

A GEOMETRIAI SZERKESZTHETŐSÉG ALGEBRAI ELMÉLETE.

Klukovits Lajos

TTIK Bolyai Intézet

20013. április 24. május 8.

A szerkesztés fogalma szemléletesen.

A naív definíció.

- 1 Mindaz, ami körzővel és egyélű vonalzóval végrehajtható.
- 2 Az, hogy e fogalom tartalma pontosan mi, az az idők folyamán jelentősen változott.
- 3 Az egyik legelső megfogalmazás Euklidesz posztulátumaiban olvasható, de a fogalom az Euklideszt megelőző időből származik.

A görök klasszikus kor.

- 1 Kiterjedt vizsgálatok folytak, amelyek közül többet ismerünk.
- 2 A fennmaradt anyagokból világos, hogy a szerkesztés fogalmán valamiféle **elvi konstrukciót** értettek.
- 3 Ennek köszönhetően a három nevezetes és sokak által tárgyalt probléma mindegyikére számos megoldás született.

A szerkesztés modern fogalma.

XVIII. század.

- Ekkor alakult ki a ma használt fogalom.
- Történetileg téves ezért az „euklideszi szerkesztés” elnevezés.
- A lényeges változásnak tudható be, hogy ebben az (utóbbi) értelemben a híres ókori problémák egyike sem oldható meg.
- Hangsúlyozni kell, hogy itt „szerkeszthetőségről”, tehát egy „elvi kérdésről” van szó, azaz NEM szerkesztési algoritmusokról.
- Például ismerjük az összes olyan n természetes számot, amelyekre a szabályos n -szög megszerkeszthető, de igen kevés esetben ismerjük a konkrét szerkesztési eljárást.
- Első pillantásra meglepő, hogy **a szerkeszthetőségi problémák algebrai eszközökkel eredményesen tárgyalhatók Galois nyomán.**

A szerkeszthetőség modern fogalma 1.

Definíció. A szerkesztés megengedett lépései

- 1 két adott vagy már megszerkesztett ponton át egyenes húzása,
- 2 adott vagy már megszerkesztett pont körül adott vagy már megszerkesztett pontok által meghatározott távolsággal, mint sugárral kör rajzolása,
- 3 már megrajzolt körök ill. egyenesek metszéspontjainak meghatározása.

1. Megjegyzés.

Az előbbi föltételeknek megfelelő szerkesztéseket szokás ma **euklideszi szerkesztésnek** nevezni.

A szerkeszthetőség modern fogalma 2.

2. Megjegyzés.

Világos, hogy csak pontok, egyenesek és körök szerkeszthetők, sőt elég csak a pontok szerkesztésével foglalkozni, hiszen

- 1 egy egyenest annak két különböző pontja meghatározza,
- 2 minden kört meghatároz legfeljebb három pont: a középpont, valamint azon két pont, amelyek távolsága a kör sugara.

Definíció.

A sík egy H ponthalmazából *közvetlenül megszerkeszthetők*:

- 1 H pontjai,
- 2 két olyan egyenes (kör) metszéspontja, amelyeket két-két (három-három) H -beli pont határoz meg,
- 3 egy olyan egyenes és kör metszéspontja(i), amelyek eleget tesznek az előbbi feltételeknek.

A szerkeszthetőség modern fogalma 3.

Definíció.

Azt mondjuk, hogy a sík egy pontja *megszerkeszthető a H halmazból*, ha eleme valamely $i \in \mathbb{N}_0$ -ra H_i -nek, ahol

- 1 $H_0 = H$,
- 2 és minden $i \in \mathbb{N}$ -re H_i jelöli a H_{i-1} halmazból közvetlenül megszerkeszthető pontok halmazát.
- 3 Ekkor azt is mondhatjuk, hogy a kérdéses pont *i -lépésben szerkeszthető H -ból*.
- 4 Világos, hogy $H = H_0 \subseteq H_1 \subseteq H_2 \subseteq \dots$
- 5 Mindig fölteszük, hogy $|H| \geq 2$ (egyetlen pontból ugyanis nem szerkeszthető újabb pont).

