

Κεφάλαιο 12

12.1 12^η Εβδομάδα

Κατασκευές με κανόνα και διαβήτη

- Ο όρος «κατασκευή» σημαίνει «γεωμετρική κατασκευή με αποκλειστική χρήση κανόνα και διαβήτη».
- Οι κατασκευές γίνονται πάνω στο επίπεδο xOy , άρα στους άξονες έχει ορισθεί το μοναδιαίο μήκος.
- Γίνεται διάκριση των όρων *ευθύγραμμο τμήμα* (γεωμετρικό αντικείμενο) από *μήκος ευθυγράμμου τμήματος* (πραγματικός αριθμός). Αν α συμβολίζει ένα ευθύγραμμο τμήμα, το $|\alpha|$ συμβολίζει το μήκος του.
- Κατασκευή πραγματικού αριθμού $x > 0$ σημαίνει κατασκευή ευθυγράμμου τμήματος α , ώστε $|\alpha| = x$ και μεταφορά, με τον διαβήτη, του α σε έναν από τους θετικούς ημιάξονες του επιπέδου με αρχή το 0. Κατασκευή πραγματικού αριθμού $x < 0$ σημαίνει κατασκευή ευθυγράμμου τμήματος α , ώστε $|\alpha| = -x$ και μεταφορά, με τον διαβήτη, του α σε έναν από τους αρνητικούς ημιάξονες του επιπέδου με αρχή το 0. Αν μπορεί να πραγματοποιηθεί η κατασκευή ενός πραγματικού αριθμού x , τότε ο x χαρακτηρίζεται *κατασκευάσιμος*.

Στοιχειώδεις γεωμετρικές κατασκευές

- *Δεδομένα:* Σημείο P και ευθεία ϵ που δεν περνά από το P .
Κατασκευή: Ευθεία που περνά από το P και είναι κάθετη στην ϵ .
- *Δεδομένα:* Ευθεία ϵ και σημείο της P .
Κατασκευή: Ευθεία κάθετη ϵ στο σημείο P .
- *Δεδομένα:* Σημείο P και ευθεία ϵ που δεν περνά από το P .
Κατασκευή: Ευθεία που περνά από το P και είναι παράλληλη στην ϵ .
- *Δεδομένα:* Δύο τεμνόμενες ημιευθείες.
Κατασκευή: Ευθεία που διχοτομεί τη γωνία που σχηματίζουν οι ημιευθείες αυτές.
- *Δεδομένο:* $m, n \in \mathbb{N}$.
Κατασκευή: Ευθύγραμμο τμήμα μήκους m/n .
- *Δεδομένα:* Ευθύγραμμο τμήματα α, β .
Κατασκευή: Το ευθύγραμμο τμήμα $\alpha + \beta$, δηλαδή, ευθύγραμμο τμήμα γ , ώστε $|\gamma| = |\alpha| + |\beta|$.
- *Δεδομένα:* Άνισα ευθύγραμμο τμήματα α, β .
Κατασκευή: Το ευθύγραμμο τμήμα $\alpha - \beta$. Αυτό σημαίνει το εξής: Αν $|\alpha| > |\beta|$, κατασκευή ευθυγράμμου τμήματος γ , ώστε $|\gamma| = |\alpha| - |\beta|$. Αν $|\alpha| < |\beta|$, κατασκευή ευθυγράμμου τμήματος

γ , ώστε $|\gamma| = |\beta| - |\alpha|$ και μεταφορά, με τον διαβήτη, του γ σε έναν από τους αρνητικούς ημιάξονες του επιπέδου

