathbf{c}_j) \parallel_1),$$

όπου $C = \{\mathbf{c}_1, ..., \mathbf{c}_w\}$ η βάση Graver της βάσης Graver του A, δηλαδή η βάση Graver του B. Σύμφωνα λοιπόν με το λήμμα 4.3.2 κι εφόσον το $\mathbf{u}'$ ανήκει στη βάση Graver του $A^{(r')}$, το $\psi(\mathbf{u}')$ ανήκει στη βάση Graver του B, δηλαδή στη βάση Graver της βάσης Graver του A. Η πολυπλοκότητα Graver $g(A)$ δηλαδή, είναι μικρότερη ή ίση από το μέγιστο των 1-νορμών της βάσης Graver της βάσης Graver του A. □

Σύμφωνα με το θεώρημα 3.1.17 το μέγιστο των 1−νορμών των στοιχείων της βάσης Graver της βάσης Graver δεν εξαρτάται από τα πρόσημα των διανυσμάτων $\mathbf{b}_1, ..., \mathbf{b}_s$ της βάσης Graver που τυχαία επιλέξαμε για να ορίσουμε το σύνολο B. Το επόμενο θεώρημα δείχνει ότι το άνω όριο για την πολυπλοκότητα Graver που δώσαμε στο θεώρημα 4.3.4 είναι το καλύτερο δυνατό.

Θεώρημα 4.3.5. *Για κάθε διάνυσμα* $\mathbf{d}$ *που ανήκει στη βάση Graver της βάσης Graver του A δηλαδή στη βάση Graver του B, υπάρχει ένα διάνυσμα* $\mathbf{u}$ *το οποίο ανήκει στο σύνολο* B^r *τέτοιο ώστε το διάνυσμα* $\mathbf{u}$ *να ανήκει στη βάση Graver του* $A^{(r)}$ *και* $\psi(\mathbf{u}) = \mathbf{d}$, *όπου* $r = \parallel \mathbf{d} \parallel_1$.

Απόδειξη. Έστω το σύνολο $B = \{\mathbf{b}_1, ..., \mathbf{b}_s\}$ η βάση Graver του A και το σύνολο $C = \{\mathbf{c}_1, ..., \mathbf{c}_w\}$ η βάση Graver του B. Έστω $\mathbf{d} = (d_1, ..., d_s)$ το οποίο ανήκει στη βάση Graver της βάσης Graver του A, δηλαδή στη βάση Graver του B, κατασκευάζουμε το $\mathbf{u}$ ως εξής:
Οι πρώτες $\mid d_1 \mid$ γραμμές του είναι ίσες με $\mathbf{b}_1$ αν το $d_1 \geqslant 0$ ή με $-\mathbf{b}_1$ αν το $d_1 < 0$. Οι επόμενες $\mid d_2 \mid$ γραμμές είναι ίσες με $\mathbf{b}_2$ αν το $d_2 \geqslant 0$ ή με $-\mathbf{b}_2$ αν το $d_2 < 0$. Όμοια οι τελευταίες $\mid d_s \mid$ γραμμές είναι ίσες με $\mathbf{b}_s$ αν το $d_s \geqslant 0$ ή με $-\mathbf{b}_s$ αν το $d_s < 0$. Δηλαδή $M(\mathbf{u}) = \begin{pmatrix} \frac{d_1}{\mid d_1 \mid}\mathbf{b}_1 \\ \vdots \\ \frac{d_1}{\mid d_1 \mid}\mathbf{b}_1 \\ \vdots \\ \frac{d_s}{\mid d_s \mid}\mathbf{b}_s \\ \vdots \\ \frac{d_s}{\mid d_s \mid}\mathbf{b}_s \end{pmatrix}$. Ακόμη $\psi(\mathbf{u}) = (\psi(\mathbf{u})_1, ..., \psi(\mathbf{u})_s) = (d_1, ..., d_s) = \mathbf{d}$ το οποίο ανήκει στη βάση Graver του B, άρα από λήμμα 4.3.2 έχουμε ότι το διάνυσμα $\mathbf{u} \in B^r$ ανήκει στη βάση Graver του $A^{(r)}$. Από τον τρόπο που κατασκευάσαμε το $\mathbf{u}$ παρατηρούμε ότι είναι $r = \mid d_1 \mid + ... + \mid d_s \mid = \parallel \mathbf{d} \parallel_1$. □

Παράδειγμα 4.3.6. Έστω το σύνολο διανυσμάτων $A = \{\mathbf{a}_1 = (3, 0), \mathbf{a}_2 = (2, 1), \mathbf{a}_3 =$

