Magasabbfokú egyenletek és geometriai szerkeszthetőség

Dormán Miklós

SZTE, Bolyai Intézet

2010. november 19.

Geometriai szerkeszthetőség komplex alaptest felett

Ha a sík pontjait (a Gauss-féle számsíkon nekik megfeleltetett) komplex számokkal adjuk meg, akkor a valós alaptest feletti szerkesztéstől eltérő –bár azzal sok rokonságot mutató– lehetőség adódik a szerkeszthetőség problémájának algebrai tárgyalására. Ennél a megközelítésnél bármely (H, u) szerkesztési feladat esetén a valós és a képzetes tengelyt úgy vesszük fel, hogy a $0, 1$ számoknak megfelelő pontok H-ban legyenek, és ezek után úgy tekintjük, hogy $H \subseteq \mathbb{C}$ és $u \in \mathbb{C}$.

Állítás.

Állítás.

(1) 0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető i.

Állítás.

(1) 0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető i.

(2) $a + bi$ akkor és csak akkor szerkeszethető meg H-ból, ha a és b megszerkeszthető.

Állítás.

(1) 0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető i.

(2) $a + bi$ akkor és csak akkor szerkeszethető meg H-ból, ha a és b megszerkeszthető.

(3) Valahányszor az $z, w \in \mathbb{C}$ megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

Állítás.

(1) 0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető i.

(2) $a + bi$ akkor és csak akkor szerkeszethető meg H-ból, ha a és b megszerkeszthető.

(3) Valahányszor az $z, w \in \mathbb{C}$ megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

   (i) $z + w$, $-z$,

Állítás.

(1) 0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető i.

(2) $a + bi$ akkor és csak akkor szerkeszethető meg H-ból, ha a és b megszerkeszthető.

(3) Valahányszor az $z, w \in \mathbb{C}$ megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

(i) $z + w$, $-z$,

(ii) zw, $1/z$ (ha $z \neq 0$),

Állítás.

(1) 0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető i.

(2) $a + bi$ akkor és csak akkor szerkeszethető meg H-ból, ha a és b megszerkeszthető.

(3) Valahányszor az $z, w \in \mathbb{C}$ megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

  (i) $z + w$, $-z$,

  (ii) zw, $1/z$ (ha $z \neq 0$),

  (iii) $\pm\sqrt{z}$.

Definíció: a szerkesztési feladat alapteste.

A (H, P) **szerkesztési feladat alaptestén** a H-beli komplex számok és konjugáltjaik által generált számtestet értjük.

Definíció: a szerkesztési feladat alapteste.

A (H, P) **szerkesztési feladat alaptestén** a H-beli komplex számok és konjugáltjaik által generált számtestet értjük.

Állítás.

A szerkesztési feladat alapteste független a Gauss-féle számsík választásától.

Definíció: négyzetgyökbővítés.

Legyenek $K \leqslant L$ számtestek. Az $L : K$ testbővítést **egyszerű négyzetgyökbővítésnek** hívjuk, ha $L = K(\sqrt{c})$ teljesül valamely nemnegatív $c \in K$ számra. Az $L : K$ tesbővítést **négyzetgyökbővítésnek** nevezzük, ha van K bővítéseinek egy olyan

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = L$$

sorozata, hogy minden j-re $(1 \leqslant j \leqslant t)$ a K_j test egyszerű négyzetgyök bővítése K_{j-1}-nek, azaz $K_j = K_{j-1}(\sqrt{c_j})$ valamely $c_j \in K_{j-1}$-re.

Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Ekkor ekvivalensek az alábbi feltételek:

Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Ekkor ekvivalensek az alábbi feltételek:

(a) u megszerkeszthető H-ból;

Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Ekkor ekvivalensek az alábbi feltételek:

(a) u megszerkeszthető H-ból;

(b) K-nak van olyan L négyzetgyökbővítése, amely tartalmazza u-t.

Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Legyen $f \in K[x]$ olyan K felett irreducibilis polinom, amelynek u gyöke. Ha az u pont megszerkeszthető, akkor f fokszáma 2-hatvány.

Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Legyen $f \in K[x]$ olyan K felett irreducibilis polinom, amelynek u gyöke. Ha az u pont megszerkeszthető, akkor f fokszáma 2-hatvány.

Tétel (Gauss-Wanzel).

Szabályos n-szög ($n > 2$) akkor és csak akkor szerkeszthető, ha n prímtényezős felbontása

$$n = 2^k p_1 \cdots p_r \quad (k, r \geqslant 0),$$

ahol $p_1, \ldots, p_r$ páronként különböző prímek, és $p_1 - 1, \ldots, p_r - 1$ mindegyike 2-hatvány.

Az általánosság megszorítása nélkül feltehető, hogy a kör, melybe a szabályos sokszöget szerkesztjük, egységnyi sugarú, s a 0 középpontjával és az 1 pontjával van megadva. Így a szerkesztés alapteste $\mathbb{Q}$. E körbe szabályos n-szög pontosan akkor szerkeszthető, ha az a szabályos n-szög megszerkeszthető, amelynek egyik csúcsa az 1 pont. Ezen szabályos n-szög megszerkeszthetősége pedig ekvivalens az

$$\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

csúcs megszerkesztésével. Az n-szög n csúcsa a következő:

$$\varepsilon_n^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad (k = 0, 1, \ldots, n-1).$$

Egyszerű észrevétel, hogy tetszőleges *n*-re a szabályos *n*-szög szerkesztése visszavezethető prímhatvány oldalú szabályos sokszögek szerkesztésére.

Egyszerű észrevétel, hogy tetszőleges n-re a szabályos n-szög szerkesztése visszavezethető prímhatvány oldalú szabályos sokszögek szerkesztésére.

Tétel.

(1) Bármely $m, n > 1$ egymáshoz relatív prím egészekre, ε_{mn} akkor és csak akkor szerkeszthető meg, ha ε_m és ε_n is megszerkeszthető.
(2) Bármely $n = p_1^{k_1} \cdots p_t^{k_t}$ egész számra, ahol $p_1, \ldots, p_t$ páronként különböző prímek, ε_n akkor és csak akkor szerkeszthető meg, ha $\varepsilon_{p_j^{k_j}}$ $(j = 1, \ldots, t)$ mindegyike megszerkeszthető.

Definíció: körosztási polinomok.

Tetszőleges p prímre a

$$\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

polinomot ***p*-edik körosztási polinomnak**, a

$$\Phi_{p^2} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1 \in \mathbb{Z}[x]$$

polinomot pedig **p^2-edik körosztási polinomnak** nevezzük.

Tétel.

Tetszőleges p prímre

Tétel.

Tetszőleges p prímre

(a) ε_p gyöke Φ_p-nek, ε_{p^2} pedig Φ_{p^2}-nek;

Tétel.

Tetszőleges p prímre

(a) ε_p gyöke Φ_p-nek, ε_{p^2} pedig Φ_{p^2}-nek;

(b) a Φ_p és Φ_{p^2} polinomok irreducibilisek $\mathbb{Q}$ felett.

Tétel.

Tetszőleges p prímre

(a) ε_p gyöke Φ_p-nek, ε_{p^2} pedig Φ_{p^2}-nek;

(b) a Φ_p és Φ_{p^2} polinomok irreducibilisek $\mathbb{Q}$ felett.

Definíció: Fermat-féle számok.

A $2^{2^n}+1$ alakú prímszámokat **Fermat-prímeknek** nevezzük. Az első öt ilyen szám,

$$2^{2^0}+1=3,\ 2^{2^1}+1=5,\ 2^{2^2}+1=17,\ 2^{2^3}+1=257,\ 2^{2^4}+1=65537$$

mind prímszám, $2^{2^5}+1=641\cdot 6700417$ azonban nem prím.

