Τμήμα Μαθηματικών, Πανεπιστήμιο Πατρών

Εισαγωγή στην Προβολική Γεωμετρία
Μία προσέγγιση μέσω Γραμμικής Άλγεβρας

Παναγιώτης Μακρής
Επιβλέπων Καθηγητής: **Ανδρέας Αρβανιτογεώργος**

Προπτυχιακή Διπλωματική Εργασία

Πάτρα
Ιούνιος 2021

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Ιστορικά χαρακτηριστικά:

Από τον 15ο αιώνα μ.Χ. είχε γίνει κατανοητό, ότι η Ευκλείδεια Γεωμετρία δεν ήταν πλέον αρκετή ώστε να μοντελοποιήσει τους μετασχηματισμούς που είχαν να κάνουν με την προοπτική ενός σχήματος. Κατά κύριο λόγο η προοπτική εμφανιζόταν στη ζωγραφική και την αρχιτεκτονική και οι τότε καλλιτέχνες και αρχιτέκτονες έψαχναν διάφορους τρόπους να την χειριστούν.

Το πρόβλημα προερχόταν από το γεγονός ότι η απόσταση μεταξύ δύο σημείων στον καμβά ενός καλλιτέχνη, δεν ήταν η ίδια με αυτή που πραγματικά είχαν τα αντικείμενα τα οποία αναπαριστόνταν στον πίνακα. Το γεγονός αυτό έδειξε ότι Ευκλείδεια απόσταση

δεν ήταν ο σωστός τρόπος να μετράμε τις αποστάσεις σε τέτοιου είδους ζητήματα. Τότε λοιπόν αναπτύχθηκε η μέθοδος της προοπτικής ζωγραφικής, αρχικά στην Ιταλία και χρησιμοποιήθηκε ευρέως από τον DaVinci.

Κατά τον 17ο αιώνα, ο αρχιτέκτονας και μηχανικός Desargues κατάφερε να περιγράψει τις κωνικές τομές, ως προοπτικές παραμορφώσεις του κύκλου και ήταν ο πρώτος που συνέλαβε την ιδέα του σημείου στο άπειρο ως το σημείο τομής δύο ευθειών ενός επιπέδου.

Αργότερα, η επαναστατική ιδέα του Descartes και Fermat να περιγράψουν τη γεωμετρία με αναλυτικό τρόπο είχε σαν αποτέλεσμα μια πρωτοφανή και απότομη πρόοδο στη δημιουργία νέων γεωμετρικών μεθόδων. Το 1822 ο Poncelet όντας φυλακισμένος έγραψε διατριβή σχετικά με τις προβολικές ιδιότητες των σχημάτων και για το αναλλοίωτο των προβολών. Αυτή η διατριβή θεωρείται η πρώτη στον τομέα της Προβολικής Γεωμετρίας. Οι Chasles και Möbius μελέτησαν γενικούς προβολικούς μετασχηματισμούς που απεικονίζουν σημεία σε σημεία, ευθείες σε ευθείες και διατηρούν τον διπλό λόγο.

Κατά το μοντέλο του Klein για τις γεωμετρίες έχουμε την εξής ιεράρχηση: η Ευκλείδεια Γεωμετρία είναι μέρος της Αφινικής (Ομοπαραλληλικής) Γεωμετρίας η οποία με τη σειρά της περιέχεται στην Προβολική Γεωμετρία. Η Προβολική Γεωμετρία όπως αναφέρθηκε, μελετάει ιδιότητες που παραμένουν αναλλοίωτες από τις προβολές (προβολικούς μετασχηματισμούς). Κατά αυτόν τον τρόπο η ευθεία μένει ευθεία αλλά οι αποστάσεις, τα μήκη και οι γωνίες αλλάζουν. Η παραλληλία επίσης είναι μια έννοια που αποκτά διαφορετικό νόημα, καθώς δύο ευθείες θα τέμνονται πάντα.

Κίνητρο:

Γενικά όταν ακούμε τη λέξη γεωμετρία, σκεφτόμαστε τρίγωνα στο επίπεδο, το Πυθαγόρειο θεώρημα ή την αναλυτική γεωμετρία που χρησιμοποιούμε εσωτερικά και εξωτερικά γινόμενα. Συνήθως σκεφτόμαστε την Ευκλείδεια Γεωμετρία στην οποία υπεισέρχονται έννοιες όπως η απόσταση, το μήκος, η γωνία κλπ. Υπάρχουν όμως ζητήματα, τα οποία η κλασική Ευκλείδεια Γεωμετρία αδυνατεί να μας δώσει τις απαντήσεις που ψάχνουμε.

Ας σκεφτούμε για παράδειγμα το εξής:
Ο χώρος στον οποίο συνήθως μελετάμε τη Ευκλείδεια Γεωμετρία, δηλαδή ο γνωστός μας δισδιάστατος και τρισδιάστατος Ευκλείδειος χώρος, δεν επαρκεί καθώς κατά κάποιες έννοιες, όπως για παράδειγμα αυτή του δυϊσμού, τον κάνουν ασύμμετρο. Δηλαδή δεν μπορούμε να βρούμε κάποια σχέση μεταξύ ευθειών και σημείων του Ευκλείδειου χώρου μας ενώ όπως θα δούμε, σε ένα προβολικό χώρο υπάρχει άρρηκτη σύνδεση μεταξύ τους. Επίσης , γνωρίζουμε ότι μεταξύ δύο σημείων του επιπέδου διέρχεται μοναδική

ευθεία. Όμως δεν μπορούμε να πούμε ότι κάθε δύο ευθείες του επιπέδου τέμνονται σε μοναδικό σημείο, γιατί υπάρχει η έννοια της παραλληλίας. Η Προβολική Γεωμετρία έρχεται να δώσει λύση σε τέτοια ζητήματα, προσθέτοντας κάποια σημεία στο άπειρο, που αποτελούν τα σημεία τομής των παράλληλων ευθειών. Συμπεριλαμβανομένων αυτών των ¨νέων σημείων¨, πολλές γεωμετρικές έννοιες ενοποιούνται. Οι κωνικές τομές (ελλείψεις, υπερβολές, παραβολές) θεωρούνται όλες προοπτικές παραμορφώσεις του κύκλου, όταν συμπεριλάβουμε τα σημεία στο άπειρο (Desargues).

Τα μαθηματικά που θα χρειαστούμε για τη μελέτη της Προβολικής Γεωμετρίας προέρχονται κυρίως από τη Γραμμική Άλγεβρα. Η Προβολική Γεωμετρία είναι επί της ουσίας μια γεωμετρική θεώρηση της Γραμμικής Άλγεβρας. Θα δούμε ότι η διαφορά μεταξύ σημείων ενός διανυσματικού χώρου και του δυϊκού του δεν είναι τίποτα άλλο από τη διαφορά ενός σημείου και μιας ευθείας σε ένα επίπεδο.

Ένας άλλος λόγος για την θεμελίωση και τη μελέτη της Προβολικής Γεωμετρίας, πηγάζει από την Αλγεβρική Γεωμετρία. Ο κλάδος των μαθηματικών που αποτελεί την επιτομή για την σύγχρονη Θεωρία Αριθμών και τη Γεωμετρία.

Ο κύριος στόχος της Αλγεβρικής Γεωμετρίας είναι η μελέτη των ιδιοτήτων γεωμετρικών αντικειμένων, όπως π.χ καμπυλών και επιφανειών, οι οποίες ορίζονται μέσω αλγεβρικών εξισώσεων.

Για παράδειγμα, η εξίσωση:

$$x^2 + y^2 - 1 = 0, \tag{1.1}$$

περιγράφει τον μοναδιαίο κύκλο στο $\mathbb{R}^2$. Γενικότερα, μπορούμε να θεωρήσουμε καμπύλες οι οποίες ορίζονται από εξισώσεις της μορφής:

$$ax^2 + by^2 + cxy + dx + ey + f = 0 \tag{1.2}$$

βαθμού 2, γνωστές και ως κωνικές τομές. Ένα ερώτημα που προκύπτει από την μελέτη τέτοιων αντικειμένων είναι αν μπορούν να ταξινομηθούν σύμφωνα με τη γεωμετρική τους αναπαράσταση. Κάτι τέτοιο είναι πράγματι δυνατό (όπως θα δούμε και στο Κεφάλαιο 4), αλλά όχι τόσο εύκολο. Ένα άλλο σημαντικό πρόβλημα είναι η μελέτη των τομών τέτοιου είδους γεωμετρικών αντικειμένων. Αν έχουμε δύο καμπύλες C_1 και C_2 βαθμού m και n αντίστοιχα, ποιος είναι ο αριθμός των κοινών σημείων τους; Η απάντηση σε αυτό το ερώτημα είναι ¨εξαρτάται¨. Ακόμα και στην περίπτωση που έχουμε ότι $m = n = 1$, υπάρχουν τρεις δυνατές περιπτώσεις. Είτε οι ευθείες ταυτίζονται, είτε είναι παράλληλες, είτε έχουν μοναδικό σημείο τομής. Γενικά, περιμένουμε ότι θα έχουμε mn σημεία τομής. Όμως κάποια από αυτά τα σημεία μπορεί να είναι αδύνατο να βρεθούν, καθώς είτε

βρίσκονται στο άπειρο, είτε ταυτίζονται, είτε είναι μιγαδικοί αριθμοί.

Αρχίζει λοιπόν να διαφαίνεται ότι τα σημεία στο άπειρο χρήζουν ειδικής αντιμετώπισης. Η Προβολική Γεωμετρία θεμελιώθηκε με τέτοιο τρόπο ώστε να παρέχει λύση στο ζήτημα με τα σημεία στο άπειρο και τη διάκριση τους με τα υπόλοιπα σημεία, θεωρώντας μάλιστα ότι δεν υπάρχει καμία διαφορά μεταξύ των δύο. Στην Προβολική Γεωμετρία τα σημεία στο άπειρο γίνονται απλά σημεία, πράγμα που απλοποιεί αρκετά τα πράγματα. Η ταξινόμηση των κωνικών τομών γίνεται απλούστερη και η εύρεση σημείων τομής γίνεται πιο ξεκάθαρη.

Από άποψη θεμελίωσης, η Προβολική Γεωμετρία μπορεί να θεμελιωθεί είτε αξιωματικά είτε μέσω Γραμμικής Άλγεβρας. Η αξιωματική προσέγγιση της Προβολικής Γεωμετρίας προηγείται ιστορικά της προσέγγισης με Γραμμική Άλγεβρα. Στην παρούσα εργασία θα αναπτυχθεί η θεωρία μέσα από τα εργαλεία που μας παρέχει η Γραμμική Άλγεβρα. Παραπέμπουμε τον αναγνώστη να μελετήσει τα βιβλία των Veblen και Young, Emil Artin, Coxeter και Ε. Βασιλείου αν θέλει να δει την αξιωματική θεμελίωση της Προβολικής Γεωμετρίας.

Στην προσέγγιση μέσω Γραμμικής Άλγεβρας, όλες οι έννοιες που θα ορίσουμε, θα θεωρούμε ότι μένουν αναλλοίωτες από τον βαθμωτό πολλαπλασιασμό. Δηλαδή, αν θεωρήσουμε δύο αντικείμενα, εκ των οποίων το ένα είναι πολλαπλάσιο του άλλου, τότε αυτά τα δύο αντικείμενα θα είναι ισοδύναμα. Για παράδειγμα, θα δούμε ότι ένα προβολικό σημείο, είναι στην πραγματικότητα μία ευθεία που διέρχεται από την αρχή των αξόνων.

Διάρθρωση εργασίας:

Στο Κεφάλαιο 2 παρέχουμε κάποιες εισαγωγικές έννοιες από τη Γραμμική Άλγεβρα οι οποίες θα φανούν χρήσιμες μετέπειτα. Συγκεκριμένα, θα ορίσουμε την έννοια του διανυσματικού χώρου, θα δούμε τι είναι διάσταση ενός διανυσματικού χώρου και θα συζητήσουμε για τις απεικονίσεις μεταξύ διανυσματικών χώρων. Τέλος, θα δοθεί ο ορισμός του δυϊκού χώρου, έννοια η οποία θα μας φανεί πολύ χρήσιμη αργότερα που θα μιλήσουμε για την Αρχή του Δυϊσμού σε προβολικούς χώρους.

Στο Κεφάλαιο 3 θα ξεκινήσουμε τη βασική μελέτη της Προβολικής Γεωμετρίας. Θα ορίσουμε την έννοια του Προβολικού χώρου και υποχώρου και θα δούμε διάφορα μοντέλα με τα οποία μπορούμε να τον περιγράψουμε. Στη συνέχεια, θα ορίσουμε και θα αναλύσουμε τις απεικονίσεις μεταξύ προβολικών χώρων και θα αποδείξουμε τα βασικά θεωρήματα της Προβολικής Γεωμετρίας, όπως το Θεώρημα της Γενικής Θέσης (Γενίκευση του Θεμελιώδους Θεωρήματος της Προβολικής Γεωμετρίας), καθώς επίσης και τα θεωρήματα του Desargues και Πάππου. Έπειτα, θα μελετήσουμε μια από τις σημαντικότερες έννοιες της Προβολικής Γεωμετρίας, την αρχή του Δυϊσμού. Μια έννοια από την οποία θα φανεί η ανωτερότητα της Προβολικής Γεωμετρίας από την Ευκλείδεια.

Τέλος, θα μελετήσουμε μια αναλλοίωτη ιδιότητα που έχουν οι προβολικοί χώροι, αυτή του διπλού λόγου και θα δούμε μια ενδιαφέρουσα εφαρμογή αυτής στην αεροφωτογραφία.

Στο Κεφάλαιο 4, πλησιάζοντας πλέον στο τέλος της εργασίας, θα μελετήσουμε εισαγωγικά τις επίπεδες προβολικές καμπύλες σε ένα προβολικό επίπεδο επί ενός αυθαίρετου σώματος $\mathbb{F}$. Θα ορίσουμε τα ομογενή πολυώνυμα κάτι που θα φανεί χρήσιμο στην προσπάθεια μας να ταξινομήσουμε τις αλγεβρικές καμπύλες δευτέρου βαθμού (κωνικές τομές) επί του προβολικού επιπέδου. Στη συνεχεία θα αποδείξουμε το διάσημο Θεώρημα του Pascal (*Hexagrammum Mysticum*), το οποίο αποτελεί το ανάλογο του θεωρήματος του Πάππου, αλλά για μη εκφυλισμένες κωνικές τομές. Θα συνεχίσουμε τη μελέτη μας με τις κυβικές καμπύλες, δηλαδή αλγεβρικές καμπύλες τρίτου βαθμού, αυτό θα μας βοηθήσει στην πορεία στον ορισμό των ελλειπτικών καμπυλών. Τέλος, θα ασχοληθούμε με μια εφαρμογή των ελλειπτικών καμπυλών στην ασύμμετρη κρυπτογραφία και συγκεκριμένα στα κρυπτοσυστήματα ελλειπτικής κρυπτογραφίας.

Κεφάλαιο 2

Εισαγωγικές Έννοιες

2.1 Στοιχεία Γραμμικής Άλγεβρας

2.1.1 Διανυσματικοί Χώροι

Στο κεφάλαιο αυτό γίνεται μια ανασκόπηση των βασικών εννοιών της Γραμμικής Άλγεβρας, για διανυσματικούς χώρους πεπερασμένης διάστασης. Έστω $\mathbb{F}$ ένα σώμα (συνήθως $\mathbb{R}$ ή $\mathbb{C}$).

Ορισμός 1. Έστω V ένα μη κενό σύνολο εφοδιασμένο με δύο πράξεις:

- την πρόσθεση διανυσμάτων :

$$+ : V \times V \to V,\ (u, v) \mapsto u + v.$$

- το βαθμωτό πολλαπλασιασμό αριθμού με διάνυσμα:

$$\cdot : \mathbb{F} \times V \to V,\ (\lambda, v) \mapsto \lambda \cdot v.$$

  Θα το συμβολίζουμε χωρίς την τελεία, δηλαδή λv.

Τότε το σύνολο V καλείται διανυσματικός χώρος επί του σώματος $\mathbb{F}$, αν ισχύουν οι παρακάτω ιδιότητες, για τυχαία διανύσματα $u, v \in V$:

1. $(u + v) + w = u + (v + w)$

2. Υπάρχει ένα διάνυσμα στο V, το οποίο συμβολίζουμε 0 και καλείται μηδενικό διάνυσμα τέτοιο ώστε, για κάθε $u \in V, u + 0 = 0 + u = u$

3. Για κάθε $u \in V$, υπάρχει ένα διάνυσμα στο V, το οποίο το συμβολίζουμε με $-u$ και καλείται αντίθετο του u, τέτοιο ώστε $u + (-u) = (-u) + u = 0$

4. $u + v = v + u$ για κάθε $u, v \in V$

   Βλέπουμε ότι το V αποτελεί αβελιανή (αντιμεταθετική) ομάδα με την πράξη της πρόσθεσης

5. $(\lambda\mu)u = \lambda(\mu u)$ για κάθε $\lambda, \mu \in \mathbb{F}$

6. Υπάρχει ένας αριθμός στο $\mathbb{F}$, τον οποίον συμβολίζουμε με 1 τέτοιος ώστε, για κάθε $u \in V$, $1u = u$

7. $\lambda(u + v) = \lambda u + \lambda v$, για κάθε u, $v \in V, \lambda \in \mathbb{F}$

8. $(\lambda + \mu)u = \lambda u + \mu u$, για κάθε $u \in V$, λ, $\mu \in \mathbb{F}$

Πόρισμα: Ισχύει ο νόμος της διαγραφής. Δηλαδή $u + v = u + w \Rightarrow v = w$.

Παρακάτω παραθέτουμε ένα παράδειγμα διανυσματικού χώρου το οποίο θα μας φανεί χρήσιμο αργότερα

Παράδειγμα 1. Το σύνολο $\mathbb{F}^n = \{(x_1, ..., x_n) : x_i \in \mathbb{F}\}$ είναι διανυσματικός χώρος με τις συνήθεις πράξεις τις πρόσθεσης και του βαθμωτού πολλαπλασιασμού επί του σώματος $\mathbb{F}$.

2.1.2 Διανυσματικοί υπόχωροι

Ορισμός 2. Έστω V ένας διανυσματικός χώρος επί του σώματος $\mathbb{F}$ και $U \subseteq V$ με $U \neq \emptyset$. Τότε το U είναι ένας υπόχωρος του U, αν το U είναι ένας διανυσματικός χώρος επί του $\mathbb{F}$, ως προς τις πράξεις της πρόσθεσης διανυσμάτων και του βαθμωτού πολλαπλασιασμού του V.

Θεώρημα 1. (Κριτήριο προσδιορισμού υποχώρου)
Έστω U ένα υποσύνολο ενός διανυσματικού χώρου V. Τότε το U είναι ένας υπόχωρος του V, εάν ικανοποιούνται οι παρακάτω δύο συνθήκες:

1. $0 \in U$

2. Για κάθε u,$v \in U$, $\lambda \in \mathbb{F}$, ισχύει ότι $u + v \in U$ και $\lambda u \in U$

Παρατηρούμε ότι αν V είναι ένα διανυσματικός χώρος, τότε αυτός περιέχει αυτομάτως δύο υποχώρους τον τετριμμένο $\{0\}$ και τον εαυτό του V.

Πρόταση 1. (Τομή υποχώρων διανυσματικού χώρου)
Έστω U,W υπόχωροι ενός διανυσματικού χώρου V. Η τομή $U \cap W$ είναι επίσης ένας υπόχωρος του V.

Απόδειξη: Προφανώς $0 \in U$, $0 \in W$ επειδή οι U, W είναι υπόχωροι. Υποθέτουμε τώρα ότι $u, v \in U \cap W$. Τότε $u, v \in U$ και $u, v \in W$. Επίσης επειδή οι U, W είναι υπόχωροι, τότε για κάθε $\lambda, \mu \in \mathbb{F}$, θα είναι $\lambda u + \mu v \in U \cap W$. Άρα $U \cap W$ είναι υπόχωρος του V.

□

2.1.3 Βάση, διάσταση και άθροισμα διανυσματικών χώρων

Έστω V διανυσματικός χώρος επί ενός σώματος $\mathbb{F}$.

Ορισμός 3. Ένα σύνολο διανυσμάτων $B = \{v_1, v_2, \ldots, v_n\}$ καλείται βάση του διανυσματικού χώρου V αν το B είναι γραμμικώς ανεξάρτητο και κάθε $v \in V$ μπορεί να γραφεί ως γραμμικός συνδυασμός των διανυσμάτων του B. Δηλαδή $\operatorname{span} B = V$.

Από τον παραπάνω ορισμό, καταλαβαίνουμε ότι μια βάση ενός διανυσματικού χώρου δεν είναι μοναδική.

Παρατήρηση 1. Έστω V διανυσματικός χώρος τέτοιος ώστε μία βάση του B_1 να έχει m στοιχεία και μια άλλη βάση του B_2 να έχει n στοιχεία. Τότε $m = n$

Ορισμός 4. Έστω V ένας διανυσματικός χώρος και μια βάση του B, η οποία περιέχει n στοιχεία. Τότε λέμε ότι ο V είναι διανυσματικός χώρος πεπερασμένης διάστασης και συγκεκριμένα ότι έχει διάσταση n και συμβολίζουμε $\dim V = n$.

Από την παραπάνω παρατήρηση και ορισμό καταλαβαίνουμε ότι όλες οι βάσεις ενός διανυσματικού χώρου έχουν το ίδιο πλήθος στοιχείων, από όπου συμπεραίνουμε ότι ο ορισμός της διάστασης είναι καλός διότι ορίζεται μονοσήμαντα για τον εκάστοτε διανυσματικό χώρο.

Παράδειγμα 2. Δίνουμε ως παράδειγμα τη βάση του διανυσματικού χώρου $\mathbb{R}^n$.

Θεωρούμε τα n το πλήθος διανύσματα $\{e_i : i = 1, 2, \ldots, n\}$, όπου το κάθε ένα από αυτά είναι μια διατεταγμένη n-άδα αριθμών που στην i-οστή της θέση βρίσκεται ο αριθμός 1 ενώ σε όλες τις άλλες θέσεις βρίσκεται ο αριθμός 0. Δηλαδή $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$. Αυτά τα διανύσματα είναι γραμμικώς ανεξάρτητα. Επιπλέον, αν θεωρήσουμε ένα τυχαίο

διάνυσμα $v \in \mathbb{R}^n$ με $v = (v_1, \ldots, v_n)$, τότε το v μπορεί να γραφεί ως πεπερασμένος γραμμικός συνδυασμός κατά μοναδικό τρόπο από τα διανύσματα e_i, $i = 1, 2, \ldots, n$. Ειδικότερα έχουμε

$$v = \sum_{i=1}^{n} v_i e_i.$$

Συνεπώς, τα διανύσματα e_i αποτελούν μια βάση του $\mathbb{R}^n$, η οποία ονομάζεται και συνήθης ορθοκανονική βάση του $\mathbb{R}^n$. Βάσει των παραπάνω, μπορούμε να πούμε ότι ο $\mathbb{R}^n$ είναι διανυσματικός χώρος διάστασης n.

Παραθέτουμε τώρα μερικά θεωρήματα πάνω στην έννοια της βάσης, τα οποία θα χρειαστούμε αργότερα.

Θεώρημα 2. Έστω V ένας διανυσματικός χώρος πεπερασμένης διάστασης n. Τότε κάθε σύνολο $B_1 = \{v_1, \ldots, v_r\}$, $r < n$, από γραμμικώς ανεξάρτητα διανύσματα του V αποτελεί μέρος μίας βάσης του V και μπορεί να επεκταθεί ώστε να γίνει βάση του V.

Το παρακάτω θεώρημα δίνει μια βασική σχέση ανάμεσα στη διάσταση ενός διανυσματικού χώρου και στη διάσταση ενός υποχώρου του.

Θεώρημα 3. Έστω V ένας διανυσματικός χώρος πεπερασμένης διάστασης n και U ένας υπόχωρος του. Τότε $\dim U \leq \dim V = n$. Ειδικότερα αν $\dim U = n$, τότε $U = V$.

Ορισμός 5. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης επί ενός σώματος $\mathbb{F}$. Έστω $U, W \subseteq V$. Το άθροισμα των U και W, το οποίο συμβολίζουμε και $U + W$, είναι το σύνολο που αποτελείται από όλα τα αθροίσματα $u + w$, όπου $u \in U$ και $w \in W$. Δηλαδή

$$U + W = \{u + w : u \in U, w \in W\}.$$

Παρατήρηση 2. Στην περίπτωση που τα υποσύνολα U, W είναι διανυσματικοί υπόχωροι του V τότε εύκολα αποδεικνύεται ότι και το άθροισμα τους είναι ένας διανυσματικός υπόχωρος του V.

Το παρακάτω θεώρημα σχετίζει τις διαστάσεις αυτών των υποχώρων.

Θεώρημα 4. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης n επί ενός σώματος $\mathbb{F}$ και U, W διανυσματικοί υπόχωροί του. Τότε ο διανυσματικός υπόχωρος

του, $U + W$ έχει πεπερασμένη διάσταση και ισχύει

$$\dim V \geq \dim (U + W) = \dim U + \dim W - \dim (U \cap W).$$

Απόδειξη: Έστω ότι $\dim U = m$, $\dim W = n$ και $\dim (U \cap W) = r$. Παρατηρούμε ότι $U \cap W$ είναι υπόχωρος του U και του W. Έστω επίσης $\{v_1, \ldots, v_r\}$ μια βάση του χώρου $U \cap W$. Από το Θεώρημα 2 μπορούμε να επεκτείνουμε τη βάση $\{v_i : i = 1, \ldots, r\}$ σε μία βάση του U και σε μια βάση του W. Έστω $\{v_1, \ldots, v_r, u_1, \ldots, u_m - r\}$ η βάση του υποχώρου U και $\{v_1, \ldots, v_r, w_1, \ldots, w_n - r\}$ η βάση του υποχώρου W.

Θεωρούμε τώρα το σύνολο

$$B = \{v_1, \ldots, v_r, u_1, \ldots, u_{m-r}, w_1, \ldots, w_{n-r}\}.$$

Παρατηρούμε ότι το σύνολο B έχει ακριβώς $m + n - r$ στοιχεία. Στόχος μας είναι να δείξουμε ότι το σύνολο B αποτελεί βάση του υποχώρου $U + W$. Αρκεί να δείξουμε ότι το B παράγει τον χώρο $U + W$ και ότι είναι γραμμικώς ανεξάρτητο σύνολο.

Επειδή το $\{v_1, \ldots, v_r, u_1, \ldots, u_{m-r}\}$ παράγει το U και το $\{v_1, \ldots, v_r, w_1, \ldots, w_{n-r}\}$ παράγει το W έπεται ότι η ένωση τους, B παράγει το χώρο $U + W$.

Θα δείξουμε τώρα ότι το B είναι ένα γραμμικώς ανεξάρτητο σύνολο. Έστω,

$$\sum_{i=1}^{r} a_i v_i + \sum_{i=1}^{m-r} b_i u_i + \sum_{i=1}^{n-r} c_i w_i = 0, \tag{2.1}$$

όπου τα a_i, b_j, $c_k \in \mathbb{F}$ για κάθε $i = 1, \ldots, r, j = 1, \ldots, m - r, k = 1, \ldots, n - r$.

Θεωρούμε τώρα ένα $v \in U$ τέτοιο ώστε

$$v = \sum_{i=1}^{r} a_i v_i + \sum_{i=1}^{m-r} b_i u_i. \tag{2.2}$$

Λόγω της (2.1) έχουμε ότι

$$v = -\sum_{i=1}^{n-r} c_i w_i. \tag{2.3}$$

Επειδή $\{w_1, \ldots, w_{n-r}\} \subset W$ έχουμε ότι $v \in W$. Άρα $v \in U \cap W$. Λόγω όμως της υπόθεσής μας έχουμε ότι $\{v_i : i = 1, \ldots, r\}$ είναι μια βάση του V, επομένως υπάρχουν

αριθμοί $d_i \in \mathbb{F}, i = 1, \ldots, r$ ώστε

$$v = \sum_{i=1}^{r} d_i v_i.$$

Συνεπώς, από την (2.3) προκύπτει ότι

$$\sum_{i=1}^{r} d_i v_i = -\sum_{i=1}^{n-r} c_i w_i \Leftrightarrow \sum_{i=1}^{r} d_i v_i + \sum_{i=1}^{n-r} c_i w_i = 0.$$

Λόγω όμως της υπόθεσής μας έχουμε ότι το $\{v_1, \ldots, v_r, w_1, \ldots, w_{n-r}\}$ είναι μια βάση του χώρου W και άρα είναι ένα γραμμικώς ανεξάρτητο σύνολο. Επομένως προκύπτει ότι $c_i = 0$, για κάθε $i = 1, \ldots, n - r$.

Μετά από αντικατάσταση του παραπάνω στην (2.1) προκύπτει ότι

$$\sum_{i=1}^{r} a_i v_i + \sum_{i=1}^{m-r} b_i u_i = 0.$$

Γνωρίζουμε όμως ότι το σύνολο $\{v_1, \ldots, v_r, u_1, \ldots, u_{m-r}\}$ είναι μία βάση του χώρου U. Έπεται ότι $a_i = b_j = 0$, για κάθε $i = 1, \ldots, r, j = 1, \ldots, m-r$ και τελικώς παίρνουμε το ζητούμενο.

□

Ορισμός 6. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης επί ενός σώματος $\mathbb{F}$. Έστω $U, W \subseteq V$. Ονομάζουμε ευθύ άθροισμα των U και W, το οποίο συμβολίζουμε με $U \oplus W$ το σύνολο που αποτελείται από όλα τα διανύσματα v που μπορούν να γραφούν με έναν και μοναδικό τρόπο ως άθροισμα $u + w$, όπου $u \in U$ και $w \in W$.

Θεώρημα 5. Έστω V διανυσματικός χώρος. Τότε ο V είναι το ευθύ άθροισμα των υποχώρων του U και W αν και μόνο αν ισχύουν:

1. $V = U + W$

2. $U \cap W = \{0\}$.

2.1.4 Γραμμικές Απεικονίσεις

Ορισμός 7. Έστω V και U διανυσματικοί χώροι επί του σώματος $\mathbb{F}$. Καλούμε μια $T : V \to U$ γραμμική απεικόνιση, αν ικανοποιούνται οι ακόλουθες συνθήκες:

1. Για κάθε $v, w \in V$, $T(v + w) = T(v) + T(w)$.

2. Για κάθε $\lambda \in \mathbb{F}$ και για κάθε $v \in V$, $T(\lambda v) = \lambda T(v)$.

Μερικές ενδιαφέρουσες παρατηρήσεις που αφορούν τις γραμμικές απεικονίσεις είναι:

- Η T είναι μια γραμμική απεικόνιση αν διατηρεί τις πράξεις ενός διανυσματικού χώρου.

- Θέτοντας $\lambda = 0$, παρατηρούμε ότι $T(0) = 0$, δηλαδή το μηδενικό διάνυσμα του διανυσματικού χώρου V, απεικονίζεται μέσω των γραμμικών απεικονίσεων στο μηδενικό διάνυσμα το διανυσματικού χώρου U.

- Δεδομένης μια γραμμικής απεικόνισης T, η έννοια της γραμμικότητας μπορεί να γενικευτεί για πεπερασμένες γραμμικές εκφράσεις.

Το παρακάτω θεώρημα μας δίνει ότι μια γραμμική απεικόνιση, προσδιορίζεται πλήρως από τις τιμές που λαμβάνει στα διανύσματα μιας βάσης του διανυσματικού χώρου επί του οποίου ορίζεται.

Θεώρημα 6. Έστω V και U διανυσματικοί χώροι ίδιας διάστασης επί ενός σώματος $\mathbb{F}$. Θεωρούμε $\{v_1, \ldots, v_n\}$ μια βάση του V και $u_1, \ldots, u_n \in U$ τυχαία διανύσματα. Τότε υπάρχει μια μοναδική γραμμική απεικόνιση $T : V \to U$, ώστε $T(v_1) = u_1, \ldots, T(v_n) = u_n$.

Ορισμός 8. Έστω τώρα δύο διανυσματικοί χώροι V και U επί ενός σώματος $\mathbb{F}$. Έστω $B_1 = \{v_1, \ldots, v_m\}$, $B_2 = \{u_1, \ldots, u_n\}$ βάσεις των V και U αντίστοιχα. Θεωρούμε επίσης μια γραμμική απεικόνιση $T : V \to U$. Εφόσον B_2 είναι μια βάση του U, μπορούμε να γράψουμε τις τιμές της απεικόνισης στα v_i, $i = 1, \ldots, n$, ως πεπερασμένους γραμμικούς συνδυασμούς των u_j κατά μοναδικό τρόπο.

Έχουμε ότι για κάθε $v_i \in V, i = 1, \ldots, n$

$$T(v_i) = \sum_{j=1}^{m} \lambda_j^i u_j, \text{ όπου } \lambda_j^i \in \mathbb{F} \text{ για κάθε } i = 1, \ldots, n, j = 1, \ldots, m.$$

Ορίζουμε τον $n \times m$ πίνακα και τον ονομάζουμε πίνακα αναπαράστασης της γραμμικής απεικόνισης T ως προς τις βάσεις B_1 και B_2 , τον πίνακα $[T]_{(B_1:B_2)} = (\lambda_j^i), i = 1, \ldots, n,$ $j = 1, \ldots, m$.

Αν μάλιστα $B_1 = B_2$ και άρα $V = U$ τότε μπορούμε να συμβολίσουμε τον πίνακα της γραμμικής απεικόνισης απλά ως $[T]_B$, ο οποίος είναι τετραγωνικός πίνακας.

Ορισμός 9. Έστω V και U δύο διανυσματικοί χώροι επί ενός σώματος $\mathbb{F}$. Ονομάζουμε τους V, U ισόμορφους και συμβολίζουμε $V \cong U$, αν υπάρχει γραμμική απεικόνιση $T : V \to U$ η οποία να είναι $1-1$ και επί. Τότε η γραμμική απεικόνιση ονομάζεται ισομορφισμός μεταξύ των διανυσματικών χώρων V και U.

Παρατήρηση 3. Έστω V και W δύο διανυσματικοί χώροι επί ενός σώματος $\mathbb{F}$. Συμβολίζουμε το σύνολο όλων των γραμμικών απεικονίσεων από ένα διανυσματικό χώρο V σε ένα διανυσματικό χώρο W, ως $\mathcal{L}(V, W)$.

2.1.5 Δυϊκός Χώρος

Έστω V, W δύο διανυσματικοί χώροι επί ενός σώματος $\mathbb{F}$. Θεωρούμε το διανυσματικό χώρο $\mathcal{L}(V, W)$ επί του ίδιου σώματος $\mathbb{F}$. Σε αυτή την υποενότητα θα μελετήσουμε τον χώρο των γραμμικών απεικονίσεων $\mathcal{L}(V, \mathbb{F})$, όπου θεωρούμε ότι το σώμα $\mathbb{F}$ είναι ένας διανυσματικός χώρος επί του εαυτού του διάστασης 1.

Ορισμός 10. Καλούμε τον διανυσματικό χώρο $\mathcal{L}(V, \mathbb{F})$ δυϊκό χώρο του V και τον συμβολίζουμε με V^*. Τα στοιχεία του V^* ονομάζονται γραμμικά συναρτησοειδή ή γραμμικές μορφές, δηλαδή

$$V^* = \{T : V \to \mathbb{F} \mid T \text{ γραμμική } \}.$$

Αν θεωρήσουμε ότι ο διανυσματικός χώρος V είναι χώρος πεπερασμένης διάστασης τότε έχουμε

$$\dim V^* = \dim \mathcal{L}(V, \mathbb{F}) = \dim V \dim \mathbb{F} = \dim V.$$

Η παραπάνω σχέση μπορεί να μας βοηθήσει να βρούμε μια βάση του V^*, εάν γνωρίζουμε μια βάση του V και αντίστροφα.

Θεώρημα 7. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης επί ενός σώματος $\mathbb{F}$ και μια βάση του $\{e_1, \ldots, e_n\}$. Ορίζουμε $e^1, \ldots, e^n \in V^*$ τα γραμμικά συναρτησοειδή ως εξής:

$$e^j(e_i) = \delta_i^j.$$

Τότε το σύνολο $\{e^1, \ldots, e^n\}$ αποτελεί βάση του V^*. Την παραπάνω βάση $\{e^i\}$ την ονομάζουμε δυϊκή βάση της $\{e_i\}$

Η παραπάνω αντιστοιχία είναι πολύ σημαντική, διότι μας επιτρέπει να εκφράσουμε στοιχεία ενός διανυσματικού χώρου ή του δυϊκού του ως προς μια βάση, χρησιμοποιώντας ως συντελεστές στοιχεία του άλλου, όπως θα δούμε και στο παρακάτω θεώρημα.

