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

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΩΝ ΑΓΩΓΗΣ

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών
"ΔΙΔΑΚΤΙΚΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΑΤΑΣΚΕΥΕΣ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

ΧΡΗΣΤΟΣ ΧΡΗΣΤΙΔΗΣ
Α.Μ. Δ200606

Επιβλέπων Καθηγητής
ΕΥΑΓΓΕΛΟΣ ΡΑΠΤΗΣ

ΑΘΗΝΑ 2010

Η παρούσα Διπλωματική Εργασία
εκπονήθηκε στα πλαίσια των σπουδών
για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης
που απονέμει το

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

«Διδακτική και Μεθοδολογία των Μαθηματικών»

Εγκρίθηκε την ……από εξεταστική Επιτροπή αποτελούμενη από τους:

Ονοματεπώνυμο	Βαθμίδα	Υπογραφή
1) Ευάγγελος Ράπτης (επιβλέπων Καθηγητής)	Αν. Καθηγητής	……
2) Ευστάθιος Γιαννακούλιας	Καθηγητής	……
3) Δημήτριος Βάρσος	Αν. Καθηγητής	……

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ όλους τους καθηγητές του μεταπτυχιακού προγράμματος οι οποίοι με τις γνώσεις τους με βοήθησαν να στοχαστώ και να προβληματιστώ πάνω στη διδακτική και τα μαθηματικά, να διευρύνω τις γνώσεις μου αλλά και τον τρόπο σκέψης μου.

Ευχαριστώ επίσης θερμά τους καθηγητές κ. Ευστάθιο Γιαννακούλια και κ. Δημήτριο Βάρσο για τις πολύτιμες συμβουλές τους. Ιδιαίτερα όμως ευχαριστώ τον επιβλέποντα καθηγητή μου κ. Ευάγγελο Ράπτη για τη συνεχή του καθοδήγηση και αμέριστη συμπαράστασή του σε όλα τα στάδια εκπόνησης αυτής της εργασίας.

Την εργασία αυτή την αφιερώνω στους δικούς μου ανθρώπους, οικογένεια και φίλους, για την υπομονή τους, τη συμπαράστασή τους και την πίστη που μου έδειξαν κατά τη διάρκεια των σπουδών μου.

ΚΑΤΑΣΚΕΥΕΣ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

Χρηστίδης Χρήστος

Υποβλήθηκε στο Πανεπιστήμιο Αθηνών
στα πλαίσια των σπουδών
για την απόκτηση του
Μεταπτυχιακού Διπλώματος Ειδίκευσης
στη Διδακτική και Μεθοδολογία των Μαθηματικών
που απονέμει
το Τμήμα Μαθηματικών

Αθήνα 2010

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή……..5

ΚΕΦ. 1: Ομάδες – Υποομάδες…… …8

ΚΕΦ. 2: Δακτύλιοι – Σώματα ……...17

ΚΕΦ. 3: Διανυσματικοί Χώροι ……22

ΚΕΦ. 4: Ανάγωγα Πολυώνυμα ……24

ΚΕΦ. 5: Επεκτάσεις Σωμάτων ……..29

ΚΕΦ. 6: Στοιχεία Θεωρίας Galois ...……38

ΚΕΦ. 7: Γεωμετρικές κατασκευές με κανόνα και διαβήτη ……...42

ΚΕΦ. 8: Κατασκευασιμότητα κανονικών πολυγώνων ……..55

ΚΕΦ. 9: Η κατασκευή του κανονικού πενταγώνου με κανόνα και διαβήτη

Α.Η κατασκευή του κανονικού πενταγώνου από τον Ευκλείδη…..63

Β.Η κατασκευή του κανονικού πενταγώνου στο σχολικό βιβλίο…70

Γ.Μία διδακτική πρόταση κατασκευής του κανονικού δεκαγώνου με την αναλυτικο-συνθετική μέθοδο……... 73

Βιβλιογραφία ……79

ΕΙΣΑΓΩΓΗ

Οι αρχαίοι Έλληνες είχαν δείξει ενδιαφέρον για το ποια είδη γεωμετρικών σχημάτων μπορούν να κατασκευαστούν μόνο με τη χρήση κανόνα και διαβήτη. Ένα από τα δυσκολότερα προβλήματα αυτής της κατηγορίας αφορούσε τα κανονικά πολύγωνα. Το ερώτημα είναι: Για ποιες τιμές του n μπορεί να κατασκευαστεί κανονικό πολύγωνο με n πλευρές (με κανόνα και διαβήτη); Τονίζουμε τη διαφορά μεταξύ της έκφρασης ότι το κανονικό n-γωνο υπάρχει και της έκφρασης ότι αυτό μπορεί να κατασκευαστεί. Τέτοια πολύγωνα υπάρχουν για όλες τις τιμές του n απλά σχηματίζοντας σε έναν κύκλο επίκεντρες γωνίες $360°/n$. Αυτό όμως απαιτεί κάτι παραπάνω από έναν κανόνα και έναν διαβήτη· απαιτεί ένα απείρως ακριβές μοιρογνωμόνιο. Για παράδειγμα, υπάρχουν κανονικά 7-γωνα αλλά όπως θα δούμε δεν κατασκευάζονται με κανόνα και διαβήτη.

Ο Carl Friedrich Gauss (1777-1855) αποτελεί μαζί με τον Αρχιμήδη και τον Νεύτωνα έναν από τους τρεις μεγαλύτερους μαθηματικούς όλων των εποχών. Ο Gauss καλείτο *Mathematicorum princeps*, (Πρίγκιπας των Μαθηματικών), και η εκτίμηση στο άτομο του θα μπορούσε σίγουρα να ήταν μεγαλύτερη, αν είχε γνωστοποιήσει το περιεχόμενο του ημερολογίου του που παρέμενε μυστικό μέχρι το 1898, σαράντα τρία χρόνια μετά τον θάνατο του. Σε αυτό υπήρχαν αποτελέσματα τα οποία προέβλεπαν πολλές από τις ανακαλύψεις στα Μαθηματικά του δεύτερου μισού του δέκατου ένατου αιώνα. Ο Gauss για λόγους τελειομανίας και αποφυγής προστριβών δεν δημοσίευε όλα του τα αποτελέσματα (Davis, 2005).

Λέγεται ότι ο Gauss ήταν σε θέση να κάνει αριθμητικές πράξεις, πριν καν μιλήσει, ενώ από μικρή ηλικία βοηθούσε τον πατέρα του να υπολογίζει την πληρωμή για τα έργα που αναλάμβανε. Έχει μείνει μάλιστα γνωστό ένα «κατόρθωμά» του που αναφέρει ότι μόλις 8 χρονών μπόρεσε, προς μεγάλη έκπληξη του δάσκαλου, να υπολογίσει αμέσως το άθροισμα των 100 πρώτων φυσικών ακεραίων ενώ στους συμμαθητές του πήρε παραπάνω από μία ώρα!

Εξ΄ αιτίας όλων αυτών των «περίεργων φαινομένων» και ταλέντων που παρουσίαζε ο νεαρός Gauss ανάγκασε ουσιαστικά τον πατέρα του να του επιτρέψει να πάει στο Γυμνάσιο αντί να σταματήσει και να βοηθήσει την οικογένειά του στα πιο πρακτικά επαγγέλματα. Εκεί ήταν που ξεδιπλώθηκε ραγδαία όλο το ταλέντο του προς τις θετικές επιστήμες.

Μετά το Γυμνάσιο συνέχισε τις σπουδές του στα Μαθηματικά στο κολλέγιο Carolinum όπου πέρασε τρία πολύ δημιουργικά χρόνια. Παρ΄ όλα αυτά τα μαθηματικά δεν είχαν ακόμα κερδίσει το 100% της καρδιάς του γιατί ταυτόχρονα είχε μεγάλη έφεση και στις γλώσσες. Κάποιοι πιστεύουν πως την τελική απόφαση, να σπουδάσει Μαθηματικά στο Πανεπιστήμιο του Gottingen, την πήρε αφού ανακάλυψε ότι μπορεί κανείς να κατασκευάσει ένα κανονικό 17-γωνο μόνο με κανόνα και διαβήτη. Ο Gauss ήταν πολύ περήφανος για αυτή του την ανακάλυψη και εξέφρασε την επιθυμία η επιτάφια πλάκα του να έχει χαραγμένο το κανονικό 17-γωνο. Η επιθυμία του δεν πραγματοποιήθηκε, αφού ο γλύπτης το αρνήθηκε λέγοντας ότι θα μοιάζει περισσότερο με κύκλο. Το κοντινότερο στην επιθυμία του ήταν το 17-κόρυφο αστέρι που κοσμεί ένα άγαλμα που ανεγέρθηκε προς τιμήν του.

Σημαντικότερος από την αναλυτική κατασκευή του κανονικού 17-γώνου υπήρξε ο κανόνας του Gauss για το ποια ακριβώς κανονικά n-γωνα είναι κατασκευάσιμα. Ο Gauss απέδειξε ότι το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη όταν $n = 2^r p_1 ... p_s$, όπου οι p_i να είναι διαφορετικοί πρώτοι της μορφής $2^{2^n} + 1$. Ο Gauss ήταν βέβαιος για την ισχύ του αντιστρόφου, δεν κατάφερε όμως να το αποδείξει. Την απόδειξη έδωσε ο Pierre Wantzel (1814-1848) το 1837.

Στην παρούσα διπλωματική εργασία δίνεται μια αναλυτική απόδειξη του παραπάνω κανόνα (ευθύ και αντίστροφο), αφού πρώτα αναφερθούν αναλυτικά όλα τα στοιχεία από την Άλγεβρα και τη Θεωρία Galois που είναι απαραίτητα για την θεμελίωσή της.

Το τελευταίο κεφάλαιο της εργασίας αναφέρεται στην κατασκευή του κανονικού πενταγώνου με κανόνα και διαβήτη.

Παρουσιάζεται η κατασκευή του κανονικού πενταγώνου με κανόνα και διαβήτη από τον Ευκλείδη όπως αυτή παρουσιάζεται στα Στοιχεία, καθώς και η κατασκευή του κανονικού πενταγώνου σύμφωνα με το σχολικό βιβλίο της Β' Λυκείου.

Επίσης παρουσιάζεται και μια διδακτική προσέγγιση κατασκευής του κανονικού δεκαγώνου (άρα και του κανονικού πενταγώνου) από τους μαθητές της Β' Λυκείου, με την αναλυτικο-συνθετική μέθοδο.

ΚΕΦΑΛΑΙΟ 1

ΟΜΑΔΕΣ – ΥΠΟΟΜΑΔΕΣ

Ορισμός 1.1. **Ομάδα** λέγεται ένα μη κενό σύνολο G εφοδιασμένο με μια πράξη * η οποία σε κάθε ζεύγος $x, y \in G$, αντιστοιχεί ένα τρίτο στοιχείο $x * y \in G$, που ικανοποιεί τα εξής αξιώματα :

(1) Υπάρχει $e \in G : x * e = e * x = x$, *για κάθε* $x \in G$. (*ύπαρξη μοναδιαίου*)

(2) Ισχύει

$(x * y) * z = x * (y * z)$, *για κάθε* $x, y, z \in G$. (*προσεταιριστική ιδιότητα*)

(3) Για κάθε $x \in G$ υπάρχει $x' \in G: x * x' = x' * x = e$. (*ύπαρξη αντιστρόφου*)

Το e λέγεται **μοναδιαίο στοιχείο** ή απλά **μονάδα**. Το x' λέγεται **αντίστροφο** του x και συμβολίζεται με x^{-1}.

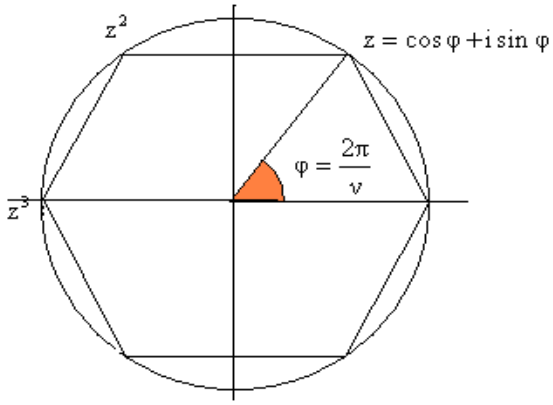
Η ομάδα λέγεται **μεταθετική** ή **αβελιανή** όταν επιπλέον ικανοποιεί το αξίωμα $x * y = y * x, \forall x, y \in G$.

Ορισμός 1.2. Αν η ομάδα είναι πεπερασμένη τότε ο ακέραιος $|G| = n > 1$ λέγεται **τάξη της ομάδας**.

Ορισμός 1.3. Αν p πρώτος, τότε μια πεπερασμένη ομάδα G θα λέγεται **p-ομάδα** αν η τάξη της είναι δύναμη του p.

Ορισμός 1.4. Αν G ομάδα, τότε **τάξη ενός στοιχείου** $x \in G$ ονομάζεται, αν υπάρχει, ο ελάχιστος θετικός ακέραιος m για τον οποίο x^m=e (διαφορετικά το άπειρο).

Παράδειγμα. Το σύνολο $G = P_n = \{z \in \mathbb{C} : z^n = 1\}$, των n-οστών μιγαδικών ριζών της μονάδος είναι ομάδα με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών. Το P_n αποτελείται από τις κορυφές ενός κανονικού πολυγώνου με κέντρο το μηδέν και μία κορυφή στο (1,0), συνεπώς εγγεγραμμένου στον μοναδιαίο κύκλο του μιγαδικού επιπέδου.



Ορισμός 1.5. Μια απεικόνιση $F: (G_1, *_1) \to (G_2, *_2)$ μεταξύ δύο ομάδων λέγεται **ομομορφισμός** ομάδων όταν ικανοποιεί την σχέση:

$F(x *_1 y) = F(x) *_2 F(y), \forall x, y \in G_1.$

Ορισμός 1.6. Ένας ομομορφισμός $F: (G_1, *_1) \to (G_2, *_2)$ μεταξύ δύο ομάδων λέγεται **μονομορφισμός** ομάδων όταν είναι 1-1. Δηλ.

$F(x) = F(y) \Longrightarrow x = y.$

Ο ομομορφισμός λέγεται **επιμορφισμός** ομάδων όταν είναι επί. Δηλ.

$\forall y \in G_2, \exists x \in G_1 : F(x) = y.$

Τέλος λέγεται **ισομορφισμός** όταν είναι ταυτόχρονα 1-1 και επί.

Παρατηρήσεις:

(1) Δύο ομάδες $(G_1,*_1),(G_2,*_2)$ λέγονται **ισόμορφες**, όταν υπάρχει κάποιος ισομορφισμός που απεικονίζει την μία στην άλλη.

(2) Δύο ισόμορφες ομάδες $(G_1,*_1),(G_2,*_2)$ έχουν τα ίδια δομικά χαρακτηριστικά και θεωρούνται κατά κάποιο τρόπο ταυτόσημες. Ένα από τα βασικά προβλήματα της θεωρίας ομάδων είναι η **ταξινόμηση** των ομάδων, δηλαδή η ανεύρεση όλων των δυνατών μη-ισομόρφων μεταξύ τους ομάδων.

Ορισμός 1.7. **Υποομάδα** μιας ομάδας G λέγεται ένα μη κενό σύνολο H κλειστό ως προς τη πράξη * της G δηλαδή, ένα μη-κενό υποσύνολο που ικανοποιεί τα αξιώματα :

(1) $\forall x,y \in H \Rightarrow x*y \in H$.

(2) $\forall x \in H \Rightarrow x^{-1} \in H$.

Παρατηρήσεις: Από τα ίδια τα αξιώματα προκύπτουν ορισμένες άμεσες συνέπειες.

(1) Κάθε υποομάδα H της G περιέχει ένα τουλάχιστον στοιχείο, το μοναδιαίο e. Πράγματι για κάθε $x \in H$ η (2) συνεπάγεται ότι και το x^{-1} θα περιέχεται στην G. Άρα κατά την (1) και το $e = x*x^{-1}$ θα περιέχεται στο H.

(2) Όλες οι υποομάδες της G έχουν κοινό με την H το μοναδιαίο e. Το μονοσύνολο {e} ικανοποιεί κατά τετριμμένο τρόπο τα αξιώματα άρα είναι υποομάδα της G. Αυτή ονομάζεται τετριμμένη υποομάδα της G και συμβολίζεται I.

(3) Από τις πιο σημαντικές υποομάδες μιας ομάδας είναι οι παραγόμενες από ένα στοιχείο x της ομάδας: $< x > = \{x^n: n \in \mathbb{Z}\}$.

Ορισμός 1.8. Μία ομάδα G λέγεται **κυκλική**, όταν υπάρχει στοιχείο της $x \in G$ τέτοιο ώστε $G = < x >$. Το στοιχείο x λέμε ότι παράγει την G και λέγεται **γεννήτορας της G**.

Παράδειγμα. Οι n-οστές μιγαδικές ρίζες της μονάδος $G = P_n = \{z \in \mathbb{C} : z^n = 1\}$ με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών αποτελούν μια κυκλική ομάδα τάξεως n. .

Έστω ζ μια n-οστή ρίζα της μονάδας ώστε G = < ζ > = {1, ζ, ζ^2, …,ζ^{n-1}}, δηλαδή το ζ παράγει όλη την κυκλική ομάδα G. Μια τέτοια ρίζα λέγεται **αρχική ρίζα της μονάδας.**

Μία άλλη ρίζα ζ^κ είναι αρχική αν έχει τάξη n και τούτο συμβαίνει όταν το κ είναι πρώτο προς το n. Άρα υπάρχουν φ(n) αρχικές ρίζες της μονάδας, όπου φ είναι η συνάρτηση του Euler. Η **συνάρτηση φ(n) του Euler** δίνει το πλήθος των μικρότερων του n ακεραίων θετικών, που είναι πρώτοι προς το n.

Για τη συνάρτηση φ του Euler ισχύει η επόμενη:

Πρόταση 1.9. Για κάθε πρώτο θετικό ακέραιο p και φυσικό $n > 0$ ισχύει

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

<u>Απόδειξη:</u> Πράγματι, αφού ο p είναι πρώτος, οι μόνοι μη-πρώτοι προς το p^n, ανάμεσα στους αριθμούς {1, 2, …, p^n}, είναι τα πολλαπλάσια του p, που είναι $\{p \cdot 1,\ p \cdot 2,\ p \cdot 3,\ p \cdot 4, \dots, p \cdot (p^{n-1} - 1),\ p \cdot p^{n-1}\}$, δηλαδή p^{n-1} το πλήθος.

Ορισμός 1.10. Έστω H⊆G μία υποομάδα της ομάδας G. Ορίζεται μια σχέση ισοδυναμίας που διαμερίζει το G με την βοήθεια του H.

Η σχέση ορίζεται ως εξής: $\boxed{x \approx y \Leftrightarrow y^{-1} x \in H}$.

Εύκολα βλέπουμε ότι η σχέση αυτή είναι πράγματι σχέση ισοδυναμίας, δηλαδή ισχύουν:

(1) $x \approx x,\ \forall\, x \in G$ (αυτοπαθής)

(2) $x \approx y \Rightarrow y \approx x$ (συμμετρική)

(3) $x \approx y,\ y \approx z \Rightarrow x \approx z$ (μεταβατική)

Τούτο σημαίνει ότι το σύνολο G διαμερίζεται σε ξένα μεταξύ τους υποσύνολα, τις κλάσεις ισοδυναμίας της σχέσης. Τις κλάσεις αυτές τις ονομάζουμε **σύμπλοκα** της υποομάδας.

Πρόταση 1.11. Κάθε σύμπλοκο της ομάδας G ως προς την υποομάδα H γράφεται με τη μορφή $xH = \{xh: h \in H\}$. Για δύο σύμπλοκα ισχύει $xH = yH$ ή $xH \cap yH = \emptyset$.

Απόδειξη: Αν $xH \cap yH \neq \emptyset$, έστω $z \in xH \cap yH$. Τότε το z γράφεται με δύο τρόπους: $z = xh_1 = yh_2$ άρα $x = yh_2h_1^{-1} \in yH$. Τότε όμως και $xH \subseteq yH$.
Ανάλογα δείχνουμε και την $yH \subseteq xH$.

Παρατήρηση. Το σύνολο των συμπλόκων της ομάδας G ως προς την υποομάδα H συμβολίζεται με G/H. Το πλήθος των συμπλόκων ονομάζεται **δείκτης** της H στην G και συμβολίζεται με [G : H] . Τούτο μπορεί να είναι άπειρο ή πεπερασμένο. Η απεικόνιση $p : G \longrightarrow G/H$ που σε κάθε $x \in G$ αντιστοιχεί το σύμπλοκο $p(x) = xH$, ονομάζεται **κανονική προβολή της ομάδας G** στο **σύνολο πηλίκο** G/H.

Ορισμός 1.12. Μία υποομάδα $H \subseteq G$ της ομάδας G λέγεται **κανονική** και συμβολίζουμε $H \triangleleft G$, όταν ισχύει $xH = Hx, \forall x \in G$. δηλαδή τα δύο σύνολα $xH = \{xh: h \in G\}$ και $Hx = \{h'x: h' \in G\}$ ταυτίζονται.

Πρόταση 1.13. Οι επόμενες προτάσεις είναι ισοδύναμες :

(1) Η υποομάδα $H \subseteq G$ είναι κανονική.

(2) $\forall x \in G \Rightarrow xHx^{-1} \subseteq H$

(3) $\forall x \in G \Rightarrow xHx^{-1} = H$

Απόδειξη: (1) ⇒ (2) Αν $h \in H$ τότε $xh \in xH = Hx$, άρα θα υπάρχει $h' \in H : xh = h'x \Rightarrow xhx^{-1} = h' \in H$, που δείχνει ότι $xHx^{-1} \subseteq H$.

(2) ⇒ (3) διότι $xHx^{-1} \subseteq H$ για κάθε $x \in G$ συνεπάγεται και την $H \subseteq x^{-1}Hx, \forall x \in G$. Άρα και $xHx^{-1} = H$.

(3) ⇒ (1) είναι τετριμμένη.

Παρατηρήσεις:

(1) Κάθε υποομάδα μιας αβελιανής ομάδας είναι κανονική. Άρα αν οι κανονικές υποομάδες έχουν κάποιο ενδιαφέρον αυτό θα φανεί στις μη αβελιανές ομάδες.

(2) Κατ' αναλογίαν προς τα σύμπλοκα, ορίζεται μέσω μιας υποομάδας H μια δεύτερη σχέση ισοδυναμίας, παρόμοια με την $\approx$ της προηγούμενης παραγράφου : $x \sim y \Leftrightarrow xy^{-1} \in H$. Οι κλάσεις ισοδυναμίας ως προς αυτήν την σχέση είναι τα σύνολα $Hx = \{hx : h \in H\}$ και το σύνολο των κλάσεων συμβολίζεται με G\H. Η υποομάδα είναι κανονική τότε ακριβώς όταν $xH = Hx$ δηλαδή οι δύο σχέσεις ισοδυναμίας έχουν τις ίδιες κλάσεις ισοδυναμίας.

(3) Η ομάδα G λέγεται **απλή** όταν δεν έχει γνήσιες (δηλαδή διάφορες του εαυτού της και της τετριμμένης {e}) κανονικές υποομάδες.

Ορισμός 1.14. Το σύνολο Z(G) των στοιχείων α της G, τα οποία αντιμετατίθενται με όλα τα στοιχεία x της G, καλείται **κέντρο της ομάδας G** . Είναι λοιπόν: $Z(G) = \{ \alpha \in G : \alpha x = x\alpha , \forall x \in G \}$.

Πρόταση 1.15. Το κέντρο Z(G) μιας ομάδας G είναι κανονική υποομάδα της G.

<u>Απόδειξη:</u> Πρώτα θα δείξουμε ότι το Z(G) είναι υποομάδα της G .

Αρκεί να δείξουμε ότι το σύνολο αυτό είναι κλειστό ως προς την πράξη της ομάδας και ότι $\forall \alpha \in Z(G)$, το $\alpha^{-1} \in Z(G)$.

- Έστω $\alpha, \beta \in Z(G)$. Είναι τότε: $x\alpha\beta = \alpha x\beta = \alpha\beta x$, $\forall x \in G$, οπότε $\alpha\beta \in Z(G)$.
- Για κάθε $x \in G$, και $\alpha \in Z(G)$ είναι $x = x\alpha\alpha^{-1} = \alpha x\alpha^{-1}$.

  Άρα $\alpha^{-1}x = \alpha^{-1}\alpha x\alpha^{-1} = x\alpha^{-1}$, δηλαδή $\alpha^{-1} \in Z(G)$.

