ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΜΗΜΑ ΜΕΘΟΔΟΛΟΓΙΑΣ, ΙΣΤΟΡΙΑΣ ΚΑΙ ΘΕΩΡΙΑΣ ΤΗΣ ΕΠΙΣΤΗΜΗΣ
ΤΜΗΜΑ ΦΙΛΟΣΟΦΙΑΣ – ΠΑΙΔΑΓΩΓΙΚΗΣ & ΨΥΧΟΛΟΓΙΑΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΩΝ ΑΓΩΓΗΣ

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

ΑΛΓΕΒΡΙΚΗ ΕΠΙΛΥΣΗ ΓΕΩΜΕΤΡΙΚΩΝ ΠΡΟΒΛΗΜΑΤΩΝ

- **Αυτόματες (Αλγοριθμικές αποδείξεις)**
- **Το τρίτο πρόβλημα Hilbert**

Νίκος Θ. Αντωνόπουλος

Α.Μ. Δ200820

Επιβλέπων καθηγητής:

Ε. Ράπτης

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΜΗΜΑ ΜΕΘΟΔΟΛΟΓΙΑΣ, ΙΣΤΟΡΙΑΣ ΚΑΙ ΘΕΩΡΙΑΣ ΤΗΣ ΕΠΙΣΤΗΜΗΣ
ΤΜΗΜΑ ΦΙΛΟΣΟΦΙΑΣ – ΠΑΙΔΑΓΩΓΙΚΗΣ & ΨΥΧΟΛΟΓΙΑΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΩΝ ΑΓΩΓΗΣ

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΔΑΚΤΙΚΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ»

Η παρούσα διπλωματική εργασία
εκπονήθηκε στα πλαίσια των σπουδών
για την απόκτηση του
Μεταπτυχιακού Διπλώματος Ειδίκευσης
που απονέμει το
Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών
«Διδακτική και Μεθοδολογία των Μαθηματικών»

Εγκρίθηκε την ……. από Εξεταστική Επιτροπή αποτελούμενη από τους:

Ονοματεπώνυμο	Βαθμίδα	Υπογραφή
Ράπτης Ευάγγελος (επιβλέπων καθηγητής)	Καθηγητής	……
Βάρσος Δημήτριος	Αναπλ. καθηγητής	…….
Λάππας Διονύσιος	Αναπλ. Καθηγητής	…….

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος…… 9

ΚΕΦΑΛΑΙΟ 1

1.1 Τα θεμέλια των Μαθηματικών

1.1.i. Ο Πλατωνισμός …….....11

1.1.ii. Ο Φορμαλισμός …….....13

1.1.iii. Ο Ιντουισιονισμός ……13

1.2. Προβλήματα στα θεμέλια

1.2.i. Ο Ευκλείδης και η αξιωματική θεμελίωση της Γεωμετρίας …….....14

1.2.ii. Μη ευκλείδειες γεωμετρίες ……...16

1. 2.iii. Οι πρώτες προσπάθειες επαναθεμελίωσης …….....18

1.2.iv. Τα νέα θεμέλια – τυπικά αξιωματικά συστήματα ……20

1.2.v. Συνέπεια – ανεξαρτησία – ισοδυναμία – πληρότητα .. ……24

1.2.vi. Το άδοξο τέλος – ο Kurt Godel ……...25

1.3 Οι ηλεκτρονικοί υπολογιστές

1.3.i. Οι υπολογιστές και ο ανθρώπινος νους …….....26

1.3.ii. Το πρόβλημα των τεσσάρων χρωμάτων ……28

ΚΕΦΑΛΑΙΟ 2

2.1. Πράξεις

2.1.i. Διμελής πράξη ……33

2.1.ii. Ιδιότητες των πράξεων ……...33

2.2. Ομάδες

2.1.i. Ομάδα ……..34

2.2.ii. Υποομάδα ……..35

2.2.iii. Ομομορφισμοί ομάδων ……...36

2.2.iv. Το σύνολο $\mathbb{Z}_n$ ……37

2.2.v. Τάξη ομάδας …….....38

2.2.vi. Κυκλική ομάδα …….……38

2.2.vii. Σύμπλοκα ……39

2.2.viii. Κανονική υποομάδα – ομάδα πηλίκο ……40

2.3. Σύνολα εφοδιασμένα με δυο πράξεις

2.3.i. Επιμεριστική ιδιότητα …….....40

2.3.ii. Δακτύλιοι – ιδεώδες δακτυλίου ……41

2.3.iii. Διαιρέτες του μηδενός – Ακέραια περιοχή ……42

2.3.iv. Σώμα …….….…43

2.4. Πολυώνυμα

2.4.i. Ο δακτύλιος των πολυωνύμων μιας μεταβλητής ……..44

2.4.ii. Η ταυτότητα της διαίρεσης στο δακτύλιο F[x] …….....46

2.4.iii. Ο μέγιστος κοινός διαιρέτης ……...47

2.4.iv. Ο δακτύλιος των πολυωνύμων πολλών μεταβλητών ……..47

2.4.v. Διάταξη – Διάταξη (λεξικογραφική) μονωνύμων …….....48

2.4.vi. Η διαίρεση στον $F[x_1, x_2, \ldots, x_v]$ ……50

2.5. Εξωτερική πράξη

2.5.i. Διανυσματικός χώρος ……52

2.5.ii. Διανυσματικός υπόχωρος ……52

2.5.iii. Γραμμική ανεξαρτησία ……53

2.5.iv. Βάση και διάσταση διανυσματικού χώρου ……..53

ΚΕΦΑΛΑΙΟ 3

3.1. Το πρόβλημα της αυτόματης απόδειξης Γεωμετρικών θεωρημάτων

3.1.i. Σύστημα πολλών εξισώσεων με πολλές μεταβλητές ……...55

3.1.ii. Ιδεώδες παραγόμενο από τα πολυώνυμα $f_1(x), f_2(x), \ldots, f_\mu(x)$ ……58

3.1.iii. Βάσεις Groebner …….....61

3.1.iv. Βάσεις Groebner στον δακτύλιο πολυωνύμων μιας μεταβλητής ……...63

3.1.v. Βάσεις Groebner στον δακτύλιο πολυωνύμων δύο μεταβλητών ……...64

3.1.vi. Ελαχιστοποιημένες και ανηγμένες βάσεις Groebner ……..66

3.1.vii. Ο αλγόριθμος του Buchberger ……..…68

3.1.viii. Το θεώρημα βάσης του Hilbert ……70

3.2. Αυτόματη απόδειξη Γεωμετρικών θεωρημάτων …….....72

ΚΕΦΑΛΑΙΟ 4

4.1. Εμβαδόν

4.1.i. Εμβαδόν και μέτρο …….77

4.1.ii. Αξιωματικός ορισμός του εμβαδού ……78

4.1.iii. Η μέθοδος της διαμέρισης ……80

4.1.iv. Η μέθοδος του συμπληρώματος ……82

4.1.v. Το Πυθαγόρειο θεώρημα …….....84

4.2. Το τρίτο πρόβλημα Hilbert

4.2.i. Το πρόβλημα …….....85

4.2.ii. Η αναλλοίωτη του Dehn ……...89

4.2.iii. Προσθετικές συναρτήσεις ……92

4.2.iv. Κατασκευή βάσης επί του $\mathbb{Q}$ ……....95

4.2.v. Το θεώρημα ρητής ανεξαρτησίας ……96

4.2.vi. Το τετράεδρο και ο κύβος ……...98

4.2.vii. Το Θεώρημα του Dehn ……...99

Συμπεράσματα – Διδακτικές προεκτάσεις……...…100

Βιβλιογραφία ……....107

Αφιερώνεται στην Όλγα,

το Θοδωρή

και τη Βασιλική

Αντί προλόγου

Η παρούσα διπλωματική εργασία αναφέρεται κυρίως σε δυο θέματα τα οποία σχετίζονται με την αλγεβρική επίλυση γεωμετρικών προβλημάτων. Πρόκειται για την αυτόματη (αλγοριθμική) επίλυση γεωμετρικών προβλημάτων και το τρίτο πρόβλημα του Hilbert.

Αν θελήσουμε να τοποθετήσουμε σε ιστορικό πλαίσιο τα γεγονότα, θα πρέπει να ξεκινήσουμε από το δεύτερο μισό του 19ου αιώνα την εποχή που η ανακάλυψη των μη Ευκλείδειων γεωμετριών, η ραγδαία ανάπτυξη του Λογισμού, που είχε προηγηθεί, και η εμφάνιση των παραδόξων, κλόνισαν τα μέχρι τότε θεωρούμενα ως στέρεα θεμέλια της μαθηματικής γνώσης. Μπορούμε παράλληλα να φτάσουμε μέχρι το δεύτερο μισό του 20ου αιώνα, όταν παρουσιάστηκε αλγοριθμική διαδικασία για την εύρεση βάσης Groebner.

Έτσι, στο πρώτο μέρος της παρούσας προσπαθούμε να περιγράψουμε την ατμόσφαιρα που επικρατούσε στην αρχή αυτής της περιόδου, αναφέροντας τα διάφορα ρεύματα και πως το καθένα από αυτά αντιλαμβανόταν τα μαθηματικά αντικείμενα. Επίσης, θα αναφερθούν οι προσπάθειες επαναθεμελίωσης των Frege, Russel, Hilbert και άλλων, μέχρι το άδοξο τέλος των προσπαθειών για πλήρη τυποποίηση των μαθηματικών, που επήλθε με την παρουσίαση των θεωρημάτων του Kurt Gödel.

Κορυφαία στιγμή της εποχής μπορεί να θεωρηθεί η διάλεξη του Hilbert στο Παρίσι στην ανατολή του εικοστού αιώνα και η παρουσίαση των είκοσι τριών προβλημάτων του. Στο τέταρτο κεφάλαιο παρουσιάζουμε μια απλή εκδοχή του τρίτου προβλήματος και συγκεκριμένα εξετάζουμε κατά πόσο είναι δυνατό, εφαρμόζοντας στοιχειώδεις μεθόδους, δηλαδή χωρίς να καταφύγουμε σε άπειρες διαδικασίες, να βρούμε τύπο που να υπολογίζει τον όγκο οποιουδήποτε πολυέδρου. Παραθέτοντας μια απόδειξη που οφείλεται στον Dehn Max, αποδεικνύουμε ότι κάτι τέτοιο είναι αδύνατο αφού, με αυτές

τις μεθόδους, δεν μπορούμε να «μετασχηματίσουμε» ένα κανονικό τετράεδρο σε κύβο που να έχει τον ίδιο όγκο.

Η εμφάνιση των ηλεκτρονικών υπολογιστών και η ραγδαία εξάπλωσή τους σε συνδυασμό με το ότι σε πολλές περιπτώσεις εκτελούν διεργασίες που μοιάζουν μ' αυτές του ανθρώπινου νου, άρχισε να γεννά ερωτηματικά ως προς την ύπαρξη ή μη ύπαρξη ορίου στην εξέλιξη των μηχανών. Συγκεκριμένα ανέκυψαν ερωτήματα όπως: Μπορούν οι μηχανές να σκέπτονται; Μπορούν να αποδεικνύουν μαθηματικές προτάσεις; Στο τρίτο μέρος παρουσιάζουμε τον τρόπο με τον οποίο διάφορα θεωρήματα της ευκλείδειας γεωμετρίας, που μπορούν να «μεταφραστούν» με μορφή πολυωνυμικών εξισώσεων, αποδεικνύονται αλγοριθμικά. Βέβαια ο προβληματισμός και η συζήτηση για το κατά πόσο μια τέτοια απόδειξη πρέπει να θεωρηθεί ως μαθηματικά έγκυρη, εξακολουθεί να υφίσταται.

Για την καλύτερη παρακολούθηση του μαθηματικού μέρους κρίναμε σκόπιμο, στο δεύτερο κεφάλαιο να παραθέσουμε τα σχετικά με τις αλγεβρικές δομές, όπως τις έννοιες της ομάδας, του δακτυλίου, του σώματος και του διανυσματικού χώρου, επιμένοντας ιδιαίτερα στους δακτυλίους των πολυωνύμων μιας ή περισσοτέρων μεταβλητών.

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα καθηγητή κ. Ευάγγελο Ράπτη τόσο για την ευκαιρία που μου έδωσε να ασχοληθώ με δυο ιδιαιτέρα ελκυστικά θέματα, όσο και για την πολύπλευρη υποστήριξη του κατά τη διάρκεια της εκπόνησης. Επίσης τους αναπληρωτές καθηγητές κ. Βάρσο και Λάππα Διονύσιο για τις εύστοχες παρατηρήσεις τους στην όλη διάρθρωση της διπλωματικής εργασίας.

Τελειώνοντας το προλογικό αυτό σημείωμα θα ήθελα επίσης να ευχαριστήσω όλους τους συντελεστές του Προγράμματος Μεταπτυχιακών Σπουδών για τη συνεργασία τους και ιδιαίτερα το συνάδελφο και φίλο Θανάση Τζιώτζιο με τον οποίο πορευθήκαμε παράλληλα σε όλη τη διάρκεια του Προγράμματος.

ΚΕΦΑΛΑΙΟ 1

1. 1 Τα θεμέλια των Μαθηματικών

Συχνά ο 19ος αιώνας όταν αναφερόμαστε στα μαθηματικά, συνδυάζεται με τη λεγόμενη κρίση στα θεμέλια των μαθηματικών. Σε κάθε συζήτηση που αναφέρεται στα θεμέλια των μαθηματικών παρουσιάζονται τρία βασικά ρεύματα (σχολές): **Ο πλατωνισμός, ο φορμαλισμός και ο ιντουισιονισμός.**

1.1.i. Ο Πλατωνισμός

Σύμφωνα με τον Πλατωνισμό, που έλκει την καταγωγή του από το **Πλατωνικό φιλοσοφικό σύστημα**, τα μαθηματικά αντικείμενα είναι πραγματικά. Η ύπαρξή τους είναι ένα αντικειμενικό γεγονός, εντελώς ανεξάρτητο από τη γνώση μας γι΄ αυτά. Συγκεκριμένα, τα μαθηματικά αντικείμενα:

- Υπάρχουν έξω από τον χώρο και το χρόνο της φυσικής ύπαρξης.
- Περιγράφουν αναλλοίωτες δομικές σχέσεις ενός σύμπαντος αναλλοίωτων αντικειμένων και δεν υπόκεινται σε χωροχρονικές μεταβολές.
- Δεν εξαρτώνται από τη δυνατότητα ή μη του μαθηματικού να τα συλλάβει.

Ο μαθηματικός για τον Πλατωνιστή είναι ένας εμπειρικός επιστήμονας όπως ο γεωλόγος και δεν μπορεί να εφεύρει τίποτε επειδή όλα υπάρχουν ήδη. Οι μαθηματικές αλήθειες υπάρχουν ανεξάρτητα απ΄ αυτόν και αναμένουν υπομονετικά την εξερεύνηση τους. **Ο μαθηματικός δεν δημιουργεί αλλά ανακαλύπτει μαθηματικά.**

Η χρήση σχημάτων, γραμμών και εικόνων σχετίζεται με την αισθητηριακή παρατήρηση που υποβοηθάει στη σύλληψη των ιδεών και όχι στην εφεύρεσή τους. Πολλές φορές η ανακάλυψη των μαθηματικών αληθειών περνάει μέσα

από δαιδαλώδεις κατασκευαστικές διαδικασίες. Αυτές είναι απαραίτητες για την ανακάλυψη της αλήθειας αλλά δεν αποτελούν απαραίτητο συστατικό της.

Μια μαθηματική πρόταση είναι αληθής ή όχι, επειδή αντιστοιχεί ή όχι σε κάποια συγκεκριμένα δομικά χαρακτηριστικά του σύμπαντος των μαθηματικών ιδεών τα οποία περιγράφει. Η συγκεκριμένη κατασκευή και γενικά η διαδικασία που θα χρησιμοποιηθεί για την ανακάλυψη της παίζει ρόλο καθαρά βοηθητικό και αντιπροσωπεύει το μίτο της Αριάδνης για την έξοδο από το λαβύρινθο. Η έξοδος από το λαβύρινθο υπάρχει ανεξάρτητα από το μίτο.

Ο Πλατωνισμός κυριάρχησε για αρκετούς αιώνες αποτελώντας έναν από τους βασικότερους αστερισμούς στο φιλοσοφικό στερέωμα, σε βαθμό που πολλές φορές εμπόδισε την ανάπτυξη αντίθετων φιλοσοφικών ρευμάτων. Ο **Gödel** τον θεώρησε ως τη μόνη ολοκληρωμένη απάντηση στο μεταφυσικό πρόβλημα της ύπαρξης ή μη ύπαρξης των μαθηματικών οντοτήτων. Επίσης, ο **Frege** ως ένα βαθμό θα μπορούσε επίσης να θεωρηθεί σαν θιασώτης του. Πριν από αυτούς Πλατωνιστές ήταν οι **Newton, Leibniz, Descartes**.

Ο Πλατωνισμός, ως φιλοσοφικό σύστημα, γοητεύει και έλκει τους μαθηματικούς σε μεγαλύτερο ποσοστό απ' ότι άλλους επιστήμονες. Το γεγονός αυτό οφείλεται, πιθανώς, στο ότι το αντικείμενο ενασχόλησης των μαθηματικών δεν έχει τον υλικό χαρακτήρα του αντικειμένου ενασχόλησης των επιστημόνων άλλων κλάδων (π.χ. φυσικών επιστημόνων). Η αισθητηριακή αντίληψη παίζει εντελώς δευτερεύοντα ρόλο και η ανακάλυψη συγκεκριμένων αληθειών με τη μορφή θεωρημάτων ακολουθεί διαδρομές που δίνουν την εντύπωση πως είναι καθαρά νοητικές. Αναπτύσσεται δηλαδή ένα είδος εποπτείας (intuition) που βοηθάει τους μαθηματικούς να διαμορφώσουν, από ένα στάδιο και πέρα, την εντύπωση πως αυτή η εποπτεία αποτελεί ένα στοιχείο του νοητικού τους οπλισμού, κατάλληλο για να παίξει ρόλο στην ανακάλυψη αληθειών τελείως ανάλογο με το ρόλο που παίζει η αισθητηριακή αντίληψη στις επιστήμες της φύσης.

1.1.ii. Ο Φορμαλισμός

Σύμφωνα με το φορμαλισμό, του οποίου θεμελιωτής υπήρξε ο **Hilbert (1862-1943) δεν υπάρχουν μαθηματικά αντικείμενα**. Απλά τα μαθηματικά αποτελούνται από αξιώματα, ορισμούς και θεωρήματα - με άλλα λόγια από τύπους. Από μια ακραία άποψη, υπάρχουν κανόνες με τους οποίους φτάνουμε από τον ένα τύπο στον άλλο, αλλά οι τύποι δεν αφορούν τίποτε. Είναι απλά σειρές συμβόλων.

Βέβαια ο φορμαλιστής γνωρίζει ότι οι μαθηματικοί τύποι εμφανίζονται και στα φυσικά προβλήματα. Όταν δίνεται μια φυσική ερμηνεία σε έναν τύπο, αυτός αποκτά μια σημασία που μπορεί να είναι αληθής ή ψευδής. Αλλά αυτή η αλήθεια ή η σφαλερότητα έχουν να κάνουν με τη συγκεκριμένη φυσική ερμηνεία. Ως καθαρά μαθηματικός τύπος δεν έχει κανένα νόημα και καμία τιμή αληθείας.

1.1.iii. Ο Ιντουισιονισμός

Οι φορμαλιστές και οι Πλατωνιστές αντιμετωπίζουν από αντίθετες πλευρές το ζήτημα της ύπαρξης και της πραγματικότητας. Αλλά δε διαφωνούν για το ποιες αρχές συλλογισμού επιτρέπονται να χρησιμοποιούνται στην μαθηματική πρακτική. Ο τρόπος δημιουργίας μαθηματικών ήταν γι' αυτούς «υπεράνω πάσης υποψίας».

Αντίθετοι και με τους δυο είναι οι ιντουισιονιστές. Ιδρυτής της σχολής των ιντουισιονιστών, η οποία αμφισβήτησε την υπάρχουσα μαθηματική πρακτική και θεσμοθέτησε την ανάγκη ξεκαθαρίσματός της, υπήρξε ο Ολλανδός μαθηματικός **L. E. J. Brouwer (1821 -1966).**

Τα ιντουισιονιστικά μαθηματικά ξεκινούν από διαφορετικές μαθηματικές προϋποθέσεις και ακολουθώντας διαφορετικές λογικές αρχές από αυτές της κλασικής λογικής, διατυπώνουν διαφορετικά θεωρήματα από αυτά των κλασικών μαθηματικών. Σ' αυτά **μπορούμε να υποστηρίξουμε την ύπαρξη μιας οντότητας x στο βαθμό που μπορούμε να δώσουμε έναν αλγόριθμο**

που βήμα προς βήμα υπολογίζει /κατασκευάζει την οντότητα x. Έτσι, για παράδειγμα, η συνεπαγωγή μπορεί να δικαιολογηθεί μόνο από μια κατασκευή η οποία μετατρέπει κάθε δεδομένη δικαιολόγηση της υπόθεσης, σε μια δικαιολόγηση του συμπεράσματος. Τα κλασικά μαθηματικά δέχονται τις αρχές της κλασικής λογικής (ταυτότητας, μη αντίφασης, απόκλισης τρίτου). Η τελευταία δεν ισχύει στα ιντουισιονιστικά μαθηματικά , όπου, όπως τονίζει ο Brower

> *«η ύπαρξη μαθηματικού συστήματος που ικανοποιεί ένα σύνολο αξιωμάτων δεν μπορεί ποτέ να αποδειχθεί από τη συνέπεια του λογικού συστήματος που βασίζεται σ' αυτά τα αξιώματα, αλλά μόνο με κατασκευή…. A fortiori (κατά μείζονα λόγο) δεν είναι βέβαιο ότι κάθε μαθηματικό πρόβλημα μπορεί είτε να λυθεί είτε να αποδειχθεί ότι δεν λύνεται».*

1. 2 Προβλήματα στα θεμέλια

1.2.i. Ο Ευκλείδης και η αξιωματική θεμελίωση της Γεωμετρίας

Το πρώτο γνωστό αξιωματικό σύστημα παρουσιάστηκε από τον **Ευκλείδη** γύρω στο 300 π.Χ. και από τότε η προσέγγιση αυτή αποτελεί την προσέγγιση κάθε παραγωγικής επιστήμης. Αυτό περιλαμβάνει:

- 23 ορισμούς βασικών εννοιών,
- 5 αιτήματα και
- 5 (7 ή κατ' άλλους 9) κοινές έννοιες.

Οι ορισμοί αυτοί δεν αξιώνουν την ύπαρξη των καθοριζόμενων εννοιών. Η ύπαρξή τους θα στηριχθεί σε αιτήματα είτε θα αποδειχθεί στις προτάσεις. Από εκεί και πέρα, κάθε πρόταση που διατυπώνεται, προκύπτει είτε απευθείας από τα δομικά συστατικά του συστήματος, είτε με τη βοήθεια της λογικής, μέσω των κανόνων συμπερασμού, από προηγουμένως αποδειχθείσες προτάσεις.

Βασικοί όροι (σύνδεσμοι) της λογικής είναι **η συνεπαγωγή, η αντίστροφη συνεπαγωγή και η αντιθετοαντίστροφη συνεπαγωγή.**

Συνεπαγωγή των προτάσεων P, Q με υπόθεση (ηγούμενη) την P και συμπέρασμα (επόμενη) την Q είναι μια πρόταση της μορφής

«Αν P, τότε Q» ή «P συνεπάγεται Q»

και συμβολίζεται $P \Rightarrow Q$.

Μια συνεπαγωγή είναι ψευδής μόνο αν η P είναι αληθής και η Q ψευδής.

Η συνεπαγωγή $Q \Rightarrow P$ λέγεται **αντίστροφη** της $P \Rightarrow Q$.

Αν οι P, Q είναι είτε και οι δύο αληθείς είτε και οι δυο ψευδείς, τότε λέμε ότι είναι **ισοδύναμες** και συμβολίζουμε $P \Leftrightarrow Q$.

Η συνεπαγωγή $\bar{Q} \Rightarrow \bar{P}$, όπου $\bar{P}, \bar{Q}$ είναι οι αρνήσεις των P, Q, λέγεται **αντιθετοαντίστροφη** της $P \Rightarrow Q$. Δυο αντιθετοαντίστροφες συνεπαγωγές έχουν το ίδιο λογικό περιεχόμενο δηλαδή είναι ισοδύναμες.

Στα «Στοιχεία» εφαρμόζονται οι ακόλουθες τρεις **αποδεικτικές μέθοδοι**:

- **Η συνθετική**: Σύμφωνα με αυτή, προκειμένου να αποδείξουμε μια πρόταση, χρησιμοποιούμε τους ορισμούς, τα αξιώματα και άλλες ήδη γνωστές προτάσεις (που κι αυτές, με τη σειρά τους, απορρέουν από τα αξιώματα και τους ορισμούς) και με λογικούς συλλογισμούς καταλήγουμε στην αποδεικτέα.
- **Η αναλυτική:** Σύμφωνα με αυτή για να αποδείξουμε μια πρόταση P, αναζητούμε μια πρόταση P_1 της οποίας η ισχύ εγγυάται και την ισχύ της P, κατόπιν μια άλλη P_2 από την οποία απορρέει η P_1 κ.ο.κ. μέχρι να καταλήξουμε σε μια αληθή πρόταση P_v από την οποία προκύπτει η P_{v-1}. Έτσι η απόδειξη της P προκύπτει με αφετηρία την αληθή πρόταση P_v και τις συνεπαγωγές $P_v \Rightarrow P_{v-1} \Rightarrow \ldots \Rightarrow P_2 \Rightarrow P_1 \Rightarrow P$.
- Η **εις άτοπον απαγωγή**: Σύμφωνα με αυτήν, για να αποδείξουμε μια συνεπαγωγή $P \Rightarrow Q$ δεχόμαστε αρχικά ότι αληθεύει η αντίθετη της. Χρησιμοποιώντας, όπως πριν, τα αξιώματα και άλλες γνωστές προτάσεις καταλήγουμε σε μία πρόταση η οποία αντιφάσκει είτε με κάποιο αξίωμα είτε με κάποιαν άλλη πρόταση, που ήδη έχει αποδειχθεί ότι αληθεύει. Η αντίφαση προκύπτει, προφανώς, επειδή ξεκινήσαμε από μια λαθεμένη υπόθεση και αίρεται αν δεχτούμε την αλήθεια της αρχικής πρότασης.

Η απαγωγή σε άτοπο συχνά συνδέεται με την αντιθετοαντίστροφη συνεπαγωγή χωρίς φυσικά να είναι το ίδιο. Για την ακρίβεια η απαγωγή σε άτοπο της $P \Rightarrow Q$ αποδίδεται με την συνεπαγωγή $(P \wedge \bar{Q}) \Rightarrow (S \wedge \bar{S})$ όπου η πρόταση S μπορεί να είναι οποιαδήποτε.

Ο πιο συνηθισμένος κανόνας συμπερασμού είναι ο κ**ανόνας απόσπασης (modus ponens)** που διατυπώνεται με την εξής μορφή

«Αν p αληθής και $p \Rightarrow q$ αληθής, τότε q αληθής».

1.2.ii. Μη Ευκλείδειες Γεωμετρίες

Μέχρι τις πρώτες δεκαετίες του 19ου αιώνα η γεωμετρία του Ευκλείδη θεωρείτο ως ο πιο σταθερός, ο πιο αξιόπιστος κλάδος της γνώσης. Οι αλήθειες της μας επιβάλλονται με τον τρόπο που λειτουργεί η νόησή μας. Ο **Kant (1724–1804)**, στο περίφημο έργο του **«Κριτική του Καθαρού Λόγου»**, θεωρεί ότι **η Ευκλείδεια Γεωμετρία είναι η μόνη γεωμετρία την οποία μπορεί να αντιληφθεί ο ανθρώπινος νους, εξαιτίας της δομής του εγκεφάλου του.** Από αυτή την άποψη καταλήγει στο συμπέρασμα ότι η γνώση του χώρου δεν είναι εμπειρική, αλλά υπάρχει a priori.

Διάφοροι νέοι κλάδοι, όπως ο απειροστικός λογισμός, κατανοήθηκαν και νομιμοποιήθηκαν μέσα από το δεσμό τους με την γεωμετρία η οποία μέχρι εκείνη την εποχή ήταν απλά γεωμετρία και μελετούσε τις ιδιότητες του χώρου. Ο όρος Ευκλείδεια γεωμετρία άρχισε να χρησιμοποιείται αφότου ανακαλύφθηκαν μη Ευκλείδειες γεωμετρίες και έγινε αποδεκτό ότι ήταν νοητές περισσότερες από μια γεωμετρίες.

Το πέμπτο αίτημα του Ευκλείδη, αν και φαίνεται συμβατό με τη διαίσθηση, εντούτοις ο τρόπος που διατυπώθηκε έδωσε την αίσθηση σε πολλούς μαθηματικούς ότι πρόκειται για κάτι πιο πολύπλοκο ώστε να ονομαστεί αίτημα και μάλλον θα έπρεπε να αποδειχθεί ως πρόταση. Προς την κατεύθυνση αυτή φαίνεται να συνηγορεί και το ότι ο Ευκλείδης καθυστέρησε όσο το δυνατόν περισσότερο να το χρησιμοποιήσει (πρώτη χρήση του γίνεται

στην πρόταση Ι. 29, ενώ είχε ήδη αποδείξει το αντίστροφό του στην πρόταση Ι. 17). Έτσι ακολούθησαν προσπάθειες οι οποίες επικεντρώθηκαν είτε στην κατάργηση και την απόδειξη του μέσω των άλλων αιτημάτων, είτε στην αντικατάστασή του με ένα πιο αποδεκτό ισοδύναμο αίτημα. Από τα διάφορα υποκατάστατα αξιώματα που προέκυψαν κατά καιρούς, το πλέον συνηθισμένο είναι το αποκαλούμενο αξίωμα του **Playfair:**

> *«Από ένα δεδομένο σημείο, που δεν βρίσκεται πάνω σε μια δεδομένη ευθεία, μπορούμε να φέρουμε μια μόνο ευθεία παράλληλη προς τη δεδομένη»*

παρόλο που είχε χρησιμοποιηθεί και διατυπωθεί ήδη από τον 5ο αιώνα μ. Χ. από τον νεοπλατωνικό φιλόσοφο **Πρόκλο.** Με τη μορφή αυτή φαίνεται να χρησιμοποιήθηκε, χωρίς να αναφέρεται, από τον **Κλαύδιο Πτολεμαίο** (περίπου 150 μ.Χ.) στην πιο παλιά απόπειρα απόδειξης 5ου αιτήματος που μας είναι γνωστή.

Πάνω στην άρνηση του αιτήματος αυτού βασίστηκε η πρώτη και σημαντικότερη μορφή μη ευκλείδειας γεωμετρίας που είναι η υπερβολική γεωμετρία. Πρόκειται για τον τύπο γεωμετρίας στην οποία αληθεύουν τα τέσσερα πρώτα αιτήματα του Ευκλείδη, το πέμπτο όμως αντικαθίσταται από την πρόταση

«υπάρχουν περισσότερες από μια ευθείες διερχόμενες από σημείο και παράλληλες σε δοθείσα ευθεία».

Η επίσημη πρωτιά της ανακάλυψης της υπερβολικής γεωμετρίας ανήκει στους **Janos Bolyai (1802 - 1860)** και **Nikolai Lobatcevsky (1793 - 1856)**, έναν Ούγγρο και έναν Ρώσο, οι οποίοι δημοσίευσαν σε βιβλίο το 1832 και 1829, αντίστοιχα, ανεξάρτητα ο ένας από τον άλλο, ότι αυτός ο τύπος γεωμετρίας αποτελεί συλλογή θεωρημάτων το ίδιο σημαντική με εκείνη της Ευκλείδειας γεωμετρίας. Και οι δυο συμμερίζονταν την άποψη ότι η υπερβολική γεωμετρία μπορούσε να περιγράψει τον φυσικό μας χώρο κατά τρόπο εξίσου επαρκή με εκείνον της Ευκλείδειας γεωμετρίας.

Η σπουδαιότητα αυτής της ανακάλυψης είναι ανυπολόγιστη. Για περισσότερες από δυο χιλιάδες χρόνια κυριαρχούσε η αίσθηση ότι η Ευκλείδεια γεωμετρία ήταν απαραίτητα η γεωμετρία του χώρου. Τα μαθηματικά και η Φυσική συνυφαίνονταν τόσους αιώνες με το νήμα αυτής της πίστης. **Η υπερβολική γεωμετρία έδειξε ότι υπάρχουν και άλλες περιγραφές του χώρου προσιτές στην ανθρώπινη νόηση.** Η μελέτη του φυσικού χώρου πέρασε στην επικράτεια της φυσικής και τα μαθηματικά απέκτησαν έναν πιο αφηρημένο χαρακτήρα. Κατέστη πλέον φανερό ότι μπορούσε κανείς να ξεκινήσει με ένα τυχαίο σύνολο αξιωμάτων και να μελετήσει τις αφηρημένες συνέπειές τους.

