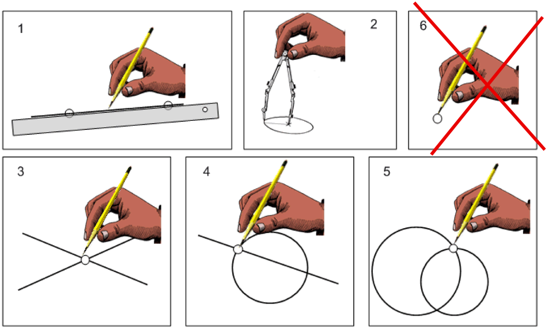
Geometriai szerkeszthetőség

Waldhauser Tamás
2015 őszi félév

Szerkesztési feladat

Adottak $P_1, \ldots, P_n$ pontok, ezekből szeretnénk egy Q pontot megszerkeszteni.



Szerkesztési lépések

Ha A, B, C, D már meg van szerkesztve akkor egy új E pontot szerkeszthetünk

- az AB és CD egyenesek metszéspontjaként,
- az AB egyenes és a C középpontú, D-n átmenő kör (egyik) metszéspontjaként, vagy
- az A középpontú B-n átmenő kör és a C középpontú, D-n átmenő kör (egyik) metszéspontjaként.

A szerkesztés menete

$$\begin{aligned}\{P_1, P_2, \ldots, P_n\} &\rightsquigarrow \{P_1, P_2, \ldots, P_n, Q_1\} \rightsquigarrow \\ &\rightsquigarrow \{P_1, P_2, \ldots, P_n, Q_1, Q_2\} \rightsquigarrow \cdots \\ &\rightsquigarrow \{P_1, P_2, \ldots, P_n, Q_1, Q_2, \ldots, Q_\ell\} \quad Q_\ell = Q.\end{aligned}$$

Megjegyzések

- A megadott $P_1, \ldots, P_n$ pontok *konkrét* pontok a síkon, pl. egy konkrét háromszög magasságpontját akarjuk megszerkeszteni. Amennyiben olyan eljárást akarunk adni, ami pl. tetszőleges háromszög magasságpontjának megszerkesztésére alkalmas, akkor *paraméteres* szerkesztési feladatról beszélünk. Az utóbbi nyilván nehezebb feladat: ha általános eljárást tudunk adni, akkor az minden speciális esetben is működni fog. Fordítva ez nem igaz, nincs például általános szerkesztési eljárás tetszőleges szög harmadolására, de ettől még speciális esetekben (pl. 90°) tudunk szöget harmadolni.
- Mindig feltesszük, hogy legalább két pont meg van adva ($n \geq 2$).
- Két pontból már lehet egy sűrű ponthalmazt szerkeszteni, ezért nem jelent megszorítást, hogy megtiltottuk, hogy „csak úgy" segédpontokat vegyünk fel.
- Kört csak adott középpontból adott kerületi ponton keresztül rajzolhatunk (euklideszi körző); nem lehet egy adott szakaszt (mint sugarat) körzőnyílásba venni, és máshol kört rajzolni vele. HF: Mutassuk meg, hogy ez sem jelent megszorítást!

Algebraizálás

Vegyünk fel egy derékszögű koordinátarendszert, amelynek origója P_1, és az első tengelyen az egységnek a P_2 pont felel meg. Ezután pontok helyett számokat szerkesztünk: minden valós szám megfelel az első tengely (mint valós számegyenes) egy pontjának. HF: Bizonyítsuk be, hogy egy $Q = (x, y)$ pont akkor és csak akkor szerkeszthető meg, ha az x, y számok(nak megfelelő pontok az első tengelyen) megszerkeszthetőek!

Szerkesztési feladat

Adottak $c_1, \ldots, c_n$ valós számok, ezekből szeretnénk egy α számot megszerkeszteni.

Szerkesztési lépések

Ha $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{R}$ már meg vannak szerkesztve akkor egy új $\alpha \in \mathbb{R}$ számot szerkeszthetünk

- az AB és CD egyenesek metszéspontjának egyik koordinátájaként,
- az AB egyenes és a C középpontú, D-n átmenő kör (egyik) metszéspontjának egyik koordinátájaként, vagy
- az A középpontú B-n átmenő kör és a C középpontú, D-n átmenő kör (egyik) metszéspontjának egyik koordinátájaként,

ahol $A = (a_1, a_2)\,, B = (b_1, b_2)\,, C = (c_1, c_2)\,, D = (d_1, d_2)$.

