A geometriai szerkeszthetőségről

KISS PÉTER és MÁTYÁS FERENC

Abstract. (On the geometrical constructibility) In this paper we deal with the algebraic theory of geometrical constructibility, especially with the case of the constructibility of regular polygons. We give such a proof of Gauss' famous theorem which can easily be understood by the students of Teachers' Training Colleges.

Dolgozatunkban a geometriai szerkeszthetőség algebrai elmélete tanításának az EKTF matematika szakos hallgatói számára kidolgozott és az elmúlt években tanított változatával foglalkozunk. E témakör tárgyalása természetesen megtalálható több helyen (pl. [1], [2], [3], [4]), de a bizonyítások sokszor csak vázlatosak, főiskolai hallgatók számára nem mindig érthetőek. Cikkünkben igyekszünk a főiskolai hallgatók matemaikai ismereteinek megfelelő bizonyításokat adni, így feltételezzük, hogy az olvasó is rendelkezik a harmadéves főiskolai hallgatóktól elvárható algebrai (testbővítési) és számelméleti alapismeretekkel.

Először tisztázzuk, hogy euklideszi szerkesztés során milyen adatokat, milyen eszközöket és milyen eljárásokat engedünk meg. A szerkesztés adatai: adott síkban véges sok pont, egyenes és kör, míg szerkesztési eszközként egyélű vonalzót, ill. körzőt használhatunk. Szerkesztési eljárásként az alábbiakat engedjük meg:

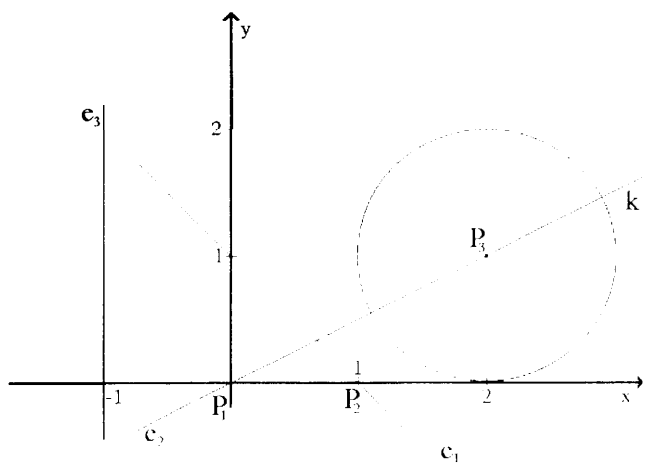
— két adott (vagy már szerkesztett) ponton át egyenes meghúzása;
— adott (vagy szerkesztett) pontok távolságával, mint sugárral adott (vagy szerkesztett) pont, mint középpont köré kör rajzolása;
— két adott egyenes metszéspontjának kijelölése;
— adott egyenes és adott kör metszéspontjainak kijelölése.

A fenti, ún. alapszerkesztések véges sorozatát euklideszi szerkesztésnek nevezzük. Egy szerkesztési feladatot megoldhatónak mondunk, ha a keresett (szerkesztendő) pont vagy ponthalmaz euklideszi szerkesztéssel előállítható.

A geometriai szerkeszthetőség algebrai jellemzése

Mivel az euklideszi szerkesztés minden lépése egy adott síkban történik, ezért mind az adatok, mind az alapszerkesztésekkel kapott újabb pontok,