- *Δεδομένα:* Ευθύγραμμο τμήματα α, β .
Κατασκευή: Το ευθύγραμμο τμήμα $\alpha \cdot \beta$, δηλαδή, ευθύγραμμο τμήμα γ , ώστε $|\gamma| = |\alpha| \cdot |\beta|$.
- *Δεδομένα:* Ευθύγραμμο τμήματα α, β .
Κατασκευή: Το ευθύγραμμο τμήμα α/β , δηλαδή, ευθύγραμμο τμήμα γ , ώστε $|\gamma| = |\alpha|/|\beta|$.
- *Δεδομένα:* Ευθύγραμμο τμήμα α .
Κατασκευή: Το ευθύγραμμο τμήμα $\sqrt{\alpha}$, δηλαδή, ευθύγραμμο τμήμα β , ώστε $|\beta| = \sqrt{|\alpha|}$.
- *Δεδομένα:* Κατασκευάσιμοι μη μηδενικοί πραγματικοί αριθμοί a, b .
Κατασκευή: Λύση της $ax + b = 0$, δηλαδή, κατασκευή του πραγματικού αριθμού $-b/a$.
- *Δεδομένα:* Κατασκευάσιμοι πραγματικοί αριθμοί a, b, c με $a \neq 0$ και τουλάχιστον έναν από τους b, c μη μηδενικό.
Κατασκευή: Λύση της $ax^2 + bx + c = 0$, δηλαδή, κατασκευή των πραγματικών αριθμών που παρέχουν οι τύποι επίλυσης της δευτεροβάθμιας εξίσωσης.

Έστω σώμα $F \geq \mathbb{Q}$. Όταν λέω «σημείο του F » εννοώ σημείο στο επίπεδο xOy , του οποίου οι συντεταγμένες x, y ανήκουν στο F . Κατ' αναλογία, «ευθεία του F » είναι κάθε ευθεία που ορίζεται από δύο διαφορετικά σημεία του F και «κύκλος του F » είναι κάθε κύκλος με κέντρο σημείο του F και ακτίνα ίση με την απόσταση δύο σημείων του F .

Εύκολα φαίνεται ότι οι ευθείες του F ορίζονται από εξισώσεις της μορφής

$$ax + by + c = 0, \quad a, b, c \in F$$

και οι κύκλοι του F ορίζονται από εξισώσεις της μορφής

$$x^2 + y^2 + ax + by + c = 0, \quad a, b, c \in F.$$

Αν επιχειρήσω να κάνω μία κατασκευή με κανόνα και διαβήτη βασισμένος στα σημεία του σώματος F , τότε κάθε νέο σημείο που προκύπτει είναι σημείο, ή του F ή μιας δευτεροβάθμιας επέκτασης του F . Αυτό εξηγείται ως εξής: Κάθε σημείο κατά τη διαδικασία μιας τέτοιας κατασκευής προκύπτει από τομές ευθειών ή κύκλων, άρα οι συντεταγμένες του προκύπτουν από επίλυση συστημάτων ζεύγους εξισώσεων όπως οι παραπάνω. Συνεπώς, οι συντεταγμένες του είναι λύσεις συστήματος που έχει μια από τις παρακάτω μορφές (σε όλες τις εξισώσεις εννοείται ότι οι συντελεστές ανήκουν στο F):

$$\begin{cases} a_1x + b_1y + c_1 = 0 \\ a_2x + b_2y + c_2 = 0 \end{cases} \quad (12.1)$$

$$\begin{cases} a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases} \quad (12.2)$$

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases} \quad (12.3)$$

Το 1^ο σύστημα δίνει σημείο με συντεταγμένες στο F . Το 2^ο σύστημα δίνει σημείο με συντεταγμένες σε επέκταση του F βαθμού το πολύ 2. Το 3^ο σύστημα ανάγεται σε σύστημα της 2^{ης} μορφής, αν αντικαταστήσω τη μια από τις εξισώσεις του με εκείνη που προκύπτει από αφαίρεση των δύο εξισώσεων.

Σε μία κατασκευή πραγματικού αριθμού γίνονται πολλά τέτοια βήματα οπότε έχω αλυσίδα επεκτάσεων $\mathbb{Q} = F_0 \leq F_1 \leq \dots \leq F_n$ στην οποία $[F_i : F_{i-1}] = 1$ ή 2 για κάθε i και στο F_n βρίσκεται ο αριθμός που κατασκεύασα ως μία συντεταγμένη του τελικού σημείου κατασκευής. Συνεπώς, απέδειξα το εξής:

Θεώρημα 12.1. Αν ο $\alpha \in \mathbb{R}$ είναι κατασκευάσιμος, τότε υπάρχει πεπερασμένη επέκταση $F/\mathbb{Q}$ με $\alpha \in F$ και $[F:\mathbb{Q}] = 2^k$ για κάποιο $k \in \mathbb{N}_0$. Συνεπώς, ο βαθμός $[\mathbb{Q}(\alpha):\mathbb{Q}]$ ισούται με δύναμη του 2.