Θεώρημα 8. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης επί ενός σώματος $\mathbb{F}$ και V^* ο δυϊκός του. Έστω επίσης μια βάση $\{e_1, \ldots, e_n\}$ του V και $\{e^1, \ldots, e^n\}$ η αντίστοιχη δυϊκή της. Τότε

- Για κάθε $v \in V$, $v = \sum_{i=1}^n e^i(v)e_i$.
- Για κάθε $\varphi \in V^*$, $\varphi = \sum_{i=1}^n \varphi(e_i)e^i$.

Αντίστοιχα, μπορούμε να ορίσουμε τον δυϊκό του δυϊκού ή όπως ονομάζεται διπλός δυϊκός να είναι ο διανυσματικός χώρος που περιέχει όλα τα γραμμικά συναρτησοειδή από το χώρο V^* στο σώμα $\mathbb{F}$. Τον διπλό δυϊκό χώρο τον συμβολίζουμε με V^{**}.

Σκοπός μας σε αυτό το σημείο είναι να δείξουμε ότι κάθε $v \in V$ προσδιορίζει μονοσήμαντα ένα στοιχείο $\widehat{v} \in V^{**}$. Έχουμε αρχικά ότι $\widehat{v} : V^* \to \mathbb{F}$. Για κάθε $\varphi \in V^*$ ορίζουμε την

$$\widehat{v}(\varphi) = \varphi(v).$$

Θα δείξουμε ότι η απεικόνιση $\widehat{v}(\varphi) = \varphi(v)$ είναι γραμμική. Πράγματι, έστω $\lambda, \mu \in \mathbb{F}$ και $\varphi_1, \varphi_2 \in V^*$. Έχουμε

$$\widehat{v}(\lambda\varphi_1 + \mu\varphi_2) = (\lambda\varphi_1 + \mu\varphi_2)(v) = \lambda\varphi_1(v) + \mu\varphi_2(v) = \lambda\widehat{v}(\varphi_1) + \mu\widehat{v}(\varphi_2).$$

Συνεπώς $\widehat{v} \in V^{**}$. Έχουμε τώρα το παρακάτω θεώρημα.

Θεώρημα 9. Έστω V ένας διανυσματικός χώρος πεπερασμένης διάστασης επί ενός σώματος $\mathbb{F}$ και V^{**} ο διπλός δυϊκός του. Τότε η απεικόνιση $S : V \to V^{**}$ με $v \mapsto \widehat{v}$ είναι ένας φυσικός ισομορφισμός.

Απόδειξη: Θεωρούμε αρχικά ότι $\dim V = n$. Θα δείξουμε ότι η απεικόνιση S με $v \mapsto \widehat{v}$, είναι γραμμική. Πράγματι, για κάθε λ, $\mu \in \mathbb{F}$, $\widehat{v_1}$, $\widehat{v_2} \in V^{**}$ και $\varphi \in V^*$, έχουμε

$$\widehat{(\lambda v_1 + \mu v_2)}(\varphi) = \varphi(\lambda v_1 + \mu v_2) = \lambda\varphi(v_1) + \mu\varphi(v_2) = \lambda\widehat{v_1}(\varphi) + \mu\widehat{v_2}(\varphi).$$

Δηλαδή $\widehat{\lambda v_1 + \mu v_2} = \lambda \widehat{v_1} + \mu \widehat{v_2}$, επομένως η S με $v \mapsto \widehat{v}$ πράγματι είναι γραμμική.

Θα δείξουμε τώρα ότι η S είναι $1-1$. Έστω $v, u \in V$, με $\widehat{v} = \widehat{u}$. Αρκεί να δείξουμε ότι $v = u$. Πράγματι, για $\varphi \in V^*$, $\widehat{v}(\varphi) = \widehat{u}(\varphi)$.

Έστω τώρα $\{e_i : i = 1, \ldots, n\}$ μια βάση του χώρου V και $\{e^i : i = 1, \ldots, n\}$ η αντίστοιχη δυϊκή της. Θα δείξουμε ότι αν

$$v = \sum_{i=1}^{n} v^i e_i \text{ και } u = \sum_{i=1}^{n} u^i e_i \text{ τότε } v^i = u^i,$$

αρκεί να το δείξουμε για $\varphi = e^j$ επειδή $\varphi = \sum_{j=1}^{n} \varphi_j e^j$. Έχουμε τα εξής:

$$e^j(v) = e^j(\sum_{i=1}^{n} v^i e_i) = \sum_{i=1}^{n} v^i e^j(e_i) = \sum_{i=1}^{n} v^i \delta_i^j = v^j,$$

$$e^j(u) = e^j(\sum_{i=1}^{n} u^i e_i) = \sum_{i=1}^{n} u^i e^j(e_i) = \sum_{i=1}^{n} u^i \delta_i^j = u^j.$$

Τότε

$$\widehat{v}(\varphi) = \widehat{u}(\varphi) \Rightarrow \varphi(v) = \varphi(u) \Rightarrow \sum_{i=1}^{n} \varphi_i e^i(v) = \sum_{i=1}^{n} \varphi_i e^i(u) \Rightarrow \sum_{i=1}^{n} \varphi_i v^i = \sum_{i=1}^{n} \varphi_i u^i \Rightarrow v^i = u^i.$$

Άρα $v = u$, οπότε πράγματι πρόκειται για μια $1-1$ απεικόνιση.

Τέλος έχουμε ότι $\dim V = \dim V^* = \dim V^{**}$, άρα η απεικόνιση $u \mapsto \widehat{u}$ είναι και επί. Συνεπώς, η απεικόνιση μας είναι ισομορφισμός.

Παρατηρούμε μάλιστα ότι ο παραπάνω ισομορφισμός $V \cong V^{**}$ δεν εξαρτάται από την επιλογή της βάσης, είναι δηλαδή ένας φυσικός ισομορφισμός.

□

Θα δούμε τώρα την έννοια του μηδενιστή (annihilator).

Ορισμός 11. Έστω V διανυσματικός χώρος και $W \subseteq V$. Ένα γραμμικό συναρτησοειδές $\varphi \in V^*$ όνομάζεται μηδενιστής του W, αν $\varphi(w) = 0$ για κάθε $w \in W$. Συμβολίζουμε το σύνολο των γραμμικών συναρτησοειδών που ικανοποιεί το παραπάνω, ως W^0 και το ονομάζουμε μηδενιστή του W.

Θα δείξουμε ότι το W^0 είναι ένας υπόχωρος του V^*. Αρχικά έχουμε ότι $0 \in W^0$. Θεωρούμε τώρα $\varphi_1, \varphi_2 \in W^0$ και $\lambda, \mu \in \mathbb{F}$. Τότε για κάθε $w \in W$ ισχύει

$$(\kappa\varphi_1 + \mu\varphi_2)(w) = \kappa\varphi_1(w) + \lambda\varphi_2(w) = 0.$$

Από την παραπάνω σχέση καταλαβαίνουμε ότι $\kappa\varphi_1+\mu\varphi_2 \in W^0$. Επειδή ικανοποιείται η κλειστότητα των πράξεων και $0 \in W^0$, το σύνολο W^0 είναι υπόχωρος του V^*.

Αναφέραμε πριν ότι το W δεν είναι απαραίτητα υπόχωρος του V, παρόλα αυτά αν θεωρήσουμε ότι είναι, προκύπτει η ακόλουθη σχέση μεταξύ του W και του μηδενιστή του W^0.

Θεώρημα 10. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης και W υπόχωρος του V. Τότε

1. $\dim W + \dim W^0 = \dim V$
2. $W^{00} = W$

Απόδειξη:

1. Θεωρούμε ότι $\dim V = n$ και $\dim W = r \leq n$. Στόχος μας είναι να δείξουμε ότι $\dim W^0 = n - r$. Έστω μια βάση του χώρου W η $\{w_1, \ldots, w_r\}$, την οποία επεκτείνουμε σε μια βάση του V, έστω η $\{w_1, \ldots, w_r, v_1, \ldots, v_{n-r}\}$. Θεωρούμε την αντίστοιχη δυϊκή της παραπάνω βάσης, έστω $\{w^1, \ldots, w^r, v^1, \ldots, v^{n-r}\}$.

   Από τον ορισμό της δυϊκής βάσης γνωρίζουμε ότι για κάθε $i = 1, \ldots, n-r$, $j = 1, \ldots, r$, ισχύει $v^i(w_j) = 0$. Επειδή κάθε στοιχείο του W είναι ένας γραμμικός συνδυασμός των w_i και επειδή οι απεικονίσεις v^i είναι γραμμικές, τότε έχουμε ότι για κάθε $w \in W$ ισχύει $v^i(w) = 0$, $i = 1, ..., n-r$. Άρα έχουμε ότι $v^i \in W^0$, για κάθε $i = 1, \ldots, n-r$. Ισχυριζόμαστε ότι τα συναρτησοειδή v^i αποτελούν βάση του μηδενιστή W^0.

   Πράγματι, επειδή το σύνολο $\{v^i\}$ είναι τμήμα μιας βάσης του δυϊκού χώρου, τότε θα πρέπει να είναι γραμμικώς ανεξάρτητο σύνολο.

   Μένει να δείξουμε ότι το σύνολο $\{v^i : i = 1, \ldots, n-r\}$ παράγει τον μηδενιστή W^0. Έστω ένα τυχαίο $v \in W^0$. Το v ως στοιχείο του δυϊκού χώρου μπορεί να γραφεί ως πεπερασμένος γραμμικός συνδυασμός των $w^1, \ldots, w^r, v^1, \ldots, v^{n-r}$, με τους συντελεστές να είναι οι τιμές του συναρτησοειδούς v με ορίσματα τα διανύσματα της αντίστοιχης βάσης του V (Θεώρημα 9). Έχουμε ότι

$$v = \sum_{i=1}^{r} v(w_i)w^i + \sum_{i=1}^{n-r} v(v_i)v^i = 0 + \sum_{i=1}^{n-r} v(v_i)v^i.$$

   Συνεπώς ο τυχαίος μηδενιστής v μπορεί να γραφεί ως πεπερασμένος γραμμικός συνδυασμός των $\{v^1, \ldots, v^{n-r}\}$. Δείξαμε με αυτό τον τρόπο ότι η διάσταση του μηδενιστή W^0 είναι $n - r$.

2. Έστω ότι $\dim V = n$ και $\dim W = r$. Άρα έχουμε ότι $\dim V^* = n$ και από 1. έχουμε ότι $\dim W^0 = n - r$. Αξιοποιώντας ότι $W^{00} = (W^0)^0$, προκύπτει ότι $\dim W^{00} = n - (n - r)$ και άρα $\dim W^{00} = \dim W$.

   Μένει να δείξουμε $W \subseteq W^{00}$. Τότε επειδή οι χώροι έχουν την ίδια διάσταση θα προκύψει ότι $W = W^{00}$. Έστω $w \in W$. Τότε για κάθε γραμμικό συναρτησοειδές $\varphi \in W^0$, $\varphi(w) = 0 = \widehat{w}(\varphi)$. Άρα $\widehat{w} \in W^{00}$. Άρα λόγω του ισομορφισμού $V \cong V^{**}$, $w \in W^{00}$. Έχουμε ότι πράγματι $W \subseteq W^{00}$, συνεπώς $W = W^{00}$.

□

Κεφάλαιο 3

Βασικές έννοιες της Προβολικής Γεωμετρίας

3.1 Προοπτική

Στην πρώτη ενότητα αυτού του κεφαλαίου θα επιχειρήσουμε να εξηγήσουμε μαθηματικά την έννοια της προοπτικής.

Σε αναλογία με την πραγματικότητα θα μπορούσαμε να θεωρήσουμε ότι η όρασή μας βασίζεται στο γεγονός ότι δέσμες φωτός, που θεωρούμε ότι ταξιδεύουν ευθύγραμμα, εισέρχονται στο μάτι μας ξεκινώντας από ένα δεδομένο σημείο, το οποίο παρατηρούμε. Θεωρούμε αυτές τις δέσμες φωτός ως δέσμες παράλληλων ευθειών του $\mathbb{R}^3$ και το σημείο το οποίο παρατηρούμε το ονομάζουμε O. Όπως ακριβώς συμβαίνει και στην οθόνη ενός ηλεκτρονικού υπολογιστή, λαμβάνουμε την πληροφορία από μια οθόνη, την οποία στην προσπάθεια μας για δημιουργία μιας αυστηρής μαθηματικής ερμηνείας, θα θεωρήσουμε ως ένα επίπεδο του $\mathbb{R}^3$, το οποίο δεν περιέχει το σημείο O.

Έστω δύο επίπεδα του Ευκλείδειου χώρου Π_1, Π_2, κανένα εκ των οποίων δεν περιέχει το σημείο O.

Ορισμός 1. Λέμε ότι δύο σημεία $P \in \Pi_1$ και $Q \in \Pi_2$ βρίσκονται σε θέση προοπτικής ως προς το O αν υπάρχει ευθεία γραμμή που να ενώνει τα O, P και Q.

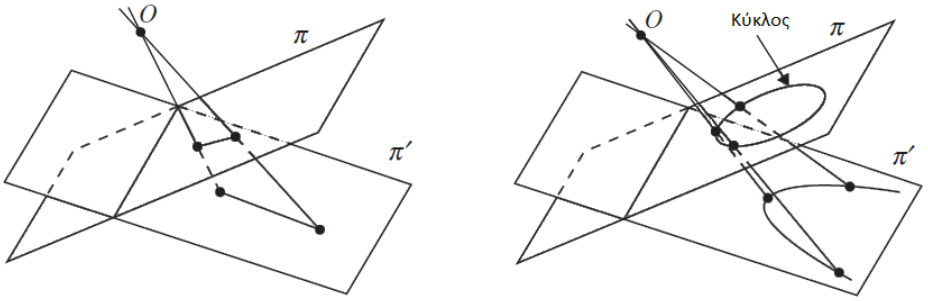
Ορισμός 2. Ονομάζουμε προοπτικότητα (perspectivity) από το Π_1 στο Π_2 με κέντρο το O μια απεικόνιση που στέλνει το σημείο P στο Q, όταν τα σημεία P και Q βρίσκονται σε θέση προοπτικής.

Μια δυσκολία που προκύπτει από τον ορισμό της προοπτικότητας μεταξύ Ευκλείδειων επιπέδων είναι ότι το πεδίο ορισμού της προοπτικότητας δεν μπορεί να είναι ολόκληρο

το επίπεδο Π_1. Πράγματι, αν θεωρήσουμε ένα σημείο $P \in \Pi_1$, ώστε ο φορέας του ευθυγράμμου τμήματος OP (στο εξής έτσι θα συμβολίζουμε τις ευθείες) να είναι ευθεία παράλληλη ως προς το επίπεδο Π_2, τότε η προοπτικότητα δεν θα μπορούσε να οριστεί στο σημείο P, διότι από την Ευκλείδεια Γεωμετρία δεν μπορεί να υπάρχει σημείο τομής της ευθείας με το παράλληλο ως προς αυτήν επίπεδο. Μία ατελής λύση θα ήταν να εξαιρέσουμε εκείνα τα σημεία του επιπέδου, τα οποία δημιουργούν πρόβλημα, αλλά όπως θα δούμε υπάρχει καλύτερος τρόπος να επιτεθούμε σε αυτό το πρόβλημα.

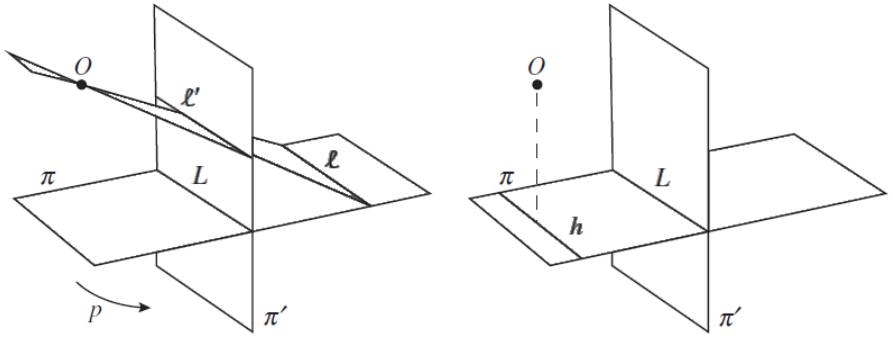
Ήδη με τον παραπάνω ορισμό της προοπτικότητας είμαστε σε θέση να καταλάβουμε έστω και διαισθητικά, ότι κάποιες ιδιότητες των σχημάτων διατηρούνται υπό κάποια προοπτικότητα. Παίρνουμε για παράδειγμα ένα ευθύγραμμο τμήμα σε ένα επίπεδο Π_1. Τότε μέσω μιας προοπτικότητας καταλαβαίνουμε ότι αυτό το ευθύγραμμο τμήμα θα απεικονιστεί σε ευθύγραμμο τμήμα στο επίπεδο Π_2. Αντιθέτως, αν πάρουμε έναν κύκλο στο επίπεδο Π_1 τότε μέσω μιας προοπτικότητας θα μπορούσε ο κύκλος να απεικονιστεί σε κάποιο παραβολικό σχήμα στο επίπεδο Π_2.

Αντιλαμβανόμαστε επομένως, ότι αν ένα σύνολο σημείων είναι συνευθειακά στο επίπεδο Π_1, τότε τα προοπτικά σημεία σε αυτά που ανήκουν στο Π_2, ως προς το O θα παραμείνουν συνευθειακά. Από την άλλη πλευρά, αν ένα σύνολο σημείων στο επίπεδο Π_1 ανήκουν σε ένα κύκλο, τότε μέσω μιας προοπτικότητας δεν είναι απαραίτητο ότι τα προοπτικά σε αυτά σημεία θα ανήκουν και αυτά σε κάποιο κύκλο του επιπέδου Π_2. Μάλιστα καταλαβαίνουμε, ότι μεγάλη σημασία έχει η ¨θέση' του κέντρου O.



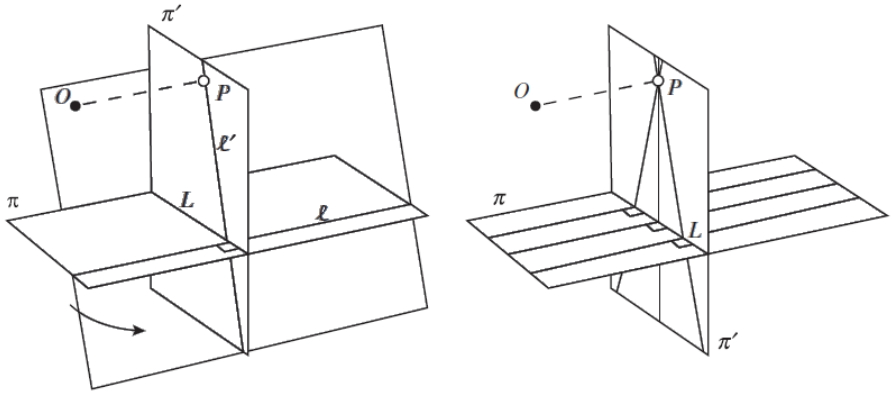
Για να γίνουμε πιο ακριβείς, ας θεωρήσουμε την προοπτικότητα p με κέντρο το O που απεικονίζει σημεία από ένα οριζόντιο επίπεδο Π_1 σε ένα κατακόρυφο Π_2, κάθετο δηλαδή στο Π_1 και έστω L η ευθεία στην οποία το Π_1 και το Π_2 τέμνονται. Μέσω της p κάθε ευθεία l του Π_1 παράλληλη ως προς την L απεικονίζεται σε μια ευθεία l' που βρίσκεται στο επίπεδο Π_2. Η ευθεία L απεικονίζεται μέσω της p στον εαυτό της. Η μόνη εξαίρεση υφίσταται, για την ευθεία που είναι παράλληλη στην L και διέρχεται από το σημείο O', που είναι το σημείο τομής της ευθείας που ενώνει κάθετα το σημείο O με το επίπεδο Π_1. Η συγκεκριμένη ευθεία δεν μπορεί να απεικονιστεί στο Π_2, εφόσον οι

ευθείες που ενώνουν τα σημεία της με το O είναι παράλληλες ως προς το επίπεδο Π_2. Αυτό γίνεται κατανοητό στο παρακάτω σχήμα.



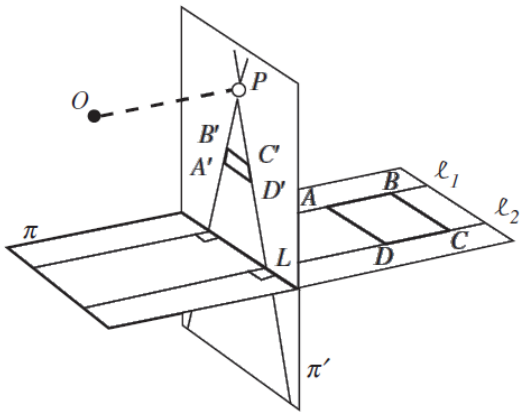
Μελετάμε τώρα την εικόνα της προοπτικότητας p, αν θεωρήσουμε ότι η ευθεία l είναι κάθετη της L. Έστω P το σημείο στο επίπεδο Π_2, το οποίο είναι το σημείο τομής της ευθείας που τέμνει κάθετα το Π_2 από το O. Παρόλο που το σημείο P δεν μπορεί να είναι εικόνα κανενός σημείου το επιπέδου Π_1 (εφόσον η ευθεία OP είναι παράλληλη με το Π_1), το επίπεδο που περιέχει το σημείο O και την ευθεία l τέμνει το επίπεδο Π_2 σε ευθεία l' που διέρχεται από το σημείο P. Προκύπτει ότι η εικόνα της ευθείας l μέσω της προοπτικότητας p είναι η ευθεία l' του Π_2, χωρίς όμως να περιέχει το σημείο P.

Τα παραπάνω επιχειρήματα ισχύουν για οποιαδήποτε ευθεία l του επιπέδου Π_1 κάθετη στην L και αν πάρουμε. Δηλαδή όποιαδήποτε ευθεία παράλληλη στην l επί του επιπέδου Π_1 και να πάρουμε, η εικόνα της μέσω της προοπτικότητας p στο επίπεδο Π_2, θα είναι μια ευθεία l' που θα διέρχεται από το P, χωρίς όμως να περιέχει το σημείο P.



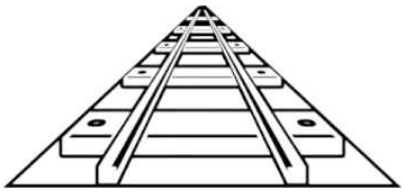
Συνδυάζοντας τις προηγούμενες παρατηρήσεις μας, θα μπορούσαμε να θεωρήσουμε ένα τετράγωνο $ABCD$ στο επίπεδο Π_1 και να εξετάσουμε ποια είναι η εικόνα του μέσω

της προοπτικότητας p στο επίπεδο Π_2. Θεωρούμε ότι οι φορείς των ευθυγράμμων τμημάτων AB και CD, έστω l_1 και l_2 τέμνουν κάθετα την ευθεία L. Συνεπώς, η εικόνα των ευθυγράμμων τμημάτων AB και CD μέσω της προοπτικότητας p στον επίπεδο Π_2, θα έπρεπε να είναι ευθύγραμμα τμήματα των ευθειών l_1' και l_2', που είναι ευθείες διερχόμενες από το σημείο P, αλλά χωρίς να το περιέχουν. Αντίστοιχα, τα ευθύγραμμα τμήματα AD και BC θα απεικονίζονται σε ευθύγραμμα τμήματα στο επίπεδο Π_2, τα οποία θα φαίνεται να έχουν μικρότερο μήκος σε σχέση με το μήκος που έχουν στο επίπεδο Π_1.



Παρατηρώντας το σχήμα βλέπουμε ότι μια προοπτικότητα απεικονίζει ευθείες σε ευθείες και άρα ευθύγραμμα τμήματα σε ευθύγραμμα τμήματα, αλλά δεν διατηρεί μεγέθη όπως το μήκος και η γωνία.

Μια ακόμα ενδιαφέρουσα παρατήρηση, η οποία οφείλεται στον Desargues, είναι ότι αν θεωρήσουμε ότι υπάρχει ένας παρατηρητής ο οποίος βλέπει από το σημείο O δια του σημείου P, αυτός θα δει τις ευθείες l_1 και l_2 να συναντώνται στο άπειρο. Ακριβώς όπως αν φανταστούμε ότι βρισκόμαστε πάνω από τις ράγες ενός τραίνου, τότε θα τις δούμε να συναντώνται στον ορίζοντα.



Το σημείο P παίζει καθοριστικό ρόλο στη θεμελίωση της Προβολικής Γεωμετρίας, καθώς είναι το επονομαζόμενο σημείο στο άπειρο. Για την ώρα όμως πρέπει να περιοριστούμε στο να το καλούμε κύριο σημείο φυγής της προοπτικότητας p.

Παρατηρούμε ότι το σημείο P δεν είναι το μοναδικό σημείο φυγής, καθώς αν θεωρήσουμε την ευθεία τομής που δημιουργείται αν πάρουμε επίπεδο παράλληλο στο Π_1

το οποίο περιέχει το σημείο P, τότε μπορούμε να δούμε ότι κάθε σημείο σε αυτήν την ευθεία (παράλληλη της L) είναι σημείο φυγής. Έστω Q ένα σημείο φυγής, τότε σε αυτό θα αντιστοιχεί η δέσμη των παράλληλων ευθείων που τέμνουν την ευθεία L στο επίπεδο Π_1 υπό τυχαία γωνία και όχι κάθετα όπως είχαμε με τη δέσμη παράλληλων ευθειών που αντιστοιχούν στο σημείο P. Κάθε τέτοιο σημείο φυγής το ονομάζουμε διαγώνιο σημείο φυγής.

Είμαστε πλέον έτοιμοι να ξεκινήσουμε τη μελέτη της προβολικής γεωμετρίας. Θα ασχοληθούμε κυρίως με τον πραγματικό προβολικό επίπεδο καθώς αυτό είναι αρκετό ώστε αποδείξουμε τα κλασικά θεωρήματα της προβολικής γεωμετρίας και να ορίσουμε τις κωνικές τομές, όπως θα δούμε έπειτα στο Κεφάλαιο 4. Παρόλα αυτά, όπου μας δίνεται η δυνατότητα, θα δίνουμε ορισμούς, επιχειρήματα και ιδιότητες που ικανοποιούνται σε τυχαίους διανυσματικούς χώρους επί τυχαίων σωμάτων ώστε να μην περιορίσουμε τη θεωρία μας στη μελέτη του $\mathbb{R}^3$.

3.2 Προβολικός χώρος

Σε αυτή την ενότητα θα ορίσουμε τη βασική έννοια της προβολικής γεωμετρίας, τον προβολικό χώρο.

Έστω V ένας διανυσματικός χώρος επί ενός σώματος $\mathbb{F}$. Συμβολίζουμε με $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ την πολλαπλασιαστική ομάδα του σώματος $\mathbb{F}$.

Ορισμός 1. Ο προβολικός χώρος $\mathbb{P}(V)$ του διανυσματικού χώρου V είναι το σύνολο όλων των μονοδιάστατων υποχώρων του V.

Μπορούμε να αναδιατυπώσουμε τον παραπάνω ορισμό, αξιοποιώντας το γεγονός ότι κάθε μονοδιάστατος υπόχωρος U είναι το σύνολο των βαθμωτών πολλαπλασίων ενός μη μηδενικού διανύσματος u, δηλαδή $U = \text{span}\{u\}$. Επιπλέον γνωρίζουμε ότι $\text{span}\{u\} = \text{span}\{w\}$ αν και μόνο αν $u = \lambda w$, $\lambda \in \mathbb{F}^*$. Έτσι προκύπτει ο ακόλουθος ισοδύναμος ορισμός.

Ορισμός 2. Ο προβολικός χώρος $\mathbb{P}(V)$ είναι ο χώρος πηλίκο ${}^{V\setminus\{0\}}\!/_{\sim}$ όπου $\sim$ η σχέση ισοδυναμίας $u \sim w$ αν και μόνο αν $u = \lambda w, \lambda \in \mathbb{F}^*$

Ισοδύναμα: Θεωρούμε τη δράση της πολλαπλασιαστικής ομάδας $\mathbb{F}^*$ στον $V \setminus \{0\}$ μέσω του βαθμωτού πολλαπλασιασμού, δηλαδή $p : \mathbb{F}^* \times V \setminus \{0\} \to V \setminus \{0\}$, όπου $p(\lambda, v) = \lambda v$. Ο προβολικός χώρος είναι

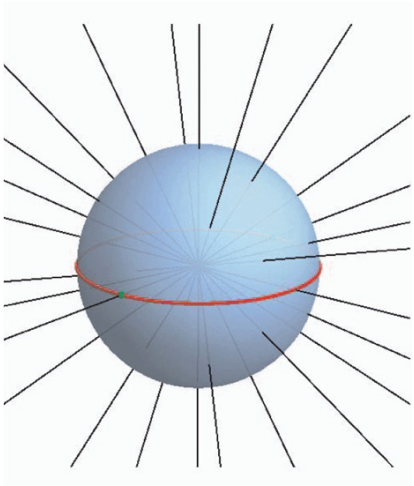
$$\mathbb{P}(V) = \mathcal{T}, \text{ όπου } \mathcal{T} = \bigcup_{x \in {}^{V-\{0\}}\!/_{\mathbb{F}^*}} t(x),$$

όπου $t(x) = \{\, p(\lambda, x) : \lambda \in \mathbb{F}^* \}$ η τροχιά του $x \in V \setminus \{0\}$ ως προς τη δράση p.

Ορισμός 3. Έστω ότι ο διανυσματικός χώρος V έχει διάσταση $n+1$. Τότε ο $\mathbb{P}(V)$ είναι ο προβολικός του χώρος και έχει διάσταση n. Αν $\dim V = 2$, τότε ο προβολικός χώρος $\mathbb{P}(V)$ έχει διάσταση 1 και καλείται προβολική ευθεία. Αν $\dim V = 3$, τότε ο προβολικός χώρος $\mathbb{P}(V)$ έχει διάσταση 2 και καλείται προβολικό επίπεδο.

Εφαρμογή 1. Για να πάρουμε μια πιο διαισθητική άποψη θα μελετήσουμε τον διανυσματικό χώρο $\mathbb{R}^{n+1}$. Ο προβολικός του χώρος, τον οποίο μπορούμε να συμβολίσουμε και με $\mathbb{RP}^n$, είναι το σύνολο όλων των ευθειών που διέρχονται από την αρχή.

Κάθε μία από αυτές τις ευθείες τέμνει την n-διάστατη μοναδιαία σφαίρα $\mathbb{S}^n$ σε δύο αντιποδικά σημεία $\pm u$. Με αυτόν τον τρόπο μπορούμε να ορίσουμε το προβολικό χώρο $\mathbb{RP}^n$ ως τον χώρο πηλίκο $\mathbb{S}^n/\sim$, όπου η σχέση $\sim$ ταυτίζει τα αντιποδικά σημεία του $\mathbb{S}^n$. Η παραπάνω κατασκευή του προβολικού χώρου ονομάζεται σφαιρικό μοντέλο.



Εφαρμογή 2. Ένας παρόμοιος τρόπος κατασκευής του προβολικού χώρου είναι το ονομαζόμενο ημισφαιρικό μοντέλο, όπου αντί να πάρουμε ολόκληρη τη σφαίρα, θεωρούμε μόνο το άνω ή το κάτω ημισφαίριο. Σε αυτή την περίπτωση, ας θεωρήσουμε το άνω ημισφαίριο, δηλαδή το $\mathbb{S}^n_+ = \{(x_1, ..., x_n) \in \mathbb{R}^n_+ : \sum_{i=1}^n x_i^2 = 1\}$. Σε αυτήν την περίπτωση οι ευθείες που διέρχονται από την αρχή τέμνουν όλα τα σημεία του ημισφαιρίου μόνο μία φορά εκτός αν αυτά βρίσκονται στον ισημερινό, όπου τέμνουν το ημισφαίριο σε δύο αντιποδικά σημεία $\pm u$. Παρόμοια με πριν, μπορούμε να ορίσουμε τον προβολικό χώρο σαν τον χώρο πηλίκο του άνω ημισφαιρίου με τη σχέση $\sim$ που ταυτίζει τα αντιποδικά σημεία, δηλαδή $\mathbb{S}^n_+/\sim$.

Παράδειγμα 1. Θα μελετήσουμε την περίπτωση $n = 2$.

Στην περίπτωση όπου $n = 2$, έχουμε το διανυσματικό χώρο $\mathbb{R}^3$ και θέλουμε να κατασκευάσουμε τον προβολικό χώρο $\mathbb{RP}^2$ με το σφαιρικό και το ημισφαιρικό μοντέλο. Κάθε ευθεία που διέρχεται από την αρχή του $\mathbb{R}^3$ τέμνει τη μοναδιαία σφαίρα σε δύο αντιποδικά σημεία, έστω (p, q, r) και $(-p, -q, -r)$. Μπορούμε επομένως να θεωρήσουμε τον προβολικό χώρο ως το σύνολο όλων αυτών των ζευγών αντιποδικών σημείων στη μοναδιαία σφαίρα, επομένως το προβολικό σημείο $[p : q : r]$ αντιστοιχεί σε δύο σημεία το (p, q, r) και το $(-p, -q, -r)$ της μοναδιαίας τρισδιάστατης σφαίρας (χρησιμοποιούμε γραφή σε ομογενείς συντεταγμένες για την οποία θα γίνει αναφορά αργότερα. Για την ώρα μπορούμε να σκεφτούμε το σημείο ως μια απλή διατεταγμένη τριάδα συντεταγμένων το οποίο είναι ισοδύναμο με κάποιο πολλαπλάσιο του, δηλαδή [π:χ:ρ]=λ[π:χ:ρ]). Με αυτόν τον τρόπο μπορούμε να δημιουργήσουμε μια $2 - 1$ αντιστοιχία $\mathbb{S}^2 \to \mathbb{RP}^2$ που στέλνει δύο σημεία (p, q, r) και $(-p, -q, -r)$ στο προβολικό σημείο $[p : q : r]$.

Αν όμως μπορούσαμε να επιλέγουμε μοναδικό σημείο της σφαίρας το οποίο να αντιστοιχεί σε ένα προβολικό σημείο, τότε θα είχαμε μια ακόμα καλύτερη εικόνα του προβολικού επιπέδου. Δυστυχώς, δεν υπάρχει φυσικός τρόπος ώστε να πάρουμε ακριβώς τα μισά από τα σημεία της σφαίρας. Θα μπορούσαμε να θεωρήσουμε τα προβολικά σημεία $[p : q : r]$ με $r \neq 0$ ως εκείνα τα σημεία τα οποία βρίσκονται στο άνω ημισφαίριο και να τα αντιστοιχίσουμε με εκείνα τα σημεία της σφαίρας (p, q, r) ή $(-p, -q, -r)$ με $r > 0$ ή $-r > 0$. Όμως όταν $r = 0$ θα δημιουργούταν πρόβλημα, επειδή το προβολικό σημείο $[p : q : 0]$ αντιστοιχεί με το $(p, q, 0)$ και με το $(-p, -q, 0)$ της σφαίρας και δεν υπάρχει άμεσος τρόπος να επιλέξουμε ένα από τα δύο. Για να ξεπεράσουμε το παραπάνω πρόβλημα θεωρούμε τον πραγματικό προβολικό χώρο $\mathbb{RP}^2$ ως τον χώρο πηλίκο

$$\mathbb{RP}^2 = \{v \in \mathbb{S}^2 \subset \mathbb{R}^3\}/(-v \sim v).$$

Με αυτόν τον τρόπο καταφέραμε να ταυτίσουμε τα αντιποδικά σημεία της σφαίρας.

3.3 Ομογενείς συντεταγμένες

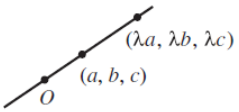
Έστω V ένας διανυσματικός χώρος διάστασης $n + 1$ επί ενός σώματος $\mathbb{F}$ και $\mathbb{P}(V)$ ο προβολικός του χώρος.

Σκοπός μας είναι να βρούμε έναν αλγεβρικό τρόπο περιγραφής ενός προβολικού χώρου. Όπως αναφέραμε ήδη, κάθε μονοδιάστατος υπόχωρος ενός διανυσματικού χώρου V είναι το σύνολο όλων των βαθμωτών πολλαπλασίων ενός μη μηδενικού διανύσματος $v \in V$. Γνωρίζουμε ότι σε ένα διανυσματικό χώρο, κάθε διάνυσμα μπορεί να γραφεί με μοναδικό τρόπο σαν πεπερασμένος γραμμικός συνδυασμός των διανυσμάτων μιας βάσης

του διανυσματικού χώρου. Επομένως, το v μπορεί να γραφεί σαν μια διατεταγμένη $(n+1)$-άδα $(x_0, \ldots, x_n)$. Οι αριθμοί x_i, $i = 0, ..., n$ ονομάζονται συντεταγμένες του διανύσματος $v \in V$.