A szerkesztés menete

$$\begin{aligned}\{c_1, c_2, \dots, c_n\} &\rightsquigarrow \{c_1, c_2, \dots, c_n, \alpha_1\} \rightsquigarrow \\ &\rightsquigarrow \{c_1, c_2, \dots, c_n, \alpha_1, \alpha_2\} \rightsquigarrow \cdots \\ &\rightsquigarrow \{c_1, c_2, \dots, c_n, \alpha_1, \alpha_2, \dots, \alpha_\ell\} \quad \alpha_\ell = \alpha.\end{aligned}$$

Megjegyzés

A koordinátarendszer választása miatt a P_1 és P_2 pontok a 0 és 1 számoknak felelnek meg, tehát ez a két szám mindig adott.

A szerkesztés alapteste

A kiindulásul megadott $c_1, \dots, c_n$ számok által generált $K = \mathbb{Q}(c_1, \dots, c_n) \leq \mathbb{R}$ számtestet a szerkesztés *alaptestének* nevezzük. Ha paraméteres szerkesztési feladatról lenne szó, akkor $c_1, \dots, c_n$ (némelyike) nem konkrét számok, hanem $\mathbb{Q}$ feletti transzcendens elemek lennének.

HF: Mutassuk meg, hogy ha $0, 1, a, b$ adottak, akkor $a \pm b$, $a \cdot b$, $a/b\,(b \neq 0)$ és $\sqrt{a}\,(a \geq 0)$ megszerkeszthető!

Következmény

A K test elemei szerkeszthetőek, ezért feltehetjük, hogy kiindulási adatunk ez a test.

Tétel

Az alaptest nem függ a koordinátarendszer választásától.

Definíció

Az $L|K$ testbővítés *egyszerű négyzetgyökbővítés*, ha $\exists a \in K : L = K\left(\sqrt{a}\right)$.
Az $L|K$ testbővítés *négyzetgyökbővítés*, ha megkapható véges sok egyszerű négyzetgyökbővítés egymásutánjaként:

$$K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L \qquad\qquad T_{i+1} = T_i\left(\sqrt{a_i}\right), \text{ ahol } a_i \in T_i.$$

HF: Mutassuk meg, hogy $L|K$ akkor és csak akkor egyszerű négyzetgyökbővítés, ha $[L : K] \leq 2$!

Következmény

Négyzetgyökbővítés foka mindig kettőhatvány. (Fordítva ez általában nem igaz, de *normális* testbővítésekre igen.)

Tétel

Az α valós szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha létezik olyan $L|K$ négyzetgyökbővítés, melyre $\alpha \in L$.

Bizonyítás

$$\alpha \text{ szerkeszthető} \quad \overset{?}{\Longleftrightarrow} \quad \exists L : \alpha \in L \text{ és } L|K \text{négyzetgyökbővítés}$$

$\Longleftarrow$: Tfh. $K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L \ni \alpha$, $\quad T_{i+1}|T_i$ egyszerű $\sqrt{\ }$-bővítés.
Megmutatjuk i szerinti indukcióval, hogy T_i minden eleme szerkeszthető.

Kezdőlépés: $T_0 = K$ elemei eleve adottak.

Indukciós lépés: tfh. T_i elemei mind szerkeszthetőek.
Legyen $T_{i+1} = T_i\left(\sqrt{\gamma}\right)$, ahol $\gamma \in T_i$. Ekkor T_{i+1} elemei $a + b\sqrt{\gamma}$ $(a, b \in T_i)$ alakúak. Az indukciós feltevés szerint a, b, γ szerkeszthetőek, így $a + b\sqrt{\gamma}$ is (HF).

$\Longrightarrow$: Tfh. α megszerkeszthető ℓ lépésben: $K \rightsquigarrow \alpha_1 \rightsquigarrow \cdots \rightsquigarrow \alpha_\ell = \alpha$.
Legyen $T_i = K(\alpha_1, \ldots, \alpha_i)$. Megmutatjuk, hogy $T_{i+1}|T_i$ egyszerű $\sqrt{\ }$-bővítés.

Az α_{i+1} szám megkapható két kögyenes metszéspontjának egyik koordinátájaként, ahol mindkét kögyenest T_i-beli koordinátákkal rendelkező pontok határozzák meg.
Pl. legyen α_{i+1} az A kp.-ú B-n átmenő és a C kp.-ú, D-n átmenő kör metszéspontjának első koordinátája, ahol $A = (a_1, a_2)$, $B = (b_1, b_2)$, $C = (c_1, c_2)$, $D = (d_1, d_2)$ és $a_1, \ldots, d_2 \in T_i$. (A többi eset HF.)