$(1,2), \mathbf{a}_4 = (0,3)\} \subseteq \mathbb{Z}^2$. Ο πίνακας του A είναι ο:

$$A = \begin{pmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}.$$

Τότε η βάση Graver του A είναι:

$Gr_A = \{\mathbf{b}_1 = (1,-2,1,0), \mathbf{b}_2 = (1,-1,-1,1), \mathbf{b}_3 = (0,1,-2,1), \mathbf{b}_4 = (1,0,-3,2), \mathbf{b}_5 = (2,-$

Ο πίνακας του συνόλου διανυσμάτων B είναι ο εξής:

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

Η βάση Graver του B, δηλαδή η βάση Graver της βάσης Graver είναι η εξής:
$C = \{\mathbf{c}_1 = (1,-1,1,0,0), \mathbf{c}_2 = (1,-2,0,1,0), \mathbf{c}_3 = (1,1,0,0,-1),$
$\mathbf{c}_4 = (2,0,1,0,-1), \mathbf{c}_5 = (2,-1,0,1,-1), \mathbf{c}_6 = (0,1,1,-1,0),$
$\mathbf{c}_7 = (1,0,-1,1,-1), \mathbf{c}_8 = (3,0,0,1,-2), \mathbf{c}_9 = (1,0,2,-1,0),$
$\mathbf{c}_{10} = (0,2,-1,0,-1), \mathbf{c}_{11} = (0,1,-2,1,-1), \mathbf{c}_{12} = (0,3,0,-1,-1),$
$\mathbf{c}_{13} = (0,0,3,-2,1)\}$.
Παρατηρούμε ότι τα διανύσματα $\mathbf{c}_8, \mathbf{c}_{13}$ έχουν τη μέγιστη $1-$ νόρμα κι άρα $g(A) = 6 = \| \mathbf{c}_8 \|_1 = \| \mathbf{c}_{13} \|_1$, σύμφωνα με τα θεωρήματα 4.3.4, 4.3.5. Για το διάνυσμα λοιπόν $\mathbf{c}_8$ που ανήκει στη βάση Graver της βάσης Graver, σύμφωνα με το θεώρημα 4.3.5 υπάρχει ένα διάνυσμα $\mathbf{u}$ το οποίο ανήκει στο σύνολο B^6 τέτοιο ώστε το διάνυσμα $\mathbf{u}$ να ανήκει στη βάση Graver του $A^{(6)}$ και $\psi(\mathbf{u}) = \mathbf{c}_8$, όπου

$$\| \mathbf{c}_8 \|_1 = |\,3\,| + |\,0\,| + |\,0\,| + |\,1\,| + |\,-2\,| = 6.$$

Το διάνυσμα αυτό είναι το εξής: $\mathbf{u} = (\mathbf{b}_1, \mathbf{b}_1, \mathbf{b}_1, \mathbf{b}_4, -\mathbf{b}_5, -\mathbf{b}_5)$ και ο αντίστοιχος πίνακας του είναι ο ακόλουθος:

$$M(\mathbf{u}) = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_1 \\ \mathbf{b}_1 \\ \mathbf{b}_4 \\ -\mathbf{b}_5 \\ -\mathbf{b}_5 \end{pmatrix}.$$

Ακόμη το διάνυσμα $\mathbf{u}$ θα μπορούσε να είναι της μορφής $\mathbf{u} = (\mathbf{b}_1, \mathbf{b}_4, -\mathbf{b}_5, \mathbf{b}_1, \mathbf{b}_1, -\mathbf{b}_5)$ και ο αντίστοιχος πίνακας του είναι ο ακόλουθος:

$$M(\mathbf{u}) = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_4 \\ -\mathbf{b}_5 \\ \mathbf{b}_1 \\ \mathbf{b}_1 \\ -\mathbf{b}_5 \end{pmatrix}.$$

Επιπλέον ισχύει

$$\| \mathbf{c}_{13} \|_1 = |\,0\,| + |\,0\,| + |\,3\,| + |\,-2\,| + |\,1\,| = 6.$$

Έτσι το διάνυσμα u το οποίο ανήκει στο σύνολο B^6 τέτοιο ώστε το διάνυσμα u να ανήκει στη βάση Graver του $A^{(6)}$ και $\psi(\mathbf{u}) = \mathbf{c}_{13}$ είναι το εξής:
$\mathbf{u} = (\mathbf{b}_3, \mathbf{b}_3, \mathbf{b}_3, -\mathbf{b}_4, -\mathbf{b}_4, \mathbf{b}_5)$ και ο αντίστοιχος πίνακας του είναι ο ακόλουθος:

$$M(\mathbf{u}) = \begin{pmatrix} \mathbf{b}_3 \\ \mathbf{b}_3 \\ \mathbf{b}_3 \\ -\mathbf{b}_4 \\ -\mathbf{b}_4 \\ \mathbf{b}_5 \end{pmatrix}.$$

