CONSTRUCȚII GEOMETRICE CU RIGLA, COMPASUL ȘI TRISECTORUL

DE

TUDOR I. ZAMFIRESCU

§ 1. CRITERII DE CONSTRUCTIBILITATE

După cum sugerează și numele, trisectorul este un instrument cu care se poate divide un unghi oarecare în trei părți egale.

Să ne amintim că orice extindere algebric generată a corpului Q al numerelor raționale este un spațiu vectorial peste Q și să observăm că orice element al ei este construibil cu rigla și compasul dacă acest lucru este posibil pentru o bază a spațiului. În adevăr, un element arbitrar α se scrie în raport cu baza $\beta_1, \ldots, \beta_n$ ca o combinație liniară $\alpha = \sum_{i=1}^{n} \xi_i \beta_i$ cu $\xi_i \in Q$, construibilă cu rigla și compasul. Un corp ale cărui elemente pot fi construite cu rigla, compasul și trisectorul îl vom denumi *construibil.*

TEOREMA 1. *Fie corpul construibil K și ecuația*

$$\alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 = 0$$

cu $\alpha_3 \neq 0$ ireductibilă peste K. Condiția necesară și suficientă ca cel puțin o rădăcină a ei să fie construibilă cu rigla, compasul și trisectorul este ca toate rădăcinile să fie reale și distincte.

Demonstrație. Simplificînd ecuația cu α_3, găsim

$$x^3 + ax^2 + bx + c = 0, \tag{1}$$

unde $a = \frac{\alpha_2}{\alpha_3}$, $b = \frac{\alpha_1}{\alpha_3}$, $c = \frac{\alpha_0}{\alpha_3}\cdot$ Facem translația $x = x' - \frac{a}{3}$ și aflăm

$$x'^3 + px' + q = 0, \tag{2}$$

unde $p = b - \frac{a^2}{3}$ şi $q = \frac{2a^3}{27} - \frac{ab}{3} + c$. Transformarea $x' = \beta X$ ne dă

$$4X^3 - 3X = \alpha, \tag{3}$$

unde $\beta = \sqrt{\frac{-4p}{3}}$ şi $\alpha = \frac{3q}{p\beta}$.

Pentru demonstrarea suficienţei condiţiei din enunţ, să presupunem că rădăcinile $x_{1,2,3}$ ale ecuaţiei date sînt reale şi distincte. Rezultă că şi rădăcinile $x'_{1,2,3} = x_{1,2,3} + \frac{a}{3}$ ale ecuaţiei (2) sînt reale şi distincte. Aceasta are loc, după cum ştim, dacă discriminantul ecuaţiei (2) satisface inegalitatea $\frac{q^2}{4} + \frac{p^3}{27} < 0$ şi numai în acest caz. Deci $p < 0$. De asemenea rezultă că $-1 < \alpha < 1$. Într-adevăr,

$$9q^2 < p^2 \cdot \frac{-4p}{3} \quad \text{sau} \quad |3q| < -p\sqrt{\frac{-4p}{3}} \quad \text{sau} \quad -1 < \frac{3q}{p\beta} < 1.$$

Evident, cu ajutorul mărimilor date $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ se pot construi cu rigla şi compasul a, b, c, apoi p, q şi β, α. Găsim cu trisectorul unghiul $\omega = \frac{\text{arc cos } \alpha}{3}$. Aflăm cu rigla şi compasul $X_1 = \cos \omega$, $X_{2,3} = \cos\left(\frac{2\pi}{3} \mp \omega\right)$ care sînt cele trei rădăcini reale ale ecuaţiei (3). Aflăm apoi $x'_{1,2,3} = \beta X_{1,2,3}$ şi $x_{1,2,3} = x'_{1,2,3} - \frac{a}{3}$ cu ajutorul riglei şi compasului. Astfel, dacă condiţia este satisfăcută, putem găsi chiar toate cele trei rădăcini reale ale ecuaţiei date, cu ajutorul riglei, compasului şi trisectorului.