Az algebrai megközelítés 1.

Két út.

- 1 Koordinátageometriai: a pontokhoz valós számpárokat rendelünk,
- 2 komplex számokat rendelünk a pontokhoz.

Megjegyzések.

A $|H| \geq 2$ feltétel jelentése most az, hogy

- 1 megszerkeszthető egy derékszögű koordináta-rendszer,
- 2 két ponthoz a 0, ill. az 1 számokat rendelhetjük.

Az algebrai megközelítés 2.

Megjegyzés.

Fölteszük, hogy az előforduló testek számtestek, azaz a $\mathbb{C}$ test résztestei.

Definíció.

Az $L|K$ testbővítés *négyzetgyökbővítés*, ha léteznek olyan $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_t = L$ testek, hogy minden $1 \leq i \leq t$ -re K_i a K_{i-1} -nek valamely $x^2 - c_i \in K_{i-1}[x]$ irreducibilis polinom egy gyökével való bővítése, vagyis

$$K_i = K_{i-1}(\sqrt{c_i}), \quad c_i \in K_{i-1}, \quad \sqrt{c_i} \notin K_{i-1}.$$

A négyzetgyökbővítések két tulajdonsága.

- 1 Ha $M|L$ és $L|K$ négyzetgyökbővítések, akkor $M|K$ is az.
- 2 Ha $L'|K$ és $L''|K$ négyzetgyökbővítések és $L = [L' \cup L'']$, akkor $L|K$ is négyzetgyökbővítés.

Az algebrai megközelítés 3.

1. Tétel.

Legyen $K \subseteq \mathbb{C}$ (szám)test. A $z \in \mathbb{C}$ pontosan akkor van benne K valamely négyzetgyökbővítésében, ha megkapható K -beli elemekből (számokból) az $+$, $-$, $\cdot$, $^{-1}$ (a négy alapművelet) és a négyzetgyökvonás véges számú alkalmazásával.

2. Tétel.

Legyen H a Gauss-féle számsík pontjai egy halmaza és $0, 1 \in H$. Jelölje K a H -beli pontok (derékszögű) koordinátái, míg $\bar{K}$ a H -beli számok és konjugáltjaik által generált testet. Tetszőleges $z \in \mathbb{C}$ -re a következő állítások ekvivalensek.

- 1. A z pont megszerkeszthető H -ból.
- 2. A z pont koordinátái benne vannak K egy valós négyzetgyökbővítésében.
- 3. A z benne van $\bar{K}$ egy négyzetgyökbővítésében.

Polinom gyökeinek szerkeszthetősége 1.

3. Tétel.

Legyen $K(\subseteq \mathbb{C})$ test, továbbá $f \in K[x]$ irreducibilis polinom.

- 1. Ha f valamely gyöke benne van K egy négyzetgyökbővítésében, akkor f Galois-csoportjának rendje 2-hatvány.
- 2. Megfordítva, ha az f polinom Galois-csoportjának rendje 2-hatvány, akkor minden gyöke eleme K egy alkalmas négyzetgyökbővítésének.

1. Következmény.

Legyen $H \subseteq \mathbb{C}$, és $\bar{K}$ a H -beli számok és konjugáltjaik által generált résztest $\mathbb{C}$ -ben. Egy $z \in \mathbb{C}$ pontosan akkor szerkeszthető meg H -ból, ha z algebrai $\bar{K}$ fölött, és minimálpolinomjának $\bar{K}$ fölötti Galois-csoportja 2-hatvány rendű.

Polinom gyökeinek szerkeszthetősége 2.