Ένα άλλο καθοριστικό γεγονός που επέδρασε καταλυτικά στις διεργασίες που ακολούθησαν ήταν η ανάπτυξη της ανάλυσης σε βαθμό που κυρίευσε τη γεωμετρική ενόραση, όπως η ανακάλυψη των καμπύλων που γεμίζουν το χώρο ή των συνεχών καμπύλων που δεν είναι πουθενά διαφορίσιμες. Αυτές οι συγκλονιστικές εκπλήξεις έδειξαν πόσο ευπρόσβλητο είναι ένα στέρεο θεμέλιο πάνω στο οποίο είχε θεωρηθεί ότι στηρίζονται τα μαθηματικά. **Η απώλεια της βεβαιότητας στη γεωμετρία ήταν φιλοσοφικά ανυπόφορη επειδή υπονοούσε την απώλεια κάθε βεβαιότητας στην ανθρώπινη γνώση.**

1.2.iii. Οι πρώτες προσπάθειες επαναθεμελίωσης

Οι μαθηματικοί του δέκατου ένατου αιώνα με πρωτεργάτες τους **Dedekind** και **Weiertrass** αναζήτησαν στην αριθμητική το θεμέλιο των μαθηματικών. Στην προσπάθειά τους αυτή ήταν αναγκαίο να δώσουν μια δομή στο γραμμικό συνεχές, δηλαδή στο σύστημα των πραγματικών αριθμών και να δείξουν πως αυτό μπορούσε να δημιουργηθεί από τους ακεραίους 1, 2, 3, … Όλες οι διαφορετικοί μέθοδοι που προτάθηκαν, από τους **Dedekind, Cantor** και **Weiertrass**, στην προσπάθειά τους να ορίσουν ή να κατασκευάσουν έναν πραγματικό αριθμό, χρειάστηκε να χρησιμοποιήσουν απειροσύνολα ρητών αριθμών. Αυτό σημαίνει ότι **η προσπάθεια αναγωγής**

της ανάλυσης και της γεωμετρίας στην αριθμητική απαιτούσε την εισαγωγή απειροσυνόλων στη θεμελίωση των μαθηματικών.

Η θεωρία των συνόλων αναπτύχθηκε από τον **Cantor** ο οποίος θεώρησε ότι η ιδέα του συνόλου ήταν τόσο απλή και θεμελιώδης, που θα μπορούσε να γίνει ο θεμέλιος λίθος στη δόμηση όλων των μαθηματικών. Στην αρχή η θεωρία συνόλων σχετίστηκε με τη λογική καθότι η σχέση του περιέχεσθε στη θεωρία συνόλων μπορεί να γραφεί με τη μορφή συνεπαγωγής «αν Α τότε Β». Οι νόμοι της λογικής θεωρήθηκαν αντικειμενικοί και αναμφισβήτητοι. Έτσι υπήρξε μια προσπάθεια αναγωγής των μαθηματικών στη λογική μέσα από το πρόγραμμα των λογικιστών. Κύριοι εκφραστές αυτής της προσπάθειας ήταν οι **Russell** και **Whitehead** με το βιβλίο τους **Principa Mathematica**. Επίσης ο **Frege** ανέλαβε ένα πρόγραμμα θεμελίωσης της αριθμητικής (αριθμητική και ανάλυση) διαμέσου ορισμών και λογικών νόμων, το οποίο ανάγει την αριθμητική (τις κύριες έννοιες και τους νόμους της) σε γενικότατες αρχές της σκέψης. Παρόλες αυτές τις προσπάθειες όμως, ο ίδιος ο Russell ανακάλυψε ότι η έννοια του συνόλου περιείχε απρόσμενες παγίδες που οδηγούσαν σε αντιφάσεις, που ονομάστηκαν παράδοξα. Ας δούμε σε τι συνίσταται **το παράδοξο του Russell.**

Την εποχή εκείνη κυριαρχούσε η εντύπωση ότι για την περιγραφή ενός συνόλου αρκούσε μια ιδιότητά του. Θεωρούσαν δηλαδή, οι μαθηματικοί, σαν σύνολο οποιαδήποτε συλλογή αντικειμένων (νοητών ή μη) και πίστευαν πως, δεδομένης μιας ιδιότητας, τα αντικείμενα που την ικανοποιούν αποτελούν τα στοιχεία μιας τέτοιας συλλογής.

Εδώ, πρέπει να τονιστεί, ότι τα στοιχεία του συνόλου μπορεί να είναι επίσης σύνολα, και ότι η έννοια του συνόλου χρησιμοποιείται διαισθητικά όπως ορίστηκε από τον Cantor. Στο πλαίσιο αυτό, πολλά σύνολα δεν είναι στοιχεία του εαυτού τους, ενώ άλλα είναι. Έτσι, για παράδειγμα, το σύνολο των ανθρώπων δεν είναι άνθρωπος, ενώ το σύνολο των αφηρημένων ιδεών είναι αφηρημένη ιδέα.

Ας θεωρήσουμε το σύνολο $A=\{x: x\notin x\}$.

Τότε έχουμε

είτε

- $A\in A$, οπότε $A\notin A$ σύμφωνα με την ορίζουσα ιδιότητα των στοιχείων του A

είτε

- $A\notin A$, οπότε $A\in A$ σύμφωνα με την ορίζουσα ιδιότητα των στοιχείων του A.

Έτσι, και στις δυο περιπτώσεις, καταλήγουμε στο παράδοξο συμπέρασμα ότι το A είναι και δεν είναι στοιχείο του A.

1.2.iv. Τα νέα θεμέλια. Τυπικά αξιωματικά συστήματα.

Αυτή η κρίση στα θεμέλια ήταν το κεντρικό θέμα στις διαμάχες που έλαβαν χώρα στο πρώτο τέταρτο του εικοστού αιώνα. Για το ξεπέρασμα της κρίσης υπήρξαν τρεις προτάσεις θεραπείας.

Η πρώτη πρόταση της σχολής των **«λογικιστών»** με εκφραστές τους **Frege** και **Russell** επιδίωκε να βρει μια αναδιατύπωση της θεωρίας συνόλων, ικανή να αποφύγει το παράδοξο του Russell και να εδραιώσει τα μαθηματικά πάνω στη λογική. Στην προσπάθειά τους αυτή η θεωρία συνόλων έγινε μια πολύπλοκη δομή που δύσκολα αναγνωριζόταν πλέον ως λογική. Ο ίδιος ο Russell παραδέχεται ότι

> *«… μετά από είκοσι χρόνια υπερβολικά επίπονης εργασίας, έφθασα στο συμπέρασμα ότι δεν μπορούσα να κάνω τίποτε περισσότερο για να γίνει η μαθηματική γνώση αναμφισβήτητη».*

Η δεύτερη σχολή ήταν αυτή των **ιντουισιονιστών** με κύριο εκφραστή τον **L. E. J. Brouwer**. Η θέση του ήταν ότι οι φυσικοί αριθμοί μας δίνονται από μια θεμελιώδη ενόραση που είναι το σημείο εκκίνησης για όλα τα

μαθηματικά. Τα μαθηματικά αντικείμενα έχουν νόημα και υπάρχουν μόνο αν δοθούν με μια κατασκευή, σε πεπερασμένα βήματα, ξεκινώντας από τους φυσικούς αριθμούς. Το γεγονός ότι η άρνηση της ύπαρξης οδηγεί σε αντίφαση δεν αρκεί. Αρχές όπως ο νόμος της τριχοτομίας δεν είναι αποδεκτές στα ιντουισιονιστικά μαθηματικά. Στην προσπάθειά του να τεκμηριώσει αυτή την άρνηση κατασκεύασε (περιέγραψε) αριθμό για τον οποίο δεν είμαστε σε θέση να αποδείξουμε κατασκευαστικά ότι είναι θετικός, αρνητικός ή μηδέν.

Η τρίτη σχολή των **φορμαλιστών** με κύριο εκφραστή τον **Hilbert,** ανέπτυξε πρόγραμμα θεμελίωσης των μαθηματικών που επεδίωκε να υπερβεί τις εγγενείς αδυναμίες του λογικισμού διατυπώνοντας το πρόγραμμα του **περατοκρατισμού** (finitism) **το οποίο προέβλεπε την κωδικοποίηση των μαθηματικών σε μια τυπική γλώσσα.** Στο πρόγραμμα ανασυγκρότησης του Hilbert δεν αμφισβητείται η αντικειμενική ύπαρξη των στοιχειωδών μαθηματικών οντοτήτων, ενώ προβάλλεται η άμεση εποπτικότητα και αναγνωσιμότητα των αληθών προτάσεων. Παραμένει όμως η ένταση μεταξύ διαισθητικής αλήθειας και αποδειξιμότητας (provability). Έτσι εγείρεται το ερώτημα, ποιες διαισθητικές αληθείς προτάσεις προκύπτουν ως θεωρήματα μέσα στα πλαίσια ενός αξιωματικού συστήματος;

Ο Ευκλείδης στην θεμελίωσή του, που ήδη έχουμε εκθέσει, δεν χρησιμοποίησε απροσδιόριστους όρους και στηρίχθηκε υπερβολικά στη διαίσθηση κατά την ανάπτυξη των επιχειρημάτων του. Ο **Morris Kline** συνόψισε με τον ακόλουθο εύστοχο τρόπο το πρόβλημα με την Ευκλείδεια προσέγγιση

> *«η Ευκλείδεια Γεωμετρία φιλοδόξησε να προσφέρει ακριβείς αποδείξεις θεωρημάτων τα οποία υποβάλλει η διαίσθηση, αντ' αυτού όμως έδωσε διαισθητικές αποδείξεις σχημάτων σχεδιασμένων με ακρίβεια».*

Οι εξελίξεις αυτές κλόνισαν την πίστη στα «διαισθητικά» προφανή δεδομένα των αξιωματικών συστημάτων και αναζήτησαν συστήματα αξιωμάτων όπου η διαίσθηση θα είχε περιοριστεί δραστικά ή θα είχε

εξαλειφθεί. Έτσι προέκυψε η δημιουργία των **τυπικών αξιωματικών συστημάτων**.

Ένα τυπικά αξιωματικό σύστημα αποτελείται από

- ορισμένους απροσδιόριστους όρους,
- πιθανώς από κάποιους προσδιορισμένους όρους (βασισμένους στους απροσδιόριστους όρους),
- ορισμένες διατυπώσεις αποκαλούμενες αξιώματα και
- άλλες διατυπώσεις που καλούνται θεωρήματα και τα οποία συνάγονται λογικά από τα αξιώματα.

Τα αξιώματα, ουσιαστικά, παρέχουν την απαραίτητη γνώση για τους απροσδιόριστους όρους.

Ο φορμαλισμός θεωρεί τα μαθηματικά ως ένα παιχνίδι ανάλογο με το σκάκι όπου τα πιόνια και η σκακιέρα «παίζουν» συμβολικούς ρόλους ή ως γενική θεωρία των συμβολικών παιχνιδιών ή ακόμα ως ένα σύστημα πλήρους νοήματος που αφορά συμβολικά αντικείμενα στη βάση των οποίων αναπτύσσεται στη συνέχεια το μαθηματικό παιχνίδι (**Resnik 1980**).

Ο Hilbert θεώρησε την φορμαλιστική ερμηνεία των μαθηματικών ως το αναγκαίο τίμημα για να πετύχει τη βεβαιότητα. Ο ίδιος στην ομιλία του με τον τίτλο **«On the Infinite»** αναφέρει:

> *«Ο στόχος της θεωρίας μου είναι να εδραιώσω μια και καλή τη βεβαιότητα των μαθηματικών μεθόδων… Η τωρινή κατάσταση ως προς τα παράδοξα, είναι αφόρητη. Σκεφθείτε μόνο ότι στα μαθηματικά, το πρότυπο της βεβαιότητας και της αλήθειας , οι ορισμοί και οι μέθοδοι παραγωγής που όλοι μαθαίνουν, διδάσκουν και χρησιμοποιούν, οδηγούν σε παραλογισμούς!* ***Και που θα βρει κανείς βεβαιότητα και αλήθεια, αν ακόμα και η μαθηματική σκέψη είναι ατελής;****»*

Η δουλειά του Hilbert στη Γεωμετρία στο τέλος του 19ου αιώνα εκπροσωπεί το αποκορύφωμα όλων αυτών των θεμελιωτικών εξελίξεων. Το πρόγραμμα εφαρμόστηκε στο έργο του **«Θεμέλια της Γεωμετρίας» (1899)** και σήμανε το τέλος στον ουσιαστικό ρόλο της διαίσθησης στην γεωμετρία. Παρόλο που η χωρική διαίσθηση ή παρατήρηση παραμένει η πηγή των αξιωμάτων της

Ευκλείδειας Γεωμετρίας, στα γραπτά του Hilbert ο ρόλος της διαίσθησης και της παρατήρησης είναι αποκλειστικά περιορισμένος στο να δοθούν κίνητρα και να είναι ευρετικός. **Εφόσον τα αξιώματα έχουν διατυπωθεί, η διαίσθηση και η παρατήρηση εξαφανίζονται. Δεν είναι μέρος των μαθηματικών.**

Το 1900 ο Hilbert στο διεθνές συνέδριο μαθηματικών που διεξήχθη στο Παρίσι σε ομιλία του **«Μαθηματικά προβλήματα»** εμφανίστηκε και μιλώντας σαν προφήτης των μαθηματικών επιτευγμάτων που θα έφερνε ο επόμενος αιώνας, παρουσίασε μια λίστα από 23 προβλήματα που θεωρούσε σημαντικότερο να λυθούν. Στην εισαγωγή του, που θύμιζε εμψυχωτικό λόγο πριν από ένα σημαντικό αγώνα, ο Hilbert ενθάρρυνε το μαθηματικό του ακροατήριο με την διαβεβαίωση ότι όσο δύσκολα και αν φαίνονται κάποια προβλήματα, η νίκη είναι αναπόφευκτη.

> *«Η πεποίθηση ότι όλα τα μαθηματικά προβλήματα μπορούν να λυθούν, αποτελεί για μας ισχυρό κίνητρο. Μέσα μας ακούμε το αέναο κάλεσμα: Ιδού το πρόβλημα. Ψάξε για τη λύση του. Μπορείς να την βρείς μέσω του καθαρού λόγου, γιατί στα μαθηματικά δεν υπάρχουν ignorabimus» και κατέληγε: «**Πρέπει να μάθουμε, θα μάθουμε (We must know, We shall know)**».*

Κάποια από τα πιο γνωστά εκ των προβλημάτων είναι τα ακόλουθα:

- η υπόθεση του συνεχούς,
- η καλή διάταξη των πραγματικών αριθμών,
- η εικασία του Goldbach,
- η υπερβατότητα των δυνάμεων αλγεβρικών αριθμών,
- η υπόθεση του Rieman κτλ.

Από αυτά άλλα έχουν απαντηθεί είτε θετικά είτε αρνητικά, για άλλα, όπως για την υπόθεση του συνεχούς, έχει αποδειχθεί ότι δεν μπορούμε να αποφανθούμε και άλλα είναι ακόμη άλυτα.

Στο τέταρτο μέρος της παρούσας εργασίας θα ασχοληθούμε με το τρίτο εκ των προβλημάτων το οποίο στη μορφή που θα το διαπραγματευθούμε διατυπώνεται ως εξής:

Είναι δυνατόν να διαμερίσουμε, με τη βοήθεια επιπέδων, ένα κανονικό τετράεδρο σε πεπερασμένα μέρη τα οποία αν επικολληθούν κατάλληλα να μας δώσουν κύβο;

1.2.ν. Συνέπεια – ανεξαρτησία- ισοδυναμία – πληρότητα

Ένα αξιωματικό σύστημα καλείται **ασυνεπές** αν οδηγεί σε κάποια αντίφαση, αν δηλαδή είναι δυνατόν να αποδειχθεί στο πλαίσιό του ότι μια πρόταση είναι ταυτόχρονα αληθής και ψευδής. Συνήθως, ως τέτοια επιλέγεται ένα αξίωμα του οποίου η αλήθεια θεωρείται κατά τετριμμένο τρόπο εξασφαλισμένη.

Ένα αξίωμα σε ένα συνεπές αξιωματικό σύστημα λέγεται **εξαρτημένο,** αν μπορεί να αποδειχθεί βάσει των άλλων αξιωμάτων του. Κατά συνέπεια, ένα τέτοιο αξίωμα περιττεύει. Ένα αξίωμα είναι **ανεξάρτητο** αν δεν μπορεί να αποδειχθεί βάσει των άλλων αξιωμάτων.

Δυο αξιωματικά συστήματα που περιλαμβάνουν τους ίδιους απροσδιόριστους όρους λέγονται **ισοδύναμα**, αν σε καθένα από αυτά μπορούν να συναχθούν τα ίδια θεωρήματα. **Δυο ισοδύναμα αξιώματα μπορούν να θεωρηθούν ως υποκατάστατα αξιώματα με την έννοια ότι το ένα μπορεί να υποκαταστήσει το άλλο, χωρίς να επέλθει καμία αλλαγή στο περιεχόμενο του αξιωματικού συστήματος.**

Ένα αξιωματικό σύστημα λέγεται **πλήρες** (complete), όταν, μπορούμε να αποφανθούμε για την ισχύ ή όχι, κάθε πρότασης η οποία μπορεί να διατυπωθεί με τους όρους και τα αξιώματα του συστήματος. Αυτό, ισοδύναμα, σημαίνει ότι δεν είναι δυνατόν να προσθέσουμε στο σύστημα κι ένα άλλο ανεξάρτητο αξίωμα.

1.2.vi. Το άδοξο τέλος. Ο Kurt Gödel

Τελικά η βεβαιότητα των μαθηματικών μεθόδων που αναζητούσε ο Hilbert δεν επρόκειτο να βρεθεί ούτε με το τίμημα της φορμαλιστικής ερμηνείας.

Το 1931, ο Αυστριακός **Kurt Gödel** δημοσίευσε μία εργασία, που ανέτρεψε καταρχήν την αντίληψη ότι το σύστημα μεγεθών, που αποτελούν οι φυσικοί αριθμοί, μπορεί να περιγραφεί πλήρως με ένα πεπερασμένο σύστημα αξιωμάτων. Το λεγόμενο **θεώρημα μη πληρότητας** του Gödel λέει ουσιαστικά ότι: **Αν, οποιαδήποτε φορμαλιστική θεωρία που είναι επαρκής για να περιλάβει την θεωρία των ακεραίων αριθμών, είναι συνεπής, τότε είναι κατ' ανάγκη μη πλήρης.**

Στην συνέχεια, και με βάση αυτό το θεώρημα, ο Gödel με το δεύτερο θεώρημά του απέδειξε ότι ποτέ δεν θα μπορέσουμε να αποδείξουμε αυτοτελώς την συνέπεια ενός αρκετά εκτενούς συστήματος αξιωμάτων. Πάντα θα είμαστε αναγκασμένοι να καταφύγουμε σε αρχές που βρίσκονται έξω από το σύστημα που εξετάζουμε. Η συνέπεια οποιουδήποτε μαθηματικού συστήματος, που είναι αρκετά εκτενές για να περιλαμβάνει την αριθμητική των ακεραίων αριθμών, δεν μπορεί να επιβεβαιωθεί μόνο με τις λογικές αρχές που αυτό περιλαμβάνει.

Τα θεωρήματα αυτά έφεραν τέλος σε μισό αιώνα προσπαθειών, που ξεκίνησαν από το έργο του Frege και κορυφώθηκαν με το Principa Mathematica και τη διατύπωση του Hilbert, για να βρεθεί ένα σύνολο αξιωμάτων, ικανό για όλα τα μαθηματικά, αφού **πάντα θα υπάρχουν μη αποκρίσιμες προτάσεις, δηλαδή προτάσεις των οποίων η αλήθεια δεν μπορεί ούτε να αποδειχθεί ούτε να διαψευσθεί** θέτοντας ένα αδυσώπητο όριο. Αυτό σημαίνει ότι δεν υπάρχει η δυνατότητα απάντησης όλων των μαθηματικών ερωτημάτων. Όπως εύστοχα έγραψε ο Γάλλος ποιητής και φιλόσοφος **Mallarmé:**

> *«Αν ο κόσμος υπάρχει για να καταλήξει σε ένα βιβλίο, ο Γκέντελ έδειξε ότι αυτό το βιβλίο θα έχει πάντα κάποιες λευκές σελίδες».*

ενώ ο Γάλλος μαθηματικός **André Weil** παρατήρησε:

> *«Ο θεός υπάρχει αφού τα μαθηματικά είναι συνεπή και ο διάβολος υπάρχει αφού δεν μπορούμε να το αποδείξουμε.»*

1. 3 Οι ηλεκτρονικοί υπολογιστές

1.3.i. Οι υπολογιστές και ο ανθρώπινος νους

Στα μέσα του 20ου αιώνα, δημιουργήθηκαν οι πρώτοι ψηφιακοί υπολογιστές και ένα από τα πρώτα ερωτήματα που τέθηκαν αφορούσε τα όρια των δυνατοτήτων ενός υπολογιστή, δεδομένου ότι επιτελεί λειτουργίες που μοιάζουν πολύ με αυτές του ανθρώπινου εγκεφάλου. Συγκεκριμένα ο προβληματισμός που αναπτύχθηκε ήταν κατά πόσο υπήρχε η δυνατότητα «να σκέπτονται οι μηχανές».

Τον Οκτώβριο του 1950 στο Mind: A Quarterly Review of Psychology and Philosophy ο Βρετανός μαθηματικός **Alan Turing**, έθεσε το ερώτημα για πρώτη φορά σαν σοβαρό θεωρητικό ζήτημα. Στο ερώτημα αν οι μηχανές μπορούν να σκέφτονται, το άρθρο του Alan Turing απαντούσε θετικά. Η μηχανή για την οποία μιλούσε ο Turing ήταν μια φανταστική κατασκευή με την ονομασία «καθολική μηχανή». Μια τέτοια μηχανή (υπολογιστής) με τον κατάλληλο προγραμματισμό θα μπορούσε να προσομοιώσει τη λειτουργία του ανθρώπινου εγκέφαλου. Ο ίδιος πρότεινε ένα πολύ απλό αλλά αποτελεσματικό τεστ που θα μπορούσε να απαντάει στο ερώτημα αν μια συγκεκριμένη μηχανή ήταν μία σκεπτόμενη μηχανή ή όχι. Ονόμασε το τεστ αυτό «Το Παιχνίδι της Μίμησης». Έτσι γεννήθηκε η **Τεχνητή Νοημοσύνη** (Artificial Intelligence), ένας καινούργιος κλάδος θεωρητικής αναζήτησης, μια καινοτόμος προσέγγιση σε ένα από τα αρχαιότερα ερωτήματα της ανθρώπινης ιστορίας σχετικά με τη φύση του ανθρώπινου νου. Μέσα από αυτή την προσέγγιση, αναδεικνύονται ερωτήματα όπως ποια είναι τα όρια μεταξύ του «ανθρώπινου» και της «τεχνολογίας» ή μεταξύ του «φυσικού» και

του «τεχνητού». Και σ' αυτά όμως τα ερωτήματα εμπλέκονται τα θεωρήματα του Kurt Gödel.

Η πρώτη εργασία που επεσήμανε τη σύνδεση ανάμεσα στο πρώτο θεώρημα μη πληρότητας του Gödel και τη φύση του ανθρώπινου νου δημοσιεύτηκε το 1961 από τον Οξφορδιανό φιλόσοφο **John Lucas**. Η επιχειρηματολογία του Lucas είναι απλή. Όσο περίπλοκες μηχανές «σκέψης» και αν κατασκευάσουμε, πάντα η λειτουργία τους θα βασίζεται σε προκαθορισμένους κανόνες που μπορούν να διατυπωθούν σε ένα τυπικό σύστημα. Έτσι, όταν φερ' ειπείν θα ζητάμε από τη μηχανή να βρει ποιες προτάσεις είναι αληθείς, για να εκτελέσει την εντολή μας, θα ελέγχει ποιες προτάσεις συμφωνούν με τους κανόνες του συστήματος. Επομένως, θα υπάρχει κάποια πρόταση που η μηχανή δεν θα μπορεί να κατατάξει ως αληθή, δηλαδή ως αποδείξιμη βάσει των κανόνων - την ίδια πρόταση, όμως, ο ανθρώπινος νους θα μπορεί να τη συλλάβει ως αληθή. Όσο και αν βελτιώσουμε τη μηχανή μας προσθέτοντας υπό μορφή αξιωμάτων τις προτάσεις που προηγουμένως της διέφευγαν, πάντα θα υπάρχει κάποια πρόταση που θα της διαφεύγει… ενώ εμείς όχι:

> *Η μηχανή θα είναι ανίκανη να παράγει αυτόν τον τύπο ως αληθή, παρόλο που ένας νους θα καταλάβαινε ότι είναι αληθής. Άρα και πάλι η μηχανή δεν θα αποτελεί ένα ικανοποιητικό μοντέλο του νου. Προσπαθούμε να δημιουργήσουμε ένα μοντέλο του νου που θα είναι μηχανικό – ουσιαστικά, δηλαδή, «νεκρό» - αλλά ο νους ακριβώς επειδή είναι «ζωντανός», θα βρίσκεται πάντα ένα βήμα μπροστά σε σχέση με οποιοδήποτε τυπικό απολιθωμένο, νεκρό σύστημα.*

Χάρη στο θεώρημα του Gödel, ο νους θα έχει πάντα τον τελευταίο λόγο.

Στο ίδιο μήκος κύματος ο διάσημος φυσικός και μαθηματικός **Penrose** υποστηρίζει ότι αυτό που αποδεικνύουν τα θεωρήματα του Gödel είναι ότι η ανθρώπινη σκέψη, ακόμη και στην πιο τεχνική και κανονιστική της μορφή, δηλαδή στα μαθηματικά, χρησιμοποιεί διαδικασίες ανακάλυψης της

αλήθειας που δεν μπορούν να αναχθούν στις μηχανιστικές διεργασίες που προγραμματίζεται να εκτελεί ένας υπολογιστής.

Άλλοι πάλι όπως ο εκ των κορυφαίων της επιστήμης των υπολογιστών **Daniel Hillis** σχετικά με αυτές τις απόψεις αυτές υποστηρίζουν ότι:

> *«Πρόκειται για ένα επιχείρημα το οποίο αγγίζει το συναίσθημά μας… Ανεξάρτητα από το αν τα ανθρώπινα όντα έχουν την ικανότητα να κάνουν διαισθητικά άλματα τα οποία παραμένουν αδύνατα για τους υπολογιστές, το θεώρημα δεν μας παρέχει κανένα λόγο να πιστέψουμε ότι υπάρχουν μαθηματικές προτάσεις που μπορεί να αποδείξει ένας μαθηματικός αλλά όχι και ένας υπολογιστής».*

Έτσι το ερώτημα τίθεται με τη μορφή. Μέχρι που μπορεί να φθάσει ο υπολογιστής; Μπορεί εφοδιασμένος με κατάλληλα προγράμματα, να παράγει μαθηματικές αποδείξεις;

1.3.ii. Το πρόβλημα των τεσσάρων χρωμάτων

Το 1976 οι **Kenneth Appel** και **Wolfang Haken** ανακοίνωσαν ότι απέδειξαν την **«υπόθεση των τεσσάρων χρωμάτων».** Η υπόθεση αυτή είχε ήδη μια ιστορία 124 ετών. Διατυπώθηκε αρχικά ως μαθηματική εικασία το 1852 από τον **Francis Guthrie** και προτάθηκε ως πρόβλημα από τον **Caley** στην Μαθηματική Εταιρεία του Λονδίνου το 1878.

Ας δούμε όμως με απλά λόγια την εν λόγω υπόθεση που αναφέρει ότι κάθε χάρτης σε επίπεδο ή σε σφαίρα μπορεί να χρωματιστεί χωρίς να χρησιμοποιήσουμε περισσότερα από τέσσερα διαφορετικά χρώματα. Οι περιορισμοί που έθετε το πρόβλημα ήταν οι ακόλουθοι:

- Δυο χώρες με κοινά σύνορα δεν πρέπει να έχουν ίδιο χρώμα.
- Αν δυο χώρες συναντιούνται μόνο σε ένα σημείο, τότε επιτρέπεται να έχουν το ίδιο χρώμα.
- Οι χώρες μπορεί να έχουν οποιοδήποτε σχήμα, αλλά κάθε χώρα πρέπει να αποτελείται από ένα μόνο ενιαίο κομμάτι.

Η ανακοίνωση των Appel και Haken, πέρα από το γεγονός ότι επικύρωσε την υπόθεση ενός διάσημου προβλήματος, είχε την ιδιαιτερότητα ότι η απόδειξη περιείχε προγράμματα υπολογιστή και το αποτέλεσμα προέκυπτε από τους υπολογισμούς σύμφωνα με τα προγράμματα.

Η χρήση αυτή του υπολογιστή ήταν εντελώς διαφορετική από τις μέχρι τότε χρήσεις του στα εφαρμοσμένα μαθηματικά ή τη θεωρία αριθμών. Στα εφαρμοσμένα μαθηματικά, ο υπολογιστής χρησιμεύει απλώς στο να υπολογίσουμε μια προσεγγιστική απάντηση, όταν η θεωρία δεν είναι σε θέση να μας δώσει μια ακριβή απάντηση. Στη θεωρία αριθμών όταν για παράδειγμα μελετάμε την κατανομή των πρώτων αριθμών ο υπολογιστής παίζει το ρόλο του δότη δεδομένων. Και στις δυο περιπτώσεις η μηχανή δεν υπεισέρχεται στα αυστηρά μαθηματικά της απόδειξης. Στην πρώτη παίζει το ρόλο **υποκατάστατου** που χρησιμοποιείται σε εκείνη την περιοχή που δεν μπορεί να πάει η θεωρία, ενώ στη δεύτερη το ρόλο του **βοηθού** στα πλαίσια της ευρετικής μεθόδου.

Στο πρόβλημα των τεσσάρων χρωμάτων η κατάσταση είναι εντελώς διαφορετική. Οι Appel και Haken ισχυρίστηκαν ότι διέθεταν μια οριστική, πλήρη και αυστηρή απόδειξη. Αυτό έδωσε τροφή για διάφορες συζητήσεις, τόσο μεταξύ των φιλοσόφων, όσο και των μαθηματικών. Οι συζητήσεις αυτές αναδεικνύουν τον προβληματισμό τους σχετικά με την έννοια της αυστηρής απόδειξης και κατά πόσο η συγκεκριμένη απόδειξη ανήκει ή όχι στο σύνολο των έγκυρων μαθηματικών αποδείξεων.

Από τη σκοπιά του φιλοσόφου, η χρήση του υπολογιστή ως ουσιαστικού τμήματος της απόδειξης περιλαμβάνει μια αποδυνάμωση των δεδομένων της μαθηματικής απόδειξης. Η απουσία παραγωγικού συλλογισμού για την πιστοποίηση της μαθηματικής γνώσης την υποβαθμίζει στο επίπεδο της κοινής γνώσης.

Από τη σκοπιά των μαθηματικών άλλοι θεώρησαν την απόδειξη Appel - Haken ως μια έμπνευση και δικαίωση, ενώ άλλοι ένιωσαν απογοήτευση όταν διαπίστωσαν ότι αυτό που βρισκόταν στον πυρήνα της απόδειξης, δεν ήταν κάποια αστραφτερή σύλληψη ή μια όμορφη ιδέα και ότι αυτή

προέκυψε με ανάλυση του προβλήματος σε χιλιάδες περιπτώσεων (η απόδειξη στηρίζεται σε αναλύσεις 2.000 περιπτώσεων με ένα σύνολο ενός δισεκατομμυρίου λογικών επιλογών) και διαδοχική εισαγωγή όλων αυτών στον υπολογιστή. Οι απόψεις όπως

«κατά την άποψή μου μια τέτοια λύση δεν ανήκει στην μαθηματική επιστήμη»

και

«ο Θεός δεν θα επέτρεπε να αποδειχθεί το θεώρημα με μια μέθοδο τόσο απαίσια όσο αυτή!!!»

είναι ενδεικτικές του κλίματος που δημιουργήθηκε. Σε αυτό πάντως που συμφωνούσαν όλοι είναι ότι η απόδειξη των Appel και Haken δεν μπορεί να θεωρηθεί μαθηματικά όμορφή ή κομψή δικαιώνοντας τον **Hardy** ο οποίος στην «Απολογία ενός μαθηματικού» είχε υποστηρίξει ότι

> *«Τα μαθηματικά σχεδιάσματα πρέπει να είναι όμορφα. Η ομορφιά είναι το πρώτο κριτήριο. Δεν υπάρχει μόνιμη θέση στον κόσμο για άσχημα μαθηματικά… Η «απαρίθμηση περιπτώσεων» είναι, πραγματικά, μια από τις πιο πληκτικές μορφές μαθηματικής επιχειρηματολογίας. Μια μαθηματική απόδειξη πρέπει να μοιάζει με έναν απλό και ευδιάκριτο αστερισμό και όχι με ένα νεφέλωμα διασκορπισμένο στο Γαλαξία μας.»,*

Ο ίδιος ανέφερε ως θεωρήματα που ο κάθε μαθηματικός θα παραδεχθεί ότι είναι πρώτης τάξεως την απόδειξη του Ευκλείδη για την ύπαρξη απείρου πλήθους πρώτων αριθμών και αυτή του Πυθαγόρα για το ότι το $\sqrt{2}$ είναι άρρητος.