Să dovedim necesitatea condiţiei enunţate. Notăm cu $f(x)$ polinomul din membrul întîi al ecuaţiei date. Să presupunem că $f(x)$ are cel puţin două rădăcini confundate. Discriminantul ecuaţiei (2) este nul: $\frac{q^2}{4} + \frac{p^3}{27} = 0$. Rezultă că $\frac{3q}{p\beta} = \pm 1$, adică $\alpha = \pm 1$ şi $\beta = \pm \frac{3q}{p}$. Ecuaţia (3) admite în acest caz o rădăcină ± 1. Deci ecuaţia (2) se anulează în $\pm \frac{3q}{p}$, prin urmare este reductibilă peste K, ceea ce atrage reductibilitatea ecuaţiei date peste K, absurd. Deci rădăcinile sînt distincte. Să presupunem că $f(x)$ are două rădăcini nereale şi una reală ρ, pe care reuşim să o construim cu instrumentele date. Avem $[K(\rho) : K] = 3$. După cum se vede îndată, ρ nu poate fi construit numai cu rigla şi compasul. Neapărat s-a folosit deci trisectorul, cu care s-a rezolvat o ecuaţie ireductibilă $P_\alpha(x) = 4x^3 - 3x - \alpha = 0$ cu $\alpha \in K$, determinîndu-se rădăcina r_α. De aici urmează că $[K(r_\alpha) : K] = 3$. Prin urmare $\rho \in K(r_\alpha)$. Ştim că oricare ar fi

$\alpha \in K$ cu $|\alpha| \leqslant 1$, $P_\alpha(x)$ are trei rădăcini reale r_α, r', r''. De asemenea se ştie că avem $K(r_\alpha) = \{\beta$; există polinomul $g(x)$ cu coeficienţi în K astfel ca $\beta = g(r_\alpha)\}$. Polinoamele minimale ale lui r_α şi ρ sînt $P_\alpha(x)$ şi $f(x)$. Fie $g_\rho(x)$ un polinom de gradul al doilea cu proprietatea că $g_\rho(r_\alpha) = \rho$. Avem $f(g_\rho(r_\alpha)) = 0$ şi $P_\alpha(r_\alpha) = 0$. Cum $P_\alpha(x)$ este polinom minimal, el îl divide pe $(f \circ g_\rho)(x)$. Rădăcinile r', r'' ale lui $P_\alpha(x)$ vor anula şi pe $(f \circ g_\rho)(x)$, deci, notînd $\rho' = g_\rho(r')$ şi $\rho'' = g_\rho(r'')$, rezultă $f(\rho') = f(\rho'') = 0$, unde $\rho', \rho'' \in R$, corpul numerelor reale. Rădăcinile r_α, r', r'' sînt distincte căci dacă două dintre ele ar fi egale, discriminantul ecuaţiei $P_\alpha(x) = 0$ ar trebui să fie nul: $\frac{\alpha^2}{4^3} - \frac{1}{4^3} = 0$, deci P_α nu ar fi ireductibil. Cum nu se poate ca polinomul g_ρ, de gradul al doilea, să ia aceeaşi valoare pentru r_α, r', r'' distincte, rezultă că există cel puţin două numere distincte printre ρ, ρ', ρ''. Deci am găsit cel puţin încă o rădăcină reală ρ' sau ρ'' pentru $f(x)$, în afară de ρ, ceea ce contrazice ipoteza făcută. Prin urmare $f(x)$ are neapărat trei rădăcini reale şi distincte.

Exprimată sub o altă formă teorema anterioară devine

TEOREMA 2. *Condiţia necesară şi suficientă ca cel puţin o rădăcină a ecuaţiei* $\alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 = 0$ *cu* $\alpha_3 \neq 0$, *ireductibilă peste corpul construibil* K, *să fie construibilă cu rigla, compasul şi trisectorul este ca*

$$18\,\alpha_0\,\alpha_1\,\alpha_2\,\alpha_3 - 4\,\alpha_0\,\alpha_2^3 - 27\,\alpha_0^2\,\alpha_3^2 + \alpha_1^2\,\alpha_2^2 - 4\,\alpha_1^3\,\alpha_3 > 0.$$

Demonstraţie. Am văzut că, relativ la coeficienţii ecuaţiei (2), am găsit condiţia necesară şi suficientă: $\frac{q^2}{4} + \frac{p^3}{27} < 0$. Înlocuind aici p şi q prin expresiile lor folosind coeficienţii ecuaţiei (1) şi apoi înlocuindu-i pe aceştia utilizînd numerele α_0, α_1, α_2, α_3, găsim condiţia din enunţ.