Ορισμός 1. Αν $v \in V$ με $v = (x_0, \ldots, x_n)$, θα γράφουμε $[v] = [x_0 : \ldots : x_n]$ και θα καλούμε την τελευταία αγκύλη ομογενείς συντεταγμένες του προβολικού σημείου $[v] \in \mathbb{P}(V)$.

Παρατήρηση 1. Από τον ισοδύναμο ορισμό του προβολικού χώρου προκύπτει ότι $[\lambda x_0, \ldots, \lambda x_n] = \lambda[x_0, \ldots, x_n] = [x_0, \ldots, x_n]$ για κάθε $\lambda \in \mathbb{F}^*$. Επομένως, οι ομογενείς συντεταγμένες ενός προβολικού σημείου δεν είναι μοναδικές.



Παράδειγμα 1. Το σημείο $[2 : 0 : 6]$ του $\mathbb{RP}^2$ αποτελείται από τις συντεταγμένες $x = 2\lambda$, $y = 0$, $z = 6\lambda$ και δεν είναι παρά η ευθεία με καρτεσιανές συντεταγμένες $y = 0$, $z = 3x$ του $\mathbb{R}^3$. Επίσης παρατηρούμε ότι το προβολικό σημείο $[2 : 0 : 6] = [1 : 0 : 3]$

Οι ομογενείς συντεταγμένες μας δίνουν μια διαφορετική οπτική για τον προβολικό χώρο. Έστω

$$U_i = \{[x_0 : ... : x_n] \in \mathbb{P}(V) : x_i \neq 0\}.$$

Για $i = 0$, το $U_0 \subset \mathbb{P}(V)$ αποτελείται από εκείνα τα σημεία του προβολικού χώρου που είναι τέτοια ώστε $x_0 \neq 0$. Τότε στο U_0 ανήκουν τα σημεία

$$[x_0 : x_1 : \ldots : x_n] = \left[1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}\right] = [1 : y_1 : \ldots : y_n],$$

όπου $y_i = \frac{x_i}{x_0}$ για $i = 1, ...n$

Επομένως μπορούμε να περιγράψουμε κάθε προβολικό σημείο, το οποίο περιέχεται στο U_0 ως $[1 : y_1 : \ldots : y_n]$.

Πρόταση 1. Έστω V διανυσματικός χώρος επί ενός σώματος $\mathbb{F}$, διάστασης $n+1$. Τότε το υποσύνολο $U_0 \subset \mathbb{P}(V)$ είναι ισόμορφο με το $\mathbb{F}^n$.

Απόδειξη: Θεωρούμε τη γραμμική απεικόνιση

$$f : U_0 \to \mathbb{F}^n,$$

με

$$[x_0 : \ldots : x_n] \mapsto \left[\frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}\right].$$

.

Αυτή η απεικόνιση είναι προφανώς $1-1$ και επί και επομένως έχουμε το ζητούμενο.

□

Εστιάζουμε τώρα στο σύνολο $\mathbb{P}(V) \setminus U_0 = \{[x_0 : ... : x_n] \in \mathbb{P}(V) : x_0 = 0\}$. Όμως αυτά τα σημεία δεν είναι παρά οι μονοδιάστατοι υπόχωροι του n-διάστατου διανυσματικού υποχώρου του V, ο οποίος παράγεται από τα $v_1, \ldots v_n$ (έχουμε θεωρήσει παραπάνω ότι $\{v_i, i = 0, \ldots n\}$ είναι μια βάση του διανυσματικού χώρου V). Άρα το $\mathbb{P}(V) \setminus U_0$ δεν είναι τίποτα άλλο παρά ο προβολικός χώρος του διανυσματικού υποχώρου του διανυσματικού χώρου V, ο οποίος παράγεται από τα $v_1, \ldots v_n$ και άρα έχει διάσταση n.

Από τα παραπάνω προκύπτει ότι αν θεωρήσουμε $V = \mathbb{F}^{n+1}$, τότε έχουμε τη σημαντική σχέση

$$\mathbb{FP}^n = \mathbb{F}^n \cup \mathbb{FP}^{n-1}. \tag{3.1}$$

Παρατήρηση 2. Σημειώνουμε ότι η επιλογή του $i = 0$ δεν επηρεάζει το αποτέλεσμα. Δηλαδή για οποιαδήποτε επιλογή του $i = 0, \ldots, n$ έχουμε ότι $U_i \cong \mathbb{F}^n$ και $\mathbb{FP}^n \setminus U_i = \mathbb{FP}^{n-1}$

Παρατήρηση 3. Από τον ορισμό των $U_i, i = 0, ..., n$ προκύπτει

$$\mathbb{FP}^n = \bigcup_{i=0}^{n} U_i.$$

Παράδειγμα 2. Αν τώρα θεωρήσουμε ότι $\mathbb{F} = \mathbb{R}$, μπορούμε να γράψουμε τον προβολικό χώρο ως $\mathbb{RP}^n = \mathbb{R}^n \cup \mathbb{RP}^{n-1}$. Με βάση την παραπάνω σχέση, βλέπουμε ότι τμήμα του προβολικού χώρου $\mathbb{RP}^n$ είναι ο γνωστός Ευκλείδειος χώρος.

Έστω ότι $n = 1$. Στην περίπτωση αυτή, έχουμε ότι τα σημεία του προβολικού χώρου $\mathbb{RP}^1$ είναι της μορφής $[x : y]$. Για το U_0 έχουμε ότι περιέχει εκείνα τα σημεία του προβολικού χώρου, τα οποία έχουν μη μηδενική πρώτη συντεταγμένη και άρα μπορούν να γραφούν στη μορφή $[1 : \frac{x}{y}]$. Με βάση όσα είπαμε παραπάνω, έχουμε ότι αυτά τα σημεία είναι σε $1-1$ και επί αντιστοιχία με τα σημεία της ευθείας των πραγματικών αριθμών. Για τα σημεία του συνόλου $\mathbb{RP}^1 \setminus U_0$ γνωρίζουμε ότι περιέχονται στο σύνολο όλων των μονοδιάστατων διανυσματικών υποχώρων του $\mathbb{RP}^1$ και είναι της μορφής $[0 : y] = [0 : 1]$.

Επομένως ο $\mathbb{RP}^1 \setminus U_0$ περιέχει μοναδικό προβολικό σημείο. Αυτό το σημείο είναι εκείνο στο οποίο αναφερόμαστε ως σημείο ∞. Τελικά, μπορούμε να γράψουμε την προβολική ευθεία $\mathbb{RP}^1 = \mathbb{R} \cup \{\infty\}$.

Διαισθητικά, καταφέραμε να δημιουργήσουμε έναν προβολικό χώρο προσθέτοντας σε ένα διανυσματικό χώρο τα σημεία στο άπειρο. Όπως είπαμε και στην εισαγωγή, αυτό δίνει στον προβολικό χώρο ιδιότητες που ο αντίστοιχος διανυσματικός χώρος δεν έχει και αφορούν κατά κύριο λόγο τη Θεωρία Τομής (Intersection Theory) της Αλγεβρικής Γεωμετρίας.

Παρατήρηση 4. Αναφερόμενοι στο παράδειγμα 2, για $\mathbb{F} = \mathbb{R}$, μπορούμε να ορίσουμε μια τοπολογία στον προβολικό χώρο, η οποία να σχετίζεται με την Ευκλείδεια τοπολογία του $\mathbb{R}^n$ ως εξής:
Έστω ότι ο περιβάλλοντας διανυσματικός χώρος μας είναι ο $\mathbb{R}^{n+1}$ και έστω το σφαρικό μοντέλο του προβολικού χώρου ως

$$\mathbb{RP}^n = \{v \in \mathbb{S}^n \subset \mathbb{R}^{n+1}\}/(-v \sim v).$$

Επομένως, έχουμε καταφέρει να αναπαραστήσουμε τον προβολικό χώρο ως τον χώρο πηλίκο της μοναδιαίας σφαίρας ως προς μια δράση της ομάδας $\mathbb{Z}_2$, της δράσης με την οποία ταυτίζουμε τα αντιποδικά σημεία. Μπορούμε επομένως να εφοδιάσουμε τον πραγματικό προβολικό χώρο με την τοπολογία πηλίκο του χώρου που αναφέραμε. Έχουμε ότι ο πραγματικός προβολικός χώρος είναι συμπαγής, διότι η μοναδιαία σφαίρα είναι συμπαγές υποσύνολο του $\mathbb{R}^n$ και χώρος Hausdorff, ως χώρος πηλίκο ενός χώρου Hausdorff ως προς τη δράση μια πεπερασμένης και άρα συμπαγούς ομάδας. Αποδείξαμε ότι ο πραγματικός προβολικός χώρος είναι μια τοπολογική πολλαπλότητα διάστασης n.

Για γενικά σώματα $\mathbb{F}$, δεν έχουμε το ανάλογο της Ευκλείδειας τοπολογίας στον $\mathbb{F}^n$, οπότε οι παραπάνω ιδέες δεν εφαρμόζονται στη συγκεκριμένη περίπτωση. Στην αλγεβρική γεωμετρία υπάρχει παρόλα αυτά μια συνήθης τοπολογία για προβολικούς χώρους επί γενικών σωμάτων , η ονομαζόμενη τοπολογία του Zariski, η οποία όμως έχει αρκετές διαφορετικές ιδιότητες. Ειδικότερα έχει λιγότερα ανοιχτά σύνολα και δεν είναι χώρος Hausdorff, αλλά δεν θα επεκταθούμε περισσότερο σε αυτό το θέμα.

Παρατήρηση 5. Μια άλλη ενδιαφέρουσα παρατήρηση είναι ότι ενώ ο πραγματικός Ευκλείδειος χώρος δεν είναι συμπαγής, ο πραγματικός προβολικός χώρος είναι συμπαγής. Η συμπάγεια είναι μια καλή ιδιότητα, διότι μια από τις πολύ σημαντικές συνέπειές της, είναι ότι κάθε ακολουθία σημείων του πραγματικού προβολικού χώρου έχει συγκλίνουσα υπακολουθία. Επίσης, μας δείχνει ότι ο προβολικός χώρος είναι ένα

κλειστό και φραγμένο σύνολο και μάλιστα ότι είναι πλήρες, δηλαδή ότι κάθε ακολουθία Cauchy με στοιχεία του πραγματικού προβολικού χώρου συγκλίνει σε κάποιο σημείο του χώρου.

Έχοντας πλέον ορίσει τα προβολικά σημεία και έχοντας βρει έναν τρόπο να γράφουμε τις συντεταγμένες τους, μπορούμε να ορίσουμε τι είναι σχήμα σε ένα προβολικό χώρο. Ως γνωστόν, στην Ευκλείδεια Γεωμετρία ένα επίπεδο σχήμα είναι ένα σύνολο σημείων του $\mathbb{R}^2$. Προκύπτει ο παρακάτω ορισμός.

Ορισμός 2. Έστω V ένας διανυσματικός χώρος και $\mathbb{P}(V)$ ο προβολικός του χώρος. Ένα υποσύνολο του $\mathbb{P}(V)$, ονομάζεται προβολικό σχήμα του $\mathbb{P}(V)$.

Αν $V = \mathbb{R}^3$ τότε ένα προβολικό σχήμα είναι απλά ένα σύνολο ευθειών του $\mathbb{R}^3$, οι οποίες διέρχονται από την αρχή. Επομένως, ο διπλός κώνος με κορυφή το O είναι παράδειγμα ενός προβολικού σχήματος, επειδή μπορεί να κατασκευαστεί από ένα σύνολο ευθειών του $\mathbb{R}^3$ που διέρχονται από το σημείο O.

3.4 Γραμμικοί υπόχωροι

Ορισμός 1. Έστω ένας διανυσματικός χώρος V επί ενός σώματος $\mathbb{F}$ και $U \subseteq V$ ένας διανυσματικός υπόχωρός του. Ένας γραμμικός υπόχωρος (linear subspace) του προβολικού χώρου $\mathbb{P}(V)$, είναι το σύνολο όλων των μονοδιάστατων διανυσματικών υποχώρων του U. Συμβολίζουμε το σύνολο αυτό $\mathbb{P}(U)$.

Προκύπτει άμεσα από τον παραπάνω ορισμό, ότι ένας γραμμικός υπόχωρος ενός προβολικού χώρου είναι και αυτός προβολικός χώρος.

Σημειώνουμε ότι ένα προβολικό σημείο, είναι στην πραγματικότητα ένας μονοδιάστατος διανυσματικός υπόχωρος ενός διανυσματικού χώρου. Αντίστοιχα μια προβολική ευθεία είναι ένα σύνολο προβολικών σημείων. Έχει μεγάλη σημασία να μπορούμε να σκεφτόμαστε τα προβολικά σημεία όχι μόνο σαν διανυσματικούς χώρους, αλλά και σαν απλά σημεία του χώρου και αντίστοιχα τις προβολικές ευθείες ως απλές ευθείες.

Λήμμα 1. Μεταξύ δύο διαφορετικών σημείων $[u], [v] \in \mathbb{P}(V)$, διέρχεται μια και μοναδική προβολική ευθεία. Δηλαδή υπάρχει μοναδικός προβολικός χώρος διάστασης 1, ο οποίος να περιέχει τα προβολικά σημεία $[u]$ και $[v]$.

Απόδειξη: Έστω τα σημεία $[u], [v] \in \mathbb{P}(V)$, ώστε $[u] \neq [v]$. Από τη στιγμή που τα σημεία αυτά είναι διαφορετικά, τότε τα διανύσματα u και v του V είναι γραμμικώς ανεξάρτητα. Πράγματι, αν δεν ήταν τότε για αυτά τα διανύσματα θα είχαμε ότι $u = \lambda v$, $\lambda \in \mathbb{F}^*$ και τότε $[u] = [v]$. Από τη στιγμή που τα διανύσματα είναι γραμμικώς

ανεξάρτητα, παράγουν το δισδιάστατο διανυσματικό υπόχωρο $U = \text{span}\{u, v\}$ του V. Επομένως, ο προβολικός χώρος $\mathbb{P}(U)$, που είναι διάστασης 1, είναι η μοναδική προβολική ευθεία η οποία περιέχει τα σημεία $[u]$ και $[v]$.

□

Μπορούμε από τώρα να διακρίνουμε ότι προβλήματα που αφορούν ιδιότητες τομής, επιλύονται με μεγαλύτερη ευκολία σε προβολικούς χώρους αντί για διανυσματικούς χώρους, χρησιμοποιώντας την ακόλουθη πρόταση.

Πρόταση 1. Έστω V ένας διανυσματικός χώρος διάστασης 3 επί ενός σώματος $\mathbb{F}$. Τότε δύο διαφορετικές προβολικές ευθείες επί του προβολικού επιπέδου $\mathbb{P}(V)$ τέμνονται σε μοναδικό σημείο.

Απόδειξη: Έστω $\mathbb{P}(V)$ το προβολικό επίπεδο. Ορίζουμε τις δύο προβολικές ευθείες $P(U_1), P(U_2)$ όπου U_1 και U_2 είναι δύο ξένοι δισδιάστατοι διανυσματικοί υπόχωροι του V. Υπενθυμίζουμε στο σημείο αυτό τη σχέση

$$\dim V \geqslant \dim (U_1 + U_2) = \dim U_1 + \dim U_2 - \dim (U_1 \cap U_2), \tag{3.2}$$

Στόχος της απόδειξης είναι να δείξουμε ότι $\dim (U_1 \cap U_2) = 1$. Σε αυτή τη περίπτωση γνωρίζουμε ότι ο προβολικός χώρος του διανυσματικού χώρου $U_1 \cap U_2$ θα περιέχει ένα και μοναδικό σημείο (γνωρίζουμε ότι τομή διανυσματικών χώρων είναι διανυσματικός χώρος) και έτσι θα έχουμε το ζητούμενο, ότι δηλαδή δύο τυχαίες διαφορετικές προβολικές ευθείες ενός προβολικού επιπέδου τέμνονται σε μοναδικό σημείο.

Λόγω της σχέσης (3.2) προκύπτει η ανισότητα

$$3 \geqslant 2 + 2 - \dim (U_1 \cap U_2) \Rightarrow \dim (U_1 \cap U_2) \geqslant 1. \tag{3.3}$$

Εδώ χρησιμοποιούμε το γεγονός ότι οι χώροι U_1 και U_2 είναι διάστασης 2 γεγονός που μας δείχνει ότι $\dim (U_1 \cap U_2) \leq 2$. Η ισότητα ισχύει αν και μόνο αν $U_1 = U_2$. Από την υπόθεσή μας όμως, κάτι τέτοιο δεν ισχύει, διότι σε αυτή την περίπτωση οι προβολικές ευθείες θα ταυτίζονταν. Καταλήγουμε στο ότι

$$\dim (U_1 \cap U_2) < 2. \tag{3.4}$$

Από τη σχέση (3.3) και (3.4) (και από το γεγονός ότι η διάσταση ενός χώρου είναι ένας μη αρνητικός ακέραιος αριθμός) έχουμε ότι $\dim (U_1 \cap U_2) = 1$.

Έχουμε το ζητούμενο, ότι δηλαδή το μοναδικό σημείο τομής των δύο προβολικών

ευθειών U_1 και U_2 δεν είναι άλλο από τον προβολικό χώρο

$$\mathbb{P}(U_1 \cap U_2) = \{[u] = U_1 \cap U_2\}.$$

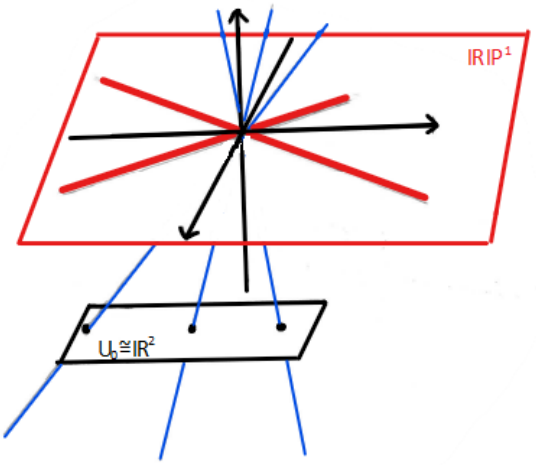
□

Η παραπάνω πρόταση στο σφαιρικό μοντέλο μεταφράζεται ως εξής: Αν θεωρήσουμε ότι ο διανυσματικός μας χώρος είναι ο $\mathbb{R}^3$, τότε δύο προβολικές ευθείες του $\mathbb{RP}^2$ είναι δύο δισδιάστατοι υποχώροι του $\mathbb{R}^3$ που τέμνουν τη μοναδιαία σφαίρα $\mathbb{S}^2$ σε δύο μέγιστους κύκλους. Αυτοί οι δύο μέγιστοι κύκλοι τέμνονται σε δύο αντιποδικά σημεία. Βάσει όμως όσων έχουμε πει, όταν ταυτίσουμε αυτά τα δύο αντιποδικά σημεία, τότε προκύπτει το μοναδικό ζητούμενο προβολικό σημείο τομής των δύο προβολικών ευθειών.

Μελετάμε τώρα την Πρόταση 1 χρησιμοποιώντας τη σχέση (3.1) για $n = 2$ και $\mathbb{F} = \mathbb{R}$. Τότε θα ισχύει

$$\mathbb{RP}^2 = \mathbb{R}^2 \cup \mathbb{RP}^1.$$

Παρατηρούμε ότι το πραγματικό προβολικό επίπεδο είναι η ένωση του $\mathbb{R}^2$ με την προβολική ευθεία $\mathbb{RP}^1$. Εξ΄ όσων έχουμε πει προηγούμενως το $\mathbb{R}^2 \cong U_0$,
όπου $U_0 = \{[x_0 : x_1 : x_2] \in \mathbb{RP}^2 : x_0 \neq 0\} \subseteq \mathbb{RP}^2$ και $\mathbb{RP}^1 = \mathbb{RP}^2 \setminus U_0$. Γεωμετρικά έχουμε



Γνωρίζουμε ότι η προβολική ευθεία $\mathbb{RP}^1$ μπορεί να εκφραστεί μέσω των ομογενών συντεταγμένων όπου $x = 0$ και άρα αντιστοιχεί στον δισδιάστατο χώρο που παράγεται από τα διανύσματα $e_2 = (0, 1, 0)$ και $e_3 = (0, 0, 1)$.

Επίσης, κάθε δισδιάστατος υπόχωρος του $\mathbb{R}^3$, όντας επίπεδο, μπορεί να περιγραφεί από την εξίσωση

$$ax + by + cz = 0, a, b, c \in \mathbb{R}.$$

Αν τώρα θεωρήσουμε ότι $x \neq 0$ και $b \neq 0$ ή $c \neq 0$, τότε η παραπάνω εξίσωση τέμνει το σύνολο $U_0 \cong \mathbb{R}^2$ στα σημεία που ικανοποιούν την εξίσωση

$$0 = a + b(y/x) + c(z/x) = a + bx_1 + cx_2.$$

Δηλαδή μια ευθεία του $\mathbb{R}^2$. Η προβολική ευθεία στο άπειρο $\mathbb{RP}^1$, παρέχει ένα σημείο παραπάνω, εκείνο όπου $x = 0$, δηλαδή το προβολικό σημείο $[0 : b : -c]$. Άρα κάθε ευθεία του $\mathbb{R}^2$ επεκτείνεται μοναδικά σε μια προβολική ευθεία του $\mathbb{RP}^2$.

Σημειώνουμε σε αυτό το σημείο προς αποφυγή σύγχυσης, ότι όποτε αναφερόμαστε σε κάποιο προβολικό σημείο, στην πραγματικότητα εννοούμε ένα μονοδιάστατο διανυσματικό χώρο.

Γνωρίζουμε ότι δύο ευθείες του $\mathbb{R}^2$ είναι παράλληλες εάν είναι της μορφής

$$a_1 + by + cz = 0, \qquad a_2 + by + cz = 0.$$

Εύκολα επαληθεύουμε ότι το γραμμικό σύστημα που προκύπτει από τις παραπάνω εξισώσεις, δεν έχει λύσεις. Παρόλα αυτά το σημείο το οποίο προσθέτουμε (βλ. σχέση (3.1», είναι το $[0 : b : -c]$ το οποίο είναι κοινό και επομένως καταλαβαίνουμε ότι οι δύο αυτές ευθείες του προβολικού επιπέδου συναντώνται σε ένα μοναδικό σημείο το οποίο ανήκει στην ονομαζόμενη ευθεία στο άπειρο $\mathbb{RP}^1$.

Ας δούμε τώρα ένα παράδειγμα υπολογισμού της εξίσωσης της ευθείας που διέρχεται μεταξύ δύο προβολικών σημείων.

Παράδειγμα 1. Έστω το πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$ και θεωρούμε επί αυτού τα προβολικά σημεία $[2 : -1 : 4]$ και $[1 : -1 : 1]$. Σκοπός μας είναι να βρούμε την εξίσωση της προβολικής ευθείας που ενώνει αυτά τα δύο σημεία. Παρατηρούμε ότι η προβολική ευθεία του $\mathbb{RP}^2$ που διέρχεται από τα προβολικά σημεία $[2 : -1 : 4]$ και $[1 : -1 : 1]$ είναι ένα επίπεδο του $\mathbb{R}^3$ που περιέχει τα διανύσματα $(2, -1, 4)$ και $(1, -1, 1) \in \mathbb{R}^3$. Παρατηρούμε ότι τα διανύσματα $(2, -1, 4)$ και $(1, -1, 1)$ είναι γραμμικώς ανεξάρητα και άρα σχηματίζουν μια βάση του επιπέδου στο οποίο ανήκουν. Ένα σημείο (x, y, z) ανήκει σε αυτό το επίπεδο αν και μόνο αν μπορεί να γραφεί ως γραμμικός συνδυασμός των $(2, -1, 4)$ και $(1, -1, 1)$, ή με άλλα λόγια αν και μόνο αν τα διανύσματα (x, y, z), $(2, -1, 4)$ και $(1, -1, 1)$ είναι γραμμικώς εξαρτημένα.

Όμως γνωρίζουμε ότι τρία διανύσματα του $\mathbb{R}^3$ είναι γραμμικώς εξαρτημένα αν και μόνο αν η 3×3 ορίζουσα που έχει για γραμμές της, τις συντεταγμένες των τριών διανυσμάτων, ισούται με 0.

Προκύπτει ότι το σημείο (x, y, z) περιέχεται στο επίπεδο το οποίο παράγεται από τα

διανύσματα $(2, -1, 4)$ και $(1, -1, 1)$ αν και μόνο αν

$$\begin{vmatrix} x & y & z \\ 2 & -1 & 4 \\ 1 & -1 & 1 \end{vmatrix} = 0.$$

Μεταφέροντας τα παραπάνω στο πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$ καταλαβαίνουμε ότι το προβολικό σημείο $[x : y : z]$ περιέχεται στην προβολική ευθεία που ενώνει τα σημεία $[2 : -1 : 4]$ και $[1 : -1 : 1]$ αν και μόνο αν

$$\begin{vmatrix} x & y & z \\ 2 & -1 & 4 \\ 1 & -1 & 1 \end{vmatrix} = 0.$$

Αναπτύσσοντας την παραπάνω ορίζουσα ως προς την πρώτη της γραμμή έχουμε ότι

$$\begin{vmatrix} x & y & z \\ 2 & -1 & 4 \\ 1 & -1 & 1 \end{vmatrix} = 3x + 2y - z,$$

συνεπώς η εξίσωση της ζητούμενης προβολικής ευθείας του $\mathbb{RP}^2$ είναι η

$$3x + 2y - z = 0.$$

Με παρόμοιο τρόπο μπορούμε να πιστοποιήσουμε πότε τρία δοσμένα προβολικά σημεία είναι συνευθειακά. Ας δούμε άλλο ένα παράδειγμα.

Παράδειγμα 2. Έστω το πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$ και θεωρούμε επί αυτού τα προβολικά σημεία $[2 : 1 : 3]$, $[1 : 2 : 1]$ και $[-1 : 4 : 3]$. Σκοπός μας είναι να εξετάσουμε αν τα παραπάνω προβολικά σημεία είναι συνευθειακά.

Το παραπάνω πρόβλημα ισοδυναμεί με το να βρούμε την εξίσωση της ευθείας που διέρχεται από οποιαδήποτε δύο από τα παραπάνω σημεία και να ελέγξουμε αν το τρίτο σημείο την ικανοποιεί. Αντί να κάνουμε όμως ολόκληρη την διαδικασία, θα μπορούσαμε απευθείας να υπολογίσουμε την 3×3 ορίζουσα, που έχει ως γραμμές της, τις συντεταγμένες των παραπάνω σημείων

$$\begin{vmatrix} 2 & 1 & 3 \\ 1 & 2 & 1 \\ -1 & 4 & 3 \end{vmatrix} = 2(-6-4) - (-3+1) + 3(4+2) = 0.$$

Επειδή η ορίζουσα ισούται με 0, τα $[2:1:3]$, $[1:2:1]$ και $[-1:4:3]$ είναι συνευθειακά.

Ας δούμε τώρα και ένα παράδειγμα εύρεσης του μοναδικού σημείου τομής δύο προβολικών ευθειών.

Παράδειγμα 3. Έστω το πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$, θεωρούμε επί αυτού τις προβολικές ευθείες με εξισώσεις $x+6y-5z=0$ και $x-2y+z=0$ αντίστοιχα.

Στο προβολικό σημείο τομής $[x:y:z]$ των δύο προβολικών ευθειών έχουμε ότι

$$\begin{cases} x+6y-5z=0 \\ x-2y+z=0 \end{cases}.$$

Αφαιρώντας την πρώτη από τη δεύτερη εξίσωση προκύπτει ότι

$$y = \frac{3}{4}z$$

και αντικαθιστώντας αυτό το αποτέλεσμα στην πρώτη εξίσωση προκύπτει

$$x = \frac{1}{2}z.$$

Συνεπώς το σημείο τομής των δυο προβολικών ευθειών με εξισώσεις $x+6y-5z=0$ και $x-2y+z=0$ είναι το $[\frac{1}{2}z:\frac{3}{4}z:z] = [2:3:4]$

3.5 Προβολικοί μετασχηματισμοί (Προβολές)

Όταν εισάγουμε στα μαθηματικά μια νέα κατηγορία μαθηματικών αντικειμένων, στη συνέχεια μας ενδιαφέρουν οι απεικονίσεις μεταξύ τους. Για παράδειγμα, με τις ομάδες ορίσαμε τους ομομορφισμούς ομάδων, με τους δακτυλίους τους ομομορφισμούς δακτυλίων, με τους τοπολογικούς χώρους θεωρήσαμε τις συνεχείς απεικονίσεις και με τους διανυσματικούς χώρους τις γραμμικές απεικονίσεις.

Προκειμένου να διατυπώσουμε τα κεντρικά αποτελέσματα της προβολικής γεωμετρίας, θα χρειαστούμε τους προβολικούς μετασχηματισμούς μέσω των οποίων δημιουργούμε απεικονίσεις από προβολικούς χώρους σε προβολικούς χώρους, μέσω αντιστρέψι-

μων γραμμικών απεικονίσεων. Έτσι μας δίνεται η δυνατότητα να συγκρίνουμε κάποια από τα χαρακτηριστικά τους, να βρούμε ομοιότητες ανάμεσα τους, κλπ.

Έχουμε ορίσει τους προβολικούς χώρους ως τα πηλίκα διανυσματικών χώρων με μια συγκεκριμένη σχέση ισοδυναμίας. Είναι φυσικό να θεωρήσουμε απεικονίσεις μεταξύ προβολικών χώρων, οι οποίες να επάγονται από γραμμικές απεικονίσεις διανυσματικών χώρων.

Έστω V, W διανυσματικοί χώροι και $T : V \to W$ μια γραμμική απεικόνιση. Τότε ένας διανυσματικός υπόχωρος $U \subseteq V$ απεικονίζεται στον διανυσματικό υπόχωρο $T(U) \subseteq W$. Αν η γραμμική απεικόνιση T έχει μη τετριμμένο πυρήνα, δηλαδή η γραμμική απεικόνιση δεν είναι $1-1$, τότε $\dim T(U) \leq \dim U$. Αν όμως $\ker T = \{0\}$ τότε $\dim T(U) = \dim U$. Ειδικότερα, αν ο U είναι μονοδιάστατος τότε και ο $T(U)$ είναι μονοδιάστατος. Η γραμμική απεικόνιση T επάγει μια καλώς ορισμένη απεικόνιση

$$\tau : \mathbb{P}(V) \to \mathbb{P}(W).$$

Ορισμός 1. Έστω V, W διανυσματικοί χώροι ίδιας διάστασης επί του σώματος $\mathbb{F}$ και $T : V \to W$ μια αντιστρέψιμη γραμμική απεικόνιση. Ένας προβολικός μετασχηματισμός ή προβολή είναι η επαγόμενη από την T απεικόνιση, $\tau : \mathbb{P}(V) \to \mathbb{P}(W)$ όπου $[v] \mapsto [T(v)]$, δηλαδή στέλνει σημεία του προβολικού χώρου του V σε σημεία του προβολικού χώρου του W. Γνωρίζουμε από την γραμμική άλγεβρα ότι κάθε αντιστρέψιμη γραμμική απεικόνιση περιγράφεται πλήρως από τον πίνακα αναπαράστασής της ως προς μια βάση του χώρου. Αν θεωρήσουμε $[T]_B$, τον πίνακα της γραμμικής απεικόνισης T ως προς τη βάση B, μπορούμε να γράψουμε για τον προβολικό μετασχηματισμό ότι $[v] \mapsto [v[T]_B]$

Παρατήρηση 1. Σημειώνουμε εδώ ότι για $\lambda \in \mathbb{F}^*$, οι λT και T ορίζουν τον ίδιο προβολικό μετασχηματισμό, επειδή

$$\tau(\lambda[v]) = [(\lambda T)(v)] = [\lambda(T(v))] = [T(v)] = \tau([v]).$$

Το αντίστροφο επίσης ισχύει, δηλαδή αν θεωρήσουμε ότι οι γραμμικοί μετασχηματισμοί T και T' ορίζουν τον ίδιο προβολικό μετασχηματισμό τ, τότε θα δείξουμε ότι ο ένας είναι το πολλαπλάσιο του άλλου.

Έστω μια βάση $\{v_0, \ldots, v_n\}$ του V. Πράγματι επειδή

$$\tau([v_i]) = [T'(v_i)] = [T(v_i)],$$

έχουμε ότι

$$T'(v_i) = \lambda_i T(v_i), \lambda_i \in \mathbb{F}^*$$

και επίσης

$$T'(\sum_{i=0}^{n} v_i) = \lambda T(\sum_{i=0}^{n} v_i), \lambda \in \mathbb{F}^*.$$

Όμως τότε

$$\sum_{i=0}^{n} \lambda T(v_i) = \lambda T(\sum_{i=0}^{n} v_i) = T'(\sum_{i=0}^{n} v_i) = \sum_{i=0}^{n} \lambda_i T(v_i).$$

Επειδή ο T είναι αντιστρέψιμος, τότε τα διανύσματα $T(v_i)$ είναι γραμμικώς ανεξάρτητα, οπότε $\lambda_i = \lambda$. Τότε $T'(v_i) = \lambda T(v_i)$ για όλα τα διανύσματα βάσης και άρα για όλα τα διανύσματα του χώρου. Οπότε προκύπτει το ζητούμενο

$$T' = \lambda T,\ \lambda \in \mathbb{F}^*.$$

Παρατήρηση 2. Μπορούμε να ελέγξουμε ότι πράγματι ο παραπάνω ορισμός είναι καλός, δηλαδή ότι ένας προβολικός μετασχηματισμός είναι καλώς ορισμένος. Θα δείξουμε ότι $\tau([u])$ είναι ανεξάρτητο από την επιλογή στοιχείου v της κλάσης ισοδυναμίας του $[u]$.

Αρχικά έχουμε ότι $[u] = [v] \Leftrightarrow u = \lambda v,\ \lambda \in \mathbb{F}^*$. Αν $u = \lambda v,\ \lambda \in \mathbb{F}^*$ τότε $T(u) = \lambda T(v)$ και άρα $[T(u)] = [\lambda T(v)] = [T(v)]$ και τελικά $\tau([u]) = \tau([v])$.

Γενικώς, ενδιαφερόμαστε για την περίπτωση όπου $V = W$. Βάσει των παραπάνω παρατηρήσεων μπορούμε να καταλάβουμε ότι η αντιστοιχία $T \mapsto \tau$ ορίζει έναν ομομορφισμό ομάδων από την $GL(V)$ (ομάδα αντιστρέψιμων μετασχηματισμών στο V) στην ομάδα των προβολικών μετασχηματισμών του $\mathbb{P}(V)$, με πράξη τη σύνθεση την οποία συμβολίζουμε με $PGL(V)$. Ο πυρήνας του παραπάνω ομομορφισμού είναι η κανονική υποομάδα της $GL(V)$ που περιέχει τα μη μηδενικά πολλαπλάσια του μοναδιαίου στοιχείου, δηλαδή του ταυτοτικού πίνακα. Λόγω του πρώτου θεωρηματος ισομορφισμού από την γραμμική άλγεβρα προκύπτει ο ακόλουθος ορισμός.

Ορισμός 2. Η ομάδα των προβολικών μετασχηματισμών του $\mathbb{P}(V)$ με πράξη τη σύνθεση είναι η

$$PGL(V) = GL(V)/\{\lambda I : \lambda \in \mathbb{F}^*\},$$

όπου με I συμβολίζουμε το μοναδιαίο στοιχείο της ομάδας $GL(V)$ δηλαδή την ταυτοτική απεικόνιση (μοναδιαίος πίνακας).

Ειδικότερα, αν $V = \mathbb{F}^{n+1}$, τότε μπορούμε να γράψουμε την ομάδα $PGL(V)$ ως $PGL(n+1, \mathbb{F})$.

Παράδειγμα 1. Θα δείξουμε ότι η απεικόνιση $\tau : \mathbb{RP}^2 \to \mathbb{RP}^2$ με τύπο

$$[x : y : z] \mapsto [2x + z : -x + 2y - 3z : x - y + 5z]$$

είναι ένας προβολικός μετασχηματισμός και θα υπολογίσουμε την εικόνα της στο προβολικό σημείο της $[2 : 3 : 5]$

Παρατηρούμε ότι η απεικόνιση τ είναι της μορφής $[x : y : z] \mapsto A[x : y : z]$ όπου A ο 3×3 πίνακας

$$A = \begin{pmatrix} -2 & 0 & 1 \\ -1 & 2 & -3 \\ 1 & -1 & 5 \end{pmatrix}$$

.