Εδώ, στο τρίτο μέρος της παρούσας εργασίας θα ασχοληθούμε με την αλγοριθμική απόδειξη θεωρημάτων της ευκλείδειας γεωμετρίας παρουσιάζοντας ένα από τα σημαντικότερα εργαλεία της υπολογιστικής αλγεβρικής γεωμετρίας, τον αλγόριθμο **Buchberger**. Στον αλγόριθμο αυτό η είσοδος (input) είναι ένα σύστημα πολυωνυμικών εξισώσεων πολλών μεταβλητών και η έξοδος (output) ένα ισοδύναμο σύστημα εξισώσεων το

οποίο ονομάζεται βάση **Groebner**. Ο αλγόριθμος Buchberger είναι μια ωραία γενίκευση των αλγορίθμων εύρεσης του μέγιστου κοινού διαιρέτη στην περίπτωση των πολυωνύμων μιας μεταβλητής και της απαλοιφής **Gauss** για την επίλυση συστημάτων γραμμικών πολυωνυμικών εξισώσεων με πολλούς αγνώστους. Ο λόγος για τον οποίο ο αλγόριθμος αυτός έχει ευρύτερο πεδίο εφαρμογής βρίσκεται στο ότι πολλά μαθηματικά προβλήματα μπορούν να τυποποιηθούν και να αναχθούν στην επίλυση πολυωνυμικών συστημάτων.

ΚΕΦΑΛΑΙΟ 2

2. 1 Πράξεις

2.1.i. Διμελής πράξη

Έστω Ε ένα σύνολο διαφορετικό από το κενό. **Διμελή πράξη** στο Ε λέμε μια συνάρτηση f με πεδίο ορισμού $E \times E$ και τιμές στο σύνολο Ε.

Παρατηρήσεις

1. Αντί του όρου διμελή πράξη, πολλές φορές χρησιμοποιούμε τους όρους **πράξη** ή και **εσωτερική πράξη**. Επίσης λέμε ότι το σύνολο Ε είναι εφοδιασμένο με μια πράξη.
2. Ο συμβολισμός που χρησιμοποιούμε για τις πράξεις, αποδίδεται είτε προσθετικά (+), είτε πολλαπλασιαστικά $(\cdot)$ είτε με άλλο σύμβολο όπως $*$, $\otimes$, κτλ.
3. Ανάλογα με το σύμβολο της πράξης, αντί του συνηθισμένου συναρτησιακού συμβολισμού f((α, β))=γ, γράφουμε α+β=γ, $\alpha * \beta = \gamma$ κτλ.

Παραδείγματα

1. Αν για οποιουσδήποτε θετικούς ρητούς α, β ορίσουμε $\alpha * \beta = \frac{\alpha}{\beta}$, τότε η ισότητα αυτή ορίζει πράξη στο σύνολο των θετικών ρητών.
2. Αν για οποιουσδήποτε θετικούς ακέραιους α, β ορίσουμε $\alpha * \beta = \frac{\alpha}{\beta}$, τότε η ισότητα αυτή δεν ορίζει πράξη στο σύνολο των θετικών ακεραίων καθότι το αποτέλεσμα δεν περιέχεται πάντοτε στο σύνολο αυτό.

2.1.ii. Ιδιότητες των πράξεων

Έστω Ε ένα σύνολο εφοδιασμένο με μια πράξη $*$. Λέμε ότι η πράξη:

- Είναι **αντιμεταθετική στο Ε**, όταν

για οποιαδήποτε $\alpha, \beta \in E$ ισχύει $\alpha * \beta = \beta * \alpha$.

- Είναι **προσεταιριστική στο Ε,** όταν

για οποιαδήποτε $\alpha, \beta, \gamma \in E$ ισχύει $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$.

- Έχει **ουδέτερο στοιχείο** στο Ε, όταν υπάρχει $e \in E$ ώστε

για κάθε $\alpha \in E$ ισχύει $\alpha * e = e * \alpha = \alpha$.

Παρατηρήσεις

1. Αποδεικνύεται ότι το ουδέτερο της πράξης, όταν υπάρχει, είναι μοναδικό.
2. Αν μια πράξη έχει ουδέτερο e και για κάθε $\alpha \in E$ υπάρχει $\alpha' \in E$ ώστε $\alpha * \alpha' = \alpha' * \alpha = e$, τότε λέμε ότι το **α' είναι το συμμετρικό του α** ως προς την πράξη $*$.
3. Αν μια πράξη είναι προσεταιριστική, τότε κάθε στοιχείο του Ε έχει το πολύ ένα συμμετρικό.

2. 2 Ομάδες

2.2.i. Ομάδα

Έστω G ένα σύνολο εφοδιασμένο με μια πράξη $*$. Λέμε ότι το G είναι **ομάδα** ως προς την πράξη αυτή, όταν:

- Η πράξη είναι προσεταιριστική.
- Η πράξη έχει ουδέτερο στοιχείο e.
- Κάθε στοιχείο α του G έχει συμμετρικό α' στο G.

Παρατηρήσεις

1. Όταν το σύνολο G εφοδιασμένο με την πράξη $*$ είναι ομάδα, τότε μιλάμε για την ομάδα $(G, *)$.
2. Αν επιπλέον η πράξη είναι και αντιμεταθετική, τότε η ομάδα λέγεται **αντιμεταθετική** ή **αβελιανή.**

3. Όταν η πράξη είναι πολλαπλασιαστική, το ουδέτερο του πολλαπλασιασμού το συμβολίζουμε με **1** και το λέμε μοναδιαίο στοιχείο ή **μονάδα.** Επίσης, το συμμετρικό του α το συμβολίζουμε με $α^{-1}$ και το λέμε **αντίστροφο του α**.
4. Όταν η πράξη είναι προσθετική, το ουδέτερο της πρόσθεσης το συμβολίζουμε με **0** και το λέμε μηδενικό στοιχείο ή **μηδέν.** Επίσης, το συμμετρικό του α το συμβολίζουμε με -α και το λέμε **αντίθετο του α**.

Παραδείγματα

1. Το σύνολο $(\mathbb{C}^*, \cdot)$ είναι ομάδα με ουδέτερο στοιχείο το 1 και συμμετρικό του τυχαίου στοιχείου z, το z^{-1}.
2. Το σύνολο $(\mathbb{Z}^+, \cdot)$ δεν είναι ομάδα, καθότι δεν περιέχει το συμμετρικό τυχαίου στοιχείου του.
3. Το σύνολο F όλων των συναρτήσεων με πεδίο ορισμού το $\mathbb{R}$ είναι ομάδα με πράξη την πρόσθεση των συναρτήσεων με ουδέτερο στοιχείο τη μηδενική συνάρτηση **0** με την ιδιότητα **0**(x)=0 για κάθε $x \in \mathbb{R}$ και συμμετρικό του τυχαίου στοιχείου της f, τη συνάρτηση –f με την ιδιότητα (–f)(x)=-f(x) για κάθε $x \in \mathbb{R}$.
4. Για κάθε $n \in \mathbb{Z}^+$ οι n ρίζες της εξίσωσης $z^n=1$ σχηματίζουν πολλαπλασιαστική ομάδα που τη λέμε πολλαπλασιαστική ομάδα των νιοστών ριζών της μονάδας.

2.2.ii. Υποομάδα

Έστω $(G, *)$ μια ομάδα και H υποσύνολο του G. Αν το H είναι ομάδα ως προς τον περιορισμό της πράξης $*$ στο H, τότε λέμε ότι το H είναι **υποομάδα** της G και συμβολίζουμε $H \leq G$.

Αποδεικνύεται ότι:

$$H \leq G \Leftrightarrow \alpha \cdot \beta^{-1} \in H \text{ για κάθε } \alpha, \beta \in H$$

Παράδειγμα.

Στην ομάδα F των πραγματικών συναρτήσεων, που έχουμε ήδη αναφέρει, το υποσύνολό της που αποτελείται από τις συνεχείς συναρτήσεις είναι υποομάδα της F καθόσον το άθροισμα συνεχών συναρτήσεων είναι συνάρτηση συνεχής, η μηδενική συνάρτηση είναι συνεχής και για οποιαδήποτε συνάρτηση f, η –f είναι επίσης συνεχής.

2.2.iii. Ομομορφισμοί ομάδων.

Έστω $(G, \circ)$ και $(G', *)$ δυο ομάδες. Μια απεικόνιση $f: G \to G'$ λέγεται **ομομορφισμός** μεταξύ των $(G, \circ)$, $(G', *)$ όταν για κάθε $\alpha, \beta \in G$ ισχύει

$$f(\alpha \circ \beta) = f(\alpha) * f(\beta).$$

Ένας ομομορφισμός ο οποίος είναι

- ένα προς ένα, λέγεται **μονομορφισμός**
- επί, λέγεται **επιμορφισμός**
- ένα προς ένα και επί, λέγεται **ισομορφισμός**.

Παρατηρήσεις

1. Οι ομομορφισμοί διατηρούν τις δομές. Έτσι απεικονίζουν το ουδέτερο της G στο ουδέτερο της G' και το συμμετρικό ενός στοιχείου α της G στο συμμετρικό του στοιχείου f(α) της G'. Επίσης η εικόνα μιας υποομάδας της G μέσω ενός ομομορφισμού f είναι υποομάδα της G'.
2. Όταν υπάρχει ένας ισομορφισμός μεταξύ δυο ομάδων $(G, \circ)$, $(G', *)$, τότε λέμε ότι αυτές είναι **ισόμορφες** και συμβολίζουμε $G \simeq G'$.
3. Αν δυο ομάδες είναι ισόμορφες, τότε δομικά δεν παρουσιάζουν καμία διαφορά και από «ομαδοθεωρητική» σκοπιά τις θεωρούμε ως ταυτιζόμενες.

Παραδείγματα

1. Αν θεωρήσουμε την προσθετική ομάδα ($\mathbb{R}$, +) και την πολλαπλασιαστική ($\mathbb{R}^*$, $\cdot$) τότε η απεικόνιση $f:\mathbb{R}\to\mathbb{R}^*$ με $f(x)=2^x$ είναι ομομορφισμός ομάδων.
2. Αν F είναι η προσθετική ομάδα όλων των συναρτήσεων μέσω των οποίων απεικονίζεται το $\mathbb{R}$ στο $\mathbb{R}$ και έχουν παράγωγο κάθε τάξης, και $\mathbb{R}$ η προσθετική ομάδα των πραγματικών αριθμών, τότε η φ: $\mathbb{R}\to\mathbb{R}$ με $\varphi(f)= f''$ είναι ομομορφισμός ομάδων.

2.2.iv. Το σύνολο $\mathbb{Z}_n$

Έστω n ένας θετικός ακέραιος. Στο σύνολο των ακεραίων ορίζουμε μια σχέση ($\equiv$) ως εξής:

Για οποιαδήποτε $\alpha, \beta \in \mathbb{Z}$ ορίζουμε

$$\alpha \equiv \beta \Leftrightarrow \beta-\alpha=\kappa n \text{ για κάποιο ακέραιο } \kappa$$

Η σχέση αυτή είναι σχέση ισοδυναμίας (ανακλαστική–συμμετρική-μεταβατική) και ως τέτοια διαμερίζει το $\mathbb{Z}$ σε κλάσεις ισοδυναμίας που τις λέμε **κλάσεις υπολοίπων mod.n**. Το σύνολο των κλάσεων αυτών το συμβολίζουμε με $\mathbb{Z}_n$ και συνηθίζεται να το αναφέρουμε ως σύνολο ακεραίων modulo n. Αν από κάθε κλάση επιλέξουμε έναν αντιπρόσωπο, τότε για κάθε θετικό ακέραιο n έχουμε

$$\mathbb{Z}_n = \{0, 1, 2, \dots ,n-1\}$$

όπου το 0 αντιπροσωπεύει όλους τους αριθμούς της μορφής κm, το 1 όλους τους αριθμούς της μορφής κn+1 κτλ.

Στο σύνολο αυτό τα αποτελέσματα των γνωστών πράξεων πρόσθεσης και πολλαπλασιασμού ορίζονται μέσω των αντιπροσώπων τους. Έτσι για παράδειγμα στο $\mathbb{Z}_4$ είναι 2+3=1, αφού στο σύνολο αυτό ο αντιπρόσωπος του εξαγόμενου (5) της πράξης είναι το 1. Για τον ίδιο λόγο στο $\mathbb{Z}_4$ ισχύει: $2\cdot 3=2$.

Αποδεικνύεται ότι το ($\mathbb{Z}_4$, +) είναι αβελιανή ομάδα και το υποσύνολό της {0, 2} είναι υποομάδα σε αντίθεση με το {0, 3} που δεν είναι υποομάδα καθόσον δεν είναι κλειστό ως προς την πρόσθεση αφού 3+3=2 και $2 \notin \{0, 3\}$.

2.2.v. Τάξη ομάδας

Αν (G, $*$) είναι μια ομάδα, τότε τον πληθάριθμο |G| του συνόλου G τον λέμε **τάξη** της ομάδας. Αν ο αριθμός |G| είναι πεπερασμένος τότε λέμε ότι η ομάδα είναι **πεπερασμένης τάξης**, ενώ αν δεν είναι πεπερασμένος, λέμε ότι η ομάδα είναι **άπειρης τάξης**.

Σύμβαση: Στα επόμενα όπου δεν αναφέρεται κάτι διαφορετικό θεωρούμε ότι η ομάδα στην οποία αναφερόμαστε είναι πολλαπλασιαστική.

2.2.vi. Κυκλική ομάδα.

Αν μια ομάδα G μπορεί να παραχθεί από ένα μόνο στοιχείο της α, τότε λέμε ότι η ομάδα είναι **κυκλική** και συμβολίζουμε G=<α>.

Παρατηρήσεις

1. Το στοιχείο α λέγεται **γεννήτορας** της ομάδας η οποία αποτελείται από όλες τις δυνάμεις της μορφής α^{κ}, με κ=0, ±1, ±2, ...
2. Αποδεικνύεται ότι, αν α είναι τυχαίο στοιχείο της G, τότε το $H=\{\alpha^n / n \in \mathbb{Z}\}$ είναι υποομάδα της G και τη λέμε **κυκλική υποομάδα <α> της G** που παράγεται από το α.
3. Αν οι δυνάμεις α^{κ} είναι διακεκριμένες, τότε η G είναι κυκλική **άπειρης τάξης**, και το α λέμε ότι είναι άπειρης τάξης.
4. Αν υπάρχει ελάχιστος n ώστε $\alpha^n=1$, τότε η G είναι κυκλική **τάξης n** και το στοιχείο α λέμε ότι είναι τάξης n.
5. Κάθε υποομάδα κυκλικής ομάδας είναι κυκλική.
6. Κάθε κυκλική ομάδα είναι αβελιανή.

7. Δυο οποιεσδήποτε κυκλικές ομάδες με την ίδια πεπερασμένη τάξη είναι ισόμορφες.

Παράδειγμα

Αν θεωρήσουμε την ομάδα U_n των νιοστών ριζών της μονάδας στο $\mathbb{C}$, τότε αυτή είναι κυκλική τάξης n και παράγεται από το στοιχείο $\alpha = \text{συν}\frac{2\pi}{n} + i\text{ημ}\frac{2\pi}{n}$.

2.2.vii. Σύμπλοκα

Αν H είναι μια υποομάδα μιας ομάδας G , $x \in G$ και K={x} τότε αντί για KH={xh: $h \in H$} γράφουμε xH. Το xH λέγεται **αριστερό σύμπλοκο** της H στην G. Ανάλογα ορίζεται και το δεξιό σύμπλοκο Hx της H στην G.

Βασικές ισοδυναμίες

Αν H υποομάδα της G τότε

$$Hx=Hy \Leftrightarrow y \in Hx \Leftrightarrow yx^{-1} \in H$$

και

$$xH=yH \Leftrightarrow y \in xH \Leftrightarrow x^{-1}y \in H$$

Συνέπεια

Αν x, $y \in G$ τότε είτε Hx=Hy είτε $Hx \cap Hy = \varnothing$ που σημαίνει ότι τα σύμπλοκα διαμερίζουν την υποομάδα.

Αποδεικνύεται ότι:

1. Τα σύμπλοκα μιας υποομάδας έχουν όλα την ίδια ισχύ (ίδιο πληθάριθμο).
2. Το πλήθος των διακεκριμένων δεξιών συμπλόκων είναι ίδιο με το πλήθος των διακεκριμένων αριστερών συμπλόκων.

Δείκτης υποομάδας.

Έστω G μια ομάδα. Αν συμβολίσουμε με G/H το σύνολο των συμπλόκων μιας υποομάδας H της G τότε το πλήθος των στοιχείων του το λέμε δείκτη της υποομάδας H στην G και το συμβολίζουμε με $|G:H|$.

2.2.viii. Κανονική υποομάδα

Έστω G μια ομάδα. Μια υποομάδα H της G λέγεται κανονική και συμβολίζουμε $H \lhd G$ όταν τα αριστερά και τα δεξιά σύμπλοκά της ταυτίζονται.

Ομάδα πηλίκο

Έστω $H \lhd G$. Στο σύνολο G/H των συμπλόκων της H στην G ορίζουμε μια πολλαπλασιαστική πράξη ως εξής: Αν A, B στοιχεία του G/H, τότε

$$AB=\{\alpha\beta: \alpha \in A, \beta \in B\}$$

Αποδεικνύεται ότι το σύνολο G/H αποτελεί ομάδα ως προς την πράξη αυτή με μοναδιαίο το σύμπλοκο H. Την ομάδα αυτή την λέμε **ομάδα πηλίκο της G ως προς H.**

1. 3 Σύνολα εφοδιασμένα με δυο πράξεις

1.3.i. Επιμεριστική ιδιότητα

Έστω E ένα σύνολο εφοδιασμένο με δυο εσωτερικές πράξεις $\cdot$, $*$. Αν για οποιαδήποτε α, β, $\gamma \in E$ ισχύουν

$$\alpha \cdot (\beta * \gamma)=(\alpha \cdot \beta) * (\alpha \cdot \gamma)$$

και

$$(\alpha * \beta) \cdot \gamma=(\alpha \cdot \gamma) * (\beta \cdot \gamma)$$

τότε λέμε ότι η πράξη $\cdot$ είναι επιμεριστική ως προς την $*$.

Παράδειγμα

Αν θεωρήσουμε τις συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού στο σύνολο των πραγματικών αριθμών, τότε ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση (διότι $\alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma$ και $(\beta+\gamma)\cdot\alpha=\beta\cdot\alpha+\gamma\cdot\alpha$), ενώ η πρόσθεση δεν είναι επιμεριστική ως προς τον πολλαπλασιασμό (διότι γενικά $\alpha+(\beta\cdot\gamma)\neq(\alpha+\beta)\cdot(\alpha+\gamma)$).

1.3.ii. Δακτύλιοι

Έστω R ένα σύνολο που είναι εφοδιασμένο με δυο πράξεις, τις οποίες σημειώνουμε προσθετικά (+) και πολλαπλασιαστικά ($\cdot$). Λέμε ότι το R είναι **δακτύλιος** ως προς τις πράξεις αυτές, όταν:

- Το R είναι αντιμεταθετική ομάδα ως προς την πρόσθεση με ουδέτερο το **0** και συμμετρικό του α, το –α.
- Ο πολλαπλασιασμός είναι προσεταιριστικός, έχει ουδέτερο στοιχείο, που συμβολίζεται με **1** (μονάδα) και είναι επιμεριστικός ως προς την πρόσθεση.

Παρατηρήσεις

1. Αν ο πολλαπλασιασμός είναι αντιμεταθετικός, τότε ο δακτύλιος λέγεται **αντιμεταθετικός**.
2. Η αντιμεταθετικότητα της πρόσθεσης θα μπορούσε να μην αναφέρεται ως ορίζουσα ιδιότητα του δακτυλίου, καθότι προκύπτει από τις άλλες.

   Πράγματι, έχουμε:

   $$(1+1)\cdot(\alpha+\beta)=1\cdot(\alpha+\beta)+1\cdot(\alpha+\beta)=(\alpha+\beta)+(\alpha+\beta)$$

   και

   $$(1+1)\cdot(\alpha+\beta)=(1+1)\cdot\alpha+(1+1)\cdot\beta=1\cdot\alpha+1\cdot\alpha+1\cdot\beta+1\cdot\beta$$

   οπότε

   $$\alpha+\beta+\alpha+\beta=\alpha+\alpha+\beta+\beta$$

απ' όπου «απλοποιώντας» αριστερά με α και δεξιά με β έχουμε α+β=β+α.

Παραδείγματα

1. Έχουμε ήδη αναφέρει ότι το σύνολο F των συναρτήσεων f: $\mathbb{R} \to \mathbb{R}$ είναι αβελιανή ομάδα με πράξη τη συνηθισμένη πρόσθεση των συναρτήσεων. Αν θεωρήσουμε το σύνολο (F, +, $\cdot$) όπου $\cdot$ η πράξη του πολλαπλασιασμού των συναρτήσεων, τότε το F είναι δακτύλιος.
2. Αν στο σύνολο $\mathbb{Z}_n$, για το οποίο είδαμε ότι είναι αβελιανή ομάδα, ορίσουμε ως γινόμενο των στοιχείων του α, β το υπόλοιπο της διαίρεσης του συνηθισμένου γινομένου αβ με το n, τότε το ($\mathbb{Z}_n$, +, $\cdot$) είναι δακτύλιος. Το δακτύλιο αυτό θα εννοούμε στη συνέχεια, όπου αναγράφουμε το συμβολισμό $\mathbb{Z}_n$.

Ιδεώδες ενός δακτυλίου

Έστω R ένας δακτύλιος και I ένα υποσύνολό του. Λέμε ότι το I είναι ιδεώδες του R και συμβολίζουμε $I \lhd R$, όταν:

- $I \neq \varnothing$ ή $\mathbf{0} \in I$
- Για οποιαδήποτε στοιχεία α, β του I ισχύει $\alpha - \beta \in I$
- Αν $\alpha \in I$ και $r \in R$, τότε $r \cdot \alpha \in I$ και $\alpha \cdot r \in I$.

1.3.iii. Διαιρέτες του μηδενός

Έστω R ένας αντιμεταθετικός δακτύλιος. Ένα στοιχείο του α με $\alpha \neq \mathbf{0}$ λέγεται διαιρέτης του μηδενός, όταν υπάρχει στοιχείο β με $\beta \neq \mathbf{0}$ ώστε $\alpha \cdot \beta = \mathbf{0}$.

Παράδειγμα

1. Ο δακτύλιος (F, +, $\cdot$) των συναρτήσεων f: $\mathbb{R} \to \mathbb{R}$ έχει διαιρέτες του μηδενός. Πράγματι, αν θεωρήσουμε τις συναρτήσεις

$$f(x)=\begin{cases} x+1, & x>0 \\ 0, & x\le 0 \end{cases} \quad \text{και} \quad g(x)=\begin{cases} x-1, & x\le 0 \\ 0, & x>0 \end{cases}$$

χωρίς καμία από αυτές να είναι η μηδενική, ισχύει $(f\cdot g)(x)=0$ για κάθε $x\in\mathbb{R}$.

2. Ο δακτύλιος $\mathbb{Z}_{12}$ έχει διαιρέτες του μηδενός, καθότι σ' αυτόν, για παράδειγμα ισχύει $3\cdot 4=0$. Γενικά αν ο n δεν είναι πρώτος, τότε ο $\mathbb{Z}_n$ έχει διαιρέτες του μηδενός.

Ακέραια περιοχή

Ένας αντιμεταθετικός δακτύλιος που δεν έχει διαιρέτες του μηδενός, λέγεται ακέραια περιοχή.

1.3.iv. Σώμα

Ένας δακτύλιος (K, +, $\cdot$) λέγεται σώμα, όταν:

- Είναι αντιμεταθετικός και
- Κάθε στοιχείο του διαφορετικό από το μηδέν έχει συμμετρικό ως προς τον πολλαπλασιασμό.

Παρατήρηση

Σε ένα σώμα K ισχύει η συνεπαγωγή: Αν $\alpha\cdot\beta=0$, τότε $\alpha=0$ ή $\beta=0$. Άμεσα πλέον από αυτή, με αντιθετοαντιστροφή, προκύπτει ότι κάθε σώμα είναι ακέραια περιοχή.

Παραδείγματα

Τα σύνολα $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ με τις γνωστές πράξεις +, $\cdot$ είναι σώματα.

2. 4 Πολυώνυμα

2.4.i. Ο δακτύλιος των πολυωνύμων μιας μεταβλητής.

Έστω F ένα σώμα και $\mathbb{N}$ το σύνολο των φυσικών αριθμών. Το σύνολο όλων των απεικονίσεων του $\mathbb{N}$ στο F είναι όλες οι ακολουθίες της μορφής $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ με $\alpha_i \in F$, i=0, 1, 2, … Θεωρούμε το σύνολο

$$A=\{(\alpha_0, \alpha_1, \alpha_2, \ldots): \exists n \in \mathbb{N} \text{ ώστε } \alpha_i=0 \text{ για κάθε } i>n\}$$

στο οποίο ορίζουμε τις πράξεις πρόσθεσης και πολλαπλασιασμού ως εξής:

$$(\alpha_0, \alpha_1, \alpha_2, \ldots)+(\beta_0, \beta_1, \beta_2, \ldots)= (\alpha_0+\beta_0, \alpha_1+\beta_1, \alpha_2+\beta_2, \ldots)$$

$$(\alpha_0, \alpha_1, \alpha_2, \ldots)\cdot(\beta_0, \beta_1, \beta_2, \ldots)=(\gamma_0, \gamma_1, \gamma_2, \ldots)$$

όπου $\gamma_0=\alpha_0\beta_0$, $\gamma_1=\alpha_0\beta_1+\alpha_1\beta_0$ και γενικά $\gamma_\kappa = \sum_{i+j=\kappa} \alpha_i\beta_j$, κ=0, 1, 2, …

Αποδεικνύεται ότι το A, εφοδιασμένο με αυτές τις πράξεις είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο το (1, 0, 0, …). Ο δακτύλιος A λέγεται **δακτύλιος των πολυωνύμων επί του F.** Τα στοιχεία του A λέγονται **πολυώνυμα.**

Παρατηρήσεις

1. Δυο πολυώνυμα $(\alpha_0, \alpha_1, \alpha_2, \ldots)$ και $(\beta_0, \beta_1, \beta_2, \ldots)$ λέγονται **ίσα** όταν $\alpha_i=\beta_i$, για όλα τα i.
2. Το τυχαίο στοιχείο α του F το ταυτίζουμε με το πολυώνυμο (α, 0, 0, …), οπότε το F θεωρείται υποσύνολο του A.
3. Αν θέσουμε x=(0, 1, 0, 0, …) τότε εύκολα βρίσκουμε x^2=(0, 0, 1, 0, 0, …) και γενικά x^n=(0, 0, 0, …0, 1, 0, …), όπου όλα τα στοιχεία εκτός από αυτό που βρίσκεται στην n+1 θέση, είναι μηδέν.
4. Αν α ένα στοιχείο του F, τότε

   $$\alpha x^n=(\alpha, 0, 0, \ldots)(0, 0, \ldots, 0, 1, 0, \ldots.)=(0, 0, \ldots, 0, \alpha, 0, \ldots)$$

   με το στοιχείο στην n+1 θέση να είναι α και όλα τα άλλα να είναι μηδέν. Αν τώρα θεωρήσουμε το πολυώνυμο $(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n, 0, 0, \ldots)$ με $\alpha_n\neq 0$ και $\alpha_i=0$ για i>n τότε

   $$(\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n, 0, 0,\ldots)=$$

$$= (\alpha_0, 0, 0,\ldots)+(0, \alpha_1, 0, 0,\ldots)+\ldots+(0, 0, \ldots,\alpha_n, 0, \ldots)$$
$$= \alpha_0(1, 0, 0, \ldots, 0)+\alpha_1(0, 1, 0, \ldots, 0)+\ldots+\alpha_n(0, 0, \ldots, 1, 0, \ldots)$$
$$=\alpha_0+\alpha_1x+\alpha_2x^2+\ldots+\alpha_nx^n.$$

Έτσι έχουμε καταλήξει στο συνήθη συμβολισμό για τα πολυώνυμα.

5. Το στοιχείο (0, 0, …, 0) είναι το μηδενικό στοιχείο του A (**μηδενικό πολυώνυμο**). Κάθε μη μηδενικό στοιχείο του A γράφεται με τη μορφή $\alpha_0+\alpha_1x+\alpha_2x^2+\ldots+\alpha_nx^n$ με $\alpha_n\neq 0$ και συμβολίζεται f(x), P(x), g(x), Q(x) κτλ.
6. Αν $P(x) = \alpha_0+\alpha_1x+\alpha_2x^2+\ldots+\alpha_nx^n$ με $\alpha_n\neq 0$, είναι ένα πολυώνυμο, τότε ο μη αρνητικός ακέραιος n λέγεται **βαθμός** του πολυωνύμου και συμβολίζεται με degP(x). Ο α_n λέγεται **μεγιστοβάθμιος συντελεστής** του πολυωνύμου και ο όρος α_nx^n , **μεγιστοβάθμιος όρος** του. Το πολυώνυμο στο οποίο ο μεγιστοβάθμιος συντελεστής του είναι η μονάδα, το λέμε **μονικό**.
7. Στο μηδενικό πολυώνυμο δεν επισυνάπτουμε βαθμό. Τα στοιχεία του A που δεν είναι μηδενικά τα θεωρούμε ως πολυώνυμα μηδενικού βαθμού και τα λέμε **σταθερά** πολυώνυμα.
8. Σε ότι αφορά στο βαθμό του πολυωνύμου που προκύπτει αν προσθέσουμε ή πολλαπλασιάσουμε δυο πολυώνυμα P(x), Q(x) ισχύει:
$$\deg(P(x)+Q(x)) \leq \max \{\deg P(x), \deg Q(x)\}$$
με την προϋπόθεση ότι το P(x)+Q(x) δεν είναι το μηδενικό και
$$\deg(P(x)\cdot Q(x))=\deg P(x)+\deg Q(x)$$
9. Τον δακτύλιο A των πολυωνύμων επί του σώματος F τον συμβολίζουμε συνήθως με F[x]. Ο δακτύλιος αυτός, δεν περιέχει το αντίστροφο κάθε μη μηδενικού στοιχείου του και κατά συνέπεια δεν είναι σώμα. Πράγματι, αν υποθέσουμε ότι το αντίστροφο ενός πολυωνύμου P(x) με $\deg P(x)\geq 1$ είναι ένα πολυώνυμο Q(x), τότε P(x)Q(x)=e(x) με e(x)=1 για κάθε $x\in F$. Τότε όμως θα έχουμε degP(x)+degQ(x)=dege(x) που αποκλείεται διότι ο degQ(x) είναι μη αρνητικός ακέραιος και deg e(x)=0.
10. Αν f(x) είναι ένα πολυώνυμο του F[x] και υπάρχει στοιχείο α του F ώστε f(α)=0, τότε το α λέγεται **ρίζα** του πολυωνύμου.

11. Αποδεικνύεται ότι κάθε πολυώνυμο του F[x] βαθμού n έχει ακριβώς n ρίζες. Από αυτό συνεπάγεται ότι αν ένα πολυώνυμο λαμβάνει την τιμή μηδέν για άπειρες τιμές του x, διαφορετικές μεταξύ τους, τότε αυτό είναι το μηδενικό.
12. Σε κάθε πολυώνυμο f(x) του F[x] μπορούμε να αντιστοιχήσουμε μια συνάρτηση $f^*:F\to F$ με την ιδιότητα $f^*(x)=f(x)$ για κάθε $x\in F$. Η συνάρτηση αυτή που τη λέμε **συνάρτηση που αντιστοιχεί στο πολυώνυμο** f(x), δεν ταυτίζεται κατ' ανάγκη με το πολυώνυμο. Συχνά, για να τονίσουμε αυτή τη διαφορά, το x που είναι η μεταβλητή της συνάρτησης, όταν μιλάμε για το πολυώνυμο, το αναφέρουμε ως απροσδιόριστο. Είναι δυνατό η συνάρτηση που αντιστοιχεί στο πολυώνυμο f(x) να είναι μηδενική χωρίς αυτό να είναι το μηδενικό. Έτσι για παράδειγμα, αν θεωρήσουμε το (μη μηδενικό) πολυώνυμο $f(x)=x^2+x$ του $\mathbb{Z}_2[x]$ τότε έχουμε $f^*(0)=0+0=0$ και $f^*(1)=1+1=0$ που σημαίνει ότι η συνάρτηση που αντιστοιχεί σ' αυτό είναι η μηδενική.

2.4.ii. Η ταυτότητα της διαίρεσης στο δακτύλιο F[x].

Έστω f(x), g(x) δυο πολυώνυμα του F[x] με το g(x) να είναι διαφορετικό από το μηδενικό. Αποδεικνύεται ότι υπάρχουν μονοσήμαντα ορισμένα πολυώνυμα π(x), υ(x) του F[x] ώστε

$$f(x)=\pi(x)g(x)+\upsilon(x)$$

όπου το πολυώνυμο υ(x) είναι είτε το μηδενικό, είτε έχει βαθμό μικρότερο από αυτόν του g(x).