Επίσης, εξ' ορισμού, τα στοιχεία α του Z(G) αντιμετατίθενται και μεταξύ τους. Άρα το Z(G) είναι αβελιανή υποομάδα της G.

Στη συνέχεια θα δείξουμε ότι $Z(G) \lhd G$.

Έστω $\alpha \in Z(G)$ και $x \in G$, αρκεί $x\,\alpha\,x^{-1} \in Z(G)$. Είναι $x\,\alpha\,x^{-1} = \alpha\,x\,x^{-1} = \alpha \in Z(G)$.

Παρατήρηση: Το κέντρο Z(G) μιας ομάδας G μπορεί να είναι τετριμμένο (π.χ. $Z(D_3) = I$).

Θα δείξουμε παρακάτω ότι αν $|G| = p^n$, όπου p πρώτος θετικός ακέραιος, τότε το κέντρο Z(G) είναι μη τετριμμένο.

Ορισμός 1.16. Το σύνολο των στοιχείων x της G, τα οποία αντιμετατίθενται με το στοιχείο α της G, καλείται **κανονικοποιούσα N(α) του στοιχείου α**.

Είναι λοιπόν: $N(\alpha) = \{ x \in G: x\alpha = \alpha x\}$.

Πρόταση 1.17. Η N(α) είναι υποομάδα της G.

<u>Απόδειξη:</u> Αρκεί να δείξουμε ότι το σύνολο αυτό είναι κλειστό ως προς την πράξη της ομάδας και ότι $\forall n \in N(\alpha)$, $\exists n^{-1} \in N(\alpha)$.

- Έστω $n, m \in N(\alpha)$. Είναι τότε: $n\,m\,\alpha = n\,\alpha\,m = \alpha\,n\,m$, οπότε $n\,m \in N(\alpha)$.
- Για κάθε $n \in N(\alpha)$ είναι $n^{-1} \in G$, και αφού $n \in N(\alpha) \rightarrow n^{-1}\alpha = n^{-1}\,\alpha\,n\,n^{-1} = n^{-1}n\,\alpha\,n^{-1}$.

  Άρα $n^{-1}\alpha = \alpha\,n^{-1}$, δηλαδή $n^{-1} \in N(\alpha)$.

Πρόταση 1.18. Κάθε πεπερασμένη ομάδα G τάξης $p^n, n \geq 1$ όπου p πρώτος αριθμός, έχει μη τετριμμένο κέντρο Z(G).

<u>Απόδειξη:</u> Έστω $G = \{e, a_1, a_2, \ldots, a_{p^n-1}\}$.

Θεωρούμε $g \in G$ και $geg^{-1}, ga_1g^{-1}, ga_2g^{-1}, \ldots, ga_{p^n-1}g^{-1}$.

Ορίζεται έτσι μια σχέση ισοδυναμίας (συζυγία) : $a \sim b \Leftrightarrow \exists\, g \in G: gag^{-1} = b$.

[Έστω G ομάδα, τα στοιχεία $a, b \in G$ θα λέγονται συζυγή αν υπάρχει $g \in G$ τέτοιο ώστε $b = gag^{-1}$. Είναι εύκολο να δούμε ότι η συζυγία είναι σχέση ισοδυναμίας. Η ομάδα G χωρίζεται λοιπόν σε ξένα μεταξύ τους υποσύνολα, τις κλάσεις ισοδυναμίας που λέγονται **κλάσεις συζυγίας**.]

• <u>Ισχυρισμός</u>:

Μία κλάση ισοδυναμίας είναι μονοσύνολο {z} αν και μόνο αν $z\in Z(G)$.

Πράγματι, αν μια κλάση ισοδυναμίας είναι μονοσύνολο τότε

$C_z = \{gzg^{-1}, g\in G\} = \{z\}$, οπότε $gzg^{-1} = z$, για κάθε $g \in G \Leftrightarrow$

$gz = zg$, για κάθε $g \in G \Leftrightarrow$

$z\in Z(G)$.

Επίσης αν $z\in Z(G)$ τότε $gzg^{-1} = zgg^{-1} = z$, οπότε

$C_z = \{gzg^{-1}, g\in G\} = \{z\}$ μονοσύνολο.•

Αφού οι συζυγείς κλάσεις αποτελούν διαμέριση της G θα έχουμε ότι :

$|G| = |Z(G)| + |C_2| + \cdots + |C_r|$ (1) , (ισότητα κλάσεων της G),

όπου $C_2,\ldots,C_r$, οι κλάσεις ισοδυναμίας με περισσότερα από ένα στοιχεία.

Έστω μία κλάση ισοδυναμίας C_a με $|C_a| \neq 1$.

Τότε $C_a = \{eae^{-1}, a_1aa_1^{-1}, a_2aa_2^{-1}, \ldots, a_{p^n-1}aa_{p^n-1}^{-1}\}$.

Κάποια στοιχεία μπορεί να είναι ίσα μεταξύ τους .

Ελέγχω πότε δύο στοιχεία είναι ίσα: $a_iaa_i^{-1} = a_jaa_j^{-1} \Leftrightarrow$

$$(a_j^{-1}a_i)a(a_i^{-1}a_j) = a \Leftrightarrow$$

$$(a_j^{-1}a_i)a(a_j^{-1}a_i)^{-1} = a \Leftrightarrow$$

$$(a_j^{-1}a_i)a = a(a_j^{-1}a_i) \Leftrightarrow$$

$$(a_j^{-1}a_i) \in N(a) \Leftrightarrow$$

$$a_iN(a) = a_jN(a)$$

δηλαδή τα a_i, a_j ανήκουν στο ίδιο σύμπλοκο της $N(a)$ στη G, όπου $N(a)$ η κανονικοποιούσα υποομάδα του στοιχείου a στη G.

Επομένως η $|C_a|$ ισούται με το πλήθος των συμπλόκων που είναι ο δείκτης της $N(a)$ στη G. Άρα από το Θεώρημα Lagrange έχουμε ότι $|C_a| / |G|$, οπότε η $|C_a|$ είναι δύναμη του p (με $|C_a| \neq 1 = p^0$).

Από τη σχέση (1) έχουμε: $p^n = |Z(G)| + p^{n_2} + \ldots + p^{n_r}$, όπου $n_2, \ldots, n_r \neq 0$,
οπότε $p / |Z(G)|$ και επειδή $|Z(G)| \geq 1$ (αφού περιέχει το e),
άρα τελικά είναι $|Z(G)| \geq p$.

Λήμμα 1.19. Αν *G* πεπερασμένη p-ομάδα, τάξης p^n, τότε η *G* έχει μια σειρά από κανονικές υποομάδες:

$$I = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G, \text{ όπου } |G_i| = p^i, \text{ για κάθε } i = 0, \ldots, n.$$

<u>Απόδειξη:</u> Θα κάνουμε επαγωγή ως προς n.

Αν $n = 0$ τότε είμαστε εντάξει.

Αν $n > 0$, τότε από την Πρόταση 1.15 είναι $Z(G) \neq I$.

Αφού η $Z(G)$ είναι αβελιανή υποομάδα της G, η τάξη της θα διαιρεί την $|G| = p^n$ οπότε $|Z(G)| = p^m$ και επομένως έχει κάποιο στοιχείο τάξης p.

Η κυκλική υποομάδα K που παράγεται από αυτό το στοιχείο, έχει τάξη p και είναι κανονική, αφού K υποομάδα της $Z(G)$.
[Έστω $u \in K \subseteq Z(G)$ τότε για κάθε $g \in G$ είναι: $g\,u\,g^{-1} = u\,g\,g^{-1} = u \in K$, άρα $K \trianglelefteq G$]

Η G/K είναι μια p-ομάδα με τάξη p^{n-1}.

[Αφού $K \trianglelefteq G \Rightarrow G/K$ ομάδα και $|G/K| = |G| / |K| = \dfrac{p^n}{p} = p^{n-1}$].

Άρα από την επαγωγική υπόθεση, η G/K θα έχει μία σειρά κανονικών υποομάδων:

$$G_0/K = G_1/K \subseteq \ldots \subseteq G_n/K, \quad \text{όπου } |G_i/K| = p^{i-1}.$$

Αλλά τότε $|G_i| = p^i$ και $G_i \triangleleft G$, θέτουμε $G_0 = I$ και έχουμε το αποτέλεσμα.

ΚΕΦΑΛΑΙΟ 2

ΔΑΚΤΥΛΙΟΙ - ΣΩΜΑΤΑ

Ορισμός 2.1. **Δακτύλιος** είναι ένα σύνολο R εφοδιασμένο με δύο διμελείς πράξεις:

- Την πρόσθεση: $(a,b)\mapsto a+b$ και
- Τον πολλαπλασιασμό: $(a,b)\mapsto a\cdot b$ έτσι ώστε:

(1) Το σύνολο R να είναι μεταθετική (αβελιανή) ομάδα ως προς την πρόσθεση

(2) Ο πολλαπλασιασμός να είναι προσεταιριστικός

(3) Να ισχύει η επιμεριστική ιδιότητα:

$(a+b)\cdot c=a\cdot c+b\cdot c$ ή $c\cdot(a+b)=c\cdot a+c\cdot b$ για κάθε $a,b,c\in R$

- Αν σε ένα δακτύλιο $(R,+,\cdot)$ ισχύει επιπλέον $a\cdot b=b\cdot a$, για κάθε $a,b\in R$ τότε λέγεται **μεταθετικός δακτύλιος**.
- Αν σε ένα δακτύλιο $(R,+,\cdot)$ υπάρχει ένα στοιχείο $1\in R$ με $1\neq 0$ (όπου 0 το ουδέτερο στοιχείο της πρόσθεσης στο R) ώστε $1\cdot a=a\cdot 1=a$ τότε το 1 λέγεται μονάδα του δακτυλίου και ο δακτύλιος ονομάζεται **δακτύλιος με μονάδα**.
- Ένας μεταθετικός δακτύλιος με μονάδα $1\neq 0$ λέγεται **σώμα** αν κάθε στοιχείο του $a\neq 0$ έχει αντίστροφο μέσα στο R.

Σημείωση: Στο εξής θα χρησιμοποιούμε τον όρο **δακτύλιος** αντί του όρου <u>μεταθετικός δακτύλιος με μονάδα</u>.

Παραδείγματα. **1)** Οι πιο γνωστοί δακτύλιοι είναι οι: $\mathbb{Z}$ (ακέραιοι αριθμοί), $\mathbb{Q}$ (ρητοί αριθμοί), $\mathbb{R}$ (πραγματικοί αριθμοί), $\mathbb{C}$ (μιγαδικοί αριθμοί),καθένας από τους οποίους θεωρείται ότι είναι εφοδιασμένος με τις συνήθεις πράξεις της

πρόσθεσης και του πολλαπλασιασμού. Οι δακτύλιοι $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ είναι σώματα ενώ ο δακτύλιος $(\mathbb{Z},+,\cdot)$ δεν είναι σώμα.

2) Αν R είναι ένας δακτύλιος, τότε ένα **πολυώνυμο f(x) με συντελεστές στον R** (συντομότερα ένα πολυώνυμο επί του R), είναι μια ακολουθία

$f(x)=(c_0, c_1, ..., c_n, 0, 0, ...)$,

όπου $c_i \in R$ για όλα τα $i=1,2,...,n$ και $c_i=0$ για όλα τα $i>n$.

Αν $g(x)=(d_0, d_1, ...)$ είναι ακόμη ένα πολυώνυμο υπεράνω του R, τότε έπεται ότι $f(x)=g(x)$ αν και μόνο αν $c_i=d_i$ για όλα τα i. Το σύνολο των πολυωνύμων συμβολίζεται με $R[x]$. Η πρόσθεση και ο πολλαπλασιασμός του $R[x]$ ορίζονται ως εξής:

$$(c_0, c_1, ...)+(d_0, d_1, ...)=(c_0+d_0, c_1+d_1, ...)$$

$$(c_0, c_1, ...)\cdot(d_0, d_1, ...)=(e_0, e_1, ...)$$

με $e_0=c_0\cdot d_0$, $e_1=c_0\cdot d_1+c_1\cdot d_0$ και γενικώς $e_k=\sum c_i\cdot d_j$, όπου η πρόσθεση εκτελείται υπεράνω όλων των δεικτών i, j με $i+j=k$. Το **μηδενικό πολυώνυμο** ορίζεται ως η ακολουθία $(0, 0, ...)$ και παρίσταται με 0. Παρόμοια το πολυώνυμο $(1, 0, 0, ...)$ συμβολίζεται με 1 (έτσι τώρα υπάρχουν δύο διαφορετικές έννοιες για το ίδιο σύμβολο). Είναι στερεότυπη αλλά μακροσκελής η επιβεβαίωση ότι ο $R[x]$ είναι ένας δακτύλιος. Αυτός ονομάζεται **πολυωνυμικός δακτύλιος επί του R**.

Ποια είναι όμως η σημασία του γράμματος x στο συμβολισμό f(x); Ας ονομάσουμε με x το εξής ιδιάζον στοιχείο του $R[x]$:

$$x=(0, 1, 0, 0, ...)$$

Εύκολα αποδεικνύεται ότι $x^2=(0, 0, 1, 0, 0, 0, ...)$ και επαγωγικά ότι το x^i συμπίπτει με την ακολουθία που έχει το 0 παντού, εκτός της i-οστής θέσης, στην οποία υπάρχει το στοιχείο 1. Έτσι επανακάμπτει ο γνώριμος συμβολισμός:

$$\begin{aligned}
f(x) &= (c_0, c_1, ..., c_n, 0, 0, ...)\\
&= (c_0, 0, 0, ...)+(0, c_1, 0, 0, ...)+(0, 0, c_2, 0, 0, ...)+...\\
&= c_0(1, 0, 0, ...)+c_1(0, 1, 0, 0, ...)+c_2(0, 0, 1, 0, 0, ...)+...\\
&= c_0+c_1x+...+c_nx^n\\
&= \sum c_ix^i
\end{aligned}$$

Εδώ βέβαια έχουμε γράψει $c_0 = c_0 1$, αφού ταυτίσαμε πρώτα το c_0 του R με το $(c_0, 0, 0, ...)$ του $R[x]$. Σημειώστε ότι το x είναι ένα αληθινό στοιχείο του δακτυλίου και δεν πρόκειται για μια μεταβλητή. Ο ρόλος του ως μεταβλητή θα του αποδοθεί αργότερα, όταν γίνει η συζήτηση που αφορά τις πολυωνυμικές συναρτήσεις.

Υπενθυμίζουμε στον αναγνώστη το γνωστό λεξιλόγιο που συνοδεύει κάθε πολυώνυμο $f(x) = c_0 + c_1 x + ... + c_n x^n$. Αν το πολυώνυμο f(x) δεν είναι μηδενικό, τότε ο **μεγιστοβάθμιος συντελεστής** του ορίζεται να είναι ο c_n, όπου n είναι ο μεγαλύτερος δείκτης με $c_n \neq 0$. Ο δείκτης n ονομάζεται **βαθμός** του πολυωνύμου και συμβολίζεται με degf(x) (δηλαδή n είναι ο μεγαλύτερος εκθέτης του x που εμφανίζεται στο f(x)). Ένα πολυώνυμο ονομάζεται **μονικό**, όταν ο μεγιστοβάθμιος συντελεστής του είναι το 1. Το μηδενικό πολυώνυμο $0 = (0, 0, ...)$ δεν διαθέτει βαθμό, αφού δεν έχει μεγιστοβάθμιο συντελεστή. Ο **σταθερός όρος** του f(x) είναι ο c_0. Κάθε **σταθερό πολυώνυμο** είναι ή το μηδενικό πολυώνυμο ή ένα πολυώνυμο μηδενικού βαθμού.

Ο βαθμός έχει τις εξής ιδιότητες: Έστω f(x), g(x) μη μηδενικά στοιχεία του $R[x]$. Ισχύει οτι:

i) Αν $f(x) \cdot g(x) \neq 0$ τότε $\deg(f(x) \cdot g(x)) \leq \deg(f(x)) + \deg(g(x))$

ii) Αν $f(x) + g(x) \neq 0$ τότε $\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$

Παρατήρηση. Ο δακτύλιος $R[x]$ δεν είναι σώμα. *Παράδειγμα*: $\frac{1}{x} \notin R[x]$.

Παρατήρηση. Ένας δακτύλιος R είναι μια **ακέραια περιοχή**, αν το γινόμενο δύο μη μηδενικών στοιχείων του R είναι και πάλι ένα μη μηδενικό στοιχείο.. Αν R είναι μια ακέραια περιοχή τότε η i) γίνεται:

Αν $f(x) \cdot g(x) \neq 0$ τότε $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$

Ορισμός 2.2. Έστω $f(x)=\sum c_i x^i$ ένα πολυώνυμο επί ενός δακτυλίου R. **Ρίζα του πολυωνύμου f(x) στον R**, ονομάζεται κάθε στοιχείο $a \in R$, τέτοιο ώστε $f(a)=0$ δηλαδή $c_0 + c_1 a + ... + c_n a^n = 0$.

Σχόλιο. Το πολυώνυμο $f(x)=x^2-2$ είναι ένα πολυώνυμο επί του $\mathbb{Q}$ και λέμε ότι το $\sqrt{2}$ είναι ρίζα του f(x), παρόλο που το $\sqrt{2}$ είναι άρρητος αριθμός. Παρακάτω, θα διαφοροποιήσουμε τον ορισμό των ριζών ενός πολυωνύμου επί του R, έτσι ώστε αυτές να ανήκουν και σε κάποιο δακτύλιο μεγαλύτερο του R.

ΥΠΟΔΑΚΤΥΛΙΟΙ - ΥΠΟΣΩΜΑΤΑ

Ορισμός 2.3. Έστω $(R,+,\cdot)$ ένας δακτύλιος και S ένα μη κενό υποσύνολο του R τέτοιο ώστε οι περιορισμοί $+ : S\times S \longmapsto S$ και $\cdot : S\times S \longmapsto S$ των δύο πράξεων του R στο $S\times S$, να είναι πράξεις στο S. Αν το S με τις πράξεις αυτές είναι δακτύλιος, θα λέμε ότι το S είναι **υποδακτύλιος** του R.

Πρόταση 2.4. Έστω $(R,+,\cdot)$ ένας δακτύλιος και S ένα μη κενό υποσύνολο του R. Το $(S,+,\cdot)$ είναι υποδακτύλιος του $(R,+,\cdot)$ αν ισχύουν:

- $a-b \in S$ για κάθε $a,b \in S$
- $a \cdot b \in S$ για κάθε $a,b \in S$

Ορισμός 2.5. Έστω $(K,+,\cdot)$ ένα σώμα και $F \subseteq K$. Το F ονομάζεται **υποσώμα** του K αν:

- Το $(F,+)$ είναι υποομάδα της $(K,+)$ και
- Το $(F^*,\cdot)$ είναι υποομάδα της $(K^*,\cdot)$ όπου $K^* = K-\{0\}$ και $F^* = F-\{0\}$.

Από τον ορισμό προκύπτει ότι ένα υπόσωμα F ενός σώματος K είναι επίσης σώμα ως προς τις ίδιες πράξεις.

Πρόταση 2.6. Έστω $(K,+,\cdot)$ένα σώμα και $F \subseteq K$.Το F είναι υπόσωμα του K αν ισχύουν:

- $0,1 \in F$ όπου 0 το ουδέτερο στοιχείο της πρόσθεσης και 1 το ουδέτερο στοιχείο του πολλαπλασιασμού στο K
- $a-b \in F,\ a \cdot b \in F$ για κάθε $a,b \in F$
- Για κάθε $a \in F$ με $a \neq 0$ και το $a^{-1} \in F$

Παράδειγμα. Τα $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ είναι υποσώματα του $(\mathbb{C},+,\cdot)$

Ορισμός 2.7. Έστω R, S δύο δακτύλιοι. Μια απεικόνιση $\varphi : R \to S$ λέγεται **ομομορφισμός** δακτυλίων αν για κάθε $a,b \in R$ ισχύουν:

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$
$$\varphi(1) = 1$$

- Αν επιπλέον η φ είναι επί λέγεται **επιμορφισμός**.
- Αν επιπλέον η φ είναι 1-1 λέγεται **μονορφισμός**.
- Αν επιπλέον η φ είναι 1-1 και επί λέγεται **ισομορφισμός** και οι δακτύλιοι R, S είναι ισόμορφοι. Τότε γράφουμε $R \cong S$.

Παράδειγμα. Αν R είναι ένας δακτύλιος, τότε το $R' = \{(r,0,0,...) : r \in R\}$ είναι υποδακτύλιος του $R[x]$ και η απεικόνιση $\varphi : R \to R'$ που ορίζεται ως $\varphi : r \mapsto (r,0,0,...)$ είναι ένας ισομορφισμός από τον R στον R'.

ΚΕΦΑΛΑΙΟ 3

ΔΙΑΝΥΣΜΑΤΙΚΟΙ ΧΩΡΟΙ

Ορισμός 3.1. Έστω F ένα σώμα. Ένας **διανυσματικός χώρος επί του F** (ή **διανυσματικός χώρος F**) αποτελείται από μία αβελιανή ομάδα V με πράξη την πρόσθεση, μαζί με μια πράξη βαθμωτού πολλαπλασιασμού των στοιχείων του V με τα στοιχεία του F από τ' αριστερά, τέτοια, ώστε για κάθε a, b $\in$ F και α, β $\in$ V να ικανοποιούνται οι ακόλουθες συνθήκες:

(1) aα $\in$ V.

(2) a(bα) = (ab)α.

(3) (a + b)α = (aα) + (bα)

(4) a(α +β) = (aα) + (aβ).

(5) 1α = α.

Τα στοιχεία του V λέγονται **διανύσματα** και τα στοιχεία του F **βαθμωτά**. Όταν ασχολούμαστε με ένα μόνο σώμα F, παύουμε να αναφερόμαστε στο F και μιλάμε για έναν διανυσματικό χώρο.

Σημειώστε ότι, ο πολλαπλασιασμός σε ένα διανυσματικό χώρο δεν είναι μια διμελής πράξη ορισμένη πάνω σε ένα σύνολο. Είναι ένας κανόνας που επισυνάπτει ένα στοιχείο aα του V σε κάθε διατεταγμένο ζεύγος (a, α), που αποτελείται από ένα στοιχείο a του F και ένα στοιχείο α του V. Μπορούμε λοιπόν να τον δούμε ως μια συνάρτηση με την οποία απεικονίζεται το F x V στο V.

Ορισμός 3.2. Έστω V ένας διανυσματικός χώρος επί του F.

Τα διανύσματα ενός υποσυνόλου $S = \{\alpha_i / i \in I\}$ του V παράγουν (ή γεννούν) το V αν για κάθε $\beta \in V$, έχουμε

$\beta = a_1\alpha_{i1} + a_2\alpha_{i2} + \ldots + a_n\alpha_{in}$ για κάποια $a_j \in F$ και $\alpha_{ij} \in S$, $j = 1,2,\ldots,n$,

Κάθε διάνυσμα $\sum_{j=1}^{n} a_j\alpha_{ij}$ λέγεται γραμμικός συνδυασμός των α_{ij} .

Ορισμός 3.3. Ένας διανυσματικός χώρος V επί ενός σώματος F λέγεται **πεπερασμένης διάστασης** αν υπάρχει ένα πεπερασμένο υποσύνολο του V, τα διανύσματα του οποίου σχηματίζουν μια βάση του V επί του F .

Ορισμός 3.4. Τα διανύσματα ενός υποσυνόλου $S = \{\alpha_i / i \in I\}$ ενός διανυσματικού χώρου V επί ενός σώματος F λέγονται **γραμμικώς ανεξάρτητα επί του F** αν από τη σχέση $\sum_{j=1}^{n} a_j\alpha_{ij} = 0$ έπεται ότι $a_j = 0$ για κάθε $j = 1,\ldots, n$.

Αν τα διανύσματα δεν είναι γραμμικώς ανεξάρτητα επί του F, τότε λέγονται **γραμμικώς εξαρτημένα επί του** F.

Έτσι, τα διανύσματα του $\{\alpha_i / i \in I\}$ είναι γραμμικώς ανεξάρτητα επί του F αν ο μόνος τρόπος με τον οποίο το διάνυσμα 0 μπορεί να γραφεί ως γραμμικός συνδυασμός των διανυσμάτων α_i είναι η εξίσωση όλων των βαθμωτών συντελεστών με το 0. Αν τα διανύσματα είναι γραμμικώς εξαρτημένα επί του F, τότε υπάρχουν $a_j \in F$ με $j = 1,\ldots, n$ τέτοια, ώστε $\sum_{j=1}^{n} a_j\alpha_{ij} = 0$, όπου δεν είναι όλα τα $a_j = 0$.