Rezultă ca o condiţie necesară, dar nu suficientă, existenţa lanţului de corpuri $\Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_n$ astfel ca $\Lambda_n \supset G$ iar $[\Lambda_m : \Lambda_{m-1}] = 2$ sau 3 ($m = 1, \ldots, n$), unde s-au notat cu Λ_0 cel mai mic corp numeric care include mulţimea F a coordonatelor punctelor esenţiale date şi cu G mulţimea coordonatelor punctelor esenţiale cerute. Pentru a asigura şi suficienţa, adăugăm condiţia ca pentru orice extindere $\Lambda_m \supset \Lambda_{m-1}$ de grad trei, să existe elementul $\lambda_m \in \Lambda_m$ astfel ca polinomul său minimal relativ la Λ_{m-1} să fie de tipul celor din teoremele 1 sau 2.

§ 2. APLICAŢIE LA POLIGOANELE REGULATE

Problema pe care ne-o punem constă în a construi cu rigla, compasul şi trisectorul un poligon regulat cu un număr dat n de laturi, înscris într-un cerc dat.

Să considerăm un sistem xOy de axe rectangulare ale cărui origine şi unitate de măsură coincid cu centrul şi raza cercului dat. Fie $(1, 0)$ un vîrf al poligonului. Atunci întreaga problemă se reduce la construirea punctului $\left(\cos\frac{2\pi}{n}, 0\right)$, întrucît un vîrf alăturat lui (1,0) este o intersecție a perpendicularei în $\left(\cos\frac{2\pi}{n}, 0\right)$ pe Ox cu cercul dat, iar celelalte se obțin imediat.

Fie N mulțimea numerelor naturale iar $Z_+ = N \cup \{0\}$.

În cele ce urmează vom folosi funcția φ a lui Euler, despre care amintim că, dacă $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ este descompunerea lui n în factori primi distincți, atunci

$$\varphi(n) = p_1^{\alpha_1-1}(p_1-1) \cdot \ldots \cdot p_r^{\alpha_r-1}(p_r-1).$$

Fie polinomul $z^n - 1$ peste corpul C al numerelor complexe. Conform scopului urmărit, vom lua $n \geqslant 3$. Știm că acest polinom posedă n rădăcini complexe distincte

$$\varepsilon_j = \cos\frac{2j\pi}{n} + i\sin\frac{2j\pi}{n} \qquad (j = 0, 1, \ldots, n-1)$$

dintre care $\varepsilon_0 = 1$, numite rădăcinile de ordin n ale unității și că acestea formează un subgrup al grupului multiplicativ $C - \{0\}$.

Cunoaștem că gradul extinderii $Q(\varepsilon_1) \supset Q$ este $\varphi(n)$. Pentru că $\varepsilon_1 + \varepsilon_1^{-1} = 2\cos\frac{2\pi}{n}$ și $\varepsilon_1 \varepsilon_1^{-1} = 1$, avem $Q(\varepsilon_1) \supset Q\left(\cos\frac{2\pi}{n}\right)$ iar gradul extinderii este doi. Rezultă că

$$\left[Q\left(\cos\frac{2\pi}{n}\right) : Q\right] = \frac{\varphi(n)}{2}.$$

TEOREMA 3. *Pentru ca un poligon regulat cu n laturi să poată fi construit cu rigla, compasul și trisectorul este necesar și suficient ca*

$$n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot p_3 \cdot \ldots \cdot p_r$$

unde $\alpha_1, \alpha_2, r \in Z_+$ *iar* $p_3, \ldots, p_r$ *sînt numere prime distincte de forma*

$$p_i = 2^{\beta_i} \cdot 3^{\gamma_i} + 1$$

cu $\beta_i \in N$, $\gamma_i \in Z_+$.

Demonstrație. Vom arăta mai întîi necesitatea condiției. Din cele prezentate în § 1 rezultă că o condiție necesară pentru constructibilitatea lui $\cos\frac{2\pi}{n}$, deci și a poligonului, este ca

$$\left[Q\left(\cos\frac{2\pi}{n}\right) : Q\right] = 2^m \cdot 3^s,$$

unde $m, s \in Z_+$, ceea ce revine la

$$\varphi(n) = 2^{m+1} \cdot 3^s.$$

Dacă

$$n = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_r^{\alpha_r}$$

este descompunerea despre care am mai vorbit, atunci:

1) $\varphi(n) = 2^{\alpha_1} \cdot 3^{\alpha_2 - 1} \cdot p_3^{\alpha_3 - 1}(p_3 - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1}(p_r - 1)$

pentru $\alpha_1, \alpha_2 \neq 0$;

2) $\varphi(n) = 2 \cdot 3^{\alpha_2 - 1} \cdot p_3^{\alpha_3 -}(p_3 - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1}(p_r - 1)$

pentru $\alpha_1 = 0, \alpha_2 \neq 0$;

3) $\varphi(n) = 2^{\alpha_1 - 1} \cdot p_3^{\alpha_3 - 1}(p_3 - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1}(p_r - 1)$

pentru $\alpha_1 \neq 0, \alpha_2 = 0$ şi

4) $\varphi(n) = p_3^{\alpha_3 - 1}(p_r - 1) \cdot \ldots \cdot p_r^{\alpha_r - 1}(p_r - 1)$

pentru $\alpha_1, \alpha_2 = 0$.