Παρατηρήσεις

1. Η παραπάνω ισότητα αναφέρεται ως **ταυτότητα της διαίρεσης του f(x) δια του g(x)** (Συμβολικά: f(x):g(x)). Τα πολυώνυμα f(x), g(x), π(x), υ(x) είναι γνωστά ως **διαιρετέος, διαιρέτης, πηλίκο και υπόλοιπο** της διαίρεσης.

2. Αν το υπόλοιπο της διαίρεσης f(x):g(x) είναι το μηδενικό πολυώνυμο, τότε λέμε ότι η διαίρεση είναι τέλεια. Στην περίπτωση αυτή λέμε επίσης ότι το f(x) είναι πολλαπλάσιο του g(x) ή το g(x) είναι διαιρέτης του f(x) και συμβολίζουμε g(x) | f(x).

2.4.iii. Μέγιστος κοινός διαιρέτης πολυωνύμων

Έστω $f_1(x), f_2(x), \ldots, f_v(x)$ μη μηδενικά πολυώνυμα του F[x]. Ένα πολυώνυμο d(x) λέγεται μέγιστος κοινός διαιρέτης (**Μ.Κ.Δ.**) των $f_i(x)$, i=1, 2, …, v, όταν:

- $d(x) \mid f_i(x)$, i=1, 2, …, v
- αν $\varphi(x) \mid f_i(x)$, i=1, 2, …, v τότε $\varphi(x) \mid d(x)$.

Αποδεικνύεται ότι:

Αν $f_1(x), f_2(x), \ldots, f_v(x)$ είναι μη μηδενικά πολυώνυμα του F[x] και d(x) ο Μ.Κ.Δ. τους, τότε υπάρχουν μοναδικά πολυώνυμα $g_1(x), g_2(x), \ldots, g_v(x)$ ώστε να ισχύει

$$g_1(x)\cdot f_1(x)+g_2(x)\cdot f_2(x)+\ldots+g_v(x)\cdot f_v(x)=d(x)$$

2.4.iv. Ο δακτύλιος των πολυωνύμων πολλών μεταβλητών

Κατ' αντιστοιχία με το δακτύλιο F[x] μπορούμε με τη βοήθεια διπλών ακολουθιών, να ορίσουμε τον δακτύλιο F[x, y] του οποίου τα στοιχεία τα λέμε πολυώνυμα δυο μεταβλητών και είναι της μορφής

$$f(x, y)=\sum_{(i,\, j)}\alpha_{ij}x^i y^j$$

όπου i, j μη αρνητικοί ακέραιοι. Ακολούθως, με επαγωγική διαδικασία, ορίζουμε τον δακτύλιο $F[x_1, x_2, \ldots, x_v]$ του οποίου τα στοιχεία τα λέμε πολυώνυμα v μεταβλητών και είναι της μορφής

$$f(x_1, x_2, \ldots, x_v)=\sum_{\kappa}\alpha_\kappa x_1^{\kappa_1} x_2^{\kappa_2}\ldots x_v^{\kappa_v}$$

όπου $\kappa=(\kappa_1, \kappa_2, \ldots, \kappa_v)$ και $\kappa_1, \kappa_2, \ldots, \kappa_v$ μη αρνητικοί ακέραιοι. Καθένας από τους όρους του αθροίσματος λέγεται **μονώνυμο v μεταβλητών**.

Σε ένα τέτοιο, μη μηδενικό, πολυώνυμο ορίζουμε:

- **Βαθμό (μερικό) του πολυωνύμου ως προς τη μεταβλητή x_i,** $i=1, 2,\ldots, \nu$, τον μεγαλύτερο εκ των μη αρνητικών ακεραίων κ_i όλων των «διανυσμάτων εκθετών» $(\kappa_1, \kappa_2, \ldots, \kappa_\nu)$ με την προϋπόθεση ότι ο αντίστοιχος συντελεστής είναι διαφορετικός από το μηδέν.
- **Ολικό βαθμό** του πολυωνύμου, τον μεγαλύτερο εκ των μη αρνητικών ακεραίων $\kappa_1+\kappa_2+\ldots+\kappa_\nu$ όλων των ν-άδων $(\kappa_1, \kappa_2, \ldots, \kappa_\nu)$ με την προυπόθεση ότι ο αντίστοιχος συντελεστής είναι διαφορετικός από το μηδέν.

Παρατήρηση

Είναι γνωστό ότι η διαδικασία της διαίρεσης στον δακτύλιο $F[x]$ προϋποθέτει διάταξη των μονωνύμων που απαρτίζουν τα πολυώνυμα κατά τις φθίνουσες δυνάμεις της μεταβλητής τους. Έτσι, για να επεκτείνουμε την έννοια της διαίρεσης πολυωνύμων στο δακτύλιο $F[x_1, x_2, \ldots, x_\nu]$ θα αναζητήσουμε κάποια διάταξη και στον $F[x_1, x_2, \ldots, x_\nu]$.

2.4.ν. Διάταξη

Έστω $x_1^{\kappa_1}x_2^{\kappa_2}\ldots x_\nu^{\kappa_\nu}$ ένα μονώνυμο. Αν σ' αυτό επισυνάψουμε το διάνυσμα εκθέτη, συντομογραφικά το συμβολίζουμε x^κ όπου $\kappa=(\kappa_1, \kappa_2, \ldots, \kappa_\nu)$. Η παράσταση του εκθέτη ως διάνυσμα, υπονοεί διάταξη $x_1>x_2>\ldots>x_\nu$ στις μεταβλητές. Μια διάταξη μονωνύμων στον $F[x_1, x_2, \ldots, x_\nu]$ είναι μια σχέση «>» στο σύνολο των μονωνύμων x^κ η οποία ικανοποιεί τις ακόλουθες συνθήκες:

i. Είναι σχέση ολικής διάταξης.

ii. «Σέβεται» τον πολλαπλασιασμό στον $F[x_1, x_2, \ldots, x_\nu]$ με την έννοια ότι αν $x^\kappa>x^\lambda$ τότε για οποιοδήποτε μονώνυμο x^μ ισχύει $x^\kappa \cdot x^\mu=x^{\kappa+\mu}>x^{\lambda+\mu}=x^\lambda \cdot x^\mu$.

iii. Είναι καλή διάταξη, δηλαδή κάθε μη κενό σύνολο μονωνύμων έχει ελάχιστο στοιχείο.

Παρατηρήσεις

1. Η πρώτη συνθήκη εξασφαλίζει ότι οι όροι κάθε πολυωνύμου του δακτυλίου $F[x_1, x_2, \ldots, x_v]$ μπορούν να διαταχθούν με μοναδικό τρόπο σε αύξουσα ή φθίνουσα σειρά σύμφωνα με την «>».
2. Από τη δεύτερη συνθήκη συνάγεται ότι η διάταξη δεν αλλάζει αν πολλαπλασιάσουμε κάποιο πολυώνυμο του $F[x_1, x_2, \ldots, x_v]$ με ένα μονώνυμο.
3. Η τρίτη συνθήκη εξασφαλίζει ότι αν κάποιος αλγόριθμος χρησιμοποιεί σύνολα μονωνύμων, τότε θα τερματίζει.

Διάταξη (λεξικογραφική) μονώνυμων.

Έστω $x_1^{\kappa_1}x_2^{\kappa_2}\ldots x_v^{\kappa_v}$ και $x_1^{\lambda_1}x_2^{\lambda_2}\ldots x_v^{\lambda_v}$ δυο μονώνυμα. Αν σ' αυτά επισυνάψουμε τα διανύσματα εκθέτες $\kappa=(\kappa_1, \kappa_2, \ldots, \kappa_v)$ και $\lambda=(\lambda_1, \lambda_2, \ldots, \lambda_v)$, τότε, στην περίπτωση που ο πρώτος μη μηδενικός όρος της v-άδας κ-λ είναι θετικός, λέμε ότι το κ προηγείται του λ. Με τον τρόπο αυτό ορίζουμε μια διάταξη που τη λέμε λεξικογραφική διάταξη των μονωνύμων. Το γεγονός ότι το κ προηγείται του λ, αποδίδεται με τον συμβολισμό $\kappa >_{lex} \lambda$. Έτσι, για παράδειγμα, $x^3y^2z >_{lex} x^3yz^5$.

Παρατήρηση

Σε ένα πολυώνυμο του $F[x_1, x_2, \ldots, x_v]$ το οποίο έχουμε διατάξει λεξικογραφικά, οι έννοιες μεγιστοβάθμιος όρος και μεγιστοβάθμιος συντελεστής ορίζονται κατ' αντιστοιχία με αυτούς των πολυωνύμων του $F[x]$.

Παράδειγμα

Έστω $f(x, y, z)=4xy^2z+4z^2-5x^3+7x^2z^2$.

Αν θεωρήσουμε ότι $x>y>z$, τότε χρησιμοποιώντας τη λεξικογραφική διάταξη λαμβάνουμε

$$f(x, y, z)= - 5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$$

Έτσι το πολυώνυμο έχει μεγιστοβάθμιο όρο ΜΟ = - $5x^3$ και μεγιστοβάθμιο συντελεστή ΜΣ = - 5.

2.4.vi. Η διαίρεση στο $F[x_1, x_2, \ldots, x_v]$

Ας δούμε τώρα ένα παράδειγμα διαίρεσης στον F[x, y]. Υποθέτουμε ότι ο διαιρετέος είναι $f(x, y)=x^2y+xy^2+y^2$ και ως διαιρέτη ας χρησιμοποιήσουμε το «διάνυσμα» πολυωνύμων (f_1, f_2) με $f_1(x, y)=xy+1$ και $f_2(x, y)=y^2-1$. Η διαδικασία διαίρεσης, που έχει αρκετές ομοιότητες με τη συνηθισμένη από το δακτύλιο F[x], φαίνεται στο παρακάτω σχήμα της διαίρεσης και περιγράφεται ακολούθως.

$f(x, y)=x^2y+xy^2+y^2$	$f_1(x, y)= xy - 1$ $f_2(x, y)= y^2-1$
$-x^2y+x$	$p_1(x, y)=x+y$
$xy^2 + x+y^2$ $- xy^2+y$	$p_2(x, y)=1$
$x+y+y^2$ $1-y^2$	
$\upsilon(x, y)=x+y+1$	

Στο πρώτο βήμα της διαδικασίας θεωρούμε τη διαίρεση του μεγιστοβάθμιου όρου του f(x, y) με εκείνον του $f_1(x, y)$. Η διαίρεση αυτή δίνει πηλίκο x το οποίο συμμετέχει ως πρώτος όρος στον σχηματισμό του $p_1(x, y)$. Κατόπιν πολλαπλασιάζουμε τον όρο αυτό του $p_1(x, y)$ με το $f_1(x, y)$ και αφαιρώντας το εξαγόμενο από το f(x, y) λαμβάνουμε ως πρώτο «μερικό υπόλοιπο» το xy^2+x+y^2.

Η επανάληψη της διαδικασίας με διαιρετέο το xy^2+x+y^2 και διαιρέτη το $f_1(x, y)$ δίνει ως δεύτερο όρο στο $p_1(x, y)$ το y και ως επόμενο «μερικό υπόλοιπο» το $x+y+y^2$ το οποίο δεν είναι περαιτέρω διαιρέσιμο με το $f_1(x, y)$. Στη συνέχεια μεταφέρουμε το x στο υπόλοιπο υ(x, y) και διαιρούμε το $y+y^2$ με

το $f_2(x, y)$ οπότε βρίσκουμε $p_2(x, y)=1$ και το εναπομείναν «μερικό υπόλοιπο» μεταφέρεται στο $\upsilon(x, y)$ το οποίο τελικά είναι το $\upsilon(x, y)=x+y+1$.

Κατ' αντιστοιχία με την ταυτότητα της διαίρεσης στον F[x] από την παραπάνω διαδικασία συνάγεται ότι:

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

Θα πρέπει να επισημάνουμε ότι δοθέντων των πολυωνύμων $f(x, y)$, $f_1(x, y)$ και $f_2(x, y)$ τα πολυώνυμα $p_1(x, y)$, $p_2(x, y)$ και $\upsilon(x, y)$ δεν είναι μονοσήμαντα ορισμένα. Έτσι, αν εδώ επαναλάβουμε τη διαδικασία με εναλλαγή της διάταξης των $f_1(x, y)$ και $f_2(x, y)$ η αντίστοιχη ταυτότητα της διαίρεσης λαμβάνει τη μορφή

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

Πολλές φορές απλώς η αλλαγή της διάταξης, είναι αρκετή να αλλοιώσει τον χαρακτήρα της διαίρεσης, με την έννοια ότι χρησιμοποιώντας μια συγκεκριμένη διάταξη κάποιος θα μπορούσε να την χαρακτηρίσει τέλεια, ενώ κάποιος άλλος αλλάζοντας τη διάταξη να την χαρακτηρίσει ατελή.

Έτσι, αν υποθέσουμε ότι $f_1(x, y)=xy+1$, $f_2(x, y)=y^2-1$ και $f(x, y)=xy^2-x$, η διαίρεση του $f(x, y)$ με το «διάνυσμα πολυωνύμων» (f_1, f_2) δίνει

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

ενώ η διαίρεση του $f(x, y)$ με το «διάνυσμα πολυωνύμων» (f_2, f_1) δίνει

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

Περισσότερα και πιο εξειδικευμένα θέματα σχετικά με τα πολυώνυμα πολλών μεταβλητών θα συναντήσουμε στο 3ο κεφάλαιο που αναφέρεται στην αυτόματη απόδειξη γεωμετρικών θεωρημάτων.

2. 5 Εξωτερική πράξη

Έστω Α, Ε δυο σύνολα διαφορετικά από το κενό. **Εξωτερική πράξη** στο Ε με **τελεστές** τα στοιχεία του Α λέμε μια συνάρτηση f: $A\times E\rightarrow E$.

Παρατηρήσεις

1. Την εξωτερική πράξη συνήθως τη συμβολίζουμε πολλαπλασιαστικά. Έτσι η τιμή f((λ, α)) της συνάρτησης με $\lambda\in A$ και $\alpha\in E$, αντί λfα γράφεται απλά $\lambda\cdot\alpha$.
2. Αν για κάθε τελεστή λ και κάθε $\alpha\in E$ ισχύει $\lambda\cdot\alpha\in E$, τότε λέμε ότι το Ε είναι κλειστό ως προς την εξωτερική πράξη, την οποία συχνά αναφέρουμε και ως **βαθμωτό πολλαπλασιασμό**.

2.5.i. Διανυσματικός χώρος

Ένα σύνολο V με μια εσωτερική πράξη + και μια εξωτερική $\cdot$ με τελεστές τα στοιχεία ενός σώματος F, λέμε ότι είναι διανυσματικός χώρος επί του F, όταν το (V, +) είναι μια αβελιανή ομάδα και επιπλέον:

- $\lambda\cdot\alpha\in V$ για οποιοδήποτε $\lambda\in F$ και $\alpha\in V$
- $(\lambda+\mu)\cdot\alpha=\lambda\cdot\alpha+\mu\cdot\alpha$ για οποιαδήποτε $\lambda, \mu\in F$ και $\alpha\in V$
- $\lambda\cdot(\alpha+\beta)=\lambda\cdot\alpha+\lambda\cdot\beta$ για οποιαδήποτε $\lambda\in F$ και $\alpha, \beta\in V$
- $\lambda\cdot(\mu\cdot\alpha)=(\lambda\cdot\mu)\cdot\alpha$ για οποιαδήποτε $\lambda, \mu\in F$ και $\alpha\in V$
- $1\cdot\alpha=\alpha$ για οποιοδήποτε $\alpha\in V$.

Παρατήρηση

Αν το F είναι το $\mathbb{R}$, τότε μιλάμε για διανυσματικό χώρο επί του $\mathbb{R}$, ενώ αν είναι το $\mathbb{Q}$, μιλάμε για διανυσματικό χώρο επί του $\mathbb{Q}$.

2.5.ii. Διανυσματικός υπόχωρος

Έστω V ένας διανυσματικός χώρος και Ε ένα μη κενό υποσύνολό του. Λέμε ότι το Ε είναι διανυσματικός υπόχωρος ή απλά υπόχωρος του V όταν για οποιαδήποτε $\alpha, \beta\in E$ και $\lambda\in F$ ισχύουν $\alpha+\beta\in E$ και $\lambda\cdot\alpha\in E$.

Είναι φανερό ότι οποιοσδήποτε υπόχωρος του V περιέχει το μηδενικό στοιχείο του.

Αποδεικνύεται ότι:

Ένα μη κενό υποσύνολο του V είναι υπόχωρος του V αν και μόνο αν για κάθε $\alpha, \beta \in E$ και $\lambda, \mu \in F$ ισχύει $\lambda \cdot \alpha + \mu \cdot \beta \in E$.

2.5.iii. Γραμμική ανεξαρτησία

Έστω V ένας διανυσματικός χώρος και $\alpha_1, \alpha_2, \ldots, \alpha_n$ στοιχεία του V. Κάθε στοιχείο x του χώρου το οποίο μπορεί να γραφεί στη μορφή $x=\lambda_1 \cdot \alpha_1+\lambda_2 \cdot \alpha_2+\ldots+\lambda_n \cdot \alpha_n$ με $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$ λέγεται **γραμμικός συνδυασμός** των στοιχείων $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Αν όλα τα στοιχεία του V μπορούν να γραφούν ως γραμμικός συνδυασμός των στοιχείων $\alpha_1, \alpha_2, \ldots, \alpha_n$ τότε λέμε ότι το σύνολο $S=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ είναι ένα **σύνολο γεννητόρων του V ή παράγει τον V**.

Θεωρούμε ένα διανυσματικό χώρο V και έστω $\alpha_1, \alpha_2, \ldots, \alpha_n$ στοιχεία του. Αν υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_n \in F$, τα οποία δεν είναι όλα μηδέν, ώστε να ισχύει

$$\lambda_1 \cdot \alpha_1+\lambda_2 \cdot \alpha_2+\ldots+\lambda_n \cdot \alpha_n =0 \qquad (1)$$

τότε λέμε ότι τα $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι **γραμμικώς εξαρτημένα** επί του F.
Αν για τα στοιχεία $\alpha_1, \alpha_2, \ldots, \alpha_n$ κάθε σχέση της μορφής (1) ισχύει, μόνο όταν όλα τα λ_i είναι μηδέν, τότε λέμε ότι τα στοιχεία αυτά είναι **γραμμικά ανεξάρτητα επί του F.**

2. 5.iv. Βάση και διάσταση ενός διανυσματικού χώρου.

Έστω $S=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ ένα υποσύνολο κάποιου διανυσματικού χώρου V. Λέμε ότι το S είναι βάση του V, όταν:

- Τα $\alpha_1, \alpha_2, \ldots, \alpha_n$ είναι γραμμικώς ανεξάρτητα.

- Το S παράγει τον χώρο V.

Αποδεικνύεται ότι κάθε άλλη βάση του χώρου έχει επίσης το ίδιο πλήθος στοιχείων. Το πλήθος των στοιχείων της βάσης το λέμε **διάσταση του V επί του F** και το συμβολίζουμε με $\dim_F V$. Στην περίπτωση (όπως εδώ) που η βάση έχει πεπερασμένο πλήθος στοιχείων μιλάμε για χώρο πεπερασμένης διάστασης, διαφορετικά λέμε ότι ο χώρος έχει άπειρη διάσταση.

ΚΕΦΑΛΑΙΟ 3

3.1. Το πρόβλημα της αυτόματης απόδειξης Γεωμετρικών θεωρημάτων

Η κεντρική ιδέα πάνω στην οποία βασίζεται η προσπάθεια της αυτόματης απόδειξης γεωμετρικών θεωρημάτων, με τη μέθοδο που θα αναπτύξουμε εδώ, είναι η ακόλουθη.

Αν οι υποθέσεις και τα συμπεράσματα ενός θεωρήματος μπορούν να διατυπωθούν με τη βοήθεια πολυωνυμικών εξισώσεων και ονομάσουμε (Σ) το σύστημα που σχηματίζουν, τότε η απόδειξη του θεωρήματος έχει να κάνει κατά κάποιο τρόπο με τη συμβατότητα ή μη, των εξισώσεων που σχηματίζουν τα συμπεράσματα με τις εξισώσεις του (Σ). Αυτό, όπως θα δούμε στη συνέχεια, σχετίζεται με την ύπαρξη ή μη ύπαρξη κάποιων πολυωνύμων σε συγκεκριμένο ιδεώδες. Το πρόβλημά μας λοιπόν σχετίζεται άμεσα με τη δυνατότητα επίλυσης συστήματος πολλών μεταβλητών.

3. 1.i. Σύστημα πολυωνυμικών εξισώσεων με πολλές μεταβλητές

Ο βασικός σκοπός μας είναι να διερευνήσουμε τη δυνατότητα επίλυσης συστημάτων μ εξισώσεων με ν αγνώστους της μορφής

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

όπου $f_i(x_1,\ x_2\ \ldots,\ x_\nu)$ είναι πολυώνυμα με ν αγνώστους (μεταβλητές) και συντελεστές από κάποιο σώμα F. Στα επόμενα, αν δεν αναφέρεται κάτι διαφορετικό, θα θεωρούμε ότι το σώμα F είναι το $\mathbb{R}$ ή το $\mathbb{C}$.

Αυτό που μας ενδιαφέρει, και κατά συνέπεια θα επιδιώξουμε, είναι ο μετασχηματισμός του (Σ) σε ένα άλλο σύστημα (Σ^*) το οποίο θα επιλύεται πιο εύκολα. Η διαδικασία αυτή δεν είναι κάτι το ασύνηθες καθότι συναντιέται συχνά στα μαθηματικά της μέσης εκπαίδευσης. Έτσι για παράδειγμα η επίλυση του συστήματος

$$\begin{cases} 2x^2 + 3y^2 = 11 \\ x^2 - y^2 = 3 \end{cases}$$

ανάγεται, με τη μέθοδο της απαλοιφής, στην επίλυση του απλούστερου συστήματος

$$\begin{cases} x^2 - 4 = 0 \\ y^2 - 1 = 0 \end{cases}$$

Επανερχόμενοι στο αρχικό μας πρόβλημα και ας θεωρήσουμε το αντίστοιχο του (Σ) στα πολυώνυμα μιας μεταβλητής. Αυτό είναι το

$$\left\{ \begin{array}{c} f_1(x) = 0 \\ f_2(x) = 0 \\ . \\ . \\ . \\ f_\mu(x) = 0 \end{array} \right\} \quad (\Sigma_1)$$

με τα πολυώνυμα $f_1(x)$, $f_2(x)$, …, $f_\mu(x)$ να είναι μιας μεταβλητής με συντελεστές από ένα σώμα F.

Ας δούμε τώρα κάποιες βασικές έννοιες που θα μας χρειαστούν για τη συνέχεια της επεξεργασίας του προβλήματος.

Πολυωνυμικός συνδυασμός των $f_1(x)$, $f_2(x)$, …, $f_\mu(x)$

Αν θεωρήσουμε τα τυχαία πολυώνυμα $h_1(x)$,$h_2(x)$,…,$h_\mu(x)$ του F[x], τότε το πολυώνυμο

$$h_1(x) \cdot f_1(x) + h_2(x) \cdot f_2(x) + \ldots + h_\mu(x) \cdot f_\mu(x)$$

το λέμε πολυωνυμικό συνδυασμό των $f_1(x)$, $f_2(x)$, …, $f_\mu(x)$

Σύνολο λύσεων συστήματος

Έστω (Σ) ένα σύστημα μ πολυωνυμικών εξισώσεων $f_i(x)=0$, i=1, 2,…, μ. Το σύνολο

$$\Lambda(\Sigma)=\{\xi\in\mathbb{R}: f_1(\xi)=0, f_2(\xi)=0, \ldots, f_\mu(\xi)=0\}$$

το λέμε σύνολο λύσεων του συστήματος (Σ).

Παρατηρήσεις

1. Είναι φανερό ότι αν $\xi\in\Lambda(\Sigma_1)$ τότε

$$h_1(\xi)\cdot f_1(\xi)+ h_2(\xi)\cdot f_2(\xi)+\ldots+ h_\mu(\xi)\cdot f_\mu(\xi)=0,$$

   που σημαίνει ότι κάθε στοιχείο του $\Lambda(\Sigma_1)$ μηδενίζει οποιοδήποτε πολυωνυμικό συνδυασμό των πολυωνύμων που απαρτίζουν το σύστημα. Από αυτό προκύπτει ότι το σύνολο λύσεων $\Lambda(\Sigma_1)$ του συστήματος είναι υποσύνολο του συνόλου λύσεων $\Lambda(g)$ του πολυωνύμου

$$g(x)= h_1(x)\cdot f_1(x)+ h_2(x)\cdot f_2(x)+\ldots+ h_\mu(x)\cdot f_\mu(x)$$

2. Αποδεικνύεται ότι, αν κάποιο από τα πολυώνυμα του συστήματος είναι πολυωνυμικός συνδυασμός των υπολοίπων, τότε η παράλειψη της αντίστοιχης εξίσωσης δεν μεταβάλλει το σύνολο λύσεων του. Έτσι, αν για παράδειγμα υποθέσουμε ότι

$$f_1(x)=\varphi_2(x)\cdot f_2(x)+ \varphi_3(x)\cdot f_3(x)+\ldots+ \varphi_\mu(x)\cdot f_\mu(x)$$

   τότε το (Σ_1) έχει το ίδιο σύνολο λύσεων με το

$$\left\{\begin{array}{c} f_2(x) = 0 \\ . \\ . \\ . \\ f_\mu(x) = 0 \end{array}\right\} \quad (\Sigma^*)$$

3. Από τα προαναφερθέντα συμπεραίνουμε ότι η αναζήτηση του συνόλου λύσεων $\Lambda(\Sigma_1)$ του συστήματος (Σ_1) ανάγεται, κατά κάποιο τρόπο, στην αναζήτηση λύσεων ενός πολυωνύμου, ή καλύτερα, ενός πολυωνυμικού

συνδυασμού. Ο ΜΚΔ $d(x)$, για τον οποίο έχουμε ήδη αναφέρει ότι γράφεται με τη μορφή

$$g_1(x)\cdot f_1(x)+g_2(x)\cdot f_2(x)+\ldots+g_\nu(x)\cdot f_\nu(x)=d(x)$$

φαίνεται στην περίπτωση αυτή να είναι ένα καλός πολυωνυμικός συνδυασμός.

3.1.ii. Ιδεώδες παραγόμενο από τα πολυώνυμα $f_1(x), f_2(x), \ldots, f_\mu(x)$

Έστω $f_1(x), f_2(x), \ldots, f_\mu(x)$ πολυώνυμα του δακτυλίου $F[x]$. Το σύνολο των πολυωνυμικών συνδυασμών τους, δηλαδή το σύνολο των πολυωνύμων της μορφής $h_1(x)\cdot f_1(x)+ h_2(x)\cdot f_2(x)+\ldots+ h_\mu(x)\cdot f_\mu(x)$ με $h_i\in F[x]$ το λέμε **ιδεώδες παραγόμενο από τα πολυώνυμα $f_1(x), f_2(x), \ldots, f_\mu(x)$** και το συμβολίζουμε

$$I=< f_1(x), f_2(x), \ldots, f_\mu(x) >.$$

Ας επανέλθουμε τώρα στο αρχικό μας σύστημα (Σ) και ας μιλήσουμε λίγο για πολυωνυμικούς συνδυασμούς στο $F[x_1, x_2, \ldots, x_\nu]$.

Πολυωνυμικοί συνδυασμοί στον δακτύλιο $F[x_1, x_2, \ldots, x_\nu]$

Έστω $f_1(x_1, x_2, \ldots, x_\nu)$, $f_2(x_1, x_2, \ldots, x_\nu)$, $\ldots$, $f_\mu(x_1, x_2, \ldots, x_\nu)$ πολυώνυμα του δακτυλίου των πολυωνύμων $F[x_1, x_2, \ldots, x_\nu]$ και $h_1(x_1, x_2, \ldots, x_\nu)$, $h_2(x_1, x_2, \ldots, x_\nu)$, $\ldots$, $h_\mu(x_1, x_2,\ldots,x_\nu)$ αυθαίρετα πολυώνυμα του $F[x_1, x_2, \ldots, x_\nu]$. Το πολυώνυμο

$$h_1(x_1, x_2, \ldots, x_\nu)\cdot f_1(x_1, x_2, \ldots, x_\nu)+ h_2(x_1, x_2, \ldots, x_\nu)\cdot f_2(x_1, x_2, \ldots, x_\nu)+\ldots$$
$$+ h_\mu(x_1, x_2, \ldots, x_\nu)\cdot f_\mu(x_1, x_2, \ldots, x_\nu)$$

το λέμε **πολυωνυμικό συνδυασμό** των

$$f_1(x_1, x_2, \ldots, x_\nu),\ f_2(x_1, x_2, \ldots, x_\nu), \ldots, f_\mu(x_1, x_2, \ldots, x_\nu).$$

Αποδεικνύεται ότι:

Αν $\{f_1(x_1, x_2, \ldots, x_\nu),\ f_2(x_1, x_2, \ldots, x_\nu), \ldots, f_\mu(x_1, x_2, \ldots, x_\nu)\}$ είναι ένα σύνολο πολυωνύμων του δακτυλίου $F[x_1, x_2, \ldots, x_\nu]$, τότε το σύνολο I των

πολυωνυμικών συνδυασμών των στοιχείων του παραπάνω συνόλου είναι ιδεώδες. Το ιδεώδες αυτό το συμβολίζουμε

$$I=\langle f_1(x_1, x_2, \ldots, x_\nu), f_2(x_1, x_2, \ldots, x_\nu), \ldots, f_\mu(x_1, x_2, \ldots, x_\nu)\rangle.$$

Η επόμενη πρόταση δηλώνει ότι το I περιέχει όλες τις πληροφορίες για το σύνολο λύσεων του συστήματος.

Πρόταση

Αν Λ(Σ) είναι το σύνολο λύσεων του συστήματος (Σ) και Λ(I) το σύνολο λύσεων του συστήματος που προκύπτει αν πάρουμε όλα τα (άπειρα) πολυώνυμα του I, τότε Λ(Σ)=Λ(I).

Απόδειξη

Έστω $(\xi_1, \xi_2, \ldots, \xi_\nu)$ ένα τυχαίο στοιχείο του συνόλου Λ(Σ). Τότε ισχύουν:

$$f_1(\xi_1, \xi_2, \ldots, \xi_\nu)=0,\ f_2(\xi_1, \xi_2, \ldots, \xi_\nu)=0,\ \ldots,\ f_\mu(\xi_1, \xi_2, \ldots, \xi_\nu)=0 \qquad \textbf{(1)}$$

Αν τώρα θεωρήσουμε ένα στοιχείο $g(x_1, x_2,\ldots,x_\nu)$ του I, αυτό είναι της μορφής

$$g(x_1, x_2, \ldots, x_\nu)=$$
$$=h_1(x_1, x_2, \ldots, x_\nu)\cdot f_1(x_1, x_2, \ldots, x_\nu)+h_2(x_1, x_2, \ldots, x_\nu)\cdot f_2(x_1, x_2, \ldots, x_\nu)+\ \ldots$$
$$+\ h_1(x_1, x_2, \ldots, x_\nu)\cdot f_1(x_1, x_2, \ldots, x_\nu) \qquad \textbf{(2)}$$

όπου $h_1(x_1, x_2, \ldots, x_\nu)$, $h_2(x_1, x_2, \ldots, x_\nu)$, …, $h_\mu(x_1, x_2, \ldots, x_\nu)$ αυθαίρετα πολυώνυμα του $F[x_1, x_2, \ldots, x_\nu]$. Από τις **(1)** προκύπτει ότι $g(\xi_1, \xi_2, \ldots, \xi_\nu)=0$, άρα $(\xi_1, \xi_2, \ldots, \xi_\nu)\in\Lambda(I)$ και κατά συνέπεια $\Lambda(\Sigma)\subseteq\Lambda(I)$.

Αντίστροφα, έστω $(\xi_1, \xi_2, \ldots, \xi_\nu)\in\Lambda(I)$. Αυτό σημαίνει ότι το $(\xi_1, \xi_2, \ldots, \xi_\nu)$ μηδενίζει κάθε πολυωνυμικό συνδυασμό των

$$f_1(x_1, x_2, \ldots, x_\nu), f_2(x_1, x_2, \ldots, x_\nu), \ldots, f_\mu(x_1, x_2, \ldots, x_\nu)$$

Ένας τέτοιος πολυωνυμικός συνδυασμός είναι και αυτός που προκύπτει από την **(2)** αν επιλέξουμε $h_1(x_1, x_2, \ldots, x_\nu)=1$ και $h_i(x_1, x_2, \ldots, x_\nu)=0$, $i=2, 3, \ldots, \mu$, δηλαδή το πολυώνυμο $f_1(x_1, x_2, \ldots, x_\nu)$. Άρα το $(\xi_1, \xi_2, \ldots, \xi_\nu)$ είναι λύση της $f_1(x_1, x_2, \ldots, x_\nu)=0$. Ομοίως προκύπτει ότι $f_i(\xi_1, \xi_2, \ldots, \xi_\nu)=0$, $i=2, 3,\ldots, \mu$, οπότε $(\xi_1, \xi_2, \ldots, \xi_\nu)\in\Lambda$, άρα $\Lambda(I)\subseteq\Lambda(\Sigma)$.