Παράδειγμα 12.2. Ο $\sqrt[3]{2}$ δεν κατασκευάζεται (με κανόνα και διαβήτη) (Δήλιον Πρόβλημα - Διπλασιασμός του Κύβου), καθώς αν υπάρχει τέτοιο σώμα F , τότε $3 = [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] \mid [F:\mathbb{Q}] = 2^k$, άτοπο!

Για μια αναλυτικότερη παρουσίαση των παραπάνω παραπέμπω στην ενότητα 1.3 των [Σημειώσεων του προπτυχιακού μαθήματος «Θεωρία Σωμάτων»](#).

Κατασκευή Κανονικού n -γώνου (γενικά)

Πρόταση 12.3. (1) Αν $n = 2^r m$, με τον m περιττό και $r \geq 0$, τότε το κανονικό n -γώνο κατασκευάζεται αν και μόνο αν το κανονικό m -γώνο κατασκευάζεται.

(2) Αν ο l είναι περιττός, όχι πρώτος και $l = mn$ με $m, n > 1$ και $\gcd(m, n) = 1$, τότε το κανονικό l -γώνο κατασκευάζεται αν και μόνο αν το κανονικό m -γώνο και το κανονικό n -γώνο κατασκευάζονται.

Απόδειξη. (1) Αν κατασκευάζεται το κανονικό m -γώνο, τότε, φέρνοντας τη μεσοκάθετο κάθε πλευράς αυτού και ενώνοντας τις κορυφές του με τα σημεία τομής των μεσοκαθέτων με τον περιγεγραμμένο στο m -γώνο κύκλο, τότε κατασκευάζω το $2m$ -γώνο. Επαναλαμβάνοντας τη διαδικασία στο νέο πολύγωνο κατασκευάζω το $4m$ -γώνο, κλπ, μέχρι να κατασκευάσω το $2^r m$ -γώνο.

Αντίστροφα, αν έχω κατασκευάσει το n -γώνο, ενώνω τις κορυφές του ανα 2^r . Το σχήμα που κατασκευάζω είναι κανονικό m -γώνο.

(2) Αν κατασκευάζεται το κανονικό l -γώνο, τότε, ενώνοντας τις κορυφές του ανα m (αντιστοίχως, ανά n) κατασκευάζω το κανονικό n -γώνο (αντιστοίχως, το κανονικό m -γώνο).

Αντίστροφα, έστω ότι κατασκευάζεται και το κανονικό m -γώνο και το κανονικό n -γώνο. Τα φαντάζομαι εγγεγραμμένα στον ίδιο κύκλο και έστω τ_m και τ_n τα τόξα που αντιστοιχούν σε μία πλευρά του m -γώνου και του n -γώνου αντιστοίχως. Τα μέτρα των τ_m και τ_n είναι, αντιστοίχως, $2\pi/m$ και $2\pi/n$.

Στον ίδιο κύκλο, το τόξο που αντιστοιχεί στο κανονικό mn -γώνο, έστω τ_{mn} , είναι αυτό που θέλω να κατασκευάσω. Το μέτρο του είναι $2\pi/(mn)$. Επειδή οι m, n είναι πρώτοι μεταξύ τους, από τη στοιχειώδη Θεωρία Αριθμών έχω ότι υπάρχουν θετικοί ακέραιοι a, b που επαληθεύουν τη σχέση $am - bn = 1$, άρα $a\frac{1}{n} - b\frac{1}{m} = \frac{1}{mn}$. Συνεπώς,

$$a\frac{2\pi}{n} - b\frac{2\pi}{m} = \frac{2\pi}{mn},$$

που σημαίνει ότι το τ_{mn} ισούται με a φορές το τ_n μείον b φορές το τ_m . Η κατασκευή τώρα του τ_{mn} είναι προφανής. $\square$