Examinînd aceste cazuri, constatăm că pentru ca

$$\varphi(n) = 2^{m+1} \cdot 3^n$$

cu $m, n \in Z_+$, trebuie ca $2 | \varphi(n)$, deci în cazul 3) trebuie exclusă posibilitatea $\alpha_1 = 1$, $r = 0$, ceea ce se presupune de la început admis (poligon nedegenerat), iar în cazul 4), $r \neq 0$, ceea ce este şi mai banal. Apoi, trebuie ca $\alpha_3 = \alpha_4 = \ldots = \alpha_r = 1$ iar $p_i = 2^{\beta_i} \cdot 3^{\gamma_i} + 1$ cu $\beta_i \in N$, $\gamma_i \in Z_+$ (nu s-ar putea ca $\beta_i = 0$, căci am avea $2 | p_i$, ceea ce e absurd).

Să dovedim acum suficienţa condiţiei din enunţ. Vom arăta la început că un poligon regulat cu $p = 2^\beta \cdot 3^\gamma + 1$ laturi ($\beta \in N$, $\gamma \in Z_+$, p prim) poate fi construit cu rigla, compasul şi trisectorul. Conform teoremei lui Euler, dacă numerele naturale b şi p sînt prime între ele, atunci

$$b^{\varphi(p)} \equiv 1 \pmod{p}$$

Dacă, în plus, p este prim, atunci

$$b^{\frac{p-1}{2}} \equiv \pm 1$$

deoarece $\varphi'(p) = p - 1$ iar dacă

$$b^{\frac{p-1}{2}} \equiv c \quad (0 \leqslant c < p),$$

atunci

$$c^2 \equiv 1$$

sau

$$(c + 1)(c - 1) = \mathcal{M}\, p,$$

deci

$$c + 1 = \mathcal{M}\, p$$

sau

$$c - 1 = \mathfrak{M}\, p$$

de unde $c = 1$ sau $c = p - 1$. Se știe că oricare ar fi numărul prim p, există un întreg a astfel încît $a^{\circ}, a^1, \ldots, a^{p-2}$ să epuizeze modulo p mulțimea $\{1, \ldots, p - 1\}$. Rezultă că $a^{\frac{p-1}{2}} \equiv -1$ căci altfel $a^{\circ}, \ldots, a^{\frac{p-1}{2}-1}$ ar fi respectiv congruente cu $a^{\frac{p-1}{2}}, \ldots, a^{p-2}$. Prin urmare $a^r = -a^q$ dacă $|r - q| = \frac{n-1}{2}$.

Notînd $\varepsilon = \varepsilon_1$ rădăcinile $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{p-1}$ ale ecuației $z^p - 1 = 0$ devin $\varepsilon^0, \ldots, \varepsilon^{p-1}$. Vom aranja ultimele $p - 1$ rădăcini în următorul mod: (P_0^1): $\varepsilon^{a^0}, \varepsilon^{a^1}, \ldots, \varepsilon^{a^{p-2}}$, unde a are semnificația anterioară. Notăm cu $(P_{n+1}^{3(m-1)+i})$ mulțimea ordonată a rădăcinilor din (P_n^m) luate din trei în trei începînd cu a i – a ($i = 1,2,3$), cînd n ia pe rînd valorile $0,1, \ldots, \gamma$. În continuare, notăm cu $(P_{n+1}^{2(m-1)+j})$ mulțimea ordonată a rădăcinilor din (P_n^m) luate din două în două începînd cu a j – a ($j = 1,2$) cînd n ia valorile $\gamma + 1, \ldots, \gamma + \beta - 1$. Sumele λ_n^m ale rădăcinilor din (P_n^m) se numesc perioadele lui Gauss. Este ușor de observat că orice $\lambda_n^m \in R$, întrucît o dată cu un termen ε^{a^r}, perioada conține și unul de forma ε^{a^q} cu $|r - q| = \frac{p-1}{2}$, deci $\varepsilon^{a^r} = \varepsilon^{-a^q}$, adică ε^{a^r} și ε^{a^q} sînt simetrice față de axa reală. Considerăm corpurile $L_n^m = Q(\lambda_n^m)$ și $\Lambda_n = L_n^1$. În particular