Ένα στοιχείο της βάσης Graver του $A^{(10)}$ είναι:
$\mathbf{v} = (0, \mathbf{b}_3, 0, \mathbf{b}_3, 0, \mathbf{b}_3, 0, -\mathbf{b}_4, -\mathbf{b}_4, \mathbf{b}_5)$ και ο αντίστοιχος πίνακας του είναι ο ακόλουθος:

$$M(\mathbf{v}) = \begin{pmatrix} 0 \\ \mathbf{b}_3 \\ 0 \\ \mathbf{b}_3 \\ 0 \\ \mathbf{b}_3 \\ 0 \\ -\mathbf{b}_4 \\ -\mathbf{b}_4 \\ \mathbf{b}_5 \end{pmatrix}.$$

Ένα άλλο στοιχείο της βάσης Graver του $A^{(10)}$ είναι το εξής:
$\mathbf{v} = (\mathbf{b}_1, 0, 0, \mathbf{b}_1, \mathbf{b}_1, \mathbf{b}_4, 0, 0, -\mathbf{b}_5, 0, -\mathbf{b}_5)$ και ο αντίστοιχος πίνακας του είναι ο ακόλουθος:

$$M(\mathbf{v}) = \begin{pmatrix} \mathbf{b}_1 \\ 0 \\ 0 \\ \mathbf{b}_1 \\ \mathbf{b}_1 \\ \mathbf{b}_4 \\ 0 \\ 0 \\ -\mathbf{b}_5 \\ 0 \\ -\mathbf{b}_5 \end{pmatrix}.$$

Από το θεώρημα 4.3.5 γνωρίζουμε ότι οποιοδήποτε άλλο στοιχείο της βάσης Graver του $A^{(10)}$ με τύπο 6 θα είναι παρόμοιας μορφής και δεν μπορούμε να βρούμε στοιχείο της βάσης Graver του $A^{(10)}$ με τύπο μεγαλύτερο του 6.

Περίληψη

Η παρούσα διατριβή σχετίζεται με τις βάσεις Markov και Graver και συγκεκριμένα με τις πολυπλοκότητες αυτών. Αναπτύσσει τη θεωρία που σχετίζεται με τις σχέσεις μεταξύ των βάσεων αυτών με τις βάσεις Gröbner και Hilbert, με στόχο την απόδειξη του θεωρήματος των F.Santos και B.Sturmfels που βρίσκει την πολυπλοκότητα Graver.

Στο πρώτο κεφάλαιο παρουσιάζουμε τις βάσεις Gröbner και σημαντικά αποτελέσματα που σχετίζονται με αυτές. Η ιδέα των βάσεων Gröbner πρωτοεμφανίστηκε το 1900 από τον διάσημο μαθηματικό Paul Gordan. Ο πρώτος που έδωσε έναν αλγόριθμο για τον υπολογισμό τους και ανέπτυξε τη θεωρία τους και το 1976 τις ονόμασε βάσεις Gröbner ήταν ο Bruno Buchberger, ενώ μία παρόμοια ιδέα για τους τοπικούς δακτυλίους αναπτύχθηκε το 1964 από τον Heisuke Hironaka στα άρθρα του [9],[10], και τις ονόμασε κανονικές βάσεις (standard bases). Στο κεφάλαιο αυτό ορίζουμε εκτός των βάσεων Gröbner και τις ανάγωγες βάσεις Gröbner και δίνουμε αλγόριθμους για τον υπολογισμο τους. Ολοκληρώνουμε το κεφάλαιο παρουσιάζοντας τις καθολικές βάσεις Gröbner οι οποίες εισήχθησαν από τον V. Weispfenning στο άρθρο [20] (1987) και τον Niels Schwartz στο άρθρο [18] (1988), και σπουδαία συμπεράσματα που σχετίζονται με αυτές.