egyenesek és körök azonosítására vegyünk fel az adott síkban egy derékszögű koordinátarendszert. Az adatok A_0 halmazának legalább két pontot tartalmaznia kell (ellenkező esetben a szerkesztési algoritmus el sem indítható), ezért a koordinátarendszer felvehető úgy, hogy A_0 egyik pontja a koordinátarendszer origója, míg egy másik pontja az egyik koordináta-tengely egységpontja legyen. Ebben a koordinátarendszerben A_0 ponjait koordinátáikkal, A_0 köreit a középpontjaik koordinátáival és sugaraik hosszával, míg A_0 egyeneseit az $a_i x + b_i y = c_i$ normál vektoros egyenletükben szereplő (a_i, b_i, c_i) számhármasokkal jellemezhetjük (ill. azonosíthatjuk). Az A_0 elemeihez így rendelt „koordináták" halmazát jelöljük K_0-lal. Az adatok A_0 halmazához így előállítot K_0-hoz rendeljük hozzá azt a legszűkebb $\mathbf{T}_0$ számtestet, melyre $K_0 \subset \mathbf{T}_0$. Konstrukciónkból adódik, hogy $\mathbf{Q} \subseteq \mathbf{T}_0 \subset \mathbf{R}$. Érdemes megjegyezni, hogy a $\mathbf{T}_0$ számtest nem függ attól, hogy A_0 mely pontját választottuk a koordinátarendszer kezdő, ill. egységpontjának, mivel az egyik koordinátarendszerből a másikba való áttérés során csak $\mathbf{T}_0$ beli alapműveleteket végzünk, így a transzformációs számítások eredményei is $\mathbf{T}_0$-ban lesznek. Például, ha $A_0 = \{P_1, P_2, P_3, e_1, e_2, e_3, k\}$, ahol P_1, P_2, P_3 az 1. ábra szerinti pontokat, e_1, e_2, e_3 egyeneseket, míg k kört jelöl, akkor A_0 elemeit az alábbi módon jellemezhetjük.



1. ábra

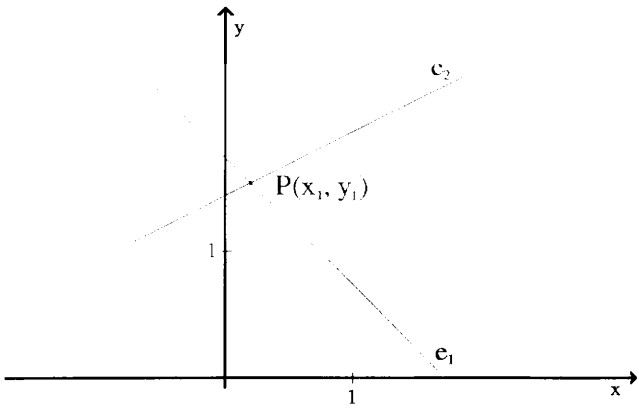
$P_1(0,0)$; $P_2(1,0)$; $P_3(2,1)$, $e_1(1,1,1)$, $e_2(1,-2,0)$, $e_3(1,0,-1)$ és $k(2,1,1,)$, mivel e_1 egyenlete: $x + y = 1$, e_2 egyenlete: $x - 2y = 0$, e_3 egyenlete: $x + 0y = -1$ és a k kör egyenlete: $(x-2)^2 + (y-1)^2 = 1^2$. Ebben az esetben $K_0 = \{0, 1, 2, -1, -2\}$ és $\mathbf{T}_0 = \mathbf{Q}$.

A továbbiakban vizsgáljuk meg az A_0-ból szerkeszthető pontok koordinátáit tartalmazó számtesteket. Erről szól a következő tétel.

1. Tétel. Az adatok A_0 (legalább két pontot tartalmazó) halmazából az A_0 elemeit tartalmazó sík P pontja akkor és csakis akkor szerkeszthető meg euklideszi szerkesztéssel, ha a P pont koordinátái egy olyan $\mathbf{T}$ számtest elemei, mely az A_0-hoz rendelt $\mathbf{T}_0$ számtest 2^j-edfokú algebrai bővítése, ahol $j \geq 0$ valamely egész szám.

Bizonyítás. Az A_0 elemeiből euklideszi alapszerkesztésekkel szerkesztett ponthoz juthatunk két egyenes metszéspontjának, egyenes és kör, ill. két kör metszésponjának meghatározásával. Vizsgáljuk meg az így szerkesztett pont koordinátáit az egyes esetekben.

a) Legyen e_1 és e_2 a két metsző egyenes, melyek egyenlete e_1: $a_1x+b_1y = c_1$ és e_2: $a_2x + b_2y = c_2$, ahol $e_1, e_2 \in A_0$, a_i, b_i, $c_i \in \mathbf{T}_0$ $(i = 1, 2)$.