$$\Lambda_{\beta+\gamma-1} = L^1_{\beta+\gamma-1} = Q(\lambda^1_{\beta+\gamma-1}) = Q(\varepsilon^{a^0} + \varepsilon^{a^{2^{\beta-1}\cdot 3^{\gamma}}}) = Q(\varepsilon + \varepsilon^{-1}) = \\ = Q\left(\cos\frac{2\pi}{p}\right).$$

Se știe că $\lambda_n^m \cdot \lambda_n^{m'}$ este o combinație liniară de perioade cu indice inferior n (vezi [2]). Așadar $L_n^m = L_n^{m'}$. De asemenea, niște ecuații aritmetice cu congruențe care se scriu imediat, arată că pentru $n \leqslant \gamma$ putem scrie $\lambda_n^1 + \lambda_n^2 + \lambda_n^3$, $\lambda_n^1\lambda_n^2 + \lambda_n^2\lambda_n^3 + \lambda_n^3\lambda_n^1$ și $\lambda_n^1\lambda_n^2\lambda_n^3$ ca niște combinații liniare de perioade de indice inferior $n - 1$, iar pentru $n > \gamma$ se pot scrie în același fel $\lambda_n^1 + \lambda_n^2$ și $\lambda_n^1\lambda_n^2$, dar nu pot fi astfel scrise și înseși perioadele de indice inferior n. Rezultă că $[\Lambda_n : \Lambda_{n-1}]$ este 3 pentru $n \geqslant \gamma$ și 2 pentru $n < \gamma$, după gradele polinoamelor minimale ale lui λ_n^1 puse în evidență. Să remarcăm și că aceste polinoame au toate rădăcinile reale, deci se conformează condițiilor puse în §1. Prin urmare am pus în evidență lanțul de extinderi $Q = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_{\beta+\gamma-1} = Q\left(\cos\frac{2\pi}{n}\right)$, satisfăcînd condiția necesară și suficientă ca poligonul să poată fi construit.

Constructibilitatea poligoanelor regulate cu p și p' laturi, unde p și p' sînt prime între ele, atrage după cum se știe constructibilitatea poligonului regulat cu pp' laturi și, avînd în vedere că poligoanele regulate cu 2^{α_1} și 3^{α_2} laturi se pot ușor construi, rezultă că suficiența condiției enunțate este dovedită.

Este interesant de remarcat că dacă se dă cercul în care trebuie înscris poligonul, atunci constructibilitatea lui cu rigla, compasul și trisectorul atrage constructibilitatea doar cu rigla și trisectorul, în baza faptului cunoscut că folosirea riglei și compasului este substituibilă cu folosirea doar a riglei în cazul cînd în planul de construcție ne este dat un cerc. Dacă însă cercul circumscris nu ne este dat, atunci întrebuințarea compasului este esențială, deci rigla și trisectorul se dovedesc insuficiente, deși condițiile de construcție par la prima vedere a fi mai largi.

Conform teoremei 3, heptagonul regulat, poligonul cu cel mai mic număr de laturi neconstruibil cu instrumentele clasice: rigla și compasul, poate fi construit utilizînd și trisectorul ($7 = 2 \cdot 3 + 1$).

Dat fiind un cerc, în afară de poligoanele regulate înscrise cu 3,4,5, 6,8,10,12,15,16,17,20,... laturi, care pot fi construite doar cu rigla, mai sînt construibile, însă folosind și trisectorul, poligoanele cu 7,9,13,14,18, 19, ... laturi. Primul care nici acum nu va putea fi construit este poligonul regulat cu 11 laturi.

Primită la redacție la 28 decembrie 1963

BIBLIOGRAFIE

1. DICKSON-BODEWIG, *Höhere Algebra.* Berlin, 1929.
2. C. IACOB, *Curs de matematici superioare.* București, 1957.
3. LUGOWSKI-WEINERT, *Grundzüge der Algebra.* vol. III, Leipzig, 1960.
4. M. POSTNIKOV, *Teoria lui Galois.* Moscova, 1963.
5. B. VAN DER WAERDEN, *Moderne Algebra.* vol. I, Berlin 1937; vol. II, Berlin, 1940.