Από τα παραπάνω συνάγουμε ότι Λ(Σ)=Λ(I).

Παρατηρήσεις

1. Επειδή αυτό που μας ενδιαφέρει είναι το σύνολο λύσεων του συστήματος και όχι οι εξισώσεις του, από τη στιγμή που ισχύει Λ(Σ)=Λ(I) μας εξυπηρετεί να καταφύγουμε στο ιδεώδες που παράγουν τα πολυώνυμα του αρχικού συστήματος. Με τον τρόπο αυτό δημιουργούμε μια γέφυρα που θα μας περάσει από το αρχικό σύστημα σε άλλο το οποίο επιλύεται ευκολότερα. Το γεγονός ότι το ιδεώδες έχει άπειρα στοιχεία, δεν αποτελεί πρόβλημα, καθότι είναι ένα οργανωμένο σύνολο με αλγεβρική δομή. Έτσι το ιδεώδες ενός δακτυλίου θα μπορούσαμε να πούμε ότι, κατά κάποιο τρόπο, αντιστοιχεί στην κανονική υποομάδα μιας ομάδας.
2. Το $I=\langle f_1(x_1, x_2, \ldots, x_v), f_2(x_1, x_2, \ldots, x_v), \ldots, f_\mu(x_1, x_2, \ldots, x_v)\rangle$ το λέμε **ιδεώδες που παράγεται από το σύνολο**

   $$\{f_1(x_1, x_2, \ldots, x_v), f_2(x_1, x_2, \ldots, x_v), \ldots, f_\mu(x_1, x_2, \ldots, x_v)\}$$

   το οποίο το λέμε και **γεννήτορα του ιδεώδους**.
3. Πιο πάνω που αναφέραμε σχετικά με την ταυτότητα της διαίρεσης του $f(x, y)=xy^2-x$, με τα «διάνυσματα πολυωνύμων» (f_1, f_2) και (f_2, f_1) είδαμε ότι

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

   είτε

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

   Από αυτό προκύπτει ότι αν και $f\in\langle f_1, f_2\rangle$ ενδέχεται η διαίρεση του με (f_1, f_2) να δίνει μη μηδενικό υπόλοιπο. Έτσι **η συνθήκη υ(x, y)=0 είναι ικανή αλλά όχι αναγκαία ώστε ένα πολυώνυμο να περιέχεται στο ιδεώδες που παράγουν κάποια άλλα.** Αυτό που μας ενδιαφέρει είναι ο προσδιορισμός «καλών» γεννητόρων για το I, δηλαδή πολυωνύμων που θα παράγουν το I και η συνθήκη υ(x, y)=**0** να είναι αναγκαία και ικανή ώστε $f\in\langle f_1, f_2\rangle$. Όπως θα δούμε παρακάτω τέτοιο «καλοί» γεννήτορες είναι τα στοιχεία μιας βάσης Groebner.

3.1.iii. Βάσεις Groebner

Όπως έχουμε ήδη αναφέρει το σύνολο λύσεων Λ(Σ) του αρχικού μας συστήματος είναι ίσο με το σύνολο λύσεων Λ(I) όπου με I συμβολίσουμε το ιδεώδες που παράγεται από τα πολυώνυμα του συστήματος. Θεωρούμε ότι σε κάθε πολυώνυμο $f(x_1, x_2,\ldots,x_v)$ του I επιλέγοντας μια λεξικογραφική διάταξη, επισυνάπτουμε τον μεγιστοβάθμιο όρο του και κατόπιν ορίζουμε το σύνολο:

$$MO(I)=\{ x_1^{\kappa_1} \cdot x_2^{\kappa_2} \cdot \ldots \cdot x_v^{\kappa_v} \text{ , όπου } x_1^{\kappa_1} \cdot x_2^{\kappa_2} \cdot \ldots \cdot x_v^{\kappa_v} \text{ κάποιος μεγιστοβάθμιος όρος πολυωνύμου του I}\}$$

που σχηματίζουν όλοι οι μεγιστοβάθμιοι όροι των πολυωνύμων του I.

Τα στοιχεία του MO(I), που είναι μονώνυμα πολλών μεταβλητών, είναι προφανώς άπειρα στο πλήθος. Αν θεωρήσουμε το ιδεώδες <MO(I)> που παράγεται από όλα τα στοιχεία του MO(I), αποδεικνύεται ότι:

Για κάθε ιδεώδες I≠{0}, του δακτυλίου $F[x_1, x_2, \ldots, x_v]$ υπάρχει πεπερασμένο πλήθος μονωνύμων του MO(I), έστω το $B=\{ x_1^{\lambda_{i1}} \cdot x_2^{\lambda_{i2}} \ldots x_v^{\lambda_{iv}}$, i=1, 2, …, κ} με την ιδιότητα <B>=<MO(I)>.

Παρατηρήσεις

1. Από την παραπάνω πρόταση προκύπτει ότι αρκεί πεπερασμένο πλήθος μονωνύμων, για να παραχθεί το ιδεώδες <MO(I)>.
2. Κάθε μονώνυμο $x_1^{\lambda_{i1}} \cdot x_2^{\lambda_{i2}} \ldots x_v^{\lambda_{iv}}$ του B είναι μεγιστοβάθμιος όρος κάποιου πολυωνύμου του I, δηλαδή υπάρχει πολυώνυμο $g_i(x_1, x_2,\ldots,x_v)$ του I το οποίο έχει ως μεγιστοβάθμιο όρο το συγκεκριμένο μονώνυμο.
3. Τόσο το <MO(I)> όσο και το <B> είναι ιδεώδη μονωνύμων με τη διαφορά ότι το <B> είναι πεπερασμένα παραγόμενο.
4. Σχετικά με τα ιδεώδη μονωνύμων αποδεικνύεται ότι ένα μονώνυμο ανήκει σε κάποιο ιδεώδες μονωνύμων αν και μόνο αν αυτό διαιρείται με κάποιο από τα μονώνυμα που παράγουν το ιδεώδες.
5. Τα πολυώνυμα $g_i(x_1, x_2, \ldots, x_v)$ του I, δεν είναι μοναδικά για δεδομένο μεγιστοβάθμιο όρο. Το πεπερασμένο σύνολο

$$G=\{ g_i(x_1, x_2, \ldots, x_v), i=1, 2, \ldots, \kappa \}$$

που σχηματίζουν, το λέμε **βάση Groebner του ιδεώδους I.**

6. Από τα παραπάνω συνάγεται ότι αν G είναι μια βάση Groebner του I, τότε

$$<MO(I)>=<MO(g_1), MO(g_2), \ldots, MO(g_\kappa)>$$

Η τελευταία ισότητα δεν ισχύει γενικά για τυχαίο σύνολο πολυωνύμων. Στην πράξη αν $I=<f_1, f_2, \ldots, f_v>$ τότε

$$<MO(f_1), MO(f_2),\ldots, MO(f_v)> \subseteq MO(I).$$

Παραδείγματα

1. Θεωρούμε τα πολυώνυμα $f_1(x, y)=x^3-2xy$, $f_2(x, y)=x^2y-2y^2+x=yx^2+x-2y^2$ (αν το διατάξουμε λεξικογραφικά) και έστω $I=<f_1, f_2>$. Τότε το πολυώνυμο x^2 είναι στοιχείο του I, καθότι

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

οπότε $x^2=MO(x^2)\in<MO(I)>$.

Από την άλλη μεριά όμως $x^2\notin<MO(f_1), MO(f_2)>$ αφού το x^2 δεν διαιρείται από τους $MO(f_1)$ και $MO(f_2)$.

Το γεγονός αυτό υποδηλώνει ότι το $\{f_1, f_2\}$ δεν είναι βάση Groebner του I. Επιπλέον φαίνεται καθαρά, όπως προαναφέραμε, ότι

$$<MO(f_1), MO(f_2)> \subseteq MO(I).$$

2. Θεωρούμε τα πολυώνυμα $g_1(x, y, z)=x+z$ και $g_2(x, y, z)=y-z$. Θα αποδείξουμε ότι το σύνολο $B=\{g_1, g_2\}$ είναι μια βάση Groebner του $I=<g_1, g_2>$. Αρκεί να αποδείξουμε ότι ο μεγιστοβάθμιος όρος κάθε μη μηδενικού πολυωνύμου του I ανήκει στο ιδεώδες που παράγουν οι $MO(g_1)$, $MO(g_2)$, οπότε

$$< MO(g_1), MO(g_2)> =<x, y>.$$

Για το σκοπό αυτό θα δείξουμε ότι ο μεγιστοβάθμιος όρος οποιουδήποτε στοιχείου του I διαιρείται με ένα τουλάχιστον εκ των x, y. Θεωρούμε το μη μηδενικό πολυώνυμο f του I και έστω $f=Ag_1+Bg_2$. Αν ο μεγιστοβάθμιος όρος του δεν διαιρείται ούτε με το x ούτε με το y, τότε θα είναι πολυώνυμο του z. Επειδή όμως για το σύστημα

$$\begin{cases} x + z = 0 \\ y - z = 0 \end{cases} \quad (\Sigma)$$

έχουμε $\Lambda(\Sigma)=\{(-z, z, z), z\in\mathbb{R}\}$, συμπεραίνουμε ότι, κάθε τριάδα της μορφής (-z, z, z) μηδενίζει το πολυώνυμο οπότε αυτό είναι το μηδενικό, άτοπο. Άρα ο μεγιστοβάθμιος όρος του πολυώνυμου διαιρείται είτε με το x είτε με το y, οπότε το B είναι μια βάση Groebner του I.

3.1.iv. Βάση Groebner στο δακτύλιο πολυωνύμων μιας μεταβλητής

Έστω F[x] ο δακτύλιος των πολυωνύμων μιας μεταβλητής με συντελεστές από κάποιο σώμα F και I ένα μη μηδενικό ιδεώδες του F[x]. Αν θεωρήσουμε τους βαθμούς των πολυωνύμων του I, οι οποίοι είναι μη αρνητικοί ακέραιοι, τότε, σύμφωνα με την αρχή του ελάχιστου, υπάρχει ελάχιστος (βαθμός). Αυτό σημαίνει ότι μεταξύ των πολυωνύμων του I υπάρχει κάποιο που έχει τον ελάχιστο βαθμό και ας υποθέσουμε ότι αυτό είναι το f(x). Θα αποδείξουμε ότι:

Αν f(x) είναι το ελαχιστοβάθμιο πολυώνυμο του I, τότε I=<f(x)>, δηλαδή κάθε άλλο πολυώνυμο του I είναι πολλαπλάσιο του f(x).

Απόδειξη

Έστω h(x) τυχαίο πολυώνυμο του I. Από την ταυτότητα της διαίρεσης προκύπτει ότι υπάρχουν μοναδικά πολυώνυμα π(x), υ(x) ώστε να ισχύει $h(x)=f(x)\cdot\pi(x)+\upsilon(x)$. Αν θεωρήσουμε ότι το υ(x) είναι διαφορετικό από το μηδενικό, τότε $0 \le \deg\upsilon(x)<\deg f(x)$ και από την ισότητα $\upsilon(x)= h(x)-f(x)\cdot\pi(x)$ προκύπτει το υ(x) περιέχεται στο I. Έτσι έχουμε μέσα στο I, πολυώνυμο με βαθμό μικρότερο από αυτόν του f(x), το οποίο είναι άτοπο, αφού υποθέσαμε ότι το f(x) είναι το πολυώνυμο του I με τον ελάχιστο βαθμό. Άρα, κάθε άλλο πολυώνυμο του I είναι πολλαπλάσιο του f(x), οπότε I=<f(x)>.

Παρατήρηση

Από τα παραπάνω προκύπτει ότι κάθε μη μηδενικό ιδεώδες I του F[x] παράγεται από ένα συγκεκριμένο στοιχείο του. Στην περίπτωση αυτή λέμε ότι το I είναι **κύριο ιδεώδες** και ο F[x] είναι **δακτύλιος κύριων ιδεωδών.**

Διαδικασία εύρεσης βάσης Groebner στο I.

1. Σχηματίζουμε το σύνολο:
   MO(I)={x^{κ}, όπου x^{κ} μεγιστοβάθμιος όρος κάποιου πολυωνύμου του I}.
2. Θεωρούμε το ιδεώδες του F[x] που παράγεται από το MO(I) και ας είναι x^{ν} η ελάχιστη δύναμη του x που βρίσκεται στο MO(I). Θα αποδείξουμε ότι $<MO(I)>=<x^{\nu}>$. Πράγματι, για οποιοδήποτε $x^{\rho}\in<MO(I)>$ ισχύει $x^{\rho}=x^{\nu}\cdot x^{\rho-\nu}$ με τον ακέραιο ρ-ν να είναι μη αρνητικός, οπότε $x^{\rho}\in<x^{\nu}>$ και κατά συνέπεια $<MO(I)>\subseteq<x^{\nu}>$. Επίσης $x^{\nu}\in MO(I)$ οπότε $<x^{\nu}>\subseteq<MO(I)>$. Άρα $<MO(I)>=<x^{\nu}>$.
3. Για να προσδιορίσουμε μια βάση Groebner πλέον, απομένει να βρούμε πολυώνυμο με μεγιστοβάθμιο όρο x^{ν}. Τέτοιο πολυώνυμο όμως, όπως αναφέραμε προηγουμένως, υπάρχει και είναι το f(x) που έχει τον ελάχιστο βαθμό και παράγει το I.

Συμπερασματικά λοιπόν, **κάθε μη μηδενικό ιδεώδες I του F[x] έχει, τουλάχιστον μια, βάση Groebner. Αυτή είναι το σύνολο {f(x)} όπου f πολυώνυμο του I με τον ελάχιστο βαθμό.**

3.1.ν. Βάση Groebner στο δακτύλιο πολυωνύμων δυο μεταβλητών.

Έστω F[x, y] ο δακτύλιος των πολυωνύμων δυο μεταβλητών με συντελεστές από ένα σώμα F και I μη μηδενικό ιδεώδες. Θα αποδείξουμε την ακόλουθη πρόταση.

Πρόταση

Αν I είναι μη μηδενικό ιδεώδες του F[x, y] τότε το I έχει, τουλάχιστον μια, βάση Groebner.

Απόδειξη

Θεωρούμε το σύνολο

$MO(I)=\{x^{\kappa}y^{\lambda}$, όπου $x^{\kappa}y^{\lambda}$ είναι μεγιστοβάθμιος όρος κάποιου πολυωνύμου του I$\}$

Αρχικά θα δείξουμε ότι το ιδεώδες <MO(I)> είναι πεπερασμένα παραγόμενο.

Θεωρούμε το ιδεώδες J του F[x] που παράγεται από όλα τα x^{κ} για τα οποία υπάρχει y^{λ} ώστε $x^{\kappa}y^{\lambda}\in$ <MO(I)>. Με τον τρόπο αυτό έχουμε κάνει με μια έννοια προβολή του ιδεώδους <MO(I)> στον δακτύλιο F[x], όποτε σύμφωνα με αυτά που εκθέσαμε προηγουμένως, το J είναι κύριο ιδεώδες. Αυτό σημαίνει ότι υπάρχει μη αρνητικός ακέραιος ν με την ιδιότητα $J=\langle x^{\nu}\rangle$ και για τον συγκεκριμένο ν υπάρχει επίσης μη αρνητικός ακέραιος ρ ώστε $x^{\nu}y^{\rho}\in$ <MO(I)>.

Το ερώτημα που εγείρεται τώρα είναι τι συμβαίνει στην περίπτωση όπου κάποιος μεγιστοβάθμιος όρος πολυωνύμου του I είναι της μορφής $x^{\mu}y^{\xi}$ με $\xi<\rho$. (Η περίπτωση όπου έχουμε $x^{\mu}y^{\xi}$ με $\xi\geq\rho$ αντιμετωπίζεται εύκολα καθότι τότε το $x^{\nu}y^{\rho}$ διαιρεί το $x^{\mu}y^{\xi}$ αφού $x^{\mu}y^{\xi}=x^{\mu-\nu}y^{\xi-\rho}x^{\nu}y^{\rho}$). Η ενδεδειγμένη αντιμετώπιση είναι η εξής:

- Για τον ακέραιο ρ-1 θεωρούμε το ιδεώδες $J_{\rho-1}$ του F[x] που παράγεται από όλα τα x^{κ} με $x^{\kappa}y^{\rho-1}\in$ <MO(I)> και δεδομένου ότι ο δακτύλιος F[x] είναι δακτύλιος κύριων ιδεωδών, συνάγεται ότι υπάρχει μη αρνητικός ακέραιος $\nu_{\rho-1}$ με $J_{\rho-1}=\langle x^{\nu_{\rho-1}}\rangle$.
- Για τον ακέραιο ρ-2 θεωρούμε το ιδεώδες $J_{\rho-2}$ του F[x] που παράγεται από όλα τα x^{κ} με $x^{\kappa}y^{\rho-2}\in$ <MO(I)> και δεδομένου ότι ο δακτύλιος F[x] είναι δακτύλιος κύριων ιδεωδών, συνάγεται ότι υπάρχει μη αρνητικός ακέραιος $\nu_{\rho-2}$ με $J_{\rho-2}=\langle x^{\nu_{\rho-2}}\rangle$.
- ……

- Για τον ακέραιο 1 θεωρούμε το ιδεώδες J_1 του F[x] που παράγεται από όλα τα x^κ με $x^\kappa y \in$ <MO(I)> και δεδομένου ότι ο δακτύλιος F[x] είναι δακτύλιος κύριων ιδεωδών, συνάγεται ότι υπάρχει μη αρνητικός ακέραιος ν_1 με $J_1 = \langle x^{\nu_1} \rangle$.
- Για τον ακέραιο 0 θεωρούμε το ιδεώδες J_0 του F[x] που παράγεται από όλα τα x^κ με $x^\kappa \in$ <MO(I)> και δεδομένου ότι ο δακτύλιος F[x] είναι δακτύλιος κύριων ιδεωδών, συνάγεται ότι υπάρχει μη αρνητικός ακέραιος ν_0 με $J_0 = \langle x^{\nu_0} \rangle$.

Επιπλέον, αποδεικνύεται ότι:

1. Το μη μηδενικό ιδεώδες <MO(I)> του δακτυλίου F[x, y] παράγεται από το πεπερασμένο σύνολο μονωνύμων $x^\nu y^\rho$, $x^{\nu_{\rho-1}} y^{\rho-1}$, … , x^{ν_0}.
2. Υπάρχουν πολυώνυμα $g_0(x, y)$, $g_1(x, y)$, … , $g_\rho(x, y)$ που ανήκουν στο ιδεώδες I με την ιδιότητα
   $MOg_0(x, y) = x^{\nu_0}$, $MOg_1(x, y) = x^{\nu_1} y$, … , $MOg_\rho(x, y) = x^\nu y^\rho$.

Από τα παραπάνω προκύπτει ότι το σύνολο $\{g_0(x, y), g_1(x, y), \dots, g_\rho(x, y)\}$ των πολυωνύμων του I είναι ένα πεπερασμένο υποσύνολο του I και ικανοποιεί τη σχέση

$$\langle MO(I) \rangle = \langle MO(g_0(x, y)), MO(g_1(x, y)), \dots, MO(g_\rho(x, y)) \rangle$$

οπότε είναι μια **βάση Groebner** του I.

Στο σημείο αυτό ας επανέλθουμε στο δακτύλιο $F[x_1, x_2, \dots, x_\nu]$.

3.1.vi. Ελαχιστοποιημένες και ανηγμένες βάσεις Groebner.

Από όσα έχουμε αναφέρει μέχρι το σημείο αυτό, σχετικά με τη βάση ενός μη τετριμμένου ιδεώδους I, δεν προκύπτει ότι αυτή είναι μοναδική. Γενικά ένα ιδεώδες έχει πολλές βάσεις Groebner. Η κρίσιμη ιδιότητα για να είναι ένα σύνολο πολυωνύμων

$$G = \{ g_i(x_1, x_2, \dots, x_\nu), i=1, 2, \dots, \kappa \}$$

βάση Groebner του ιδεώδους I, είναι:

$$<MO(I)>=<MO(g_1), MO(g_2), \ldots, MO(g_\kappa)>$$

Αν ο μεγιστοβάθμιος όρος κάποιου πολυωνύμου της G ανήκει στο ιδεώδες που παράγουν οι μεγιστοβάθμιοι όροι των υπολοίπων, τότε παραλείποντας αυτό το πολυώνυμο μπορούμε να κατασκευάσουμε μια νέα βάση Groebner του I.

Έστω I ένα μη τετριμμένο ιδεώδες του δακτυλίου $F[x_1, x_2, \ldots, x_v]$. Το πεπερασμένο υποσύνολο $G=\{ g_i(x_1, x_2,\ldots,x_v), i=1, 2, \ldots, \kappa \}$ του I ονομάζεται **ελαχιστοποιημένη (minimal) βάση Groebner του ιδεώδους I,** αν:

- Όλοι οι συντελεστές των μεγιστοβάθμιων όρων των πολυωνύμων του G είναι μονάδες.
- Για οποιοδήποτε $i\in\{1, 2, \ldots, \kappa\}$ ο μεγιστοβάθμιος όρος του πολυωνύμου $g_i(x_1, x_2, \ldots, x_v)$ δεν ανήκει στο ιδεώδες που παράγουν οι υπόλοιποι μεγιστοβάθμιοι όροι.

Παρατηρήσεις

1. Αν κάποιος ή κάποιοι από τους μεγιστοβάθμιους όρους έχει συντελεστή διαφορετικό της μονάδας, τότε λόγω του ορισμού του ιδεώδους, το ιδεώδες που παράγουν δεν μεταβάλλεται αν θεωρήσουμε ότι κάθε μεγιστοβάθμιος συντελεστής είναι ίσος με τη μονάδα.
2. Από κάθε βάση Groebner του ιδεώδους I, μπορούμε να καταλήξουμε σε μια ελαχιστοποιημένη βάση Groebner του I, αφαιρώντας όλα τα πολυώνυμα των οποίων οι μεγιστοβάθμιοι όροι ανήκουν στο ιδεώδες που παράγουν οι υπόλοιποι.
3. Όπως και η απλή βάση, έτσι και η ελαχιστοποιημένη βάση Groebner δεν είναι μοναδική.

Έστω I ένα μη τετριμμένο ιδεώδες του δακτυλίου $F[x_1, x_2, \ldots, x_v]$. Το πεπερασμένο υποσύνολο $G=\{ g_i(x_1, x_2,\ldots,x_v), i=1, 2, \ldots, \kappa \}$ του I ονομάζεται **ανηγμένη (reduced) βάση Groebner του ιδεώδους I,** αν:

- Όλοι οι συντελεστές των μεγιστοβάθμιων όρων των πολυωνύμων του G είναι μονάδες (όπως και στην ελαχιστοποιημένη).
- Κανένας όρος του πολυωνύμου $g_i(x_1, x_2, \ldots, x_v)$ δεν ανήκει στο ιδεώδες που παράγουν οι υπόλοιποι μεγιστοβάθμιοι όροι, για οποιοδήποτε $i \in \{1, 2, \ldots, \kappa\}$ (και όχι μόνο ο μεγιστοβάθμιος όπως στην ελαχιστοποιημένη).

Παρατηρήσεις

1. Επισημαίνουμε ότι στην ανηγμένη βάση Groebner δεν υπάρχει μεγιστοβάθμιος όρος κανενός πολυωνύμου που να περιέχεται στο ιδεώδες που παράγουν οι υπόλοιποι μεγιστοβάθμιοι όροι.
2. Αποδεικνύεται ότι, οποιοδήποτε μη τετριμμένο ιδεώδες του δακτυλίου $F[x_1, x_2, \ldots, x_v]$, έχει, μια μοναδική, ανηγμένη βάση Groebner.

3.1.vii. Ο αλγόριθμος του Buchberger.

Μέχρι το σημείο αυτό έχουμε αναφέρει ότι κάθε ιδεώδες I δέχεται μια βάση Groebner. Ας δούμε τώρα ένα αλγόριθμο για τον υπολογισμό βάσης Groebner. Ο αλγόριθμος αυτός οφείλεται στον **Buchberger** ο οποίος ήταν μαθητής του Groebner και παρουσιάσθηκε το 1965. Αξίζει να τονίσουμε ότι το ίδιο έτος ο Ιάπωνας μαθηματικός **Hironaka** μελετώντας δακτυλίους δυναμοσειρών ανακάλυψε ανεξάρτητα την ίδια έννοια.

Πριν όμως εκθέσουμε τον αλγόριθμο, ας ξεκινήσουμε με κάποιους ορισμούς.

Έστω $f_1(x_1, x_2, \ldots, x_v)$ και $f_2(x_1, x_2, \ldots, x_v)$ δυο πολυώνυμα τα οποία περιέχονται στον δακτύλιο $F[x_1, x_2, \ldots, x_v]$ και ας είναι $\alpha \cdot x_1^{\kappa_1} x_2^{\kappa_2} \ldots x_v^{\kappa_v}$ και $\beta \cdot x_1^{\rho_1} x_2^{\rho_2} \ldots x_v^{\rho_v}$ οι αντίστοιχοι μεγιστοβάθμιοι όροι τους.

- **Ελάχιστο κοινό πολλαπλάσιο** των μονωνύμων $x_1^{\kappa_1} x_2^{\kappa_2} \ldots x_v^{\kappa_v}$ και $x_1^{\rho_1} x_2^{\rho_2} \ldots x_v^{\rho_v}$ είναι το μονώνυμο $x_1^{\xi_1} x_2^{\xi_2} \ldots x_v^{\xi_v}$ όπου $\xi_i = \max(\kappa_i, \rho_i)$, $i=1, 2, \ldots, v$.

- **S – πολυώνυμο** των f_1, f_2 ονομάζουμε το πολυώνυμο

$$S(f_1, f_2) = \frac{x_1^{\xi_1} x_2^{\xi_2} \ldots x_v^{\xi_v}}{\alpha \cdot x_1^{\kappa_1} x_2^{\kappa_2} \ldots x_v^{\kappa_v}} \cdot f_1 - \frac{x_1^{\xi_1} x_2^{\xi_2} \ldots x_v^{\xi_v}}{\beta \cdot x_1^{\rho_1} x_2^{\rho_2} \ldots x_v^{\rho_v}} \cdot f_2$$

Παρατήρηση

Από τον τρόπο που ορίστηκε το $S(f_1, f_2)$ προκύπτει ότι σ΄ αυτό έχουν απαλειφθεί οι μεγιστοβάθμιοι όροι των f_1, f_2.

Παράδειγμα

Αν θεωρήσουμε τα πολυώνυμα $f_1(x, y)=x^3y^2+x$ και $f_2(x, y)=3x^4y+y^2$ του $\mathbb{R}[x, y]$ τότε ΕΚΠ$(x^3y^2, x^4y)=x^4y^2$ και

$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f_1 + \frac{x^4y^2}{3x^4y} \cdot f_2 = x \cdot f_1 - \frac{1}{3} y \cdot f_2$$

$$= -x^3y^3 + x^2 - \frac{1}{3} y^3$$

Αποδεικνύεται ότι:

Αν $F[x_1, x_2, \ldots, x_v]$ είναι ο δακτύλιος των πολυωνύμων και $I=\langle f_1, f_2, \ldots, f_\mu \rangle$ ένα ιδεώδες του, τότε το σύνολο $G=\{f_1, f_2, \ldots, f_\mu\}$ είναι βάση Groebner του I, αν και μόνο αν το υπόλοιπο της διαίρεσης του $S(f_i, f_j)$ δια του G είναι μηδενικό για οποιοδήποτε ζεύγος i, j με $i \neq j$ και $i, j=1, 2, \ldots, v$.

Η παραπάνω πρόταση, που αποτελεί κριτήριο για τον χαρακτηρισμό ενός συνόλου ως βάση Groebner, οδηγεί στον αλγόριθμο του οποίου τα βήματα είναι τα ακόλουθα:

1. Τοποθετούμε τα πολυώνυμα $f_1, f_2, \ldots, f_\mu$ σε μια σειρά.
2. Υπολογίζουμε το πολυώνυμο $S(f_1, f_2)$
3. Υπολογίζουμε το υπόλοιπο $\upsilon(S(f_1, f_2))$ της διαίρεσης του $S(f_1, f_2)$ δια του συνόλου $\{f_1, f_2, \ldots, f_\mu\}$.
4. Αν το προηγούμενο υπόλοιπο είναι μηδενικό, τότε συνεχίζουμε με το $S(f_1, f_3)$ διαιρώντας το με το σύνολο $\{f_1, f_2, \ldots, f_\mu\}$. Αν το υπόλοιπο δεν είναι μηδενικό, τότε θεωρούμε το νέο σύνολο $\{f_1, f_2, \ldots, f_\mu, \upsilon(S(f_1, f_2))\}$ στη θέση του προηγούμενου.

5. Συνεχίζουμε τον αλγόριθμο ελέγχοντας για όλα τα $S(f_i, f_j)$ τα υπόλοιπά τους και προσθέτοντας, αν χρειαστεί, στο αρχικό σύνολο και τα πολυώνυμα $\upsilon(S(f_i, f_j))$.
6. Ο αλγόριθμος τερματίζει όταν σε όλους τους ελέγχους που αναφέραμε, όλα τα υπόλοιπα είναι μηδενικά.

3.1.viii. Το θεώρημα βάσης του Hilbert

Αν I είναι ένα ιδεώδες του δακτυλίου πολυωνύμων $F[x_1, x_2, \ldots, x_v]$, τότε υπάρχει ένα πεπερασμένο πλήθος πολυωνύμων του $F[x_1, x_2, \ldots, x_v]$ το οποίο παράγει το I.

Απόδειξη

- Αν το I είναι το μηδενικό ιδεώδες, τότε μπορούμε να ισχυριστούμε ότι αυτό παράγεται από το μηδενικό πολυώνυμο του $F[x_1, x_2, \ldots, x_v]$ οπότε το ζητούμενο ισχύει.
- Υποθέτουμε ότι $I \neq \{0\}$. Στην περίπτωση αυτή, όπως έχουμε ήδη αναφέρει το I έχει, τουλάχιστον μια βάση Groebner και ας θεωρήσουμε ως τέτοια το

$$B=\{g_1(x_1, x_2, \ldots, x_v), g_2(x_1, x_2, \ldots, x_v), \ldots, g_\kappa(x_1, x_2, \ldots, x_v)\}$$

Θα αποδείξουμε ότι το B παράγει το I με την έννοια ότι το σύνολο των πολυωνυμικών συνδυασμών του B είναι το I. Έστω $f_1(x_1, x_2, \ldots, x_v)$ ένα πολυώνυμο του ιδεώδους. Αν κάνουμε τη διαίρεση του $f_1(x_1, x_2, \ldots, x_v)$ με το B τότε έχουμε

$$f_1(x_1, x_2, \ldots, x_v)=$$
$$=h_1(x_1, x_2, \ldots, x_v)\cdot g_\kappa(x_1, x_2, \ldots, x_v)+\ldots+ h_\kappa(x_1, x_2, \ldots, x_v)\cdot g_\kappa(x_1, x_2, \ldots, x_v)$$
$$+Y(x_1, x_2, \ldots, x_v)$$

όπου $Y(x_1, x_2, \ldots, x_v)$ είναι το υπόλοιπο της διαίρεσης. Η σχέση αυτή γράφεται επίσης

$$Y(x_1, x_2, \ldots, x_v)=$$
$$=f_1(x_1, x_2, \ldots, x_v) - h_1(x_1, x_2, \ldots, x_v)\cdot g_\kappa(x_1, x_2, \ldots, x_v) -\ldots -$$
$$h_\kappa(x_1, x_2, \ldots, x_v)\cdot g_\kappa(x_1, x_2, \ldots, x_v)$$

Τα πολυώνυμα όμως

$$f_1(x_1, x_2, \ldots, x_v), g_1(x_1, x_2, \ldots, x_v), g_2(x_1, x_2, \ldots, x_v), \ldots, g_\kappa(x_1, x_2, \ldots, x_v)$$

ανήκουν στο ιδεώδες I, οπότε και το $Y(x_1, x_2, \ldots, x_v)$ ανήκει επίσης στο ιδεώδες του I.

Δεδομένου ότι το σύνολο B είναι μια βάση Groebner του I, ο μεγιστοβάθμιος όρος του $Y(x_1, x_2, \ldots, x_v)$ θα ανήκει στο ιδεώδες που παράγουν οι μεγιστοβάθμιοι όροι των πολυωνύμων του B.

Για το $Y(x_1, x_2, \ldots, x_v)$ υπάρχουν οι ακόλουθες δυο περιπτώσεις

- Το $Y(x_1, x_2, \ldots, x_v)$ είναι το μηδενικό πολυώνυμο, το οποίο σημαίνει ότι το $f_1(x_1, x_2, \ldots, x_v)$ ανήκει στο ιδεώδες που παράγεται από το σύνολο B, που είναι το ζητούμενο.
- Το $Y(x_1, x_2, \ldots, x_v)$ δεν είναι το μηδενικό πολυώνυμο, οπότε έχει κάποιο μεγιστοβάθμιο όρο (μη μηδενικό). Ο όρος αυτός θα διαιρείται από το μεγιστοβάθμιο όρο κάποιου πολυωνύμου του B. Αυτό όμως αποκλείεται διότι τότε η αρχική διαίρεση θα είχε προχωρήσει και δεν θα έδινε ως υπόλοιπο το $Y(x_1, x_2, \ldots, x_v)$.