Ορισμός 3.5. Αν V είναι ένας διανυσματικός χώρος επί ενός σώματος F, λέμε ότι τα διανύσματα ενός υποσυνόλου $B = \{ \beta_i / i \in I \}$ του V σχηματίζουν μία **βάση του V επί του F,** αν αυτά παράγουν τον V και είναι γραμμικώς ανεξάρτητα.

Ορισμός 3.6. Αν V είναι ένας πεπερασμένης διάστασης διανυσματικός χώρος επί ενός σώματος F, τότε το πλήθος των στοιχείων μιας βάσης του (που είναι ανεξάρτητο από την επιλογή της βάσης) λέγεται **διάσταση του V επί του F,** και συμβολίζεται $\mathbf{dim_F V}$.

ΚΕΦΑΛΑΙΟ 4

ΑΝΑΓΩΓΑ ΠΟΛΥΩΝΥΜΑ

Ορισμός 4.1. Έστω F ένα σώμα. Ένα μη μηδενικό πολυώνυμο $f(x) \in F[x]$ με $\deg f(x) \geq 1$ καλείται **ανάγωγο** επί του F αν από κάθε ανάλυση του f(x) της μορφής $f(x) = g(x) \cdot h(x)$ με $g(x), h(x) \in F[x]$ προκύπτει ότι g(x) σταθερό ή h(x) σταθερό πολυώνυμο.

Σημείωση. Το κατά πόσον ένα πολυώνυμο είναι ανάγωγο ή όχι εξαρτάται από το σώμα των συντελεστών. Για παράδειγμα, το $x^2 + 1$ είναι ανάγωγο επί του $\mathbb{R}$, αλλά δεν είναι επί του $\mathbb{C}$. Επίσης, το $x^2 - 2$ είναι ανάγωγο επί του $\mathbb{Q}$ αλλά δεν είναι επί του $\mathbb{R}$.

Προφανώς τα γραμμικά πολυώνυμα ($1^{ου}$ βαθμού) είναι πάντα ανάγωγα, όποιο και αν είναι το σώμα F. Παρακάτω θα διερευνήσουμε την αναγωγιμότητα των πολυωνύμων $2^{ου}$ βαθμού και πάνω επί των σωμάτων $\mathbb{C}$, $\mathbb{R}$ και $\mathbb{Q}$.

Ανάγωγα Πολυώνυμα επί του $\mathbb{C}$

Αν $f(x) = a_n x^n + ... + a_1 x + a_0$ με $\deg f(x) = n > 1$ τότε $f(x) = a_n (x - z_1)(x - z_2) \cdot ... \cdot (x - z_n)$ όπου $z_1, z_2, ..., z_n \in \mathbb{C}$. Άρα το f(x) δεν είναι ανάγωγο. Άρα τα μόνα ανάγωγα πολυώνυμα στο $\mathbb{C}$ είναι αυτά του $1^{ου}$ βαθμού.

Ανάγωγα Πολυώνυμα επί του $\mathbb{R}$

<u>$2^{ου}$ Βαθμού:</u> Τα πολυώνυμα επί του $\mathbb{R}$ $2^{ου}$ βαθμού θα είναι της μορφής $f(x) = ax^2 + bx + c$ με $a, b, c \in \mathbb{R}$,και $a \neq 0$ Εδώ διακρίνουμε τις εξής περιπτώσεις:

α) Αν $\Delta = b^2 - 4ac > 0$ τότε $f(x) = a(x-\rho_1)(x-\rho_2)$ όπου ρ_1, ρ_2 είναι οι ρίζες της εξίσωσης $ax^2 + bx + c = 0$. Άρα το f(x) δεν θα είναι ανάγωγο.

β) Αν $\Delta = b^2 - 4ac = 0$ τότε $f(x) = a(x-\rho)(x-\rho)$ όπου ρ είναι η ρίζα της εξίσωσης $ax^2 + bx + c = 0$. Άρα το f(x) δεν θα είναι ανάγωγο.

γ) Αν $\Delta = b^2 - 4ac < 0$, τότε το πολυώνυμο δεν παραγοντοποιείται στο $\mathbb{R}$ άρα θα είναι ανάγωγο.

<u>3ου Βαθμού:</u> Τα πολυώνυμα επί του $\mathbb{R}$ 3ου βαθμού θα είναι της μορφής $f(x) = ax^3 + bx^2 + cx + d$ με $a, b, c, d \in \mathbb{R}$, και $a \neq 0$. Τότε υπάρχει $\rho \in \mathbb{R} : (x-\rho) / f(x)$. Δηλαδή $f(x) = (x-\rho)(a'x^2 + b'x + c')$ άρα το f(x) δεν θα είναι ανάγωγο στο $\mathbb{R}$. Ομοίως, ισχύει ότι κάθε πολυώνυμο περιττού βαθμού δηλαδή αν $f(x) = a_n x^n + ... + a_1 x + a_0$ με $\deg f(x) = 2\kappa + 1$, $\kappa \in \mathbb{N}$ δεν θα είναι ανάγωγο στο $\mathbb{R}$.

<u>4ου Βαθμού:</u> Τα πολυώνυμα επί του $\mathbb{R}$ 4ου βαθμού θα είναι της μορφής $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ με $a, b, c, d, e \in \mathbb{R}$, $a \neq 0$.Οι ρίζες αυτού του πολυωνύμου θα είναι πραγματικές ή μιγαδικές. Αν υπάρχει έστω και μία πραγματική ρίζα ρ τότε το πολυώνυμο θα γράφεται $f(x) = (x-\rho)(a_3x^3 + a_2x^2 + a_1x + a_0)$ και άρα το f(x) δεν θα είναι ανάγωγο στο $\mathbb{R}$. Μένει, λοιπόν, η περίπτωση όπου όλες οι ρίζες θα είναι μιγαδικές. Αυτές τότε θα είναι της μορφής $\rho_1 = \alpha_1 + i\beta_1$, $\rho_2 = \alpha_1 - i\beta_1$, $\rho_3 = \alpha_2 + i\beta_2$ και $\rho_4 = \alpha_2 - i\beta_2$, δηλαδή θα είναι ανά δύο συζυγής και το f(x) θα γράφεται:

$$\begin{aligned} f(x) &= a(x-\rho_1)(x-\rho_2)(x-\rho_3)(x-\rho_4) \\ &= a\left[x^2 - (\rho_1+\rho_2)\cdot x + \rho_1\rho_2\right]\left[x^2 - (\rho_3+\rho_4)\cdot x + \rho_3\rho_4\right] \\ &= a\left(x^2 - 2\alpha_1 x + \alpha_1^2 + \beta_1^2\right)\left(x^2 - 2\alpha_2 x + \alpha_2^2 + \beta_2^2\right) \end{aligned}$$

άρα το f(x) δεν είναι ανάγωγο. Ομοίως, ισχύει κάθε πολυώνυμο άρτιου βαθμού, δηλαδή αν $f(x) = a_n x^n + ... + a_1 x + a_0$ με $\deg f(x) = 2n$, $n \in \mathbb{N}$, $n > 1$ δεν θα είναι ανάγωγο στο $\mathbb{R}$.

Άρα τα μόνα ανάγωγα πολυώνυμα στο $\mathbb{R}$ είναι αυτά του 1ου βαθμού από του 2ου βαθμού εκείνα που έχουν $\Delta < 0$.

Ανάγωγα Πολυώνυμα επί του $\mathbb{Q}$

Λήμμα 4.2. (Gauss). Αν ένα πολυώνυμο με ακέραιους συντελεστές είναι δυνατόν να γραφεί ως γινόμενο δύο πολυωνύμων, μικρότερου βαθμού, με ρητούς συντελεστές, τότε γράφεται και ως γινόμενο δύο πολυωνύμων, μικρότερου βαθμού, με ακέραιους συντελεστές.

Απόδειξη. Έστω $f = gh$ όπου το πολυώνυμο f έχει ακέραιους συντελεστές, ενώ τα πολυώνυμα g και h ρητούς. Υποθέτουμε ότι έχουμε διαιρέσει με το μέγιστο κοινό διαιρέτη των συντελεστών των g και h αντίστοιχα, τους συντελεστές των g και h. Γράφουμε, λοιπόν:

$$g(x) = \frac{\alpha_n}{\beta_n}x^n + \frac{\alpha_{n-1}}{\beta_{n-1}}x^{n-1} + \ldots + \frac{\alpha_0}{\beta_0} \text{ και } h(x) = \frac{\gamma_m}{\delta_m}x^m + \frac{\gamma_{m-1}}{\delta_{m-1}}x^{m-1} + \ldots + \frac{\gamma_0}{\delta_0}$$

όπου όλοι οι συντελεστές είναι ανάγωγα κλάσματα. Αν Β και Δ είναι το γινόμενο όλων των παρανομαστών β και δ αντίστοιχα, τότε το Bg(x) και το Δh(x) έχουν ακέραιους συντελεστές. Αν Α ο μέγιστος κοινός διαιρέτης των β και Γ ο μέγιστος κοινός διαιρέτης των δ, έχουμε τελικά τα πολυώνυμα:

$$\frac{B}{A}g(x) = A_n x^n + A_{n-1}x^{n-1} + \ldots + A_0 \text{ και } \frac{\Delta}{\Gamma}h(x) = \Gamma_m x^m + \Gamma_{m-1}x^{m-1} + \ldots + \Gamma_0$$

Η σχέση $f = gh$ τώρα γίνεται: $B\Delta \cdot f = A\Gamma\left(\frac{B}{A}g\right)\left(\frac{\Delta}{\Gamma}h\right)$. Παρατηρούμε ότι $A\Gamma \mid B\Delta$.

Θέτουμε, λοιπόν, $E = \frac{B\Delta}{A\Gamma} \in \mathbb{Z}$ και γράφουμε:

$$E \cdot f(x) = \left(A_n x^n + A_{n-1}x^{n-1} + \ldots + A_0\right)\left(\Gamma_m x^m + \Gamma_{m-1}x^{m-1} + \ldots + \Gamma_0\right) \quad (1)$$

Το Λήμμα θα έχει αποδειχθεί αν δείξουμε ότι $E = \pm 1$. Αν $E \neq \pm 1$ τότε το Ε θα έχει κάποιον πρώτο παράγοντα p. Ο p δεν διαιρεί όμως όλους τους συντελεστές Α, ούτε όλους τους συντελεστές Γ. Έστω, λοιπόν, A_i και Γ_j οι μικρότεροι συντελεστές από τους Α και Γ αντίστοιχα, που ο p δεν διαιρεί. Ας δούμε τώρα τον συντελεστή του x^{i+j}. Στο πολυώνυμο f(x), στην (1), ο συντελεστής του όρου αυτού, διαιρείται από τον Ε και συνεπώς από τον p. Αν κάνουμε τον πολλαπλασιασμό που σημειώνεται

στην (1), θα βρούμε για συντελεστή του όρου x^{i+j} τον $\sum_{k=0}^{i-1} A_k \Gamma_{i+j-k} + \sum_{k=i+1}^{i+j} A_k \Gamma_{i+j-k} + A_i \Gamma_j$. Ο p διαιρεί όλους τους A_k, $\forall k \neq i$ και όλους τους Γ_λ, $\forall \lambda \neq j$. Ο p συνεπώς, διαιρεί τους δύο πρώτους όρους του προηγούμενου αθροίσματος, δεν διαιρεί όμως τον όρο $A_i \Gamma_j$. Άτοπο.

Πόρισμα 4.3. Ένα πολυώνυμο που είναι ανάγωγο στο $\mathbb{Z}[x]$, είναι ανάγωγο και στο $\mathbb{Q}[x]$.

Θεώρημα 4.4. (Κριτήριο αναγωγιμότητας του Eisenstein).

Έστω το πολυώνυμο $f \in \mathbb{Z}[x]$, με $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Αν υπάρχει πρώτος p τέτοιος ώστε:

α) Ο p διαιρεί όλους τους συντελεστές $a_i, i = 0,1,\ldots,n-1$ ενώ δεν διαιρεί το a_n

β) Ο p^2 δεν διαιρεί το a_0

τότε το f είναι ανάγωγο εν $\mathbb{Q}[x]$.

<u>*Απόδειξη.*</u> Έστω ότι το f δεν είναι ανάγωγο στο $\mathbb{Q}[x]$. Τότε γράφεται ως γινόμενο δύο πολυωνύμων $g(x) = \beta_k x^k + \beta_{k-1} x^{k-1} + \ldots + \beta_0$ και $h(x) = \gamma_m x^m + \gamma_{m-1} x^{m-1} + \ldots + \gamma_0$ όπου είναι $k, m \geq 1$ και $a_n = \beta_k \gamma_m$ και $a_0 = \beta_0 \gamma_0$.

Αφού ο p δεν διαιρεί τον a_n, δεν διαιρεί ούτε τον β_k ούτε τον γ_m.

Επίσης, επειδή ο p^2 δεν διαιρεί τον a_0, ο p δεν διαιρεί έναν από τους β_0 και γ_0 και διαιρεί τον άλλο. Έστω, λοιπόν, ότι $p | \beta_0$, αλλά ο p δεν διαιρεί τον γ_0. Έστω, τώρα, ότι $\beta_j, j \geq 1$ εκείνος ο συντελεστής β με τον μικρότερο δείκτη j, τον οποίο ο p δεν διαιρεί. Ο συντελεστής a_j του x^j στο πολυώνυμο f διαιρείται από τον p. Στο γινόμενο gh ο συντελεστής του όρου x^j είναι ο $\sum_{k=0}^{j} \beta_k \gamma_{j-k}$, ο οποίος δεν διαιρείται από τον p. Άτοπο.

Παρατήρηση. Αν δεν εφαρμόζεται το κριτήριο του Eisenstein, τότε δεν μπορούμε να συμπεράνουμε ότι το f(x) δεν είναι ανάγωγο.

Λήμμα 4.5. Το πολυώνυμο f(x) είναι ανάγωγο αν και μόνο αν το $f(x+1)$ είναι ανάγωγο.

Απόδειξη: Πράγματι, $f(x+1)=g(x)h(x)$ αν και μόνο αν $f(x)=g(x-1)h(x-1)$.

Παραδείγματα. **1)** $f(x)=x^5-2$ με $f\in\mathbb{Z}[x]$. Εφαρμόζουμε το κριτήριο του Eisenstein για $p=2$ και τότε το f(x) είναι ανάγωγο επί του $\mathbb{Q}$.

2) $f(x)=x^5+4x^4+2x+6$ με $f\in\mathbb{Z}[x]$. Εφαρμόζουμε το κριτήριο του Eisenstein για $p=2$ και τότε το f(x) είναι ανάγωγο επί του $\mathbb{Q}$.

3) $f(x)=x^3+3x+2$ με $f\in\mathbb{Z}[x]$. $f(x+1)=x^3+3x^2+6x+6$

Εφαρμόζουμε το κριτήριο του Eisenstein στο $f(x+1)$ για $p=3$ άρα το $f(x+1)$ είναι ανάγωγο επί του $\mathbb{Q}$ οπότε από το Λήμμα 4.5 και το f(x) είναι ανάγωγο επί του $\mathbb{Q}$.

Ορισμός 4.6. Αν p πρώτος αριθμός, τότε το $\varphi_p(x)=\dfrac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\ldots+x+1$ ονομάζεται **p-οστό κυκλοτομικό πολυώνυμο**.

Πόρισμα 4.7. Το p-οστό κυκλοτομικό πολυώνυμο είναι ανάγωγο επί του $\mathbb{Q}$ για κάθε πρώτο αριθμό p.

Απόδειξη. $\varphi_p(x+1)=\dfrac{(x+1)^p-1}{(x+1)-1}=x^{p-1}+\binom{p}{1}x^{p-2}+\binom{p}{2}x^{p-3}+\ldots+\binom{p}{p-1}$.

Είναι γνωστό ότι για κάθε $k=1,2,\ldots,p-1$ ο διωνυμικός συντελεστής $\binom{p}{k}$ είναι πολλαπλάσιο του p, $p\nmid 1$ και $p\mid\binom{p}{k}$ για κάθε $k=1,2,\ldots,p-1$. Επίσης, $p^2\nmid\binom{p}{p-1}$ γιατί $\binom{p}{p-1}=p$. Άρα από κριτήριο Eisenstein το $\varphi_p(x+1)$ είναι ανάγωγο οπότε και το πολυώνυμο $\varphi_p(x)$ είναι ανάγωγο.

Σημείωση. Με την ίδια μέθοδο αποδεικνύεται ότι και το $\dfrac{x^{p^2}-1}{x-1}=x^{p(p-1)}+x^{p(p-2)}+\ldots+x^p+1$ είναι ανάγωγο εν $\mathbb{Q}[x]$.

ΚΕΦΑΛΑΙΟ 5

ΕΠΕΚΤΑΣΕΙΣ ΣΩΜΑΤΟΣ

Ορισμός 5.1. Έστω $(K,+,\cdot)$ ένα σώμα και F ένα υποσύνολο του K. Το F καλείται **υπόσωμα** του K αν

- Το $(F,+)$ είναι υποομάδα της $(K,+)$ και
- Το $(F^*,+)$ είναι υποομάδα της $(K^*,+)$, όπου $K^* = K-\{0\}$, $F^* = F-\{0\}$.

- Από τον ορισμό προκύπτει ότι ένα υπόσωμα F ενός σώματος K είναι επίσης ένα σώμα ως προς τις ίδιες πράξεις.

- Αν το F είναι υπόσωμα του K τότε λέμε ότι το K είναι **επέκταση** του σώματος F και συμβολίζουμε $K|F$.

- Αν $F \neq K$ τότε το K λέγεται **γνήσια επέκταση** του F και το F **γνήσιο υπόσωμα** του K.

Ορισμός 5.2. Ένα σώμα λέγεται **πρώτο** αν δεν περιέχει γνήσια υποσώματα.

Παρατήρηση. Έστω K μια επέκταση ενός σώματος F. Τότε μπορούμε να δούμε το K ως έναν διανυσματικό χώρο επί του F, στον οποίο η πρόσθεση των διανυσμάτων είναι η συνήθης πρόσθεση στο K και ο βαθμωτός πολλαπλασιασμός aα είναι ο συνήθης πολλαπλασιασμός του σώματος K, με a $\in$F και α $\in$ K. Τα αξιώματα προκύπτουν αμέσως από τα αξιώματα του σώματος για το K. Σ' αυτή την περίπτωση, το σώμα των βαθμωτών είναι ένα υποσύνολο του χώρου των διανυσμάτων.

Τώρα το K ως διανυσματικός χώρος επί του F έχει μια διάσταση $\dim_F K$.

Ορισμός 5.3. Καλούμε **βαθμό μιας επεκτάσεως K/F** τη διάσταση $\dim_F K$ του διανυσματικού χώρου K επί του F. Τον βαθμό αυτό τον συμβολίζουμε με $[K:F]$. Άρα $[K:F]=\dim_F K$.

Ο βαθμός $[K:F]$ μπορεί να είναι ένας **άπειρος ή πεπερασμένος πληθικός αριθμός.** Αν ο $[K:F]$ είναι ένας πεπερασμένος αριθμός, τότε η επέκταση K/F λέγεται **πεπερασμένη**, διαφορετικά λέμε ότι η K/F είναι **άπειρη επέκταση**.

Παραδείγματα. **1)** Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι μια επέκταση του σώματος $\mathbb{R}$ των πραγματικών αριθμών. Εδώ $[\mathbb{C}:\mathbb{R}]=2$ διότι τα 1, i αποτελούν μια βάση του $\mathbb{C}$ επί του $\mathbb{R}$.

2) Αν F(x) παριστάνει το σώμα των ρητών εκφράσεων επί του σώματος F, τότε η F(x)/F είναι μια άπειρη επέκταση γιατί τα στοιχεία $1, x, x^2, \ldots, x^n, \ldots$, για παράδειγμα, είναι γραμμικώς ανεξάρτητα επί του F. Προφανώς τα $1, x, x^2, \ldots$ δεν αποτελούν βάση του F(x) επί του F.

Πρόταση 5.4. Έστω F, E, K τρία σώματα με $F \subseteq E \subseteq K$. Αν οι E/F και K/E είναι πεπερασμένες επεκτάσεις, τότε η K/F είναι πεπερασμένη επέκταση και ισχύει ότι:

$$[K:F]=[K:E][E:F]$$

<u>*Απόδειξη.*</u> Έστω $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ μια βάση του K επί του E και $\{\beta_1,\beta_2,\ldots,\beta_m\}$ μια βάση του E επί του F. Αρκεί να δείξουμε ότι το $M=\{\alpha_i\beta_j \,/\, i=1,2,\ldots,n,\ j=1,2,\ldots,m\}$ είναι μια βάση του K επί του F.

Έστω $a \in K$. Τότε:

$a=c_1\alpha_1+\ldots+c_n\alpha_n$, $c_i \in E$ αφού η $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ είναι μια βάση του K επί του E.

Επίσης, για κάθε c_i έχουμε:

$c_i=d_{i1}\beta_1+\ldots+d_{im}\beta_m$, $d_{ij} \in F$ αφού η $\{\beta_1,\beta_2,\ldots,\beta_m\}$ είναι μια βάση του E επί του F.

Επομένως:

$$a=\sum_{i=1}^{n}c_i\alpha_i=\sum_{i=1}^{n}\left(\sum_{j=1}^{m}d_{ij}\beta_j\right)\alpha_i=\sum_{i=1,j=1}^{n,m}d_{ij}\alpha_i\beta_j$$

Άρα το M παράγει το K επί του F.

Έστω, τώρα, $\sum_{i=1,j=1}^{n,m}d_{ij}\alpha_i\beta_j=0$. Τότε: $\sum_{i=1}^{n}\left(\sum_{j=1}^{m}d_{ij}\beta_j\right)\alpha_i=0$ και επειδή $\sum_{j=1}^{m}d_{ij}\beta_j\in E$ και η $\{\alpha_1,\alpha_2,...,\alpha_n\}$ μια βάση του K επί του E, παίρνουμε ότι: $\sum_{j=1}^{m}d_{ij}\beta_j=0,\ i=1,2,...,n$.

Αλλά $d_{ij}\in F$ και $\{\beta_1,\beta_2,...,\beta_m\}$ μια βάση του E επί του F. Άρα $d_{ij}=0$, $i=1,2,...,n$, $j=1,2,...,m$. Συνεπώς, το M είναι μια βάση του K επί του F.

Επειδή $|M|=nm$ παίρνουμε: $[K:F]=[K:E][E:F]$

Παρατήρηση. Αν K/F είναι πεπερασμένη επέκταση και $F\subseteq E\subseteq K$, τότε η E/F είναι πεπερασμένη επέκταση, διότι το E είναι διανυσματικός υπόχωρος του K επί του F. Ομοίως, η K/E είναι πεπερασμένη αφού παράγεται από ένα πεπερασμένο σύνολο (μια βάση του K επί του F) επί του E.

Πόρισμα 5.5. Αν $F_1,F_2,...,F_n$, $n\geq 3$ είναι σώματα και F_i/F_{i-1} είναι μια επέκταση για $i=1,2,...,n$ τότε:

$$[F_n:F_1]=[F_n:F_{n-1}][F_{n-1}:F_{n-2}]...[F_2:F_1]$$

<u>Απόδειξη.</u> Για $n=3$ ισχύει από την προηγούμενη πρόταση. Έστω ότι ισχύει για $n=n-1$. Τότε:

$$[F_{n-1}:F_n]=[F_{n-1}:F_{n-2}]...[F_2:F_1]\ (1)$$

Το $F_1\subseteq F_{n-1}\subseteq F_n$ άρα:

$$[F_n:F_1]=[F_n:F_{n-1}][F_{n-1}:F_1]$$

Και άρα η (1) γίνεται:

$$[F_n:F_1]=[F_n:F_{n-1}][F_{n-1}:F_{n-2}]...[F_2:F_1]$$

Πόρισμα 5.6. Αν K/F είναι πεπερασμένη επέκταση και $F \subseteq E \subseteq L \subseteq K$ τότε ο βαθμός [L:E] διαιρεί τον [K:F].