Υπολογίζουμε τώρα την ορίζουσα του A και έχουμε

$$\det A = \begin{vmatrix} -2 & 0 & 1 \\ -1 & 2 & -3 \\ 1 & -1 & 5 \end{vmatrix} = 2(10 - 3) + (1 - 2) = 13 \neq 0.$$

Συνεπώς, ο πίνακας A είναι ο αντιστρέψιμος πίνακας αναπαράστασης της γραμμικής απεικόνισης $T : \mathbb{R}^3 \to \mathbb{R}^3$ και άρα από αυτήν επάγεται ο προβολικός μετασχηματισμός $\tau : \mathbb{RP}^2 \to \mathbb{RP}^2$ με

$$[x : y : z] \mapsto [2x + z : -x + 2y - 3z : x - y + 5z].$$

Επίσης, $[2 : 3 : 5] \mapsto [9 : -11 : 24]$

Παράδειγμα 2. Μελετάμε τώρα τους μετασχηματισμούς του Möbius ως προβολικούς μετασχηματισμούς

$$\tau : \mathbb{CP}^1 \to \mathbb{CP}^1.$$

Περιγράφουμε τα σημεία του $\mathbb{CP}^1$ με ομογενείς συντεταγμένες ως $[z_0 : z_1]$ και έχουμε ότι η τ στέλνει ένα σημείο του $\mathbb{CP}^1$ σε ένα άλλο σημείο του $\mathbb{CP}^1$, δηλαδή $[z_0 : z_1] \mapsto [az_0 + bz_1 : cz_0 + dz_1]$ όπου $ad - bc \neq 0$ (αν ήταν $ad - bc = 0$, τότε η ορίζουσα του πίνακα της γραμμικής απεικόνισης θα ήταν 0 και άρα δεν θα ήταν αντι-

στρέψιμη). Ο γραμμικός μετασχηματισμός που αντιστοιχεί στον παραπάνω προβολικό μετασχηματισμό είναι ο $T : \mathbb{C}^2 \to \mathbb{C}^2$ και ο πίνακάς του ως προς τη συνήθη βάση του $\mathbb{C}^2$, $B = \{(1,0),(0,1),(i,0),(0,i)\}$, είναι ο

$$[T]_B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Έστω ότι το σημείο του προβολικού χώρου με ομογενείς συντεταγμένες $[1:1]$ είναι το σημείο που αντιστοιχεί στο διάνυσμα: $(1,0)+(0,1)+(i,0)+(0,i) \in \mathbb{C}^2$

Έχουμε ότι $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$, όπου

$$\mathbb{C} \cong U_1 = \{[z_0 : z_1] \in \mathbb{CP}^1 : z_1 \neq 0\} = \{[z:1] : z \in \mathbb{C}\}$$

και

$$\{\infty\} = \{[z_0 : z_1] \in \mathbb{CP}^1 : z_1 = 0\} = \{[1:0]\}.$$

Επομένως αν $[z_0 : z_1] \in U_1$, τότε $[z_0 : z_1] = [z:1]$ και

$$\tau([z:1]) = [az+b, cz+d].$$

Αν επίσης $[az+b, cz+d] \in U_1$, τότε $[az+b, cz+d] = [\frac{az+b}{cz+d} : 1]$ και άρα

$$\tau([z:1]) = [az+b, cz+d] = [\frac{az+b}{cz+d} : 1],$$

η οποία είναι η συνήθης μορφή ενός μετασχηματισμού Möbius, δηλαδή για $z \in \mathbb{C}$

$$z \mapsto \frac{az+b}{cz+d}.$$

Το πλεονέκτημα της προβολικής γεωμετρίας και συγκεκριμένα για το παράδειγμα του εκτεταμένου μιγαδικού επιπέδου, είναι ότι θεωρούμε το σημείο $\infty = [1:0]$ ως ένα από τα υπόλοιπα σημεία, χωρίς να υπάρχει κάτι που να το ξεχωρίζει. Αυτό μας δίνει τη δυνατότητα απλώς να το αντικαταστήσουμε στον προβολικό μετασχηματισμό, χωρίς να το αντιμετωπίσουμε σαν κάποια οριακή περίπτωση.

Έχουμε ότι αν $cz+d=0$, μπορούμε να γράψουμε

$$\tau([z:1]) = [az+b, 0] = [1:0] = \infty$$

και αν $z_1 = 0$ δηλαδή, $z = \infty = [1 : 0]$, τότε

$$\tau([1 : 0]) = [az_0 : cz_0] = [a : c].$$

Παράδειγμα 3. Έστω διανυσματικός χώρος V επί ενός σώματος $\mathbb{F}$, ώστε $\dim V = 3$. Θεωρούμε δύο υποχώρους του $U, W \subset V$ ώστε $\dim U = \dim W = 2$. Έχουμε ότι ο προβολικός χώρος του V πρόκειται για το προβολικό επίπεδο $\mathbb{P}(V)$ και οι δύο διανυσματικοί υπόχωροι του V είναι δύο προβολικές ευθείες του, οι οποίες ανήκουν στο $\mathbb{P}(V)$. Θεωρούμε επίσης ένα προβολικό σημείο $[v] \in \mathbb{P}(V)$, τέτοιο ώστε $[v] \notin \mathbb{P}(U)$ και $[v] \notin \mathbb{P}(W)$. Σκοπός μας είναι να δείξουμε ότι για κάθε $[u] \in \mathbb{P}(U)$, η μοναδική ευθεία που συνδέει το σημείο $[v]$ με το σημείο $[u]$, τέμνει την προβολική ευθεία $\mathbb{P}(W)$ σε ένα μοναδικό σημείο $[w]$.

Έστω ο προβολικός μετασχηματισμός

$$\tau : \mathbb{P}(U) \to \mathbb{P}(W).$$

Έστω ο μονοδιάστατος υπόχωρος του V, έστω $X = \text{span}(v)$. Επειδή το $[v] \notin \mathbb{P}(W)$ τότε $v \notin W$ και άρα έχουμε ότι $X \cap W = \emptyset$, συνεπώς

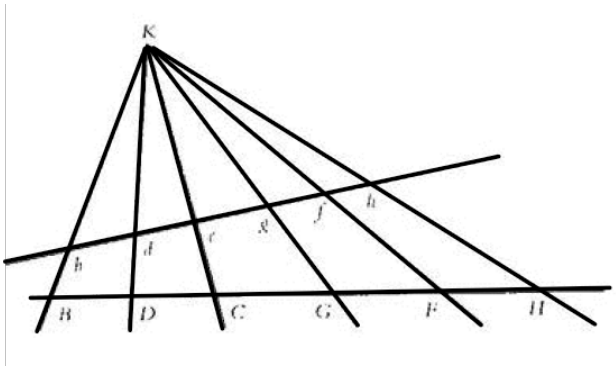
$$V = X \oplus W. \tag{3.5}$$

Λόγω της (3.5) έχουμε ότι το διάνυσμα $u \in U \Rightarrow u \in V$ μπορεί να εκφραστεί κατά μοναδικό τρόπο ως το άθροισμα $u = x + w, x \in X, w \in W$.

Η προβολική ευθεία που ενώνει τα προβολικά σημεία $[v]$ και $[u]$, ορίζεται ως ο δισδιάστατος διανυσματικός υπόχωρος του V που παράγεται από τα διανύσματα v και u και άρα $w = u - x$, δηλαδή το προβολικό σημείο $[w]$ ανήκει στην παραπάνω προβολική ευθεία. Ορίζουμε $[w] = \tau([u]) = [u - x]$, επειδή $x \in X = \text{span}\{v\}$ έχουμε $x = \lambda v$, $\lambda \in \mathbb{F}$.

Με ορολογία γραμμικής άλγεβρας μπορούμε να πούμε ότι η απεικόνιση
$u \mapsto u - x$, είναι απλά η προβολή $P|_U : V \to W$. Εύκολα βλέπουμε ότι είναι μία $1 - 1$ και επί απεικόνιση και άρα πράγματι ο $\tau : \mathbb{P}(U) \to \mathbb{P}(W)$ είναι ένας προβολικός μετασχηματισμός που ενώνει το σημείο $[v]$ με το $[u]$ και δίνει το σημείο τομής της ευθείας που παράγουν με την προβολική ευθεία $\mathbb{P}(W)$.

Το παραπάνω παράδειγμα ερμηνεύεται γεωμετρικά όταν $V = \mathbb{R}^3$ μέσω του παρακάτω σχήματος.



Μια ενδιαφέρουσα ιδιότητα των προβολικών μετασχηματισμών.

Θα μελετήσουμε τώρα μια πολύ σημαντική ιδιότητα των προβολικών μετασχηματισμών. Όπως αναφέραμε και στην ενότητα περί προοπτικής, μια προοπτικότητα p από ένα επίπεδο Π_1 σε ένα επίπεδο Π_2, απεικονίζει ευθείες σε ευθείες. Θα δείξουμε ότι την συγκεκριμένη ιδιότητα πληρούν και οι προβολικοί μετασχηματισμοί, ότι δηλαδή η εικόνα μιας προβολικής ευθείας μέσω ενός προβολικού μετασχηματισμού είναι προβολική ευθεία και ότι συνευθειακά προβολικά σημεία απεικονίζονται σε συνευθειακά.

Για χάριν ευκολίας ας θεωρήσουμε ότι ο περιβάλλοντας διανυσματικός μας χώρος είναι ο $\mathbb{R}^3$. Μια προβολική ευθεία στο πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$ είναι ένα επίπεδο του $\mathbb{R}^3$ το οποίο περιέχει το O. Σε ένα επίπεδο του $\mathbb{R}^3$ γνωρίζουμε ότι περιέχονται σημεία $(x, y, z) \in \mathbb{R}^3$ τα οποία ικανοποιούν μια εξίσωση της μορφής

$$ax + by + cz = 0,$$

όπου τα a, b, c δεν είναι όλα μηδέν. Ισοδύναμα, μπορούμε να γράψουμε την παραπάνω σχέση στη μορφή $Cv = 0$, όπου C είναι ο μη μηδενικός πίνακας $\begin{pmatrix} a & b & c \end{pmatrix}$ και $x = \begin{pmatrix} x & y & z \end{pmatrix}^\intercal$.

Έστω ο προβολικός μετασχηματισμός

$$\tau : \mathbb{RP}^2 \to \mathbb{RP}^2, \text{ με } [v] \mapsto [Av],$$

όπου ο A είναι ένας 3×3 αντιστρέψιμος πίνακας και $[v] \in \mathbb{RP}^2$ ένα τυχαίο προβολικό σημείο. Μέσω του μετασχηματισμού τ, το $[v]$ απεικονίζεται στο προβολικό σημείο $[v'] = [Av]$. Έστω διάνυσμα v ικανοποιεί την εξίσωση $Cv = 0$, προκύπτει ότι $C(A^{-1}v') = 0 \Rightarrow (CA^{-1})v' = 0$. Επομένως, βλέπουμε ότι όποιο σημείο ανήκει στην προβολική ευθεία $Cv = 0$, απεικονίζεται σε προβολικό σημείο που ανήκει στην ευθεία $(CA^{-1})v = 0$.

Εφόσον η εικόνα μιας προβολικής ευθείας του $\mathbb{RP}^2$ είναι μια προβολική ευθεία, προκύπτει άμεσα ότι συνευθειακά σημεία του $\mathbb{RP}^2$ απεικονίζονται σε συνευθειακά.

Ας δούμε την παραπάνω ιδιότητα μέσω ενός παραδείγματος.

Παράδειγμα 4. Έστω το πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$, επί του οποίου δίνεται η προβολική ευθεία $2x + y - 3z = 0$. Θεωρούμε τον προβολικό μετασχηματισμό

$$\tau : \mathbb{RP}^2 \to \mathbb{RP}^2, \text{ με } [x : y : z] \mapsto [x + z : x + y + 3z : -2x + z]$$

και θέλουμε να βρούμε την εικόνα της παραπάνω ευθείας μέσω του προβολικού μετασχηματισμού τ.

Ελέγχουμε αρχικά, ότι ο παραπάνω μετασχηματισμός είναι πράγματι προβολικός, ή ισοδύναμα ότι ο πίνακας αναπαράστασης του είναι αντιστρέψιμος. Ο πίνακας αναπαράστασης, του παραπάνω μετασχηματισμού είναι ο 3×3 πίνακας

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

Υπολογίζοντας την ορίζουσά του, βλέπουμε ότι $\det A = 3 \neq 0$. Οπότε πράγματι, η παραπάνω απεικόνιση είναι ένας προβολικός μετασχηματισμός, ο οποίος αντιστοιχεί στον αντιστρέψιμο γραμμικό μετασχηματισμό $\mathbb{R}^3 \to \mathbb{R}^3$ που έχει σαν πίνακα αναπαράστασης, ως προς τη συνήθη βάση του $\mathbb{R}^3$, τον πίνακα A.

Από τα παραπάνω προκύπτει επίσης, ότι η δεδομένη εξίσωση της ευθείας μπορεί να γραφεί και στη μορφή $Cx = 0$, όπου στην προκειμένη περίπτωση έχουμε ότι
$C = \begin{pmatrix} 2 & 1 & 3 \end{pmatrix}$.

Έχουμε ότι η προβολική ευθεία $2x + y - 3z = 0$, απεικονίζεται μέσω του τ σε μια προβολική ευθεία και στόχος μας είναι να βρούμε την εξίσωση της.

Γνωρίζουμε ότι η νέα εξίσωση της ευθείας θα πρέπει να είναι της μορφής

$$(CA^{-1})x = 0.$$

Υπολογίζουμε και έχουμε ότι

$$A^{-1} = \begin{pmatrix} 1/3 & 0 & -1/3 \\ -7/3 & 1 & -2/3 \\ 2/3 & 0 & 1/3 \end{pmatrix},$$

άρα

$$CA^{-1} = \begin{pmatrix} \frac{-11}{3} & 1 & \frac{-7}{3} \end{pmatrix}.$$

Συνεπώς προκύπτει η εξίσωση της προβολικής ευθείας $\frac{-11}{3}x + y + \frac{-7}{3}z = 0$, δηλαδή $-11x + 3y - 7z = 0$.

Ένας γραμμικός μετασχηματισμός ενός n-διάστατου διανυσματικού χώρου, καθορίζεται πλήρως από τις τιμές που παίρνει σε μια βάση του. Μια παρόμοια πρόταση ισχύει και για προβολικούς χώρους. Θα πρέπει όμως να βρούμε έναν τρόπο να εκφράσουμε το ανάλογο της γραμμικής ανεξαρτησίας, με γλώσσα προβολικής γεωμετρίας. Ακριβώς αυτό πετυχαίνουμε με τον παρακάτω ορισμό.

Ορισμός 3. Έστω V ένας διανυσματικός χώρος διάστασης $n+1$ και $\mathbb{P}(V)$ ο προβολικός του χώρος. Λέμε ότι $n+2$ σημεία $[v_1], \ldots, [v_{n+2}] \in \mathbb{P}(V)$ βρίσκονται σε γενική θέση αν οι αντιπρόσωποι (διανύσματα του V, σύμφωνα με τον δεύτερο ορισμό του προβολικού χώρου που θεωρεί τα προβολικά σημεία ως κλάσεις ισοδυναμίας διανυσμάτων του χώρου) κάθε υποσυνόλου $n+1$ προβολικών σημείων από τα παραπάνω, είναι γραμμικώς ανεξάρτητα διανύσματα του χώρου V.

Αν για παράδειγμα θεωρήσουμε δύο διαφορετικά σημεία $[u], [v]$ σε μια προβολική ευθεία $\mathbb{P}(V)$, τότε αυτό σημαίνει ότι τα διανύσματα $u, v \in V$ είναι γραμμικώς ανεξάρτητα. Επειδή αν ήταν γραμμικώς εξαρτημένα θα έπρεπε να ήταν τα ίδια προβολικά σημεία. Οπότε κάθε τρία διαφορετικά σημεία βρίσκονται σε γενική θέση.

Θεώρημα 1. (Θεώρημα Γενικής Θέσης) Έστω V και W δύο διανυσματικοί χώροι διάστασης $n+1$ και $\mathbb{P}(V), \mathbb{P}(W)$ οι προβολικοί τους χώροι αντίστοιχα. Αν τα σημεία $[v_1], \ldots, [v_{n+2}] \in \mathbb{P}(V)$ και $[w_1], \ldots, [w_{n+2}] \in \mathbb{P}(W)$ βρίσκονται σε γενική θέση, τότε υπάρχει μοναδικός προβολικός μετασχηματισμός

$$\tau : \mathbb{P}(V) \to \mathbb{P}(W),$$

ώστε $\tau([v_i]) = [w_i], i = 1, \ldots, n+2$.

Απόδειξη: Από τον ορισμό της γενικής θέσης έχουμε αρχικά, ότι επειδή τα $n+2$ σημεία $[v_1], \ldots, [v_{n+2}] \in \mathbb{P}(V)$ βρίσκονται σε γενική θέση, τότε τα $v_1, \ldots, v_{n+1} \in V$ είναι $n+1$ το πλήθος, γραμμικώς ανεξάρτητα διανύσματα του V, με $\dim V = n+1$, άρα αποτελούν μια βάση του χώρου V. Τότε υπάρχουν λ_i, $i = 1, \ldots, n+1$ ώστε

$$v_{n+2} = \sum_{i=1}^{n+1} \lambda_i v_i. \tag{3.6}$$

Αν $\lambda_i = 0$ για κάποιο i, τότε από τη σχέση (3.6) έχουμε ότι

$$\lambda_1 v_1 + \ldots + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + \ldots + v_{n+2} = 0,$$

όπου $\lambda_i \neq 0$, για κάθε $i = 1, \ldots, i-1, i+1, n+1$. Επομένως προκύπτει γραμμική εξάρτηση $n+1$ διανυσμάτων, κάτι που είναι αδύνατο λόγω του Ορισμού 7, οπότε καταλαβαίνουμε ότι $\lambda_i = 0$, για κάθε $i = 1, \ldots, i-1, i+1, n+1$. Άρα έχουμε ότι κάθε ένα από τα $\lambda_i v_i$ αντιστοιχεί σε κάποιο προβολικό σημείο $x_i = [v_i]$ και επομένως μπορούμε να επιλέξουμε κατάλληλους αντιπροσώπους των κλάσεων $[v_i]$ ώστε

$$v_{n+2} = \sum_{i=1}^{n+1} v_i. \tag{3.7}$$

Εύκολα βλέπουμε επίσης, ότι δεδομένου του v_{n+2} η έκφραση (3.7) είναι μοναδική. Επειδή πάντα μπορούμε να επιλέγουμε αντιπροσώπους, ώστε ο συντελεστής του κάθε ενός από τα v_i να γίνεται το μοναδιαίο στοιχείο το σώματος.

Τώρα επαναλαμβάνουμε την ίδια διαδικασία για τα προβολικά σημεία $[w_1], \ldots, [w_{n+2}] \in \mathbb{P}(W)$ και καταλήγουμε στη σχέση

$$w_{n+2} = \sum_{i=1}^{n+1} w_i. \tag{3.8}$$

Ομοίως, τα $w_i, i = 1, \ldots, n+1$ σχηματίζουν μία βάση του $(n+1)$-διάστατου, διανυσματικού χώρου W.

Επομένως υπάρχει μοναδικός γραμμικός μετασχηματισμός $T : V \to W$ ώστε

$$v_i \mapsto w_i, \text{ για κάθε } i = 1, \ldots, n+1$$

και λόγω της γραμμικής ανεξαρτησίας των διανυσμάτων w_i προκύπτει ότι ο γραμμικός μετασχηματισμός T είναι αντιστρέψιμος.

Επίσης, από τις σχέσεις (3.7), (3.8) έχουμε

$$T(v_{n+2}) = T(\sum_{i=1}^{n+1} v_i) = \sum_{i=1}^{n+1} T(v_i) = \sum_{i=1}^{n+1} w_i = w_{n+2}.$$

Άρα ο αντιστρέψιμος γραμμικός μετασχηματισμός T επάγει έναν προβολικό μετασχηματισμό $\tau : \mathbb{P}(V) \to \mathbb{P}(W)$, τέτοιον ώστε $\tau([v_i]) = [w_i], i = 1, \ldots, n+2$.

Για να δείξουμε τώρα τη μοναδικότητα ενός τέτοιου προβολικού μετασχηματισμού θεωρούμε $T' : V \to W$ έναν άλλο αντιστρέψιμο γραμμικό μετασχηματισμό, ο οποίος να επάγει τον προβολικό μετασχηματισμό τ' που να ικανοποιεί την ίδια ιδιότητα. Τότε θα είχαμε ότι $T'(v_i) = \lambda_i w_i$ και

$$\lambda_{n+2}w_{n+2} = T'(v_{n+2}) = \sum_{i=1}^{n+1} T'(v_i) = \sum_{i=1}^{n+1} \lambda_i w_i.$$

Όμως λόγω της μοναδικότητας της σχέσης (3.8), θα πρέπει να έχουμε ότι $\frac{\lambda_i}{\lambda_{n+2}} = 1$, από όπου προκύπτει τελικά ότι $\tau' = \tau$.

□

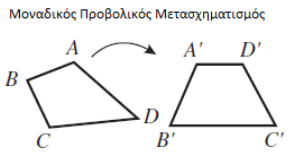
Ως εφαρμογή του Θεωρήματος Γενικής Θέσης για τυχαίο προβολικό χώρο $\mathbb{P}(V)$, θα παρουσιάσουμε το Θεμελιώδες Θεώρημα της Προβολικής Γεωμετρίας, το οποίο αποτελεί ειδική περίπτωση του Θεωρήματος Γενικής Θέσης για το πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$.

Εφαρμογή 1. (Θεμελιώδες Θεώρημα Προβολικής Γεωμετρίας) Έστω $ABCD$ και $A'B'C'D'$ δύο τετράπλευρα του πραγματικού προβολικού επιπέδου $\mathbb{RP}^2$. Τότε υπάρχει μοναδικός προβολικός μετασχηματισμός $\tau : \mathbb{RP}^2 \to \mathbb{RP}^2$ με $A \mapsto A', B \mapsto B', C \mapsto C'$ και $D \mapsto D'$.

Απόδειξη: Από τη διατύπωση του θεωρήματος καταλαβαίνουμε ότι τα σημεία A, B, C, D και A', B', C', D' βρίσκονται σε γενική θέση επί του πραγματικού προβολικού επιπέδου. Αυτό απορρέει από το γεγονός ότι τα $ABCD$ και $A'B'C'D'$ είναι τετράπλευρα, αποτρέποντας έτσι οποιαδήποτε τρία από τα τέσσερα σημεία να είναι γραμμικώς εξαρτημένα, επειδή τότε θα είχαμε τρίγωνα. Το ζητούμενο έπεται από απλή εφαρμογή του Θεωρήματος Γενικής Θέσης.

□

Ένα ενδιαφέρον πόρισμα του Θεμελιώδους Θεωρήματος της Προβολικής Γεωμετρίας, είναι ότι τα τετράπλευρα του πραγματικού προβολικού επιπέδου είναι προβολικώς ισοδύναμα. Καθώς από ένα δεδομένο τετράπλευρο, οποιοδήποτε άλλο μπορεί να προκύψει ως η εικόνα του, μέσω ενός προβολικού μετασχηματισμού.



Από το Θεμελιώδες Θεώρημα της Προβολικής Γεωμετρίας, δοθέντων τεσσάρων σημείων σε γενική θέση, υπάρχει μοναδικός προβολικός μετασχηματισμός που αντιστοιχεί τα τέσσερα σημεία στα προβολικά σημεία $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$, $[1 : 1 : 1]$.

Εφόσον η επιλογή της τετράδας σημείων είναι τυχαία (αρκεί αυτά να βρίσκονται σε γενική θέση) το παραπάνω ισχύει για οποιαδήποτε τέσσερα σημεία σε γενική θέση. Τα τρία πρώτα από τα παραπάνω προβολικά σημεία $[1:0:0]$, $[0:1:0]$, $[0:0:1]$ τα ονομάζουμε τρίγωνο αναφοράς και το $[1:1:1]$ το λέμε μοναδιαίο προβολικό σημείο. Λόγω του Θεωρήματος Γενικής Θέσης μπορούμε να γενικεύσουμε για πέντε σημεία σε προβολικούς χώρους διάτασης 3 και άρα να ορίσουμε αντίστοιχα τετράγωνο αναφοράς κλπ. Παρόλα αυτά, θα μας απασχολήσει μονάχα η περίπτωση του πραγματικού προβολικού επιπέδου.

Δύο ακόμα εφαρμογές του Θεωρήματος Γενικής Θέσης που θα αποδείξουμε είναι δύο από τα κλασικά Θεωρήματα της Προβολικής Γεωμετρίας, το Θεώρημα του Desargues και το Θεώρημα του Πάππου.

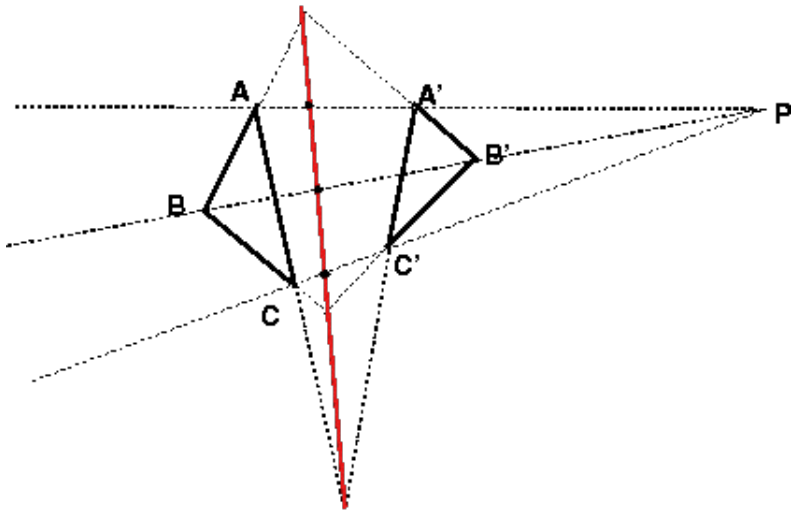
Θεώρημα 2. (Desargues) Έστω P, A, A', , B, B', C, C' επτά διαφορετικά σημεία ενός προβολικού χώρου $\mathbb{P}(V)$ έτσι ώστε οι ευθείες AA', BB', CC' να είναι διαφορετικές και να τέμνονται στο σημείο P. Τότε τα σημεία τομής $AB \cap A'B'$, $BC \cap B'C'$ και $CA \cap C'A'$ είναι συνευθειακά. Αν θεωρήσουμε δηλαδή μία προβολική ευθεία η οποία περιέχει δύο από αυτά τα σημεία, τότε θα περιέχει και το τρίτο.

Απόδειξη: Όπως και στην απόδειξη του Θεωρήματος Γενικής Θέσης, μπορούμε να επιλέξουμε αντιπροσώπους των P, A, A', B, B', C, C', δηλαδή διανύσματα του V. Έστω τα διανύσματα p, a, a', b, b', c, c' τα αντίστοιχα διανύσματα των παραπάνω προβολικών σημείων.

Εφόσον τα σημεία P, A, A' βρίσκονται στην ίδια προβολική ευθεία και είναι διαφορετικά, βρίσκονται σε γενική θέση. Επομένως τα διανύσματα a, a' είναι γραμμικώς ανεξάρτητα και το διάνυσμα p μπορεί να γραφεί στη μορφή $p = a + a'$. Αντίστοιχα, $p = b + b'$ και $p = c + c'$. Οι παραπάνω εξισώσεις υποδεικνύουν ότι $a - b = b' - a'$, άρα είναι το διάνυσμα του V που αντιστοιχεί στο προβολικό σημείο $AB \cap A'B'$. Παρόμοια $b - c$ και $c - a$ είναι τα διανύσματα του V που αντιστοιχούν στα προβολικά σημεία $BC \cap B'C'$ και $CA \cap C'A'$ αντίστοιχα.

Παρατηρούμε όμως ότι $(a - b) + (b - c) + (c - a) = 0$, επομένως τα τρία αυτά διανύσματα είναι γραμμικώς ανεξάρτητα και έτσι τα προβολικά σημεία που αντιστοιχούν σε αυτά είναι συνευθειακά, επειδή δεν βρίσκονται σε γενική θέση.

□



Αν εφαρμόσουμε το Θεώρημα του Desargues στο πραγματικό προβολικό επίπεδο, αντί για κάποιο γενικό προβολικό χώρο, τότε σχηματίζονται δύο τρίγωνα τα $\triangle ABC$ και $\triangle A'B'C'$ των οποίων τα σημεία είναι σε θέση προοπτικής ένα προς ένα, ως προς το σημείο P.

Θεώρημα 3. (Πάππου) Έστω το πραγματικό προβολικό επίπεδο $\mathbb{RP}^2$. Έστω A, B, C και A', B', C' έξι σημεία επί αυτού, τέτοια ώστε τα A, B, C να είναι συνευθειακά και τα A', B', C' να είναι επίσης συνευθειακά. Τότε τα τρία σημεία $A'B \cap AB'$, $A'C \cap AC'$ και $B'C \cap BC'$ είναι συνευθειακά.

Απόδειξη: Χωρίς βλάβη της γενικότητας επιλέγουμε τέσσερα σημεία, έστω τα A, B, C', B'. Η επιλογή αυτής της τετράδας, έγινε με μοναδικό κριτήριο τα σημεία να είναι σε γενική θέση, όπως και συμβαίνει. Πράγματι, έχοντας θεωρήσει ότι τα A, B, C είναι συνευθειακά, όπως και τα A', B', C', οδηγούμαστε στο συμπέρασμα ότι, οποιαδήποτε τυχαία επιλογή τριών εκ των τεσσάρων επιλεγμένων A, B, C', B' και αν πάρουμε, τότε τα αντίστοιχα διανύσματα τους a, b, c', $b' \in \mathbb{R}^3$ είναι γραμμικώς ανεξάρτητα. Αν δεν ήταν τότε θα είχαμε ότι δύο από τα τρία σημεία θα ταυτίζονταν και έτσι το ζητούμενο έπεται κατά προφανή τρόπο.

Εφόσον τα A, B, C', B' βρίσκονται σε γενική θέση, από το Θεώρημα Γενικής Θέσης (στην παρούσα περίπτωση Θεμελιώδες Θεώρημα Προβολικής Γεωμετρίας), μπορούμε να θεωρήσουμε ότι τα προβολικά σημεία A, B, C' να είναι το τρίγωνο αναφοράς του $\mathbb{RP}^2$ και το B' να είναι το μοναδιαίο προβολικό σημείο του $\mathbb{RP}^2$. Δηλαδή είναι

$$A = [1:0:0],\ B = [0:1:0],\ C' = [0:0:1] \text{ και } B' = [1:1:1].$$

Παρατηρούμε αρχικά ότι η ευθεία AB διέρχεται από τα προβολικά σημεία $[1:0:0]$ και $[1:1:1]$ και επομένως προκύπτει από το δισδιάστατο διανυσματικό υπόχωρο του

$\mathbb{R}^3$

$$\{(x, y, z) \in \mathbb{R}^3 : z = 0\}.$$

Άρα καταλαβαίνουμε ότι το προβολικό σημείο C, το οποίο ανήκει στην ευθεία AB, θα πρέπει να είναι της μορφής $C = [1 : c : 0]$ με $c \neq 0$ εφόσον $A \neq C$.

Παρατηρούμε επίσης, ότι η ευθεία $B'C'$ διέρχεται από τα προβολικά σημεία $[0 : 0 : 1]$ και $[1 : 1 : 1]$ και επομένως προκύπτει από τον δισδιάστατο διανυσματικό υπόχωρο του $\mathbb{R}^3$

$$\{(x, y, z) \in \mathbb{R}^3 : x = y\}.$$

Άρα καταλαβαίνουμε ότι το προβολικό σημείο A', το οποία ανήκει στην ευθεία $B'C'$, θα πρέπει να είναι της μορφής $A' = [1 : 1 : a]$, όπου $a \neq 0$ εφόσον $A' \neq B'$.

Ας δούμε τώρα τι συμβαίνει με τα σημεία τομής. Έχουμε ότι η προβολική ευθεία BC', προκύπτει από το δισδιάστατο διανυσματικό υπόχωρο

$$\{(x, y, z) \in \mathbb{R}^3 : x = 0\}.$$

Ενώ η ευθεία $B'C$, προκύπτει από το διανυσματικό υπόχωρο

$$\{(x, y, z) \in \mathbb{R}^3 : cx - y + (1 - c)z = 0\} = \text{span}\{(1, 1, 1), (1, c, 0)\}.$$

Έχουμε ότι το προβολικό σημείο τομής θα πρέπει να ανήκει στην τομή των δύο παραπάνω υποχώρων, δηλαδή θα πρέπει να είναι στοιχείο του μονοδιάστατου υποχώρου

$$\{(x, y, z) \in \mathbb{R}^3 : cx - y + (1 - c)z = 0, x = 0\} = \{(x, y, z) \in \mathbb{R}^3 : y + (1 - c)z = 0\}.$$

Θα μπορούσαμε να θεωρήσουμε ότι το προβολικό σημείο τομής με χρήση ομογενών συντεταγμένων είναι το

$$B'C \cap BC' = [0 : 1 - c : 1].$$

Παρόμοια, βρίσκουμε ότι η προβολική ευθεία $C'A$, προκύπτει από τον δισδιάστατο υπόχωρο

$$\{(x, y, z) \in \mathbb{R}^3 : y = 0\},$$

ενώ η ευθεία CA', από τον δισδιάστατο υπόχωρο

$$\{(x, y, z) \in \mathbb{R}^3 : -acx - ay + cz - z = 0\}.$$

Έχουμε ότι το προβολικό σημείο τομής θα πρέπει να ανήκει στην τομή των δύο παραπάνω υποχώρων, δηλαδή θα πρέπει να είναι στοιχείο του μονοδιάστατου υποχώρου

$$\{(x, y, z) \in \mathbb{R}^3 : -acx-ay+cz-z = 0, y = 0\} = \{(x, y, z) \in \mathbb{R}^3 : -acx+(c-1)z = 0\}.$$

Θα μπορούσαμε να θεωρήσουμε ότι το προβολικό σημείο τομής με χρήση ομογενών συντεταγμένων είναι το

$$A'C \cap AC' = [c - 1 : 0 : ac].$$

Τέλος, έχουμε ότι η προβολική ευθεία AB', προκύπτει από τον δισδιάστατο υπόχωρο

$$\{(x, y, z) \in \mathbb{R}^3 : y = z\},$$

ενώ η ευθεία $A'B$, προκύπτει από το δισδιάστατο υπόχωρο

$$\{(x, y, z) \in \mathbb{R}^3 : ax = z\}.$$

Έχουμε ότι το προβολικό σημείο τομής θα πρέπει να ανήκει στην τομή των δύο παραπάνω υποχώρων, δηλαδή θα πρέπει να είναι στοιχείο του μονοδιάστατου υποχώρου

$$\{(x, y, z) \in \mathbb{R}^3 : y = z, ax = z\}.$$

Θα μπορούσαμε να θεωρήσουμε ότι το προβολικό σημείο τομής με χρήση ομογενών συντεταγμένων είναι το

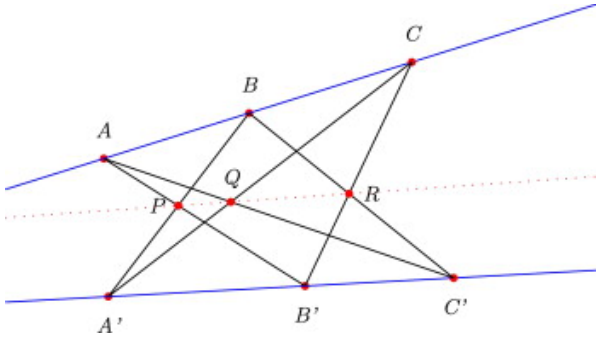
$$AB' \cap A'B = [1 : a : a].$$

Παρατηρούμε όμως ότι

$$\det\begin{pmatrix}\cdots(AB'\cap A'B)\cdots\\ \cdots(AC'\cap A'C)\cdots\\ \cdots(BC'\cap B'C)\cdots\end{pmatrix}=\begin{vmatrix}1 & a & a\\ c-1 & 0 & ac\\ 0 & 1-c & 1\end{vmatrix}$$
$$=(c-1)a-ac(1+c)-(1-c)(c-1)a=0.$$

Έπεται το ζητούμενο, δηλαδή ότι τα τρία σημεία $A'B\cap AB'$, $A'C\cap AC'$ και $B'C\cap BC'$ είναι συνευθειακά.

□



3.6 Αρχή του δυϊσμού

Σε αυτή την ενότητα θα μελετήσουμε μια πολύ ενδιαφέρουσα αντιστοιχία που υπάρχει μεταξύ προβολικών σημείων και υπερεπιπέδων ενός προβολικού χώρου. Θα δούμε ότι υπάρχει μια $1-1$ αντιστοιχία μεταξύ αυτών, η οποία είναι μεγάλης σημασίας για την προβολική γεωμετρία. Αυτή ονομάζεται αρχή του δυϊσμού.