Επομένως, σε κάθε περίπτωση, το B παράγει το I.

Από τα παραπάνω προκύπτει το ακόλουθο βασικό

Πόρισμα

Ένα πολυώνυμο $f_1(x_1, x_2, \ldots, x_v)$ του $F[x_1, x_2, \ldots, x_v]$ ανήκει στο ιδεώδες I αν και μόνο αν το υπόλοιπο του από τη διαίρεση με μια βάση Groebner του I είναι μηδενικό.

Στο σημείο αυτό και πριν περάσουμε στην επόμενη ενότητα, ας δούμε πως σχετίζονται τα προηγούμενα με την απαλοιφή Gauss, όπως έχουμε ήδη αναφέρει από το πρώτο κεφάλαιο.

Θεωρούμε το σύστημα των πολυωνύμων

$$\begin{cases} 3x - 6y - 2z = 0 \\ 2x - 4y + 4w = 0 \\ x - 2y - z - w = 0 \end{cases}$$

Εύκολα βρίσκουμε ότι ο πίνακας των συντελεστών του είναι

$$\begin{pmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \\ 1 & -2 & -1 & -1 \end{pmatrix}$$

ο γραμμικά ισοδύναμος κλιμακωτός πίνακας είναι

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

και ο αντίστοιχος γραμμικά ισοδύναμος ανηγμένος κλιμακωτός είναι

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

Αν I είναι το ιδεώδες που παράγουν τα πολυώνυμα του συστήματος, τότε αποδεικνύεται ότι:

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

και τα πολυώνυμα $f_1=x-2y-z-w$, $f_2=z+3w$ που προκύπτουν από τον πίνακα (1) αποτελούν μια **ελαχιστοποιημένη βάση Groebner του I.**

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

και τα πολυώνυμα $g_1=x-2y+2w$, $g_2=z+3w$ που προκύπτουν από τον πίνακα (2) αποτελούν την **ανηγμένη βάση Groebner του I.**

3.2. Αυτόματη απόδειξη Γεωμετρικών θεωρημάτων

Στην αρχή ήδη του κεφαλαίου αναφέραμε ότι η κεντρική ιδέα πάνω στην οποία βασίζεται η προσπάθεια της αυτόματης απόδειξης είναι η ακόλουθη:
Αν οι υποθέσεις και τα συμπεράσματα ενός θεωρήματος μπορούν να διατυπωθούν με πολυώνυμα, τότε η απόδειξη του θεωρήματος έχει να κάνει με την ύπαρξη ή μη ύπαρξη κάποιων πολυωνύμων σε συγκεκριμένο ιδεώδες.

Η επόμενη πρόταση μας δίνει μια λίστα μερικών από τις πιο συνηθισμένες γεωμετρικές ιδιότητες οι οποίες επιδέχονται μετάφραση που οδηγεί σε πολυωνυμικές εξισώσεις. Συγκεκριμένα αποδεικνύεται ότι:

Πρόταση

Έστω Α, Β, Γ, Δ, Ε, Ζ σημεία του επιπέδου. Καθεμιά από τις επόμενες γεωμετρικές ιδιότητες μπορεί να εκφραστεί από μια ή περισσότερες πολυωνυμικές εξισώσεις.

i) Η ΑΒ είναι παράλληλη στην ΓΔ.

ii) Η ΑΒ είναι κάθετη στην ΓΔ.

iii) Τα σημεία Α, Β, Γ είναι συνευθειακά.

iv) Η απόσταση του σημείου Α από το Β είναι ίση με την απόσταση του Γ από το Δ.

v) Το Γ είναι σημείο του κύκλου με κέντρο Α και ακτίνα ΑΒ.

vi) Το σημείο Γ είναι το μέσο του τμήματος ΑΒ.

vii) Η οξεία γωνία $\widehat{ΑΒΓ}$ είναι ίση με την επίσης οξεία γωνία $\widehat{ΔΕΖ}$.

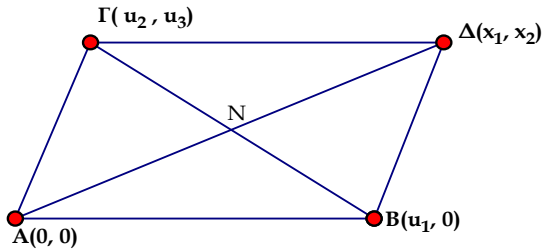
viii) Η ΒΔ είναι διχοτόμος της γωνίας $\widehat{ΑΒΓ}$.

Παρατηρήσεις

1. Οι παραπάνω ιδιότητες δεν είναι οι μοναδικές που επιδέχονται «πολυωνυμική μετάφραση».
2. Ένα γεωμετρικό θεώρημα λέμε ότι είναι αποδεκτό, αν τόσο η υπόθεση όσο και το συμπέρασμά του επιδέχονται «πολυωνυμική μετάφραση».
3. Οποιοδήποτε αποδεκτό θεώρημα επιδέχεται πολλές «πολυωνυμικές μεταφράσεις» με την έννοια ότι υπάρχουν διάφορες ισοδύναμες τυποποιήσεις του.

Ας ξεκινήσουμε με μια απλή γεωμετρική πρόταση που αναφέρεται στις ιδιότητες του παραλληλογράμμου.

Θεωρούμε ότι Α, Β, Γ, Δ είναι οι κορυφές ενός παραλληλογράμμου και θα αναφερθούμε στο θεώρημα που δηλώνει ότι οι διαγώνιες του ΑΔ και ΒΓ διχοτομούνται.



Η προσπάθειά μας είναι να εκφράσουμε τόσο τις υποθέσεις του θεωρήματος (ότι τα σημεία Α, Β, Γ, Δ είναι κορυφές παραλληλογράμμου και το Ν το σημείο τομής των διαγωνίων του) όσο και το συμπέρασμα (ότι το Ν είναι το μέσο των Δ και ΒΓ) με τη μορφή πολυωνυμικών εξισώσεων.

Επειδή η μεταφορά και η στροφή στο επίπεδο δεν αλλοιώνουν τις ιδιότητες του παραλληλογράμμου, μπορούμε να θεωρήσουμε ότι μέσα από αυτούς τους μετασχηματισμούς έχουμε τοποθετήσει το παραλληλόγραμμο ώστε το Α να είναι στην αρχή Ο και η Β στον οριζόντιο άξονα ενός συστήματος συντεταγμένων, οπότε $A(0, 0)$ και $B(u_1, 0)$ για κάποιο $u_1 \neq 0$. Επίσης θεωρούμε ότι η κορυφή Γ του παραλληλογράμμου είναι το σημείο $Γ(u_2, u_3)$ με $u_2, u_3 \in \mathbb{R}$ και $u_3 \neq 0$. Είναι φανερό ότι οι αριθμοί u_1, u_2, u_3 μπορούν να λάβουν οποιαδήποτε από τις επιτρεπόμενες τιμές. Από τη στιγμή που καθορίσουμε τα σημεία Α, Β, Γ το σημείο Δ καθορίζεται μέσω αυτών με μοναδικό τρόπο. Έτσι θεωρούμε ότι $Δ(x_1, x_2)$ όπου τα x_1, x_2 εξαρτώνται από τα u_1, u_2, u_3.

Το γεγονός ότι ΑΒ//ΓΔ εκφράζεται από την εξίσωση $x_2-u_3=0$. Επίσης η παραλληλία των διανυσμάτων $\overrightarrow{AΓ}, \overrightarrow{BΔ}$ μεταφράζεται ως

$$\begin{vmatrix} u_2 & u_3 \\ x_1-u_1 & x_2 \end{vmatrix}=0$$

που οδηγεί στην εξίσωση $(x_1-u_1)u_3-x_2u_3=0$. Έτσι το γεγονός ότι το ΑΒΔΓ είναι παραλληλόγραμμο μπορούμε να το αποδώσουμε με τις πολυωνυμικές εξισώσεις

$$f_1= x_2-u_3=0 \qquad \text{και}$$

(1)

$$f_2=(x_1-u_1)u_3-x_2u_3=0$$

Μια διαφορετική προσέγγιση των δεδομένων μέσω της θεώρησης του $\overrightarrow{\text{ΑΔ}}$ ως διανυσματικό άθροισμα των $\overrightarrow{\text{ΑΓ}}, \overrightarrow{\text{ΒΔ}}$ οδηγεί στις απλούστερες εξισώσεις

$$f_1'=x_1-u_1-u_2=0 \quad \text{και}$$

(1′)

$$f_2'=x_2-u_3=0$$

Αυτό καταδεικνύει ότι ο τρόπος μετάφρασης των δεδομένων – φυσικά και των ζητούμενων – δεν είναι μοναδικός.

Στη συνέχεια θα προσπαθήσουμε να «κατασκευάσουμε» το σημείο τομής των διαγωνίων. Αν $N(x_3, y_3)$ είναι φανερό ότι το Ν περιέχεται τόσο στο ΑΔ όσο και στο ΒΓ που σημαίνει ότι τόσο τα Α, Ν, Δ όσο και τα Β, Ν, Γ είναι συνευθειακά. Η απαίτηση αυτή μέσω της παραλληλίας των $\overrightarrow{\text{ΑΝ}}, \overrightarrow{\text{ΑΔ}}$ και $\overrightarrow{\text{ΒΝ}}, \overrightarrow{\text{ΒΓ}}$ οδηγεί στις πολυωνυμικές εξισώσεις

$$f_3=x_4x_1-x_3u_3=0 \quad \text{και}$$

(2)

$$f_4=x_4(u_2-u_1)-(x_3-u_1)\,u_3=0$$

Τα συστήματα των εξισώσεων (1) (ή (1′)) και (2) μας δίνουν μια μετάφραση των δεδομένων του θεωρήματος.

Ας δούμε τώρα πως μπορούμε να μεταφράσουμε το συμπέρασμα του. Η απαιτήσεις ΑΝ=ΝΔ και ΒΝ=ΝΓ οδηγούν στις ισότητες

$$\sqrt{x_3^2+x_4^2}=\sqrt{(x_3-x_1)^2+(x_4-x_2)^2}$$

και

$$\sqrt{(x_3-u_1)^2+x_4^2}=\sqrt{(x_3-u_2)^2+(x_4-u_3)^2}$$

οι οποίες, μετά τις απαραίτητες πράξεις και απλοποιήσεις, δίνουν τις πολυωνυμικές εξισώσεις

$$g_1=x_1^2-2x_1x_3-2x_4x_2+x_2^2=0 \quad \text{και}$$

(3)

$$g_2=2x_3u_1-2x_3u_2-2x_4u_3-u_1^2+u_2^2+u_3^2=0$$

Έτσι, η μετάφραση του θεωρήματος μας λέει ότι οι εξισώσεις της (3) ισχύουν όταν ισχύουν οι υποθέσεις που αναγράφονται στις (1) και (2).

Ας δούμε πάλι τώρα αυτά που ουσιαστικά έχουμε αναφέρει για το συγκεκριμένο θεώρημα στην μέχρι τώρα πορεία μας. Έχουμε μεταφράσει τις υποθέσεις του, ώστε αυτές να είναι ισοδύναμες με το μηδενισμό των πολυωνύμων

$f_1(x_1, x_2, u_1, u_2, u_3)$, $f_2(x_1, x_2, u_1, u_2, u_3)$, $f_3(x_1, x_2, u_1, u_2, u_3)$, $f_4(x_1, x_2, u_1, u_2, u_3)$

και το συμπέρασμά του, ώστε αυτό να είναι ισοδύναμο με το μηδενισμό των πολυωνύμων

$$g_1(x_1, x_2, u_1, u_2, u_3), g_2(x_1, x_2, u_1, u_2, u_3)$$

Αν τα πολυώνυμα g_1, g_2 ανήκουν στο ιδεώδες που παράγουν τα f_1, f_2, f_3, f_4, τότε αυτά είναι πολυωνυμικοί συνδυασμοί των στοιχείων του $\{ f_1, f_2, f_3, f_4\}$ πράγμα που σημαίνει ότι ο ταυτόχρονος μηδενισμός των f_1, f_2, f_3, f_4, συνεπάγεται και το μηδενισμό των g_1, g_2. Έτσι λοιπόν, ο υπολογιστής, στην προσπάθειά του να αποδείξει το θεώρημα, θα υπολογίσει αρχικά μια βάση Groebner του ιδεώδους $I=<f_1, f_2, f_3, f_4>$ και στη συνέχεια το υπόλοιπο της διαίρεσης των g_1 και g_2 με τη βάση αυτή. Δεδομένου ότι τα υπόλοιπα της διαίρεσης με τη βάση Groebner είναι μοναδικά, τα πολυώνυμα θα ανήκουν στο ζητούμενο ιδεώδες, αν και μόνο αν, το υπόλοιπο είναι το μηδενικό πολυώνυμο, κάτι που στην περίπτωσή μας συμβαίνει.

ΚΕΦΑΛΑΙΟ 4

4.1.i. Εμβαδόν και μέτρο

Η έννοια του μέτρου όπως αυτή αναπτύχθηκε στα τέλη του 19ου αιώνα και στις πρώτες δεκαετίες του 20ου, αποτελεί μια επέκταση της έννοιας του εμβαδού όπως την χρησιμοποίησαν οι αρχαίοι Έλληνες. Αυτοί όρισαν ως εμβαδόν ορθογωνίου το γινόμενο των διαστάσεών του και από εκεί πέρασαν στο εμβαδόν του τριγώνου και μέσω αυτού στο εμβαδόν κάθε πολυγώνου. Για το εμβαδόν του κύκλου ακολούθησαν την μέθοδο της εξάντλησης για την οποία θα μιλήσουμε στα επόμενα. Στην πραγματικότητα το ολοκλήρωμα Riemann είναι μια εφαρμογή αυτής της μεθόδου. Ποιες ιδιότητες όμως θα θέλαμε να έχει η έννοια του εμβαδού στο Ευκλείδειο επίπεδο;

Αν συμβολίσουμε με s(E) το εμβαδόν ενός χωρίου E, οι ιδιότητες που θα επιθυμούσαμε να έχει θα ήταν οι:

- $s(E)\geq 0$ (μη αρνητικές τιμές) και
- $s(E\cup F)=s(E)+s(F)$ (προσθετική), όταν τα E, F δεν έχουν κοινά εσωτερικά σημεία.

Οι ιδιότητες αυτές συνδέουν το εμβαδόν με μια γενικότερη έννοια, αυτή του μέτρου ενός συνόλου. Για το εμβαδόν θα απαιτούσαμε επίσης να παραμένει αναλλοίωτο κάτω από τους συνηθισμένους Ευκλείδειους μετασχηματισμούς (μεταφορά – στροφή - ανάκλαση). Αυτό όμως δεν είναι μια αναγκαία ιδιότητα του μέτρου μ. Επίσης, η προσθετική ιδιότητα έχει αντικατασταθεί από μια ισχυρότερη υπόθεση, αυτή της **αριθμήσιμης προσθετικότητας** που περιγράφεται από την ισότητα

$$\mu\left(\bigcup_{j=1}^{\infty} E_j\right)=\sum_{j=1}^{\infty}\mu(E_j)$$

με την προϋπόθεση ότι $E_j\cap E_k\neq\varnothing$ για οποιαδήποτε j, k με $j\neq k$.

Ας δούμε όμως την έννοια του μέτρου όταν αναφερόμαστε γενικά σε οικογένεια υποσυνόλων κάποιου συνόλου Χ.

Έστω Χ ένα σύνολο και $\mathcal{M}$ μια οικογένεια υποσυνόλων του Χ. Μια συνολοσυνάρτηση μ ορισμένη στο $\mathcal{M}$ λέμε ότι είναι ένα **μέτρο**, όταν:

- λαμβάνει μη αρνητικές τιμές και
- έχει την ιδιότητα της αριθμήσιμης προσθετικότητας.

4.1.ii. Αξιωματικός ορισμός του εμβαδού

Αν στο επίπεδο θεωρήσουμε ένα πολύγωνο, τότε αυτό, μαζί με τα εσωτερικά του σημεία, ορίζει ένα χωρίο το οποίο το ονομάζουμε **πολυγωνικό χωρίο.**

Στο σύνολο των πολυγωνικών χωρίων του επιπέδου θεωρούμε μια πραγματική συνάρτηση s, η οποία ικανοποιεί τα ακόλουθα αξιώματα:

α. Η s λαμβάνει μη αρνητικές τιμές, δηλαδή για οποιοδήποτε πολυγωνικό χωρίο F ισχύει $s(F)\geq 0$.

β. Η s είναι προσθετική, με την έννοια ότι αν F, F′ είναι δυο πολυγωνικά χωρία που δεν περιέχουν κοινό εσωτερικό σημείο, τότε

$$s(F\cup F')=s(F)+s(F').$$

γ. Αν F′ ένα πολυγωνικό χωρίο που προκύπτει από κάποιο άλλο F με μεταφορά, τότε $s(F)=s(F')$, δηλαδή η τιμή της συνάρτησης s δεν μεταβάλλεται κατά τη μεταφορά του πολυγώνου.

δ. Αν Q είναι το μοναδιαίο τετράγωνο, τότε $s(Q)=1$.

Τη συνάρτηση s, η οποία προφανώς είναι ένα μέτρο στο Ευκλείδειο επίπεδο, τη λέμε **εμβαδόν** και την τιμή της s(F), όπου F τυχαίο πολυγωνικό χωρίο, εμβαδόν του πολυγωνικού χωρίου ή **εμβαδόν του πολυγώνου F**.

Αποδεικνύεται ότι:

i) Μια τέτοια συνάρτηση υπάρχει και είναι μοναδική.

ii) Τα παραπάνω αξιώματα είναι ανεξάρτητα (§ 1. 2.ν) με την έννοια ότι κανένα από αυτά δεν αποδεικνύεται με τη βοήθεια των άλλων.

iii) Αν δυο πολυγωνικά χωρία είναι ίσα, τότε έχουν και ίσα εμβαδά, είναι όπως λέμε **ισεμβαδικά ή ισοδύναμα**. Το αντίστροφο δεν ισχύει.

Με τη βοήθεια των παραπάνω αξιωμάτων μπορούμε να αποδείξουμε κάποιες ιδιότητες του εμβαδού, εκ των οποίων δυο, έχουν ομοιότητα με τα αξιώματα (α) και (γ) και μπορούν να τα αντικαταστήσουν σε μια διαφορετική προσέγγιση της έννοιας του εμβαδού. Αν συμβολίσουμε αυτές με ($α^*$) και ($γ^*$) έχουμε:

α*. Αν για δυο πολύγωνα F, H ισχύει $F \subset H$, τότε $s(F) \leq s(H)$.

$γ^*$. Το εμβαδόν παραμένει αναλλοίωτο στις συνήθεις κινήσεις (μεταφορά – στροφή). Το ($γ^*$) είναι ισχυρότερο του (γ).

Στην περίπτωση που θέλουμε να υπολογίσουμε το εμβαδόν χωρίου το οποίο δεν είναι κατ' ανάγκη πολυγωνικό, τότε από το αξίωμα (α) ή το ισοδύναμό του ($α^*$), μπορούμε, με κατάλληλες επαναληπτικές διαδικασίες, να δημιουργήσουμε ανισοτικές σχέσεις οι οποίες μας παρέχουν εκτιμήσεις για το εμβαδόν του χωρίου. Από αυτές τις εκτιμήσεις μέσα από τη διαδικασία του ορίου, περνάμε σε ισότητες που μας δίνουν το εμβαδόν του συγκεκριμένου χωρίου. Τέτοιες ανισότητες χρησιμοποιούμε κατά την εφαρμογή της μεθόδου της εξάντλησης

- είτε στον υπολογισμό εμβαδού κύκλου,
- είτε για να υπολογίσουμε το εμβαδόν του χωρίου που ορίζεται από τον άξονα x'x τις ευθείες x=α, x=β και τη γραφική παράσταση μιας συνεχούς συνάρτησης που λαμβάνει μη αρνητικές τιμές στο διάστημα [α, β].

Η μέθοδος αυτή χρησιμοποιεί την έννοια του ορίου και τη χρήση τεχνικών που συνδέονται με τον (εψιλοντικό) ορισμό του και φυσικά δεν μπορεί να θεωρηθεί ως στοιχειώδης.

Ως στοιχειώδη θεωρούμε κάθε μέθοδο που στηρίζεται στα αξιώματα (β), (γ) ή (γ^*) και (δ) χωρίς να κάνει χρήση του αξιώματος της επιλογής που σχετίζεται με προτάσεις που αναφέρονται σε απειροσύνολα. Μια τέτοια είναι η μέθοδος της διαμέρισης που στηρίζεται στα αξιώματα (β) και (γ^*).

4.1.iii. Η μέθοδος της διαμέρισης

Η βασική ιδέα της μεθόδου είναι η ανάλυση (διαμέριση) ενός πολυγώνου F σε πεπερασμένο πλήθος τριγώνων, ώστε αυτά, κατάλληλα συναρμοζόμενα, να δίνουν ένα πολύγωνο G του οποίου μπορούμε να υπολογίσουμε το εμβαδόν.

Έστω F, G δυο πολύγωνα. Λέμε ότι τα F, G είναι **ισοδιαμερίσιμα** και συμβολίζουμε $F \sim G$ όταν είναι δυνατόν να τα διαμερίσουμε σε πεπερασμένο πλήθος τριγώνων τα οποία είναι, ανά ζεύγη, ίσα μεταξύ τους. Αυτό σημαίνει ότι υπάρχουν τρίγωνα $F_1, F_2, \ldots, F_\kappa$ και $G_1, G_2, \ldots, G_\kappa$ ώστε να ισχύουν

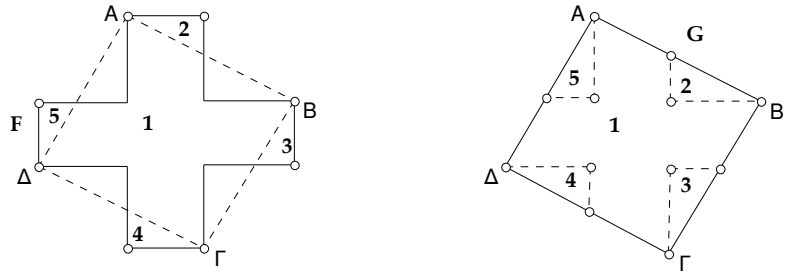
$$F=F_1+F_2+\ldots+F_K\ ,\ G=G_1+G_2+\ldots+G_\kappa \text{ και}$$

$$F_1=G_1,\ F_2=G_2,\ \ldots,\ F_\kappa=G_\kappa$$

Από τα αξιώματα (β) και (γ^*) προκύπτει άμεσα ότι:

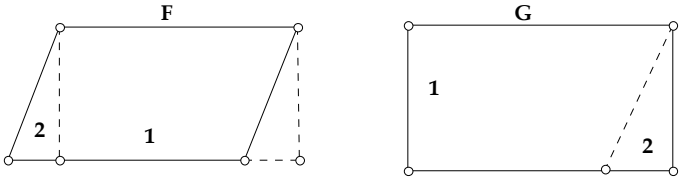
Αν $F \sim G$, τότε s(F)=s(G) δηλ. αν δυο πολύγωνα είναι ισοδιαμερίσιμα, τότε έχουν και ίσα εμβαδά.

Στο παρακάτω σχήμα το πολυγωνικό χωρίο (σταυρός) F και το τετράγωνο G είναι ισοδιαμερίσιμα, καθότι το τμήμα (1) που είναι κοινό μπορούμε εύκολα να το χωρίσουμε σε τρίγωνα, ενώ για τα υπολειπόμενα τρίγωνα του πολυγωνικού χωρίου F η αντιστοίχισή τους με αυτά του G είναι προφανής.

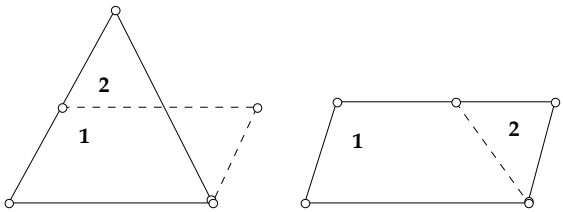


Παραδείγματα

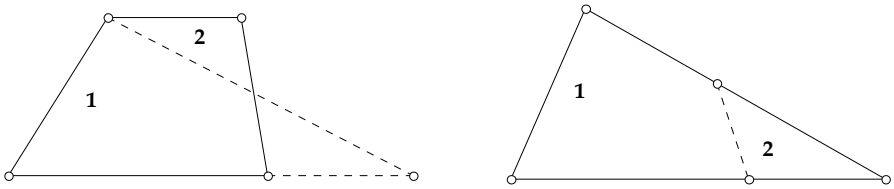
1. Ένα παραλληλόγραμμο F είναι ισοδιαμερίσιμο, κατά συνέπεια και ισεμβαδικό, με ορθογώνιο G της ίδιας βάσης και του αυτού ύψους. Αυτό σημαίνει ότι αν θεωρήσουμε γνωστό τον τύπο που μας δίνει το εμβαδόν ορθογωνίου, εύκολα μπορούμε να οδηγηθούμε στον τύπο για το εμβαδόν παραλληλογράμμου.



2. Ένα τρίγωνο είναι ισοδιαμερίσιμο με παραλληλόγραμμο το οποίο έχει την ίδια βάση με αυτό και το μισό ύψος (μας παρέχει τύπο για το εμβαδόν τριγώνου).



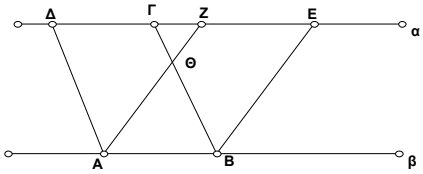
2. Ένα τραπέζιο είναι ισοδιαμερίσιμο με τρίγωνο ίδιου ύψους και βάση ίση με το άθροισμα των βάσεων (εμβαδόν τραπεζίου).



Η μέθοδος αυτή ήταν γνωστή και κατά την αρχαιότητα. Για παράδειγμα ο Ευκλείδης στην πρόταση Ι. 35 των Στοιχείων αναφέρει:

Τα παραλληλόγραμμα τα επί της αυτής βάσεως όντα και εν ταις αυταίς παραλλήλοις ίσα αλλήλοις εστίν.

(Τα παραλληλόγραμμα που έχουν την ίδια βάση και βρίσκονται μεταξύ παραλλήλων είναι ισεμβαδικά).



Στην απόδειξή του αποκολλάει από τα δυο ίσα τρίγωνα ΑΔΖ και ΒΓΕ το τρίγωνο ΘΓΖ και κατόπιν επικολλάει στα υπολειπόμενα μέρη το τρίγωνο ΑΒΘ οπότε προκύπτει ότι τα ΑΒΓΔ και ΑΒΕΖ είναι ισεμβαδικά.

Ο Πρόκλος στο χωρίο [394,8 - 395,21] σχολιάζει την πρόταση αυτή επικροτώντας την άποψη ότι αντιβαίνει στη διαίσθηση («παράδοξη πρόταση») κατά την οποία η περίμετρος σχετίζεται με το εμβαδόν. Μια τέτοια συσχέτιση θα είχε ως συνέπεια, όταν αυξάνεται η περίμετρος (κάτι που συμβαίνει όταν τα Ε, Ζ ληφθούν ώστε τα ΑΖ και ΒΕ να είναι εμφανώς μεγαλύτερα των ΑΔ και ΒΓ αντίστοιχα) να αυξάνεται και το εμβαδόν.

Από τη στιγμή που βρίσκουμε τον τύπο για το εμβαδόν τριγώνου, μπορούμε να υπολογίσουμε το εμβαδόν κάθε πολυγώνου ως εξής:

- χωρίζουμε το πολύγωνο σε τρίγωνα τα οποία ανά δυο δεν έχουν κοινό εσωτερικό σημείο και
- αθροίζουμε κατά το αξίωμα (β), τα εμβαδά των τριγώνων αυτών.

Παρότι η ανάλυση σε τρίγωνα δεν είναι μοναδική, αποδεικνύεται ότι το άθροισμα των επί μέρους εμβαδών, που είναι το εμβαδόν του πολυγώνου, είναι σταθερό.

4.1.iv. Η μέθοδος του συμπληρώματος

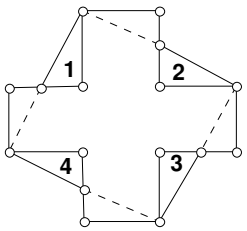
Μια άλλη μέθοδος υπολογισμού εμβαδού είναι αυτή του συμπληρώματος. Αυτή συνίσταται στην επισύναψη ίσων σχημάτων σε δυο αρχικά, ώστε τα σχήματα που προκύπτουν να είναι ίσα.

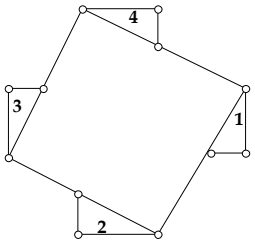
Δυο πολύγωνα F, G λέγονται **ισοσυμπληρώσιμα**, αν μπορούμε να επισυνάψουμε σ' αυτά πεπερασμένο πλήθος ισοδιαμερίσιμων πολυγώνων F_i, G_i αντίστοιχα ώστε

$$F+F_1+F_2+\ldots+F_\kappa = G+G_1+G_2+\ldots+G_\kappa$$

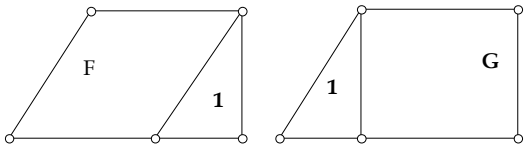
Τα ισοσυμπληρώσιμα πολύγωνα έχουν ίσα εμβαδά.

Στα παρακάτω σχήματα, ο σταυρός (F) και το τετράγωνο (G) είναι ισοσυμπληρώσιμα, καθότι αν προσθέσουμε τόσο στο F όσο και στο G τέσσερα ίσα τρίγωνα, προκύπτουν σχήματα ισεμβαδικά οπότε τα F, G είναι ισεμβαδικά.





Στο επόμενο σχήμα φαίνεται πως η επισύναψη ενός ορθογωνίου τριγώνου σε πλάγιο παραλληλόγραμμο και ορθογώνιο τα οποία έχουν ίσες βάσεις και ίσα ύψη, μας οδηγεί σε ισοδύναμα τραπέζια απ' όπου προκύπτει, ότι ένα παραλληλόγραμμο F είναι ισεμβαδικό με ορθογώνιο G της ίδιας βάσης και του αυτού ύψους.



Εύκολα μπορούμε να διαπιστώσουμε ότι:

- Δυο παραλληλόγραμμα με ίσες βάσεις και ίσα ύψη, είναι μεταξύ τους ισοσυμπληρώσιμα.
- Δυο τρίγωνα με ίσες βάσεις και ίσα ύψη είναι μεταξύ τους ισοσυμπληρώσιμα.

4.1.ν. Το Πυθαγόρειο θεώρημα

Αν και η παράδοση έχει αποδώσει το θεώρημα στον Πυθαγόρα, πήλινοι πίνακες με σφηνοειδή γραφή που βρέθηκαν στην Μεσοποταμία τον περασμένο αιώνα αποκαλύπτουν ότι οι αρχαίοι Βαβυλώνιοι, περίπου 1000 χρόνια πριν τον Πυθαγόρα, γνώριζαν το θεώρημα. Το ίδιο θεώρημα γνώριζαν επίσης τόσο οι Κινέζοι, όσο και οι Ινδοί της εποχής του Πυθαγόρα ή λίγο πιο πριν.

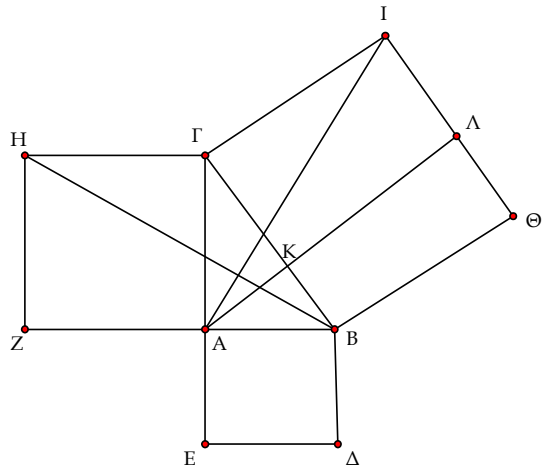
> Ο Πρόκλος [426, 1 – 429, 16] αναφέρει γενικώς ότι οι «Αρχαίοι λένε» ότι το Πυθαγόρειο θεώρημα οφείλεται στους Πυθαγόρειους. Μάλλον πρόκειται για ασθενή αναφορά αν τη συγκρίνουμε με άλλες, όπως για παράδειγμα για την Πυθαγόρεια προέλευση των όρων παραβολή, έλλειψη, υπερβολή όπου αποδίδει αυτά στους «περί τον Εύδημον». Πάντως θεωρεί την απόδειξη των Στοιχείων (Πρόταση Ι. 47) ρητά Ευκλείδεια και θαυμάζει τον Ευκλείδη γι' αυτή.