Bizonyítás (folyt.)

$$\alpha \text{ szerkeszthető} \quad \overset{?}{\Longleftrightarrow} \quad \exists L : \alpha \in L \text{ és } L|K \text{négyzetgyökbővítés}$$

A két kör egyenlete:

$$(x-a_1)^2 + (y-a_2)^2 = (b_1-a_1)^2 + (b_2-a_2)^2 =: r^2$$
$$(x-c_1)^2 + (y-c_2)^2 = (d_1-c_1)^2 + (d_2-c_2)^2 =: s^2.$$

Vonjuk ki a két egyenletet egymásból:

$$(2x-a_1-c_1)(a_1-c_1) + (2y-a_2-c_2)(a_2-c_2) = s^2 - r^2.$$

Fejezzük ki ebből y-t: $y = px + q \ \ (p, q \in T_i)$, majd helyettesítsük ezt be valamelyik kör egyenletébe. Így egy másodfokú egyenletet kapunk T_i felett:

$$ux^2 + vx + w = 0 \ \ (u, v, w \in T_i).$$

Vagyis α_{i+1} gyöke az $f = ux^2 + vx + w \in T_i[x]$ polinomnak. Ezért $m_{\alpha_{i+1}, T_i} \mid f$, tehát $[T_{i+1} : T_i] = [T_i(\alpha_{i+1}) : T_i] \leq 2$, így $T_{i+1}|T_i$ egyszerű $\sqrt{\ }$-bővítés (HF).

Azt kaptuk, hogy a $K = T_0 \leq T_1 \leq \cdots \leq T_\ell =: L$ testtorony minden lépésében egyszerű $\sqrt{\ }$-bővítés történik, azaz $L \mid K$ $\sqrt{\ }$-bővítés, és $\alpha \in K(\alpha_1, \ldots, \alpha_\ell) = L$. $\square$

Következmény

Ha $\alpha \in \mathbb{R}$ szerkeszthető, akkor α algebrai K fölött, és $m_{\alpha,K}$ foka kettőhatvány.

Bizonyítás

$$
\begin{aligned}
\alpha \text{ szerkeszthető} \quad &\Longrightarrow \quad \exists L : \alpha \in L \text{ és } L|K \text{négyzetgyökbővítés} \\
&\Longrightarrow \quad \deg m_{\alpha,K} \mid [L:K] = 2^{\ell} \\
&\Longrightarrow \quad \deg m_{\alpha,K} = 2^{*}
\end{aligned}
$$

□

Megjegyzés

A fenti állítás megfordítása nem igaz: abból, hogy $\deg m_{\alpha,K}$ kettőhatvány még nem következik, hogy α szerkeszthető.
(Pl. $x^4 + 7x + 7$ gyökei nem szerkeszthetőek $\mathbb{Q}$ fölött.)

Tétel

Az α valós szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α algebrai K fölött, és $m_{\alpha,K}$ *felbontási testének* foka kettőhatvány.

Tétel (szögharmadolás)

Nem lehet adott szöghöz harmadakkora szöget szerkeszteni.

Bizonyítás

Ez egy paraméteres szerkesztési feladat; megmutatjuk, hogy nemcsak általános szögharmadolási eljárás nincs, de még olyan „ad hoc” eljárás sem, ami a 60°-os szög harmadát megszerkesztené. Ekkor $K = \mathbb{Q}$ és a megszerkesztendő szám $\alpha = \cos 20^\circ$. Node $m_{\alpha,K} = x^3 - \frac{3}{4}x - \frac{1}{8}$ foka nem kettőhatvány. □

Tétel (kockakettőzés)

Nem lehet adott kockához kétszerakkora térfogatú kockát szerkeszteni.

Bizonyítás

Igazából ez is paraméteres feladat; nézzük az egységkocka esetét. Ekkor $K = \mathbb{Q}$ és a megszerkesztendő szám $\alpha = \sqrt[3]{2}$. Node $m_{\alpha,K} = x^3 - 2$ foka nem kettőhatvány. □

Tétel (körnégyszögesítés)

Nem lehet adott körhöz vele azonos területű négyzetet szerkeszteni.

Bizonyítás

Nézzük az egységkör esetét. Ekkor $K = \mathbb{Q}$ és a megszerkesztendő szám $\alpha = \sqrt{\pi}$, ami még csak nem is algebrai K fölött. □

Ikerfeladatok

- Adott a derékszögű háromszög derékszögű csúcsból induló magassága és
  - a derékszögő csúcsból induló szögfelezője, vagy
  - egy másik csúcsból induló szögfelezője.