Όπως αναφέραμε και στο κεφάλαιο των εισαγωγικών εννοιών, σε κάθε διανυσματικό χώρο V, αντιστοιχεί ένας διανυσματικός χώρος V^* τον οποίο και καλούμε δυϊκό.

Υπενθυμίζουμε ακόμα, ότι αν ο διανυσματικός χώρος V είναι ένας χώρος πεπερασμένης διάστασης με $\dim V=n$, τότε ισχύει ότι $\dim V^*=n$ και ότι σε κάθε βάση του διανυσματικού χώρου V αντιστοιχεί μια βάση του V^* και αντίστροφα.

Λαμβάνοντας υπόψη τα παραπάνω, μπορούμε να αντιστοιχίσουμε σε κάθε προβολικό χώρο $\mathbb{P}(V)$ τον $\mathbb{P}(V^*)$. Θα μελετήσουμε όμως πρώτα, τι συμβαίνει με τα σημεία του $\mathbb{P}(V^*)$ ως προς τα σημεία του $\mathbb{P}(V)$.

Από τον δεύτερο ορισμό που δώσαμε για τον προβολικό χώρο, καταλαβαίνουμε ότι ένα σημείο του $\mathbb{P}(V^*)$ είναι μια κλάση ισοδυναμίας στοιχείων του δυϊκού χώρου V^*. Έτσι αν θεωρήσουμε ένα σημείο $\varphi\in\mathbb{P}(V^*)$, τότε $\varphi\in V^*$ με $\varphi\neq 0$. Δηλαδή είναι ο επιμορφισμός $\varphi: V\to\mathbb{F}$.

Από το πρώτο Θεώρημα ισομορφισμού, έχουμε ότι $V/\ker\varphi = \operatorname{Im}\varphi$. Επειδή, είπαμε ότι η φ είναι επί, έχουμε ότι $\operatorname{Im}\varphi = \mathbb{F}$ και άρα

$$\dim V - \dim\ker\varphi = \dim\mathbb{F} \Rightarrow \dim V - 1 = \dim\ker\varphi.$$

Δεδομένου ότι τα προβολικά σημεία είναι ανεξάρτητα του βαθμωτού πολλαπλασιασμού, έχουμε δηλαδή ότι $[\varphi] = [\lambda\varphi]$, μπορούμε να καταλάβουμε ότι είτε θεωρήσουμε το γραμμικό συναρτησοειδές φ είτε το γραμμικό συναρτησοειδές $\lambda\varphi$, για κάποιο $\lambda \in \mathbb{F}^*$, τότε αυτό αντιστοιχεί στο ίδιο προβολικό σημείο και άρα προκύπτει ότι $\dim\ker\varphi = \dim\ker\lambda\varphi$. Γνωρίζουμε ότι ο πυρήνας μιας γραμμικής απεικόνισης είναι ένας διανυσματικός υπόχωρος του περιβάλλοντα διανυσματικού χώρου V. Καταλήγουμε, στο ότι ένα προβολικό σημείο $[\varphi] \in \mathbb{P}(V^*)$ ορίζει ένα διανυσματικό υπόχωρο $U \subset V$, με $\dim U = \dim V - 1$ και έτσι έναν αντίστοιχο γραμμικό υπόχωρο $\mathbb{P}(U)$ του $\mathbb{P}(V)$.

Ορισμός 1. Έστω V ένας διανυσματικός χώρος και $\mathbb{P}(V)$ ο αντίστοιχος προβολικός του χώρος. Ένα υπερεπίπεδο του προβολικού χώρου $\mathbb{P}(V)$ είναι ένας γραμμικός υπόχωρός του $\mathbb{P}(V)$ διάστασης $\dim\mathbb{P}(V) - 1$.

Θα δείξουμε, ότι υπάρχει μια αντιστοιχία μεταξύ γραμμικών υποχώρων του $\mathbb{P}(V)$ και γραμμικών υποχώρων του $\mathbb{P}(V^*)$, η οποία προκύπτει συνδέοντας τον $\mathbb{P}(U^0)$ με τον $\mathbb{P}(V)$.

Ειδικότερα μπορούμε να πούμε, ότι σημεία του $\mathbb{P}(V^*)$ αντιστοιχούν σε υπερεπίπεδα του $\mathbb{P}(V)$ και τελικά σε $n-1$-διάστατους υποχώρους του V, θεωρώντας ότι $\dim V = n$. Έχουμε άρα ότι αυτή η αντιστοιχία προκύπτει αντιστοιχώντας το $\operatorname{span}\varphi$, όπου $\varphi \in V^* - \{0\}$, με το υπερεπίπεδο $\mathbb{P}(\ker\varphi)$ που είναι γραμμικός υπόχωρος του $\mathbb{P}(V)$.

Χρησιμοποιόντας τις ομογενείς συντεταγμένες, ένα σημείο του δυϊκού προβολικού χώρου $\mathbb{P}(V^*)$, έστω το $[v_1 : \ldots : v_n]$, αντιστοιχίζεται με το υπερεπίπεδο $v_1x_1 + \ldots + v_nx_n = 0$, το οποίο είναι γραμμικός υπόχωρος του $\mathbb{P}(V)$. Ανάλογα, τα υπερεπίπεδα του $\mathbb{P}(V^*)$ αντιστοιχούν σε σημεία του $\mathbb{P}(V^{**})$, όμως λόγω του ισομορφισμού $V \cong V^{**}$, είναι το ίδιο με το να πούμε ότι τα υπερεπίπεδα του $\mathbb{P}(V^*)$ αντιστοιχούν σε σημεία του προβολικού χώρου $\mathbb{P}(V)$.

Γενικά, αν θεωρήσουμε ότι $\mathbb{P}(U)$ είναι ένας m-διάστατος γραμμικός υπόχωρος του $\mathbb{P}(V)$, τότε ο χώρος U έχει διάσταση $m+1$. Από Θεώρημα 10 στο Κεφάλαιο 2, έχουμε ότι ο U^0 έχει διάσταση $(n+1) - (m+1) = n - m$ και άρα ο προβολικός χώρος του μηδενιστή $\mathbb{P}(U^0)$ είναι ένας γραμμικός υπόχωρος του $\mathbb{P}(V^*)$ διάστασης $n - m - 1$.

Προκύπτει επομένως η ακόλουθη πρόταση που είναι γνωστή στη βιβλιογραφία ως αρχή του δυϊσμού.

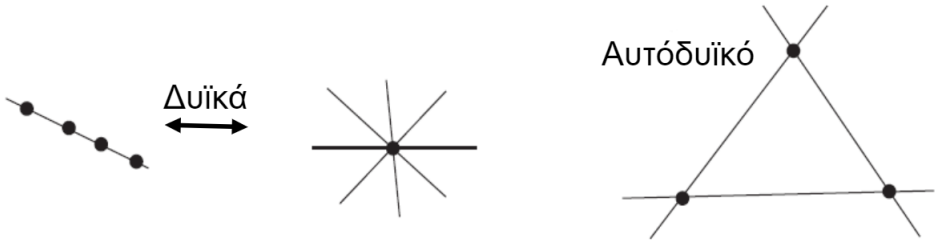
Πρόταση 1. (Αρχή του Δυϊσμού) Τα σημεία ενός δυϊκού προβολικού χώρου $\mathbb{P}(V^*)$ βρίσκονται σε $1-1$ αντιστοιχία με υπερεπίπεδα του $\mathbb{P}(V)$ και αντίστροφα.

Ισοδύναμα μπορούμε να εκφράσουμε την αρχή του δυϊσμού περιγραφικά, ως εξής:

Μια πρόταση που ικανοποιείται σε ένα προβολικό χώρο, η οποία αναφέρεται σε κάποια σχέση μεταξύ προβολικών σημείων και υπερεπιπέδων επί του προβολικού χώρου, ισχύει ακόμα και αν εναλλάξουμε τα προβολικά σημεία με υπερεπίπεδα και τα υπερεπίπεδα με προβολικά σημεία.

Συγκεκριμένα, εάν θεωρήσουμε ότι έχουμε ένα προβολικό επίπεδο, τότε ένα υπερεπίπεδο αυτού είναι μια προβολική ευθεία. Άρα η αρχή του δυϊσμού παρουσιάζει ενδιαφέρον, διότι μας δίνει τη δυνατότητα να εναλλάξουμε προβολικά σημεία με προβολικές ευθείες. Το Λήμμα 1 και η Πρόταση 1 της ενότητας 3.4, τα οποία έλεγαν ότι μεταξύ δύο προβολικών σημείων διέρχεται μοναδική προβολική ευθεία και ότι δύο διαφορετικές προβολικές ευθείες τέμνονται σε μοναδικό προβολικό σημείο, είναι λόγω της αρχής του δυϊσμού μια πρόταση και η αντίστοιχη δυϊκή της έκφραση.

Δηλαδή αν $[u]$ και $[v]$, είναι δύο σημεία επί μιας προβολικής ευθείας L, τότε οι προβολικές ευθείες $[u]^*$ και $[v]^*$ συναντώνται στο μοναδικό προβολικό σημείο L^*. Γενικότερα, ένα σύνολο συνευθειακών προβολικών σημείων αντιστοιχεί μέσω της Αρχής του Δυϊσμού σε ένα σύνολο προβολικών ευθειών που συντρέχουν σε κάποιο προβολικό σημείο, το οποίο αντιστοιχεί ΄δυϊκά' στην προβολική ευθεία που διέρχεται από το σύνολο των προβολικών σημείων.



Παρόμοια, ένα τρίγωνο είναι ένα σύνολο τριών μη συνευθειακών σημείων και των τριών ευθειών που διέρχονται από αυτά, οπότε το αντίστοιχο δυϊκό του είναι ένα σύνολο τριών ευθειών που δεν συντρέχουν σε κοινό σημείο και τα τρία σημεία στα οποία αυτές συναντώνται. Παρατηρούμε ότι το δυϊκό ενός τριγώνου είναι και πάλι ένα τρίγωνο. Τέτοιου είδους σχήματα τα ονομάζουμε αυτόδυϊκά.

Θα δούμε τώρα ως παράδειγμα μια διαφορετική έκφραση του Θεωρήματος του Desargues. Όπως έχουμε αναφέρει το θεώρημα Desargues ισχύει, δοθέντων επτά διαφορετικών σημείων επί ενός προβολικού επιπέδου $\mathbb{P}(V)$. Αν όμως το εφαρμόσουμε στο δυϊκό προβολικό επίπεδο $\mathbb{P}(V^*)$ τότε λόγω της Αρχής του Δυϊσμού τα επτά σημεία εναλλάσσονται με επτά προβολικές ευθείες και οι προβολικές ευθείες με προβολικά σημεία.

Θεώρημα 1. (Desargues, Δυϊκή Έκφραση) Έστω $\alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta$ επτά διαφορετικές προβολικές ευθείες ενός προβολικού επιπέδου $\mathbb{P}(V)$, έτσι ώστε από τα σημεία $\alpha \cap \alpha'$, $\beta \cap \beta'$, $\gamma \cap \gamma'$ να διέρχεται η προβολική ευθεία δ (είναι δηλαδή συνευθειακά). Τότε οι ευθείες που ενώνουν τα προβολικά σημεία $\alpha \cap \beta'$, $\alpha' \cap \beta$ και $\beta \cap \gamma'$, $\beta' \cap \gamma$ και $\alpha \cap \gamma'$, $\alpha' \cap \gamma$ συντρέχουν σε κοινό σημείο.

Θεώρημα 2. (Πάππου, Δυϊκή Έκφραση) Έστω ένα σύνολο τριών συντρεχουσών ευθειών α, β, γ και ένα άλλο σύνολο τριών συντρεχουσών ευθειών α', β', γ'. Τότε οι ευθείες x, y, z, που είναι οι ευθείες που διέρχονται από τα σημεία $\alpha \cap \beta', \alpha' \cap \beta$ και $\beta \cap \gamma', \beta' \cap \gamma$ και $\alpha \cap \gamma', \alpha' \cap \gamma$ αντίστοιχα, είναι συντρέχουσες.

Σημειώνουμε εδώ ότι το Θεώρημα του Πάππου, αποτελεί το ανάλογο του Θεωρήματος του Pascal (hexagrammum mysticum theorem) για εκφυλισμένες κωνικές τομές. Το θεώρημα του Pascal αποτελεί με τη σειρά του το ανάλογο του θεωρήματος Cayley-Bacharach το οποίο αφορά επίπεδες καμπύλες βαθμού 3 στο πραγματικό προβολικό επίπεδο.

Παράδειγμα 1. Σε προηγούμενο παράδειγμα είδαμε ότι αν έχουμε τρία προβολικά σημεία του πραγματικού προβολικού επιπέδου $\mathbb{RP}^2$, έστω $[a : b : c]$, $[d : e : f]$, $[l : m : n]$, τότε αυτά είναι συνευθειακά αν και μόνο αν

$$\begin{vmatrix} a & b & c \\ d & e & f \\ l & m & n \end{vmatrix} = 0.$$

Αντίστοιχα, λόγω της Αρχής του Δυϊσμού, μπορούμε να εναλλάξουμε τα τρία προβολικά σημεία σε τρεις προβολικές ευθείες και θα έχουμε ότι οι τρεις αυτές προβολικές ευθείες είναι συντρέχουσες αν και μόνο αν ορίζουσα των συντελεστών του γραμμικού συστήματος

$$\begin{cases} ax + by + cz = 0 \\ dx + ey + fz = 0 \\ lx + my + nz = 0 \end{cases}$$

ισούται με το μηδέν.

Παράδειγμα 2. Μπορούμε να αξιοποιήσουμε την Αρχή του Δυϊσμού ώστε να βγάλουμε ένα πολύ ενδιαφέρον συμπέρασμα που αφορά τον χώρο των ευθειών του Ευκλείδειου επιπέδου $\mathbb{R}^2$. Είδαμε προηγουμένως ότι μπορούμε να γράψουμε το πραγματικό προβολικό επίπεδο χρησιμοποιώντας τη σχέση $\mathbb{RP}^2 = \mathbb{R}^2 \cup \mathbb{RP}^1$. Γνωρίζουμε ότι οι προβολικές ευθείες του $\mathbb{RP}^2$ είναι σε $1-1$ αντιστοιχία με τα προβολικά σημεία του δυϊκού

πραγματικού προβολικού επιπέδου. Επομένως, βλέπουμε ότι αρκεί να αφαιρέσουμε ένα προβολικό σημείο από το δυϊκό πραγματικό προβολικό επίπεδο (το δυΙκό της ευθείας στο άπειρο) ώστε να αποκτήσουμε τον χώρο των ευθειών στο $\mathbb{R}^2$. Στο σφαιρικό μοντέλο αυτό είναι ισοδύναμο με το να αφαιρέσουμε τα αντιποδικά σημεία του βόρειου και νότιου πόλου και έπειτα να ταυτίσουμε τα εναπομένοντα αντιποδικά σημεία.

Χρησιμοποιώντας μάλιστα σφαιρικές συντεταγμένες έχουμε ότι

$$\begin{cases} x = \sin\theta \sin\varphi \\ y = \sin\theta \cos\varphi \\ z = \quad \cos\theta \end{cases}.$$

Εφόσον όμως έχουμε εξαιρέσει τα σημεία στους δύο πόλους της σφαίρας, έχουμε ότι

$$0 < \theta < \pi, \quad 0 \leq \varphi < 2\pi.$$

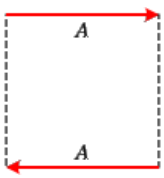
Η απεικόνιση με την οποία ταυτίζουμε τα αντιποδικά σημεία είναι η

$$\theta \mapsto \pi - \theta, \quad \varphi \mapsto \varphi + \pi.$$

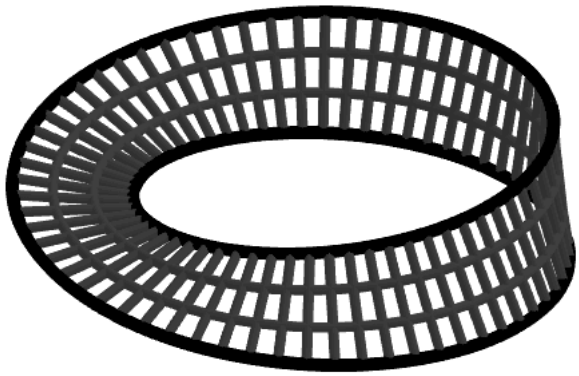
Έτσι μπορούμε να περιγράψουμε το χώρο των ευθειών στο $\mathbb{R}^2$ ως τα ζεύγη

$$(\theta, \varphi) \in (0, \pi) \times [0, \pi],$$

όπου αναγνωρίζουμε το $(\theta, 0) \sim (\pi - \theta, \pi)$.



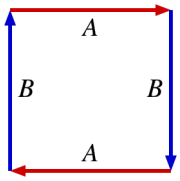
Συνεπώς προκύπτει η λωρίδα του Möbius.



Αξίζει να σημειώσουμε ότι αν δεν εξαιρέσουμε το σημείο στο άπειρο του δυϊκού πραγματικού προβολικού επιπέδου, δηλαδή την αντίστοιχη ευθεία στο άπειρο, τότε το πραγματικό προβολικό επίπεδο μπορεί να εκφραστεί ως τα ζεύγη

$$(\theta, \varphi) \in [0, \pi] \times [0, \pi],$$

όπου αναγνωρίζουμε το $(\theta, 0) \sim (\pi - \theta, \pi)$ και το $(0, \varphi) \sim (\pi, \varphi + \pi)$.



3.7 Διπλός Λόγος

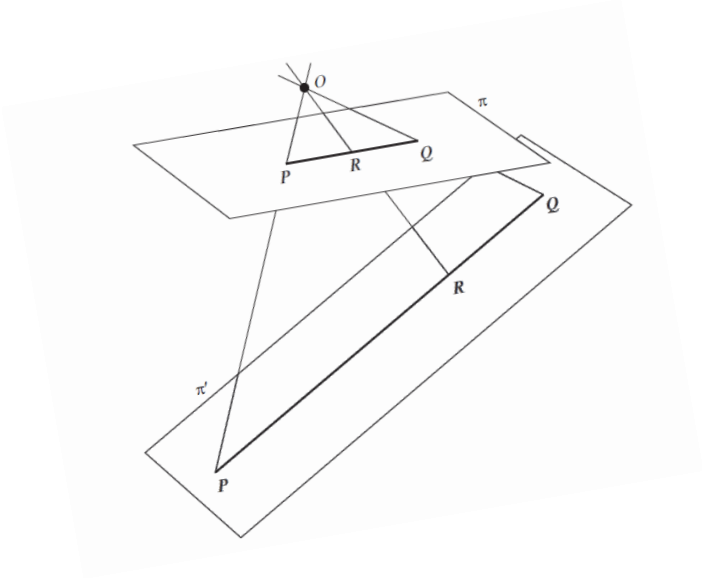
Σε αυτή την ενότητα θα περιοριστούμε στο προβολικό επίπεδο ώστε να μελετήσουμε την έννοια του διπλού λόγου.

Ο διπλός λόγος ήταν γνωστός από τον Ευκλείδη και η θεμελιώδης ιδιότητα του, ότι δηλαδή είναι αναλλοίωτη ποσότητα κάτω από τους προβολικούς μετασχηματισμούς, είχε αποδειχθεί από τον Πάππο. Από την Ευκλείδεια Γεωμετρία γνωρίζουμε ότι οι λόγοι αποστάσεων κατά μήκος μιας ευθείας είναι μια αναλλοίωτη ποσότητα. Δηλαδή αν θεωρήσουμε τρία σημεία P, Q, R επί μιας ευθείας, τότε η εικόνα της ευθείας μέσω ενός

μετασχηματισμού δεν θα επηρεάσει τον λόγο των αποστάσεων αυτών των σημείων ανά δύο.

Αντίστοιχα, δοθέντων δύο σημείων P, Q επί μιας ευθείας l, μπορούμε να προσδιορίσουμε τη θέση ενός σημείου R επί της l αν γνωρίζουμε τον λόγο $PR : RQ$. Άρα έχει νόημα να μιλάμε για το μέσο ενός ευθύγραμμου τμήματος.

Παρόλα αυτά στην προβολική γεωμετρία, τα παραπάνω δεν ισχύουν, καθώς δεν υπεισέρχεται η έννοια της απόστασης. Όπως αναφέραμε και στην παράγραφο περί προοπτικής, μια προοπτικότητα δεν διατηρεί τις αναλογίες των μηκών πάνω σε μια ευθεία, οπότε το μήκος δεν είναι μια προβολική ιδιότητα. Με τον όρο προβολική ιδιότητα εννοούμε ποσότητες που μένουν αναλλοίωτες κάτω από τη δράση της γραμμικής προβολικής ομάδας. Τα παραπάνω παρουσιάζονται από το παρακάτω σχήμα.



Παρόλα αυτά, υπάρχει μία ποσότητα που παραμένει αναλλοίωτη κάτω από τους προβολικούς μετασχηματισμούς, αυτή του διπλού λόγου. Για να δούμε πώς ορίζεται, θεωρούμε τέσσερα προβολικά σημεία ενός προβολικού επιπέδου, τα A, B, C και $D \in \mathbb{FP}^2$, με αντίστοιχα διανύσματα θέσης a, b, c, $d \in \mathbb{F}^3$. Θεωρούμε επίσης ότι τα διανύσματα αυτά είναι γραμμικώς εξαρτημένα και έτσι μπορούμε να γράψουμε τις σχέσεις

$$c = \kappa a + \lambda b \text{ και } d = \mu a + \nu b,$$

για κατάλληλους αριθμούς κ, λ, μ, $\nu \in \mathbb{F}$. Ορίζουμε τότε τον διπλό λόγο να είναι ο λόγος των λόγων λ/κ και ν/μ.

Ορισμός 1. Έστω A, B, C, D τέσσερα προβολικά σημεία του προβολικού επιπέδου $\mathbb{FP}^2$, τα οποία περιγράφονται από τα γραμμικώς εξαρτημένα διανύσματα θέσης a, b, c, $d \in \mathbb{F}^3$, έτσι ώστε

$$c = \kappa a + \lambda b \text{ και } d = \mu a + \nu b.$$

Ο διπλός λόγος των A, B, C, D ορίζεται ως $(ABCD) = \frac{\lambda}{\kappa}/\frac{\nu}{\mu} = \frac{\lambda\mu}{\kappa\nu}$.

Θα δούμε τώρα ένα παράδειγμα υπολογισμού του διπλού λόγου τεσσάρων σημείων, όπου φαίνεται ότι ο διπλός λόγος δεν εξαρτάται από από την επιλογή αντιπροσώπου για το κάθε προβολικό σημείο.

Παράδειγμα 1. Έστω $A = [1 : -1 : -1]$, $B = [1 : 3 : -2]$, $C = [3 : 5 : -5]$, $D = [1 : -5 : 0] \in \mathbb{RP}^2$. Να υπολογιστεί ο διπλός λόγος $(ABCD)$.

Επιλέγουμε ως διανύσματα ¨περιγραφής' των προβολικών σημείων τα $a = (1, -1, -1)$, $b = (1, 3, -2)$, $c = (3, 5, -5)$ και $d = (1, -5, 0)$. Υπολογίζουμε αρχικά, τους πραγματικούς αριθμούς κ, λ έτσι ώστε

$$(3, 5, -5) = \kappa(1, -1, -1) + \lambda(1, 3, -2) \Rightarrow \begin{cases} 3 = \kappa + \lambda \\ 5 = -\kappa + 3\lambda \\ 5 = -\kappa - 2\lambda \end{cases} \Rightarrow \begin{cases} \kappa = 1 \\ \lambda = 2 \end{cases}.$$

Στη συνέχεια, υπολογίζουμε τους πραγματικούς αριθμούς μ, ν που είναι τέτοιοι ώστε

$$(1, -5, 0) = \mu(1, -1, -1) + \nu(1, 3, -2) \Rightarrow \begin{cases} 1 = \mu + \nu \\ 5 = -\mu + 3\nu \\ = -\kappa - 2\lambda \end{cases} \Rightarrow \begin{cases} \mu = 2 \\ \nu = -1 \end{cases}.$$

Από τον ορισμό του διπλού λόγου έπεται ότι $(ABCD) = \frac{\lambda}{\kappa}/\frac{\nu}{\mu} = -4$.

Σε αυτό το σημείο αξίζει να παρατηρήσουμε ότι αν δεν επιλέγαμε τα διανύσματα περιγραφής να είναι τα a, b, c, d και αντί αυτών επιλέγαμε τα a', b', c', d' ώστε $a' = c_1 a$, $b' = c_2 b$, $c' = c_3 c$ και $d' = c_4 d$, όπου $c_1, c_2, c_3, c_4 \in \mathbb{R}$. τότε θα παίρναμε

$$\begin{cases} \kappa = \frac{c_3}{c_1} \\ \lambda = \frac{2c_3}{c_2} \\ \mu = \frac{2c_4}{c_1} \\ \nu = \frac{-c_4}{c_2} \end{cases}.$$

Βλέπουμε ότι και πάλι $(ABCD) = \frac{\lambda}{\kappa}/\frac{\nu}{\mu} = -4$.

Από το παρακάτω παράδειγμα διαπιστώνουμε ότι ενώ η επιλογή των ομογενών συντεταγμένων των τεσσάρων προβολικών σημείων δεν επηρεάζει την τιμή του διπλού λόγου,

η σειρά με την οποία εμφανίζονται τα σημεία στο διπλό λόγο την επηρεάζει.

Θεώρημα 1. Έστω A, B, C, D τέσσερα διαφορετικά προβολικά σημεία του προβολικού επιπέδου $\mathbb{FP}^2$, τέτοια ώστε να είναι συνεπίπεδα και ο διπλός του λόγος $(ABCD) = r$. Τότε

(i) $(BACD) = (ABDC) = \frac{1}{r}$

(ii) $(ACBD) = (DBCA) = 1 - r$

Απόδειξη: Έστω a, b, c, $d \in \mathbb{F}^3$ τα διανύσματα περιγραφής των προβολικών σημείων A, B, C, D αντίστοιχα. Έστω επίσης κ, λ, μ, $\nu \in \mathbb{F}$ ώστε

$$c = \lambda b + \kappa a \text{ και } d = \nu b + \mu a. \tag{3.9}$$

Τότε από τον ορισμό του διπλού λόγου θα έχουμε ότι $(ABCD) = \frac{\lambda}{\kappa}/\frac{\nu}{\mu} = r$.

(i) Στόχος μας είναι να προσδιορίσουμε το διπλό λόγο $(BACD)$, Ανταλλάσσουμε τις θέσεις μεταξύ των σημείων A και B και προκύπτουν οι παρακάτω σχέσεις

$$c = \lambda b + \kappa a \text{ και } d = \nu b + \mu a \tag{3.10}$$

Άρα $(BACD) = \frac{\kappa}{\lambda}/\frac{\mu}{\nu} = \frac{1}{r}$.

Παρόμοια, αν θέλουμε να υπολογίσουμε το διπλό λόγο $(ABDC)$, ανταλλάσσουμε τις θέσεις των C και D. Προκύπτουν οι παρακάτω σχέσεις:

$$d = \mu a + \nu b \text{ και } c = \kappa a + \lambda b. \tag{3.11}$$

Άρα $(ABDC) = \frac{\nu}{\mu}/\frac{\lambda}{\kappa} = \frac{1}{r}$.

(ii) Σκοπός μας είναι να υπολογίσουμε το διπλό λόγο $(ACBD)$, ανταλλάσσουμε θέσεις μεταξύ των B και C. Έχουμε τις σχέσεις

$$c = \kappa a + \lambda b \text{ και } d = \mu a + \nu b. \tag{3.12}$$

στο σημείο αυτό, θέλουμε να εκφράσουμε τα διανύσματα b και d συναρτήσει των διανυσμάτων a και c, πράγμα που πετυχαίνουμε αξιοποιώντας τις παραπάνω σχέσεις.

Χρησιμοποιώντας την πρώτη σχέση από την (3.9) και λύνοντας ως προς β έχουμε

$$b = \frac{-\kappa}{\lambda}a + \frac{1}{\lambda}c \tag{3.13}$$

Αντικαθιστώντας την (3.13) στη δεύτερη σχέση της (3.9) έχουμε

$$d = \frac{\lambda\mu - \kappa\nu}{\beta}a + \frac{\nu}{\lambda}c. \tag{3.14}$$

Με αυτόν τον τρόπο καταφέραμε να γράψουμε τα διανύσματα b και d συναρτήσει των a και c (σχέσεις (3.13),(3.14)) και έτσι τώρα μπορούμε να αξιοποιήσουμε τον ορισμό του διπλού λόγου και να βρούμε ότι

$$(ACBD) = \frac{\frac{1}{\lambda}}{\frac{-\kappa}{\lambda}} \Big/ \frac{\frac{\nu}{\lambda}}{\frac{\lambda\mu-\kappa\nu}{\lambda}} = -(\frac{\lambda\mu - \kappa\nu}{\kappa\nu}) = 1 - \frac{\lambda\mu}{\kappa\nu} = 1 - r.$$

Για το τελευταίο σκέλος της απόδειξης θέλουμε να υπολογίσουμε το διπλό λόγο $(DBCA)$, μόνο που τώρα μπορούμε να χρησιμοποιήσουμε τα παραπάνω. Θα έχουμε ότι

$$(DBCA) = (BDAC) = 1 - (BADC) = 1 - (ABCD) = 1 - r.$$

□

Έχοντας πλέον δει κάποιες από τις ιδιότητες του διπλού λόγου είμαστε πλέον σε θέση να αποδείξουμε τη βασική του ιδιότητα, ότι δηλαδή ο διπλός λόγος είναι μια προβολική ιδιότητα δηλαδή παραμένει αναλλοίωτος μέσα από τους προβολικούς μετασχηματισμούς.

Θεώρημα 2. Έστω $\tau \in PGL(2, \mathbb{F})$ και A, B, C, $D \in \mathbb{FP}^2$ τέσσερα συνευθειακά σημεία του προβολικού επιπέδου. Αν ισχύουν

$$A' = \tau(A), B' = \tau(B), C' = \tau(C) \text{ και } D' = \tau(D),$$

τότε

$$(ABCD) = (A'B'C'D').$$

Απόδειξη: Έστω $\tau : \mathbb{FP}^2 \to \mathbb{FP}^2$ με $[x] \mapsto [Mx]$ όπου $M \in GL(3, \mathbb{F})$. Αν θεωρήσουμε ότι $A = [a]$, $B = [b]$, $C = [c]$ και $D = [d]$ και $A' = [a']$, $B' = [b']$, $C' = [c']$ και $D' = [d']$, τότε από τα δεδομένα του θεωρήματος έχουμε

$$a' = Ma, b' = Mb, c' = Mc \text{ και } d' = Md.$$

Επειδή τα σημεία A, B, C, D είναι συνευθειακά, υπάρχουν κ, λ, μ, $\nu \in \mathbb{F}$ ώστε

$$c = \kappa a + \lambda b \text{ και } d = \mu a + \nu b. \tag{3.15}$$

Οπότε θα έχουμε

$$(ABCD) = \frac{\lambda}{\kappa} \Big/ \frac{\nu}{\mu}.$$

Πολλαπλασιάζοντας και τις δύο σχέσεις της (3.15) με τον πίνακα M παίρνουμε τις σχέσεις

$$c' = \kappa a' + \lambda b' \text{ και } d' = \mu a' + \nu b',$$

απ΄ όπου

$$(A'B'C'D') = \frac{\lambda}{\kappa} \Big/ \frac{\nu}{\mu},$$

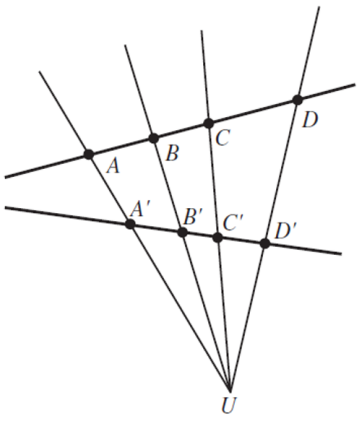
δηλαδή $(ABCD) = (A'B'C'D')$

□

Ένα άλλο πολύ σημαντικό αποτέλεσμα που μας δίνει ο διπλός λόγος είναι το παρακάτω θεώρημα. Βασιζόμενοι στο Θεώρημα 2, θα δείξουμε ότι αν τέσσερα διαφορετικά σημεία επί μιας ευθείας βρίσκονται σε προοπτική θέση με τέσσερα διαφορετικά σημειά μιας άλλης ευθείας, τότε ο διπλός λόγος της πρώτης τετράδας ισούται με τον διπλό λόγο της άλλης τετράδας.

Θεώρημα 3. Έστω A, B, C, D τέσσερα διαφορετικά σημεία μιας προβολικής ευθείας και A', B', C', D' τέσσερα διαφορετικά σημεία μιας άλλης προβολικής ευθείας έτσι ώστε οι ευθείες AA', BB', CC', DD' να συντρέχουν όλες σε σημείο U. Τότε

$$(ABCD) = (A'B'C'D').$$



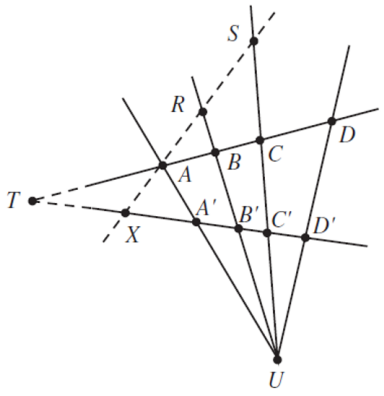
Απόδειξη: Παρατηρούμε ότι τα προβολικά σημεία B, B', C και C' βρίσκονται σε γενική θέση. Έτσι από το Θεμελιώδες Θεώρημα της Προβολικής Γεωμετρίας, γνωρίζουμε ότι υπάρχει μοναδικός προβολικός μετασχηματισμός τ, ο οποίος απεικονίζει το B στο B', το C στο C', το B' στο B και το C' στο C. Θα δείξουμε ότι $\tau(A) = A'$ και $\tau(D) = D'$ και έτσι από το παραπάνω θεώρημα θα έχουμε ότι $(ABCD) = (A'B'C'D')$.

Αρχικά παρατηρούμε ότι ο προβολικός μετασχηματισμός $\tau \circ \tau$ στέλνει τα προβολικά σημεία B στο B, C στο C, B' στο B' και C' στο C'. Από το Θεμελιώδες Θεώρημα της Προβολικής Γεωμετρίας γνωρίζουμε ότι υπάρχει μοναδικός προβολικός μετασχηματισμός που ικανοποιεί τα παραπάνω και είναι ο ταυτοτικός. Άρα $\tau \circ \tau = id$ και $\tau = \tau^{-1}$.

Στη συνέχεια, παρατηρούμε ότι ο προβολικός μετασχηματισμός τ απεικονίζει την προβολική ευθεία BC στην $B'C'$ και αντίστροφα, λόγω αυτού, το μοναδικό σημείο τομής των δύο αυτών ευθειών απεικονίζεται στον εαυτό του μέσω του τ. Αντίστοιχα, ο τ απεικονίζει την προβολική ευθεία BB' στον εαυτό της, ομοίως και την προβολική ευθεία CC'. Άρα, με το ίδιο επιχείρημα, το κοινό τους σημείο U θα πρέπει να απεικονίζεται στον εαυτό του μέσω του τ.

Ας υποθέσουμε, ότι το προβολικό σημείο X είναι η εικόνα του σημείου A, μέσω του προβολικού μετασχηματισμού τ. Τότε το σημείο X βρίσκεται πάνω στην προβολική ευθεία $B'C'$. Στόχος μας είναι να δείξουμε ότι $X = A'$.

Έστω $X \neq A'$, θα καταλήξουμε σε άτοπο. Η ευθεία AX δεν μπορεί να διέρχεται από το σημείο U, άρα θα πρέπει να τέμνει την ευθεία BB' σε ένα προβολικό σημείο R και την ευθεία CC' σε ένα προβολικό σημείο S, όπου τα σημεία R, S και U είναι διαφορετικά.



Από τα παραπάνω έχουμε ότι ο τ ισούται με τον αντίστροφό του, δηλαδή $\tau^{-1}(X) = A$, συνεπώς η προβολική ευθεία AX απεικονίζεται στον εαυτό της μέσω του τ. Αν ίσχυε όμως κάτι τέτοιο, θα σήμαινε ότι ο προβολικός μετασχηματισμός τ σταθεροποιεί τέσσερα σημεία, τα R, S, U, T. Οπότε από το Θεμελιώδες Θεώρημα της Προβολικής Γεωμετρίας θα είχαμε ότι ο τ είναι ο ταυτοτικός, πράγμα που μας οδηγεί σε άτοπο επειδή έχουμε θεωρήσει ότι οι ευθείες $ABCD$ και $A'B'C'D'$ είναι διαφορετικές. Το ζητούμενο έπεται, δηλαδή $X = A'$. Συνεπώς $\tau(A) = A'$ και με ανάλογα επιχειρήματα προκύπτει ότι $\tau(D) = D'$.