Παρατήρηση 12.4. Έστω $m = p_1^{k_1} \cdots p_l^{k_l}$ η κανονική ανάλυση του m σε πρώτους (τα $k_i \geq 1$ και τα p_i διαφορετικά ανά 2) Από το παραπάνω, το m -γώνο κατασκευάζεται αν και μόνο αν τα $p_i^{k_i}$ κατασκευάζονται. Άρα μένει να εξετάσω ποια q -γώνα με $q = p^k$, p περιττό πρώτο και $k \geq 1$ κατασκευάζονται. Έστω $\omega = \cos \theta + i \sin \theta \in \mathbb{C}$ (αρχική q -ρίζα της μονάδας). Το q -γώνο έχει κεντρική γωνία $\theta = \frac{2\pi}{q}$, συνεπώς το κανονικό q -γώνο κατασκευάζεται αν και μόνο αν το $\cos \theta$ κατασκευάζεται. Αλλά $2 \cos \theta = \omega + \omega^{-1}$, άρα $\omega^2 - (2 \cos \theta)\omega + 1 = 0$. Το πολώνυμο $X^2 - (2 \cos \theta)X + 1 \in \mathbb{Q}(\cos \theta)[X]$ είναι ανάγωγο γιατί έχει ρίζες του τα $\omega, \omega^{-1} \notin \mathbb{R}$, ενώ $\mathbb{Q}(\cos \theta) \subset \mathbb{R}$. Επομένως

$$\begin{array}{c} E_q = \mathbb{Q}(\omega) \\ \quad \mid_2 \\ K = \mathbb{Q}(\cos(\theta)) \\ \quad \mid \\ \mathbb{Q} \end{array}$$

Η $E_q/\mathbb{Q}$ είναι κυκλοτομική, οπότε $[E_q : \mathbb{Q}] = \phi(q)$. Άρα $[K : \mathbb{Q}] = \frac{1}{2}\phi(q) = \frac{1}{2}p^{k-1}(p-1)$ ή $p^{k-1}(p-1)$. Για να κατασκευάζεται ο $\cos \theta$ πρέπει (Θεώρημα 12.1) ο αριθμός $[K : \mathbb{Q}]$ να είναι δύναμη του 2. Αυτό συνεπάγεται ότι $k = 1$ και ο $(p-1)$ είναι δύναμη του 2, δηλαδή, $p = 2^r + 1$ για κάποιο $r \in \mathbb{N}$. Η τελευταία ισότητα, με τη σειρά της, συνεπάγεται ότι ο r είναι δύναμη του 2, διότι, αν $r = l\nu$ με τον $\nu > 1$ και περιττό, τότε, λόγω της ταυτότητας

$$x^\nu + y^\nu = (x+y)(x^{\nu-1} - x^{\nu-2}y + \dots - xy^{\nu-2} + y^{\nu-1})$$

(εφαρμόζόμενης στα $x = 2^l, y = 1$) ο $2^l + 1$ είναι διαιρέτης του πρώτου p . άτοπο.

Βάσει των παραπάνω καταλήγουμε στο εξής:

Θεώρημα 12.5. *Το κανονικό n -γωνο κατασκευάζεται αν και μόνο αν $n = 2^r p_1 \dots p_k$ όπου $r \geq 0$ και $p_1, \dots, p_k$ είναι διαφορετικοί πρώτοι του Fermat, δηλαδή $p_i = 2^{2^{r_i}} + 1$ για κάποιο $r_i \geq 0$ για κάθε $i = 1, \dots, k$.*

Κατασκευή του κανονικού 17-γώνου Η θεωρία των κυκλοτομικών σωμάτων πάνω από το $\mathbb{Q}$, εξειδικευμένη στο 17-ο κυκλοτομικό σώμα πάνω από το $\mathbb{Q}$, συνοψίζεται στα παρακάτω:

$$\theta = \frac{2\pi}{17}, \quad \omega = \cos \theta + i \sin \theta, \quad 2 \cos \theta = \omega + \omega^{-1} = \omega + \omega^{16},$$

$$E_{17} = \mathbb{Q}(\omega), \quad \mathcal{G}(E_{17}/\mathbb{Q}) = \langle \sigma \rangle, \quad \sigma(\omega) = \omega^3, \quad \sigma^k(\omega) = \omega^{3^k}, \quad \sigma(\omega^k) = \omega^{3k}.$$