  Megszerkeszthető-e a háromszög?

- HF: Adott az egyenlő szárú háromszög beírt körének sugara és
  - a szára, vagy
  - az alapja.

  Megszerkeszthető-e a háromszög?

A szerkeszthetőség elméletét fel lehet építeni úgy is, hogy egy pontnak nem egy valós számpárt, hanem egy komplex számot feleltetünk meg.

Tétel

Az α komplex szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α algebrai K fölött, és $m_{\alpha,K}$ *felbontási testének* foka kettőhatvány.

Az egységkörbe írt szabályos n-szög akkor és csak akkor szerkeszthető meg, ha az $\varepsilon_1 = \operatorname{cis} \frac{2\pi}{n}$ komplex szám (primitív n-edik egységgyök) megszerkeszthető. Először az $m_{\varepsilon_1,\mathbb{Q}}$ polinomot, majd pedig ennek a felbontási testét fogjuk meghatározni.

Körosztási polinomok

Az n-edik *körosztási polinom* az a Φ_n polinom, amelynek gyökei éppen a primitív n-edik egységgyökök (mindegyik egyszeres gyök):

$$\Phi_n = \prod_{\substack{k=1,\dots,n \\ \mathrm{lnko}(k,n)=1}} (x - \varepsilon_k) .$$

(Itt $\varepsilon_k = \varepsilon_1^k = \operatorname{cis} \frac{2k\pi}{n}$.) Vegyük észre, hogy $\deg \Phi_n = \varphi(n)$.

Néhány példa körosztási polinomra

- $\Phi_1 = x - 1$
- $\Phi_2 = x - (-1) = x + 1$
- $\Phi_3 = \left(x - \operatorname{cis} \frac{2\pi}{3}\right)\left(x - \operatorname{cis} \frac{4\pi}{3}\right) = \frac{x^3-1}{x-1} = x^2 + x + 1$
- $\Phi_4 = (x - i)(x + i) = \frac{x^4-1}{(x-1)(x+1)} = x^2 + 1$
- $\Phi_5 = \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6 = \frac{x^6-1}{\Phi_1\Phi_2\Phi_3} = \frac{x^6-1}{x^4+x^3-x-1} = x^2 - x + 1$
- $\Phi_7 = \frac{x^7-1}{\Phi_1} = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\Phi_8 = \frac{x^8-1}{\Phi_1\Phi_2\Phi_4} = \frac{x^8-1}{x^4-1} = x^4 + 1$
- $\Phi_9 = \frac{x^9-1}{\Phi_1\Phi_3} = \frac{x^9-1}{x^3-1} = x^6 + x^3 + 1$
- $\dots$
- $\Phi_{105} = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1$

Tétel

$$\Phi_n = \frac{x^n - 1}{\prod\limits_{\substack{d|n \\ d<n}} \Phi_d}$$

Bizonyítás

A bizonyítandó egyenlőség azzal ekvivalens, hogy $x^n - 1 = \prod\limits_{d|n} \Phi_d$.

A bal oldali polinom gyökei éppen az n-edik egységgyökök (mindegyik egyszeres). A jobb oldali polinom gyökei ugyanezek, mert

$$\forall z \in \mathbb{C}: \quad z^n = 1 \iff d := o(z) \mid n.$$

□

Következmény

A körosztási polinomok egész együtthatósak.

Bizonyítás

Teljes indukcióval. Ha már tudjuk, hogy $\Phi_1, \ldots, \Phi_{n-1} \in \mathbb{Z}[x]$ (IH), akkor a fenti képlettel Φ_n kiszámítható, mint két egész együtthatós polinom hányadosa, így $\Phi_n \in \mathbb{Q}[x]$. Mivel a nevező főpolinom, a (maradékos) osztás elvégzésekor nem lépnek fel törtek, azaz $\Phi_n \in \mathbb{Z}[x]$. □

Tétel

A körosztási polinomok irreducibilisek $\mathbb{Q}$ felett.