Από το Θεώρημα 2 προκύπτει τώρα το ζητούμενο, δηλαδή $(ABCD) = (A'B'C'D')$.

□

Στην Ευκλείδεια Γεωμετρία, δεδομένων δύο σημείων A και B, η αναλογία AC/BC προσδιορίζει κατά μοναδικό τρόπο το σημείο C το οποίο βρίσκεται στην ευθεία AB. Το επόμενο θεώρημα εκφράζει την ανάλογη πρόταση για την προβολική γεωμετρία. Συγκεκριμένα, αν έχουμε τρία συνευθειακά σημεία A, B, $C \in \mathbb{FP}^2$, τότε η τιμή του διπλού λόγου $(ABCD)$ προσδιορίζει κατά μοναδικό τρόπο το τέταρτο σημείο D.

Θεώρημα 4. Έστω A, B, C, D, X, Y συνευθειακά σημεία του προβολικού επιπέδου $\mathbb{FP}^2$ τέτοια ώστε

$$(ABCX) = (ABCY).$$

Τότε $X = Y$.

Απόδειξη: Έστω ότι $A = [a]$, $B = [b]$, $C = [c]$, $X = [x]$ και $Y = [y]$. Από τη στιγμή που τα προβολικά σημεία A, B, C, X, Y είναι συνευθειακά, υπάρχουν αριθμοί κ, λ, μ, ν, ξ, $\pi \in \mathbb{F}$ ώστε

$$c = \kappa a + \lambda b, \ x = \lambda a + \mu b, \ \text{και} \ y = \xi a + \pi b.$$

Τότε έχουμε

$$(ABCX) = \frac{\lambda\mu}{\kappa\nu}, \quad (ABCY) = \frac{\lambda\xi}{\kappa\pi}.$$

Επειδή $(ABCX) = (ABCY)$, έχουμε ότι

$$\frac{\mu}{\nu} = \frac{\xi}{\pi},$$

απ΄ όπου προκύπτει ότι $\xi = \frac{\mu\pi}{\nu}$. Αντικαθιστώντας αυτή τη σχέση, στη σχέση που μας δίνει το y ως γραμμικό συνδυασμό των a και b, προκύπτει ότι

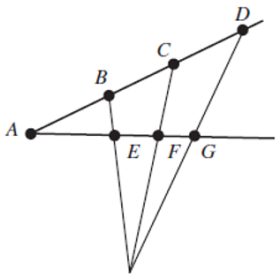
$$y = \frac{\mu\pi}{\nu}a + \pi b = \frac{\pi}{\nu}x.$$

Εφόσον έχουμε ότι το y είναι πολλαπλάσιο του x, τότε $X = Y$.

□

Στο Θεώρημα 3 δείξαμε ότι οι διπλοί λόγοι $(ABCD)$ και $(A'B'C'D')$ είναι ίσοι αν τα προβολικά σημεία A, B, C, D και A', B', C', D' βρίσκονται σε θέση προοπτικής. Το επόμενο θεώρημα περιγράφει ένα μερικώς αντίστροφο αποτέλεσμα.

Θεώρημα 5. Έστω A, B, C, D και A, E, F, G δύο σύνολα συνευθειακών προβολικών σημείων (επί διαφορετικών προβολικών ευθειών) τέτοια ώστε $(ABCD) = (AEFG)$. Τότε οι ευθείες BE, CF και DG συντρέχουν.

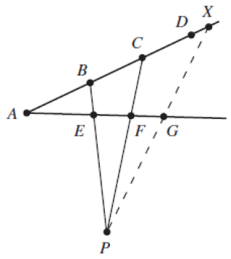


Απόδειξη: Έστω ότι P είναι το προβολικό σημείο στο οποίο συναντώνται οι ευθείες BE και CF. Έστω X το σημείο στο οποίο η ευθεία PG τέμνει την ευθεία $ABCD$. Τότε τα σημεία A, B, C και X βρίσκονται σε θέση προοπτικής από το P σε σχέση με τα A, E, F, G και άρα έχουμε ότι

$$(ABCX) = (AEFG).$$

Γνωρίζουμε όμως ότι $(ABCD) = (AEFG)$ και άρα έχουμε ότι $(ABCD) = (ABCX)$. Το ζητούμενο προκύπτει από το Θεώρημα 4 διότι έχουμε ότι θα πρέπει $X = D$. Τελικά

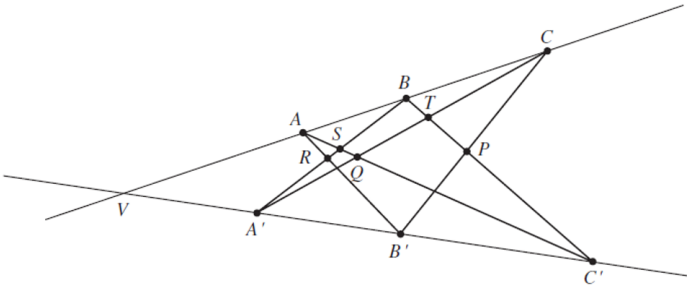
τα σημεία A, B, C, D και A, E, F, G βρίσκονται σε θέση προοπτικής ως προς το σημείο P.



□

Είμαστε πλέον σε θέση να αξιοποιήσουμε όλες τις παραπάνω ιδιότητες του διπλού λόγου και να παρουσιάσουμε την απόδειξη του Θεωρήματος του Πάππου.

Θεώρημα 6. *(*Θεώρημα του Πάππου) Έστω A, B και C τρία προβολικά επί μιας προβολικής ευθείας στο $\mathbb{FP}^2$ και A', B', C' τρία προβολικά σημεία επί μίας διαφορετικής προβολικής ευθείας. Έστω ότι οι ευθείες BC' και $B'C$ συναντώνται στο σημείο P, οι AC' και $A'C$ συναντώνται στο σημείο Q, οι AB' και $A'B$ στο σημείο R. Τότε τα σημεία P, Q και R είναι συνευθειακά.



Απόδειξη: Έστω V το κοινό σημείο των δύο προβολικών ευθειών.Έστω S το σημείο τομής των προβολικών ευθειών $A'B$, AC' και T το σημείο τομής των προβολικών ευθειών BC' και AC'.

Τα σημεία V, A', B', C' βρίσκονται σε θέση προοπτικής ως προς το σημείο A με τα σημεία B, A', R, S. Άρα λόγω του Θεώρηματος 3 προκύπτει

$$(VA'B'C') = (BA'RS) \tag{3.16}$$

Παρομοίως, τα προβολικά σημεία V, A', B', C' είναι σε θέση προοπτικής ως προς το σημείο C με τα σημεία B, T, P, C' και άρα έχουμε ότι

$$(VA'B'C') = (BTPC'). \tag{3.17}$$

Από τις σχέσεις (3.17) και (3.18) έχουμε

$$(BA'RS) = (BTPC').$$

Από το Θεώρημα 5 έχουμε ότι οι προβολικές ευθείες $A'T$, RP και SC' συντρέχουν. Μπορούμε να εκφράσουμε την παραπάνω πρόταση και ως εξής. Η προβολική ευθεία RP διέρχεται από εκείνο το προβολικό σημείο στο οποίο συναντώνται οι προβολικές ευθείες $A'T$ και SC', δηλαδή η ευθεία RP διέρχεται από το σημείο Q. Άρα τα σημεία P, Q και R είναι συνευθειακά.

□

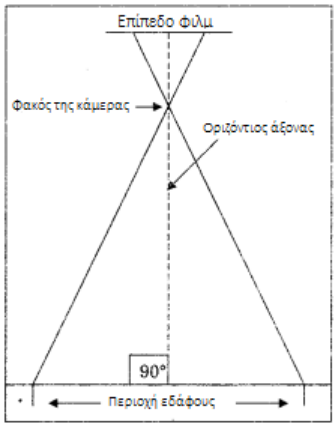
3.7.1 Μια ενδιαφέρουσα εφαρμογή του διπλού λόγου

Προηγουμένως περιγράψαμε τον τρόπο με τον οποίο η προβολική γεωμετρία μας επιτρέπει να αναπαραστήσουμε τρισδιάστατες εικόνες σε δύο μόνο διαστάσεις. Με αυτήν την εφαρμογή θα περιγράψουμε τον τρόπο με τον οποίο μπορούμε να αξιοποιήσουμε το διπλό λόγο ώστε να αντλήσουμε πληροφορίες για μια τρισδιάστατη εικόνα από την δισδιάστατη αναπαράσταση της. Θα πετύχουμε το παραπάνω μέσω του παραδείγματος της αεροφωτογραφίας.

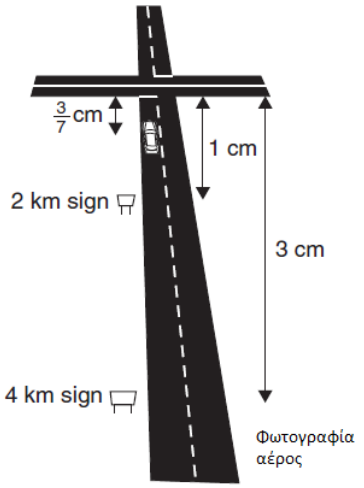
Για λόγους απλότητας, ας θεωρήσουμε ότι η φωτογραφική μηχανή καταγράφει τις φωτογραφίες σε ένα επίπεδο φιλμ, το οποίο βρίσκεται πίσω από το φακό της, έστω L (lens). Άρα αναπαριστά σε ένα επίπεδο την τρισδιάστατη εικόνα που υπάρχει μπροστά από τον φακό, όπου θεωρούμε ότι ο φακός είναι ένα σημείο. Έστω ένα σημείο στο τρισδιάστατο τοπίο, το οποίο συνδέεται μέσω μίας ευθείας με το σημείο L, τότε αυτή η ευθεία θα διέρχεται από ένα σημείο πάνω στο επίπεδο φιλμ. Με αυτόν τον τρόπο

μπορούμε να θεωρήσουμε τη διαδικασία λήψης μια εικόνας ως μια προοπτικότητα ως προς το σημείο L.

Εφόσον μέσω μιας προοπτικότητας οι ευθείες απεικονίζονται σε ευθείες (όπως έχουμε δείξει στην Ενότητα 3.1 περί προοπτικότητας), κάθε ευθεία του τρισδιάστατου τοπίου απεικονίζεται σε μια ευθεία στο επίπεδο φιλμ. Επιπρόσθετα, στην προηγούμενη ενότητα αναφέραμε ότι ο διπλός λόγος μεταξύ τεσσάρων συνευθειακών σημείων, διατηρείται μέσω μιας προοπτικότητας, επομένως ο διπλός λόγος τεσσάρων σημείων πάνω σε οποιαδήποτε ευθεία του τρισδιάστατου τοπίου, έστω l, θα πρέπει να είναι ο ίδιος και στα αντίστοιχα προοπτικά τους σημεία επί του επίπεδου φιλμ.



Για παράδειγμα, έστω ότι έχουμε φωτογραφική μηχανή η οποία φωτογραφίζει ένα αυτοκίνητο το οποίο κινείται σε ένα επίπεδο δρόμο προς μια διασταύρωση. Πριν από τη διασταύρωση υπάρχουν δύο προειδοποιητικές πινακίδες. Η μία βρίσκεται 4 χιλιόμετρα ενώ η άλλη 2 χιλιόμετρα πριν τη διασταύρωση. Στο επίπεδο φιλμ η πρώτη πινακίδα παρουσιάζεται 3 εκατοστά ενώ η δεύτερη 1 εκατοστό πριν τη διασταύρωση. Το αυτοκίνητο μάλιστα εμφανίζεται να είναι 3/7 εκατοστά πριν τη διασταύρωση. Το ερώτημα που καλούμαστε να απαντήσουμε είναι το πόσο πριν τη διασταύρωση βρίσκεται το αυτοκίνητο στο πραγματικό τρισδιάστατο τοπίο.



Θεωρούμε A να είναι η πρώτη πινακίδα, B να είναι η δεύτερη πινακίδα και C να είναι το αυτοκίνητο, επίσης με D θα συμβολίσουμε τη διασταύρωση ως προς το πραγματικό τρισδιάστατο τοπίο. Στη συνέχεια, θεωρούμε ότι A', B', C', D' είναι τα αντίστοιχα σημεία πάνω στο επίπεδο φιλμ. Έχουμε

$$(A'B'C'D') = \frac{A'C'}{C'B'} \Big/ \frac{A'D'}{D'B'} = \frac{3}{2}.$$

Έστω ότι το αυτοκίνητο βρίσκεται n χιλιόμετρα από την διασταύρωση στον πραγματικό κόσμο. Τότε θα έχουμε

$$(ABCD) = \frac{AC}{CB} \Big/ \frac{AD}{DB} = \frac{4-n}{2(2-n)}.$$

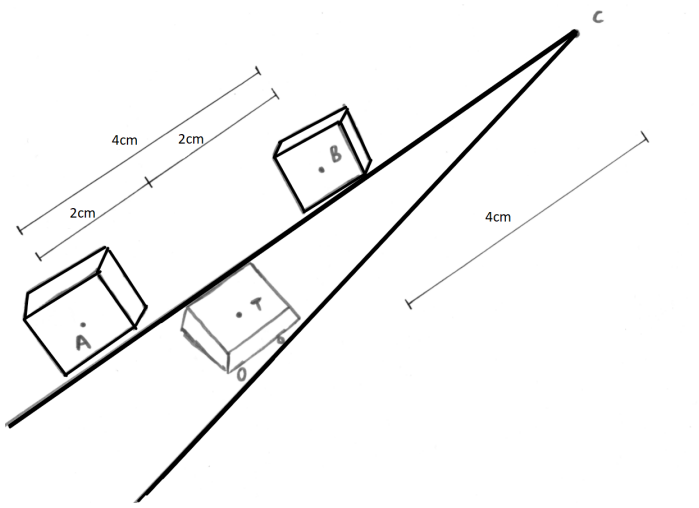
Με βάση όσα είπαμε παραπάνω θα πρέπει να έχουμε ότι $(A'B'C'D') = (ABCD)$. Βρίσκουμε ότι $n = 1$. Άρα από την αεροφωτογραφία που τραβήχτηκε μπορούμε να καταλάβουμε ότι το αυτοκίνητο βρίσκεται 1 χιλιόμετρο πριν από τη διασταύρωση.

Αν γνωρίζουμε ότι δύο ευθείες είναι παράλληλες στο πραγματικό έδαφος αλλά παρουσιάζεται να συναντώνται στο επίπεδο φιλμ, τότε το σημείο τομής τους αντιστοιχεί στο σημείο ∞. Μπορούμε και πάλι να αξιοποιήσουμε την παραπάνω διαδικασία, ακόμα και όταν ένα από τα σημεία είναι το σημείο ∞. Θυμίζουμε ότι η προβολική γεωμετρία θεωρεί τα σημεία στο άπειρο ως απλά σημεία χωρίς να τα διακρίνει σε σχέση με τα υπόλοιπα σημεία. Επομένως, μπορούμε να υπολογίσουμε τον διπλό λόγο με τον ίδιο ακριβώς τρόπο.

Θεωρούμε για παράδειγμα ότι μία φωτογραφική μηχανή, φωτογραφίζει ένα τραίνο να ταξιδεύει μεταξύ δύο σταθμών. Θεωρούμε ότι το τραίνο ταξιδεύει σε επίπεδο έδαφος,

ότι δηλαδή δεν υπάρχουν ανηφόρες ή κατηφόρες στη διαδρομή του, καθώς επίσης και ότι ταξιδεύει ευθύγραμμα. Γνωρίζουμε ότι η απόσταση των δύο σταθμών είναι 50 χιλιόμετρα, όταν όμως παρατηρούμε το επίπεδο φιλμ, δηλαδή τη συγκεκριμένη φωτογραφία, παρατηρούμε ότι οι δύο σταθμοί απέχουν μόλις 4 εκατοστά. Επίσης από την φωτογραφία βλέπουμε ότι το τραίνο είναι ακριβώς στη μέση της διαδρομής και άρα απέχει από τον σταθμό αναχώρησης του 2 εκατοστά. Τέλος βλέπουμε ότι οι δύο παράλληλες ράγες φαίνεται να συναντώνται 4 εκατοστά μετά το δεύτερο σταθμό. Καλούμαστε να υπολογίσουμε την απόσταση του τραίνου από το σταθμό του προορισμού του, στο πραγματικό τρισδιάστατο τοπίο.

Έστω ότι A είναι ο πρώτος σταθμός, B είναι ο δεύτερος σταθμός, C είναι το σημείο συνάντησης των δύο ραγών και T είναι το τραίνο ως προς το επίπεδο φιλμ. Αντίστοιχα, έχουμε τα A', B', C' και T' να είναι τα αντίστοιχα στον πραγματικό κόσμο. Η ζητούμενη ποσότητα που έχουμε να υπολογίσουμε είναι η $T'B'$.



Από τα δεδομένα μας έχουμε

$$(ATBC) = \frac{AB}{BT} \Big/ \frac{AC}{CT} = \frac{3}{2}.$$

Αν θεωρήσουμε ότι η πραγματική απόσταση του τραίνου από το δεύτερο σταθμό είναι n και επειδή το σημείο D' αντιστοιχεί στο σημείο D που είναι το σημείο στο άπειρο στο επίπεδο φιλμ έχουμε

$$(A'T'B'C') = \frac{A'B'}{B'T'} = \frac{50}{n}.$$

Γνωρίζουμε ότι η τιμή του διπλού λόγου θα διατηρείται μέσω μιας προοπτικότητας

και έτσι έχουμε ότι $(ATBC) = (A'T'B'C')$. Απ΄ όπου προκύπτει

$$\frac{50}{n} = \frac{3}{2} \Rightarrow n = \frac{100}{3}.$$

Βλέπουμε άρα ότι το τραίνο απέχει $\frac{100}{3}$ χιλιόμετρα από τον δεύτερο σταθμό. Αξίζει να σημειώσουμε, ότι ενώ το τραίνο παρουσιάζεται στα μισά της διαδρομής του μέσω του επίπεδου φιμλ, στην πραγματικότητα βρίσκεται αρκετά πιο κοντά στην αφετηρία του (δηλαδή στο τρισδιάστατο τοπίο).

Κεφάλαιο 4

Επίπεδες προβολικές καμπύλες

Σε αυτό το κεφάλαιο θα περιορίσουμε τη μελέτη των προβολικών χώρων στη μελέτη του προβολικού επιπέδου $\mathbb{FP}^2$ επί ενός σώματος $\mathbb{F}$.

Ακριβώς όπως ένα πολυώνυμο με δύο μεταβλητές $p \in \mathbb{F}[x, y]$ ορίζει μια αλγεβρική επίπεδη καμπύλη $Z(p) \subseteq \mathbb{F}^2$, θα δούμε ότι ένα ομογενές πολυώνυμο ή ομογενής μορφή, με τρεις μεταβλητές $p \in \mathbb{F}[x, y, z]$ ορίζει μια επίπεδη προβολική καμπύλη $Z(p) \subseteq \mathbb{FP}^2$. Με βάση τα παραπάνω, θα μελετήσουμε διάφορες γεωμετρικές ιδιότητες των επίπεδων προβολικών καμπυλών. Στη συνέχεια, θα επιχειρήσουμε να ταξινομήσουμε τις προβολικές κωνικές τομές. Τέλος, θα δείξουμε ότι το σύνολο των μη ιδιαζόντων σημείων μιας δεδομένης λείας καμπύλης δευτέρου βαθμού, έχει τη δομή αβελιανής ομάδας.

Τα παραπάνω έχουν μεγάλη σημασία σε ζητήματα αλγβερικής γεωμετρίας και αποτελούν το μαθηματικό υπόβαθρο για την ανάπτυξη κρυπτοσυστημάτων ελλειπτικών καμπυλών.

4.1 Ομογενή πολυώνυμα και μηδενοχώροι

Ορισμός 1. Ένα πολυώνυμο $p(x, y, z) \in \mathbb{F}[x, y, z]$ ονομάζεται ομογενές βαθμού n ή μορφή βαθμού n αν μπορεί να γραφεί στη μορφή

$$p(x, y, z) = \sum_{i+j+k=n} a_{ijk} x^i y^j z^k,$$

όπου $a_{ijk} \in \mathbb{F}$.

Ενώ συνήθως θεωρούμε ότι τουλάχιστον ένα από τα $a_{ijk} \neq 0$, σε πολλές περιπτώσεις θα μας φανεί χρήσιμο, το μηδενικό πολυώνυμο να είναι βαθμού n για κάθε $n \in \mathbb{Z}_+$.

Έστω p ένα ομογενές πολυώνυμο βαθμού n. Τότε για κάθε $k \in \mathbb{F}$, έχουμε

$$p(kx, ky, kz) = k^n \sum_{i+j+k=n} p(x, y, z). \tag{4.1}$$

Έστω ένα πολυώνυμο $p \in \mathbb{F}[x, y]$ βαθμού n

$$p(x, y) = \sum_{i+j \leq d} a_{ij} x^i y^j.$$

Τότε σε αυτό μπορούμε να αντιστοιχίσουμε ένα πολυώνυμο τριών μεταβλητών, μέσω της ονομαζόμενης ομογενοποίησης του, ώστε να είναι

$$\bar{p}(x, y, z) = \sum_{i+j \leq 0} a_i j x^i y^j z^{d-(i+j)}.$$

Η παραπάνω αντιστοιχία επάγει μία $1-1$ και επί απεικόνιση $p \mapsto \bar{p}$ μεταξύ των πολυωνύμων δύο μεταβλητών και βαθμού n και των ομογενών πολυωνύμων τριών μεταβλητών και βαθμού n. Η αντίστροφη της παραπάνω απεικόνισης είναι η $p(x, y, z) \mapsto p(x, y, 1)$.

Έστω ένα ομογενές πολυώνυμο $p(x, y, z) \in \mathbb{F}[x, y, z]$. Τότε μπορούμε να θεωρήσουμε το υποσύνολο $Z(p) \subseteq \mathbb{FP}^2$ το οποίο ισούται με

$$Z(p) = \{[x : y : z] \in \mathbb{FP}^2 : p(x, y, z) = 0\}.$$

Το παραπάνω έχει νόημα αν το $p(x, y, z) = 0$ εξαρτάται μόνο από την κλάση ισοδυναμίας $[x : y : z]$, όπως απορρέει από τη σχέση (4.1).

Ορισμός 2. Έστω ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$ με $0 \leq \deg(p)$. Καλούμε το σύνολο $Z(p) \subseteq \mathbb{FP}^2$ μηδενοχώρο του πολυωνύμου p. Ένα σύνολο $S \subseteq \mathbb{FP}^2$ που ισούται με το $Z(p)$ για κάποιο ομογενές πολυώνυμο p καλείται επίπεδη προβολική καμπύλη. Το πολυώνυμο p καλείται εξίσωση ορισμού της επίπεδης προβολικής καμπύλης S. Αν τώρα θεωρήσουμε $p \in \mathbb{F}[x, y]$ να είναι ένα μη σταθερό πολυώνυμο, ο μηδενοχώρος $Z(\bar{p}) \subseteq \mathbb{FP}^2$ της ομογενοποίησης του p καλείται προβολική πλήρωση του $Z(p) \subseteq \mathbb{F}^2$.

Παρατήρηση 1. Αξίζει να σημειώσουμε ότι η προβολική πλήρωση του $Z(p)$ εξαρτάται σε μεγάλο βαθμό από το πολυώνυμο το οποίο ορίζει το υποσύνολο $Z(p)$, δηλαδή στην πραγματικότητα δεν είναι εσωτερική ιδιότητα του συνόλου $Z(p)$. Παρατηρούμε δηλαδή ότι για κάποιο πολυώνυμο $p \in \mathbb{F}[x, y]$ έχουμε ότι $\bar{p}(x, y, 1) = p(x, y)$, οπότε το σημείο $(x, y) \in Z(p)$ αν και μόνο αν το προβολικό σημείο $[x : y : 1] \in \mathbb{FP}^2$,

ανήκει στο σύνολο $Z(\bar{p})$. Δηλαδή έχουμε τη σχέση

$$Z(\bar{p}) \cap \mathbb{F}^2 = Z(p).$$

Παρατήρηση 2. Αν θεωρήσουμε τώρα ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$, τότε το $p(x, y, 0) \in \mathbb{F}[x, y]$ είναι ομογενές. Έχουμε ότι

$$Z(p) \cap \mathbb{FP}^1 = \{[x : y] \in \mathbb{FP}^1 : p(x, y, 0) = 0\}.$$

4.2 Λεία και ιδιάζοντα σημεία

Ορισμός 1. Έστω ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$ και $P \in Z(p)$. Καλούμε το P λείο σημείο του $Z(p)$ εάν $p_x^2(P) + p_y^2(P) + p_z^2(P) \neq 0$, δηλαδή όταν τουλάχιστον μία από τις μερικές παραγώγους έχει μη μηδενική τιμή στο σημείο P. Διαφορετικά, καλούμε το P ιδιάζον σημείο του $Z(p)$ εάν $p_x(P) = p_y(P) = p_z(P) = 0$. Συμβολίζουμε το υποσύνολο του $Z(p)$ που περιέχει τα λεία σημεία με $Z(p)^{\text{sm}}$, ενώ το υποσύνολο του $Z(p)$ που περιέχει τα ιδιάζοντα σημεία ως $Z(p)^{\text{sing}}$. Αν για κάποιο ομογενές πολυώνυμο έχουμε ότι $Z(p)^{\text{sing}}(\bar{\mathbb{F}}) = \emptyset$, τότε ονομάζουμε αυτό το πολυώνυμο λείο και κατ΄ επέκταση η επίπεδη προβολική καμπύλη που ορίζεται από αυτό ονομάζεται λεία. Όπου $\bar{\mathbb{F}}$ είναι οποιαδήποτε επέκταση του σώματος $\mathbb{F}$.

Παρατήρηση 1. Παρατηρούμε ότι ένα ομογενές πολυώνυμο ονομάζεται λείο αν και μόνο αν $\nabla p|_{P \in Z(p)} \neq \vec{0}$.

Λήμμα 1. Έστω ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$, με $\deg(p) = n$. Έχουμε

$$dp = x\frac{\partial p}{\partial x} + y\frac{\partial p}{\partial y} + z\frac{\partial p}{\partial z}.$$

Συνεπάγεται ότι αν $n \neq 0$ και $\mathbb{F}$ είναι ένα οποιοδήποτε σώμα χαρακτηριστικής μηδέν, τότε ένα σημείο $P \in \mathbb{FP}^2$ είναι ιδιάζον σημείο της καμπύλης $Z(p)$ αν και μόνο αν

$$\frac{\partial p}{\partial x} = \frac{\partial p}{\partial y} = \frac{\partial p}{\partial z} = 0.$$

Ορισμός 2. Έστω $p \in \mathbb{F}[x,y,z]$ ένα ομογενές πολυώνυμο και $Z(p)$ η αντίστοιχη προβολική του καμπύλη. Για ένα λείο σημείο $P \in Z(p)$, ορίζουμε την εφαπτόμενη ευθεία της $Z(p)$ στο σημείο P να είναι η ευθεία

$$T_P Z(p) = Z\left(x\frac{\partial p}{\partial x}\Big|_P + y\frac{\partial p}{\partial y}\Big|_P + z\frac{\partial p}{\partial z}\Big|_P\right),$$

όπου

$$Z\left(x\frac{\partial p}{\partial x}\Big|_P + y\frac{\partial p}{\partial y}\Big|_P + z\frac{\partial p}{\partial z}\Big|_P\right) = \left\{[x:y:z] \in \mathbb{FP}^2 : x\frac{\partial p}{\partial x}\Big|_P + y\frac{\partial p}{\partial y}\Big|_P + z\frac{\partial p}{\partial z}\Big|_P = 0\right\}.$$

4.3 Προβολική ισοδυναμία

Έστω ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x,y,z]$, με $\deg(p) = n$ και ένα αντιστρέψιμο πίνακα $A \in GL(3,\mathbb{F})$. Τότε ορίζεται το ομογενές πολυώνυμο
$p \cdot A \in \mathbb{F}[x,y,z]$, με $\deg(p \cdot A) = n$, θέτοντας

$$(p \cdot A)(x,y,z) = p(A \cdot (x,y,z)).$$

Εδώ θεωρούμε ότι το όρισμα του πολυωνύμου (x,y,z) είναι ένας πίνακας στήλη.

Ορισμός 1. Έστω δύο ομογενή πολυώνυμα $p, q \in \mathbb{F}[x,y,z]$. Καλούμε τα p, q προβολικώς ισοδύναμα αν υπάρχει αντιστρέψιμος πίνακας $A \in GL(3,\mathbb{F})$ και $\lambda \in \mathbb{F}^*$ έτσι ώστε $p(x,y,z) = \lambda g(A \cdot (x,y,z))$. Δύο υποσύνολα $S, T \subseteq \mathbb{FP}^2$ καλούνται προβολικώς ισοδύναμα αν και μόνο αν υπάρχει προβολικός μετασχηματισμός $\tau \in PGL(2,\mathbb{F})$ τέτοιος ώστε $\tau(S) = T$.

Αν θεωρήσουμε ότι ο προβολικός μετασχηματισμός περιγράφεται από έναν 3×3 αντιστρέψιμο πίνακα A, τότε μπορούμε αντίστοιχα να πούμε ότι δύο υποσύνολα του προβολικού επιπέδου $\mathbb{FP}^2$, έστω τα S και T, είναι προβολικώς ισοδύναμα αν και μόνο αν $A(S) = T$.

Είναι εύκολο να αποδείξουμε ότι η προβολική ισοδυναμία είναι μια σχέση ισοδυναμίας. Συγκεκριμένα, είναι ανακλαστική, εφόσον μπορούμε να θεωρήσουμε ότι κάθε ανάγωγο πολυώνυμο είναι προβολικά ισοδύναμο με τον εαυτό του για $A = I_3$ και $\lambda = 1$. Αντίστοιχα αν το ομογενές πολυώνυμο p είναι προβολικά ισοδύναμο με το ομογενές πολυώνυμο q, δηλαδή υπάρχουν $A \in GL(3,\mathbb{F})$ και $\lambda \in \mathbb{F}$ ώστε $p(x,y,z) = \lambda(q \cdot A)(x,y,z)$, τότε $q(x,y,z) = \lambda^{-1}(p \cdot A^{-1})(x,y,z)$ και άρα και το πολυώνυμο q είναι προβολικώς ισοδύναμο

με το p, απ΄ όπου προκύπτει και η συμμετρική ιδιότητα. Τέλος, αν ένα ομογενές πολυώνυμο p είναι προβολικώς ισοδύναμο με ένα ομογενές πολυώνυμο q και το ομογενές πολυώνυμο q είναι προβολικώς ισοδύναμο με ένα ομογενές πολυώνυμο r, τότε θέλουμε να δείξουμε ότι και το p είναι προβολικώς ισοδύναμο με το r. Πράγματι έχουμε ότι για $\lambda_1 \in \mathbb{F}$, $A \in GL(3, \mathbb{F})$

$$p = \lambda_1(q \cdot A) \tag{4.2}$$

Αντίστοιχα, έχουμε ότι για $\lambda_2 \in \mathbb{F}$, $B \in GL(3, \mathbb{F})$

$$q = \lambda_2(r \cdot B) \tag{4.3}$$

Έχουμε από τις σχέσεις (4.2) και (4.3) ότι

$$p = \lambda_1(\lambda_2(r \cdot B) \cdot A) = \lambda_1\lambda_2(r \cdot BA).$$

Οπότε τελικά θα έχουμε ότι και το πολυώνυμο p θα είναι προβολικά ισοδύναμο με το πολυώνυμο r.

Μπορούμε επίσης να δούμε ότι αν $p(x, y, z) = \lambda q(A \cdot (x, y, z))$ οι αντίστοιχες επίπεδες προβολικές καμπύλες σχετίζονται από τη σχέση

$$Z(p) = A^{-1}(Z(q)) \tag{4.4}$$

Επίσης, προκύπτει ότι δύο προβολικά ισοδύναμα ομογενή πολυώνυμα έχουνε προβολικά ισοδύναμους μηδενοχώρους. Αυτή η ιδιότητα μας επιτρέπει να ταξινομήσουμε τα ομογενή πολυώνυμα σε κλάσεις προβολικής ισοδυναμίας όπως θα δούμε παρακάτω.

4.4 Αναλλοίωτες ποσότητες κωνικών τομών

Η διακρίνουσα ενός πραγματικού πολυωνύμου δευτέρου βαθμού $f(x, y) \in \mathbb{R}[x, y]$ έχει μια πολύ ενδιαφέρουσα γεωμετρική ερμηνεία την οποία θα δούμε στη συνέχεια. Αρχικά χρειαζόμαστε το παρακάτω λήμμα.

Λήμμα 1. Έστω $a, b, c \in \mathbb{R}$ με $a^2 + b^2 + c^2 \neq 0$. Τότε το υποσύνολο

$$S = \{[x : y] \in \mathbb{RP}^1 : ax^2 + bxy + cy^2 = 0\}$$

του πραγματικού προβολικού επιπέδου είναι

(i) το κενό αν $b^2 - 4ac < 0$,

(ii) έχει μοναδικό σημείο αν $b^2 - 4ac = 0$,

(iii) έχει δύο διαφορετικά σημεία αν $b^2 - 4ac > 0$.

Απόδειξη: Ας θεωρήσουμε αρχικά ότι το σημείο στο άπειρο είναι το $\infty = [1 : 0] \in \mathbb{RP}^1$, ανήκει στο S αν και μόνο αν $a = 0$. Κάθε άλλο σημείο εκτός του ∞ μπορεί που ανήκει στην πραγματική προβολική ευθεία $\mathbb{RP}^1$, μπορεί να γραφεί ως $[x : 1]$ για ένα μοναδικό πραγματικό αριθμό x. Κάθε τέτοιο σημείο μπορεί να ανήκει στο υποσύνολο S αν και μόνο αν $ax^2 + bxy + cy^2 = 0$.

Διακρίνουμε δύο περιπτώσεις. Αν $a = 0$ τότε το $\infty \in S$ και το $[x : 1] \in S$ αν και μόνο αν $bx + c = 0$. Η εξίσωση $bx + c = 0$ έχει μοναδική ρίζα ως γραμμική όταν $b \neq 0$ και δεν έχει καμία ρίζα αν $b = 0$ (επειδή τότε θα έπρεπε να είναι $c \neq 0$, το οποίο είναι άτοπο διότι έχουμε υποθέσει ότι $a^2+b^2+c^2 \neq 0$). Αν $b \neq 0$ έχουμε ότι $b^2-4ac > 0$ και άρα το σύνολο S περιέχει δύο σημεία, το ∞ και το $[-c/b : 1]$, ενώ αν το $b = 0$ τότε το S περιέχει μοναδικό σημείο και έχουμε $b^2 - 4ac = 0$. Επομένως το λήμμα ισχύει στην περίπτωση που $A = 0$.

Αν τώρα θεωρήσουμε ότι $A \neq 0$, τότε $\infty \notin S$ και άρα τα στοιχεία του S είναι οι πραγματικοί αριθμοί x που είναι τέτοιοι ώστε $ax^2+bx+c = 0$. Εφόσον έχουμε θεωρήσει ότι $a \neq 0$, έχουμε μια απλή δευτεροβάθμια εξίσωση με πραγματικούς συντελεστές και άρα το λήμμα είναι αληθές.

□

Παρατήρηση 1. Αν $\mathbb{F} = \mathbb{C}$, αντί για $\mathbb{R}$, το αντίστοιχο λήμμα μας λέει ότι το υποσύνολο S περιέχει μοναδικό σημείο αν $b^2 - 4ac = 0$, ενώ περιέχει δύο διαφορετικά σημεία σε οποιαδήποτε άλλη περίπτωση. Μπορούμε να θεωρήσουμε το μοναδικό σημείο ως μια ρίζα αλγεβρικής πολλαπλότητας δύο.

Τώρα είμαστε σε θέση να δούμε ότι η διακρίνουσα ενός δευτεροβάθμιου πολυωνύμου $f(x, y) \in \mathbb{R}[x, y]$ είναι ένας τρόπος να πούμε ότι η προβολική πλήρωση $Z(\bar{f}) \subseteq \mathbb{RP}^2$ του $Z(f) \subseteq \mathbb{R}^2$ τέμνει την ευθεία στο άπειρο $\mathbb{RP}^1 \subseteq \mathbb{RP}^2$.

Πρόταση 1. Έστω $p(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$ ένα πολυώνυμο με $\deg(p) \leq 2$ και συντελεστές a, b, c, d, e, $f \in \mathbb{R}$ και διακρίνουσα $D(p) = b^2 - 4ac$. Τότε

(i) $D(p) < 0$ αν και μόνο αν $Z(\bar{p})$ δεν τέμνει πουθενά την ευθεία στο άπειρο,

(ii) $D(p) > 0$ αν και μόνο αν $Z(\bar{p}) \cap \mathbb{RP}^1$ έχει δύο κοινά σημεία,

(iii) $D(p) = 0$ αν και μόνο αν $Z(\bar{p}) \cap \mathbb{RP}^1$ έχει μοναδικό κοινό σημείο.