Tétel.

Legyen p tetszőleges páratlan prímszám.

Tétel.

Legyen p tetszőleges páratlan prímszám.

(1) ε_{p^2} nem szerkeszthető meg.

Tétel.

Legyen p tetszőleges páratlan prímszám.

(1) ε_{p^2} nem szerkeszthető meg.

(2) Ha p nem Fermat-prím, akkor ε_p sem szerkeszthető meg.

Tétel.

Legyen p tetszőleges páratlan prímszám.

(1) ε_{p^2} nem szerkeszthető meg.

(2) Ha p nem Fermat-prím, akkor ε_p sem szerkeszthető meg.

Tétel.

Ha p Fermat-prím, akkor ε_p megszerkeszthető.

Tétel (A szerkeszthetőség egy szükséges feltétele).

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Ha u megszerkeszthető H-ból, akkor u algebrai K felett, melynek foka 2-hatvány.

Tétel (A szerkeszthetőség egy szükséges feltétele).

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Ha u megszerkeszthető H-ból, akkor u algebrai K felett, melynek foka 2-hatvány.

Tétel (A szerkeszthetőség egy elegendő feltétele).

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Ha u algebrai K felett és u $(K \text{ feletti})$ minimálpolinomjának a foka 2-hatvány, továbbá $K(u)$ ezen polinom minden (komplex) gyökét tartalmazza, akkor az u pont megszerkeszthető H-ból.

Az előbbi tétel feltétele távolról sem szükséges feltétele a szerkeszthetőségnek. Ha például $\mathbb{Q}$ az alaptest, akkor $u = \sqrt[4]{2}$ megszerkeszthető, de $\mathbb{Q}(u)$ nem tartalmazza az $m_{\sqrt[4]{2},\mathbb{Q}} = x^4 - 2$ minimálpolinomjának összes gyökét.

Az előbbi tétel feltétele távolról sem szükséges feltétele a szerkeszthetőségnek. Ha például $\mathbb{Q}$ az alaptest, akkor $u = \sqrt[4]{2}$ megszerkeszthető, de $\mathbb{Q}(u)$ nem tartalmazza az $m_{\sqrt[4]{2},\mathbb{Q}} = x^4 - 2$ minimálpolinomjának összes gyökét.

Tétel.

Legyen K tetszőleges számtest, $u \in \mathbb{C}$ pedig tetszőleges komplex szám. Ha u algebrai K felett és u (K feletti) minimálpolinomjának a fokszáma 2-hatvány, továbbá $K(u)$ ezen polinom minden (komplex) gyökét tartalmazza, akkor $K(u)$ négyzetgyökbővítése K-nak.

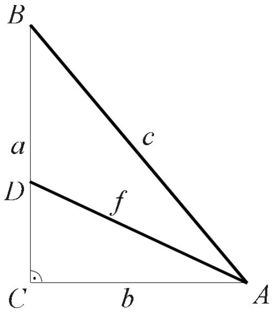
21. Tétel (A szerkeszthetőség szükséges és elegendő feltétele).

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste K. Az u pont akkor és csak akkor szerkeszthető meg, u algebrai K felett, és u K feletti minimálpolinomjának K feletti felbontási teste K-nak 2-hatvány fokú bővítése.

A szerkesztési problémák esetében többnyire van a megszerkesztendő alakzatnak olyan adata, amelynek segítségével az alakzat már könnyen megszerkeszthető. A célunk az lesz, hogy erre az adatra a megadott adatok segítségével alkalmas algebrai egyenletet állítsunk fel. A szerkeszthetőség kivitelezhetőségét pedig ezen polinom vizsgálatával döntjük el.

Feladat.

Megszerkeszthető-e az ABC derékszögű háromszög, ha adott az AB átfogójának és az A csúcsból kiinduló szögfelezőjének a hossza?