Bizonyítás

Nehéz. Ha p prím, akkor $\Phi_p = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Vezessük be az $y = x - 1$ új határozatlant; ekkor a polinom így alakul:

$$\begin{aligned}
\Phi_p(y+1) &= \frac{(y+1)^p - 1}{(y+1)-1} \\
&= \frac{y^p + py^{p-1} + \binom{p}{2}y^{p-2} + \cdots + \binom{p}{p-2}y^2 + py + 1 - 1}{y} \\
&= y^{p-1} + py^{p-2} + \binom{p}{2}y^{p-3} + \cdots + \binom{p}{p-2}y + p.
\end{aligned}$$

Erre a polinomra pedig már alkalmazható a Schönemann–Eisenstein-féle irreducibilitási kritérium. □

Következmény

A primitív n-edik egységgyökök közös minimálpolinomja Φ_n, speciálisan $m_{\varepsilon_1,\mathbb{Q}} = \Phi_n$. (Tehát a primitív n-edik egységgyökök konjugáltak $\mathbb{Q}$ felett.) □

Tétel

A Φ_n polinom $\mathbb{Q}$ feletti felbontási teste $\mathbb{Q}(\varepsilon_1)$.

Bizonyítás

Definíció szerint Φ_n felbontási teste $L_{\Phi_n,\mathbb{Q}} = \mathbb{Q}(\varepsilon_1, \ldots)$, ahol a zárójelben az összes primitív n-edik egységgyököt fel kell sorolni. Az világos, hogy $L_{\Phi_n,\mathbb{Q}} \supseteq \mathbb{Q}(\varepsilon_1)$. A másik irányú tartalmazáshoz elég azt megfigyelni, hogy $\varepsilon_k = \varepsilon_1^k \in \mathbb{Q}(\varepsilon_1, \ldots)$, tehát minden n-edik egységgyök benne van a $\mathbb{Q}(\varepsilon_1)$ testben. $\square$

Tétel (Gauss 1801, Wantzel 1837)

A szabályos n-szög akkor és csak akkor szerkeszthető, ha az n prímfelbontásában fellépő páratlan prímek mind Fermat-prímek, és mindegyik első hatványon lép fel.

Bizonyítás

Mivel $m_{\varepsilon_1,\mathbb{Q}} = \Phi_n$ felbontási teste $\mathbb{Q}(\varepsilon_1)$, és $[\mathbb{Q}(\varepsilon_1) : \mathbb{Q}] = \deg m_{\varepsilon_1,\mathbb{Q}} = \varphi(n)$, a szabályos n-szög akkor és csak akkor szerkeszthető meg, ha $\varphi(n)$ kettőhatvány. Legyen n prímfelbontása $n = 2^k \cdot p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$, ahol $p_1, \ldots, p_t$ páratlan prímek. Ekkor $\varphi(n) = 2^{k-1} \cdot \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_t^{k_t})$. Ez a szorzat akkor és csak akkor lesz kettőhatvány, ha minden i-re $\varphi(p_i^{k_i}) = p_i^{k_i-1}(p_i - 1) = 2^*$. Ez pedig csak akkor lehetséges, ha $k_i = 1$ és $p_i = 2^* + 1$.

Tény

Ha 2^n+1 prím, akkor n kettőhatvány.

Fermat azt sejtette, hogy $F_n = 2^{2^n}+1$ mindig prím, de ez nem igaz: Euler észrevette, hogy $F_5 = 641 \cdot 6700417$. Minden további Fermat-szám, amit megvizsgáltak szintén összetettnek bizonyult. Tehát csak öt Fermat-prímet ismerünk:

- $F_0 = 2^1+1 = 3$ (szerk.: ókori görögök)
- $F_1 = 2^2+1 = 5$ (szerk.: ókori görögök)
- $F_2 = 2^4+1 = 17$ (szerk.: Gauss 1796, Erchinger ∼1800)
  $\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\right)$
- $F_3 = 2^8+1 = 257$ (szerk.: Richelot 1832)
- $F_4 = 2^{16}+1 = 65537$ (szerk.: Hermes 1894; 10 év, 200 oldal)

HF: Tegyük fel, hogy ismerjük a szabályos n-szög szerkesztésének menetét. Adjunk eljárást a szabályos $2n$-szög megszerkesztésére.

HF: Tegyük fel, hogy ismerjük a szabályos n-szög és a szabályos m-szög szerkesztésének menetét. Adjunk eljárást a szabályos $[n,m]$-szög megszerkesztésére.

HF: Milyen n természetes számok esetén szerkeszthető meg az n fokos szög?

Nemeuklideszi szerkesztések

- Mohr 1672, Mascheroni 1797
  csak körző $\equiv$ körző és vonalzó
- Poncelet 1822, Steiner 1833
  csak vonalzó és egy megrajzolt kör a középpontjával együtt $\equiv$ körző és vonalzó
- köbös szerkesztések (fok$=2^k 3^\ell$)
  betolóvonalzó, papírhajtogatás

Szögharmadolás betolóvonalzóval