Στο δεύτερο κεφάλαιο βασικό μας εργαλείο είναι τα τορικά ιδεώδη. Ορίζουμε και μελετούμε τις βάσεις Graver, των οποίων η σύνδεση με τη θεωρία των βάσεων Gröbner περιγράφεται στο βιβλίο [19] του B.Sturmfels. Η θεωρία αλγορίθμων των βάσεων Graver και η εφαρμογή τους στον ακέραιο προγραμματισμό περιγράφεται στα βιβλία [12] και [13] του Shmuel Onn. Στην άλγεβρα ωστόσο πολλά υποσύνολα διωνύμων του ιδεώδους όπως τα κυκλωμάτα, οι ανάγωγες βάσεις Gröbner, η καθολική βάση Gröbner, μια τουλάχιστον ελαχιστοτική βάση Markov, ανήκουν στη βάση Graver και την καθιστούν ιδιαίτερα σημαντική. Εισάγουμε την έννοια του Lawrence πίνακα $A^{(2)}$ που συμβάλλει στον υπολογισμό της βάσης Graver. Ενώ δίνουμε δύο διαφορετικούς αλγορίθμους υπολογισμού της.

Στο τρίτο κεφάλαιο αναπτύσσουμε τη θεωρία των βάσεων Markov και παρουσιάζουμε το σημαντικό θεώρημα των P.Diakonis και B.Sturmfels το οποίο περιέχεται στο άρθρο τους [5], το 1988. Στη συνέχεια ορίζουμε το ημισύμμορφο και ισχυρά ημισύμμορφο άθροισμα και παρουσιάζουμε ένα βασικό θεώρημα, που θα μας χρειαστεί στο τέταρτο κεφάλαιο στην απόδειξη ενός θεωρήματος των F.Santos και B.Sturmfels. Τέλος εισάγουμε την έννοια των αναντικατάστατων διωνύμων.

Στο τέταρτο κεφάλαιο σιόχος μας είναι να παρουσιάσουμε το θεώρημα των F.Santos και B.Sturmfels, το οποίο σχετίζεται με τις πολυπλοκότητες Markov και Graver. Έτσι αρχικά ορίζουμε το Lawrence πίνακα $A^{(r)}$, για $r \geq 2$, τις πολυπλοκότητες Markov και Graver. Παρουσιάζουμε λήμματα και πορίσματα που συσχετίζουν στοιχεία της βάσης Graver του πίνακα $A^{(r)}$ με στοιχεία της βάσης Graver του πίνακα $A^{(s)}$, για $s > r$, και σύμμορφα αθροίσματα επί των διανυσμάτων τους.

Ορίζουμε τη βάση Graver της βάσης Graver και βλέπουμε πως αυτή συνδέεται με τη βάση Graver. Έτσι φτάνουμε στο σημαντικότερο θεώρημα της διατριβής, που αποδεικνύει ότι οι πολυπλοκότητες Markov και Graver είναι πεπερασμένες και ανεξάρτητες του r. Ολοκληρώνουμε το κεφάλαιο αποδεικνύοντας το θεώρημα το οποίο εξασφαλίζει ότι το άνω όριο της βάσης Graver που βρήκαμε είναι το καλύτερο δυνατό.

Summary

This thesis is related to the bases Markov and Graver and specifically with their complexities. Develops the theory relating to the relationships between those bases, the bases Gröbner and Hilbert, in order to prove the theorem of F.Santos and B.Sturmfels which finds the Graver complexity.
In the first chapter we present the Gröbner bases and significant results associated with them. The idea originated in 1900 by the famous mathematician Paul Gordan. The first who gave an algorithm for calculation and developed their theory in 1976 and named them Gröbner bases was Bruno Buchberger, while a similar concept for local rings was developed in 1964 by Heisuke Hironaka in the articles [9], [10], and called them normal bases (standard bases). In this chapter we define the Gröbner bases and irreducible Gröbner bases and we give algorithms to compute them. We conclude the chapter by presenting the universal Gröbner bases which were introduced by V. Weispfenning in the article [20] (1987) and Niels Schwartz in the article [18] (1988), and important information related to them.
In the second chapter, our main tools are the toric ideals. We define and study the Graver bases, whose connection with the theory of Gröbner bases is described in the book [19] of B.Sturmfels. The theory of algorithms of Graver bases and their application to the integer programming are described in the books [12] and [13] of Shmuel Onn. In algebra many subsets of binomial ideals such as circuits, irreducible Gröbner bases, the universal Gröbner basis, at least one Markov basis, belong to the Graver basis and make it particularly important. We introduce the concept of Lawrence table $A^{(2)}$ contributing to the calculation of Graver basis. Whilst we give two different algorithms for calculating it.
In the third chapter we develop the theory of Markov bases and present the important theorem of P.Diakonis and B.Sturmfels which contained in the article [5], 1988. Then we define semiconformal and strongly semiconformal sum and present a basic theorem, we need at the fourth chapter in the proof of a theorem of F.Santos and B.Sturmfels. Finally we introduce the concept of binomial indispensable.
In the fourth chapter we present the theorem of F.Santos and B.Sturmfels, which is releated to the complexities Markov and Graver.First we define Lawrence table $A^{(r)}$, for $r \geq 2$, Markov and Graver complexities. We define the Graver basis of the Graver basis and we see how it is releated to the Graver basis. Finally we prove the main theorem which gives an upper bound for the Graver complexity and we prove that it is the best possible.