Το διάγραμμα της αντιστοιχίας Galois είναι το εξής:

$$\begin{array}{ccc} \langle id \rangle & \longleftrightarrow & L_4 = E_{17} \\ | 2 & & | 2 \\ \langle \sigma^8 \rangle & \longleftrightarrow & L_3 \\ | 2 & & | 2 \\ \langle \sigma^4 \rangle & \longleftrightarrow & L_2 \\ | 2 & & | 2 \\ \langle \sigma^2 \rangle & \longleftrightarrow & L_1 \\ | 2 & & | 2 \\ \mathcal{G}(E_{17}/\mathbb{Q}) \langle \sigma \rangle & \longleftrightarrow & L_0 = \mathbb{Q} \end{array}$$

Επειδή η ομάδα $\mathcal{G}(E_{17}/\mathbb{Q})$ είναι κυκλική, οι μόνες υποομάδες της είναι αυτές των οποίων οι τάξεις είναι διαιρέτες του 16 και για κάθε διαιρέτη d υπάρχει ακριβώς μία υποομάδα της $\mathcal{G}(E_{17}/\mathbb{Q})$ τάξεως d . Συνεπώς, το «δίκτυο» υποομάδων της $\mathcal{G}(E_{17}/\mathbb{Q})$ είναι πολύ απλό: αυτό στην αριστερή στήλη του παραπάνω διαγράμματος. Συνεπώς, το «δίκτυο» υποσωμάτων του E_{17} είναι αυτό της δεξιάς στήλης του διαγράμματος. Οι αριθμοί 2, στην αριστερή στήλη δείχνουν τον δείκτη της υποομάδας στην αμέσως μεγαλύτερη υποομάδα και στη δεξιά στήλη δηλώνουν ότι $[L_i : L_{i-1}] = 2$ για $i = 1, \dots, 4$. Επίσης $\sum_{i=1}^{16} \omega^{16} = -1$.

Βήμα 1. Ορίζω

$$\begin{aligned} \eta_1 &:= \omega + \omega^2 + \omega^4 + \omega^8 + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} \\ \eta_2 &:= \omega^3 + \omega^5 + \omega^6 + \omega^7 + \omega^{10} + \omega^{11} + \omega^{12} + \omega^{14} \end{aligned}$$

Με απλές πράξεις διαπιστώνεται ότι $\sigma(\eta_1) = \eta_2$ και $\sigma(\eta_2) = \eta_1$, άρα $\sigma^2(\eta_i) = \eta_i$ για $i = 1, 2$. Έπεται ότι $\mathbb{Q}(\eta_i) \leq \mathcal{F}(\sigma^2) = L_1$ για $i = 1, 2$. Αφετέρου, $\eta_1 + \eta_2 = \sum_{i=1}^2 \omega^{16} = -1$ και $\eta_1 \eta_2 = -4$. Έπεται ότι τα η_i είναι ρίζες του $X^2 + X - 4$, το οποίο είναι ανάγωγο πάνω από το $\mathbb{Q}$. Άρα $\mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2)$ και $[\mathbb{Q}(\eta_i) : \mathbb{Q}] = 2 = [L_1 : \mathbb{Q}]$, οπότε

$$L_1 = \mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2) = \mathbb{Q}(\sqrt{17}).$$

Ένας προσεγγιστικός υπολογισμός με υπολογιστή ταυτοποιεί τις ρίζες του $X^2 + X - 4$ με τα η_i :

$$\eta_1 = \frac{1}{2}(-1 + \sqrt{17}), \quad \eta_2 = \frac{1}{2}(-1 - \sqrt{17}).$$

Βήμα 2. Διασπώ τα η_i ως εξής:

$$\begin{aligned} \eta_1 &= \underbrace{(\omega + \omega^4 + \omega^{13} + \omega^{16})}_{\eta_{11}} + \underbrace{(\omega^2 + \omega^8 + \omega^9 + \omega^{15})}_{\eta_{12}} \\ \eta_2 &= \underbrace{(\omega^3 + \omega^5 + \omega^{12} + \omega^{14})}_{\eta_{21}} + \underbrace{(\omega^6 + \omega^7 + \omega^{10} + \omega^{11})}_{\eta_{22}} \end{aligned}$$