2. Következmény.

Legyen $H \subseteq \mathbb{C}$, és $\bar{K}$ a H -beli számok és konjugáltjaik által generált résztest $\mathbb{C}$ -ben. Ha $a \in \mathbb{C}$ megszerkeszthető H -ból, akkor z algebrai $\bar{K}$ fölött, és minimálpolinomjának fokszáma 2-hatvány.

Nevezetes ókori szerkesztési feladatok.

- 1. E feladatokat először a görögök fogalmazták meg a Kr.e. V. században. Eredetük nem ismert pontosan, de számos legenda ismert róluk.
- 2. Számos teljes és részleges megoldás született rájuk e korban, de akkor mást értettek szerkesztésen. Például gond nélkül „szerkesztettek” térbeli parabolákat.

Az ókori szerkesztési feladatok.

Körnégyzögesítés.

- 1. Szerkesszünk egy adott sugarú körrel azonos területű négyzet.
- 2. Legyen az adott kör sugarának két végpontja 0 és 1.
- 3. A feladat azt jelenti, hogy a $H = \{0, 1\}$ -ből egy olyan a hosszúságú szakaszt kell szerkesztenünk, amelyre $a^2 = \pi$, azaz $a = \sqrt{\pi}$.
- 4. Világos, hogy most $\bar{K} = \mathbb{Q}$.
- 5. Mivel az $a = \sqrt{\pi}$ nem algebrai $\mathbb{Q}$ fölött (ugyanis a π transzcendens szám, amit a XIX. század végén igazoltak), **a feladat nem oldható meg.**
- 6. **Megjegyzés.** E problémára az ókorban kizárólag rész megoldások születtek, csak bizonyos ún. „holdacskákat”, két körív által határolt alakzatokat tudtak „négyzögeíteni”, kört nem.

Az ókori szerkesztési feladatok.

Kockakettőzés.

- Ez az ún. **(Dél-osi probléma)**
- Megszerkesztendő egy adott kockánál kétszer nagyobb térfogatú kocka (éle).
- Legyen az adott kocka egy oldalának két végpontja 0 és 1.
- A feladat azt tűzi ki, hogy szerkesszük meg $H = \{0, 1\}$ -ből a $\sqrt[3]{2}$ -t.
- Az előbbihez hasonlóan $\overline{K} = \mathbb{Q}$. Mivel a $\sqrt[3]{2} \notin \mathbb{Q}$ fölötti minimálpolinomja $x^3 - 2$, s ennek fokszáma nem 2-hatvány, **e feladat sem oldható meg.**
- Megjegyzés.** Az ókorban számos szellemes megoldást adtak meg **DE AKKOR MÁS VOLT A SZERKESZTÉS DEFINÍCIÓJA.**

Az ókori szerkesztési feladatok.

Szögharmadolás.

- Szerkesszünk meg egy olyan szöget, amely egyharmada egy adott szögnek.
- A válasz ismételten nem.
- Az egyszerűség kedvéért azt mutatjuk meg, hogy a 60° -os szög nem harmadolható, azaz nem szerkeszthető 20° -os szög.
- A 20° -os szög szerkeszthetősége egyenértékű azzal, hogy a $H = \{0, 1\}$ -ből megszerkeszthető a $\cos 20^\circ$ hosszúságú szakasz.
- Mivel $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, a $\cos 20^\circ$ gyöke a $4x^3 - 3x - \frac{1}{2}$ polinomnak, vagyis a $8x^3 - 6x - 1$ (irreducibilis) polinomnak.
- A harmadfokú irreducibilis polinomok gyökei azonban nem szerkeszthetők.
- Megjegyzés.** Eliszi Hippiasz Quadratrixe.

A szabályos n -szög szerkeszthetősége.

Mely $n \in \mathbb{N}$ -re szerkeszthető szabályos n -szög? 1.