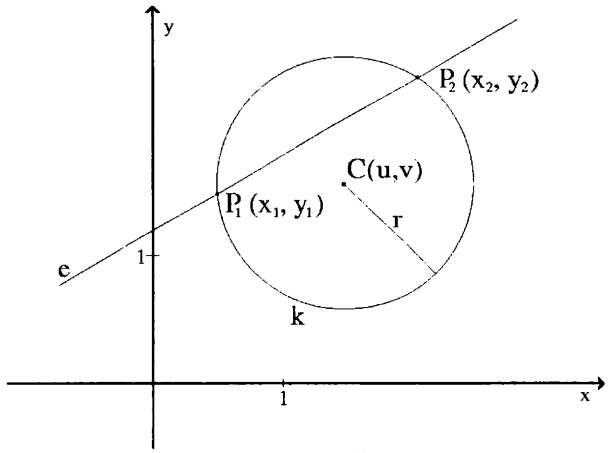
2. ábra

A P metszéspont x_1 és y_1 koordinátáit az

$$x_1 = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} \quad \text{és} \quad y_1 = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}$$

formulák adják, azaz $x_1, y_1 \in \mathbf{T} = \mathbf{T}_0$.

b) Legyen az egymást metsző e egyenes, ill. k kör egyenlete e: $ax+by = c$, ill. k: $(x-u)^2 + (y-v)^2 = r^2$, ahol $e, k \in A_0$ és $a, b, c, u, v, r \in \mathbf{T}_0$ $(r > 0)$.



3. ábra

Az így megszerkeszthető P_1 és P_2 metszéspontok (x_1, y_1), ill. (x_2, y_2) koordinátáit az

$$\left.\begin{aligned} ax + by &= c \\ (x-u)^2 + (y-v)^2 &= r^2 \end{aligned}\right\}$$

egyenletrendszer megoldásai adják. Az $a^2 + b^2 \neq 0$ miatt feltehetjük, hogy pl. $b \neq 0$ és így x_1, x_2 értékét az

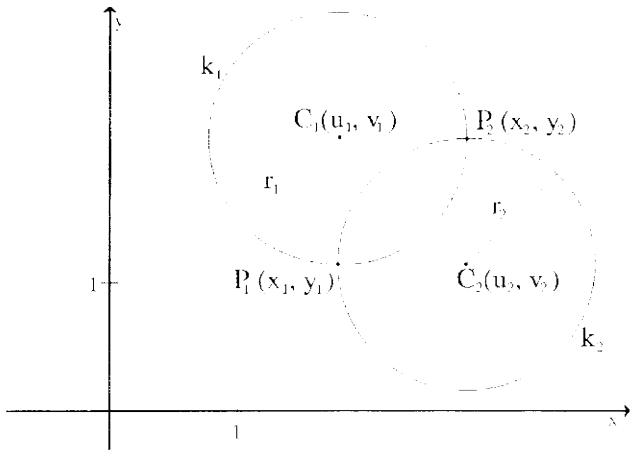
$$(x-u)^2 + \left(\frac{c-ax}{b} - v\right)^2 = r^2,$$

vagy az ebből rövid átalakítással kapható $x^2 + Ax + B = 0$ alakú másodfokú egyenlet

$$x_{1,2} = \frac{-A \pm \sqrt{D}}{2}$$

gyökei adják, ahol A és B az a, b, u, v és r-től lineárisan függő konstans, $D = A^2 - 4B$ és $A, B, D(\geq 0) \in \mathbf{T}_0$, továbbá $y_{1,2} = \frac{1}{b}(c - ax_{1,2})$. Ha $\sqrt{D} \in \mathbf{T}_0$, akkor x_1, x_2, y_1 és y_2 is $\mathbf{T}_0$-beli elem, míg $\sqrt{D} \notin \mathbf{T}_0$ esetén az x_1, x_2, y_1 és y_2 koordináták egy olyan $\mathbf{T}_1$ számtest elemei, melyre $\mathbf{T}_0 \subset \mathbf{T}_1$ és $\mathbf{T}_1 = \mathbf{T}_0(\sqrt{D})$, azaz a $\mathbf{T}_1$ számtest a $\mathbf{T}_0$ másodfokú algebrai bővítése.

c) Legyen az egymást metsző k_1 és k_2 körök egyenlete k_1: $(x-u_1)^2 + (y-v_1)^2 = r_1^2$, ill. k_2: $(x-u_2)^2 + (y-v_2)^2 = r_2^2$, ahol $k_1, k_2 \in A_0$, míg $u_i, v_i, r_i \in \mathbf{T}_0$ és $r_i > 0$ $(i = 1, 2)$.