Απόδειξη. Προκύπτει αμέσως από τη σχέση $[K:F]=[K:L][L:E][E:F]$

Ορισμός 5.7. Έστω ότι K/F είναι μια επέκταση σώματος και ότι $\alpha_1,\alpha_2,...,\alpha_n \in K$. Η τομή όλων των υποσωμάτων του K που περιέχουν το σώμα F και το σύνολο $\{\alpha_1,\alpha_2,...,\alpha_n\}$ ονομάζεται **το σώμα που προκύπτει με επισύναψη των** $\alpha_1,\alpha_2,...,\alpha_n$ **στο F** και συμβολίζεται ως $F(\alpha_1,\alpha_2,...,\alpha_n)$. Μια επέκταση K/F είναι **απλή** αν προκύπτει με επισύναψη ενός μόνο στοιχείου α στο F, δηλαδή αν

$$K = F(\alpha) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in F[x] \text{ και } g(\alpha) \neq 0\}$$

Μπορούμε να πάρουμε την επέκταση $F(\alpha_1,\alpha_2,...,\alpha_n)$ με n διαδοχικές απλές επεκτάσεις. Φαίνεται εύκολα ότι το $F(\alpha_1,\alpha_2,...,\alpha_n)$ είναι το μικρότερο υπόσωμα του K που περιέχει και το F και το $\{\alpha_1,\alpha_2,...,\alpha_n\}$ και με αυτό εννοούμε ότι το $F(\alpha_1,\alpha_2,...,\alpha_n) \subset K$ για οποιοδήποτε άλλο υπόσωμα K που περιέχει τα F και $\{\alpha_1,\alpha_2,...,\alpha_n\}$.

Ορισμός 5.8. Έστω K μια επέκταση του σώματος F και $\alpha \in K$. Αν υπάρχει πολυώνυμο $f(x) \in F[x]$ με $f(x) \neq 0$ (δηλαδή f(x) διάφορο του μηδενικού πολυωνύμου) με $f(\alpha)=0$, τότε λέμε ότι το α είναι **αλγεβρικό** επί του F. Αν δεν υπάρχει τέτοιο πολυώνυμο τότε λέμε ότι το α είναι **υπερβατικό** επί του F.

Παραδείγματα. **1)** Έστω $F=\mathbb{Q}$, $E=\mathbb{R}$, $\alpha=\sqrt{2} \in E$ και $f(x)=x^2-2 \in \mathbb{Q}[x]$. Το f(x) είναι μη μηδενικό και $f(\sqrt{2})=0$ άρα το $\sqrt{2}$ είναι αλγεβρικό επί του $\mathbb{Q}$.

2) Έστω $F=\mathbb{Q}$, $E=\mathbb{C}$ και $\alpha=\sqrt{2}+i \in \mathbb{C} \Rightarrow \alpha^2=2+2i\sqrt{2}+i^2 \Rightarrow \alpha^2=1+2i\sqrt{2} \Rightarrow$ $2i\sqrt{2}=\alpha^2-1 \Rightarrow 4i^2(\sqrt{2})^2=\alpha^4-2\alpha^2+1 \Rightarrow \alpha^4-2\alpha^2+9=0$.

Άρα υπάρχει το $f(x)=x^4-2x^2+9\in\mathbb{Q}[x]$ με $f(x)\neq 0$ και $f(\alpha)=0$ άρα το $\alpha=\sqrt{2}+i$ είναι αλγεβρικό επί του $\mathbb{Q}$.

Παρατήρηση. Έχει αποδειχθεί ότι οι πραγματικοί αριθμοί π και e δεν είναι αλγεβρικοί, δηλαδή είναι υπερβατικοί επί του $\mathbb{Q}$.

Ορισμός 5.9. Μια επέκταση K/F λέγεται **αλγεβρική** αν κάθε στοιχείο του K είναι αλγεβρικό επί του F. Αν το K περιέχει υπερβατικά στοιχεία επί του F, τότε λέγεται **υπερβατική επέκταση** του F.

Πρόταση 5.10. Μια πεπερασμένη επέκταση είναι αλγεβρική επέκταση.

Απόδειξη. Έστω $[K:F]=n$. Έστω $\alpha\in K$, $\alpha\neq 0$ και οι δυνάμεις $\alpha^0=1,\alpha,\alpha^2,\ldots,\alpha^n$. Τα στοιχεία αυτά είναι $n+1$ το πλήθος και επομένως είναι γραμμικώς εξαρτημένα επί του F. Άρα υπάρχουν $c_0,c_1,\ldots,c_n\in F$ με $(c_0,c_1,\ldots,c_n)\neq(0,0,\ldots,0)$ ώστε:

$$c_0+c_1\alpha+c_2\alpha^2+\ldots+c_n\alpha^n=0 \quad (1)$$

Το πολυώνυμο $f(x)=c_0+c_1x+c_2x^2+\ldots+c_nx^n$ ανήκει στο $F[x]$ και είναι μη μηδενικό. Επιπλέον λόγω της (1) έχουμε $f(\alpha)=0$. Άρα κάθε στοιχείο του K είναι αλγεβρικό επί του F και επομένως η επέκταση K/F είναι αλγεβρική.

Παρατήρηση. Το αντίστροφο δεν αληθεύει. Δηλαδή, υπάρχουν αλγεβρικές επεκτάσεις που δεν είναι πεπερασμένες.

Έστω K/F μια επέκταση και $\alpha\in K$ ένα στοιχείο αλγεβρικό επί του F. Επιλέγουμε ένα πολυώνυμο $h(x)\in F[x]$, $h(x)\neq 0$ με $h(\alpha)=0$ και $h(x)$ **ελάχιστου βαθμού.**

Λήμμα 5.11. Έστω $h_1(x), h_2(x)\in F[x]$ δύο πολυώνυμα ελαχίστου βαθμού με $h_1(\alpha)=h_2(\alpha)=0$. Τότε το $h_1(x)$ διαιρεί το $h_2(x)$ και το $h_2(x)$ διαιρεί το $h_1(x)$.

Απόδειξη. Επειδή $\deg h_1(x) = \deg h_2(x)$ υπάρχουν σταθερό πολυώνυμο $\pi(x) = c$ με $c \in F^*$ και $\upsilon(x) \in F[x]$ τέτοια ώστε

$$h_1(x) = \pi(x) \cdot h_2(x) + \upsilon(x) \quad (1)$$

όπου $\upsilon(x) = 0$ ή $\upsilon(x) \neq 0$, με $\deg \upsilon(x) < \deg h_2(x)$.

Αν $\upsilon(x) \neq 0$ από την σχέση (1) για $x = \alpha$ παίρνουμε ότι $\upsilon(\alpha) = 0$, άτοπο διότι $h_2(x)$ ελαχίστου βαθμού πολυώνυμο με την ιδιότητα $h_2(\alpha) = 0$.

Άρα $\upsilon(x) = 0$ οπότε $h_1(x) = c \cdot h_2(x)$ άρα το $h_2(x)$ διαιρεί το $h_1(x)$.
Ομοίως, το $h_1(x)$ διαιρεί το $h_2(x)$.

Ορισμός 5.12. Το μονοσήμαντα ορισμένο πολυώνυμο που είναι ένα μονικό πολυώνυμο μη μηδενικό και ελαχίστου βαθμού που μηδενίζεται από το α καλείται **το ελάχιστο πολυώνυμο του α επί του F** και συμβολίζεται $\varphi_\alpha(x)$. Ο βαθμός $n = \deg \varphi_\alpha(x)$ καλείται **βαθμός του α επί του F**.

Παραδείγματα. **1)** Έστω i η φανταστική μονάδα. Το στοιχείο i είναι ένα στοιχείο αλγεβρικό επί του $\mathbb{R}$. Το ελάχιστο πολυώνυμο του i επί του $\mathbb{R}$ είναι το $x^2 + 1$.

2) Έστω $\alpha = \sqrt{2} + \sqrt{3}$. Από την $\alpha = \sqrt{2} + \sqrt{3}$ παίρνουμε $\left(\alpha - \sqrt{2}\right)^2 = \left(\sqrt{3}\right)^2$ ή $\alpha^2 - 2\sqrt{2}\alpha - 1 = 0$. Έτσι, το α είναι αλγεβρικό επί του $\mathbb{Q}\left(\sqrt{2}\right)$ και μηδενίζει το $x^2 - 2\sqrt{2}x - 1$, που είναι και το ελάχιστο πολυώνυμο του α επί του $\mathbb{Q}\left(\sqrt{2}\right)$. Από την $\alpha^2 - 2\sqrt{2}\alpha - 1 = 0$ παίρνουμε, τώρα, $\left(\alpha^2 - 1\right)^2 = \left(2\sqrt{2}\alpha\right)^2$ ή $\alpha^4 - 10\alpha^2 + 1 = 0$. Είναι εύκολο να δειχθεί ότι το $x^4 - 10x^2 + 1$ είναι ανάγωγο επί του $\mathbb{Q}$ και επομένως το α είναι βαθμού 4 επί του $\mathbb{Q}$.

Πόρισμα 5.13. Έστω K/F μια επέκταση και $\alpha \in K$ αλγεβρικό επί του F. Το ελάχιστο πολυώνυμο $\varphi_\omega(x)$ του α επί του F είναι ανάγωγο.

Απόδειξη. Έστω ότι υπάρχουν $g(x), h(x) \in F[x]$ με $\varphi_\omega(x) = g(x) \cdot h(x)$. Για $x = \alpha$ έχουμε: $\varphi_\omega(\alpha) = g(\alpha) \cdot h(\alpha) \Rightarrow 0 = g(\alpha) \cdot h(\alpha) \Rightarrow g(\alpha) = 0$ ή $h(\alpha) = 0$. Επομένως, ένα από τα $g(x), h(x)$ είναι σταθερό πολυώνυμο, αφού το $\varphi_\omega(x)$ είναι ελάχιστο πολυώνυμο του α.

Πρόταση 5.14. Αν το στοιχείο α είναι αλγεβρικό βαθμού n επί του σώματος F, τότε κάθε στοιχείο του F(α) γράφεται μονοσήμαντα με την μορφή:

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1},\ c_i \in F,\ i = 1, 2, \ldots, n-1$$

Απόδειξη. Αν m(x) είναι το ελάχιστο πολυώνυμο του α επί του F, τότε $\deg m(x) = n$. Τα στοιχεία $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ είναι γραμμικώς ανεξάρτητα επί του F. [Πράγματι, αν $b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1} = 0$ για $b_i \in F,\ i = 1, 2, \ldots, n-1$, τότε $b_0 = b_1 = b_2 = \ldots = b_{n-1} = 0$ γιατί διαφορετικά το $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1}$ θα ήταν ένα μη μηδενικό πολυώνυμο βαθμού $< n$ με $g(\alpha) = 0$, που είναι αδύνατο αφού ο βαθμός του α είναι n].

Αν τώρα $\sigma(x) \in F[x]$ και $\deg \sigma(x) > n-1$, τότε υπάρχουν $q(x), r(x) \in F[x]$ τέτοια ώστε $\sigma(x) = q(x) \cdot m(x) + r(x)$ με $r(x) = 0$ ή $\deg r(x) \le n-1$. Τώρα, για $x = \alpha$ παίρνουμε $\sigma(\alpha) = q(\alpha) \cdot m(\alpha) + r(\alpha) = r(\alpha)$. Επειδή $F[\alpha] = F(\alpha)$ η πρόταση έχει αποδειχθεί.

Παρατηρούμε ότι το αντίστροφο ενός στοιχείου $g(\alpha) \in F(\alpha)$, όπου $g(x) \in F[x]$, $\deg g(x) < n$, $g(\alpha) \ne 0$ βρίσκεται ως εξής: Επειδή το ελάχιστο πολυώνυμο m(x) του α είναι ανάγωγο επί του F, τα πολυώνυμα m(x) και g(x) είναι πρώτα μεταξύ τους και επομένως υπάρχουν $\sigma(x), r(x) \in F[x]$ ώστε $\sigma(x)m(x) + r(x)g(x) = 1$. Άρα $\sigma(\alpha)m(\alpha) + r(\alpha)g(\alpha) = 1$ και επειδή $m(\alpha) = 0$ έχουμε $r(\alpha)g(\alpha) = 1$. Άρα $r(\alpha) = g(\alpha)^{-1}$.

Πόρισμα 5.15. Αν n είναι ο βαθμός του αλγεβρικού στοιχείου α επί του F, τότε $[F(\alpha):F]=n$. Το F(α) είναι ένας διανυσματικός χώρος επί του F διάστασης n.

Εφαρμογές. **1)** Το $\sqrt{2}$ είναι αλγεβρικό στο $\mathbb{Q}$ διότι είναι ρίζα του πολυωνύμου $\varphi(x)=x^2-2\in\mathbb{Q}[x]$ με $\varphi(x)\neq 0$. Επίσης, από κριτήριο του Eisenstein για $p=2$ το $\varphi(x)$ ανάγωγο στο $\mathbb{Q}$ και $\deg\varphi(x)=2$. Άρα η βάση του διανυσματικού χώρου $\mathbb{Q}(\sqrt{2})$ επί του $\mathbb{Q}$ είναι $\{1,c\}=\{1,\sqrt{2}\}$ και $\mathbb{Q}(\sqrt{2})=\{q_0+q_1\sqrt{2},\ q_0,q_1\in\mathbb{Q}\}$.

2) Το $\sqrt[3]{2}$ είναι αλγεβρικό στο $\mathbb{Q}$ διότι είναι ρίζα του πολυωνύμου $\varphi(x)=x^3-2\in\mathbb{Q}[x]$ που είναι ανάγωγο στο $\mathbb{Q}$ (κριτήριο του Eisenstein για $p=2$) και $\deg\varphi(x)=3$ άρα η βάση του διανυσματικού χώρου $\mathbb{Q}(\sqrt[3]{2})$ επί του $\mathbb{Q}$ είναι $\{1,c,c^2\}=\{1,\sqrt[3]{2},\sqrt[3]{4}\}$ και $\mathbb{Q}(\sqrt[3]{2})=\{q_0+q_1\sqrt[3]{2}+q_2\sqrt[3]{4},\ q_i\in\mathbb{Q}, i=0,1,2\}$ και $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$.

3) Ας βρούμε, τώρα, τη μορφή επέκτασης $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Θεωρούμε τρία σώματα:

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$$

Έχουμε δείξει ότι: $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$.

Από την εφαρμογή 1) βρήκαμε ότι η βάση του διανυσματικού χώρου $\mathbb{Q}(\sqrt{2})$ επί του $\mathbb{Q}$ είναι η $\{1,\sqrt{2}\}$.

Θα βρούμε, τώρα, μια βάση του διανυσματικού χώρου $\mathbb{Q}(\sqrt{2},\sqrt{3})$ επί του $\mathbb{Q}(\sqrt{2})$. Θέτουμε $\mathbb{Q}(\sqrt{2})=K$ και έχουμε $[K(\sqrt{3}):K]$ και $\varphi(x)=x^2-3\in K[x]$ το οποίο για να είναι ανάγωγο θα πρέπει $\pm\sqrt{3}\notin K=\mathbb{Q}(\sqrt{2})$ (εδώ δεν ισχύει το κριτήριο του Eisenstein γιατί δεν είμαστε στο $\mathbb{Q}[x]$).

Έστω $\sqrt{3} \in \mathbb{Q}\left(\sqrt{2}\right) = \left\{q_0 + q_1\sqrt{2},\ q_0, q_1 \in \mathbb{Q}\right\}$

δηλαδή $\sqrt{3} = q_0 + q_1\sqrt{2} \Rightarrow 3 = q_0^{\ 2} + 2q_1^{\ 2} + 2q_0q_1\sqrt{2} \Rightarrow 0 = \left(q_0^{\ 2} + 2q_1^{\ 2} - 3\right) + 2q_0q_1\sqrt{2}$.

Όμως, $\left\{1, \sqrt{2}\right\}$ γραμμικώς ανεξάρτητα ως βάση άρα $q_0^{\ 2} + 2q_1^{\ 2} - 3 = 0$ και $2q_0q_1 = 0$ $\Rightarrow q_0 = 0$ ή $q_1 = 0$.

Άρα για $q_0 = 0 \Rightarrow 2q_1^{\ 2} - 3 = 0$ άρα το πολυώνυμο $f(x) = 2x^2 - 3 \in \mathbb{Q}[x]$ έχει ρητή ρίζα το $q_1 \in \mathbb{Q}$. Από κριτήριο του Eisenstein για $p = 3$ είναι ανάγωγο. Άτοπο.

Για $q_1 = 0 \Rightarrow q_0^{\ 2} - 3 = 0$ άρα το πολυώνυμο $f(x) = x^2 - 3 \in \mathbb{Q}[x]$ έχει ρητή ρίζα το $q_0 \in \mathbb{Q}$. Από κριτήριο του Eisenstein για $p = 3$ είναι ανάγωγο. Άτοπο.

Άρα $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$.

Ομοίως, $-\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$. Άρα το φ(x) ανάγωγο στο K και $\deg \varphi(x) = 2$. Άρα $\left\{1, \sqrt{3}\right\}$ βάση του $K\left(\sqrt{3}\right)$ επί του K.

Πολλαπλασιάζουμε τις δύο βάσεις $\left\{1, \sqrt{2}\right\}$, $\left\{1, \sqrt{3}\right\}$.

Το σύνολο $\left\{1, \sqrt{3}, \sqrt{2}, \sqrt{2}\cdot\sqrt{3}\right\}$ είναι βάση του $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ επί του $\mathbb{Q}$ δηλαδή:

$$\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{q_0 + q_1\sqrt{3} + q_2\sqrt{2} + q_3\sqrt{2}\sqrt{3},\ q_i \in \mathbb{Q}\right\}$$

και $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4$.

ΚΕΦΑΛΑΙΟ 6

ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ GALOIS

Ορισμός 6.1. Έστω K/F επέκταση σωμάτων και H υποομάδα της ομάδας των αυτομορφισμών του σώματος K. Το σύνολο Fix H= { $\alpha\in$ K : T(α)= α, $\forall$ T$\in$ H} είναι ένα σώμα, υπόσωμα του K και λέγεται **σταθερό σώμα** της ομάδας H.

Ορισμός 6.2. **Ομάδα Galois** μιας επέκτασης K/F (σμβ. Gal(K/F)) είναι οι F-ισομορφισμοί του K, δηλ. ισομορφισμοί του K που δρουν ταυτοτικά στα στοιχεία του F.

Αν K=F($\alpha_1,\alpha_2,\ldots,\alpha_n$) , τότε οι F- ισομορφισμοί του K καθορίζονται πλήρως από τη δράση τους στα στοιχεία $\alpha_1,\alpha_2,\ldots,\alpha_n$.

Στην ειδική περίπτωση που τα $\alpha_1,\alpha_2,\ldots,\alpha_n$ είναι οι ρίζες του πολυωνύμου f(x) $\in$ F[x], τότε η ομάδα των F – αυτομορφισμών δηλ. η ομάδα Galois μπορεί να θεωρηθεί σαν την ομάδα μεταθέσεων των ριζών του πολυωνύμου f(x).

Ορισμός 6.3. Μία πεπερασμένη επέκταση σωμάτων K/F λέγεται **επέκταση Galois** αν το σταθερό σώμα της Gal(K/F) συμπίπτει με το F, δηλ.αν Fix Gal(K/F) = F.

Ορισμός 6.4. Μία επέκταση K/F λέγεται **κανονική** αν για κάθε $\alpha\in$ K το ανάγωγο πολυώνυμο του α επί του F έχει όλες τις ρίζες του στο K.

Παράδειγμα. Η $\mathbb{C}/\mathbb{R}$ είναι κανονική, ενώ η $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ όχι, αφού το ανάγωγο πολυώνυμο του $\sqrt[3]{2}$ στο $\mathbb{Q}$ έχει ρίζες τις $\sqrt[3]{2}$,$\omega\sqrt[3]{2}$ και $\omega^2\sqrt[3]{2}$, όπου ω πρωταρχική 3-ρίζα του 1, αλλά $\omega\sqrt[3]{2}\notin\mathbb{Q}\left(\sqrt[3]{2}\right)$. Όμως η $\mathbb{Q}\left(\sqrt[3]{2},\omega\right)/\mathbb{Q}$ είναι κανονική.

Θεώρημα 6.5. Μία πεπερασμένη επέκταση επί του $\mathbb{Q}$ είναι επέκταση Galois αν και μόνο αν είναι κανονική. (γενικά πρέπει να είναι και διαχωρίσιμη. Όμως κάθε επέκταση επί του $\mathbb{Q}$ είναι πάντα διαχωρίσιμη).

Ορισμός 6.6. **Σώμα ριζών** ενός πολυωνύμου $f(x) \in F[x]$ είναι το μικρότερο σώμα K που περιέχει το F και τις ρίζες του πολυωνύμου f(x).

Πόρισμα 6.7. Η επέκταση K/F είναι επέκταση Galois $\Leftrightarrow$ $|Gal(K/F)| = [K:F]$

Σχόλιο. Η βασική ιδέα της θεωρίας Galois είναι να αντιστοιχίζουμε τα ενδιάμεσα σώματα μιας επέκτασης Galois K/F με τις υποομάδες της ομάδας Gal(K/F).

Θεώρημα 6.8. (Θεμελιώδες Θεώρημα θεωρίας Galois).

Έστω K/F πεπερασμένη επέκταση Galois και G= Gal (K/F). Τότε:

i. Υπάρχει 1 -1 και επί αντιστοιχία ανάμεσα στα :

   $A=\{ J$ σώμα : $F \subseteq J \subseteq K \}$ και $B= \{ H$ ομάδα : $H \leq G\}$

   $\varphi: A \to B$ με $J \mapsto Gal(K/J)$

   $\psi: B \to A$ με $H \mapsto Fix\ H$

ii. Επιπλέον $[K:J] = |Gal(K/J)|$

   $[K:F] = |Gal(K/F) : Gal(K/J)|$

iii. J/F είναι επέκταση Galois $\Leftrightarrow Gal(K/J) \lhd Gal(K/F)$

   Τότε $Gal(J/F) \cong Gal(K/F) / Gal(K/J)$.

Παράδειγμα: Η επέκταση σωμάτων $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ είναι επέκταση Galois, γιατί είναι κανονική επέκταση(το $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι σώμα διάσπασης των x^2-3 ,x^2-2), και διαχωρίσιμη (κάθε επέκταση του $\mathbb{Q}$ είναι διαχωρίσιμη).

Επειδή $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}\right]=4$ άρα $|Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}| = 4$.

Τα στοιχεία της ομάδας Galois είναι μεταθέσεις των ριζών των ανάγωγων επί του $\mathbb{Q}$ πολυωνύμων $x^2 - 3$ και $x^2 - 2$.

Έστω λοιπόν φ ∈ Gal($\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$), και θα δούμε ποιες είναι οι δυνατές εικόνες των $\sqrt{2},\sqrt{3}$ (ρίζες των ανάγωγων πολυωνύμων) μέσω της φ

$$\sqrt{2} \to \pm\sqrt{2} \quad \text{και} \quad \sqrt{3} \to \pm\sqrt{3}$$

Άρα οι δυνατές μεταθέσεις είναι:

$id: \sqrt{2} \to \sqrt{2}$ και $\sqrt{3} \to \sqrt{3}$

$\theta: \sqrt{2} \to -\sqrt{2}$ και $\sqrt{3} \to \sqrt{3}$

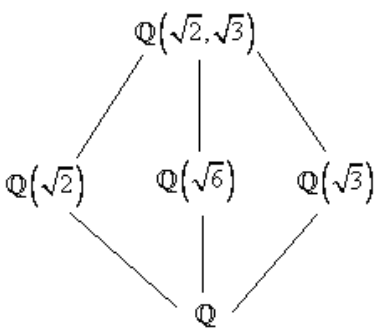
$\sigma: \sqrt{2} \to \sqrt{2}$ και $\sqrt{3} \to -\sqrt{3}$

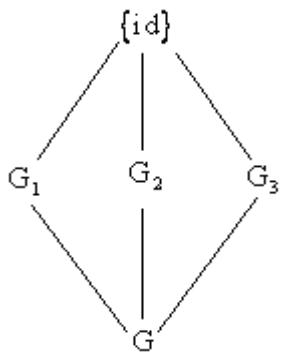
$\tau: \sqrt{2} \to -\sqrt{2}$ και $\sqrt{3} \to -\sqrt{3}$

Άρα Gal($\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)/\mathbb{Q}$) = { id, θ, σ, τ} = { $id, \theta, \sigma, \theta \circ \sigma$ } = G.

Εύκολα υπολογίζεται ότι $\theta^2 = id$, $\sigma^2 = id$, $(\theta \circ \sigma)^2 = id$ και η G είναι πράγματι ομάδα τάξης 4 (είναι ισοδύναμη με την τετραδική ομάδα του Klein).

Έστω $G_1 = < \theta >$, $G_2 = < \theta \circ \sigma >$ και $G_3 =< \sigma >$, οι υποομάδες της ομάδας Galois που παράγονται από τα θ, $\theta \circ \sigma$ και σ αντίστοιχα, τότε το παρακάτω σχήμα δείχνει την αντιστοιχία των ενδιάμεσων σωμάτων της επέκτασης με τις υποομάδες της ομάδας Galois.