Η απόδειξη του Ευκλείδη φαίνεται στο παρακάτω σχήμα όπου από την προφανή ισότητα των τριγώνων ΓΒΗ και ΓΑΙ προκύπτει ότι και ΑΓΗΖ και ΚΛΙΓ είναι ισεμβαδικά, καθότι το καθένα εξ αυτών έχει εμβαδόν διπλάσιο από το εμβαδόν των ίσων τριγώνων. Με ανάλογο συλλογισμό προκύπτει ότι και τα ΑΕΔΒ και ΒΘΛΚ είναι ισεμβαδικά. Έτσι, αν χρησιμοποιήσουμε

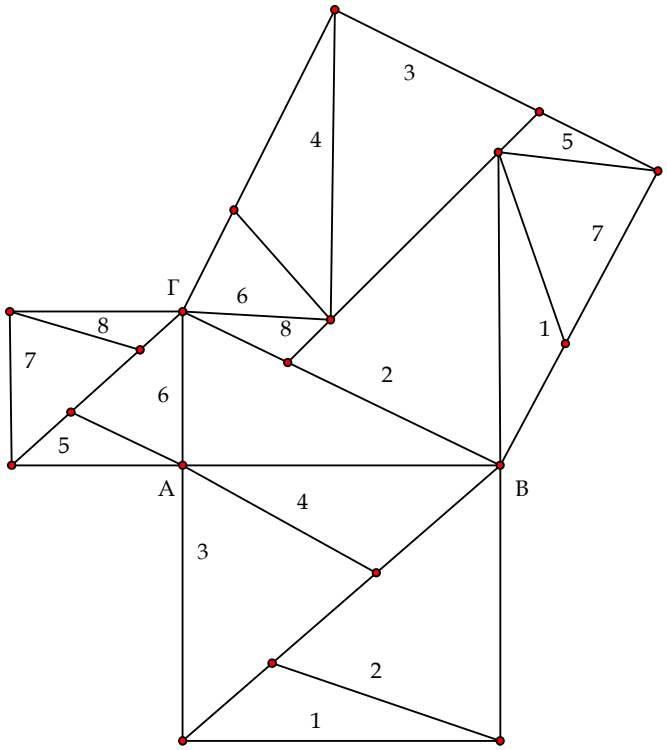
σύγχρονο συμβολισμό για το εμβαδόν, έχουμε:

$$(ΑΒΔΕ)+(ΑΓΗΖ)=(ΒΘΛΚ)+(ΚΛΙΓ)=(ΒΘΙΓ),$$

οπότε $ΑΒ^2+ΑΓ^2=ΒΓ^2$.



Στο επόμενο σχήμα βλέπουμε μια «απόδειξη διαμέρισης» του ίδιου θεωρήματος.



4.2. Το τρίτο πρόβλημα Hilbert

4.2.i Το πρόβλημα

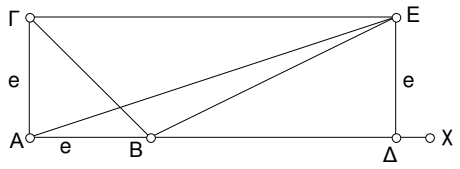
Είδαμε ότι όταν δυο πολύγωνα είναι είτε ισοδιαμερίσιμα, είτε ισοσυμπληρώσιμα, τότε είναι ισεμβαδικά.

Ο Ούγγρος μαθηματικός **F. Bolyai (1832) –** και ο Γερμανός **Gerwien (1833)** απέδειξαν ότι ισχύει και το αντίστροφο: **Αν δυο πολύγωνα είναι ισεμβαδικά, τότε είναι και ισοσυμπληρώσιμα.** Αποδεικνύεται επίσης ότι αν δυο πολύγωνα είναι ισοδιαμερίσιμα, τότε είναι και ισοσυμπληρώσιμα.

Ως συμπέρασμα από όσα έχουμε εκθέσει προηγουμένως, προκύπτει ότι η ισότητα εμβαδών, η ισοδιαμερισιμότητα και η ισοσυμπληρωσιμότητα είναι ισοδύναμες ιδιότητες στα πολύγωνα, όταν τουλάχιστον αναφερόμαστε στο Ευκλείδειο επίπεδο. Αυτό δεν συμβαίνει αν το πλαίσιο αναφοράς μας είναι για παράδειγμα μη Αρχιμήδειες Γεωμετρίες, δηλαδή Γεωμετρίες στις οποίες

έχουμε υποθέσει ότι δεν ισχύει το Αρχιμήδειο αξίωμα. Σε μια τέτοια Γεωμετρία, όπως έδειξε ο Hilbert στα «Θεμέλια της Γεωμετρίας», μπορούμε να κατασκευάσουμε ισοσυμπληρώσιμα τρίγωνα τα οποία δεν είναι ισοδιαμερίσιμα.

Πράγματι, στα πλαίσια μιας μη Αρχιμήδειας Γεωμετρίας θεωρούμε μια ημιευθεία Ax και πάνω σ' αυτή δυο τμήματα ΑΒ = e και ΑΔ = α τα οποία δεν εκπληρώνουν τη σχέση ne ≥ α για κανένα θετικό ακέραιο n. Έστω επίσης ΑΓ και ΔΕ τα κάθετα τμήματα προς την Ax το καθένα από τα οποία είναι ίσο με e. Τότε τα τρίγωνα ΑΒΓ



και ΑΒΕ, ως έχοντα ίδια βάση και ίσα ύψη, είναι ισοσυμπληρώσιμα. Επιπλέον από την ΒΓ<e+e=2e και δεδομένου ότι κάθε ευθύγραμμο τμήμα που βρίσκεται στο εσωτερικό ενός τριγώνου είναι μικρότερο από την μεγαλύτερη πλευρά του, συνάγουμε ότι κάθε τμήμα που βρίσκεται εξ ολοκλήρου στο εσωτερικό του ΑΒΓ είναι μικρότερο από 2e.

Υποθέτουμε ότι έχει γίνει μια διαμέριση των τριγώνων ΑΒΓ και ΑΒΕ σε ένα πεπερασμένο πλήθος κ, κατά ζεύγη ίσων, τριγώνων. Κάθε πλευρά ενός τέτοιου τριγώνου είτε βρίσκεται εξ ολοκλήρου στο εσωτερικό του είτε βρίσκεται πάνω σε κάποια πλευρά του ΑΒΓ, είναι μικρότερη από 2e. Έτσι η περίμετρος ενός τέτοιου τριγώνου θα είναι μικρότερη από 6e, οπότε αν θεωρήσουμε το συνολικό άθροισμα s των περιμέτρων όλων των τριγώνων, θα ισχύει s<6κε. Ο τρόπος διαμέρισης επιβάλλει να συμβαίνει το ίδιο και για τα αντίστοιχα μερικά τρίγωνα του ΑΒΕ. Σ' αυτό το άθροισμα όμως περιλαμβάνεται εξ ολοκλήρου και η πλευρά ΑΕ του τριγώνου οπότε ΑΕ<6κe και κατά μείζονα λόγο

$$\alpha<6\kappa e \Rightarrow ne>\alpha \text{ με } n = 6\kappa,$$

το οποίο όμως είναι άτοπο.

Επομένως τα τρίγωνα ΑΒΓ και ΑΒΕ δεν είναι ισοδιαμερίσιμα.

Στο Ευκλείδειο επίπεδο λοιπόν, γνωρίζοντας τον τύπο του εμβαδού ορθογωνίου και χρησιμοποιώντας είτε τη μέθοδο της διαμέρισης είτε αυτή του συμπληρώματος, μπορούμε να υπολογίσουμε το εμβαδόν ενός πολυγώνου.

Το ερώτημα που εγείρεται είναι αν μπορούμε να κάνουμε κάτι ανάλογο και στο χώρο, δηλαδή αν μπορούμε να αποδείξουμε ότι δυο ισοδιαμερίσιμα πολύεδρα έχουν ίσους όγκους, οπότε χρησιμοποιώντας τον τύπο για τον όγκο ορθογωνίου παραλληλεπιπέδου και κάποια από τις στοιχειώδεις μεθόδους, να υπολογίσουμε τον όγκο συνηθισμένων πολυέδρων. Αυτό το πρόβλημα είναι γνωστό ως **τρίτο πρόβλημα Hilbert** το οποίο, στη μορφή που θα διαπραγματευθούμε εδώ, αναφέρεται στο κανονικό τετράεδρο. Συγκεκριμένα θα ασχοληθούμε με το ακόλουθο πρόβλημα:

Είναι δυνατόν να διαμερίσουμε, με τη βοήθεια επιπέδων, ένα κανονικό τετράεδρο σε πεπερασμένα μέρη τα οποία αν επικολληθούν κατάλληλα να μας δώσουν κύβο;

Το πρόβλημα, όπως έχουμε ήδη αναφέρει, περιελήφθη από τον Hilbert ως τρίτο μέσα στη λίστα των 23 προβλημάτων που έθεσε στο συνέδριο το 1900 ως πρόκληση για τους μαθηματικούς του 20ου αιώνα.

Το πρόβλημα αυτό πριν τεθεί από τον Hilbert είχε την ιστορία του. Ήδη από το 1844 οι F. Bolyai και Gauss, είχαν θέσει το ίδιο ερώτημα. Ο R. Bricard σε άρθρο του το 1896 παρουσίασε μια απλή λύση του προβλήματος, βασιζόμενος στο ακόλουθο θεώρημα (υπόθεση Bricard):
Αν δυο πολύεδρα S, P είναι ισοδιαμερίσιμα, τότε υπάρχουν θετικοί ακέραιοι n_i και n_j' ώστε

$$n_1\alpha_1 + n_2\alpha_2 + \ldots + n_q\alpha_q = n_1\beta_1 + n_2\beta_2 + \ldots + n_r\beta_r + p\pi$$

όπου $\alpha_1, \alpha_2, \ldots, \alpha_q$ οι δίεδρες γωνίες του πολυέδρου S, $\beta_1, \beta_2, \ldots, \beta_r$ οι δίεδρες του P και p ακέραιος. Αυτή παρέχει άμεση λύση του προβλήματος, καθότι στην περίπτωση του τετραέδρου και του κύβου

οδηγεί στην ισότητα $m\alpha=n\cdot\frac{\pi}{2}$ η οποία δεν μπορεί να ισχύει, καθότι μπορούμε να αποδείξουμε ότι ο αριθμός $\frac{\alpha}{\pi}$ είναι άρρητος.

Γρήγορα όμως διαπιστώθηκε ότι στην απόδειξη που είχε παρουσιάσει υπήρχε ένα κενό. Παρόλο που η απόδειξη της συνθήκης του δεν ήταν ορθή, εντούτοις αυτή ήταν μια αληθής μαθηματική πρόταση. Οι προσπάθειες διόρθωσης της απόδειξης που κατά καιρούς παρουσιάσθηκαν, εμφάνιζαν τη συνθήκη ως συνέπεια της λύσης του τρίτου προβλήματος. Στην ιδέα του Bricard βασίστηκε και η λύση που παρουσιάζουμε στα επόμενα. Τον ίδιο χρόνο, ο Άγγλος μαθηματικός Hill παρουσίασε τετράεδρα (τετράεδρα του Hill) που είναι ισοδιαμερίσιμα με κύβο. Βέβαια, αυτό αφορά μια ειδική περίπτωση και η αναμενόμενη εκ μέρους του Hilbert αρνητική απάντηση φαίνεται να είναι και ο λόγος που, λίγα χρόνια μετά, το συμπεριέλαβε στη λίστα των 23 προβλημάτων. Το 2007 ο David Benko παρουσίασε μια απόδειξη της βελτιωμένης όπως την αποκάλεσε συνθήκης του Bricard χρησιμοποιώντας ένα μαθηματικό πολυεργαλείο, τη γνωστή αρχή της περιστεροφωλιάς.

Λίγους μήνες αργότερα ο 23χρονος γεωμέτρης Dehn Max, φοιτητής του Hilbert, έλυσε το πρόβλημα δίνοντας αρνητική απάντηση στο συγκεκριμένο ερώτημα. Ο Dehn εστίασε στις δίεδρες γωνίες του πολυέδρου και χρησιμοποίησε μια απλή μέθοδο. Αν θεωρήσουμε ότι μπορούμε να διαμερίσουμε το τετράεδρο και κατόπιν με κατάλληλη επικόλληση δημιουργήσουμε κύβο, τότε διαισθητικά είναι σαν να έχουμε καταφέρει να σχηματίσουμε τις ορθές (δίεδρες) γωνίες του κύβου από τις δίεδρες γωνίες του τετραέδρου. Βέβαια, στην πραγματικότητα τα πράγματα δεν είναι τόσο απλά διότι κάποιες τέτοιες επικολλήσεις θα λάβουν χώρα στο εσωτερικό του κύβου, όπου κατά κάποιο τρόπο μπορούμε να υποθέσουμε ότι (με το σχηματισμό πλήρους δίεδρης γωνίας) έχουμε απαλοιφή αυτών των γωνιών.

4.2.ii. Η αναλλοίωτη του Dehn

Είναι φανερό ότι κόβοντας και επανασυναρμολογώντας ένα πολύεδρο, ο όγκος του παραμένει σταθερός. Πέρα όμως από τον όγκο, ο Dehn απέδειξε, ότι υπάρχει και άλλο μέγεθος το οποίο έχει την ιδιότητα της διατηρησιμότητας. Το μέγεθος αυτό, το οποίο θα μπορούσαμε να το αποκαλέσουμε **διεδρικό περιεχόμενο**, συνδέει τις δίεδρες γωνίες με τις ακμές τους. Το διεδρικό περιεχόμενο που ορίζεται (κατασκευάζεται) από μια δίεδρη γωνία α και μια ακμή μήκους ℓ το συμβολίζουμε με $\ell \otimes \alpha$.

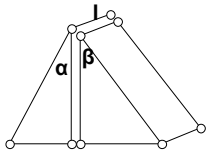
Το ολικό διεδρικό περιεχόμενο D(S) ενός πολυέδρου ή ενός πεπερασμένου συνόλου S από πολύεδρα γράφεται

$$D(S)=\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa$$

όπου $\ell_1, \ell_2, \ldots, \ell_\kappa$ είναι τα μήκη των ακμών του που αντιστοιχούν στις δίεδρες γωνίες $\alpha_1, \alpha_2, \ldots, \alpha_\kappa$. Η πρόσθεση εδώ, προφανώς λειτουργεί αντιμεταθετικά και προσεταιριστικά καθότι ο τρόπος ομαδοποίησης και διάταξης των όρων του $\ell \otimes \alpha$ δεν επηρεάζει το τελικό αποτέλεσμα, οπότε μπορούμε να τη σχετίζουμε με τη συνηθισμένη πρόσθεση.

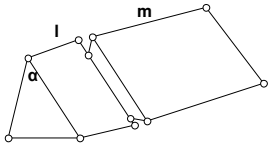
Για συγκεκριμένο πολύεδρο το D(S) είναι μια έκφραση που περιέχει κάποιες πληροφορίες σχετικά με αυτό. Προκειμένου όμως να την χρησιμοποιήσουμε για να περιγράψουμε διάφορα σύνολα $S_1, S_2, \ldots, S_\kappa$ που προκύπτουν από τεμαχισμό και επικόλληση του S, χρειαζόμαστε κάποιους κανόνες οι οποίοι θα μετασχηματίζουν το D(S) σε $D(S_1)$, $D(S_2)$,… και αντίστροφα. Ως τέτοιους θα μπορούσαμε να εκλάβουμε τους ακόλουθους:

- $\ell \otimes (\alpha + \beta) = \ell \otimes \alpha + \ell \otimes \beta$ (κ_1)
- $(\ell + m) \otimes \alpha = \ell \otimes \alpha + m \otimes \alpha$ (κ_2)
- $\ell \otimes \pi = 0$ (κ_3)

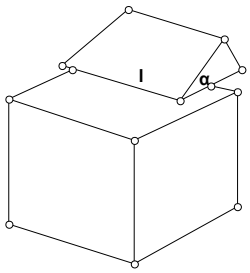


Ο πρώτος κανόνας (κ_1) καταδεικνύει τι συμβαίνει όταν η τομή γίνει κατά μήκος μιας ακμής χωρίζοντας τη δίεδρη γωνία α+β σε δύο άλλες με μέτρα α, β. Συνεπώς, μας λέει

επίσης τι συμβαίνει όταν δύο δίεδρες γωνίες συγκολληθούν σε μια.



Ο δεύτερος κανόνας (κ_2) καταδεικνύει τι συμβαίνει όταν η τομή είναι εγκάρσια σε μια ακμή μήκους $\ell+m$ διαχωρίζοντας την σε δυο άλλες με μήκη ℓ, m. Συνεπώς, μας λέει επίσης τι συμβαίνει όταν συνδέσουμε διαδοχικά δυο δίεδρες.



Ο τρίτος κανόνας (κ_3) μας λέει ότι μια δίεδρη γωνία μέτρου π μπορεί να παραληφθεί καθότι δεν πρόκειται για πραγματική γωνία. Έτσι για παράδειγμα $\ell \otimes (\pi + \alpha) = \ell \otimes \alpha$.

Στα παραπάνω σχήματα για λόγους απλούστευσης έχουμε υποθέσει ότι η ακμή ℓ είναι κάθετη στην έδρα που βρίσκεται στα άκρα της ώστε να έχουμε μια οπτική εικόνα της δίεδρης. Ακόμα όμως και όταν δεν έχουμε οπτική εικόνα της γωνίας, οι κανόνες (κ_1), (κ_2) και (κ_3) εκφράζουν τι πραγματικά συμβαίνει σ' αυτήν κατά τη διαδικασία της τομής και της επικόλλησης.

Οι κανόνες (κ_1) και (κ_2) είναι τόσο συνηθισμένοι ώστε όταν κάποιο σύστημα τους ικανοποιεί, να αναφέρεται ως **τανυστικό γινόμενο**. Για το λόγο αυτό, ο τρίτος κανόνας (κ_3) θα πρέπει να θεωρηθεί μάλλον ως ιδιότητα του συνόλου των δίεδρων γωνιών παρά ως ιδιότητα του τελεστή $\otimes$. Το σύνολο αυτό, λέγεται σύνολο πηλίκο του $\mathbb{R}$ ως προς $\pi\mathbb{Z}$, συμβολίζεται με $\mathbb{R}/\pi\mathbb{Z}$, και μιλώντας απλοϊκά είναι αυτό που προκύπτει από το $\mathbb{R}$, αν θεωρήσουμε ότι π=0 (τα πολλαπλάσια του π έχουν «απορροφηθεί» από το μηδέν). Τα στοιχεία του είναι σύνολα της μορφής

$$\{\ldots, \alpha-2\pi, \alpha-\pi, \alpha, \alpha+\pi, \alpha+2\pi, \ldots\}$$

για οποιοδήποτε πραγματικό αριθμό α.

Είναι κάτι αντίστοιχο με το σύνολο των γωνιών του επιπέδου, οι οποίες στην πραγματικότητα είναι στοιχεία του συνόλου $\mathbb{R}/2\pi\mathbb{Z}$. Στο σύνολο αυτό όλα τα πολλαπλάσια της γωνίας 2π εκλαμβάνονται ως μηδέν, ενώ στην

αναλλοίωτη του Dehn αυτό που εκλαμβάνεται ως μηδέν είναι το π, διότι μια δίεδρη γωνία π, στην πραγματικότητα δεν είναι γωνία.

Τα αντικείμενα $\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa$ που προκύπτουν ως τιμές της αναλλοίωτης Dehn ονομάζονται **τανυστές**. Το σύνολο τους ονομάζεται τανυστικό γινόμενο των $\mathbb{R}$ και $\mathbb{R}/\pi\mathbb{Z}$ και συμβολίζεται με $\mathbb{R} \otimes \mathbb{R}/\pi\mathbb{Z}$. Εδώ δεν θα ασχοληθούμε ιδιαίτερα με τανυστές, καθότι οι δυο πρώτοι κανόνες που αναφέραμε επαρκούν να αποδείξουμε αυτά τα οποία μας είναι απαραίτητα.

Παρατήρηση

Από τους παραπάνω κανόνες προκύπτει ότι $\ell \otimes 0 = 0$. Πράγματι, διότι $\ell \otimes \alpha = \ell \otimes (\alpha + 0) = \ell \otimes \alpha + \ell \otimes 0$, οπότε $\ell \otimes 0 = 0$.

Ομοίως μπορούμε να αποδείξουμε ότι $0 \otimes \alpha = 0$

Το D(S), το οποίο υπόκειται σ' αυτούς τους κανόνες, από τον ορισμό του παραμένει το ίδιο όταν στο S εφαρμοστεί η διαδικασία τομής και επικόλλησης, ονομάζεται **αναλλοίωτη του Dehn**.

Παράδειγμα

Η αναλλοίωτη του Dehn στο μοναδιαίο κύβο είναι μηδέν. Πράγματι, διότι στην περίπτωση αυτή έχουμε: $D(S) = 12 \otimes \frac{\pi}{2} = 0$, καθότι

$$2 \otimes \frac{\pi}{2} = 1 \otimes \frac{\pi}{2} + 1 \otimes \frac{\pi}{2} = 1 \otimes (\frac{\pi}{2} + \frac{\pi}{2}) = 1 \otimes \pi = 0.$$

Παρατήρηση

Είναι φανερό ότι η παραπάνω ιδιότητα ισχύει σε οποιοδήποτε κύβο.

Αποδεικνύεται ότι:

Αν P, Q είναι δυο ισοδιαμερίσιμα πολύεδρα, τότε D(P)=D(Q).

Παρατήρηση

Από τα προαναφερθέντα προκύπτει ότι αν για δυο πολύεδρα P, Q ισχύει $D(P) \neq D(Q)$, τότε δεν είναι ισοδιαμερίσιμα, οπότε λογικό είναι να εστιάσουμε

την προσοχή μας στην απόδειξη της σχέσης $D(S')\neq 0$, όπου S′ είναι ένα κανονικό τετράεδρο με ακμή 1.

4.2.iii. Προσθετικές συναρτήσεις

Το πιο οικείο μαθηματικό αντικείμενο που μπορούμε να βρούμε στην Άλγεβρα ή την Ανάλυση, ώστε να προσομοιάζει με την έκφραση (τανυστή)

$$\ell_1\otimes\alpha_1+\ell_2\otimes\alpha_2+\ldots+\ell_\kappa\otimes\alpha_\kappa$$

είναι το άθροισμα

$$\ell_1 f(\alpha_1)+\ell_2 f(\alpha_2)+\ldots+\ell_\kappa f(\alpha_\kappa),$$

όπου f συνάρτηση η οποία έχει τις ιδιότητες

- $\ell f(\alpha+\beta)=\ell f(\alpha)+\ell f(\beta)$
- $(\ell+m)f(\alpha)=\ell f(\alpha)+mf(\alpha)$
- $f(\pi)=0$

κατ′ αντιστοιχία με τους κανόνες (κ_1), (κ_2) και (κ_3) για τους τανυστές.

Φυσικά ο δεύτερος από αυτούς τους κανόνες ισχύει για οποιαδήποτε πραγματική συνάρτηση (επιμεριστική ιδιότητα) οπότε στην πραγματικότητα, η συνάρτηση f είναι εκείνη η οποία ικανοποιεί την προσθετική ιδιότητα $f(x+y)=f(x)+f(y)$ και επιπλέον $f(\pi)=0$.

Θα αποδείξουμε ότι το ακόλουθο θεώρημα:

Η μοναδική συνεχής συνάρτηση f: $\mathbb{R}\to\mathbb{R}$ που ικανοποιεί την προσθετική ιδιότητα και επιπλέον $f(\pi)=0$, είναι η $f(x)=0$ (μηδενική συνάρτηση).

Απόδειξη

Από την ισότητα $f(x+y)=f(x)+f(y)$ που ισχύει για όλα τα $x,y\in\mathbb{R}$ προκύπτουν τα ακόλουθα.

Με $x=y=0$

$$f(0)=2f(0)\Rightarrow f(0)=0$$

Με $y=-x$

$$f(x+(-x))=f(x)+f(-x)\Rightarrow f(x)+f(-x)=0\Rightarrow f(-x)=-f(x) \qquad \textbf{(1)}$$

Έστω $n\in\mathbb{N}^*$. Είναι:

$$f(nx)=f[x+(n-1)x]=f(x)+f[(n-1)x]$$

οπότε

$$f(nx)=f(x)+f[(n-1)x]$$
$$f[(n-1)x]=f(x)=f[(n-2)x]$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$f(2x)=f(x)+f(x)$$
$$f(x)=f(x)$$

Με πρόσθεση των n προηγουμένων ισοτήτων λαμβάνουμε $f(nx)=nf(x)$ για οποιοδήποτε θετικό ακέραιο n.

Αν ο n είναι αρνητικός ακέραιος, τότε ο αριθμός –n είναι θετικός ακέραιος και έχουμε

$$f(nx) = f[-(-n)x] = f[(-n)(-x)] = - nf(-x) \overset{(1)}{=} nf(x)$$

Άρα, για οποιοδήποτε ακέραιο n ισχύει $f(nx)=nf(x)$ για κάθε πραγματικό αριθμό x.

Ας θεωρήσουμε τώρα τον τυχαίο ρητό αριθμό p. Τότε υπάρχουν $m\in\mathbb{Z}$ και $n\in\mathbb{N}^*$ ώστε να ισχύει $p=\frac{m}{n}$ και

$$f(mx)=f(\frac{m}{n}nx)\Rightarrow mf(x)=nf(\frac{m}{n}x)\Rightarrow f(\frac{m}{n}x)=\frac{m}{n}f(x)\Rightarrow f(px)=pf(x)$$

για κάθε $x\in\mathbb{R}$.

Ας υποθέσουμε τώρα ότι r είναι ένας τυχαίος πραγματικός αριθμός. Τότε υπάρχει ακολουθία ρητών (r_n) ώστε $\lim r_n=r$. Από τη συνέχεια της f συνάγουμε ότι

$$f(rx)=\lim f(r_nx)=\lim[r_nf(x)]=rf(x)$$

Επομένως, για κάθε $r\in\mathbb{R}$ και οποιοδήποτε πραγματικό αριθμό x ισχύει $f(rx)=rf(x)$, η οποία για x=1 οδηγεί στην ισότητα $f(r)=rf(1)$, δηλαδή $f(r)=\alpha\cdot r$, με $\alpha=f(1)$.

Αν επιπλέον συνυπολογίσουμε και την απαίτηση f(π)=0, λαμβάνουμε α=0, οπότε τελικά η μοναδική συνάρτηση που ικανοποιεί τις απαιτήσεις που τέθηκαν είναι η f(x)=0 για κάθε $x\in\mathbb{R}$.

Αυτό βέβαια, παρόλο που φαίνεται να μην μας εξυπηρετεί, δεν δημιουργεί ιδιαίτερα προβλήματα, διότι στην πραγματικότητα δεν ενδιαφερόμαστε για προσθετικές συναρτήσεις που ορίζονται στο $\mathbb{R}$ και είναι συνεχείς σ' αυτό. Μας αρκεί να είναι προσθετικές σε πεπερασμένα σύνολα. Ας δούμε τώρα πως μπορούμε να βρούμε κάποιες τέτοιες προσθετικές συναρτήσεις περνώντας στους διανυσματικούς χώρους επί του $\mathbb{Q}$.

Ορισμός: Έστω S ένα πεπερασμένο σύνολο πραγματικών αριθμών. Λέμε ότι ένα σύνολο $\{\beta_1, \beta_2, \ldots, \beta_n\}$ είναι μια **βάση για το S επί του** $\mathbb{Q}$, όταν

- Κάθε $x\in S$ μπορεί να γραφεί με τη μορφή $x=r_1\beta_1+r_2\beta_2+\ldots+r_n\beta_n$ όπου $r_1, r_2, \ldots, r_n\in\mathbb{Q}$, δηλ. γράφεται, όπως λέμε, ως **ρητός συνδυασμός** των στοιχείων $\beta_1, \beta_2, \ldots, \beta_n$ της βάσης.
- Η ισότητα $r_1\beta_1+r_2\beta_2+\ldots+r_n\beta_n=0$, ισχύει μόνο όταν $r_1=r_2=\ldots=r_n=0$, δηλ. τα $\beta_1, \beta_2, \ldots, \beta_n$ είναι **ρητά ανεξάρτητα**.

Άμεσες συνέπειες του ορισμού είναι τα ακόλουθα:

1. Κάθε $x\in S$ γράφεται με μοναδικό τρόπο ως γραμμικός (ρητός) συνδυασμός των στοιχείων της βάσης.

   Πράγματι, αν υποθέσουμε ότι υπάρχει και δεύτερη έκφραση για το x , έστω

   $$x=s_1\beta_1 + s_1\beta_1 +\ldots+s_n\beta_n \text{ με } s_i\in\mathbb{Q}$$

   τότε, έχουμε

   $$r_1\beta_1 + r_2\beta_2 +\ldots+ r_n\beta_n = s_1\beta_1 + s_1\beta_1 +\ldots+s_n\beta_n$$
   $$\Rightarrow (r_1-s_1)\beta_1 +(r_2-s_2)\beta_2 +\ldots+(r_n-s_n)\beta_n = 0$$
   $$\Rightarrow r_1-s_1 = r_2-s_2 = r_n-s_n =0 \Rightarrow r_i = s_i ,$$

   για όλα τα i, καθόσον τα β_i είναι ρητά ανεξάρτητα.

2. Η συνάρτηση $f_i(x)=r_i$ όπου $x= r_1\beta_1 + r_2\beta_2 +\ldots+ r_n\beta_n$, δηλαδή η συνάρτηση που απεικονίζει το x στον i συντελεστή του όταν αυτό γραφεί ως γραμμικός (ρητός) συνδυασμός των στοιχείων της βάσης, είναι καλά ορισμένη για κάθε $x\in S$.

   Θα αποδείξουμε ότι είναι και προσθετική.

   Πράγματι, αν υποθέσουμε ότι $x' = r_1'\beta_1 + r_2'\beta_2 + \ldots + r_n'\beta_n$ τότε έχουμε

$$x + x' = (r_1 + r_1')\beta_1 + (r_2 + r_2')\beta_2 + \ldots + (r_n + r_n')\beta_n$$

   οπότε

$$f_i(x+x') = r_i+r_i' = f_i(x)+f_i(x')$$

   Επιπλέον, αν για παράδειγμα υποθέσουμε ότι $x=\beta_1$, τότε $f_1(x)=f_1(\beta_1)=1$ και $f_i(x)=0$, για κάθε $i=2, 3, \ldots, n$.

Επομένως, η βάση $\{ \beta_1, \beta_2, \ldots, \beta_n \}$ επί του $\mathbb{Q}$ μας δίνει συναρτήσεις f_i οι οποίες

- είναι προσθετικές και
- λαμβάνουν την τιμή 1 στα β_i και 0 στα άλλα στοιχεία της βάσης.

Οι συναρτήσεις αυτές, είναι ακριβώς οι προσθετικές συναρτήσεις που χρειαζόμαστε. Λογικό είναι λοιπόν να εστιάσουμε την προσοχή μας στην κατασκευή βάσεων για κάθε πεπερασμένο σύνολο S επί του $\mathbb{Q}$.

4.2.iv. Κατασκευή βάσης επί του $\mathbb{Q}$

Θεώρημα

Κάθε πεπερασμένο σύνολο πραγματικών αριθμών έχει μια βάση επί του $\mathbb{Q}$.

Απόδειξη

Έστω $S =\{x_1, x_2, \ldots, x_n\}$ ένα πεπερασμένο σύνολο πραγματικών αριθμών. Επιλέγουμε το x_1 ως πρώτο στοιχείο της βάσης. Κατόπιν εξετάζουμε τα x_1, x_2, … και θεωρούμε ως β_2 το πρώτο εξ αυτών το οποίο δεν είναι ρητό

πολλαπλάσιο του β_1, έστω β_3 το επόμενο εκ των x_i που δεν είναι γραμμικός συνδυασμός των β_1 και β_2, κοκ.

Ισχυριζόμαστε ότι το σύνολο { $\beta_1, \beta_2, \ldots, \beta_n$ } που λαμβάνουμε με αυτό τον τρόπο είναι γραμμικά (ρητά) ανεξάρτητο.

Πράγματι, διότι αν υποθέσουμε ότι κάτι τέτοιο δεν συμβαίνει, τότε υπάρχουν ρητοί $r_1, r_2, \ldots, r_n$, όχι όλοι μηδέν, ώστε

$$r_1\beta_1 + r_2\beta_2 + \ldots + r_n\beta_n = 0 \qquad \textbf{(1)}$$

Αν τώρα υποθέσουμε ότι r_i είναι ο τελευταίος από αυτούς που δεν είναι μηδέν, τότε από την **(1)** προκύπτει ότι:

$$\beta_i = -\frac{r_1}{r_i}\beta_1 - \frac{r_2}{r_i}\beta_2 - \ldots - \frac{r_{i-1}}{r_i}\beta_{i-1}$$

που έρχεται σε αντίφαση από την επιλογή των β_i εκ των x_j, με την απαίτηση κανένα εξ αυτών να μην είναι ρητός συνδυασμός των προηγούμενών του.

Επομένως, για κάθε x_j στο S υπάρχουν οι εξής δυνατότητες:

- είτε είναι στοιχείο της επιλεγόμενης βάσης,
- είτε είναι ρητός συνδυασμός των προηγουμένως επιλεγέντων στοιχείων της βάσης,

οπότε σε κάθε περίπτωση αυτό είναι ρητός συνδυασμός των $\beta_1, \beta_2, \ldots, \beta_n$. Άρα το σύνολο { $\beta_1, \beta_2, \ldots, \beta_n$ } είναι μια βάση επί του $\mathbb{Q}$.