4. ábra

A megszerkeszthető P_1 és P_2 pontok (x_1, y_1), ill. (x_2, y_2) koordinátáit az

$$\left.\begin{aligned}(x-u_1)^2+(y-v_1)^2&=r_1^2\\(x-u_2)^2+(y-v_2)^2&=r_2^2\end{aligned}\right\}$$

egyenletrendszer megoldásai adják. Látható, hogy pl. az x_1, x_2 megoldások ebben az esetben is egy alkalmas

$$x^2+Ax+B=0 \quad (A,B,D(=A^2-4B\geq 0)\in \mathbf{T}_0)$$

egyenlet gyökei. Ezért — hasonlóan a b) esethez — x_1, x_2, y_1 és y_2 elemei $\mathbf{T}_0$-nak ha $\sqrt{D}\in \mathbf{T}_0$, míg $\sqrt{D}\notin \mathbf{T}_0$ esetén $x_1, x_2, y_1, y_2 \in \mathbf{T}_1 = \mathbf{T}_0(\sqrt{D})$.

Ha az adatok A_0 és a már megszerkesztett pontok halmazából újabb pontot (vagy pontokat) szerkesztünk, akkor az a), b) vagy c) esetek ismételt alkalmazásával láthatjuk, hogy az új pontok koordinátái $\mathbf{T}_0$ vagy a $\mathbf{T}_1$ számtestben, vagy a $\mathbf{T}_2 = \mathbf{T}_1(\sqrt{D_1})$ testben találhatók, ahol $D_1 \in \mathbf{T}_1$, de $\sqrt{D_1}\notin \mathbf{T}_1$ és $\mathbf{Q}\subseteq \mathbf{T}_0 \subset \mathbf{T}_1 \subset \mathbf{T}_2$. Tovább folytatva a szerkeszthető pontok koordinátáinak meghatározását láthatjuk, hogy minden szerkeszthető pont koordinátája $\mathbf{T}_0$-ban, vagy valamely $\mathbf{T}_j = \mathbf{T}_{j-1}(\sqrt{D_{j-1}})$ számtestben található, ahol $D_{j-1}\in \mathbf{T}_{j-1}$, $\sqrt{D_{j-1}}\notin \mathbf{T}_{j-1}$ és

$$\mathbf{Q}\subseteq \mathbf{T}_0 \subset \mathbf{T}_1 \subset \mathbf{T}_2 \subset \cdots \subset \mathbf{T}_j \subset \cdots \subset \mathbf{T}_k \subset \mathbf{R}$$

$(1\leq j\leq k)$. Mivel $\mathbf{T}_j$ minden esetben másodfokú algebrai bővítése $\mathbf{T}_{j-1}$-nek, ezért — tudva, hogy az egymás utáni algebrai bővítések során a bővítések fokszáma szorzódik — $\mathbf{T}_j$ valóban 2^j-edfokú (algebrai) bővítése $\mathbf{T}_0$-nak.

Bizonyításunk második részében megmutatjuk, hogy a $\mathbf{T}_j = \mathbf{T}_{j-1}(\sqrt{D_{j-1}})$ $(D_{j-1} \in \mathbf{T}_{j-1})$ test elemeivel, mint koordinátákkal adott minden pont valóban szerkeszthető euklideszi szerkesztéssel.

Ismert, hogy a $\mathbf{T}_j(\sqrt{D_{j-1}})$ test minden eleme $a_{j-1} + b_{j-1}\sqrt{D_{j-1}}$ $(a_{j-1}, b_{j-1}, D_{j-1} \in T_{j-1})$ alakú, ezért az elemek szerkeszthetősége a_{j-1}, b_{j-1}, $D_{j-1} \in \mathbf{R}^+$ esetén egyenértékű szakaszok összegének, különbségének, szorzatának, hányadosának és négyzetgyökének euklideszi szerkesztéssel való előállításával. Elemi geomeriai tanulmányainkból ismert, hogy a fenti szerkesztések mind elvégezhetők a megengedett euklideszi alapszerkesztésekkel. Sőt, ha a komplex számokat vektorként vesszük fel, a műveleteket pedig a komplex számok abszolút értéke és irányszöge segítségével végezzük, akkor $a_{j-1}, b_{j-1}, d_{j-1} \in \mathbf{C}$ esetén is elvégezhető valamennyi fenti szerkesztési lépés. (Néhány szerkesztés menetét lásd. [3]-ban.) Az alaptest minden 2^j-edfokú bővítését másodfokú bővítések sorozata adja, így a tételek állítása bizonyított.