Η παραπάνω αντιστοιχία αποδεικνύεται εύκολα, υπολογίζοντας τα

Fix(< θ >), Fix(< σ >) και Fix(<θ o σ >).

Αν αριθμήσουμε τις ρίζες:

$$\sqrt{2} \to 1, -\sqrt{2} \to 2, \sqrt{3} \to 3, -\sqrt{3} \to 4$$

μπορούμε να δούμε τις μεταθέσεις σαν στοιχεία της S_n και θα έχουμε

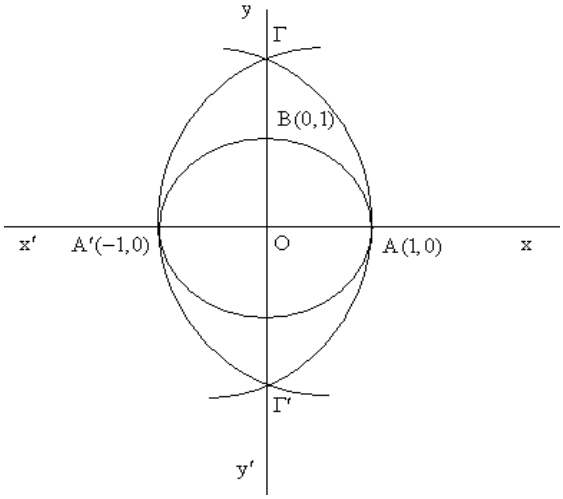
θ= (12), σ= (34) και θ o σ = (12)(34).

ΚΕΦΑΛΑΙΟ 7

ΓΕΩΜΕΤΡΙΚΕΣ ΚΑΤΑΣΚΕΥΕΣ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

Έστω ότι P και Q είναι δύο σημεία του επιπέδου. Το ευθύγραμμο τμήμα με άκρα τα P και Q θα το συμβολίζουμε με PQ και το αντίστοιχο μήκος του με $|PQ|$. Ένας **κανόνας** (ή **χάρακας**) είναι ένα εργαλείο που μπορεί να σχεδιάζει την ευθεία $L(P,Q)$ η οποία ορίζεται από τα P και Q. Ένας **διαβήτης** είναι ένα εργαλείο που μπορεί να σχεδιάζει την περιφέρεια με ακτίνα $|PQ|$ και κέντρο είτε το P είτε το Q. Οι περιφέρειες αυτές θα συμβολίζονται αντίστοιχα με $C(P;Q)$ και $C(Q;P)$. Επειδή κάθε κατασκευή με κανόνα και διαβήτη αποτελείται πάντοτε μόνο από πεπερασμένο πλήθος βημάτων, μπορούμε να ορίσουμε επαγωγικά τα λεγόμενα «κατασκευάσιμα» σημεία.

Εγκαθιστούμε στο επίπεδο ένα σύστημα συντεταγμένων κατά τον εξής τρόπο: Επιλέγουμε πρώτα δύο σαφώς διακεκριμένα σημεία A και A' και ονομάζουμε **άξονα των x** την ευθεία που ορίζεται από αυτά. Χρησιμοποιώντας τον διαβήτη σχεδιάζουμε τις περιφέρειες $C(A;A')$ και $C(A';A)$ με ακτίνα $|AA'|$ και κέντρα τα A και A' αντίστοιχα. Οι περιφέρειες αυτές τέμνονται σε δύο σημεία Γ και Γ' και ονομάζουμε **άξονα των y** την ευθεία που ορίζεται από αυτά. Αυτή είναι μεσοκάθετος του AA' και τέμνει τον άξονα των x σε ένα σημείο O που το ονομάζουμε **αρχή των αξόνων.** Το μήκος $|OA|$ το ορίζουμε ίσο με 1. Με τον τρόπο αυτό εισάγουμε συντεταγμένες στο επίπεδο. Ιδιαιτέρως $A(1,0)$ και $A'(-1,0)$. Ακολούθως σχεδιάζουμε την περιφέρεια $C(O;A)$ που τέμνει τον άξονα των **y** στα σημεία $B(0,1)$ και $B'(0,-1)$ αφού $|OB|=|OB'|=1$.



Έτσι κατασκευάσαμε ένα ορθοκανονικό σύστημα αξόνων κάνοντας στοιχειώδεις κατασκευές. Σαν **στοιχειώδεις κατασκευές** εννοούμε:

- Την κατασκευή μιας ευθείας (με τον κανόνα) η οποία διέρχεται από δύο δεδομένα σημεία (π.χ. η xx') ή από δύο σημεία ήδη κατασκευασμένα (π.χ. η yy').
- Κατασκευή ενός κύκλου με κέντρο δεδομένο ή κατασκευασμένο σημείο και ακτίνα δεδομένο ή κατασκευασμένο μήκος (π.χ. οι κύκλοι $C(A;A')$, $C(A';A)$, $C(O;A)$)
- Κατασκευή ενός σημείου που είναι τομή δύο κατασκευάσιμων κύκλων (π.χ. Γ και Γ') ή τομή κατασκευάσιμης ευθείας και κατασκευάσιμου κύκλου (π.χ. το B).

Ορισμός 7.1. Ένα σημείο είναι **κατασκευάσιμο** αν προκύπτει μετά από πεπερασμένα βήματα στοιχειωδών κατασκευών.

Θα εκθέσουμε τώρα το θέμα μας με αυστηρότητα.

Ορισμός 7.2. Έστω E, F, G και H σημεία το επιπέδου (όχι απαραίτητα σαφώς διακεκριμένα). Ένα σημείο Z είναι **κατασκευάσιμο** από τα E, F, G και H αν προκύπτει με έναν από τους παρακάτω τρόπους:

i) $Z \in L(E,F) \cap L(G,H)$, όπου $L(E,F) \neq L(G,H)$

ii) $Z \in L(E,F) \cap C(G;H)$

iii) $Z \in C(E;F) \cap C(G;H)$ όπου $C(E;F) \neq C(G;H)$

Ένα σημείο Z είναι κατασκευάσιμο αν ή $Z = A$ ή $Z = A'$ ή αν υπάρχουν σημεία $P_1, P_2, ..., P_n$ με $Z = P_n$, τέτοια ώστε για κάθε $j \geq 1$, το P_{j+1} να είναι κατασκευάσιμο από τα σημεία του συνόλου $\{A, A', P_1, P_2, ..., P_j\}$.

Σημείωση. Παρακάτω θα χρησιμοποιήσουμε ορισμένα γνωστά αποτελέσματα της Ευκλείδειας Γεωμετρίας, χωρίς όμως να τα αναφέρουμε διεξοδικά κάθε φορά. Για παράδειγμα, κάθε γωνία διχοτομείται με κανόνα και διαβήτη, δηλαδή αν το $(\cos\theta, \sin\theta)$ είναι κατασκευάσιμο σημείο, τότε και το $(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$ είναι επίσης κατασκευάσιμο σημείο.

Ορισμός 7.3. Ένας μιγαδικός αριθμός $z = x + iy$ ονομάζεται κατασκευάσιμος αν το σημείο (x, y) είναι κατασκευάσιμο.

Για παράδειγμα, εύκολα διαπιστώνουμε ότι οι αριθμοί $1, -1, 0, i\sqrt{3}, -i\sqrt{3}$ και i είναι κατασκευάσιμοι.

Λήμμα 7.4. Ένας μιγαδικός αριθμός $z = x + iy$ είναι κατασκευάσιμος αν και μόνο αν το πραγματικό και το φανταστικό μέρος του είναι κατασκευάσιμοι αριθμοί.

Απόδειξη. Αν z είναι ένας κατασκευάσιμος αριθμός, τότε με μια γνωστή κατασκευή της Ευκλείδειας Γεωμετρίας σχεδιάζεται η κάθετη (ως προς τον άξονα των x) ευθεία L που διέρχεται από το (x, y) και είναι παράλληλη προς τον άξονα των y. Έτσι ο x είναι ένας κατασκευάσιμος αριθμός, αφού το $(x, 0)$ είναι κατασκευάσιμο σημείο ως τομή της L και του άξονα των x. Παρόμοια, το σημείο $(0, y)$ είναι η τομή του άξονα των y και της ευθείας που διέρχεται από το (x, y) και είναι παράλληλη προς τον άξονα των x. Συνεπώς, το $P = (y, 0)$ είναι κατασκευάσιμο ως σημείο του άξονα των x της περιφέρειας $C(O; P)$ και γι' αυτό ο y είναι ένας κατασκευάσιμος αριθμός.

Αντίστροφα, ας υποθέσουμε ότι οι x και y είναι κατασκευάσιμοι αριθμοί, δηλαδή ότι τα $Q=(x,0)$ και $P=(y,0)$ είναι κατασκευάσιμα σημεία. Το $(0,y)$ είναι κατασκευάσιμο ως τομή του άξονα των y και της περιφέρειας $C(O;P)$. Τώρα, φέροντας την κάθετη (ως προς τον άξονα των x) ευθεία γραμμή που διέρχεται από το $(x,0)$ και την οριζόντια (δηλαδή την παράλληλη ως προς τον άξονα των x) ευθεία γραμμή που διέρχεται από το $(0,y)$, παίρνουμε το (x,y) ως τομή αυτών των δύο ευθειών. Έτσι το (x,y) είναι κατασκευάσιμο και σύμφωνα με τον ορισμό ο $z=x+iy$ είναι ένας κατασκευάσιμος αριθμός.

Συμβολισμός 7.5. Θα συμβολίζουμε με K το υποσύνολο του $\mathbb{C}$ που αποτελείται από όλους τους κατασκευάσιμους αριθμούς.

Λήμμα 7.6. i) Αν $K\cap\mathbb{R}$ είναι υπόσωμα του $\mathbb{R}$, τότε το K είναι υπόσωμα του $\mathbb{C}$.
ii) Αν $K\cap\mathbb{R}$ είναι υπόσωμα του $\mathbb{R}$ και αν $\sqrt{a}\in K$, για κάθε θετικό $a\in K\cap\mathbb{R}$, τότε το K είναι κλειστό ως προς τον σχηματισμό των τετραγωνικών ριζών.

Απόδειξη. i) Αν $z=a+ib$ και $w=c+id$ είναι κατασκευάσιμοι αριθμοί, τότε σύμφωνα με το Λήμμα 7.4, τα $a,b,c,d\in K\cap\mathbb{R}$. Επομένως, $a+c,b+d\in K\cap\mathbb{R}$ διότι το $K\cap\mathbb{R}$ είναι υπόσωμα και έτσι από το Λήμμα 7.4. έχουμε $(a+c)+i(b+d)\in K$. Παρόμοια, παίρνουμε $zw=(ac-bd)+i(ad+bc)\in K$. Αν $z\neq 0$ τότε $z^{-1}=\frac{a}{z\bar{z}}-i\frac{b}{z\bar{z}}$. Τώρα, τα $a,b\in K\cap\mathbb{R}$, σύμφωνα με το Λήμμα 7.4, και έτσι $z\bar{z}=a^2+b^2\in K\cap\mathbb{R}$, διότι το $K\cap\mathbb{R}$ είναι υπόσωμα του $\mathbb{C}$. Επομένως, $z^{-1}\in K$.
ii) Αν $z=a+ib\in K$ τότε σύμφωνα με το Λήμμα 7.4. τα $a,b\in K\cap\mathbb{R}$, και όπως και στο ερώτημα i) έπεται $r^2=a^2+b^2\in K\cap\mathbb{R}$. Εφόσον, ο r^2 δεν είναι αρνητικός, η υπόθεση του Λήμματος δίνει ότι οι $r\in K\cap\mathbb{R}$ και $\sqrt{r}\in K\cap\mathbb{R}$. Τώρα επειδή ο $z=re^{i\theta}\in K$ και το K είναι υπόσωμα του $\mathbb{C}$ έπεται ότι $e^{i\theta}=r^{-1}z\in K$. Τέλος, από το γεγονός ότι κάθε γωνίας διχοτομείται, προκύπτει $e^{i\theta/2}\in K$ και έτσι τελικά έχουμε $\sqrt{z}=\sqrt{r}e^{i\theta/2}\in K$, όπως ακριβώς θέλαμε.

Θεώρημα 7.7. Το σύνολο Κ όλων των κατασκευάσιμων αριθμών είναι ένα υπόσωμα του $\mathbb{C}$, το οποίο είναι κλειστό ως προς τον σχηματισμό των τετραγωνικών ριζών και τη μιγαδική συζυγία.

Απόδειξη. Σχετικά με τις δύο πρώτες αποφάνσεις είναι επαρκές να αποδείξουμε ότι για το $K \cap \mathbb{R}$ ικανοποιούνται οι σχετικές ιδιότητες που αναφέρονται στο Λήμμα 7.6 που αποδείξαμε προηγουμένως.

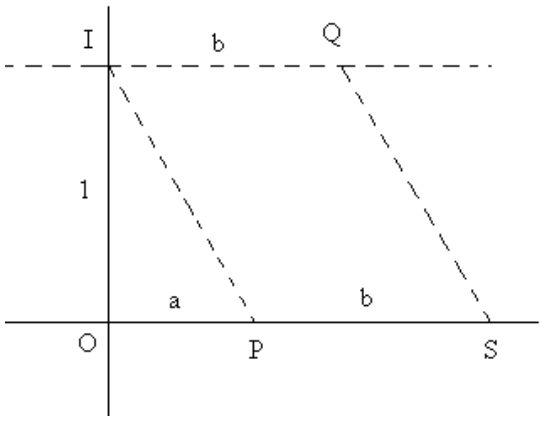
Έστω ότι a και b είναι δύο κατασκευάσιμοι πραγματικοί αριθμοί.

i) Ο αριθμός $-a$ είναι κατασκευάσιμος.

Αν $P=(a,0)$ είναι κατασκευάσιμοι σημείο, τότε το $(-a,0)$ αποτελεί την άλλη τομή του άξονα των x και της περιφέρειας $C(O;P)$.

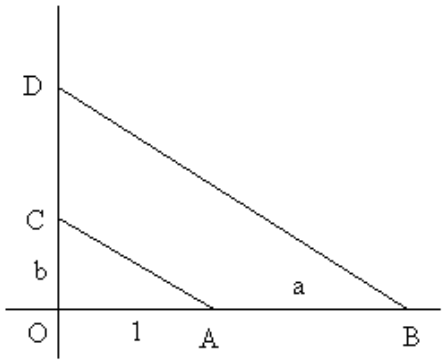
ii) Ο αριθμός $a+b$ είναι κατασκευάσιμος.

Θεωρούμε τα $I=(0,1), P=(a,0)$ και $Q=(b,1)$. Το Q είναι κατασκευάσιμο, επειδή αποτελεί την τομή της οριζόντιας ευθείας που διέρχεται από το I και την κάθετης ευθείας που διέρχεται από το $(b,0)$ (το τελευταίο σημείο είναι κατασκευάσιμο, σύμφωνα με την υπόθεση). Η ευθεία, η οποία διέρχεται από το Q και είναι παράλληλη προς το ευθύγραμμο τμήμα IP, τέμνει τον άξονα των x στο σημείο $S=(a+b,0)$ που είναι ακριβώς το σημείο που θέλαμε. Μολονότι στο διπλανό σχήμα τα a, b παρουσιάζονται ως θετικοί, είναι εύκολο να δει κανείς ότι η κατασκευή λειτουργεί όποιο και αν είναι το πρόσημο των a, b.



iii) Ο αριθμός ab είναι κατασκευάσιμός.

Σύμφωνα με το i) μπορούμε να υποθέσουμε ότι και οι δύο αριθμοί a και b είναι θετικοί. Στο διπλανό σχήμα, θεωρούμε τα σημεία $A=(1,0)$, $B=(1+a,0)$ και $C=(0,b)$. Ορίζουμε το D ως τομή του άξονα των y και της ευθείας που διέρχεται από το B και είναι παράλληλη προς το ευθύγραμμο τμήμα AC. Αφού τα τρίγωνα OAC και OBC είναι όμοια έχουμε:

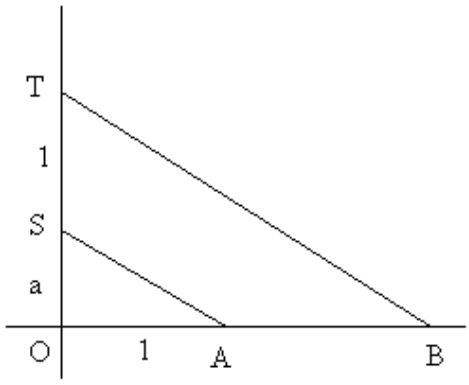


$$\frac{|OB|}{|OA|}=\frac{|OD|}{|OC|}\Leftrightarrow\frac{a+1}{1}=\frac{b+|CD|}{b}\Leftrightarrow|CD|=ab$$

Συνεπώς, ο αριθμός $b+ab$ είναι κατασκευάσιμος. Εφόσον ο αριθμός –b είναι κατασκευάσιμος (σύμφωνα με το i), άρα και ο $ab=(b+ab)-b$ είναι κατασκευάσιμος (σύμφωνα με το ii).

iv) Αν $a\neq 0$ τότε ο αριθμός a^{-1} είναι κατασκευάσιμος.

Έστω ότι $A=(1,0), S=(0,a)$ και $T=(0,1+a)$. Ορίζουμε το B ως την τομή του άξονα των x και της ευθείας που διέρχεται από το T και είναι παράλληλη προς το ευθύγραμμο τμήμα AS. Έτσι, $B=(1+u,0)$ για κάποιο u. Από την ομοιότητα των τριγώνων OSA και OTB έχουμε ότι:

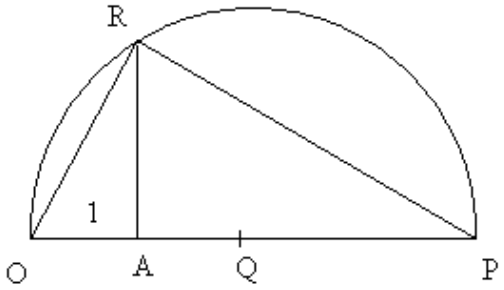


$$\frac{|OT|}{|OS|}=\frac{|OB|}{|OA|}\Leftrightarrow\frac{1+a}{a}=\frac{1+u}{1}\Leftrightarrow u=a^{-1}$$

Συνεπώς, ο αριθμός $1+a^{-1}$ είναι κατασκευάσιμος και γι' αυτό ο $(1+a^{-1})-1=a^{-1}$ είναι κι αυτός κατασκευάσιμος.

v) Αν $a \geq 0$ τότε ο αριθμός $\sqrt{a}$ είναι κατασκευάσιμος.

Έστω ότι $A = (1,0)$ και $P = (1+a,0)$. Κατασκευάζουμε πρώτα το μέσον Q του ευθύγραμμου τμήματος OP. Στη συνέχεια ορίζουμε το σημείο R ως την τομή της περιφέρειας $C(Q;O)$ με την κάθετη ευθεία που διέρχεται από το A. Τα ορθογώνια τρίγωνα AOR και ARP είναι όμοια. Επομένως:



$$\frac{|OA|}{|AR|} = \frac{|AR|}{|AP|} \Leftrightarrow |AR|^2 = |OA||AR| \Leftrightarrow |AR|^2 = a \Leftrightarrow |AR| = \sqrt{a}$$

vi) Αν $z = a + ib \in K$ τότε ο αριθμός $\overline{z} = a - ib$ είναι κατασκευάσιμος.

Σύμφωνα με το Λήμμα 7.6. το K είναι υπόσωμα του $\mathbb{C}$. Τώρα σύμφωνα με το Λήμμα 7.4, τα a και b ανήκουν στο K. Η φανταστική μονάδα i ανήκει στο K. Άρα $-ib \in K$ και επομένως $a - ib \in K$

Θα θεωρήσουμε, τώρα, ορισμένα υποσώματα του $\mathbb{C}$ που πρόκειται να χρησιμοποιηθούν στην απόδειξη του επαγωγικού βήματος του βασικού Θεωρήματος 7.10 που ακολουθεί.

Λήμμα 7.8. Έστω F ένα υπόσωμα του $\mathbb{C}$ που περιέχει τη φανταστική μονάδα i και είναι κλειστό ως προς τη μιγαδική συζυγία. Θεωρούμε δύο στοιχεία $z = a + ib$ και $w = c + id \in F$ και έστω ότι $P = (a,b)$ και $Q = (c,d)$.

i) Αν $a + ib \in F$ τότε $a \in F$ και $b \in F$.

ii) Αν η εξίσωση της $L = (P,Q)$ είναι $y = mx + q$ όπου $m,q \in \mathbb{R}$ τότε $m,q \in F$.

iii) Αν η εξίσωση της $C(P;Q)$ είναι $(x-a)^2 + (y-b)^2 = r^2$, όπου $a,b,r \in \mathbb{R}$, τότε $r^2 \in F$.

<u>*Απόδειξη.*</u> i) Αν $z = a + ib \in F$ τότε $a = \frac{1}{2}(z + \overline{z}) \in F$ και $ib = \frac{1}{2}(z - \overline{z}) \in F$ και επειδή έχουμε υποθέσει ότι $i \in F$, έχουμε ότι $b \in F$.

ii) Αν η ευθεία $L=(P,Q)$ δεν είναι κάθετη (στον άξονα των x) τότε η εξίσωση της είναι: $y-b=m(x-a)$. Ο αριθμός $m=\frac{d-b}{c-a}\in F$, αφού τα $a,b,c,d\in F$ και έτσι το $q=-ma+b\in F$.

iii) Η εξίσωση της περιφέρειας $C(P;Q)$ είναι $(x-a)^2+(y-b)^2=r^2$ και γι' αυτό $r^2=(c-a)^2+(d-b)^2\in F$.

Λήμμα 7.9. Έστω F ένα υπόσωμα του $\mathbb{C}$, το οποίο περιέχει τη φανταστική μονάδα i και είναι κλειστό ως προς τη μιγαδική συζυγία. Έστω ότι P, Q, R, S είναι κάποια σημεία, οι συντεταγμένες των οποίων ανήκουν στο σώμα F και ότι $\alpha=u+iv\in\mathbb{C}$, με $A(u,v)$. .

Αν είτε $A\in L(P,Q)\cap L(R,S)$, όπου $L(P,Q)\neq L(R,S)$

είτε $A\in L(P,Q)\cap C(R;S)$

είτε $A\in C(P;Q)\cap C(R;S)$, όπου $C(P;Q)\neq C(R;S)$

τότε $[F(\alpha):F]\leq 2$.

<u>Απόδειξη.</u> Αν η ευθεία $L(P,Q)$ δεν είναι κάθετη στον άξονα των x, τότε έχει εξίσωση $y=mx+b$, όπου $m,b\in F$ (Λήμμα 7.8.ii). Αν η $L(P,Q)$ είναι κάθετη στον άξονα των x, τότε η εξίσωση της είναι $x=b$, με $b\in F$ (Λήμμα 7.8.i).

Παρόμοια, η εξίσωση της $L(R,S)$ είναι ή $y=nx+c$ ή $x=c$, όπου $n,c\in F$.

Εφόσον οι δύο αυτές ευθείες δεν είναι παράλληλες, το σύστημα των γραμμικών εξισώσεων ως προς τις συντεταγμένες (u,v) του $A\in L(P,Q)\cap L(R,S)$ έχει λύση και μάλιστα αυτές οι συντεταγμένες ανήκουν και πάλι στο σώμα F.

Έτσι στην περίπτωση αυτή έχουμε $[F(\alpha):F]=1$.

Έστω ότι η εξίσωση της $L(P,Q)$ είναι ή $y=mx+b$ ή $x=b$ και ότι η εξίσωση της περιφέρειας $C(R;S)$ είναι $(x-c)^2+(y-d)^2=r^2$. Από το Λήμμα 7.8.γνωρίζουμε ότι τα $m,b,r^2\in F$. Επειδή το $A\in L(P,Q)\cap C(R;S)$ έχουμε:

$$r^2=(u-c)^2+(v-d)^2=(u-c)^2+(mu+b-d)^2$$

και έτσι το u είναι θέση μηδενισμού ενός δευτεροβάθμιου πολυωνύμου με συντελεστές στο $F\cap\mathbb{R}$. Επομένως, $[F(u):F]\leq 2$.

Επειδή $v = mu + b$ έχουμε $v \in F(u)$ και επειδή $i \in F$ έχουμε $\alpha \in F(u)$. Επομένως, $\alpha = u + iv \in F(u)$ και γι' αυτό $[F(\alpha):F] \le 2$.

