Testelmélet és Galois-elmélet

Euklideszi szerkesztések

2009. május 8.

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.
- Adott pont körül adott körzőnyílással kört rajzolhatunk.

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.
- Adott pont körül adott körzőnyílással kört rajzolhatunk.

Új pontokat pedig a következőképpen kaphatunk:

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.
- Adott pont körül adott körzőnyílással kört rajzolhatunk.

Új pontokat pedig a következőképpen kaphatunk:

(E_1) Két metsző egyenes metszéspontját megkereshetjük.

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.
- Adott pont körül adott körzőnyílással kört rajzolhatunk.

Új pontokat pedig a következőképpen kaphatunk:

(E_1) Két metsző egyenes metszéspontját megkereshetjük.

(E_2) Egy kör és az azt metsző egyenes metszéspontjait megkereshetjük.

A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.
- Adott pont körül adott körzőnyílással kört rajzolhatunk.

Új pontokat pedig a következőképpen kaphatunk:

(E_1) Két metsző egyenes metszéspontját megkereshetjük.

(E_2) Egy kör és az azt metsző egyenes metszéspontjait megkereshetjük.

(E_3) Két egymást metsző kör metszéspontjait megkereshetjük.

Definíció: euklideszi szerkesztés.

Ha egy szerkesztési feladatot pusztán az (E_1)–(E_3) lépések véges sokszori alkalmazásával végzünk, akkor a szerkesztést **euklideszi szerkesztésnek** nevezzük.

Definíció: H-egyenesek és H-körök.

Legyen H az $\mathcal{S}$ sík tetszőleges részhalmaza. Az $e \subseteq \mathcal{S}$ egyenest H-**egyenesnek** nevezzük, ha e legalább két különböző S-beli pontot tartalmaz. A $k = k(O, r) \subseteq \mathcal{S}$ kör(vonala)t H-**körnek** nevezzük, ha a k kör O középpontja H-ban van, és r sugara megegyezik két H-beli pont távolságával.

Definíció.

Legyen H az $\mathcal{S}$ sík tetszőleges részhalmaza. Definiáljuk a $\mathcal{E}_1(H)$, $\mathcal{E}_2(H)$ és $\mathcal{E}_3(H)$ halmazokat a következőképpen:

Definíció.

Legyen H az $\mathcal{S}$ sík tetszőleges részhalmaza. Definiáljuk a $\mathcal{E}_1(H)$, $\mathcal{E}_2(H)$ és $\mathcal{E}_3(H)$ halmazokat a következőképpen:

- $\mathcal{E}_1(H)$ azon P pontok halmaza, amelyekhez vannak olyan különböző e és f H-egyenesek, amelyekre $P = e \cap f$;

Definíció.

Legyen H az $\mathcal{S}$ sík tetszőleges részhalmaza. Definiáljuk a $\mathcal{E}_1(H)$, $\mathcal{E}_2(H)$ és $\mathcal{E}_3(H)$ halmazokat a következőképpen:

- $\mathcal{E}_1(H)$ azon P pontok halmaza, amelyekhez vannak olyan különböző e és f H-egyenesek, amelyekre $P = e \cap f$;
- $\mathcal{E}_2(H)$ azon P pontok halmaza, amelyekhez van olyan e H-egyenes és k H-kör, amelyekre $P = e \cap k$;

Definíció.

Legyen H az $\mathcal{S}$ sík tetszőleges részhalmaza. Definiáljuk a $\mathcal{E}_1(H)$, $\mathcal{E}_2(H)$ és $\mathcal{E}_3(H)$ halmazokat a következőképpen:

- $\mathcal{E}_1(H)$ azon P pontok halmaza, amelyekhez vannak olyan különböző e és f H-egyenesek, amelyekre $P = e \cap f$;
- $\mathcal{E}_2(H)$ azon P pontok halmaza, amelyekhez van olyan e H-egyenes és k H-kör, amelyekre $P = e \cap k$;
- $\mathcal{E}_3(H)$ azon P pontok halmaza, amelyekhez vannak olyan különböző k_1 és k_2 H-körök, amelyekre $P = k_1 \cap k_2$.

Definíció.

Legyen H az $\mathcal{S}$ sík tetszőleges részhalmaza. Definiáljuk a $\mathcal{E}_1(H)$, $\mathcal{E}_2(H)$ és $\mathcal{E}_3(H)$ halmazokat a következőképpen:

- $\mathcal{E}_1(H)$ azon P pontok halmaza, amelyekhez vannak olyan különböző e és f H-egyenesek, amelyekre $P = e \cap f$;
- $\mathcal{E}_2(H)$ azon P pontok halmaza, amelyekhez van olyan e H-egyenes és k H-kör, amelyekre $P = e \cap k$;
- $\mathcal{E}_3(H)$ azon P pontok halmaza, amelyekhez vannak olyan különböző k_1 és k_2 H-körök, amelyekre $P = k_1 \cap k_2$.