Megjegyzés. Ha az adatok A_0 halmazához rendelt $\mathbf{T}_0$ számtestre $\mathbf{T}_0 = \mathbf{Q}$, akkor az 1. Tétel szerint pontosan azon P pontok szerkeszthetők meg euklideszi értelemben, melyek koordinátái $\mathbf{Q}$-nak valamely 2^j-edfokú algebrai bővítésében találhatók, azaz — az algebrai bővítésekről tanultak szerint — a koordináták, mint valós számok zérushelyei egy $\mathbf{Q}$ fölött irreducibilis 2^j-edfokú racionális együtthatós polinomnak. A z komplex számot reprezentáló P pont esetén a szerkeszthetőség kérdése nyilvánvalóan ekvivalens azzal, hogy z gyöke-e egy $\mathbf{Q}$ fölött irreducibilis 2^j-edfokú racionális együtthatós polinomnak.

Klasszikus szerkeszthetőségi problémák

Az 1. Tétel alkalmazásaként könnyen adhatunk választ néhány nevezetes, szerkeszthetőségi problémára.

— **A kockakettőzés** (déloszi probléma) néven ismert szerkesztési feladatban egy adott kocka éléből kell egy kétszer akkora térfogatú kocka élét megszerkeszteni. Tekintsük az adott él, mint szakasz két végpontját egy koordinátarendszer origójának és (egyik tengelye) egységpontjának. Ebben a koordinátarendszerben az adatok jellemezhetők a $K_0 = \{0, 1\}$ halmazzal és így a hozzá tartozó $\mathbf{T}_0$ testre $\mathbf{T}_0 = \mathbf{Q}$. A feladat megoldásához a kettő térfogatú kocka $\sqrt[3]{2}$ hosszúságú élét kellene megszerkeszteni. De az 1. Tétel után tett megjegyzésünk szerint ez nem lehetséges, mivel $\sqrt[3]{2}$ az $f(x) = x^3 - 2$ racionális együtthatós, $\mathbf{Q}$ fölött irreducibilis de nem 2^j-edfokú polinom zérushelye.

Ha olyan szerkesztési lépéseket is megengedünk, melyek nem euklideszi alapszerkesztések, akkor e probléma szerkesztéssel megoldható lehet, lásd pl. [2], 123. oldal.

— **A szögharmadolás** (triszekció) néven olyan véges szerkesztési eljárás keresése a feladat, mely tetszőleges szög harmadának a szerkesztését adja. Konkrét szög, pl. 90° harmadolására könnyen tudunk euklideszi szerkesztési eljárást adni, ugyanakkor az általános eljárás létezését cáfolhatjuk, ha találunk olyan szöget, melynek harmada nem szerkeszthető euklideszi értelemben. Állítjuk, hogy pl. 60° harmada nem szerkeszthető.

Legyen adott két pont, mely egy koordinátarendszer origója, ill. egységpontja (e két pont ismeretében a 60°-os szög már szerkeszthető). Így $K_0 = \{0,1\}$ és $\mathbf{T}_0 = \mathbf{Q}$. Mivel 60° harmadának, 20°-nak a szerkeszthetősége nyilvánvalóan ekvivalens cos 20° (ill. sin 20°) szerkeszthetőségével, ezért elegendő megmutatnunk, hogy cos 20° nem szerkeszthető. Az $\frac{1}{2} = \cos 60° = 4\cos^3 20° - 3\cos 20°$ trigonometrikus egyenlőségből $x = \cos 20°$ helyettesítésével a $8x^3 - 6x - 1 = 0$ egyenlőséghez jutunk, azaz $x = \cos 20°$ zérushelye az $f(x) = 8x^3 - 6x - 1$ polinomnak. Könnyen ellenőrizhetjük, hogy a Rolle-tétel szerint lehetséges $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ racionális számok nem zérushelyei az $f(x)$ polinomnak, ezért $f(x)$ irreducibilis $\mathbf{Q}$ fölött. Mivel $f(x)$ nem 2^j-edfokú polinom, így cos 20° (és vele együtt 20° nem szerkeszthető euklideszi szerkesztéssel.