Έστω ότι η περιφέρεια $C(P;Q)$ έχει εξίσωση $(x-a)^2 + (y-b)^2 = r^2$ και η περιφέρεια $C(R,S)$ έχει εξίσωση $(x-c)^2 + (y-d)^2 = s^2$. Σύμφωνα με το Λήμμα 7.8. έχουμε $r^2, s^2 \in F \cap \mathbb{R}$. Επειδή το $A \in C(P;Q) \cap C(R;S)$ ισχύουν οι ισότητες:

$$(u-a)^2 + (v-b)^2 = r^2 \text{ και } (u-c)^2 + (v-d)^2 = s^2$$

Αν τις αναπτύξουμε, τότε διαπιστώνουμε ότι είναι και οι δύο της μορφής $u^2 + v^2 + \text{"κάτι ακόμη"} = 0$. Εξισώνοντας αυτά τα "κάτι ακόμη", προκύπτει μια εξίσωση της μορφής $tu + t'v + t'' = 0$, όπου $t, t', t'' \in F$. Αν αυτή τη συζεύξουμε με μια από τις εξισώσεις που αντιστοιχούν στις περιφέρειες, τότε επιστρέφουμε στην κατάσταση της αμέσως προηγούμενης περίπτωσης.

Θεώρημα 7.10. Ένας μιγαδικός αριθμός z είναι κατασκευάσιμος αν και μόνον αν υπάρχει πεπερασμένη ακολουθία σωμάτων $Q = K_0 \subset K_1 \subset \ldots \subset K_n$, όπου $z \in K_n$ και $[K_{j+1} : K_j] \le 2$ για όλα τα j.

<u>Απόδειξη.</u> Αν z είναι κατασκευάσιμος αριθμός, τότε υπάρχει μια ακολουθία σημείων $1, -1, z_1, \ldots, z_n = z$, όπου κάθε z_j προέρχεται από το $\{1, -1, z_1, \ldots, z_{j-1}\}$.

Επειδή η φανταστική μονάδα i είναι κατασκευάσιμος αριθμός, μπορούμε να υποθέσουμε ότι $z_1 = i$. Θέτουμε $K_j = \mathbb{Q}(z_1, \ldots, z_j)$.

Αν $u = z_{j+1}$ τότε υπάρχουν κάποια σημεία $E, F, G, H \in K_j$, τέτοια ώστε να ισχύει ένα από τα παρακάτω: $u \in L(E,F) \cap L(G,H)$

$$u \in L(E,F) \cap C(G;H)$$

$$u \in C(E;F) \cap C(G;H)$$

Χρησιμοποιώντας επαγωγή ως προς $j \ge 1$, μπορούμε να υποθέσουμε ότι το K_j είναι κλειστό ως προς τη μιγαδική συζυγία. Η παραδοχή αυτή επιτρέπει την εφαρμογή του Λήμματος 7.9 και έτσι έχουμε ότι $[K_{j+1} : K_j] \le 2$.

Τέλος, διαπιστώνουμε ότι και το K_{j+1} είναι κλειστό ως προς τη μιγαδική συζυγία, αφού αν z_{j+1} είναι μια θέση μηδενισμού του δευτεροβάθμιου $f(x) \in K_j[x]$, τότε το $\overline{z}_{j+1}$ είναι η άλλη θέση μηδενισμού του f(x).

Για το <u>αντίστροφο</u>, αρκεί να δείξουμε ότι αν $[B:F]=2$ με $F \subset K$, τότε η B/F αποτελεί μια καθαρή επέκταση τύπου 2, ας πούμε $B = F(\beta)$, όπου $\beta \in L(P,Q) \cap C(R;S)$ για κάποια $P,Q,R,S \in F$. Από αυτό θα προκύψει κατόπιν ότι $B \subset K$. Αφού, λοιπόν, $[B:F]=2$ υπάρχει κάποιο α ώστε $B = F(\alpha)$, όπου το α είναι μια θέση μηδενισμού κάποιου ανάγωγου δευτεροβάθμιου πολυωνύμου $x^2 + bx + c \in F[x]$. Άρα το α είναι της μορφής $\alpha = -\frac{b}{2} \pm \frac{\sqrt{b^2-4c}}{2}$.

Θέτοντας $\beta = \sqrt{b^2-4c}$, τότε επειδή $B = F(\beta)$ έπεται ότι η επέκταση B/F είναι καθαρή τύπου 2. Τέλος, για να διαπιστώσουμε ότι το β υλοποιείται ως σημείο τομής μιας ευθείας με μια περιφέρεια, επαναλαμβάνουμε την κατασκευή του προηγούμενου Θεωρήματος 7.7.v. Έστω ότι L είναι η ευθεία που είναι κάθετη (στον άξονα των x) και διέρχεται από το $A = (1,0)$ και ότι C είναι η περιφέρεια κέντρου $Q = \left(\frac{1}{2}\left(1+\beta^2\right), 0\right)$ και ακτίνας $\frac{1}{2}\left(1+\beta^2\right)$.

Πόρισμα 7.11. Αν ένας μιγαδικός αριθμός z είναι κατασκευάσιμος, τότε ο βαθμός $[\mathbb{Q}(z):\mathbb{Q}]$ είναι δύναμη του 2.

<u>Απόδειξη.</u> Προκύπτει αμέσα από το Θεώρημα 7.10 και το Πόρισμα 5.5.

Παρατήρηση. Το αντίστροφο του πορίσματος δεν ισχύει γενικά.

Το πολυώνυμο $p(x) = x^4 - 4x + 2$ είναι ανάγωγο επί του $\mathbb{Q}$.

Αν E είναι ένα σώμα ριζών του p(x) στο $\mathbb{Q}$ τότε $Gal(E/\mathbb{Q}) = S_4$.

Αν κάθε θέση μηδενισμού του p(x) ήταν κατασκευάσιμη, τότε θα ήταν και κάθε στοιχείο του E κατασκευάσιμο, αφού σύμφωνα με το Θεώρημα 7.7 όλοι οι κατασκευάσιμοι αριθμοί σχηματίζουν ένα υπόσωμα του $\mathbb{C}$.

Αν όμως H είναι μια 2-υποομάδα Sylow της $G \cong S_4$, τότε $[G:H]=3$. Αυτό δίνει το συμπέρασμα ότι το ενδιάμεσο σώμα E^H είναι βαθμού $\left[E^H:Q\right]=\left[G:H\right]=3$ και έτσι σύμφωνα με το προηγούμενο Πόρισμα, κανένα από τα στοιχεία του δεν μπορεί να είναι κατασκευάσιμο. Η αντίφαση αυτή δείχνει ότι κάποια από τις θέσεις μηδενισμού του p(x) δεν είναι κατασκευάσιμη, παρά το γεγονός ότι κάθε θέση μηδενισμού του είναι βαθμού 4 υπεράνω του σώματος $\mathbb{Q}$.

Πρόταση 7.12. Αν F υπόσωμα του $\mathbb{R}$, παραγόμενο από τις συντεταγμένες των σημείων κάποιου $P \subseteq \mathbb{R}^2$ και αν x, y $\in$ K, όπου K υπόσωμα του $\mathbb{R}$, κανονική επέκταση του F, βαθμού $[K:F] = 2^r$, τότε το (x, y) κατασκευάζεται από το P.

<u>Απόδειξη:</u> Επειδή η επέκταση K/ F είναι κανονική και διαχωρίσιμη (αφού η χαρακτηριστική του σώματος F είναι μηδέν), άρα είναι επέκταση Galois, οπότε $|Gal(K/F)| = [K:F] = 2^r$.

Θέτουμε G = Gal(K/F).

Επειδή η G είναι μια 2-ομάδα άρα από το Λήμμα 1.19 έχει πεπερασμένη ακολουθία κανονικών υποομάδων:

$$I = G_0 \lhd G_1 \lhd \ldots \lhd G_r = G \quad (1), \qquad \text{με } |G_i| = 2^i \text{ για κάθε } i = 0,1,\ldots,r.$$

Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois θα έχουμε την αντίστοιχη ακολουθία ενδιάμεσων σωμάτων:

$$F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = K$$

και οι υποομάδες G_i της (1) γράφονται σαν ομάδες Galois των σωμάτων αυτών:

$$I_0 = Gal(K/K) \leq Gal(K/K_{r-1}) \leq \ldots \leq Gal(K/K_1) \leq Gal(K/F) = G,$$

όπου $|Gal(K/K_{r-i})| = 2^i$, για κάθε i = 0,1,...,r.

Είναι:

$$[K_1 : F] = |Gal(K_1 / F)| = \frac{|Gal(K / F)|}{|Gal(K / K_1)|} = \frac{2^r}{2^{r-1}} = 2$$

$$[K_2 : F] = |Gal(K_2 / F)| = \frac{|Gal(K / F)|}{|Gal(K / K_2)|} = \frac{2^r}{2^{r-2}} = 2^2$$

.

.

.

$$[K_r : F] = |Gal(K_r / F)| = \frac{|Gal(K / F)|}{|Gal(K / K_r)|} = \frac{2^r}{2^{r-r}} = 2^r$$

Άρα από πολλαπλασιαστικότητα των βαθμών επέκτασης (Πόρισμα 5.5.) έχουμε:

$[K_{j+1} : K_j] = 2$, για κάθε $j = 0,..., r - 1$.

Επομένως, σύμφωνα με το Θεώρημα 7.10, το (x, y) κατασκευάζεται από το P.

<u>Τώρα, πλέον είναι απλή υπόθεση η επίλυση ορισμένων ονομαστών προβλημάτων.</u>

1) Ο «τετραγωνισμός του κύκλου» είναι αδύνατος.

Το πρόβλημα συνίσταται στην κατασκευή με κανόνα και διαβήτη ενός τετραγώνου με εμβαδόν ίσο με το εμβαδόν ενός κύκλου ακτίνας 1. Με άλλα λόγια εξετάζουμε το αν ο αριθμός $\sqrt{\pi}$ είναι κατασκευάσιμος.

Ο F. Lindermann το 1882 απέδειξε ότι ο αριθμός π είναι υπερβατικός επί του $\mathbb{Q}$. Επομένως, και ο αριθμός $\sqrt{\pi}$ είναι υπερβατικός επί του $\mathbb{Q}$ και γι' αυτό δεν υπάρχει πεπερασμένη επέκταση του $\mathbb{Q}$ που να τον περιέχει. Συνεπώς, δεν μπορεί να τον περιέχει ούτε κάποια επέκταση του $\mathbb{Q}$, ο βαθμός της οποίας να είναι δύναμη του 2.

2) Ο «διπλασιασμός του κύβου» είναι αδύνατος.

Το πρόβλημα συνίσταται στην κατασκευή με κανόνα και διαβήτη ενός κύβου με όγκο 2. Με άλλα λόγια, εξετάζουμε αν η πραγματική κυβική ρίζα του 2, ας την πούμε α, είναι κατασκευάσιμη. Όμως σύμφωνα με το κριτήριο Eisenstein, το x^3-2 είναι ανάγωγο επί του $\mathbb{Q}$, και γι' αυτό $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$ που δεν είναι δύναμη του 2. Άρα η ρίζα α δεν είναι κατασκευάσιμη. Η πρώτη απόδειξη του έγινε από τον P. L. Wantzel το 1837.

3) Η τριχοτόμηση μιας οποιασδήποτε γωνίας είναι αδύνατη.

Μια γωνία θ ορίζεται από δύο τεμνόμενες ευθείες γραμμές. Δεν αποτελεί περιορισμό της γενικότητας το να δεχθούμε ότι οι δύο ευθείες τέμνονται στην αρχή των αξόνων και ότι μια από αυτές είναι ο άξονας των x. Αν ήταν δυνατό να κατασκευάσουμε την τριχοτόμο της γωνίας, τότε θα μπορούσαμε να κατασκευάσουμε και το σημείο $(\cos\frac{\theta}{3},\sin\frac{\theta}{3})$ που είναι η τομή της τριχοτόμου και της μοναδιαίας περιφέρειας. Όμως, τότε σύμφωνα με το Λήμμα 7.4. θα ήταν κατασκευάσιμος και ο αριθμός $\cos\frac{\theta}{3}$.

• Με τη βοήθεια της προηγούμενης παρατήρησης θα αποδείξουμε ότι η γωνία 60° δεν τριχοτομείται. Γνωρίζουμε την τριγωνομετρική ταυτότητα:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

Θέτοντας $u=2\cos\theta$ και $\theta=20^\circ$, καταλήγουμε στη σχέση: $u^3-3u-1=0$

Το πολυώνυμο $f(x)=x^3-3x-1$ είναι ανάγωγο επί του $\mathbb{Q}$ (αφού δεν διαθέτει καμία ρητή θέση μηδενισμού) και επομένως $[\mathbb{Q}(u):\mathbb{Q}]=3$. Επομένως ο αριθμός u δεν είναι κατασκευάσιμος. Το αποτέλεσμα αυτό αποδείχθηκε επίσης από τον P. L. Wantzel το 1837.

Σχόλιο. Στο επόμενο κεφάλαιο θα ασχοληθούμε αναλυτικά με την κατασκευασιμότητα των κανονικών πολυγώνων με κανόνα και διαβήτη.

ΚΕΦΑΛΑΙΟ 8

ΚΑΤΑΣΚΕΥΑΣΙΜΟΤΗΤΑ ΚΑΝΟΝΙΚΩΝ ΠΟΛΥΓΩΝΩΝ

Σε όσα ακολουθούν θεωρείται γνωστό ότι είναι δυνατόν, με κανόνα και διαβήτη, να γίνουν τα παρακάτω:

1. Μπορούμε να κατασκευάσουμε ευθεία ε_1, κάθετη σε δοσμένη ευθεία ε_2, που να διέρχεται από δοθέν σημείο $A \in \varepsilon_2$.
2. Μπορούμε να κατασκευάσουμε ευθεία ε_1, κάθετη σε δοσμένη ευθεία ε_2, που να διέρχεται από δοθέν σημείο $A \notin \varepsilon_2$.
3. Μπορούμε να κατασκευάσουμε ευθεία ε_1, παράλληλη σε δοσμένη ευθεία ε_2, που να διέρχεται από δοθέν σημείο $A \notin \varepsilon_2$.

Λήμμα 8.1. Αν το κανονικό n-γωνο είναι κατασκευάσιμο και m/n (ο m διαιρεί τον n), τότε και το κανονικό m-γωνο είναι κατασκευάσιμο.

Απόδειξη. Αν το κανονικό n-γωνο είναι κατασκευάσιμο και m/n, τότε κατασκευάζουμε το κανονικό m-γωνο ενώνοντας κάθε $\frac{n}{m}$ – οστή κορυφή του κανονικού n-γωνου.

Λήμμα 8.2. Το κανονικό 2^r-γωνο είναι κατασκευάσιμο για κάθε $r \in \mathbb{N}$, με $r > 1$.

Απόδειξη. Σύμφωνα με τις κατασκευές 1 και 2 το τετράγωνο κατασκευάζεται . Η διχοτόμηση ενός τόξου είναι κατασκευάσιμη, άρα το κανονικό 2^r-γωνο είναι κατασκευάσιμο για κάθε $r \in \mathbb{N}$, με $r > 1$.

Λήμμα 8.3. Αν $(m,n)=1$, τα κανονικά m-γωνο και n-γωνο είναι κατασκευάσιμα αν και μόνον αν είναι κατασκευάσιμο το κανονικό $m \cdot n$ -γωνο.

Απόδειξη. Αν το κανονικό $m \cdot n$ -γωνο είναι κατασκευάσιμο και $A_1, A_n, A_{2n}, ..., A_{mn}$ οι κορυφές του τότε τα σημεία $A_1, A_n, A_{2n}, ..., A_{mn}$ είναι κορυφές κανονικού m-γωνου.

Αντιστρόφως: Έστω ότι τα κανονικά m-γωνο και n-γωνο με $(m,n)=1$ είναι κατασκευάσιμα. Επειδή $(m,n)=1$, υπάρχουν $k, \ell \in \mathbb{Z}$ με $km + \ell n = 1$ και επομένως $\frac{2\pi}{mn} = k\frac{2\pi}{n} + \ell\frac{2\pi}{m}$. Επειδή τα κανονικά m-γωνο και n-γωνο είναι κατασκευάσιμα, άρα οι γωνίες $\frac{2\pi}{n}, \frac{2\pi}{m}$ είναι κατασκευάσιμες οπότε είναι κατασκευάσιμη και η γωνία $\frac{2\pi}{mn}$. Επομένως το κανονικό $m \cdot n$ -γωνο είναι κατασκευάσιμο.

Παράδειγμα. Είναι γνωστή η γεωμετρική κατασκευή του ισόπλευρου τριγώνου και του κανονικού πενταγώνου .

Είναι: $(3,5)=1$ και $2 \cdot 5 - 3 \cdot 3 = 1$ τότε $2 \cdot \frac{1}{3} - 3 \cdot \frac{1}{5} = \frac{1}{15}$.

Αν από 2 φορές το τόξο πλευράς κανονικού τριγώνου αφαιρέσουμε τρεις φορές το τόξο πλευράς κανονικού πενταγώνου προκύπτει το τόξο πλευράς κανονικού δεκαπενταγώνου.

Λήμμα 8.4. Έστω p περιττός πρώτος αριθμός. Αν το κανονικό p-γωνο είναι κατασκευάσιμο τότε: $p = 2^{2^\nu} + 1$ για κάποιον φυσικό αριθμό ν≥0.

Απόδειξη. Επειδή το κανονικό p-γωνο είναι κατασκευάσιμο άρα και το $\cos\frac{2\pi}{p}$ είναι κατασκευάσιμο. Επομένως σύμφωνα με το Πόρισμα 7.11. είναι: $\left[\mathbb{Q}\left(\cos\frac{2\pi}{p}\right):\mathbb{Q}\right] = \text{δύναμη του } 2$.

Το κυκλοτομικό πολυώνυμο $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ είναι ανάγωγο επί του $\mathbb{Q}$ (Πόρισμα 4.7) και έχει ρίζα το $z = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, άρα $[\mathbb{Q}(z):\mathbb{Q}] = p-1$.

Όμως, $\cos\frac{2\pi}{p}=\frac{1}{2}\left(z+z^{-1}\right)$ άρα $\left[\mathbb{Q}(z):\mathbb{Q}\left(\cos\frac{2\pi}{p}\right)\right]=2$.

Είναι:
$$p-1=\begin{cases}\mathbb{Q}(z)\\ 2\\ \mathbb{Q}\left(\cos\frac{2\pi}{p}\right)\\ \text{δύναμη του } 2\\ \mathbb{Q}\end{cases}$$

Ισχύει η πολλαπλασιαστικότητα των βαθμών επέκτασης (Πόρισμα 5.5) άρα $p-1=$ δύναμη του 2. Δηλαδή, $p-1=2^k$ οπότε $p=2^k+1$.

Αν υπάρχει περιττός ℓ τέτοιος ώστε $k=m\cdot\ell$ τότε:

$p=2^{m\cdot\ell}+1=\left(2^m\right)^{\ell}+1=\text{πολ}(2^m+1)$ άτοπο, γιατί ο p είναι πρώτος .

Επομένως ο k είναι δύναμη του 2 δηλαδή υπάρχει φυσικός αριθμός ν≥0 ώστε $k=2^{\nu}$ οπότε: $p=2^{2^{\nu}}+1$.

Λήμμα 8.5. Αν p περιττός πρώτος, τότε το κανονικό p^n-γωνο για $n\geq 2$ δεν είναι κατασκευάσιμο.

<u>Απόδειξη.</u> Έστω ότι το κανονικό p^n-γωνο για $n\geq 2$ είναι κατασκευάσιμο. Τότε το $\cos\frac{2\pi}{p^n}$ είναι κατασκευάσιμο και $\cos\frac{2\pi}{p^n}\notin\mathbb{Q}$ οπότε $\left[\mathbb{Q}\left(\cos\frac{2\pi}{p^n}\right):\mathbb{Q}\right]=2^{\mu}$ (δύναμη του 2).

Αν $z=\cos\frac{2\pi}{p^n}+\sin\frac{2\pi}{p^n}$ τότε είναι $\left[\mathbb{Q}(z):\mathbb{Q}\right]=p^{n-1}(p-1)$, γιατί $\varphi(p^n)=p^{n-1}(p-1)$ όπου φ η συνάρτηση του Euler.

Όμως, $\cos\frac{2\pi}{p^n}=\frac{1}{2}(z+z^{-1})$ άρα $\left[\mathbb{Q}(z):\mathbb{Q}\left(\cos\frac{2\pi}{p^n}\right)\right]=2$.

Είναι:

$$p^{n-1}(p-1)=\begin{cases}\mathbb{Q}(z)\\ 2\\ \mathbb{Q}\left(\cos\frac{2\pi}{p^n}\right)\\ 2^{\mu}\\ \mathbb{Q}\end{cases}$$

Ισχύει η πολλαπλασιαστικότητα των βαθμών επέκτασης (Πόρισμα 5.5) άρα $p^{n-1}(p-1)=$ δύναμη του 2, άρα p άρτιος που είναι άτοπο.

Λήμμα 8.6. Αν F σώμα με χαρακτηριστική 0 και K το σώμα ριζών του πολυωνύμου x^p-1 στο F, όπου p πρώτος, τότε η ομάδα Gal(K/F) είναι αβελιανή.

Απόδειξη. Οι ρίζες του πολυωνύμου x^p-1, δηλαδή οι p-ρίζες του 1, αποτελούν πολλαπλασιαστική ομάδα τάξης p, άρα κυκλική. Αν z ένας γεννήτοράς της, τότε K = F(z).

Κάθε F-αυτομορφισμός του K καθορίζεται από τη δράση του στο z και είναι μια μετάθεση των ριζών του πολυωνύμου x^p-1. Άρα θα είναι της μορφής $\sigma_j(z)=z^j$. Όμως τότε η ομάδα θα είναι αβελιανή αφού $\sigma_i \circ \sigma_j(z)=z^{ij}=\sigma_j \circ \sigma_i(z)$.

Θεώρημα 8.7. (Gauss). Το κανονικό n-γωνο είναι κατασκευάσιμο με κανόνα και διαβήτη αν και μόνο αν ο n μπορεί να γραφτεί στη μορφή $n = 2^r p_0 ... p_k$ όπου οι αριθμοί $r, k \in \mathbb{N} \cup \{0\}$, $p_0 = 1$ και $p_1, ..., p_k$ είναι περιττοί πρώτοι της μορφής $2^{2^v} + 1$, με ν μη αρνητικό ακέραιο.

(Οι πρώτοι αριθμοί της μορφής $2^{2^v} + 1$ λέγονται πρώτοι του Fermat).

Απόδειξη. Έστω ότι το κανονικό n-γωνο είναι κατασκευάσιμο. Έστω $n = 2^r \cdot p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$, $3 \le p_1 < p_2 < ... < p_k$ η μονοσήμαντη ανάλυση του n σε γινόμενο πρώτων παραγόντων (p_i, i=1,…,k διακριτοί πρώτοι).

Αν $m = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$ τότε $n = 2^r \cdot m$. Επειδή το κανονικό n-γωνο με $n = 2^r \cdot m$ είναι κατασκευάσιμο, το κανονικό 2^r-γωνο είναι κατασκευάσιμο και $(2^r, m) = 1$, άρα από το Λήμμα 8.3 το κανονικό m-γωνο θα είναι κατασκευάσιμο.

Επομένως, το κανονικό $p_i^{\alpha_i}$-γωνο είναι κατασκευάσιμο για κάθε $i = 1, 2, ..., k$.

Σύμφωνα με το Λήμμα 8.5 πρέπει $\alpha_i = 1$ για κάθε $i = 1, 2, ..., k$.

Άρα το p_i-γωνο είναι κατασκευάσιμο οπότε με βάση το Λήμμα 8.4 έχουμε ότι $p_i = 2^{2^{v_i}} + 1$ όπου με $v_i \ge 0$ μη αρνητικοί ακέραιοι, $i = 1, 2, ..., k$.

Άρα αναγκαία συνθήκη ώστε ένα κανονικό n-γωνο να είναι κατασκευάσιμο είναι το n να γράφεται στη μορφή $n = 2^r p_0 ... p_k$ όπου οι αριθμοί $r, k \in \mathbb{N} \cup \{0\}$, $p_0 = 1$ και $p_1, ..., p_k$ είναι περιττοί πρώτοι της μορφής $2^{2^v} + 1$, με ν μη αρνητικό ακέραιο.

Αντίστροφο:

Σύμφωνα με το Λήμμα 8.2 το κανονικό 2^r-γωνο είναι κατασκευάσιμο.