Το παραπάνω θεώρημα μας δίνει αρκετές προσθετικές συναρτήσεις. Τώρα θα το χρησιμοποιήσουμε για να συνδέσουμε τη ρητή ανεξαρτησία με την ιδιότητα της ισοδιαμέρισης μέσω του επομένου θεωρήματος.

4.2.ν. Θεώρημα ρητής ανεξαρτησίας.

Αν $\alpha_1, \alpha_2, \ldots, \alpha_\kappa$ και π είναι ρητά ανεξάρτητα, με την έννοια ότι κανένα από αυτά δεν είναι ρητό πολλαπλάσιο κάποιου άλλου, τότε:

$$\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa = 0 \Leftrightarrow \ell_1 = \ell_2 = \ldots = \ell_\kappa = 0$$

Απόδειξη

Από τον ορισμό των τανυστών η ισότητα

$$\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa = 0$$

σημαίνει ότι ο τανυστής

$$\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa$$

μπορεί, εφαρμόζοντας τους κανόνες

$$\ell \otimes (\alpha + \beta) = \ell \otimes \alpha + \ell \otimes \beta$$

$$(\ell + m) \otimes \alpha = \ell \otimes \alpha + m \otimes \alpha$$

$$\ell \otimes \pi = 0$$

να μετατραπεί σε μηδέν.

Ομοίως, ακολουθώντας ανάλογη πορεία, κάθε έκφραση της μορφής

$$\ell_1 f(\alpha_1) + \ell_2 f(\alpha_2) + \ldots + \ell_\kappa f(\alpha_\kappa)$$

όπου η συνάρτηση f ορίζεται στο πεπερασμένο σύνολο S των γωνιών που εμφανίζονται στην απόδειξη του

$$\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa = 0$$

και έχει τις ιδιότητες

$$\ell f(\alpha+\beta) = \ell f(\alpha) + \ell f(\beta)$$

$$(\ell + m) f(\alpha) = \ell f(\alpha) + m f(\beta)$$

$$f(\pi) = 0,$$

μπορεί να μετατραπεί σε μηδέν.

Αν τώρα τα α_1, α_2, …,α_κ, π είναι ρητά ανεξάρτητα, μπορούμε να τα θεωρήσουμε ως μέλη μιας βάσης επί του $\mathbb{Q}$ για κάθε πεπερασμένο σύνολο που τα περιέχει, όπως είναι το S. Αυτό επιτυγχάνεται για παράδειγμα αν θέσουμε τα α_1, α_2, …, α_κ και π πρώτα στη λίστα των μελών του S και χρησιμοποιήσουμε την προηγούμενη κατασκευή.

Επομένως, μπορούμε να έχουμε προσθετικές συναρτήσεις f_i στο S με την ιδιότητα $f_i(\alpha_i)=1$ και $f_i(\rho)=0$, για οποιοδήποτε στοιχείο ρ της βάσης με $\rho \neq \alpha_i$. Δεδομένου ότι οι f_i είναι ορισμένες στο S, το οποίο είναι το σύνολο όλων των γωνιών που εμφανίζονται στην απόδειξη

$$\ell_1 \otimes \alpha_1 + \ell_2 \otimes \alpha_2 + \ldots + \ell_\kappa \otimes \alpha_\kappa = 0.$$

μπορούμε, ομοίως, να αποδείξουμε ότι

$$\ell_1 f_i(\alpha_1)+ \ell_2 f_i(\alpha_2)+\ldots+ \ell_\kappa f_i(\alpha_\kappa)=0.$$

Για τυχαίο i, δεδομένης της ιδιότητας της f_i, η τελευταία ισότητα γίνεται $\ell_i=0$. Άρα $\ell_1=\ell_2=\ldots=\ell_\kappa=0$.

Το αντίστροφο του θεωρήματος είναι προφανές.

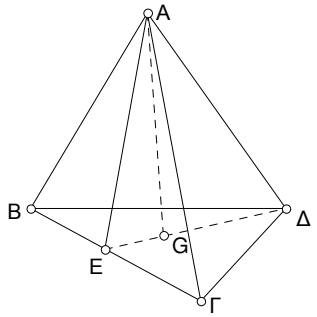
4.2.vi. Το τετράεδρο και ο κύβος

Από το θεώρημα ρητής ανεξαρτησίας συνάγουμε ότι αν το α είναι ρητά ανεξάρτητο του π, που σημαίνει ότι το α δεν είναι ρητό πολλαπλάσιο του π και $\ell\neq 0$, τότε $\ell\otimes\alpha\neq 0$.

Ας δούμε τώρα τι συμβαίνει με την αναλλοίωτη του Dehn σε ένα κανονικό τετράεδρο S στο οποίο , για λόγους απλούστευσης, θεωρούμε ότι η ακμή είναι ίση με τη μονάδα. Είναι φανερό ότι ισχύει $D(S)=6\otimes\alpha$, όπου α είναι γωνία του κανονικού τετραέδρου. Επίσης γνωρίζουμε ότι το κανονικό τετράεδρο είναι ισοδιαμερίσιμο με τον κύβο μόνο αν οι αναλλοίωτες του Dehn των δυο στερεών είναι ίδιες. Όπως έχουμε ήδη αναφέρει στην περίπτωση του κύβου, ισχύει $D(s)=0$.

Συμπερασματικά λοιπόν, **αρκεί να αποδείξουμε ότι η δίεδρη γωνία α ενός κανονικού τετραέδρου δεν είναι ρητό πολλαπλάσιο του π, απ' όπου προκύπτει άμεσα ότι $D(s)\neq 0$.**

Πριν προχωρήσουμε όμως, ας αναφέρουμε λίγα πράγματα για τις γωνίες του τετραέδρου.



Έστω ΑΒΓΔ ένα τετράεδρο με ακμή ίση με τη μονάδα. Αν ΑΕΔ=α είναι η αντίστοιχη επίπεδη της δίεδρης γωνίας του τετραέδρου και G το βαρύκεντρο του τριγώνου ΒΓΔ, τότε εύκολα βρίσκουμε ότι

$$EG=\frac{1}{3}E\Delta \Rightarrow EG=\frac{1}{3}AE$$

$$\frac{EG}{AE}=\frac{1}{3}\Rightarrow \text{συνα}=\frac{1}{3}.$$

Έτσι, προκειμένου να αποδείξουμε ότι $D(s)\neq 0$, το οποίο καταδεικνύει ότι το τετράεδρο δεν είναι ισοδιαμερίσιμο με τον κύβο, αρκεί να αποδείξουμε ότι μια γωνία της οποίας το συνημίτονο είναι $\frac{1}{3}$, δεν μπορεί να είναι ρητό πολλαπλάσιο του π.

4.2.vii. Το θεώρημα του Dehn.

Το κανονικό τετράεδρο δεν είναι ισοδιαμερίσιμο με τον κύβο.

Απόδειξη.

Έστω α η γωνία του τετραέδρου. Σύμφωνα με τα όσα εκθέσαμε προηγουμένως, αρκεί να αποδείξουμε ότι ο α δεν είναι ρητό πολλαπλάσιο του π. Ας υποθέσουμε λοιπόν ότι ο α είναι ένα ρητό πολλαπλάσιο του π. Αυτό σημαίνει ότι υπάρχουν θετικοί ακέραιοι m, n ώστε

$$\alpha=\frac{m}{n}\cdot\pi \Rightarrow n\alpha=m\pi \Rightarrow \text{συν}n\alpha=\pm 1.$$

Θα αποδείξουμε ότι κάτι τέτοιο είναι αδύνατο για οποιοδήποτε φυσικό αριθμό n. Συγκεκριμένα, θα αποδείξουμε επαγωγικά ως προς n την ισχυρότερη πρόταση

S_n: Για κάθε $n\in\mathbb{N}^*$ υπάρχει $q_n\in\mathbb{Z}$ με $q_n\neq$πολ. 3, ώστε $\text{συν}n\alpha=\frac{q_n}{3^n}$

- Διαπιστώνουμε ότι η πρόταση είναι αληθής για n=1.

Πράγματι, αυτό συμβαίνει διότι $\text{συν}\alpha=\frac{1}{3}$.

- Θεωρούμε ότι η πρόταση ισχύει για 2, 3, …,κ δηλ. δεχόμαστε ότι καθεμιά εκ των $S_2, S_3, \ldots, S_\kappa$ είναι αληθής.
- Θα αποδείξουμε ότι ισχύει και για n+1, δηλ. S_{n+1} αληθής. Από τις τριγωνομετρικές ταυτότητες

$$\text{συν}(\kappa+1)\alpha=\text{συν}\kappa\text{συν}\alpha-\text{ημ}\kappa\text{ημ}\alpha$$

και

$$\text{συν}(\kappa-1)\alpha=\text{συν}\kappa\text{συν}\alpha+\text{ημ}\kappa\text{ημ}\alpha$$

προκύπτει ότι

$$\text{συν}(\kappa+1)\alpha+\text{συν}(\kappa-1)\alpha=2\text{συν}\kappa\text{συν}\alpha$$

οπότε,

$$\text{συν}(\kappa+1)\alpha=2\text{συν}\kappa\alpha\,\text{συν}\alpha-\text{συν}(\kappa-1)\alpha \qquad (1)$$

Από την επαγωγική υπόθεση υπάρχουν ακέραιοι q_κ, $q_{\kappa-1}$ οι οποίοι δεν είναι πολλαπλάσια του 3, τέτοια ώστε

$$\text{συν}\kappa\alpha=\frac{q_\kappa}{3^\kappa} \text{ και } \text{συν}(\kappa-1)\alpha=\frac{q_{\kappa-1}}{3^{\kappa-1}}.$$

Δεδομένου ότι $\text{συν}\alpha=\frac{1}{3}$, η (1) δίνει

$$\text{συν}(\kappa+1)\alpha=\frac{\frac{2}{3}q_\kappa}{3^\kappa}-\frac{q_{\kappa-1}}{3^{\kappa-1}}=\frac{2q_\kappa-9q_{\kappa-1}}{3^{\kappa+1}}=\frac{q_{\kappa+1}}{3^{\kappa+1}}$$

όπου $q_{\kappa+1}=2q_\kappa-9q_{\kappa-1}$.

Απομένει να αποδείξουμε ότι $q_{\kappa+1}\neq$πολ.3.

Πράγματι, διότι αν $q_{\kappa+1}=$πολ.3 τότε από την $q_{\kappa+1}=2q_\kappa-9q_{\kappa-1}$ προκύπτει ότι $2q_\kappa=$πολ.3 και, δεδομένου ότι (2, 3)=1, οδηγούμαστε τελικά στο άτοπο $q_\kappa=$πολ.3.

Άρα $\text{συν}n\alpha\neq\pm1$ για όλους τους φυσικούς αριθμούς n, οπότε η γωνία α δεν είναι ρητό πολλαπλάσιο της γωνίας π.

Συμπεράσματα – διδακτικές προεκτάσεις

Είδαμε ότι στο Ευκλείδειο επίπεδο, μέσα από τη διαδικασία είτε της ισοδιαμέρισης είτε της ισοσυμπλήρωσης, μπορούμε να μετατρέψουμε ένα ορθογώνιο σε ισεμβαδικό τρίγωνο. Αυτό σημαίνει ότι με αφετηρία το τετράγωνο, μπορούμε να περάσουμε στο εμβαδόν του ορθογωνίου και στη συνέχεια να υπολογίσουμε το εμβαδόν του τριγώνου. Από εκεί και πέρα μπορούμε να υπολογίσουμε το εμβαδόν οποιουδήποτε πολυγώνου, αρκεί να το χωρίσουμε σε τρίγωνα, πράγμα το οποίο είναι πάντα εφικτό. Αποδεικνύεται ότι, ανεξάρτητα από τον τρόπο χωρισμού του πολυγώνου, το αποτέλεσμα είναι σταθερό. Για την εύρεση τύπου υπολογισμού του εμβαδού που σχηματίζεται από μη πολυγωνικό χωρίο, όπως εμβαδόν κυκλικού δίσκου, εφαρμόζονται μη στοιχειώδεις διαδικασίες, δηλαδή διαδικασίες που

χρησιμοποιούν την έννοια του ορίου και δεν μας απασχολούν στα πλαίσια της παρούσας εργασίας.

Το ερώτημα είναι αν μπορούμε να εφαρμόσουμε κάποια από τις διαδικασίες που προαναφέραμε και στον χώρο, προκειμένου, με στοιχειώδεις μεθόδους, να βρούμε τύπο που υπολογίζει το εμβαδόν κάθε πολυέδρου, χρησιμοποιώντας ως «δομικό συστατικό» το τετράεδρο, δεδομένου ότι, όπως αποδεικνύεται, κάθε πολύεδρο διαιρείται σε τετράεδρα με άπειρους τρόπους. Η απάντηση στο ερώτημα, όπως προκύπτει από την επεξεργασία του θέματος είναι αρνητική, καθότι η τομή του τετραέδρου με επίπεδα και η επικόλληση στη συνέχεια των πολυεδρικών τμημάτων που θα προκύψουν, δεν είναι δυνατόν να μας δώσει κύβο (Θ. Dehn). Αυτό σημαίνει ότι δεν υπάρχει η δυνατότητα, μέσα από αυτή τη διαδικασία, να μετασχηματίσουμε ένα τετράεδρο σε κύβο ίσου όγκου.

Η αρνητική αυτή απάντηση στο τρίτο πρόβλημα Hilbert, που είναι το μόνο που σχετίζεται με τα μαθηματικά της Μέσης Εκπαίδευσης, οδηγεί στο συμπέρασμα ότι, αν θέλουμε να βρούμε τύπο ο οποίος θα υπολογίζει τον όγκο τυχαίου πολυέδρου, πρέπει να καταφύγουμε στην έννοια του ορίου.

Ας δούμε τώρα δυο προτάσεις για διδακτική αξιοποίηση του τρίτου προβλήματος Hilbert.

Πρόταση 1. (ΣΤ΄ Δημοτικού)

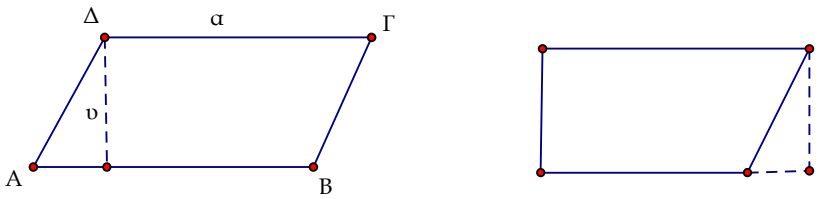
Στο βιβλίο της ΣΤ΄ Δημοτικού (Όλγα Κασούτη κλπ) και συγκεκριμένα στα κεφάλαια 62-64, που αναφέρονται στο εμβαδόν, θα μπορούσαμε να εντάξουμε την επόμενη δραστηριότητα. Ο στόχος μας είναι, οι μαθητές να αποκτήσουν τη δυνατότητα:

- να διαπιστώνουν ότι διαφορετικά σχήματα μπορεί να έχουν ίδιο εμβαδόν (ύπαρξη ισοδύναμων σχημάτων)

- να μετασχηματίζουν με τη διαδικασία κοπής και επικόλλησης επίπεδα σχήματα σε άλλα και μέσα από αυτό το μετασχηματισμό
- να ανακαλύπτουν τους τύπους που δίνουν το εμβαδόν τυχαίου παραλληλογράμμου, τριγώνου και τραπεζίου, με αφετηρία το εμβαδόν ορθογωνίου
- να υπολογίζουν το εμβαδόν τυχαίου πολυγώνου, αναλύοντας το σε επιμέρους τρίγωνα

Στη δραστηριότητα που ακολουθεί θεωρούμε γνωστό ότι το εμβαδόν του ορθογωνίου με μήκος α και πλάτος β είναι (μήκος) x (πλάτος)

1. Στο επόμενο σχήμα, θεωρήστε ότι κόβουμε το πλάγιο παραλληλόγραμμο όπως δείχνει η διακεκομμένη γραμμή και κατόπιν το κολλάμε ώστε να πάρουμε το δεύτερο σχήμα.



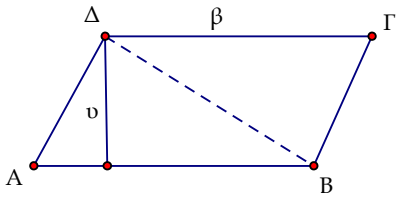
i. Γιατί νομίζετε ότι τα δυο σχήματα έχουν ίσα εμβαδά; ……..

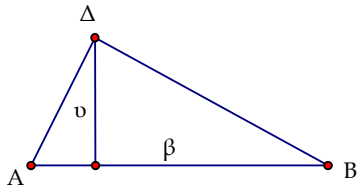
ii. Ποιος είναι ο τύπος που μας δίνει το εμβαδόν του δευτέρου σχήματος; $E_{(ορθογωνίου)}$=……..

iii. Αφού συνδυάσετε τα αποτελέσματα στα δυο προηγούμενα ερωτήματα, ποιος νομίζετε ότι είναι ο τύπος που μας δίνει το εμβαδόν τυχαίου παραλληλογράμμου;

$E_{(παραλληλογράμου)}$=……..

2. Αντιγράψτε το παραλληλόγραμμο του παρακάτω σχήματος σε ένα χαρτί και στη συνέχεια κόψτε το χαρτί ώστε να μείνει μόνο το παραλληλόγραμμο.





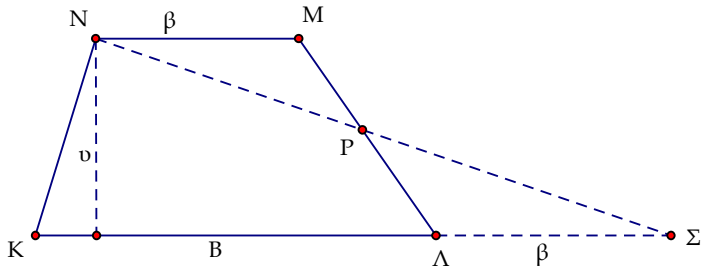
i. Μπορείτε να διπλώσετε το χαρτί κατά μήκος της ΒΔ ώστε το Γ να πέσει πάνω στο Α;……

ii. Κόψτε το χαρτί όπως δείχνει η διακεκομμένη γραμμή και τοποθετήστε το ώστε η πλευρά ΓΔ να πέσει πάνω στην ΑΒ. Τι σχέση έχει το σχήμα που πήρατε με το τρίγωνο ΔΑΒ του σχήματος; ……

iii. Το παραλληλόγραμμο του σχήματος αποτελείται από δυο τρίγωνα ίσα με αυτό που βλέπουμε. Άρα η σχέση που συνδέει τα εμβαδά των δυο σχημάτων είναι $E_{(παραλληλογράμμου)}$=….$E_{(τριγώνου)}$

iv. Το εμβαδόν παραλληλογράμμου είναι $E_{(παραλληλογράμμου)}=β\cdot υ$, οπότε το εμβαδόν του τριγώνου δίνεται από τον τύπο $E_{(τριγώνου)}=(β\cdot υ)$: ….

3. Αντιγράψτε το παρακάτω σχήμα σε ένα χαρτί, κόψτε το τρίγωνο ΜΝΡ και προσπαθήστε να το τοποθετήσετε ώστε να συμπέσει με το τρίγωνο ΛΣΡ.



i. Η πλευρά ΚΣ του τριγώνου ΝΚΣ είναι ίση με το ……των βάσεων Β και β του τραπεζίου ΚΛΜΝ, δηλαδή ΚΣ=….+….

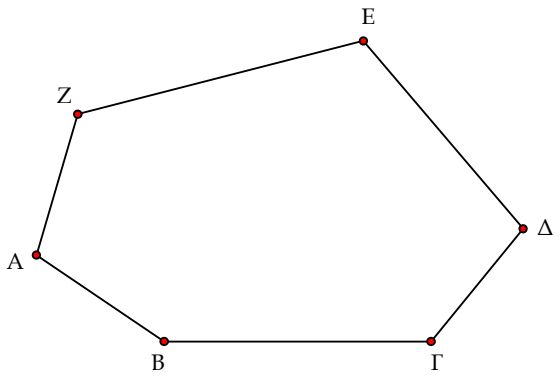
ii. Ποιος είναι ο τύπος που μας δίνει το εμβαδόν Ε του τριγώνου ΝΚΣ με τη βοήθεια των Β, β και υ; $E_{(ΝΚΣ)}$=[(Β+…)·…]:2

iii. Το εμβαδόν του τραπεζίου ΚΛΜΝ είναι …….. … με το εμβαδόν του τριγώνου ΝΚΣ.

iv. Άρα το εμβαδόν του τραπεζίου δίνεται από τον τύπο

$E_{(Τραπεζίου)}$=……

4. Στο παρακάτω σχήμα απεικονίζεται ένας αγρός ΑΒΓΔΕΖ.



i. Δοκιμάστε να χωρίσετε τον αγρό σε τρίγωνα τα οποία να μην έχουν κοινά εσωτερικά σημεία.

ii. Ποιος είναι ο μικρότερος αριθμός τέτοιων τριγώνων; ……

iii. Αν μπορούμε να υπολογίσουμε το εμβαδόν οποιουδήποτε τριγώνου, ποια είναι η διαδικασία που προτείνεται για να υπολογίσουμε το εμβαδόν του αγρού; …… ……

Πρόταση 2. (Β΄ Λυκείου)

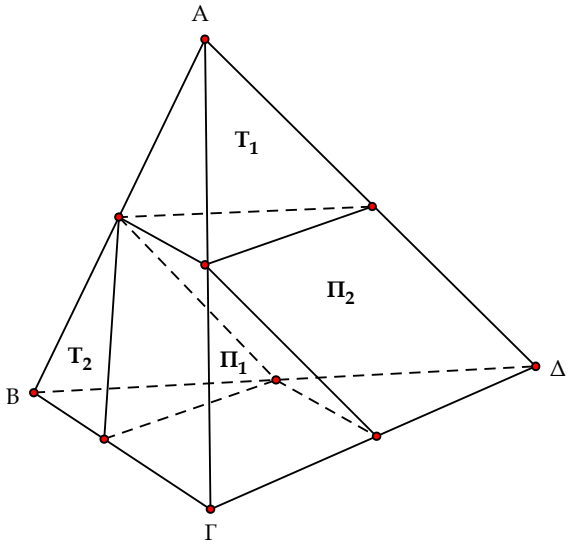
Στο βιβλίο της Άλγεβρας Β΄ Λυκείου και συγκεκριμένα στην παράγραφο 3. 3 αναφέρεται το άπειρο άθροισμα όρων γεωμετρικής προόδου, θα μπορούσαμε να εντάξουμε την επόμενη δραστηριότητα. Ο στόχος μας είναι, οι μαθητές:

- να εξοικειωθούν με άπειρες διαδικασίες
- να συνδέσουν αντικείμενα από διαφορετικά γνωστικά πεδία των μαθηματικών

- να διαπιστώσουν τη χρησιμότητα των μαθηματικών σε πραγματικές καταστάσεις

Στη δραστηριότητα που ακολουθεί θεωρούμε γνωστό ότι ο όγκος κάθε πρίσματος είναι ίσος με το γινόμενο του εμβαδού της βάσης επί το ύψος του.

Το τετράεδρο του σχήματος έχει κοπεί με επίπεδα παράλληλα στις έδρες του, τα οποία διέρχονται από τα μέσα των ακμών που δεν συμμετέχουν στο σχηματισμό της συγκεκριμένης έδρας. Έτσι έχουν δημιουργηθεί δυο τετράεδρα T_1, T_2 όμοια με το αρχικό το και δυο τριγωνικά πρίσματα Π_1, Π_2.



1. Σε καθένα από τα τριγωνικά πρίσματα του σχήματος η τριγωνική βάση του είναι ίση με το …… της αντίστοιχης έδρας και το ύψος του είναι ίσο με …….. του ύψους του αρχικού τετραέδρου. Άρα το κάθε πρίσμα έχει όγκο ίσο με το $\frac{1}{8}$ του γινομένου (εμβαδόν βάσης)x(ύψος), οπότε το άθροισμα των όγκων τους είναι ίσο με το ….. του γινομένου (εμβαδόν βάσης)x(ύψος).

2. Αν επαναλάβουμε την ίδια διαδικασία στα τετράεδρα T_1 και T_2 τότε σε καθένα από αυτά τα δυο τριγωνικά πρίσματα που σχηματίζονται έχουν

όγκο ίσο με το $\frac{1}{4}$ του γινομένου (εμβαδόν βάσης του T_1)x(ύψος του T_1).

Να αιτιολογήσετε γιατί:

(εμβαδόν βάσης του T_1)x(ύψος του T_1)= $\frac{1}{8}$ (εμβαδόν βάσης)x(ύψος)

……

……

Έτσι, μετά την επανάληψη της διαδικασίας, συνολικός όγκος των πρισμάτων που έχει σχηματισθεί είναι

$$(\frac{1}{4}+\frac{1}{4^2})\text{ (εμβαδόν βάσης)x(ύψος)}$$

3. Αν επαναλάβουμε τη διαδικασία «άπειρες φορές» τότε το άθροισμα των όγκων όλων των πρισμάτων που σχηματίζονται δίνονται από τη σχέση

$$(\frac{1}{4}+\frac{1}{4^2}+\frac{1}{4^3}+\text{...άπειροι όροι})\text{ (εμβαδόν βάσης)x(ύψος)}$$

4. Υπολογίσατε το άπειρο άθροισμα s=$\frac{1}{4}+\frac{1}{4^2}+\frac{1}{4^3}+...$

s=……

5. Αν V είναι ο όγκος του τετραέδρου ποια σχέση συνδέει το V με το άθροισμα των όγκων των άπειρων πρισμάτων που σχηματίζονται;

……

……

6. Δείξτε ότι V=$\frac{1}{3}$(εμβαδόν βάσης)x(ύψος).

……

……

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. DAVID HILBERT: ΤΑ ΘΕΜΕΛΙΑ ΤΗΣ ΓΕΩΜΕΤΡΙΑΣ
   (Μετάφραση Σ. Παπαδόπουλος. Εκδόσεις: ΤΡΟΧΑΛΙΑ 1995)
2. GOTLOB FREGE: ΤΑ ΘΕΜΕΛΙΑ ΤΗΣ ΑΡΙΘΜΗΤΙΚΗΣ
   (Μετάφραση Γ. Ρουσσόπουλος. Εκδόσεις: ΝΕΦΕΛΗ 1990)
3. DONALD DAVIS: Η ΦΥΣΗ ΚΑΙ Η ΔΥΝΑΜΗ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
   (Μετάφραση Δ. Καραγιαννάκης – Μ. Μαγειρόπουλος. Εκδόσεις: Π.Ε.Κ. 2007)
4. STEWART SHAPIRO: ΣΚΕΨΕΙΣ ΓΙΑ ΤΑ ΜΑΘΗΜΑΤΙΚΑ
   (Μετάφραση Κ. Δρόσος Δ. Σπανός. Εκδόσεις Πανεπιστημίου Πατρών 2006)
5. P. DAVIS – R. HERSH: Η ΜΑΘΗΜΑΤΙΚΗ ΕΜΠΕΙΡΙΑ
   (Μετάφραση Γ. Αναστασιάδης. Εκδόσεις: ΤΡΟΧΑΛΙΑ 1996)
6. Δ. ΑΝΑΠΟΛΙΤΑΝΟΣ: ΕΙΣΑΓΩΓΗ ΣΤΗ ΦΙΛΟΣΟΦΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ (Εκδόσεις: ΝΕΦΕΛΗ 2005)
7. Δ. ΑΝΑΠΟΛΙΤΑΝΟΣ (επιμ.): ΣΤΙΓΜΕΣ ΚΑΙ ΔΙΑΡΚΕΙΕΣ
   (Εκδόσεις: ΝΕΦΕΛΗ 2010)
8. Π. ΧΡΙΣΤΟΔΟΥΛΙΔΗΣ (επιμ.): Η ΦΙΛΟΣΟΦΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ
   (Εκδόσεις Γ. Α. ΠΝΕΥΜΑΤΙΚΟΥ 1993)
9. Γ. Ρουσσόπουλος: ΜΑΘΗΜΑΤΙΚΟΣ ΡΕΑΛΙΣΜΟΣ
   (Εκδόσεις: ΕΛΛΗΝΙΚΑ ΓΡΑΜΜΑΤΑ 1999)
10. Howard Eves: ΜΕΓΑΛΕΣ ΣΤΙΓΜΕΣ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ (2)
    (Εκδόσεις: ΤΡΟΧΑΛΙΑ)
11. John B. Fraleigh: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΛΓΕΒΡΑ
    (Μετάφραση: Απ. Γιαννόπουλος Εκδόσεις: Π. Ε. Κ. 2006)
12. John Stillwell: NUMBERS AND GEOMETRY
    (Εκδόσεις: Springer 1997)
13. D. Cox – J. Little – D. O' Shea: IDEALS, VARIETES, AND ALGORITHMS
    (Εκδόσεις: Springer 1996)
14. Vladimir Boltiánskiĭ: HILBERT'S THIRD PROBLEM
    (Trans. in English: R. Silverman Εκδόσεις: V. H. WINSTON & SONS 1978)

15. Martin Aigner – Günter Ziegler: Proofs from the Book
(Εκδόσεις: Springer)
16. Dmitri Fuchs – Serge Tabachnikov: Mathematical omnibus thirty lectures on classic mathematics (American Mathematical Society)
17. Robin Hartshorne: GEOMETRY: EYCLID AND BEYOND
(Εκδόσεις: Springer)
18. Robert A. Beezer: A First Course in Linear Algebra
(Univ. of Puget Sound - Washington)
19. E. H. Connell: Elements of Abstract and Linear Algebra
(Univ. of Miami)
20. B. Buchberger & F. Winkler: Gröbner Basis and Applications
(CAMBRIDGE UNIV. PRESS 1998)
21. Γ. Κουμουλλής – Σ. Νεγρεπόντης: Θεωρία Μέτρου
(Εκδόσεις: Συμμετρία 2005)
22. Mark Antony Armstrong: Ομάδες και Συμμετρία
(Μετάφραση: Δ. Νταής Εκδόσεις: Leader Books Αθήνα 2002)

Ηλεκτρονικές και διαδικτυακές πηγές.

1. Stephen G. Simpson: Partial Realizations of Hilbert's Program
(Journal of Symbolic Logic, volume 53, 1988)
2. D. H. Sattinger: Measure theory & Integration
(Lecture Notes 2004 Yale University)
3. Walter D. Neuman: Hilbert's 3rd problem and invariants of 3-manifolds
(Geometry and Topology Monographs Vol. 1 1998)
4. Inna Zakharevich: Hilbert's Third Problem
(mathcircle. Berkeley.edu)
5. Rich Schwartz: Dehn's Dissection Theorem
(www.math.brown.edu/~res/papers/dehn.pdf)
6. A. M. Cohen: Computers (Ac)counting for Mathematical Problems
(SMS Research 1996)

7. Bruno Buchberger: Grobner Bases: A short introduction for systems Theorists
(Un. of Linz, A 4232 Schloss Hagenberg, Austria)
8. A. Sharifi, E. Mehra, etc.: Algebraic Attacs from a Groebner Basis Perspective
9. Henri Lombardi – Hervé Perdry: The Buchberger Algorithm as a Tool for ideal theory of polynomial
(Univ. of Franche- Comté)
10. David Benko: A New Approach to Hilbert's Third Problem
(American Mathematical Monthly Vol. 114 p. 665-676)
11. Robert A. Beezer: A First Course in Linear Algebra
(Department of Mathematics and Computer Science University of Puget Sound)
12. Jinhyun Park: Hilbert's Third Problem
(Pizza seminar talk on Hilbert's 3rd problem and the scissors-congruence groups Febr.14 2004)
13. Jeremy D. Sher: How Real are the Real Numbers?
(MIT Undergraduate Journal of Mathematics p. 179-188)
14. Abhijit Champanerkar: Scissors Congruence & Hilbert's 3rd Problem
(College of Staten Island CUNY April 2004)
15. Stephen G. Simpson: Logic and Mathematics
(Department of Mathematics Pennsylvania St. Univ. April 4 1999)
16. Thomas Tymoczko: THE FOUR – COLOR PROBLEM AND ITS PHILOSOPHICAL SIGNIFICANCE
(The Journal of Philosophy Febr. 1979 p. 57-83)
17. Kevin Woods: Cubin the Pyramid or Why we need Calculus
18. Karl W. Lee: Axiomatic systems
(Department of Mathematics Centucky Univ.)
19. Graeme Taylor: Buchberger's Algorithm
(http://www.everything2. com/index.pl)

Σημειώσεις από τις παραδώσεις των μαθημάτων

1. Ε. Ράπτης: Άλγεβρα
2. Ε. Ράπτης: Υπολογιστική Άλγεβρα
3. Σ. Νεγρεπόντης: Ιστορία των αρχαίων Ελληνικών μαθηματικών
4. Ε. Βασιλείου: Γεωμετρία για τη Διδακτική
5. Δ. Λάππας: Ιστορία των Νεώτερων Μαθηματικών