Εύκολα ελέγχω ότι, για $i = 1, 2$ ισχύει $\sigma^2(\eta_{i1}) = \eta_{i2}$ και $\sigma^2(\eta_{i2}) = \eta_{i1}$, άρα, για $i, j \in \{1, 2\}$ ισχύει $\sigma^4(\eta_{ij}) = \eta_{ij}$, που σημαίνει ότι $\mathbb{Q}(\eta_{ij}) \leq \mathcal{F}(\sigma^4) = L_2$. Αφετέρου, για $i = 1, 2$ είναι $\eta_{i1} + \eta_{i2} = \eta_i$ (εκ κατασκευής) και διαπιστώνω, ακόμη, ότι $\eta_{i1}\eta_{i2} = -1$, άρα τα η_{i1}, η_{i2} είναι ρίζες του $X^2 - \eta_i X - 1 \in L_1[X]$. Οι ρίζες αυτές δεν μένουν αναλλοίωτες από τον σ^2 , άρα δεν ανήκουν στο L_1 . Συνεπώς, το δευτεροβάθμιο αυτό πολυώνυμο είναι ανάγωγο πάνω από το L_1 . Άρα, $\mathbb{Q}(\eta_{i1}) = \mathbb{Q}(\eta_{i2})$ και $[\mathbb{Q}(\eta_{i1}) : L_1] = 2 = [L_2 : L_1]$, οπότε

$$L_2 = \mathbb{Q}(\eta_{i1}) = \mathbb{Q}(\eta_{i2}), \quad i = 1, 2.$$

Ένας προσεγγιστικός υπολογισμός με υπολογιστή ταυτοποιεί, για κάθε $i = 1, 2$, τις ρίζες του $X^2 - \eta_i X - 1$ με τα η_{i1}, η_{i2} . Έτσι,

$$\eta_{11} = -\frac{1}{4} + \frac{1}{4}\sqrt{17} + \frac{1}{4}\sqrt{34 - 2\sqrt{17}}, \quad \eta_{21} = -\frac{1}{4} - \frac{1}{4}\sqrt{17} + \frac{1}{4}\sqrt{34 + 2\sqrt{17}}$$

(τα η_{12}, η_{22} δεν θα μας χρειασθούν).

Βήμα 3. Διασπώ το η_{11} ως εξής:

$$\eta_{11} = \underbrace{(\omega + \omega^{16})}_{\eta_{111}} + \underbrace{(\omega^4 + \omega^{13})}_{\eta_{112}}.$$

Δουλεύοντας όπως στο προηγούμενο βήμα δείχνω ότι τα η_{111}, η_{112} είναι ρίζες του $X^2 - \eta_{11}X + \eta_{21}$, το οποίο είναι ανάγωγο πάνω από το L_2 και, συνεπώς,

$$L_3 = \mathbb{Q}(\eta_{111}) = \mathbb{Q}(\eta_{112}).$$

Οι ρίζες του τελευταίου δευτεροβάθμιου πολυωνύμου υπολογίζονται, αφού οι συντελεστές του έχουν ήδη υπολογισθεί στο βήμα 2. Ένας προσεγγιστικός υπολογισμός δείχνει με ποια ρίζα είναι ίσο το $\eta_{111} = \omega + \omega^6 = \omega + \omega^{-1} = 2 \cos \theta$. Έτσι βρίσκω ότι

$$2 \cos \theta = \frac{\eta_{11} + \sqrt{\eta_{11}^2 - 4\eta_{21}}}{2}.$$

Τώρα, όποιος έχει υπομονή (ή πακέτο συμβολικού υπολογισμού στον υπολογιστή του), υπολογίζει

$$\begin{aligned} \cos \frac{2\pi}{17} &= -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{2(17 - \sqrt{17})} \\ &\quad + \frac{1}{8}\sqrt{4(17 + 3\sqrt{17}) - 2\sqrt{2(17 - \sqrt{17})} + 2\sqrt{17}\sqrt{2(17 - \sqrt{17})} - 16\sqrt{2(17 + \sqrt{17})}}. \end{aligned}$$

Είναι σαφές ότι καθένα από τα επιμέρους «κομμάτια» αυτού του αλγεβρικού αριθμού είναι κατασκευάσιμο.