A $H \cup \mathcal{E}_1(H) \cup \mathcal{E}_2(H) \cup \mathcal{E}_3(H)$ halmaz elemei éppen azok a pontok, amelyek az (E_1)—(E_3) elemi szerkesztési lépések egyszeri végrehajtásával adódnak.

Ha $|H| \leqslant 1$, akkor H-ból új pontot nem tudunk szerkeszteni. Ezért a továbbiakban feltesszük, hogy H legalább két pontot tartalmaz.
A (H, P) párt, ahol H az adott ponthalmaz, P pedig a megszerkesztendő pont, **szerkesztési feladatnak** nevezzük.

Ha $|H| \leqslant 1$, akkor H-ból új pontot nem tudunk szerkeszteni. Ezért a továbbiakban feltesszük, hogy H legalább két pontot tartalmaz.
A (H, P) párt, ahol H az adott ponthalmaz, P pedig a megszerkesztendő pont, **szerkesztési feladatnak** nevezzük.

A geometriai problémát a koordináta-geometria segítségével fogjuk algebrai problémává átfogalmazni. Ennek egyik kézenfekvő módja, ha felveszünk egy Descartes-féle koordináta-rendszert: az adott H ponthalmazból kiválasztunk két különböző pontot, amelyeket a továbbiakban O, illetve E jelöl, és a koordináta-rendszer tengelyeit úgy vesszük fel, hogy O az origó, E pedig az $(1, 0)$ pont legyen.

1. Állítás.

1. Állítás.

(1) A H-beli O, E pontokból a két tengely megszerkeszthető.

1. Állítás.

(1) A H-beli O, E pontokból a két tengely megszerkeszthető.

(2) Egy (a, b) pont akkor és csak akkor szerkeszethető meg H-ból, ha $(a, 0)$ és $(b, 0)$ megszerkeszthető.

1. Állítás.

(1) A H-beli O, E pontokból a két tengely megszerkeszthető.

(2) Egy (a, b) pont akkor és csak akkor szerkeszethető meg H-ból, ha $(a, 0)$ és $(b, 0)$ megszerkeszthető.

(3) Valahányszor az $(a, 0)$, $(b, 0)$ pontok megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

1. Állítás.

(1) A H-beli O, E pontokból a két tengely megszerkeszthető.

(2) Egy (a, b) pont akkor és csak akkor szerkeszethető meg H-ból, ha $(a, 0)$ és $(b, 0)$ megszerkeszthető.

(3) Valahányszor az $(a, 0)$, $(b, 0)$ pontok megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

   (i) $(a + b, 0)$, $(-a, 0)$,

1. Állítás.

(1) A H-beli O, E pontokból a két tengely megszerkeszthető.

(2) Egy (a, b) pont akkor és csak akkor szerkeszethető meg H-ból, ha $(a, 0)$ és $(b, 0)$ megszerkeszthető.

(3) Valahányszor az $(a, 0)$, $(b, 0)$ pontok megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

- (i) $(a + b, 0)$, $(-a, 0)$,
- (ii) $(ab, 0)$, $(1/a, 0)$ (ha $a \neq 0$),

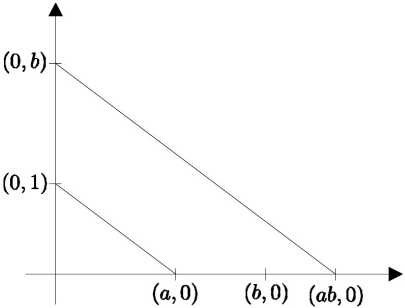
1. Állítás.

(1) A H-beli O, E pontokból a két tengely megszerkeszthető.

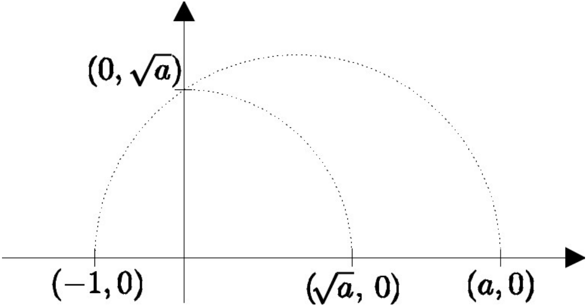
(2) Egy (a, b) pont akkor és csak akkor szerkeszethető meg H-ból, ha $(a, 0)$ és $(b, 0)$ megszerkeszthető.

(3) Valahányszor az $(a, 0)$, $(b, 0)$ pontok megszerkeszthetők H-ból, mindannyiszor megszerkeszthetők a következő pontok is:

- (i) $(a + b, 0)$, $(-a, 0)$,
- (ii) $(ab, 0)$, $(1/a, 0)$ (ha $a \neq 0$),
- (iii) $(\sqrt{a}, 0)$ (ha $a \geqslant 0$).



1. ábra: Az $(ab, 0)$ és $(1/a, 0)$ pontok szerkesztése.



