1. Geometriai szerkeszthetőség

Szerkeszthetetlenség csak vonalzóval.

6.8.1. Állítás
Kockás papíron csak vonalzóval *nem* tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok
A négyzetrács csúcspontjai.

Megengedett lépések

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.

(2) Két megszerkesztett egyenes metszéspontjának kijelölése.

Ezt a kétféle lépést véges sokszor szabad alkalmazni. A végén a keresett pontot kell megkapnunk (2) típusú lépéssel.

A feladat algebraizálása.

A négyzetrács ad egy természetes *koordinátarendszert*: $(0, 0)$ és $(1, 0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p, q) pontját *racionálisnak*, ha $p, q \in \mathbb{Q}$. Minden egyenest megadhatunk egyenlettel:

$ax + by + c = 0$, ahol a, b, c valós számok.

Hívjunk egy egyenest *racionálisnak,* ha $a, b, c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz, a (2) lépésben két racionális egyenesből racionális pont lesz, mert mindkétszer lineáris egyenletrendszert kell megoldani. Ezért az eljárásban végig minden egyenes és pont racionális. Azaz csak racionális pont lehet szerkeszthető. A keresett $(1/2, \sqrt{3}/2)$ nem racionális pont, így *nem szerkeszthető.* $\square$

Euklideszi szerkesztés.

Kiinduló adatok
Pontok, egyenesek, körök, szakaszok, stb. a síkon.

További megengedett lépések

(3) Két adott vagy megszerkesztett pont körzőnyílásba vétele, és ezzel a sugárral egy adott vagy megszerkesztett pont körüli kör rajzolása.

(4) Adott vagy megszerkesztett kör és egyenes metszéspontjainak kijelölése.

(5) Két adott vagy megszerkesztett kör metszéspontjainak kijelölése.

Szerkesztés: az ötféle lépést véges sokszor alkalmazzuk.

Az euklideszi szerkesztés algebraizálása.

Felveszünk egy *koordinátarendszert* úgy, hogy $(0,0)$ és $(1,0)$ adott vagy szerkeszthető legyen.

A pontokat (p,q) alakban adjuk meg, ahol $p,q \in \mathbb{R}$. Minden egyenest megadhatunk egyenlettel:

$ax+by+c=0$, ahol a,b,c valós számok.

Minden kört megadhatunk egyenlettel:

$(x-p)^2+(y-q)^2=r^2$, ahol p,q,r valós számok.

Feltesszük, hogy a kiinduló adatok csak pontok. Ezek koordinátái és $\mathbb{Q}$ által generált test az *alaptest*, jele K_0. Az $(1)-(5)$ típusú lépések során kapott új alakzat „koordinátái" minden lépésnél egy testbővítést adnak. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ *testláncot* eredményez.

Szerkeszthető számok.

6.8.3. Lemma
A K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0<d\in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei *algebraiak* K_0 fölött, és *fokuk 2-hatvány.*

Bizonyítás
Másodfokú egyenletet kell megoldani. □

6.8.5. Definíció
Az $r\in\mathbb{R}$ *szerkeszthető szám*, ha $(r,0)$ szerkeszthető pont.

Beláttuk
Minden szerkeszthető szám foka K_0 fölött 2-hatvány.

Kockakettőzés.

6.8.6. Probléma
Kockakettőzés, vagy *Déloszi Probléma*: szerkesztendő egy olyan kocka élhossza, aminek *térfogata* egy adott élhosszúságú kocka térfogatának *kétszerese*.

Megoldás
Adott a síkon az első kocka élhossza, vagyis egy szakasz. Vegyük föl a koordinátarendszert úgy, hogy $(0,0)$ és $(1,0)$ a megadott szakasz két végpontja legyen. Az alaptest tehát $K_0=\mathbb{Q}(0,0,1,0)=\mathbb{Q}$. A keresett szakasz hossza $\sqrt[3]{2}$, azaz szerkesztendő $(\sqrt[3]{2},0)$. Az a kérdés tehát, hogy $\sqrt[3]{2}$ szerkeszthető szám-e $\mathbb{Q}$ fölött. *Nem szerkeszthető*, mert foka 3, ami nem 2-hatvány. □

Körnégyszögesítés.

6.8.7. Probléma
Körnégyszögesítés: szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Megoldás
Adott a síkon a kör sugara, vagyis egy szakasz. Vegyük föl a koordinátarendszert úgy, hogy $(0, 0)$ és $(1, 0)$ a megadott szakasz két végpontja legyen. Az alaptest tehát $K_0 = \mathbb{Q}(0, 0, 1, 0) = \mathbb{Q}$. A kör területe ekkor π, tehát a keresett szakasz hossza $\sqrt{\pi}$. Az a kérdés tehát, hogy a $\sqrt{\pi}$ szerkeszthető szám-e $\mathbb{Q}$ fölött. *Nem szerkeszthető*, mert $\sqrt{\pi}$ transzcendens szám. Mert ha algebrai lenne, akkor a négyzete, π is algebrai lenne. (Lindemann analízis-tételét használtuk föl.) □

Szögharmadolás.