Ασκήσεις Στις παρακάτω ασκήσεις, όπου ζητείται «γραφική» κατασκευή, εννοείται ότι πρέπει να την κάνετε σχεδιαστικά, πάνω σε χαρτί, χρησιμοποιώντας πραγματικά όργανα (κανόνα και διαβήτη), έχοντας επιλέξει αρχικά ένα ευθύγραμμο τμήμα του οποίου το μήκος είναι το μοναδιαίο (η επιλογή είναι, φυσικά, αυθαίρετη, αρκεί να βολεύει σχεδιαστικά).

Άσκηση 12.6. Έστω c το συνημίτονο της επίκεντρης γωνίας που αντιστοιχεί στην πλευρά κανονικού n -γώνου. Εκφράστε, συναρτήσει του c , το μήκος της πλευράς του κανονικού n -γώνου και εξηγήστε γιατί αυτό είναι κατασκευάσιμος αριθμός.

Άσκηση 12.7. Αναπτύξτε για το κανονικό 5-γωνο «θεωρία» ανάλογη με αυτήν του κανονικού 17-γώνου (είναι, φυσικά, πολύ απλούστερη) και, κατόπιν, κατασκευάστε γραφικά την πλευρά του κανονικού 5-γώνου.

Άσκηση 12.8. Κατασκευάστε γραφικά τον αριθμό $\frac{5}{3} \sqrt[4]{\sqrt{13} + \sqrt{11}}$.

Το τεταρτοβάθμιο πολυώνυμο

Έστω σώμα F του οποίου η χαρακτηριστική είναι 0 ή $\neq 2, 3$. Σκοπός μας είναι η μελέτη της ομάδας Galois των αναγώνων πολωνύμων τετάρτου βαθμού με συντελεστές στο F . Κάθε $X^4 + aX^3 + bX^2 + cX + d \in F[X]$ μπορεί να πάρει αυτή τη μορφή

$$f(X) = X^4 + qX^2 + rX + s, \quad q, r, s \in F$$

να μετασχηματισθεί σε πολυώνυμο με μηδενικό συντελεστή στο X^3 , ύστερα από αντικατάσταση του X από το $X - a/4$ και f έχει το ίδιο σώμα διάσπασης και την ίδια διακρίνουσα με το αρχικό.

Έστω E σώμα διάσπασης του f πάνω από το F και $t_1, \dots, t_4 \in E$ οι ρίζες του f . Την S_4 βλέπουμε ως ομάδα μεταθέσεων των t_1, t_2, t_3, t_4 . Από την άσκηση 11.12, το f είναι διαχωρίσιμο και, σύμφωνα με τον συμβολισμό της άσκησης,

$$G = \mathcal{G}(E/F) \leq S_4 \quad \text{και} \quad V = \langle (t_1 t_2)(t_3 t_4), (t_1 t_3)(t_2 t_4) \rangle \leq S_4.$$

Έχουν ορισθεί τα

$$u = (t_1 + t_2)(t_3 + t_4), \quad v = (t_1 + t_3)(t_2 + t_4), \quad w = (t_1 + t_4)(t_2 + t_3),$$

και (στην άσκηση) έχει αποδειχθεί ότι είναι διαφορετικά και ότι το πολυώνυμο

$$g(X) = (X - u)(X - v)(X - w)$$

έχει συντελεστές στο F , άρα είναι διαχωρίσιμο πολυώνυμο του $F[X]$ (όχι κατ' ανάγκη ανάγωγο). Θέτουμε

$$K = F(u, v, w) \leq E.$$

Η E/K είναι επέκταση Galois, αφού το K είναι σώμα διάσπασης του διαχωρίσιμου πολωνύμου $g \in F[X]$.

Ένας υπολογισμός ρουτίνας δείχνει ότι $V \leq S_4$ και

$$S_4/V = \{V, (t_1 t_2)V, (t_2 t_3)V, (t_1 t_3)V, (t_1 t_2 t_3)V, (t_1 t_3 t_2)V\}. \quad (12.4)$$

Λήμμα 12.9. $\mathcal{G}(E/K) = G \cap V$. Ισοδύναμα $\mathcal{F}(G \cap V) = K$.