Persze, nem-euklideszi szerkesztési lépéseket is megengedve, vagy az adatok A_0 halmazának alkalmas bővítésével e feladat is megoldható, lásd pl. Bolyai János szerkesztési eljárását [2] 129 oldalán.

— **A kör négyszögesítése, ill. kiegyenesítése** néven ismertek azok a szerkesztési feladatok, amikor adott kör területével egyenlő területű négyzet oldalát, ill. adott kör kerületével egyenlő hosszú szakaszt kell szerkeszteni. Legyen ebben az esetben is adott két pont, az egyik a kör középpontja, a másik a kör egy kerületi pontja, melyek a koordinátarendszerünk origója, ill. egységpontjai lesznek. Így $K_0 = \{0,1\}$ és $\mathbf{T}_0 = \mathbf{Q}$. A feladatok nem megoldhatóságát az $f(x) = x^2 - \pi$, ill. a $g(x) = x - 2\pi$ polinomok zérushelyeinek nem szerkeszthetősége adja. Ugyanis π transzcendens volta miatt $\sqrt{\pi}$ és 2π is transzcendens, holott az 1. Tétel szerint csak (speciális) algebrai számok szerkeszthetők euklideszi szerkesztéssel.

— **A szabályos sokszögek euklideszi szerkeszthetőségére** vonatkozik a következő, Gauss-tól származó híres tétel:

Gauss-tétel: Az n-oldalú szabályos sokszög akkor és csakis akkor szerkeszthető meg euklideszi szerkesztéssel, ha $n = 2^k p_1 p_2 \cdots p_r$ alakú ($n \geq 3$, $k \geq 0$, $r \geq 0$), ahol $p_1, p_2, \ldots, p_r$ különböző Fermat-féle prímek. (Egy

p prímszám Fermat-féle, ha $p = 2^{2^t} + 1$ alakú, ahol $t \in \mathbf{N}$).

Megjegyzés. Mivel egy adott szög 2^k-ad része szögfelezéssel mindig szerkeszthető, ezért a bizonyításban feltehetjük, hogy $n(\geq 3)$ páratlan egész, továbbá a tétel bizonyítását az alábbi tételek (részállítások) bizonyítására bontjuk.

2. Tétel. Legyen $n = p \geq 3$ prímszám. A p oldalú szabályos sokszög akkor és csak akkor szerkeszthető euklideszi szerkesztéssel, ha p Fermat-féle prím.

3. Tétel. Legyen $n = p_1 p_2 \cdots p_r$, ahol $p_1, p_2, \ldots, p_k$ különböző páratlan prím és $r \geq 2$. Az n-oldalú szabályos sokszög akkor és csak akkor szerkeszthető euklideszi szerkesztéssel, ha $p_1, p_2, \ldots, p_r$ Fermat-féle prímek.

4. Tétel. Legyen p páratlan prím. A szabályos p^2 oldalú sokszög nem szerkeszthető euklideszi szerkesztéssel.

5. Tétel. Legyen n páratlan és $p^2 \mid n$, ahol $p \geq 3$ prím. Az n-oldalú szabályos sokszög nem szerkeszthető euklideszi szerkesztéssel.

A tételek bizonyításában felhasználjuk azt az ismert tételt, miszerint a $\binom{p}{k}$ binomiális együttható osztható p-vel, ha p prím és $0 < k < p$. Felhasználjuk továbbá az úgynevezett Schönemann—Eisenstein irreducibilitási kritériumot, mely kimondja: ha $f(x) = a_n x^n + \cdots + a_0$ egy egész együtthatós polinom és p egy prím, mely eleget tesz $p \nmid a_n$, $p \mid a_i$ $(i = 0, \ldots, n-1)$, $p^2 \nmid a_0$ feltételeknek, akkor $f(x)$ irreducibilis a racionális számtest felett.