6.8.8. Probléma
Szögharmadolás: szerkesszük meg egy adott szög harmadát.

Megoldás
Mivel $60°$ szerkeszthető az egységszakaszból kiindulva, elég belátni, hogy 20 fokos szög nem szerkeszthető. Azaz, hogy a $\cos(20°)$ szám nem szerkeszthető $\mathbb{Q}$ fölött.
HF: minimálpolinomja $x^3 - (3/4)x - (1/8)$ (5.10.15. Feladat). Ezért $\mathbb{Q}$ fölött $\cos(20°)$ harmadfokú, így *nem szerkeszthető*. □

20 fokos szög szerkesztése = szabályos 18-szög szerkesztése.
Jobb $\cos(20°)$ helyett $\varepsilon = \cos(20°) + i\sin(20°)$-ot nézni! Ugyanis ε minimálpolinomja $\Phi_{18}(x)$, ezért foka $\varphi(18) = 6$.
Hogyan ad ez információt a $\cos(20°)$ fokára?

$\cos(2\pi/n)$ **foka.**

Láttuk: $\varepsilon = \cos(20°) + i\sin(20°)$ foka $\mathbb{Q}$ fölött $\varphi(18) = 6$.
Nyilván $\varepsilon^{-1} = \overline{\varepsilon} = \cos(20°) - i\sin(20°) \in \mathbb{Q}(\varepsilon)$, és így $\cos(20°) = (\varepsilon + \overline{\varepsilon})/2 \in \mathbb{Q}(\varepsilon)$, azaz $\mathbb{Q}\big(\cos(20°)\big) \leq \mathbb{Q}(\varepsilon)$.
Továbbá $\big(i\sin(20°)\big)^2 = \cos(20°)^2 - 1 \in \mathbb{Q}\big(\cos(20°)\big)$, és így $\mathbb{Q}(\varepsilon)$ foka $\mathbb{Q}\big(\cos(20°)\big)$ fölött 1 vagy 2 (hiszen $\sqrt{\cos(20°)^2 - 1}$-gyel való bővítéssel kapható).
A $\mathbb{Q} \leq \mathbb{Q}\big(\cos(20°)\big) \leq \mathbb{Q}(\varepsilon)$ láncból $\mathrm{gr}_{\mathbb{Q}}\big(\cos(20°)\big) = 3$ vagy 6. Egyik sem 2-hatvány. □

Ez nyilván általánosítható, azaz beláttuk:

6.8.10. Állítás
Ha $n \geq 1$, akkor $\mathrm{gr}_{\mathbb{Q}}\big(\cos(2\pi/n)\big)$ értéke $\varphi(n)$, vagy $\varphi(n)/2$.

A pontos érték a 6.8.24. Feladatban olvasható.

Szabályos sokszögek szerkeszthetősége.

6.8.11. Tétel (félig bizonyítva)
Akkor és csak akkor szerkeszthető *szabályos n-szög*, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \dots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző *Fermat-prímek* (vagyis $2^{2^k} + 1$ alakú prímszámok).

Mivel $\cos(2\pi/n)$ foka $\varphi(n)$ vagy $\varphi(n)/2$, ha szerkeszthető szabályos n-szög, akkor $\varphi(n)$ 2-hatvány. A Fermat-prímes jellemzés elemi számelméleti gondolatmenet.
A megfordítás az alábbi tételből következik.

6.8.15. Tétel (NB)
Legyen α minimálpolinomja K_0 fölött t. Ha t *felbontási testének* foka K_0 fölött 2-hatvány, akkor α szerkeszthető.

2. Egyenletek megoldóképlete

A gyökképlet létezése.

Tanultuk
Másodfokú egyenletre gyökképlet: középiskolában.
Harmadfokú egyenlet: Cardano-képlet.
Negyedfokú egyenlet: van képlet, de bonyolult (Ferrari).

Gyökképlet: négy alapművelet, gyökvonás az együtthatókból.

6.9.7. Tétel (Abel-Ruffini, NB)
A legalább ötödfokú általános egyenletre *nincs* gyökképlet. Sőt, az $x^5 - 4x + 2 = 0$-ra sincs (vö. 6.6.15. Feladat).

Tehát *nem* arról van szó, hogy még nem találtuk meg a képletet, hanem arról, hogy a képlet *nem is létezik*.
A bizonyítás testbővítéseket használ, és az egyenlet „szimmetriáit” vizsgálja. Ez a Galois-elmélet kiindulópontja.