- Legyen az $n > 2$ természetes szám prímszámra bontása $n = p_1^{k_1} \dots p_s^{k_s}$, ahol $p_1, \dots, p_s$ különböző prímek.
- A kiindulási halmaz most is a $H = \{0, 1\}$, így $\overline{K} = \mathbb{Q}$.
- szabályos n -szög szerkeszthető $\iff$ primitív n -edik egységyökök szerkeszthető,**
- primitív n -edik egységyökök szerkeszthető $\iff \forall i$ -re $p_i^{k_i}$ -adik egységyökök szerkeszthető.**
- Így azt a kérdést kell megválaszolni, hogy mikor szerkeszthető p^k -adik primitív egységyökök.

A szabályos n -szög szerkeszthetősége.

Mely $n \in \mathbb{N}$ -re szerkeszthető szabályos n -szög? 2.

- Tekintsük a

$$\Phi_{p^k} = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = \frac{(x^{p^{k-1}})^p - 1}{x^{p^{k-1}} - 1} = x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \dots + x^{p^{k-1}} + 1$$

ún. p^k -adik körosztási polinomot.

- Világos, hogy e polinom gyökei éppen a p^k -adik primitív egységyökök, és irreducibilis $\mathbb{Q}$ fölött.
- Legyen ε primitív p^k -adik egységyök. Mivel $\mathbb{Q}(\varepsilon)$ test tartalmazza az összes p^k -adik egységyököket, az a Φ_{p^k} polinom fölbonthatási teste.
 $|G(\Phi_{p^k}, \mathbb{Q})| = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = p^{k-1}(p-1),$
- azaz a polinom Galois-csoportjának rendje $p^{k-1}(p-1)$.

A szabályos n -szög szerkeszthetősége.

Mely $n \in \mathbb{N}$ -re szerkeszthető szabályos n -szög? 3.

Kérdés: $p^{k-1}(p-1)$ mikor (mely p, k -ra) 2-hatvány?

Mely $n \in \mathbb{N}$ -re szerkeszthető szabályos n -szög? 4.

- 1 Ha $p = 2$, vagy
- 2 $k = 1$ és $p - 1 = 2^t$ $t > 1$, azaz 2-hatvány.
- 3 Ez utóbbi pontosan akkor teljesül, ha $p = 2^{2^m} + 1$, azaz p egy ún. Fermat-prím.

Gauss tétele.

A szabályos n -szög akkor és csak akkor szerkeszthető, ha $n = 2^k p_1 \dots p_t$, ahol a $p_1, \dots, p_t$ különböző Fermat-prímek.

Amire Gauss nagyon büszke volt.

Eljárást adott a szabályos 17-szög szerkesztésére.

Mit tudunk a Fermat-prímekről a XIX. század közepéig.

Fermat sejtése.

Az

$$F_n = 2^{2^n} + 1$$

ún. alakú **Fermat-számok** minden $n \in \mathbb{N}_0$ -ra prímek.

Már Fermat tudta.

Ha $0 \leq n \leq 4$, akkor F_n prím. Ezek rendre

3, 5, 17, 257, 65537.

Euler.

$$F_5 = 2^{32} + 1$$

összetett szám, osztható ugyanis 641-gyel.

Mit tudunk a Fermat-prímekről 2000-ben?

Szemelvények.

- 1 F_n összetett szám minden $5 \leq n < 24$ -re és még néhány további n -re.
- 2 Egy rekorder F_{23471} , amelynek több mint 10^{7000} decimális jegye van, és osztható $2 \cdot 2^{23473} + 1$ -gyel.
- 3 Nem ismeretes újabb prím az F_n , ($n > 4$) számok között.
- 4 F_{14} -ről tudjuk, hogy összetett, de nem ismerjük egyetlen prímosztóját sem.
- 5 Csak $n = 5, 6, 7, 8, 9, 11$ -re ismert F_n teljes prímfölbontása.
- 6 Ha $n = 5, 6, 7$, akkor F_n -nek pontosan két prímosztója van.