2. tétel bizonyítása. Egy szabályos p oldalú (pl. egységsugarú körbe írt) sokszög szerkeszthetősége nyilvánvalóan ekvivalens olyan véges algoritmus megadásával, mellyel az $\alpha = \frac{2\pi}{p}$ szög szerkeszthető. Mivel $\alpha = \frac{2\pi}{p}$ szög akkor és csak akkor szerkeszthető, ha $\cos \frac{2\pi}{p}$ (ill. $\sin \frac{2\pi}{p}$) szerkeszthető, ezért vizsgálhatjuk az $\varepsilon(p) = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ komplex p-edik egységgyök szerkeszthetőségét. Ebben az esetben is indulhatunk a $K_0 = \{0, 1\}$ halmazból, azaz $\mathbf{T}_0 = \mathbf{Q}$. Az 1. tétel után tett megjegyzés szerint $\varepsilon(p)$ akkor és csak akkor szerkeszthető, ha $\varepsilon(p)$ zérushelye egy $\mathbf{Q}$ fölött irreducibilis 2^j-edfokú racionális együtthatós polinomnak. Tudjuk, hogy $\varepsilon(p)$ zérushelye az

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p+2} + \cdots + x + 1,$$

úgynevezett p-edik körosztási polinomnak, melynek $\mathbf{Q}$ fölötti irreducibilitása az alábbi módon igazolható. Helyettesítsünk x helyére $y + 1$-et, ekkor

$$f(x) = f(y+1) = \frac{(y+1)^p - 1}{y} =$$

$$= y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-2} y + \binom{p}{p-1}.$$

Mivel $p \mid \binom{p}{1}, p \mid \binom{p}{2}, \ldots, p \mid \binom{p}{p-1}$, de $p^2 \nmid \binom{p}{p-1}$, ezért az említett Schönemann—Eisenstein-tétel szerint $f(y+1)$ (és vele együtt $f(x)$ is) irreducibilis $\mathbf{Q}$ fölött. Így a szerkeszthetőség szükséges és elégséges feltétele ha $p-1 = 2^j$, azaz $p = 2^j + 1$, ahol $j \in \mathbf{N}$. Mivel $p = 2^j + 1$ prím, ezért j csak $j = 2^t$ ($t \in \mathbf{N}$) alakú lehet, mert ellenkező esetben p nem prím (ugyanis $j = 2^t m$, $m \geq 3$ páratlan esetben $2^{2^t} + 1 \mid (2^{2^t})^m + 1$).

3. Tétel bizonyítása. Legyenek $p_1, p_2, \ldots, p_r$ különböző Fermat-féle prímek ($r \geq 2$). A 2. Tétel szerint a $p_1, p_2, \ldots, p_r$ oldalú szabályos sokszögek szerkeszthetők, azaz az

$$\alpha_1 = \frac{2\pi}{p_1}, \quad \alpha_2 = \frac{2\pi}{p_2}, \quad \ldots, \quad \alpha_r = \frac{2\pi}{p_r}$$

szögek szerkeszthetők. Állítjuk, hogy léteznek olyan $k_1, k_2, \ldots, k_r$ egész számok, melyekre

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_r\alpha_r = \alpha,$$

ahol $\alpha = \frac{2\pi}{p_1 p_2 \cdots p_r}$, azaz az $n = p_1 p_2 \cdots p_3$ oldalú szabályos sokszög szerkeszthetőségével ekvivalens α szög szerkeszthető. Ugyanis a helyettesítéseket elvégezve és a $q_j = \frac{\prod_{i=1}^{r} p_i}{p_j}$ jelölést bevezetve a

$$q_1 k_1 + q_2 k_2 + \cdots + q_r k_r = 1$$

lineáris diofantoszi egyenletet kapjuk, mely $(q_1, q_2, \ldots, q_r) = 1$ miatt mindig megoldható.

A tétel állításának szükséges részét indirekt módon igazoljuk. Tegyük fel, hogy az $n = p_1 p_2 \cdots p_r$ oldalú szabályos sokszög szerkeszthető és pl. p_1 nem Fermat-féle prím. Ekkor a megszerkesztett n-oldalú szabályos sokszög minden $p_2 p_3 \cdots p_r$-edik csúcsát összekötve egy p_1 (nem Fermat-féle prím) oldalú szabályos sokszöget kapunk, mely ellentmond a 2. Tételnek.