Απόδειξη. Ένας απλός έλεγχος δείχνει ότι κάθε $\sigma \in V$ αφήνει αναλλοίωτα τα u, v, w , επομένως, αφήνει αναλλοίωτο και κάθε στοιχείο του K . Άρα, $G \cap V \leq \mathcal{G}(E/K)$. Αντιστρόφως, έστω $\sigma \in \mathcal{G}(E/K)$. Λόγω της (12.4) είναι $\sigma = \tau\sigma_0$, όπου $\sigma_0 \in V$ και $\tau \in \{id, (t_1 t_2), (t_2 t_3), (t_1 t_3), (t_1 t_2 t_3), (t_1 t_3 t_2)\}$. Το σ_0 αφήνει αναλλοίωτα τα u, v, w , άρα $\sigma(u) = \tau(u)$, $\sigma(v) = \tau(v)$, $\sigma(w) = \tau(w)$. Ένας απλός έλεγχος, και πάλι, αρκεί για να μας δείξει ότι από τους έξι αυτομορφισμούς του παραπάνω συνόλου, ο μόνος που αφήνει αναλλοίωτα και τα τρία u, v, w είναι ο id . Αλλά ο $\sigma \in \mathcal{G}(E/K)$ αφήνει αναλλοίωτα τα στοιχεία του K , άρα αφήνει αναλλοίωτα και τα τρία u, v, w . επομένως $\tau = id$ και $\sigma = \sigma_0 \in V$, άρα $\sigma \in G \cap V$. Συνεπώς, $\mathcal{G}(E/K) \leq G \cap V$, οπότε $\mathcal{G}(E/K) = G \cap V$. $\square$

Έστω $[K : F] = m$. Έχουμε το παρακάτω διάγραμμα αντιστοιχίας Galois:

$$\begin{array}{ccc} E & \longleftrightarrow & \langle id \rangle \\ \downarrow & & \downarrow \\ K & \longleftrightarrow & G \cap V \\ \downarrow m & & \downarrow \\ F & \longleftrightarrow & G \end{array}$$

Επειδή η K/F είναι επέκταση Galois, συμπεραίνουμε ότι $G \cap V \trianglelefteq V$ και

$$\mathcal{G}(K/F) \cong G/(G \cap V) \quad \therefore \quad \frac{|G|}{|G \cap V|} = |G/(G \cap V)| = |\mathcal{G}(K/F)| = [K : F] = m. \quad (12.5)$$

Είναι η $G \cap V$ υποομάδα της V , άρα $|G \cap V| \in \{1, 2, 4\}$. Επίσης, επειδή m είναι ο βαθμός του σώματος διάσπασης κυβικού πολωνύμου, είναι $m \in \{1, 2, 3, 6\}$. Συγκεκριμένα, αν το g είναι ανάγωγο πάνω από το F , τότε $m = 3$ ή $m = 6$, ανάλογα με το αν $D(g)$ είναι ή δεν είναι ίση με τετράγωνο ενός στοιχείου του F (βλ. Παράδειγμα 8.14).

Ακόμη, είναι $F(t_1) \leq E$ και $[F(t_1) : F] = 4$ γιατί το f είναι ανάγωγο πάνω από το F , άρα $|G| = [E : F]$ είναι πολλαπλάσιο του 4. Όμως $|G|$ είναι και διαιρέτης του $|S_4| = 24$, άρα, συνοψίζοντας τα παραπάνω:

$$|G| \in \{4, 8, 12, 24\}, \quad |G \cap V| \in \{1, 2, 4\}, \quad m \in \{1, 2, 3, 6\}, \quad |G| = m \cdot |G \cap V|. \quad (12.6)$$

Ασκήσεις

Άσκηση 12.10. Έστω σώμα F και $f \in F[X]$ βαθμού $n > 1$. Έστω E σώμα διάσπασης του F πάνω από το F και $t_1, \dots, t_n \in E$ ρίζες του f , διαφορετικές μεταξύ τους. Αποδείξτε το εξής: Αν για κάθε $i = 1, \dots, n$ υπάρχει F -αυτομορφισμός του E που στέλνει το t_1 στο t_i , τότε το f είναι ανάγωγο πάνω από το F .