1. ábra: Az ABC háromszög adatai.

A Szögfelező-tétel szerint $\overline{BD} : \overline{DC} = c : b$. Mivel $\overline{DC} = a - \overline{BD}$, ezért

$$\overline{DC} = \frac{b}{b+c} a.$$

Alkalmazzuk Pithagorasz tételét az ABC és ADC háromszögekre:

$$a^2 + b^2 = c^2,$$

$$\overline{DC}^2 + b^2 = f^2 \iff \left(\frac{b}{b+c} a\right)^2 + b^2 = f^2.$$

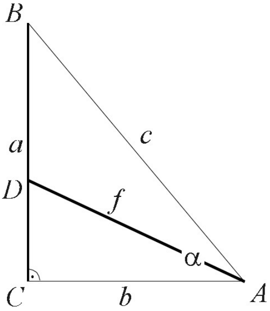
A fenti egyenlőségek felhasználásával azt kapjuk, hogy b gyöke a

$$p = (2c)b^2 - f^2 b - f^2 c$$

polinomnak. Válasszuk a c hosszúságot egységnyinek. Ekkor a szerkesztés K alapteste az f által generált számtest, a szerkesztendő b pont pedig a $p \in K[x]$ másodfokú polinom gyöke. A 9. Tétel szerint b — és így az ABC háromszög is — szerkeszthető.

Feladat.

Megszerkeszthető-e az ABC derékszögű háromszög, ha adott az BC befogójának és az A csúcsból kiinduló szögfelezőjének a hossza?



2. ábra: Az ABC háromszög adatai.

Felhasználva, hogy az α szöghöz tartozó szögfelező hossza

$$f = \frac{2bc}{b+c} \cos \frac{\alpha}{2},$$

valamint $c^2 = a^2 - b^2$ (Pithagorasz-tétel) és $\cos \frac{\alpha}{2} = \frac{b}{f}$, azt kapjuk, hogy

$$f = \frac{2}{\frac{1}{b} + \frac{1}{c}} \frac{b}{f} \iff \frac{2b}{f^2} - \frac{1}{b} = \frac{1}{c} \iff c(2b^2 - f^2) = f^2 b$$

$$\iff c^2(2b^2 - f^2)^2 = f^4 b^2$$

$$\iff (a^2 + b^2)(2b^2 - f^2)^2 = f^4 b^2,$$

azaz b gyöke a $p = 4x^6 + 4(a^2 - f^2)x^4 - 4a^2 f^2 x^2 + a^2 f^4$ polinomnak.

Mivel b pontosan akkor szerkeszthető, ha b^2 szerkeszthető, ezért jelen esetben érdemesebb b^2-et választani szerkesztendő adatnak, mivel b^2 a harmadfokú

$$4x^3 + 4(a^2 - f^2)x^2 - 4a^2f^2x + a^2f^4 \tag{1}$$

polinomnak gyöke.

Mivel b pontosan akkor szerkeszthető, ha b^2 szerkeszthető, ezért jelen esetben érdemesebb b^2-et választani szerkesztendő adatnak, mivel b^2 a harmadfokú

$$4x^3 + 4(a^2 - f^2)x^2 - 4a^2f^2x + a^2f^4 \tag{1}$$

polinomnak gyöke.

Megmutatjuk, hogy az a és f hosszúságok alkalmas választása esetén az ABC háromszög létezik, de nem szerkeszthető meg. Legyen $a = f = 1$, ekkor a szerkesztés alapteste $\mathbb{Q}$, és (1) szerint b^2 gyöke a $4x^3 - 4x + 1 \in \mathbb{Q}[x]$ polinomnak. Rolle tételét alkalmazva azt kapjuk, hogy e polinomnak nincs racionális gyöke. Így b^2 nem szerkeszthető, de a háromszög létezik ($b \approx 0,915$).