4. Tétel bizonyítása. Az 1. Tétel szerint elegendő megmutatni, hogy az

$$\varepsilon(p^2) = \cos\frac{2\pi}{p^2} + i\sin\frac{2\pi}{p^2}$$

komplex szám zérushelye egy nem 2^j-edfokú, $\mathbf{Q}$ fölött irreducibilis racionális együtthatós polinomnak. Tudjuk, hogy $\varepsilon(p^2)$ zérushelye az

$$f(x) = \frac{x^{p^2} - 1}{x^p - 1} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$$

polinomnak, melynek $\mathbf{Q}$ fölötti irreducibilitása az alábbi módon igazolható. Helyettesítsünk x helyébe $y+1$-et, ekkor

$$f(x) = f(y+1) = \frac{(y+1)^{p^2}-1}{(y+1)^p-1} = (y+1)^{p(p-1)} + \\ + (y+1)^{p(p-2)} + \cdots + (y+1)^p + 1 = y^{p(p-1)} + \cdots + p,$$

és

$$(y+1)^p - 1 = y^p + \binom{p}{1} y^{p-1} + \cdots + \binom{p}{p-1} y = y^p + ph_1(y),$$

ahol $h_1(y)$ egy egész együtthatós, $p-1$-edfokú polinom. Mivel

$$(y+1)^{p^2} = (y^p + ph_1(y) + 1)^p,$$

így

$$(y+1)^{p^2} - 1 = ((y^p+1) + ph_1(y))^p - 1 = (y^p+1)^p + ph_2(y) - 1 = \\ = y^{p^2} + ph_3(y),$$

ahol $h_2(y)$ és $h_3(y)$ egész együtthatós polinomok, melyek fokszáma $p(p-1)$. Ezért

$$f(x) = f(y+1) = \frac{(y+1)^{p^2}-1}{(y+1)^p-1} = \frac{y^{p^2} + ph_3(y)}{y^p + ph_1(y)} = \\ = y^{p^2-p} + p\frac{h_3(y) - y^{p^2-p}h_1(y)}{y^p + ph_1(y)} = \\ = y^{p^2-p} + ph_4(y)$$

ahol $h_4(y)$ alkalmas egész együtthatós, p^2-p-1-edfokú polinom. Mivel $f(y+1) = y^{p(p-1)} + \cdots + p$ is igaz, ezért az ismert Schönemann—Eisenstein-tétel szerint $f(y+1)$ (és vele együtt $f(x)$ is) irreducibilis $\mathbf{Q}$ fölött, de $p^2 - p \neq \neq 2^j$, mert p páratlan prím.

5. Tétel bizonyítása. Indirekt bizonyítást választva, tegyük fel, hogy az $n = p^2 m$ oldalú szabályos sokszög szerkeszthető (p páratlan prím és $m \geq 3$). Ekkor a megszerkesztett n oldalú szabályos sokszög minden m-edik csúcsát összekötve egy p^2 oldalú szabályos sokszöget kapunk, mely ellentmond a 4. Tételnek.

A 2—5. Tételekből Gauss tétele már következik.

Végezetül választ adunk arra a kérdésre, hogy mely egész fokos szögek szerkeszthetők euklideszi szerkesztéssel.

6. Tétel. $n°$ $(n \in N)$ akkor és csak akkor szerkeszthető euklideszi szerkesztéssel, ha $3 \mid n$.

Bizonyítás. Gauss tétele szerint a szabályos ötszög szerkeszthető, mert $5 = 2^{2^1} + 1$ alakú Fermat-féle prím, azaz $\frac{360°}{5} = 72°$ szerkeszthető. Mivel $60°$ könnyen szerkeszthető az ismert módon, ezért a kettő különbsége — $70° - 60° = 12°$ — is szerkeszthető. $12°$-ból szögfelezéssel szerkeszthető a $6°$, ill. $3°$. $3°$ ismeretében $n = 3k$ esetén $n° = (k3)°$ $(k \in \mathbf{N})$ nyilván szerkeszthető.

Ha $n = 3k \pm 1$ alakú természetes szám és $n°$ szerkeszthető lenne, akkor — $(k3)°$ szerkeszthetősége miatt — $1°$ is szerkeszthető lenne, amiből a $20 \cdot 1° = 20°$ szerkeszthetősége következne, ami ellentmond a szögharmadolás témában bizonyított állításnak.

Irodalom

[1] FUCHS LÁSZLÓ: Algebra. *Tankönyvkiadó*, Bp., 1992.

[2] SAIN MÁRTON: Nincs királyi út. *Gondolat Kiadó*, Bp., 1986.

[3] SZENDREI JÁNOS: Algebra és számelmélet. *Tankönyvkiadó*, Bp., 1975.

[4] SZŐKEFALVI NAGY GYULA: Geometriai szerkesztések elmélete. *Akadémiai Kiadó*, Bp., 1968.