Απόδειξη: Σημειώνουμε εδώ ότι ομογενοποιώντας το πολυώνυμο p έχουμε το ομογενές πολυώνυμο $\bar{p}$, όπου

$$\bar{p} = ax^2 + bxy + cy^2 + dxz + eyz + fz^2.$$

Συνεπώς, ένα σημείο που ανήκει στην προβολική ευθεία στο άπειρο είναι της μορφής $[x : y : 0]$ και ανήκει στη $Z(p)$ αν και μόνο αν $\bar{p}(x, y, 0) = 0$, δηλαδή $ax^2+bxy+cy^2 = 0$. Οπότε το ζητούμενο έπεται από το προηγούμενο λήμμα.

4.5 Ταξινόμηση προβολικών κωνικών τομών

Σε αυτήν την ενότητα θα μελετήσουμε το πρόβλημα της ταξινόμησης επίπεδων προβολικών καμπυλών και ομογενών πολυωνύμων τριών μεταβλητών ως προς προβολική ισοδυναμία. Θα ταξινομήσουμε ομογενή πολυώνυμα $2^{ου}$ βαθμού (ορισμένα επί του $\mathbb{R}$ ή $\mathbb{C}$) και τις αντίστοιχες επίπεδες προβολικές καμπύλες που καλούνται επίσης προβολικές κωνικές τομές. Η προβολική ταξινόμηση είναι σε πολλά σημεία απλούστερη από ότι η κλασική ταξινόμηση.

Πολλά από τα βήματα της ταξινόμησης έχουν νόημα επί ενός αυθαίρετου σώματος, αλλά με χαρακτηριστική διάφορη του 2. Έστω η δευτεροβάθμια εξίσωση

$$p = ax^2 + bxy + cy^2 + dxz + eyz + fz^2, \tag{4.5}$$

όπου $a, b, c, d, e, f \in \mathbb{F}$. Θεωρούμε επίσης τον συμμετρικό 3×3 πίνακα

$$M(p) = \begin{pmatrix} a & \frac{b}{2} & \frac{d}{2} \\ \frac{b}{2} & c & \frac{e}{2} \\ \frac{d}{2} & \frac{e}{2} & f \end{pmatrix}.$$

Τα ορίσματα του πίνακα ανήκουν στο σώμα $\mathbb{F}$. Άρα μπορούμε να καταλάβουμε γιατί θέλουμε το σώμα μας να έχει χαρακτηριστική διάφορη 2 (αν είχε χαρακτηριστική 2, δεν θα μπορούσαμε να διαιρέσουμε με αυτό, αφού θα διαιρούσαμε με το μηδέν). Συμβολίζουμε στο εξής το (x, y, z) ως $\vec{x}$, το οποίο είναι διάνυσμα στήλης και αποτελεί όρισμα του πολυωνύμου. Έχουμε

$$p(\vec{x}) = (\vec{x})^{\intercal} M(p) \vec{x}. \tag{4.6}$$

Συγκεκριμένα αν θεωρήσουμε ότι $A \in GL(3, \mathbb{F})$ η σχέση (4.6) μας δίνει

$$p(A\vec{x}) = (A\vec{x})^{\intercal} M(p) A\vec{x} = (\vec{x})^{\intercal} A^{\intercal} M(p) A\vec{x}.$$

Βλέπουμε ότι οι πίνακες $M(p)$ και $M(p \cdot A)$ σχετίζονται μέσω της

$$M(p \cdot A) = A^{\intercal} M(p) A.$$

Πρόταση 1. Έστω $\mathbb{F}$ ένα σώμα. Για ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$, $\deg(p) = 2$ τότε τα εξής είναι ισοδύναμα

(i) Το ομογενές πολυώνυμο εκφράζεται ως $p = qr$, όπου $q, r \in \mathbb{F}[x, y]$ είναι δύο γραμμικώς ομογενή πολυώνυμα. Έτσι έχουμε ότι $Z(p) = Z(q) \cup Z(r)$, δηλαδή η επίπεδη προβολική καμπύλη είναι η ένωση δύο (ενδεχομένως ίσων) επίπεδων προβολικών καμπυλών. Εφόσον μάλιστα αυτές οι δύο επίπεδες προβολικές καμπύλες είναι γραμμικές (εφόσον ένα πολυώνυμο δευτέρου βαθμού διασπάται μοναδικά σε πολυώνυμα πρώτου βαθμού), τότε έχουμε ότι η επίπεδη προβολική καμπύλη είναι η ένωση δύο προβολικών ευθειών.

(ii) Το υποσύνολο $Z(p) \subseteq \mathbb{FP}^2$ περιέχει μια προβολική ευθεία. Οι δύο προηγούμενες ισοδύναμες εκφράσεις δίνουν δύο ακόμα ισοδύναμες εκφράσεις οι οποίες ισχύουν μόνο αν το $\mathbb{F}$ δεν έχει χαρακτηριστική δύο.

(iii) Υπάρχει ένα ιδιάζον σημείο στο υποσύνολο $Z(p)$.

(iv) Η ορίζουσα του πίνακα $M(p)$ είναι μηδενική (δηλαδή ο πίνακας είναι μη αντιστρέψιμος)

Ορισμός 1. Έστω ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$, με $\deg(p) = 2$. Το πολυώνυμο p καλείται εκφυλισμένο αν περιέχει ιδιάζον σημείο και μη εκφυλισμένο αν δεν περιέχει κανένα εκφυλισμένο σημείο.

Θεώρημα 1. Έστω $\mathbb{F}$ ένα σώμα που δεν έχει χαρακτηριστική δύο, επίσης θεωρούμε ένα ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$, με $\deg(p) = 2$. Τότε υπάρχει πίνακας $M \in GL(3, \mathbb{F})$ τέτοιος ώστε

$$p \cdot M = ax^2 + by^2 + cz^2$$

για κάποια a, b, $c \in \mathbb{F}$.

Απόδειξη: Θεωρούμε ένα τυχαίο ομογενές πολυώνυμο $p \in \mathbb{F}[x, y, z]$. Στόχος μας είναι μέσα από πεπερασμένες αλλαγές μεταβλητών να απαλείψουμε τους όρους xy, xz, yz. Η μέθοδος την οποία θα ακολουθήσουμε (γνωστή και ως μέθοδος Lagrange) θα μας επιτρέψει να δημιουργήσουμε τετράγωνα χωρίς όμως τα περιττά γινόμενα.

Βήμα 1 Το πρώτο μας βήμα είναι να απαλείψουμε τους όρους bxy και dxz. Αν έχουμε εξ αρχής ότι $b = d = 0$, τότε παρακάμπτουμε αυτό το βήμα και πηγαίνουμε κατευθείαν στο Βήμα 3. Αν $a \neq 0$ τότε πηγαίνουμε στο Βήμα 2. Αν έχουμε ότι $a = 0$ και $c \neq 0$ τότε βάζουμε όπου x το y και αντίστροφα και έπειτα συνεχίζουμε στο Βήμα 2. Αν $a = c = 0$ και $b \neq 0$ τότε το πολυώνυμο μας είναι στη μορφή

$$bxy + dxz + eyz + fz^2$$

και μέσω της αλλαγής μεταβλητών $(x, y, z) \mapsto (x, x + y, z)$ παίρνουμε το πολυώνυμο

$$bx^2 + (b + e)xy + (d + e)xz + eyz + fz^2,$$

οπου ο συντελεστής του x^2 είναι μη μηδενικός και άρα μπορούμε να προχωρήσουμε στο Βήμα 2. Στην εναπομένουσα περίπτωση, όπου $a = c = 0$ και $d \neq 0$, μπορούμε να κάνουμε την παρόμοια αλλαγή συντεταγμένων $(x, y, z) \mapsto (x, y, x + z)$ και έπειτα να προχωρήσουμε στο Βήμα 2.

Βήμα 2 Μέχρι στιγμής έχουμε το πολυώνυμο

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2$$

όπου $a \neq 0$. Κάνοντας την αλλαγή μεταβλητών

$$(x, y, z) \mapsto \left(x - \frac{b}{2a}y - \frac{c}{2a}z, y, z\right),$$

(έχουμε θεωρήσει ότι $\mathbb{F}$ έχει χαρακτηριστική διάφορη του 2) το πολυώνυμο μας παίρνει τη μορφή

$$ax^2 + \left(c + \frac{b^2}{4a}\right)y^2 + \left(\frac{bd}{2a^2} - \frac{bd}{a} + e\right)yz + \left(\frac{d^2}{4a^2} - \frac{d^2}{2a} + f\right)z^2.$$

Οι συγκεκριμένοι συντελεστές είναι μικρής σημασίας. Αυτό το οποίο όμως καταφέραμε με το Βήμα 2 είναι να μην υπάρχει γινόμενο που να περιέχει το x. Βλέπουμε μάλιστα ότι το μόνο γινόμενο που υπάρχει είναι το yz.

Βήμα 3 Σε αυτό το βήμα ξεκινάμε από ένα πολυώνυμο της μορφής

$$ax^2 + cy^2 + eyz + fz^2.$$

Σκοπός μας είναι να απαλείψουμε το γινόμενο yz από τη σχέση. Προφανώς αν έχουμε ότι $e = 0$, δεν έχουμε να αποδείξουμε κάτι, οπότε θεωρούμε ότι $e \neq 0$. Αν έχουμε επίσης ότι $c = 0$ και $f \neq 0$ τότε βάζουμε το z στη θέση του y και αντίστροφα, έχουμε δηλαδή την αλλαφή συντεταγμένων $(x, y, z) \mapsto (x, z, y)$ και προχωράμε στο Βήμα 4. Η περίπτωση που μένει είναι αν $c = f = 0$ και όπως είπαμε $e \neq 0$. Σε αυτήν την περίπτωση το πολυώνυμο μας είναι στη μορφή

$$ax^2 + eyz$$

και μέσω της αλλαγής μεταβλητών $(x, y, z) \mapsto (x, y, y + z)$ παίρνουμε το πολυώνυμο

$$ax^2 + ey^2 + eyz,$$

όπου ο συντελεστής του y^2 είναι μη μηδενικός. Προχωράμε τώρα στο Βήμα 4.

Βήμα 4 Σε αυτό το βήμα έχουμε ένα πολυώνυμο της μορφής

$$ax^2 + cy^2 + eyz + fz^2,$$

όπου $c \neq 0$. Μέσω της αλλαγής μεταβλητών

$$(x, y, z) \mapsto \left(x, y - \frac{e}{2c}z, z\right),$$

το πολυώνυμο μας τότε παίρνει την ζητούμενη μορφή

$$ax^2 + cy^2 + \left(- \frac{e}{4c} + f\right)z^2.$$

□

Πόρισμα 1. Κάθε μη μηδενικό δευτεροβάθμιο ομογενές πολυώνυμο $p \in \mathbb{R}[x, y, z]$ είναι προβολικά ισοδύναμο με ακριβώς μια από τις παρακάτω εκφράσεις

(i) $x^2 + y^2 + z^2$

(ii) $x^2 + y^2 - z^2$

(iii) $x^2 + y^2$

(iv) $x^2 - y^2$

(v) x^2

Απόδειξη: Από το παραπάνω θεώρημα έχουμε ότι ένα ομογενές πολυώνυμο είναι προβολικά ισοδύναμο με τη μορφή

$$ax^2 + by^2 + cz^2,$$

για κάποια a, b, $c \in \mathbb{R}$. Για κάθε μη μηδενικό συντελεστή μπορούμε να πολλαπλασιάσουμε την αντίστοιχη μεταβλητή του με το κλάσμα που θα έχει για παρονομαστή την τετραγωνική ρίζα της απόλυτης τιμής του αντίστοιχου συντελεστή. Συνεπώς έχουμε ότι το πολυώνυμο p είναι ισοδύναμο με ένα πολυώνυμο της ίδιας μορφής που όμως τώρα a, b, $c \in \{0, 1, -1\}$. Μπορούμε να δούμε ότι πολλαπλασιάζοντας αν χρειάζεται με -1 σε κάποια περίπτωση, ή αν απαιτείται εναλλάσσοντας κάποιες μεταβλητές πάντα θα προκύπτουν τα αποτελέσματα που αναγράφονται στο πόρισμα.

Αυτό που μένει τώρα να δείξουμε είναι ότι κανένα από τα πολυώνυμα που αναγράφονται στο πόρισμα δεν είναι ισοδύναμο με κάποιο από τα υπόλοιπα. Αλλά αυτό μπορούμε να το δούμε άμεσα από τις επίπεδες προβολικές καμπύλες που αντιστοιχούν στο κάθε πολυώνυμο. Αν θεωρήσουμε p_i το κάθε πολυώνυμο με $i \in \{1, \ldots, 5\}$ τότε έχουμε

(i) $Z(p_1) = \emptyset$

(ii) $Z(p_2) =$ κύκλος

(iii) $Z(p_3) = \{[0 : 0 : 1]\}$

(iv) $Z(p_4) =$ δύο ευθείες που τέμνονται

(v) $Z(p_5) =$ μια διπλή ευθεία

□

Πόρισμα 2. Κάθε μη μηδενικό δευτεροβάθμιο ομογενές πολυώνυμο $p \in \mathbb{C}[x, y, z]$ είναι προβολικά ισοδύναμο με ακριβώς μια από τις παρακάτω εκφράσεις:

(i) $x^2 + y^2 + z^2$

(ii) $x^2 + y^2$

(iii) x^2

Απόδειξη: Αυτό το πόρισμα αποδεικνύεται με παρόμοιο τρόπο όπως και το προηγούμενο. Μια πολύ σημαντική διαφορά όμως τώρα είναι ότι μπορούμε να κάνουμε την αλλαγή συντεταγμένων $x \mapsto ix$ ώστε να επιβεβαιώσουμε ότι κάθε ομογενές πολυώνυμο είναι προβολικά ισοδύναμο με ένα ομογενές πολυώνυμο της μορφής $ax^2 + by^2 + cz^2$ όπου a, b, $c \in \{0, 1\}$.

Παρατήρηση 1. Το τελευταίο πόρισμα είναι ισχύει για κάθε αλγεβρικά κλειστό σώμα που δεν έχει χαρακτηριστική 2 μέσω της ίδιας απόδειξης. Το νόημα είναι ότι κάθε στοιχείο a του σώματος έχει τετραγωνική ρίζα, επειδή το πολυώνυμο $x^2 - a \in \mathbb{F}[x]$ πρέπει να έχει ρίζα. Εφόσον έχω θεωρήσει ότι το σώμα είναι αλγεβρικά κλειστό δηλαδή, κάθε πολυώνυμο έχει ρίζα επί του σώματος και δεν χρειάζεται να πάρουμε κάποια επέκταση του.

Παρατήρηση 2. Στην περίπτωση που το σώμα $\mathbb{F}$ έχει χαρακτηριστική 2, δεν μπορούμε να απαλείψουμε τα γινόμενα xy, xz, yz επομένως όλα όσα είπαμε παραπάνω δεν έχουν νόημα.

4.6 Σημεία τομής αλγεβρικών καμπυλών και ο βαθμός πολλαπλότητάς τους

Στην αλγεβρική γεωμετρία τα σημεία τομής και η βαθμός πολλαπλότητας τους γενικεύει την αναζήτηση σημείων τομής μεταξύ δύο καμπυλών για μεγαλύτερες διαστάσεις. Έστω p_1, p_2 δύο μη σταθερά πολυώνυμα του $\mathbb{F}[x, y]$ για κάποιο σώμα $\mathbb{F}$, ή αντίστοιχα δύο μη σταθερά ομογενή πολυώνυμα του $\mathbb{F}[x, y, z]$. Έστω ότι $C_1 = Z(p_1)$ και $C_2 = Z(p_2)$ να είναι οι αντίστοιχες αλγεβρικές καμπύλες στο $\mathbb{F}^2$, ή αντίστοιχα οι επίπεδες προβολικές καμπύλες στο $\mathbb{FP}^2$. Έστω ότι υπάρχουν πεπερασμένα σημεία στο σύνολο $C_1 \cap C_2$ του $\bar{\mathbb{F}}^2$ ή αντίστοιχα του $\bar{\mathbb{F}}\mathbb{P}^2$, όπου $\bar{\mathbb{F}}$ είναι η αλγεβρική κλειστότητα του $\mathbb{F}$. Υπό αυτές τις προϋποθέσεις μπορούμε να ορίσουμε ένα θετικό ακέραιο αριθμό $m(p_1, p_2, P)$ στο κάθε σημείο που ανήκει στην τομή $C_1 \cap C_2$ και καλούμε αυτόν τον αριθμό βαθμό πολλαπλότητας του σημείου τομής P. Είμαστε πλέον σε θέση να δούμε το παρακάτω θεώρημα, γνωστό και ως θεώρημα του Bezout. Παραλείπουμε όμως την απόδειξη καθώς ξεφεύγει από τα πλαίσια της μελέτης μας.

Θεώρημα 1. (Θεώρημα Bezout) Έστω $\mathbb{F}$ ένα αλγεβρικά κλειστό σώμα και p_1, $p_2 \in \mathbb{F}[x, y, z]$ να είναι ομογενή πολυώνυμα βαθμών d_1, $d_2 > 0$ αντίστοιχα. Έστω

$C_i = Z(p_i) \subseteq \mathbb{FP}^2$. Θεωρούμε επίσης ότι $|C_1 \cap C_2| = n$, $n \in \mathbb{N}$. Τότε

$$\sum_{P \in C_1 \cap C_2} m(p_1, p_2, P) = d_1 d_2.$$

Ο γενικός ορισμός του $m(p_1, p_2, P)$ απαιτεί αρκετές γνώσεις αντιμεταθετικής άλγεβρας. Αυτός είναι και ο λόγος που δεν θα αναλύσουμε περισσότερο τις προαναφερθείσες έννοιες. Παρόλα αυτά θα περιοριστούμε στην περίπτωση που ένα από τα p_1, p_2 είναι βαθμού 1.

Η ιδέα για την κατασκευή του ορισμού του βαθμού πολλαπλότητας ενός σημείου τομής, θα βασιστεί στην ιδέα της πολλαπλότητας μιας ρίζας ενός πολυωνύμου μιας μεταβλητής.

Έστω $p \in \mathbb{F}[x]$ ένα πολυώνυμο βαθμού $d > 0$. Από την άλγεβρα, γνωρίζουμε ότι μπορούμε να βρούμε μια επέκταση του σώματος $\mathbb{F}$, έστω την $\bar{\mathbb{F}}$, τέτοια ώστε το πολυώνυμο μας να μπορεί να γραφτεί επί του $\bar{\mathbb{F}}$ ως γινόμενο γραμμικών όρων (δηλαδή πρωτοβάθμιων πολυωνύμων). Γενικά καλούμε το $\bar{\mathbb{F}}$ σώμα διάσπασης του πολυωνύμου p. Επί του $\bar{\mathbb{F}}$ μπορούμε να γράψουμε

$$p(x) = c \prod_{i=1}^{d} (x - a_i),$$

όπου $c \in \mathbb{F}^*$ και $a_i \in \bar{\mathbb{F}}$. Προφανώς τα a_i είναι όλες οι ρίζες του πολυωνύμου $p(x)$. Αν a είναι μια ρίζα του πολυωνύμου p, ορίζουμε την πολλαπλότητα της να είναι ο αριθμός $m = m(a, p) = |\{i \in \{1, \ldots, d\} : a = a_i\}|$.

Από τα παραπάνω καταλαβαίνουμε ότι $m \in \{1, \ldots, d\}$. Προφανώς ο παραπάνω ορισμός έχει νόημα ακόμα και αν το a δεν είναι ρίζα, μάλιστα στην προκειμένη περίπτωση θα ισχύει $m(a, p) = 0$. Αν η παραγοντοποίηση του p μπορεί να γίνει εντός του $\mathbb{F}$, δηλαδή το $\mathbb{F}$ είναι το σώμα διάσπασης του p τότε είναι ξεκάθαρη η σχέση που μας δίνει το θεώρημα του Bezout, δηλαδή

$$\sum_{m} (p, a) = d.$$

Από αυτό το απλό επιχείρημα προκύπτει η ειδική περίπτωση του θεωρήματος Bezout που θα μας χρειαστεί παρακάτω.

Ορισμός 1. Έστω $p \in \mathbb{F}[x, y, z]$ ένα ομογενές πολυώνυμο. Ένα λείο σημείο $P \in Z(p)$ ονομάζεται σημείο καμπής της $Z(p)$ αν και μόνο αν ο βαθμός πολλαπλότητας του, αν θεωρήσουμε τις δύο καμπύλες να είναι οι $Z(p)$ και $T_P Z(p)$, είναι μεγαλύτερος του δύο.

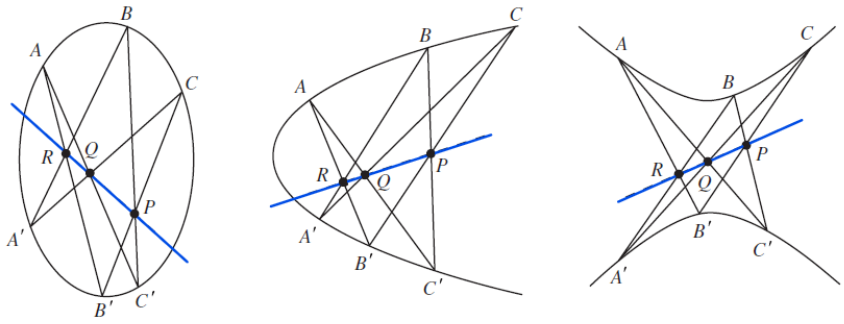
4.7 Το θεώρημα του Pascal

Σε αυτήν την ενότητα θα αποδείξουμε ένα κεντρικό θεώρημα της Προβολικής Γεωμετρίας, το Θεώρημα του Pascal. Το δημοφιλές αυτό θεώρημα αποδείχθηκε από τον Blaise Pascal, ο οποίος μάλιστα το απέδειξε σε ηλικία μόλις 16 ετών. Δυστυχώς η απόδειξη που έδωσε ο ίδιος για το θεώρημά του δεν έχει διασωθεί, παρόλα αυτά ποικίλες αποδείξεις διαφόρων μαθηματικών έχουν δοθεί από το έτος 1639 και μετά. Πολλές σύγχρονες αποδείξεις του Θεωρήματος Pascal έχουν γίνει αξιοποιώντας το Θεώρημα Bezout, αλλά επειδή το Θεώρημα Bezout είναι ένα δύσκολο θεώρημα στην απόδειξη του, επιλέγουμε να παρουσιάσουμε την απόδειξη του Gillam, ο οποίος παρουσιάζει μια σχετικά απλή απόδειξη, βασισμένη στη γραμμική άλγεβρα και σε απλές αλγεβρικές ιδιότητες.

Θεώρημα 1. (Θεώρημα του Pascal) Έστω $P_1, \ldots, P_6$ έξι διαφορετικά σημεία που ανήκουν σε μια μη εκφυλισμένη κωνική τομή $C \subseteq \mathbb{RP}^2$. Τότε τα σημεία

$$X = P_1P_2 \cap P_4P_5, Y = P_2P_3 \cap P_5P_6 \text{ και } Z = P_3P_4 \cap P_1P_6$$

είναι συνευθειακά.



Απόδειξη: Τρία διαφορετικά σημεία πάνω σε μια μη εκφυλισμένη κωνική τομή δεν μπορεί να είναι συνευθειακά, έτσι τα $P_1, \ldots, P_6$ βρίσκονται σε γενική θέση. Ένας προβολικός μετασχηματισμός απεικονίζει ευθείες σε ευθείες και κωνικές τομές σε κωνικές τομές και έτσι εφαρμόζοντας το Θεμελιώδες Θεώρημα της Προβολικής Γεωμετρίας (ειδική περίπτωση Θεωρήματος Γενικής Θέσης εφόσον είμαστε σε διάσταση 2) μπορούμε να θεωρήσουμε

$$P_1 = [1 : 0 : 0],$$

$$P_2 = [0 : 1 : 0],$$

$$P_3 = [0 : 0 : 1],$$

$$P_4 = [1 : 1 : 1],$$

$$P_5 = [a : b : c],$$

$$P_6 = [u : v : w].$$

Για τις παρακάτω προβολικές ευθείες έχουμε ότι περιγράφονται από τις σχέσεις

$$P_1P_2 : \ z = 0,$$

$$P_1P_3 : \ y = 0,$$

$$P_1P_4 : \ y - z = 0,$$

$$P_2P_4 : \ x - z = 0,$$

$$P_3P_4 : \ x - y = 0.$$

Εφόσον έχουμε υποθέσει ότι τα έξι σημεία μας είναι σε γενική θέση, τότε τα σημεία P_5 και P_6 δεν μπορούν να ανήκουν σε καμία από τις παραπάνω ευθείες. Προκύπτει ότι οι παρακάτω αριθμοί δεν μπορούν να ισούνται με μηδέν

$$c, b, b - c, a - c, a - b, w, v, v - w, u - w, u - v$$

.

Έτσι επιτρέπεται η διαίρεση με τους παραπάνω αριθμούς.

Θεωρούμε επίσης την εξίσωση της κωνικής τομής C να είναι η

$$Ax^2 + Bxy + Cy^2 + Dxz + Eyz + Fz^2 = 0,$$

Επειδή έχουμε ότι P_1, P_2, $P_3 \in C$, τότε προκύπτει ότι $A = 0$, $C = 0$, $F = 0$. Άρα η εξίσωση της κωνικής τομής C γίνεται:

$$Bxy + Dxz + Eyz = 0.$$

Επίσης όμως έχουμε ότι $P_4 \in C$ και άρα $B + D + E = 0$ δηλαδή $E = -B - D$. Παρατηρούμε ότι δεν θα μπορούσαμε να έχουμε $B = 0$, διότι τότε θα είχαμε εκφυλισμένη κωνική τομή, πράγμα που αντιβαίνει την υπόθεση μας, άρα προκύπτει ότι $B \neq 0$ και μάλιστα μπορούμε να θεωρήσουμε ότι $B = 1$. Προκύπτει ότι η κωνική τομή μας θα έχει

τη μορφή

$$xy + Dxz\Gamma(1+D)yz = 0 \Rightarrow y(x-z) + Dz(x-y) = 0 \Rightarrow D = \frac{y(z-x)}{z(x-y)}.$$

Λαμβάνοντας τώρα υπόψιν ότι $P_5 \in C$, προκύπτει ότι $D = \frac{b(c-a)}{c(a-b)}$ και επειδή έχουμε και ότι $P_6 \in C$ προκύπτει

$$v(u-w) + \frac{b(c-a)}{c(a-b)} w(u-v) = 0.$$

Πολλαπλασιάζοντας τώρα με το μη μηδενικό παρονομαστή και κάνοντας τις επιμεριστικές παίρνουμε

$$cv(a-b)(u-w) + bw(c-a)(u-v) = 0 \Rightarrow$$

$$\Rightarrow acuv - acvw - bcuv + bcvw + bcuw - bcvw - abuw + abvw = 0 \Rightarrow$$

$$\Rightarrow abuw - bcuw + acvw = acuv - bcuv - abvw$$

Έχουμε ότι η ευθεία P_1P_2 δίνεται από την εξίσωση $z = 0$ και αντίστοιχα η ευθεία P_4P_5 από την εξίσωση $(c-b)x + (a-c)y + (b-a)z = 0$. Προκύπτει επομένως ότι $X = [a-c : b-c : 0]$.

Όμοια έχουμε ότι η ευθεία P_2P_3 δίνεται από την εξίσωση $x = 0$ και αντίστοιχα η ευθεία P_5P_6 από την εξίσωση $(bw-cv)x + (cu-aw)y + (av-bu)z = 0$. Προκύπτει επομένως $Y = [0 : bu-av : cu-aw]$.

Τέλος έχουμε ότι η ευθεία P_3P_4 δίνεται από την εξίσωση $y = x$ και αντίστοιχα η ευθεία P_1P_6 από την εξίσωση $wy = vz$. Προκύπτει ότι $Z = [v : v : w]$.

Για να δείξουμε άρα ότι τα σημεία X, Y, Z είναι συνευθειακά, αρκεί να δείξουμε ότι ένα από τα σημεία είναι γραμμικός συνδυασμός των άλλων δύο σημείων ή μπορούμε ισοδύναμα να υπολογίσουμε την ορίζουσα που έχει για γραμμές τις συντεταγμένες των σημείων

$$\begin{vmatrix} \cdots X \cdots \\ \cdots Y \cdots \\ \cdots Z \cdots \end{vmatrix} = \begin{vmatrix} a-c & b-c & 0 \\ 0 & bu-av & cu-aw \\ v & v & w \end{vmatrix} = abuw - bcuw + acvw - acuv + bcuv - abvw = 0.$$

Έπεται το ζητούμενο, δηλαδή ότι τα σημεία X, Y, Z είναι πράγματι συνευθειακά.

□

Παρατήρηση 1. Το αντίστοιχο αποτέλεσμα ικανοποιείται και για εκφυλισμένες κωνικές τομές και είναι το γνωστό μας θεώρημα του Πάππου.

4.8 Κυβικές Καμπύλες

Μέχρι τώρα είχαμε περιορίσει τη μελέτη μας των επίπεδων προβολικών καμπυλών στην περίπτωση των ευθειών και των κωνικών τομών, δηλαδή το μηδενοχώρο ομογενών πολυωνύμων μέχρι και βαθμού 2. Θα μελετήσουμε τώρα το μηδενοχώρο ομογενών πολυωνύμων βαθμού 3, τα οποία ονομάζονται κυβικές μορφές. Για τεχνικούς λόγους αλλά και για διευκόλυνση στους υπολογισμούς μας, θα θεωρήσουμε ότι το σώμα επί του οποίου είναι ορισμένος ο χώρος μας, έχει χαρακακτηριστική διάφορη του 2 ή 3.

Ορισμός 1. Έστω $\mathbb{F}$ σώμα με χαρακακτηριστική διάφορη του 2. Λέμε ότι ένα πολυώνυμο $p \in \mathbb{F}[x, y]$, με $\deg(p) = 3$ είναι σε μορφή Weierstraß αν είναι της μορφής

$$p(x, y) = y^2 - f(x),$$

όπου $f \in \mathbb{F}[x]$ είναι ένα μονικό πολυώνυμο με $\deg(f) = 3$.

Ορισμός 2. Έστω $\mathbb{F}$ σώμα με χαρακακτηριστική διάφορη του 2. Ένα πολυώνυμο $\bar{p} \in \mathbb{F}[x, y, z]$ με $\deg(\bar{p}) = 3$, καλείται κυβική Weierstraß αν είναι ίσο με την ομογενοποίηση ενός τριτοβάθμιου πολυωνύμου $p(x, y) \in \mathbb{F}[x, y]$. Με άλλα λόγια μια κυβική Weierstraß είναι μια κυβική μορφή $\bar{p}$ που μπορεί να γραφεί ως

$$\bar{p}(x, y, z) = y^2 z - \bar{f}(x, z),$$

όπου $\bar{f}(x, z) \in \mathbb{F}[x, z]$ είναι ένα μονικό πολυώνυμο με $\deg(\bar{f}) = 3$, το οποίο προκύπτει ως η ομογενοποίηση του μονικού $f \in \mathbb{F}[x]$.

Βλέπουμε τώρα μερικές ιδιότητες των κυβικών Weierstraß.

Πρόταση 1. Έστω σώμα $\mathbb{F}$ με χαρακακτηριστική διάφορη του 2. Έστω ένα πολυώνυμο βαθμού 3 σε μορφή Weierstraß, $p(x, y) = y^2 - f(x) \in \mathbb{F}[x, y]$ όπου $\bar{p}(x, y, z) \in \mathbb{F}[x, y, z]$ είναι η ομογενοποίηση του. Τότε έχουμε

(i) Τα ιδιάζοντα σημεία της επίπεδης προβολικής καμπύλης $Z(\bar{p})$ είναι τα σημεία της μορφής $(a, 0) = [a : 0 : 1]$, όπου a είναι μια πολλαπλή ρίζα του πολυωνύμου f. Συγκεκριμένα, ένα πολυώνυμο βαθμού 3 σε μορφή Weierstraß μπορεί να έχει το πολύ ένα ιδιάζον σημείο και αν το πολυώνυμο f δεν έχει πολλαπλή ρίζα σε κάποια αλγεβρική κλειστότητα του σώματος $\mathbb{F}$ τότε η $Z(\bar{p})$ είναι λεία.

(ii) Το σημείο ∞ που ορίζεται ως το προβολικό σημείο $[0:1:0]$, είναι το μοναδικό σημείο της $Z(\bar{p})$ που ανήκει στην ευθεία στο άπειρο. Είναι μάλιστα ένα σημείο καμπής της $Z(\bar{p})$ με εφαπτόμενη $T_\infty Z(\bar{p})$ να είναι η ευθεία στο άπειρον.

(iii) Το πολυώνυμο $\bar{p}(x,y,z)$ μένει αναλλοίωτο υπό τη γραμμική αλλαγή συντεταγμένων $(x,y,z) \mapsto (x,-y,z)$. Δηλαδή, η $Z(\bar{p})$ μένει αναλλοίωτη κάτω από τη $[x:y:z] \mapsto [x:-y:z]$ του $\mathbb{FP}^2$. (Όταν λέμε αναλλοίωτη εννοούμε ότι παραμένει η ίδια κάτω από τη δράση της ομάδας $PGL(2,\mathbb{F})$)

(iv) Τα σημεία της $Z(\bar{p})$, τα οποία παραμένουν ίδια μετά από την παραπάνω αλλαγή συντεταγμένων είναι το ∞ και τα σημεία της μορφής $(a,0) = [a:0:1]$, όπου α είναι μια ρίζα του πολυωνύμου f.

(v) Το $\bar{p}$ δεν μπορεί να παραγοντοποιηθεί σε δύο p_1, p_2 όπου το p_1 είναι ένα πρωτοβάθμιο πολυώνυμο και p_2 είναι ένα δευτεροβάθμιο πολυώνυμο, ακόμα και αν οι συντελεστές των p_1 και p_2 ανήκουν σε κάποια επέκταση του σώματος $\mathbb{F}$.

Απόδειξη:

(i) και (ii): Για τις μερικές παραγώγους του p έχουμε τα εξής:

$$\frac{\partial p}{\partial x} = -f'(x), \ \frac{\partial p}{\partial y} = 2y.$$

Εφόσον έχουμε ότι το σώμα $\mathbb{F}$ δεν έχει χαρακτηριστική 2, έχουμε ότι αν $(a,b) \in \mathbb{F}^2$

$$p(a,b) = \left.\frac{\partial p}{\partial x}\right|_{(a,b)} = \left.\frac{\partial p}{\partial x}\right|_{(a,b)} = 0 \Leftrightarrow$$

$$\Leftrightarrow b = 0 \text{ και } f(a) = f'(a) = 0.$$

Από την παραπάνω ισοδυναμία έχουμε ότι οι παράγωγοι ισούνται με μηδέν, αν και μόνο αν το σημείο $(a,0)$ είναι πολλαπλή ρίζα του πολυωνύμου f. Το ζητούμενο έπεται για το (i), δηλαδή τα ιδιάζοντα σημεία της επίπεδης προβολικής καμπύλης, είναι πεπερασμένα και μάλιστα είναι της μορφής $(a,0)$ όπου a είναι μια πολλαπλή ρίζα του πολυωνύμου f.

Συνεχίζουμε τώρα για το (ii). Εφόσον το f είναι ένα μονικό πολυώνυμο τρίτου βαθμού, έχουμε ότι $\bar{g}(x,y,0) = 0y^2 + \bar{f}(x,0) = x^3$, άρα το $\infty = [0:1:0]$ είναι το μοναδικό προβολικό σημείο της $Z(\bar{p})$, το οποίο βρίσκεται στην ευθεία στο άπειρο. Η επίπεδη προβολική καμπύλη $Z(\bar{p})$ τέμνει την ευθεία στο άπειρο στο ∞ με βαθμό πολλαπλότητας του σημείου τομής 3. Παρατηρούμε ότι το $\bar{f}(x,z)$ είναι ένα ομογενές

πολυώνυμο βαθμού 2 και άρα έχουμε

$$\left.\frac{\partial \bar{p}}{\partial z}\right|_{(0,1,0)} = 1^2 - \left.\frac{\partial \bar{f}}{\partial z}\right|_{(0,1,0)} = 1 \neq 0$$

και άρα πρόκειται για ομαλό σημείο της $Z(\bar{p})$.