Βιβλιογραφία

[1] W.Adams and P.Loustaunau. An introduction to Gröbner Bases. American Mathematical Society, Graduate Studies in Mathematics, **3**, (1991).

[2] S.Aoki and A.Takemura. Minimal basis for connacted Markov chain over $3 \times 3 \times K$ contingency tables with fixed two-dimensional marginals . Aust.N.Z.J.Stat. , 45, **2**, pages 229-249, (2003).

[3] M.F Atiyah and I.G.MacDonald. Introduction to Commutative Algebra. ABP, Addison-Wesley Series, University of Oxford , (1969).

[4] H.Charalambous and A.Katsabekis and A.Thoma. *Minimal systems of Binomial Generators and the indispensable complex oh a toric ideal.* Proceedings of American Mathematical Society, **135**, pages 3443-3451, (2007).

[5] P.Diakonis and B.Sturmfels. *Algebraic algorithms for sampling from conditional distributions.* Ann.Statist, No.26, pages 363-397, (1998).

[6] M.Drton and B.Sturmfels and S.Sullivant. Lectures on Algebraic Statistics. Birkhaüser Basel, Oberwolfach Seminars Series**39** , (2009).

[7] V.Ene and J.Herzog. Gröbner bases in Commutative Algebra. American Mathematical Society, Graduate Studies in Mathematics, **130**, (2012).

[8] J.Graver. On the foundation of linear and integer linear programming. I.Math Programming, no **2**, **9**, pages 207-226, (1975).

[9] H.Hironaka. *Resolution of singularities of an algebraic variety over a field of characteristic zero.* I, Annals of Mathematics, (2) **79**, pages 109-203, (1964).

[10] H.Hironaka. *Resolution of singularities of an algebraic variety over a field of characteristic zero.* II, Annals of Mathematics, (2) **79**, pages 205-326, (1964).

[11] S.Hosten and S.Sullivant. *A finiteness theorem for Markov bases of hierarchical models.* Journal of Combinatorial Theory, Series A **114**, pages 311-321, (2007).

[12] S. Onn. Nonlinear Discrete Optimization, An Algorithmic Theory. European Mathematical Society, Zurich Lectures in Advanced Mathematics, (2010).

[13] S. Onn. Linear and Nonlinear Integer Optimization. Mathematical Sciences Research Institute, Online Video Lecture Series, Berkeley, (2011).

[14] L.Pachter and B.Sturmfels. Algebraic Statistics for Computational Biology. Department of Mathematics, **53**, pages 171-186, (2005).

[15] G.Pistone and E.Riccomagno and H.Wynn. Algebraic Statistics:Computational Commutative Algebra in Statistics. Chapman and Hall/CRC, Chapman and Hall/CRC Monographs on Statistics and Applied Probability Series, **89** , (2000).

[16] Fr.Santos and B.Sturmfels. *Higher Lawrence configuratios*. Journal of Combinatorial Theory, Series A **103**, pages 151-164, (2003).

[17] A.Schrijrer. Theory of Linear and Integer Programming. Wiley, Chichester, NY, (1986).

[18] N.Schwartz. *Stability of Gröbner bases*. Journal of Pure and Applied Algebra, **53**, pages 171-186, (1988).

[19] B. Sturmfels. Gröbner bases and Convex Polytopes. American Mathematical Society, University Lecture Series, **8** , (1996).

[20] V.Weispfenning. *Constructing Universal Gröbner bases*. Proceedings AAE−EC 5,Menorca, Springer Lecture Notes in Comput. Science, **356**, pages 408-417, (1987).

[21] 4ti2 team. 4ti2-A Software package for algebraic geometric and combinatorial promblems on linear spaces. Available at www.4ti2.de .

[22] Χ.Τατάκης. Τορικά Ιδεώδη και Θεωρία Γραφημάτων στη Συνδυαστική Μεταθετική Άλγεβρα. Πανεπιστήμιο Ιωαννίνων, Μεταπτυχιακή Διατριβή , (2007).

ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