Άρα σύμφωνα με το Λήμμα 8.3 αρκεί να δείξουμε ότι τα κανονικά p_i-γωνα i=1,…,k είναι κατασκευάσιμα, όπου $p_1, ..., p_k$ είναι περιττοί πρώτοι της μορφής $2^{2^v} + 1$, για μη αρνητικούς ακέραιους ν.

Για να δείξουμε την κατασκευασιμότητα των κανονικών p_i-γώνων αρκεί να δείξουμε ότι το $\cos\frac{2\pi}{p_i}$ είναι κατασκευάσιμο.

Το κυκλοτομικό πολυώνυμο $f(x) = x^{p_i-1} + x^{p_i-2} + \ldots + x + 1$ είναι ανάγωγο επί του $\mathbb{Q}$ και έχει ρίζα την p_i-οστή πρωταρχική ρίζα της μονάδας στο $\mathbb{C}$, $z = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$,

άρα $[\mathbb{Q}(z):\mathbb{Q}] = p_i - 1 = 2^{2^n} + 1 - 1 = 2^{2^n} := 2^{\alpha}$.

Θέλουμε να αποδείξουμε ότι το $\cos\frac{2\pi}{p} = \frac{1}{2}(z+z)^{-1} \in \mathbb{Q}(z) \cap \mathbb{R}$ είναι κατασκευάσιμο. Θα χρησιμοποιήσουμε την Πρόταση 7.12

Έστω K = $\mathbb{R} \cap \mathbb{Q}(z)$.

- Είναι: $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(z)$
- Είναι $[\mathbb{Q}(z):K] = 2$, αφού το ελάχιστο πολυώνυμο του z στο K είναι το

  $(x-z)(x-z^{-1}) = x^2 - (z+z^{-1})x + zz^{-1} = x^2 - 2\cos(\frac{2\pi}{p_i})x + 1 \in K[x]$.
- Είναι $[\mathbb{Q}(z):\mathbb{Q}] = [\mathbb{Q}(z):K][K:\mathbb{Q}] \Rightarrow 2^{\alpha} = 2[K:\mathbb{Q}]$ άρα $[K:\mathbb{Q}] = 2^{\alpha-1}$

Το $\mathbb{Q}(z)$ είναι το σώμα ριζών του πολυωνύμου $f(x)$ στο $\mathbb{Q}$,
άρα $\mathbb{Q}(z)/\mathbb{Q}$ κανονική και διαχωρίσιμη (αφού το $\mathbb{Q}$ έχει χαρακτηριστική 0),
άρα $\mathbb{Q}(z)/\mathbb{Q}$ επέκταση Galois.
Από το Λήμμα 8.6 η $Gal(\mathbb{Q}(z)/\mathbb{Q})$ είναι αβελιανή.

Τότε $Gal(\mathbb{Q}(z)/K) \triangleleft Gal(\mathbb{Q}(z)/\mathbb{Q})$, αφού κάθε υποομάδα αβελιανής ομάδας είναι κανονική. Επομένως από το Θεμελιώδες Θεώρημα της Θεωρίας Galois έχουμε ότι η επέκταση $K/\mathbb{Q}$ είναι Galois, άρα κανονική.

Αφού λοιπόν η $K/\mathbb{Q}$ είναι κανονική επέκταση βαθμού δύναμη του 2, από την Πρόταση 7.12 έχουμε ότι κάθε στοιχείο του *K* είναι κατασκευάσιμο.

Επομένως το $\cos\frac{2\pi}{p_i}$ είναι κατασκευάσιμο.

Σημείωση. Οι πρώτοι της μορφής $F_\nu = 2^{2^\nu} + 1$ ονομάζονται πρώτοι του Fermat. Ο Fermat διατύπωσε τον ισχυρισμό ότι όλοι οι αριθμοί της μορφής αυτής είναι πρώτοι. Όμως ο Euler έδειξε ότι ο 641 διαιρεί τον $F_5 = 2^{2^5} + 1$, και έτσι ο ισχυρισμός αυτός κατερίφθηκε.

Μέχρι σήμερα δεν έχει βρεθεί άλλος πρώτος του Fermat μετά τον F_4. Δηλαδή οι $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ και $F_4 = 65537$ είναι οι μόνοι γνωστοί πρώτοι του Fermat. Με τη βοήθεια υπολογιστή έχει αποδειχθεί ότι αν υπάρχει άλλος αυτός θα πρέπει να είναι μεγαλύτερος από 10^{40000}.

Είδαμε ότι αν το κανονικό m-γωνο και το κανονικό n-γωνο είναι κατασκευάσιμα και (m,n) = 1, τότε και το κανονικό mn-γωνο είναι κατασκευάσιμο. Επομένως σύμφωνα και με το Θεώρημα Gauss για να κατασκευαστεί ένα κανονικό n-γωνο, αρκεί να κατασκευάσουμε κανονικά πολύγωνα με 2^r πλευρές ή με p πλευρές, όπου p πρώτος της μορφής $F_\nu = 2^{2^\nu} + 1$. Ένα κανονικό 2^r-γωνο κατασκευάζεται εύκολα με διαδοχικές διχοτομήσεις του κύκλου. Επομένως το πρόβλημα της κατασκευασιμότητας των κανονικών n-γώνων ανάγεται στο πρόβλημα της κατασκευής των κανονικών p-γώνων, όπου p πρώτος του Fermat.

Τώρα, η κατασκευή του ισόπλευρου τριγώνου και του κανονικού πενταγώνου είναι γνωστή από την Ευκλείδεια Γεωμετρία και ήταν επίσης γνωστή και στους αρχαίους Έλληνες.Ο Ευκλείδης κατασκεύασε με κανόνα και διαβήτη το ισόπλευρο τρίγωνο καθώς και το κανονικό πεντάγωνο. (Στοιχεία, 300 π.Χ., Προτάσεις IV. 11,15).

Το κανονικό 17-γωνο κατασκευάστηκε από τον Gauss (έδωσε το μήκος $\cos\frac{2\pi}{17}$ σε κατασκευάσιμη έκφραση) και ακολούθησε μια γεωμετρική απόδειξη από τον Johannes Erchinger.

Το 1832 ο R. J. Richelot σε μια σειρά δημοσιεύσεων έδωσε την κατασκευή ενός κανονικού 257-γωνου και ο J. Hermes το 1894 δουλεύοντας για δέκα χρόνια κατασκευάζει, σε μία εργασία 200 σελίδων, το κανονικό 65537-γωνο (Τσακνάκης, 2007).

ΚΕΦΑΛΑΙΟ 9

Η ΚΑΤΑΣΚΕΥΗ ΤΟΥ ΚΑΝΟΝΙΚΟΥ ΠΕΝΤΑΓΩΝΟΥ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

Α) Η κατασκευή του κανονικού πενταγώνου κατά τον Ευκλείδη

Είδαμε ότι το πρόβλημα κατασκευής κανονικού n-γώνου με κανόνα και διαβήτη ανάγεται στο πρόβλημα κατασκευής κανονικού p-γώνου, όπου p πρώτος του Fermat. Οι πρώτες κατασκευές τέτοιων p-γώνων έγιναν περίπου 2000 χρόνια πριν από τον Gauss, από τους αρχαίους Έλληνες. Αυτές ήταν οι κατασκευές του ισοπλεύρου τριγώνου και του κανονικού πενταγώνου (Στοιχεία του Ευκλείδη, βιβλίο IV, 300 π.Χ.).Στα παρακάτω παρουσιάζεται η κατασκευή του κανονικού πενταγώνου από τον Ευκλείδη.

Πρόταση 9.1. (Διαίρεση ευθυγράμμου τμήματος σε μέσο και άκρο λόγο)

Να διαιρεθεί δοσμένο ευθύγραμμο τμήμα ώστε το ορθογώνιο που ορίζει το τμήμα και το ένα μέρος του, να είναι ισοδύναμο με το τετράγωνο που έχει πλευρά το άλλο μέρος.

[Τὴν δοθεῖσαν εὐθεῖαν τεμεῖν ὥστε τὸ ὑπὸ τῆς ὅλης καὶ

τοῦ ἑτέρου τῶν τμημάτων περιεχόμενον ὀρθογώνιον ἴσον

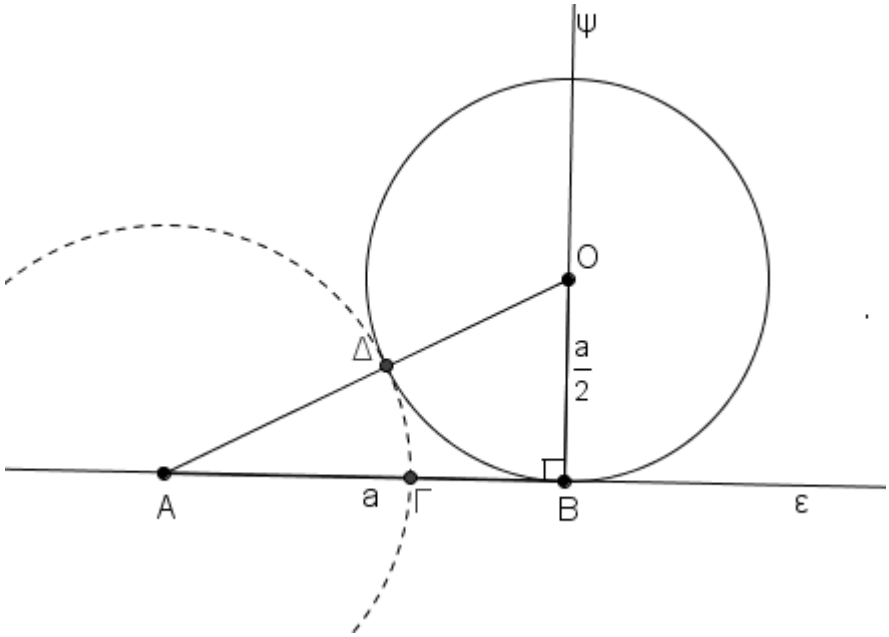
εἶναι τῷ ἀπὸ τοῦ λοιποῦ τμήματος τετραγώνῳ.] ***(Στοιχεία, Πρόταση II.11)***

Απόδειξη: Έστω ΑΒ το δοσμένο ευθύγραμμο τμήμα μήκους a.

Αναζητούμε σημείο Γ τέτοιο ώστε ΑΒ·ΒΓ=ΑΓ^2.

Αν x είναι το μήκος του ΑΓ, θα πρέπει να ισχύει η σχέση:

$$x^2 = (a - x)\cdot a \quad \text{ή} \quad x^2 = a^2 - a\cdot x \quad \text{ή} \quad x^2 + a\cdot x - a^2 = 0 \qquad (1)$$



Σε μία ευθεία ε παίρνουμε ευθύγραμμο τμήμα ΑΒ= a.

Φέρουμε ημιευθεία Βψ κάθετη στην ε και σε αυτήν σημείο Ο ώστε $OB = \frac{a}{2}$

Γράφουμε το ευθύγραμμο τμήμα ΟΑ και κατασκευάζουμε τον κύκλο (O, OB) ο οποίος τέμνει το τμήμα ΟΑ στο σημείο Δ.

Από το Πυθαγόρειο Θεώρημα έχουμε:

$$(A\Delta + \frac{a}{2})^2 = a^2 + \frac{a^2}{4}$$

$$A\Delta^2 + \frac{a^2}{4} + a \cdot A\Delta = a^2 + \frac{a^2}{4}$$

$$A\Delta^2 + a \cdot A\Delta = a^2$$

Κατασκευάζουμε τον κύκλο $(A, A\Delta)$ ο οποίος τέμνει το τμήμα ΑΒ στο σημείο Γ που είναι το ζητούμενο σημείο.

Παρατηρήσεις:

1. Ο Ευκλείδης δίνει μια άλλη απόδειξη, αλλά χρησιμοποιεί τα ίδια μέσα.

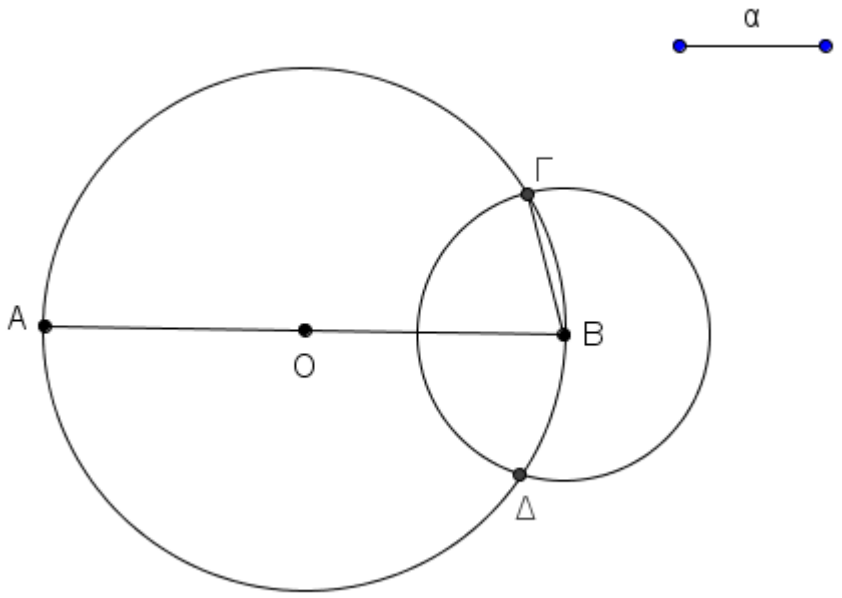
2. Στην Πρόταση ΙΙ.11 των Στοιχείων ο Ευκλείδης δεν δίνει όνομα στην παραπάνω κατασκευή. Όμως στην Πρόταση VI.30 επαναλαμβάνεται η κατασκευή αυτή και καλείται διαίρεση ευθυγράμμου τμήματος σε μέσο και άκρο λόγο.

Πρόταση 9.2.: Αν δοθούν κύκλος και ευθύγραμμο τμήμα μικρότερο ή ίσο από τη διάμετρο του κύκλου, να κατασκευαστεί χορδή του κύκλου ίση προς το δοθέν ευθύγραμμο τμήμα.

[Εἰς τὸν δοθέντα κύκλον τῇ δοθείσῃ εὐθείᾳ μὴ μείζονι

οὔσῃ τῆς τοῦ κύκλου διαμέτρου ἴσην εὐθεῖαν ἐναρμόσαι.] ***(Στοιχεία, IV. 1)***

Απόδειξη: Έστω κύκλος (Ο,ρ) και ευθύγραμμο τμήμα μήκους α μικρότερο ή ίσο με τη διάμετρο του κύκλου.



Φέρνουμε μια διάμετρο του κύκλου, έστω την ΑΒ.

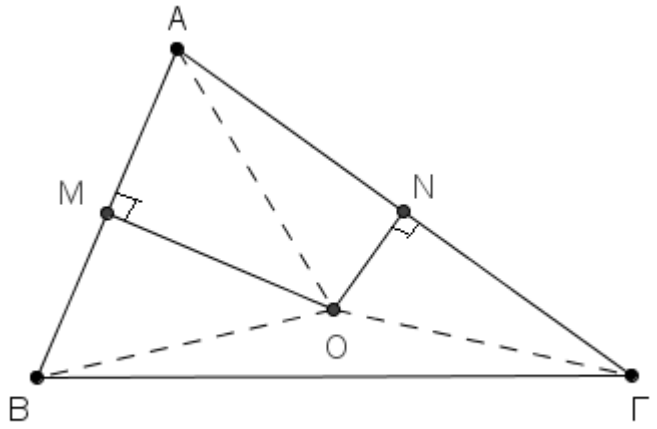
•Αν το α είναι ίσο με τη διάμετρο τελειώσαμε.

•Αν το α είναι μικρότερο από τη διάμετρο, φέρνουμε κύκλο κέντρου Β και ακτίνας α ο οποίος τέμνει τον κύκλο (Ο,ρ) στα Γ και Δ.

Τότε η ΒΓ= α είναι η ζητούμενη χορδή.

Πρόταση 9.3.: Σε δοσμένο τρίγωνο να περιγραφεί κύκλος.

[Περὶ τὸ δοθὲν τρίγωνον κύκλον περιγράψαι.] ***(Στοιχεία, Πρόταση IV.5)***



<u>Απόδειξη:</u> Δίνεται τρίγωνο ΑΒΓ και θέλουμε να φέρουμε τον περιγεγραμμένο κύκλο του, δηλαδή να κατασκευάσουμε κύκλο που να διέρχεται από τις κορυφές του.

Κατασκευάζουμε τις μεσοκαθέτους ε, ζ των πλευρών ΑΒ και ΑΓ αντίστοιχα, οι οποίες τέμνονται εντός του τριγώνου ή σε σημείο της ΒΓ ή εκτός του τριγώνου.

Έστω Μ και Ν τα μέσα των ΑΒ και ΑΓ αντίστοιχα.

• <u>Οι ε, ζ τέμνονται σε σημείο Ο εσωτερικό του τριγώνου.</u>

Φέρνουμε τα ευθύγραμμα τμήματα ΟΑ,ΟΒ και ΟΓ.

Τα ορθογώνια τρίγωνα ΜΑΟ και ΜΒΟ έχουν $AM = MB = \frac{AB}{2}$ και ΟΜ κοινή,

άρα είναι ίσα, επομένως ΟΑ=ΟΒ.

Ομοίως αποδεικνύεται ότι ΟΑ=ΟΓ. Άρα ΟΑ=ΟΒ=ΟΓ.

Κατασκευάζουμε τον κύκλο (Ο, ΟΑ) ο οποίος διέρχεται από τις κορυφές Α, Β, Γ και είναι ο περιγεγραμμένος κύκλος του τριγώνου ΑΒΓ.

•<u>Όμοια εργαζόμαστε και στις άλλες περιπτώσεις</u>.

Πρόταση 9.4.: Να κατασκευαστεί ισοσκελές τρίγωνο, του οποίου η γωνία της βάσης να είναι διπλάσια από τη γωνία της κορυφής του.

[Ἰσοσκελὲς τρίγωνον συστήσασθαι ἔχον ἑκατέραν τῶν πρὸς τῇ βάσει γωνιῶν διπλασίονα τῆς λοιπῆς.] ***(Στοιχεία, Πρόταση IV.10)***

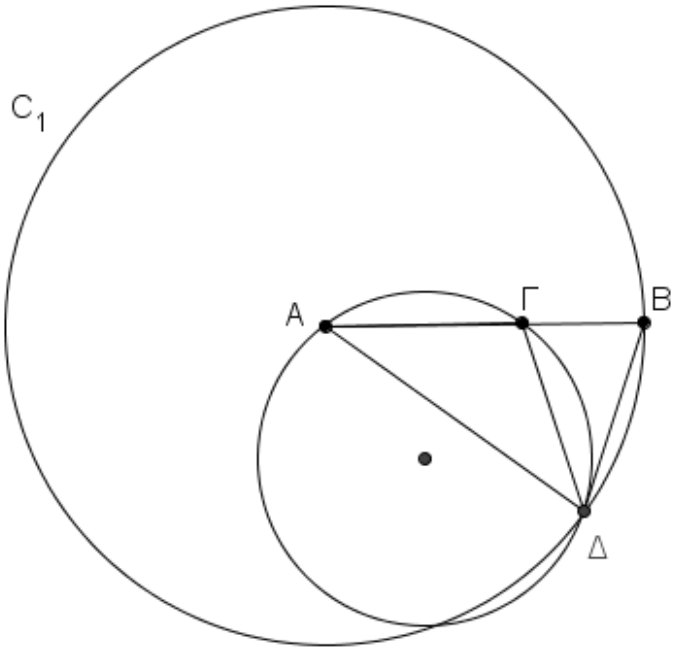
Απόδειξη: Παίρνουμε ευθύγραμμο τμήμα ΑΒ και σημείο του Γ, τέτοιο ώστε $ΑΒ·ΒΓ=ΑΓ^2$ (Πρόταση 9.1.).

Με κέντρο το Α και ακτίνα ΑΒ γράφουμε κύκλο C_1 και κατασκευάζουμε χορδή του ΒΔ=ΑΓ, η οποία δεν είναι μεγαλύτερη από τη διάμετρο του κύκλου (Πρόταση 9.2.).

Φέρνουμε τα ΑΔ, ΓΔ και τον περιγεγραμμένο κύκλο C_2 του τριγώνου ΑΓΔ (Πρόταση 9.3.).

Επειδή $ΑΒ·ΒΓ=ΑΓ^2$ και ΒΔ=ΑΓ άρα $ΑΒ·ΒΓ=ΒΔ^2$.

Από το σημείο Β, που βρίσκεται εκτός του κύκλου C_2, διέρχονται δυο ευθείες, εκ των οποίων η μία τέμνει τον C_2 στα σημεία Α και Γ και η άλλη έχει κοινό σημείο με τον C_2 το Δ και επειδή $ΑΒ·ΒΓ=ΒΔ^2$,άρα η ΒΔ θα εφάπτεται στον C_2 στο σημείο Δ.



Είναι: $B\hat{\Delta}A = B\hat{\Delta}\Gamma + \Gamma\hat{\Delta}A$

άρα $B\hat{\Delta}A = \Gamma\hat{A}\Delta + \Gamma\hat{\Delta}A$ ($B\hat{\Delta}\Gamma = \Gamma\hat{A}\Delta$ ως γωνία χορδής και εφαπτομένης),

οπότε $B\hat{\Delta}A = B\hat{\Gamma}\Delta$ ($B\hat{\Gamma}\Delta = \Gamma\hat{A}\Delta + \Gamma\hat{\Delta}A$ αφού η $B\hat{\Gamma}\Delta$ εξωτερική του $A\Gamma\Delta$).

Επίσης $B\hat{\Delta}A = \Delta\hat{B}A$,γιατί το τρίγ. ΑΒΔ είναι ισοσκελές (ΑΒ=ΑΔ ακτίνες C_1).

Άρα $\underline{B\hat{\Delta}A = B\hat{\Gamma}\Delta = \Delta\hat{B}A}$.

Επειδή $B\hat{\Gamma}\Delta = \Delta\hat{B}A$ το τρίγ. ΔΒΓ είναι ισοσκελές οπότε

$\Delta B = \Delta\Gamma \xleftrightarrow{\Delta B=A\Gamma} A\Gamma = \Delta\Gamma$ Επειδή $A\Gamma = \Delta\Gamma$ άρα το τρίγ. ΓΑΔ είναι ισοσκελές

οπότε $\Gamma\hat{A}\Delta = \Gamma\hat{\Delta}A$.

Επειδή $B\hat{\Gamma}\Delta = \Gamma\hat{A}\Delta + \Gamma\hat{\Delta}A$ ($B\hat{\Gamma}\Delta$ εξωτερική του τριγ. ΑΓΔ) και

$B\hat{\Delta}A = B\hat{\Gamma}\Delta = \Delta\hat{B}A$ άρα $B\hat{\Delta}A = \Delta\hat{B}A = 2\cdot\Gamma\hat{A}\Delta$.

Επομένως το τρίγ. ΑΒΔ είναι το ζητούμενο τρίγωνο.

Παρατήρηση: Προφανώς το τρίγωνο που κατασκευάστηκε με την παραπάνω Πρόταση έχει γωνίες 36°,72°,72°.

Πρόταση 9.5.: Σε δοθέντα κύκλο να εγγραφεί πεντάγωνο ισόπλευρο και ισογώνιο.

[Εἰς τὸν δοθέντα κύκλον πεντάγωνον ἰσόπλευρόν τε

καὶ ἰσογώνιον ἐγγράψαι.] ***(Στοιχεία, Πρόταση IV.11)***

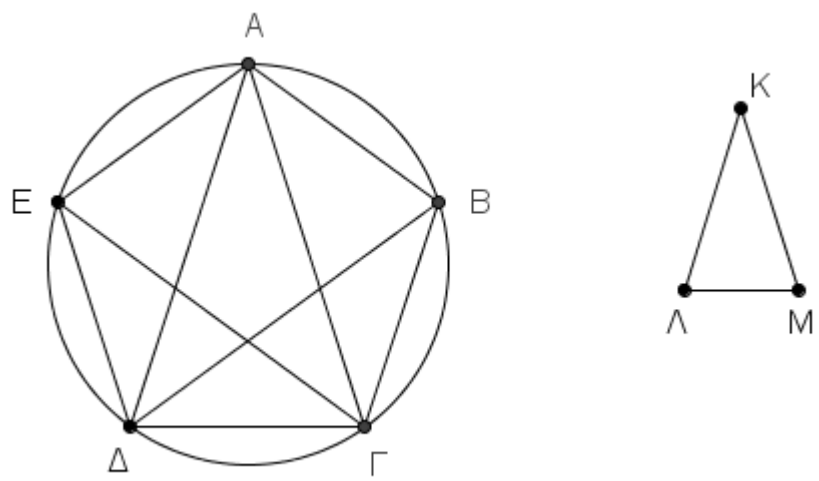
Απόδειξη: Έστω ότι δίνεται κύκλος κέντρου Ο και ακτίνας ρ και θέλουμε να εγγράψουμε πεντάγωνο ισόπλευρο και ισογώνιο.