(iii) : Το ότι το ομογενές πολυώνυμο $\bar{p}$ μένει αναλλοίωτο κάτω από την αλλαγή μεταβλητών $(x, y, z) \mapsto (x, -y, z)$, προκύπτει προφανώς από το γεγονός ότι παρουσιάζεται στον τύπο του ο όρος y^2. Επομένως η επίπεδη προβολική καμπύλη παραμένει αναλλοίωτη από τον $[x : y : z] \mapsto [x : -y : z]$, διότι αν έχουμε δύο προβολικά ισοδύναμα ομογενή πολυώνυμα τότε για τις επίπεδες προβολικές καμπύλες ισχύει η σχέση $Z(\bar{p}) = A^{-1}(Z(q))$, όπου $A \in GL(3, \mathbb{F})$ όπως έχουμε δείξει. Στην προκειμένη περίπτωση έχουμε

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Απ' όπου προκύπτει ότι $\bar{p}(\bar{x}) = q(A\bar{x}) = \bar{p}(\bar{x})$ και άρα η $Z(\bar{p})$ μένει αναλλοίωτη.

(iv) : Η παραπάνω αλλαγή συντεταγμένων στέλνει το $\mathbb{F}^2$ στον εαυτό του μέσω της $(x, y) \mapsto (x, -y)$. Άρα ένα σημείο του $\mathbb{F}^2$ μένει σταθερό αν και μόνο αν είναι της μορφής $(a, 0)$. Ένα σημείο αυτής της μορφής όμως ανήκει στο $Z(p)$ αν και μόνο αν έχουμε ότι $p(a, 0) = 0$, δηλαδή $f(a) = 0$. Αντίστοιχα, έχουμε για την ευθεία στο άπειρο έχουμε ότι κάθε προβολικό σημείο μέσω της αλλαγής μεταβλητών $[x : y : 0] \mapsto [x : -y : 0]$. Συνεπώς η ευθεία έχει ακριβώς δύο σταθερά σημεία, το $[1 : 0 : 0]$ και το $[0 : 1 : 0]$, όμως μόνο το $[0 : 1 : 0] \in Z(\bar{p})$.

(v) : Έστω ότι $\bar{p} = p_1 p_2$ και θα καταλήξουμε σε άτοπο. Έστω $p_1, p_2 \in \bar{\mathbb{F}}[x, y, z]$ όπου $\mathbb{F} \subseteq \bar{\mathbb{F}}$ είναι μια επέκταση του σώματος $\mathbb{F}$ που περιέχει τους συντελεστές των p_1 και p_2.

Επειδή το πολυώνυμο $\bar{f}$ που εμφανίζεται στο $\bar{p}$ είναι μονικό, τότε μπορούμε να γράψουμε τα p_1, p_2 ως

$$p_2 = x^2 + Bxy + Cy^2 + Dxy + Eyz + Fz^2,$$

$$p_1 = x + Gy + Hz,$$

όπου B, C, D, E, F, G, $H \in \bar{\mathbb{F}}$. Απ' όπου προκύπτει

$$\bar{p}(x, y, z) = (x + Gy + Hz)(x^2 + Bxy + Cy^2 + Dxz + Ayz + Fz^2).$$

Επίσης έχουμε ότι εφόσον $\bar{g}(x, y, 0) = x^3$, βρίσκουμε

$$B + G = 0, \tag{4.7}$$

$$CG = 0, \tag{4.8}$$

$$C + BG = 0. \tag{4.9}$$

Ας θεωρήσουμε αρχικά ότι $G = 0$. Τότε από τις παραπάνω εξισώσεις προκύπτει ότι $B = C = 0$. Αλλά τότε θα έχουμε

$$p_1 = x^2 + Dxz + Eyz + Fz^2,$$

$$p_2 = x + Hz.$$

Βλέπουμε ότι ενώ θα έπρεπε $p_1 p_2 = \bar{p} = yz^2 - \bar{f}(x, z)$, δεν μπορεί να προκύψει ο όρος $y^2 z$ από τον γινόμενο των δύο παραγόντων και άρα η περίπτωση ότι $G = 0$ δεν ισχύει.

Έστω ότι $G \neq 0$. τότε από τη σχέση (4.8) προκύπτει ότι $C = 0$ και από τα παραπάνω και τη σχέση (4.9) προκύπτει ότι $B = 0$. Σε αυτήν την περίπτωση βλέπουμε ότι δεν θα μπορούσε να ικανοποιείται η σχέση (4.7).

Οδηγηθήκαμε σε άτοπο, έτσι βρίσκουμε ότι δεν μπορεί να υπάρξει τέτοιου είδους παραγοντοποίηση για το ομογενές πολυώνυμο $\bar{p}$.

□

Θα δείξουμε τώρα, ότι κάθε κυβικό πολυώνυμο που ικανοποιεί τα παραπάνω είναι προβολικώς ισοδύναμο με μια κυβική Weierstraß.

Θεώρημα 1. Έστω $\mathbb{F}$ σώμα, επί του οποίου θεωρούμε μια κυβική μορφή $h \in \mathbb{F}[x, y, z]$ για την οποία υπάρχει ένα σημείο καμπής $p \in Z(h)$και έστω ένας προβολικός μετασχηματισμός $\tau : \mathbb{FP}^2 \to \mathbb{FP}^2$, ο οποίος επάγεται από τη γραμμική απεικόνιση $T : \mathbb{F}^3 \to \mathbb{F}^3$, που έχει πίνακα αναπαράστασης τον αντιστρέψιμο πίνακα $M \in GL(3, \mathbb{F})$. Έστω ότι ο M ικανοποιεί τα εξής:

(i) $\tau^2 = Id$,

(ii) Το σύνολο των σταθερών σημείων του πυρήνα του τ περιέχει το p και μια ευθεία L που δεν περιέχει το p,

(iii) $h \cdot M$ είναι ένα μη μηδενικό πολλαπλάσιο του h.

Τότε το σώμα $\mathbb{F}$ έχει χαρακτηριστική διάφορη του 2 και το h είναι προβολικώς ισοδύναμο με την κυβική $y^2z - \bar{f}(x,z)$, το οποίο είναι σε μορφή Weierstraß.

Παρατήρηση 1. Ισχύει γενικά ότι κάθε λεία κυβική καμπύλη C με ένα σημείο $p \in C$ είναι ισόμορφη με μια κυβική Weierstraß, μέσω ενός ισομορφισμού που απεικονίζει το σημείο p στο σημείο ∞. Σε αυτήν την εργασία όμως δεν έχουν εισαχθεί τέτοιες έννοιες μεταξύ αυτού του είδους των αντικειμένων, παρά μόνο έχουμε μιλήσει για την προβολική ισοδυναμία. Γενικά δεν είναι αλήθεια ότι κάθε λεία κυβική καμπύλη C είναι προβολικά ισοδύναμη με μια κυβική Weierstraß μέσω ενός προβολικού μετασχηματισμού που απεικονίζει το p στο σημείο ∞, λόγω του ότι το p ενδεχομένως να μην είναι σημείο καμπής της C.

Παρόλα αυτά αυτό που μας λέει το παραπάνω θεώρημα, είναι ότι δεν απομακρυνόμαστε πολύ από τη γενικότητα με τον περιορισμό της μελέτης μας σε κυβικές που βρίσκονται σε μορφή Weierstraß.

4.9 Ελλειπτικές Καμπύλες

Οι ελλειπτικές καμπύλες είναι ένα εργαλείο που αρχικά βοήθησε στην προσπάθεια υπολογισμού των ελλειπτικών ολοκληρωμάτων, κλάδος στον οποίο είχαν συνεισφορά μεγάλοι μαθηματικοί όπως ο Abel, Weierstraß, Jacobi.

Στα σύγχρονα μαθηματικά οι ελλειπτικές καμπύλες έχουν πολλές εφαρμογές στα θεωρητικά μαθηματικά και κυρίως στη Θεωρία Αριθμών. Χαρακτηριστικό παράδειγμα αποτελεί η απόδειξη του τελευταίου θεώρηματος του Fermat από τον Wiles, ο οποίος αξιοποίησε τη θεωρία των ελλειπτικών καμπυλών.

Μια ελλειπτική καμπύλη είναι μια αλγεβρική καμπύλη δηλαδή, σε γενικές γραμμές, είναι το σύνολο των σημείων που μηδενίζουν ένα κατάλληλο πολυώνυμο, αλλά παράλληλα έχουν και την αλγεβρική δομή της αβελιανής ομάδας.

Σε αυτό το σημείο θα κάνουμε μια συνοπτική αναφορά στη θεωρία των ελλειπτικών καμπυλών προσπαθώντας να τις συνδέσουμε με έννοιες που έχουμε ήδη συζητήσει.

Ορισμός 1. Μια ελλειπτική καμπύλη είναι το ζεύγος (C, p), όπου C είναι μια λεία προβολική κυβική καμπύλη και p είναι ένα σημείο της.

Όπως αναφέραμε και παραπάνω, έχουμε ότι κάθε κυβική καμπύλη μπορεί να γραφεί σε μορφή Weierstraß. Έχουμε ότι κάθε ελλειπτική καμπύλη μπορεί να γραφεί σε μορφή Weierstraß.

Παρατήρηση 1. Η μορφή Weierstraß δεν είναι η μοναδική χρήσιμη μορφή με την οποία μπορούμε να γράψουμε την εξίσωση κάποιας ελλειπτικής καμπύλης. Δίνουμε

τυπικά κάποιες άλλες μορφές στις οποίες μπορούμε να γράψουμε μια ελλειπτική καμπύλη $E = (C, p)$

(i) $E : y^2 = x(x-1)(x-\lambda)$ (μορφή του *Legendre*), όπου $\lambda \in \mathbb{R} \setminus \{0, 1\}$.

(ii) $E : y^2 = (1-x^2)(1-k^2x^2)$ (μορφή του *Jacobi*), όπου $k \in \mathbb{C} \setminus \{0, \pm 1\}$.

Ορισμός 2. Έστω ότι C είναι μια καμπύλη η οποία ορίζεται από τη σχέση

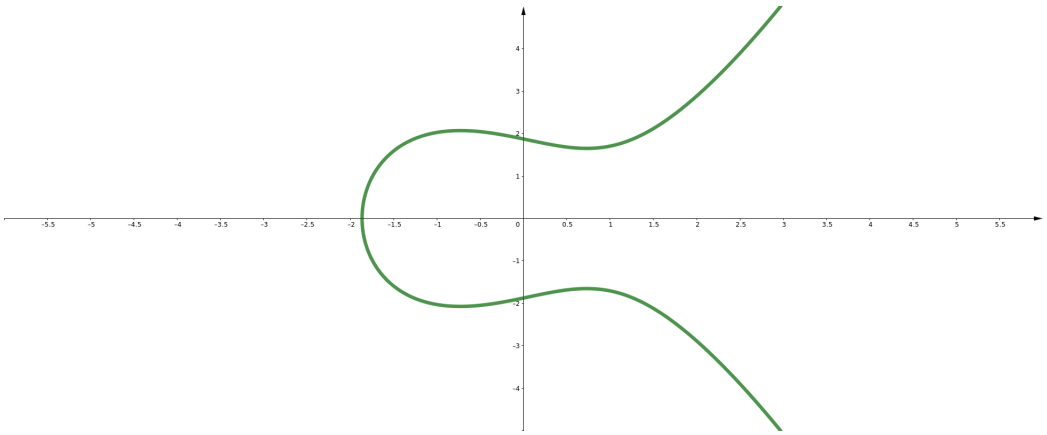
$$y^2 = x^3 + ax + b,$$

όπου a, $b \in \mathbb{F}$.

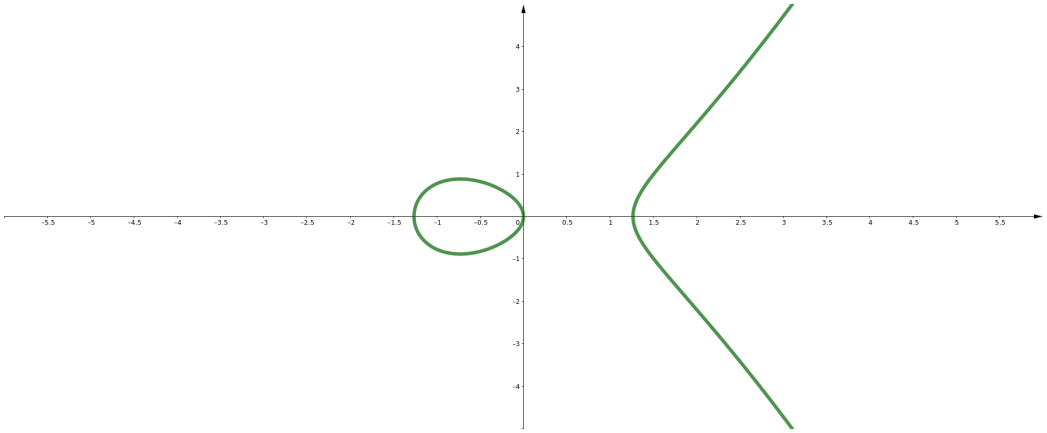
Ορίζουμε τη διακρίνουσα της C να είναι

$$\Delta = -16(4a^3 + 27b^2).$$

Εάν έχουμε $\Delta < 0$, τότε η ελλειπτική καμπύλη αναπαριστάται γεωμετρικά ως



Ενώ εάν έχουμε ότι $\Delta > 0$ τότε η ελλειπτική καμπύλη αναπαρίσταται γεωμετρικά ως



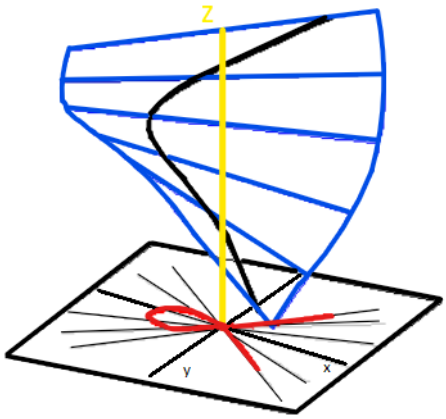
Λήμμα 1. Έστω ότι C είναι μια καμπύλη που δίνεται ως

$$y^2 = x^3 + ax + b. \tag{4.10}$$

Αν ομογενοποιήσουμε την (4.10) θα πάρουμε

$$\bar{C} : y^2 z = x^3 z + axz + bz^2.$$

Τότε θα έχουμε ότι αν $\bar{C}$ είναι η καμπύλη που προκύπτει από την ομογενοποίηση, το ζεύγος $(\bar{C}, [0 : 1 : 0])$ είναι μια ελλειπτική καμπύλη αν και μόνο αν $\Delta \neq 0$.



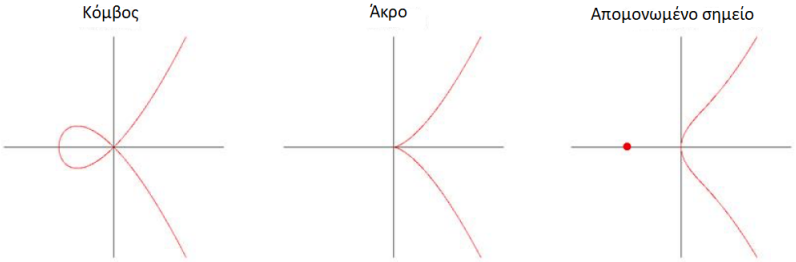
Απόδειξη: Παρατηρούμε ότι αν έχουμε μια καμπύλη C ορισμένη όπως η σχέση (4.10) τότε το προβολικό σημείο $[0 : 1 : 0]$ ανήκει στην $\bar{C}$. Οπότε για να αποδείξουμε το ζητούμενο θα αξιοποιήσουμε το Θεώρημα 4.8.1. Από Θεώρημα 4.8.1 (ii) έχουμε ότι το σημείο $[0 : 1 : 0]$ είναι σημείο καμπής και άρα θέλουμε να αποδείξουμε ότι η C είναι λεία αν και μόνο αν $\Delta \neq 0$.

Ας θεωρήσουμε τώρα ότι $f(x) = x^3 + ax + b$. Παρατηρούμε ότι η ποσότητα Δ είναι ακριβώς η διακρίνουσα αυτού του τριτοβάθμιου πολυωνύμου όπως προκύπτει και από τη σχέση του Cardano.

Μελετώντας τώρα τις μερικές παραγώγους της (4.10) και συνδυάζοντας και με τα αποτελέσματα της Πρότασης 4.8.1(i) έχουμε ότι η C έχει ιδιάζον σημείο αν και μόνο αν το f έχει πολλαπλή ρίζα και άρα αν και μόνο αν $\Delta = 0$.

□

Παρατήρηση 2. Παρατηρούμε ότι αν μια καμπύλη C παρουσιάζει ιδιάζον σημείο, τότε τα ρητά σημεία της μπορούν να μελετηθούν προβάλλοντας τα από ιδιάζον σημείο. Δηλαδή βρίσκουμε προβολικό μετασχηματισμό που απεικονίζει το ιδιάζον σημείο στο σημείο ∞ και μελετάμε τις εικόνες των σημείων μέσα από αυτόν τον προβολικό μετασχηματισμό.



4.9.1 Μία εφαρμογή στην κρυπτογραφία

Τα κρυπτοσυστήματα ελλειπτικών καμπυλών, προτάθηκαν από τους Miller και Koblitz ανεξάρτητα και επομένως μπορούμε να πούμε ότι δεν είναι κάτι καινούργιο στο χώρο της κρυπτογραφίας. Οι ελλειπτικές καμπύλες αποτελούν ένα εργαλείο με το οποίο μπορούν να υλοποιηθούν γνωστά κρυπτοσυστήματα δημόσιου κλειδιού.

Μπορούμε να ορίσουμε ελλειπτικές καμπύλες σε διάφορα σώματα, παρόλα αυτά στην κρυπτογραφία οι ελλειπτικές καμπύλες αποκτούν χρησιμότητα, όταν ορίζονται επί πεπερασμένων σωμάτων. Για τους σκοπούς αυτής της ενότητας θα δούμε κάποιες βασικές έννοιες της ελλειπτικής κρυπτογραφίας όπου θα έχουμε θεωρήσει τις ελλειπτικές καμπύλες ορισμένες στο σώμα των πραγματικών αριθμών. Προτρέπουμε μάλιστα τον αναγνώστη να διαβάσει τα [18], [19], [20] εάν θέλει να αποκομίσει περισσότερες πληροφορίες για το θέμα.

Όπως έχουμε αναφέρει και παραπάνω, η εξίσωση μια ελλειπτικής καμπύλης δίνεται σε μορφή Weierstraß από την

$$y^2 = x^3 + ax + b,$$

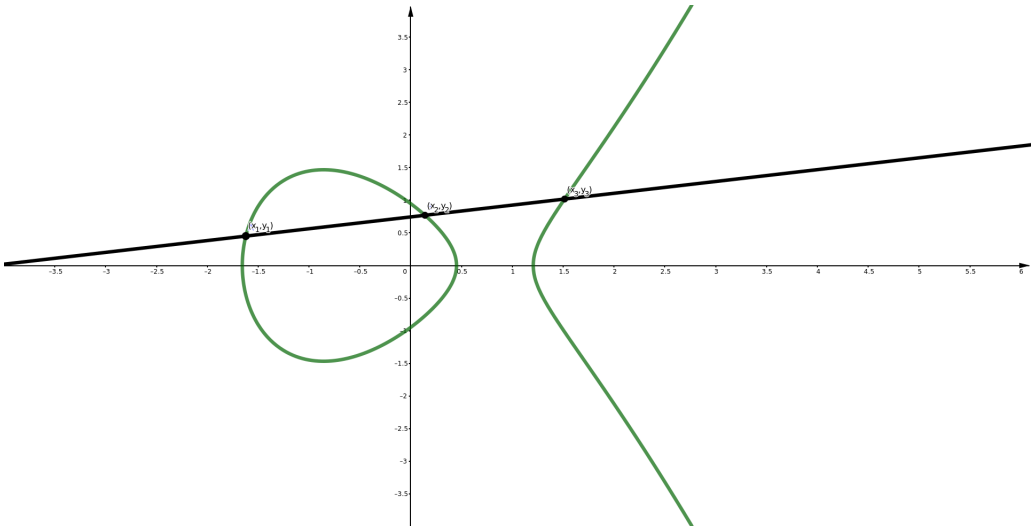
όπου a, $b \in \mathbb{R}$.

Θεωρούμε δύο διαφορετικά σημεία επί της ελλειπτικής καμπύλης έστω (x_1, y_1) και (x_2, y_2) και μια ευθεία με εξίσωση $\varepsilon : y = \lambda x + c$, όπου λ, $c \in \mathbb{R}$. Θεωρούμε ότι η ε τέμνει την ελλειπτική καμπύλη στα δύο σημεία που ορίσαμε.

Αντικαθιστώντας τώρα την εξίσωση της ευθείας στην ελλειπτική καμπύλη έχουμε

$$(\lambda x + c)^2 = x^3 + ax + b. \tag{4.11}$$

Η (4.11) είναι μία τριτοβάθμια εξίσωση, της οποίας γνωρίζουμε ότι δύο ρίζες της είναι τα x_1 και x_2. Θα υπάρχει και μια τρίτη ρίζα που αντιστοιχεί στο σημείο της ε, $(x_3, \lambda x_3 + c)$. Συνεπώς η ευθεία τέμνει την καμπύλη σε τρία σημεία.

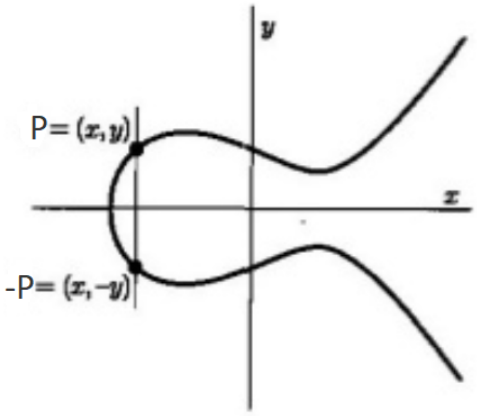


Όπως βλεπουμε και στο παραπάνω σχήμα η ελλειπτική καμπύλη αποτελείται από τις δύο καμπύλες και ένα σημείο O, το οποίο είναι το σημείο στο άπειρο. Όπως αναφέραμε και παραπάνω αν έχουμε ένα ιδιάζον σημείο, προκειμένου να μελετήσουμε τα ρητά σημεία της ελλειπτικής καμπύλης, προβάλλουμε την καμπύλη από το ιδιάζον σημείο, μέσω ενός προβολικού μετασχηματισμού που στέλνει το ιδιάζον σημείο στο σήμειο ∞.

Οταν η διακρίνουσα της ελλειπτικής καμπύλης είναι $\Delta = 0$ τότε την ονομάζουμε ιδιάζουσα. Ειδικότερα για μια ιδιάζουσα ελλειπτική καμπύλη, υπάρχουν κατάλληλα a και b, ώστε τα κοινά σημεία της καμπύλης με την ευθεία να μην είναι τρία.

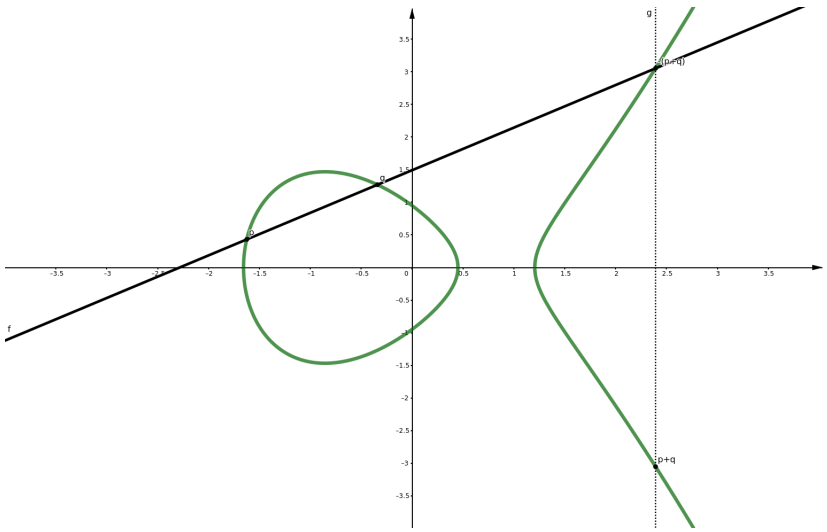
Ενδιαφέρον παρουσιάζει το γεγονός, ότι μπορούμε να ορίσουμε πρόσθεση σημείων μιας ελλειπτικής καμπύλης. Η πρόσθεση μάλιστα βασίζεται στο γεγονός, ότι μια ευθεία μπορεί να τέμνει την ελλειπτική καμπύλη σε τρία σημεία.

Αποτελεί προφανές συμπέρασμα παρατηρώντας γεωμετρικά μια ελλειπτική καμπύλη, ότι αυτή είναι συμμετρική ως προς τον άξονα x. Κατά αυτόν τον τρόπο μάλιστα μπορούμε να ορίσουμε και το αντίθετο σημείο ενός σημείου p της καμπύλης, να είναι το συμμετρικό του ως προς τον άξονα x. Το οποίο μάλιστα το συμβολίζουμε $-p$.



Παρατηρούμε τώρα ότι αν $p = (x, y)$ τότε $-p = (x, -y)$. Γεωμετρικά αυτό περιγράφεται ως εξής. Αρχικά, υπολογίζουμε την ευθεία που διέρχεται από το σημείο p και σημείο O. Το τρίτο σημείο της καμπύλης είναι $-p$. Αυτό συμβαίνει επειδή, το σημείο O είναι εκείνο το σημείο, στο οποίο τέμνονται όλες οι παράλληλλες με τον άξονα y.

Έχουμε ότι το ουδέτερο στοιχείο της πρόσθεσης σημείων μιας ελλειπτικής καμπύλης είναι το O. Θεωρούμε τώρα τα σημεία p και q μιας ελλειπτικής καμπύλης. Η ευθεία, η οποία διέρχεται από τα p και q, τέμνει την καμπύλη σε ένα τρίτο σημείο το $\Gamma(p+q)$. Το σημείο $p + q$ θα είναι το συμμετρικό του παραπάνω, ως προς τον άξονα x. Γεωμετρικά αυτό φαίνεται στο παρακάτω σχήμα.



Στην περίπτωση όπου $p = q$, η ευθεία που ορίζεται είναι η T_pC, όπου με C εννοούμε την καμπύλη μας. Θα έχουμε ότι η T_pC θα τέμνει την καμπύλη μας στο σημείο q το οποίο είναι το $-2p$ και το συμμετρικό του είναι το $2p$.

Θα προσπαθήσουμε τώρα να περιγράψουμε την πρόσθεση σε μια ελλειπτική καμπύλη αλγεβρικά. Έστω δύο σημεία $p = (x_1, y_1)$ και $q = (x_2, y_2)$. Τότε έχουμε ότι η ευθεία που διέρχεται από αυτά τα σημεία είναι η

$$y = \frac{y_2 - y_1}{x_2 - x_1}x + \frac{y_2(x_2 - x_1) - x_2(y_2 - y_1)}{x_2 - x_1}.$$

Αν θέλουμε να βρούμε το άθροισμα αυτών των δύο σημείων θα έχουμε ότι για $p + q = (x_3, y_3)$

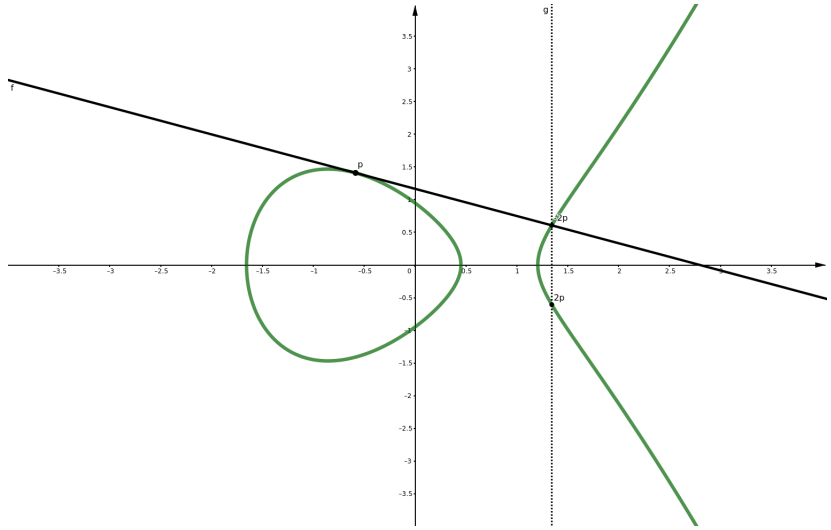
$$x_3 = \frac{y_2 - y_1}{x_2 - x_1}^2 - x_1 - x_2,$$
$$y_3 = \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1.$$

Σημειώνουμε ότι για τις παραπάνω σχέσεις θεωρήσαμε ότι τα σημεία είναι διαφορετικά. Μελετάμε εδώ κάποιες σημαντικές περιπτώσεις.

Έστω ότι $q = -p$. Τότε σε αυτήν την περίπτωση η κλίση γίνεται άπειρη, άρα η ευθεία θα είναι παράλληλη με τον άξονα y και άρα οδηγούμαστε στο σημείο στο άπειρο το O.

Έστω ότι $q = p$. Τότε η κλίση της ευθείας υπολογίζεται από την παραγώγιση της εξίσωσης της ελλειπτικής καμπύλης και είναι ίση με

$$\frac{3x_1^2 + a}{2y_1}.$$



Ενώ οι συντεταγμένες ορίζονται από τις σχέσεις που υπολογίστηκαν παραπάνω για διαφορετικά p και q. Όπως αναφέραμε, οι ελλειπτικές καμπύλες αποκτούν ενδιαφέρον για την κρυπτογραφία όταν ορίζονται σε πεπερασμένα σώματα και συγκεκριμένα στο σώμα $\mathbb{Z}_p$ όπου ο p είναι πρώτος αριθμός μεγαλύτερος του 2. Η πράξη της πρόσθεσης είναι επίσης καλά ορισμένη για το $\mathbb{Z}_p$. Απαραίτητο είναι η ελλειπτική καμπύλη να έχει τρεις διαφορετικές ρίζες, όποτε προκύπτει ο παρακάτω ορισμός.

Ορισμός 3. Μια ελλειπτική καμπύλη ορισμένη στο $\mathbb{Z}_p$ για κάποιον πρώτο $p > 3$, είναι το σύνολο των στοιχείων $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ τα οποία ικανοποιούν την εξίσωση

$$y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p),$$

όπου a, $b \in \mathbb{Z}_p$ και $\Delta \equiv 0 (\mathrm{mod}\, p)$.

Η πρόσθεση δύο σημείων της ελλειπτικής καμπύλης ορίζεται ακριβώς με τον ίδιο τρόπο σε πεπερασμένο σώμα, όπως γινόταν και για το $\mathbb{R}$. Δηλαδή αν θεωρήσουμε δύο σημεία $q = (x_1, y_1)$ και $r = (x_2, y_2)$ τότε το $q + r = (x_3, y_3)$ είναι ένα σημείο πάνω στην ελλειπτική καμπύλη με

$$x_3 \equiv \lambda^2 - x_1 - x_2 (\mathrm{mod}\, p),$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, p).$$

όπου

$$\lambda \equiv \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\, p), q \neq r \\ \frac{3x_1^2 + a}{2y_1} (\mathrm{mod}\, p), q = r \end{cases}.$$

Μια πολύ σημαντική ιδιότητα στις ελλειπτικές καμπύλες που είναι ορισμένες επί ενός

σώματος $\mathbb{Z}_p$, είναι το γεγονός ότι όλα τα σημεία της ελλειπτικής καμπύλης μαζί με το σημείο στο άπειρο O ορίζουν κυκλική υποομάδα και άρα οποιοδήποτε σημείο ανήκει στην ελλειπτική καμπύλη, πέραν του O, είναι γεννήτορας της.

Αντίστοιχα με την πρόσθεση, μπορούμε να ορίσουμε τον βαθμωτό πολλαπλασιασμό σημείου μιας αλγεβρικής καμπύλης με στοιχείο από το σώμα. Αν έχουμε ένα σημείο $q \in C$ και $n \in \mathbb{F}$ τότε μπορούμε να ορίσουμε το σημείο nq να είναι εκείνο που προκύπτει μετά από $n-1$ επαναλήψεις της πρόσθεσης του q με τον εαυτό του.

Ορισμός 4. Έστω μια ελλειπτική καμπύλη C ορισμένη στο $\mathbb{Z}_p$. Έστω ένα σημείο $q \in C$ και ένα σημείο p το οποίο αποτελεί κάποιο πολλαπλάσιο του q. Το πρόβλημα του διακριτού λογαρίθμου στην ελλειπτική καμπύλη είναι ο καθορισμός της λύσης n, για την οποία έχουμε ότι $np = q$.

Έχει δειχθεί ότι η πολυπλοκότητα των μεθόδων που επιχειρούν να λύσουν το πρόβλημα του διακριτού λογαρίθμου στις ελλειπτικές καμπύλες είναι της μορφής n^a, $a > 0$. Είναι δηλαδή εκθετικά πιο αργοί από τη λογαριθμική πολυπλοκότητα του υπολογισμού βαθμωτών γινομένων του q. Δηλαδή τα κρυπτοσυστήματα ελλειπτικών καμπυλών είναι πολύ ασφαλή, με τα τωρινά δεδομένα.

Παρόλα αυτά υπάρχει η κατηγορία των υπεριδιάζουσων ελλειπτικών καμπυλών, οι οποίες δεν θεωρούται ασφαλείς, διότι καταρρέουν σε επιθέσεις που στοχεύουν στον ισομορφισμό μεταξύ των ελλειπτικών καμπυλών και των πεπερασμένων σωμάτων.

Τα κρυπτοσυστήματα ελλειπτικών καμπυλών βασίζονται πάνω στην αλγεβρική δομή που προσδίδει η πράξη της πρόσθεσης σε αυτά και δύο από αυτά είναι τα εξής:

- Κρυπτοσύστημα ElGamal
- Κρυπτοσύστημα Massey-Omura

Βιβλιογραφία

[1] Ι.Δ. Πλατής : *Γεωμετρία, Σημειώσεις Μέρος ΙΙ*. Πανεπιστήμιο Κρήτης, 2020.

[2] D.Hilbert, S. Cohn-Vossen: *Geometry and the Imagination*. Chelsea Publishing Company, 1990.

[3] Δ. Α. Βάρσος, Δ. Ι. Δεριζιώτης, Ι. Π. Εμμανουήλ, Μ. Π. Μαλιάκας, Α. Δ. Μελάς, Ολ. Π Ταλέλλη : *Μια Εισαγωγή στη Γραμμική Άλγεβρα*. Εκδόσεις Σοφία, 2012.

[4] Igor R. Shafarevich, Alexey Remizov: *Linear Algebra and Geometry*. Springer-Verlag Berlin Heidelberg, 2013.

[5] Stephen H. Friedberg, Arnold J. Insel, Lawrence E. Spence: *Linear Algebra (*2^{nd} *Edition)*. Pearson Education, 2003.

[6] Seymour Lipschutz: *Schaum's Outline of Theory and Problems of Linear Algebra*. McGraw-Hill, 1991.

[7] John B. Fraleigh: *Εισαγωγή στην Άλγεβρα*, Μετάφραση του Απόστολος Γιαννόπουλος:. Πανεπιστημιακές εκδόσεις Κρήτης, 2015.

[8] Δημήτρης Ι. Δεριζιώτης, Δημήτρης Β. Βάρσος, Ιωάννης Π. Εμμανουήλ, Μιχαήλ Π. Μαλιάκας, Ολυμπία Π. Ταλέλλη: *Μια εισαγωγή στην Άλγεβρα* Γ΄ Έκδοση. Εκδόσεις Σοφία, 2012.

[9] Ε. Βασιλείου: *Στοιχεία Προβολικής Γεωμετρίας*. Εκδόσεις Συμμετρία, 2010.

[10] Nigel Hitchin: *Projective Geometry*. b3 Course,University of Oxford, 2003.

[11] Jean Gallier: *Geometric Methods and Applications*. Springer, New York, NY, 2001.

[12] David A. Brannan, Matthew F. Esplen, Jeremy J. Gray: *Geometry*. Cambridge University Press, 2011.

[13] Andrew Dancer, Balazs Szendroi: *Lecture Notes on Projective Geometry*. University of Oxford, 2020.

[14] Cameron Krulewski: *Real Projective Space: An Abstract Manifold*. Colby College, 2017.

[15] Jürgen Richter-Gebert: *Perspectives on Projective Geometry*. Springer-Verlag Berlin Heidelberg, 2011.

[16] W.D. Gillam: *Projective Geometry*. Lecture Notes, Bogazici University, 2014.

[17] Dino Festi: *Notes on Elliptic Curves*. Johannes Gutenberg University, 2018.

[18] Albrecht Beutelspacher, Ute Rosenbaum: *Projective Geometry: From Foundations to Applications*. Cambridge University Press, 1998.

[19] Raymond van Bommel: *Lecture notes on elliptic curve cryptography* Leiden University, 2017.

[20] Β. Κάτος, Γ. Στεφανίδης: *Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης*. Εκδόσεις ΖΥΓΟΣ, 2003.