Κατασκευάζουμε ισοσκελές τρίγωνο ΚΛΜ με $\hat{\Lambda} = \hat{\text{Μ}} = 2 \cdot \hat{\text{Κ}}$. (Πρότ. 1.3).
Εγγράφουμε στον κύκλο (Ο,ρ) τρίγωνο ΑΔΓ όμοιο με το ΚΛΜ, τέτοιο ώστε $\text{Γ}\hat{\text{Α}}\text{Δ} = \hat{\text{Κ}}$ και $\text{Α}\hat{\text{Γ}}\text{Δ} = \hat{\text{Μ}} = \hat{\Lambda} = \text{Α}\hat{\text{Δ}}\text{Γ}$. Προφανώς είναι: $\text{Α}\hat{\text{Γ}}\text{Δ} = \text{Γ}\hat{\text{Δ}}\text{Α} = 2 \cdot \text{Γ}\hat{\text{Α}}\text{Δ}$

Φέρνουμε τις διχοτόμους ΓΕ και ΔΒ των γωνιών $\text{Α}\hat{\text{Γ}}\text{Δ}$ και $\text{Γ}\hat{\text{Δ}}\text{Α}$ αντίστοιχα και τα ευθύγραμμα τμήματα ΑΒ, ΒΓ, ΓΔ, ΔΕ και ΕΑ.

Επειδή $\text{Α}\hat{\text{Γ}}\text{Δ} = \text{Γ}\hat{\text{Δ}}\text{Α} = 2 \cdot \text{Γ}\hat{\text{Α}}\text{Δ}$ και οι *ΓΕ, ΔΒ* είναι οι διχοτόμοι των $\text{Α}\hat{\text{Γ}}\text{Δ}$ και $\text{Γ}\hat{\text{Δ}}\text{Α}$ αντίστοιχα, θα έχουμε $\text{Α}\hat{\text{Δ}}\text{Β} = \text{Β}\hat{\text{Δ}}\text{Γ} = \text{Γ}\hat{\text{Α}}\text{Δ} = \text{Ε}\hat{\text{Γ}}\text{Δ} = \text{Α}\hat{\text{Γ}}\text{Ε}$.
Άρα τα αντίστοιχα τόξα $\overset{\frown}{\text{ΑΒ}}, \overset{\frown}{\text{ΒΓ}}, \overset{\frown}{\text{ΓΔ}}, \overset{\frown}{\text{ΔΕ}}, \overset{\frown}{\text{ΕΑ}}$ θα είναι ίσα, συνεπώς και οι αντίστοιχες πλευρές, δηλαδή $\text{ΑΒ} = \text{ΒΓ} = \text{ΓΔ} = \text{ΔΕ} = \text{ΕΑ}$. Επομένως το πεντάγωνο είναι ισόπλευρο.

Επειδή $\overset{\frown}{\text{ΑΒ}} = \overset{\frown}{\text{ΔΕ}}$ άρα $\overset{\frown}{\text{ΑΒ}} + \overset{\frown}{\text{ΒΓΔ}} = \overset{\frown}{\text{ΔΕ}} + \overset{\frown}{\text{ΒΓΔ}}$ οπότε $\overset{\frown}{\text{ΑΒΓΔ}} = \overset{\frown}{\text{ΕΔΓΒ}}$.
Επομένως και οι εγγεγραμμένες γωνίες $\text{Α}\hat{\text{Ε}}\text{Δ}$ και $\text{Β}\hat{\text{Α}}\text{Ε}$ που βαίνουν στα τόξα αυτά είναι ίσες. Όμοια αποδεικνύουμε ότι $\text{Β}\hat{\text{Α}}\text{Ε} = \text{Α}\hat{\text{Β}}\text{Γ} = \text{Β}\hat{\text{Γ}}\text{Δ} = \text{Γ}\hat{\text{Δ}}\text{Ε} = \text{Α}\hat{\text{Ε}}\text{Δ}$.
Επομένως το πεντάγωνο είναι και ισογώνιο.



Β) Η κατασκευή του κανονικού πενταγώνου στο σχολικό βιβλίο

Πρόταση 9.7. (Διαίρεση ευθυγράμμου τμήματος σε μέσο και άκρο λόγο)

Να διαιρεθεί δοσμένο ευθύγραμμο τμήμα σε δύο άνισα τμήματα ώστε το μεγαλύτερο ευθύγραμμο τμήμα να είναι μέσο ανάλογο του μικρότερου και του αρχικού ευθύγραμμου τμήματος. ***(Πρόβλημα της «χρυσής τομής»)***

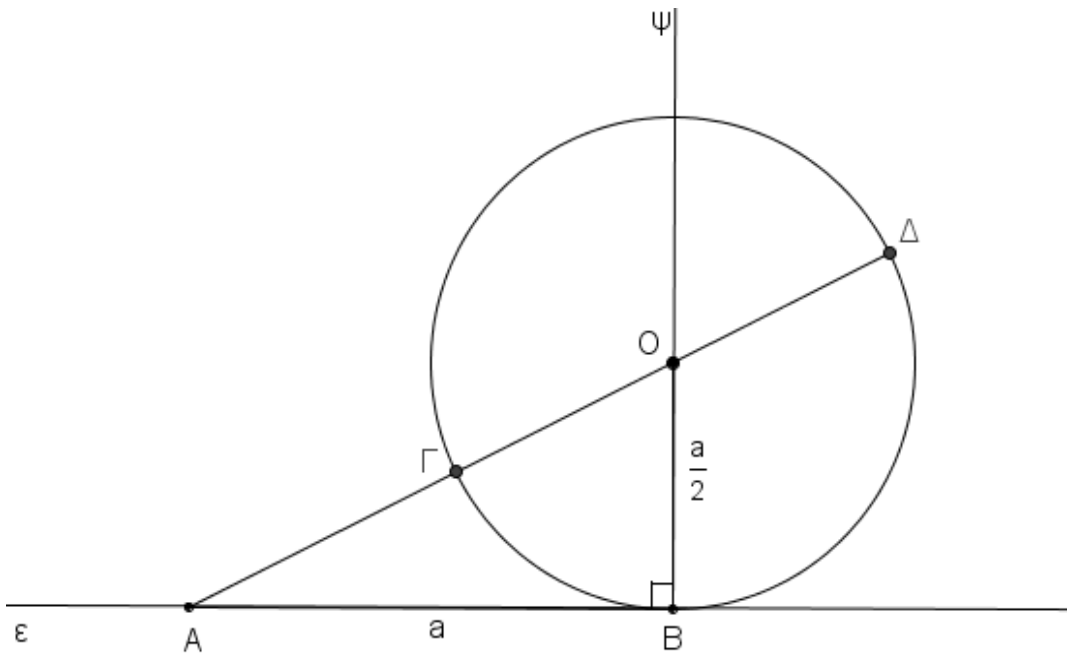
Απόδειξη: Έστω ΑΒ το δοσμένο ευθύγραμμο τμήμα μήκους a. Αν x είναι το μήκος του μεγαλύτερου τμήματος, θα πρέπει να ισχύει η σχέση:

$$\frac{x}{a}=\frac{a-x}{x} \quad \text{ή} \quad x^2=(a-x)\cdot a \quad \text{ή} \quad x^2=a^2-a\cdot x \quad \text{ή} \quad x^2+a\cdot x-a^2=0 \qquad (1)$$

Σε μία ευθεία ε παίρνουμε ευθύγραμμο τμήμα ΑΒ= a.

Φέρουμε ημιευθεία Βψ κάθετη στην ε, και σε αυτήν σημείο Ο ώστε $BO=\frac{a}{2}$

Κατασκευάζουμε τον κύκλο (O,OB) ο οποίος είναι εφαπτόμενος στην ευθεία ε. Φέρουμε την ευθεία η οποία διέρχεται από τα σημεία Α και Ο, και έστω Γ και Δ τα σημεία στα οποία τέμνει τον κύκλο.



Από το θεώρημα χορδής και εφαπτομένης έχουμε:

$$AB^2 = A\Gamma \cdot A\Delta \qquad \text{ή}$$

$$a^2 = A\Gamma \cdot (A\Gamma + a) \qquad \text{ή}$$

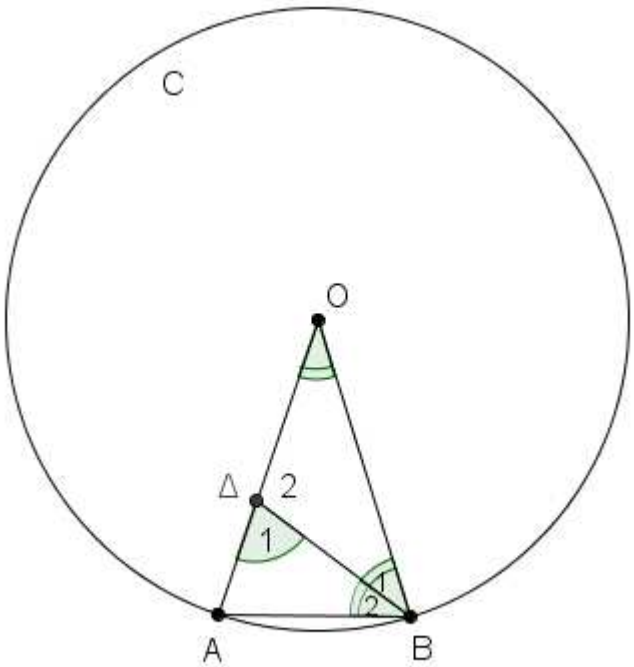
$$a^2 = A\Gamma^2 + a \cdot A\Gamma \qquad \text{ή}$$

$$A\Gamma^2 + a \cdot A\Gamma - a^2 = 0$$

Άρα το μήκος του ευθυγράμμου τμήματος ΑΓ είναι η θετική ρίζα της εξίσωσης (1).

Πρόταση 9.8.: Σε δοθέντα κύκλο να εγγραφεί κανονικό πεντάγωνο.

Κατασκευή: Έστω AB=λ_{10} η πλευρά του κανονικού δεκαγώνου που θέλουμε να εγγράψουμε στον κύκλο (O,R). Είναι $\omega_{10} = \frac{360^\circ}{10} = 36^\circ$ και καθεμιά από τις γωνίες της βάσης του ισοσκελούς τριγώνου OAB είναι $\hat{A} = \hat{B} = 72^\circ$.



Φέρνουμε τη διχοτόμο ΒΔ του τριγώνου ΟΑΒ.

Τα τρίγωνα ΔΟΒ και ΒΑΔ είναι ισοσκελή, γιατί:

$\hat{B}_1 = 36^o = \hat{O}$ και $\hat{\Delta}_1 = \hat{B}_1 + \hat{O} = 72^o = \hat{A}$. Άρα ΟΔ=ΒΔ=ΑΒ= λ_{10} και ΑΔ= R- λ_{10}.

Εφαρμόζουμε το Θεώρημα εσωτερικής διχοτόμου στο τρίγωνο ΟΑΒ και έχουμε:

$$\frac{AB}{OB} = \frac{\Delta A}{\Delta O} \Leftrightarrow \frac{\lambda_{10}}{R} = \frac{R - \lambda_{10}}{\lambda_{10}} \Leftrightarrow \lambda_{10}^2 = R(R - \lambda_{10})$$

και επειδή λ_{10}=ΑΒ>ΔΑ= R- λ_{10} (αφού $\hat{\Delta}_1 > \hat{B}_2$) η τελευταία ισότητα εκφράζει ότι το λ_{10} είναι το μεγαλύτερο από τα τμήματα που προκύπτουν αν διαιρέσουμε την ακτίνα R σε μέσο και άκρο λόγο.

Για την κατασκευή του κανονικού πενταγώνου που είναι εγγεγραμμένο σε κύκλο (Ο,R) διαιρούμε την ακτίνα του κύκλου σε μέσο και άκρο λόγο και στη συνέχεια ορίζουμε τα διαδοχικά τόξα ΑΒ, ΒΓ,… που έχουν το καθένα χορδή ίση με το μεγαλύτερο τμήμα στα οποία χωρίζεται η ακτίνα με τη διαίρεσή της σε μέσο και άκρο λόγο.

Έτσι χωρίζουμε τον κύκλο σε 10 ίσα τόξα και παίρνοντάς τα ανά δύο ο κύκλος χωρίζεται σε 5 ίσα τόξα. Φέρνοντας τις αντίστοιχες χορδές έχουμε εγγράψει στον κύκλο (Ο,R) κανονικό πεντάγωνο.

Γ) Μία διδακτική πρόταση κατασκευής του κανονικού δεκαγώνου με την αναλυτικο-συνθετική μέθοδο.

Το προτεινόμενο θέμα αφορά την κατασκευή με κανόνα και διαβήτη του κανονικού δεκαγώνου.

Πλαίσιο εφαρμογής:

Σε ποιους απευθύνεται:

Το σενάριο απευθύνεται στους μαθητές της Β΄ Λυκείου.

Χρόνος υλοποίησης :

Για την εφαρμογή του σεναρίου εκτιμάται ότι απαιτείται 1 διδακτική ώρα.

Προαπαιτούμενες γνώσεις:

Οι μαθητές πρέπει να έχουν ενημερωθεί από το διδάσκοντα για την αναλυτικο-συνθετική μέθοδο. Πρέπει να γνωρίζουν τα υποχρεωτικά βήματα (ανάλυση – σύνθεση – απόδειξη – διερεύνηση), που πρέπει να ακολουθηθούν κατά την εφαρμογή αυτής της μεθόδου. Επίσης πρέπει να την έχουν εφαρμόσει σε προβλήματα γεωμετρικών κατασκευών με κανόνα και διαβήτη.

Ένα από τα προβλήματα που οι μαθητές πρέπει να έχουν εφαρμόσει την αναλυτικο-συνθετική θέθοδο είναι το πρόβλημα της «χρυσής τομής».
Οι μαθητές πρέπει να μπορούν, με κανόνα και διαβήτη, να διαιρούν ένα ευθύγραμμο τμήμα σε δύο άνισα τμήματα ώστε το μεγαλύτερο ευθύγραμμο τμήμα να είναι μέσο ανάλογο του μικρότερου και του αρχικού ευθύγραμμου τμήματος.

Απαιτούμενα βοηθητικά εργαλεία:

Κάθε ομάδα είναι απαραίτητο να διαθέτει ένα φύλλο εργασίας μέσα στο οποίο ο διδάσκων θα έχει θέσει συγκεκριμένα ερωτήματα και οδηγίες. Επιπλέον καλό θα είναι οι μαθητές να διαθέτουν ένα τετράδιο σημειώσεων.

Κοινωνική ενορχήστρωση της τάξης.

Οι μαθητές εργαζόμενοι σε ομάδες των δύο μαθητών (ανά θρανίο) και καθοδηγούμενοι από το φύλλο εργασίας, καλούνται να εξερευνήσουν συγκεκριμένα σχήματα και να απαντήσουν σε συγκεκριμένες ερωτήσεις. Επομένως η διερεύνηση αυτή θα γίνει συνεργατικά. Για να υπάρχει κοινός στόχος και καλή συνεργασία οι μαθητές καλούνται να συμπληρώσουν ένα κοινό φύλλο εργασίας που περιέχει ερωτήσεις σχετικές με το θέμα. Φυσικά το φύλλο εργασίας αυτό θα πρέπει να αφήνει μια αρκετά μεγάλη ελευθερία στους μαθητές ώστε να θέτουν τα δικά τους ερωτήματα και να απαντούν σ' αυτά.

Στη διάρκεια της υλοποίησης του σεναρίου ο εκπαιδευτικός θα πρέπει να ελέγχει τα συμπεράσματα των μαθητών, να συνεργάζεται μαζί τους, να τους καθοδηγεί ώστε να αντιλαμβάνονται καλύτερα τα αποτελέσματά τους και να τους ενθαρρύνει να συνεχίσουν την διερεύνηση.

Οι στόχοι του σεναρίου

Γνωστικοί στόχοι:

- Οι μαθητές να κατασκευάσουν την πλευρά του κανονικού δεκαγώνου με κανόνα και διαβήτη.
- Οι μαθητές να κατασκευάσουν κανονικό δεκάγωνο εγγεγραμμένο σε δοσμένο κύκλο.
- Οι μαθητές να ανακαλύψουν ότι είναι πάντα δυνατή η κατασκευή κανονικού δεκαγώνου με κανόνα και διαβήτη.

Ανάλυση του σεναρίου:

Η πορεία υλοποίησης του σεναρίου περιγράφεται μέσα από το επόμενο φύλλο εργασίας που δίνεται στους μαθητές.

Ενδεικτικό φύλλο εργασίας:

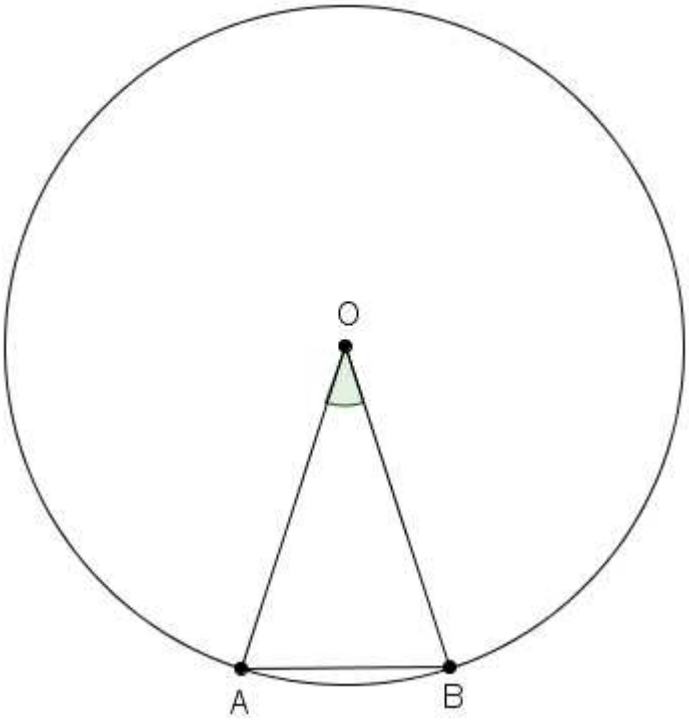
ΕΓΓΡΑΦΗ ΚΑΝΟΝΙΚΟΥ ΔΕΚΑΓΩΝΟΥ ΣΕ ΔΟΣΜΕΝΟ ΚΥΚΛΟ (Ο,R).

Ονοματεπώνυμα μαθητών:

1. ……
2. ……

ΦΥΛΛΟ ΕΡΓΑΣΙΑΣ

Α) ΑΝΑΛΥΣΗ



1. Έστω ότι ΑΒ=λ_{10} η πλευρά του κανονικού δεκαγώνου.
   Υπολογίστε την κεντρική του γωνία ω_{10}.

   ……

   ……

2. Να φέρετε τη διχοτόμο ΒΔ του τριγώνου ΑΟΒ, και να υπολογίσετε τα μέτρα όλων των γωνιών των τριγώνων ΔΟΒ και ΒΔΑ του σχήματος.

.....

.....

.....

.....

3. Συγκρίνετε τα τρίγωνα ΟΑΒ και ΒΔΑ και βρείτε τη σχέση που συνδέει το τετράγωνο της πλευράς ΑΒ με την ακτίνα R του κύκλου.

.....

.....

.....

.....

.....

.....

4. Παρατηρήστε προσεκτικά τη σχέση, στην οποία καταλήξατε και σκεφθείτε σε ποια γνωστή κατασκευή με κανόνα και διαβήτη σας οδηγεί.

.....

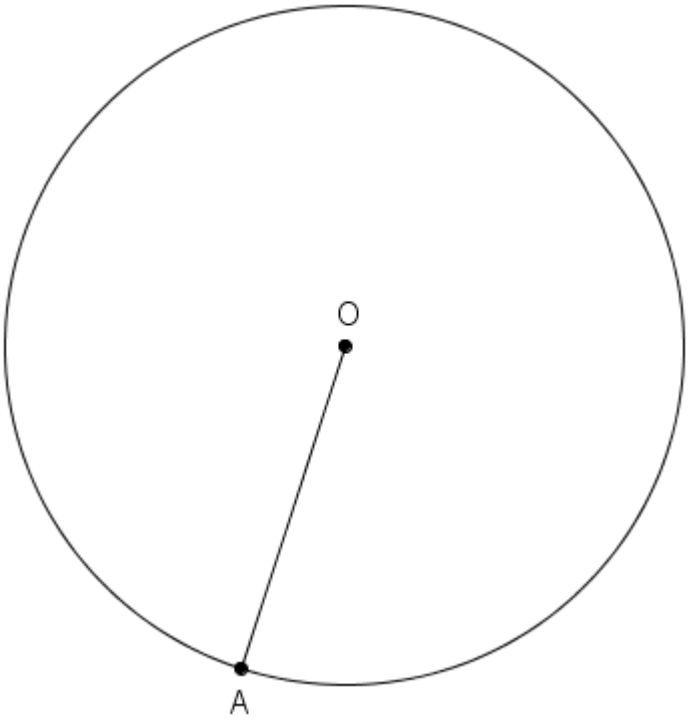
.....

.....

.....

.....

Β) **ΣΥΝΘΕΣΗ**



1. Εφαρμόστε τη γνωστή κατασκευή, που σκεφτήκατε στο προηγούμενο ερώτημα, στο ευθύγραμμο τμήμα ΟΑ.
   (Με την κατασκευή αυτή κατασκευάσατε την πλευρά του κανονικού δεκαγώνου).
   Περιγράψτε σύντομα τη διαδικασία αυτής της κατασκευής
   .....
   .....
   .....
   .....
   .....

2. Κατασκευάστε το κανονικό δεκάγωνο ξεκινώντας από το σημείο Α.

Γ) **ΑΠΟΔΕΙΞΗ**

Αν ΑΒ είναι μία πλευρά του κανονικού δεκαγώνου που κατασκευάσατε προηγουμένως, προσπαθήστε συγκρίνοντας τα τρίγωνα ΟΑΒ και ΒΔΑ να συμπεράνετε ότι $\hat{A} = 2A\hat{O}B$ και στη συνέχεια ότι $A\hat{O}B = 36^{o}$

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Δ) **ΔΙΕΡΕΥΝΗΣΗ**

Εξετάστε αν η κατασκευή της πλευράς του κανονικού δεκαγώνου, σύμφωνα με τα βήματα που ακολουθήσατε στο στάδιο της σύνθεσης, είναι πάντοτε δυνατή.

.....
.....
.....

ΒΙΒΛΙΟΓΡΑΦΙΑ

Δ.Βάρσος, Δ.Δεριζιώτης, Μ.Μαλιάκας, Σ.Παπασταυρίδης, Ε.Ράπτης, Ο.Ταλέλλη: Μια Εισαγωγή στην Άλγεβρα, Εκδόσεις «σοφία», 2003.

Ευάγγελος Ράπτης, Σημειώσεις μαθήματος Άλγεβρα για τη Διδακτική, ΠΜΣ Διδακτική & Μεθοδολογία των Μαθηματικών, 2007-08.

Εμμανουήλ Τσακνάκης: Gauss και Αριθμητική, Μεταπτυχιακή Εργασία, Τμήμα Μαθηματικών Πανεπιστημίου Κρήτης, 2007.

Ευκλείδη Στοιχεία, Τόμος 1, Κέντρο Έρευνας Επιστήμης και Εκπαίδευσης, Αθήνα 2001.

Η.Αργυρόπουλος, Π.Βλάμος, Γ.Κατσούλης, Σ.Μαρκάτης, Π.Σιδέρης: Ευκλείδεια Γεωμετρία, ΟΕΔΒ, Αθήνα.

Στυλιανός Ανδρεαδάκης: Θεωρία Galois, Εκδόσεις Συμμετρία, Αθήνα 1999.

B.L.Van Der Waerden: Η Αφύπνιση της Επιστήμης, Παναπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 2000.

Donald Davis: Η Φύση και η Δύναμη των Μαθηματικών, Παναπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 2005.

Joseph Rotman: Θεωρία Galois, Εκδόσεις Leader Books, Αθήνα 2000.

John Fraleigh: Εισαγωγή στην Άλγεβρα, Παναπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 2006.