2. ábra: A $(\sqrt{a}, 0)$ pont szerkesztése.

Definíció: négyzetgyökbővítés.

Legyen K tetszőleges számtest. Az L testet **egyszerű négyzetgyökbővítésnek** hívjuk, ha $L = K(\sqrt{c})$ valamely nemnegatív $c \in K$ számra. Az L testet **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 négyzetgyökbővítése K_{j-1}-nek, azaz $K_j = K_{j-1}(\sqrt{c_j})$ valamely $c_j \in K_{j-1}$-re $(c_j \geqslant 0)$.

2. Tétel.

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

2. Tétel.

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

(1) P megszerkeszthető H-ból;

2. Tétel.

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

(1) P megszerkeszthető H-ból;

(2) K-nak van olyan L négyzetgyökbővítése, amely P mindkét koordinátáját tartalmazza;

2. Tétel.

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

(1) P megszerkeszthető H-ból;

(2) K-nak van olyan L négyzetgyökbővítése, amely P mindkét koordinátáját tartalmazza;

(3) K-nak van olyan L', illetve L'' négyzetgyökbővítése, amely P első, illetve második koordinátáját tartalmazza.

2. Tétel.

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

(1) P megszerkeszthető H-ból;

(2) K-nak van olyan L négyzetgyökbővítése, amely P mindkét koordinátáját tartalmazza;

(3) K-nak van olyan L', illetve L'' négyzetgyökbővítése, amely P első, illetve második koordinátáját tartalmazza.

3. Lemma.

Legyen $f = ax^2 + bx + c \in \mathbb{R}[x]$ tetszőleges másodfokú polinom, melynek diszkriminánsa $D = b^2 - 4ac$. Ha az f polinom gyökei α és β, akkor $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.

A 2. Tétel bizonyítás.

(1)$\Longrightarrow$(2): Mivel a szerkesztés véges sok közvetlen szerkesztés egymás utáni végrehajtása, ezért az alábbi tényt belátva már adódik a bizonyítandó állítás:
Ha egy P pont a H ponthalmazból közvetlenül szerkeszthető, s a H-beli pontok koordinátái által generált számtest K, akkor a $H \cup \{P\}$ ponthalmazbeli pontok koordinátái által generált számtest vagy K, vagy egyszerű négyzetgyökbővítése K-nak.
Tegyük fel, hogy P közvetlenül szerkeszthető H-ból, azaz
$P \in H \cup \mathcal{E}_1(H) \cup \mathcal{E}_2(H) \cup \mathcal{E}_3(H)$.

A 2. Tétel bizonyítás (folytatás).

Koordináta-geometriából jól ismert, hogy a H-egyenesek, illetve H-körök egyenletének alakja:

$$ax + by = c, \text{ illetve}$$
$$(x - v)^2 + (y - w)^2 = r^2,$$

ahol $a, b, c, v, w, r^2 \in K$. A P pont koordinátái két fenti alakú egyenletrendszer megoldásaként adódnak. Ha mindkét egyenlet egyenes egyenlete, akkor P koordinátái szintén K-ban lesznek, míg a többi esetben az egyenletrendszer megoldása K-beli együtthatós másodfokú egyenletre vezet; ha e másodfokú egyenlet diszkriminánsa D ($D \in K$), akkor a 3. Lemma szerint P mindkét koordinátája a $K(\sqrt{D})$ test eleme.

A 2. Tétel bizonyítás (folytatás).

(2)$\Longrightarrow$(3): nyilvánvaló.
(3)$\Longrightarrow$(1): Tegyük fel, hogy u, illetve v benne van a K test egy L', illetve L'' négyzetgyökbővítésében. Legyen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = L',$$

ahol $K_j = K_{j-1}(\sqrt{c_j})$ $(c_j \in K_{j-1},\ c_j \geqslant 0)$ minden j-re $(1 \leqslant j \leqslant t)$. Az állítást j szerinti teljes indukcióval bizonyítjuk, azaz belátjuk, hogy tetszőleges j-re $(0 \leqslant j \leqslant t)$ bármely K_j-beli valós szám megszerkeszthető H-ból.

A 2. Tétel bizonyítás (folytatás).

Amiből már következik, hogy $u \in L' = K_t$ is megszerkeszthető H-ból. Hasonló meggondolással kapjuk, hogy $v \in L''$ is megszerkeszthető H-ból, és így a $P = (u, v)$ pont is megszerkeszthető H-ból.
Az 1. Állítás (3)(i) és (3)(ii) részéből következik, hogy H-ból a $K = K_0$ test megszerkeszthető. Tegyük fel, hogy valamely j-re $(1 \leqslant j \leqslant t)$ a K_{j-1} test elemei megszerkeszthetők H-ból. Az 1. Állítás (3)(iii) részéből az is következik, hogy $\sqrt{c_j}$ megszerkeszthető H-ból, így a $K_{j-1} \cup \{\sqrt{c_j}\}$ által generált $K_j = K_{j-1}(\sqrt{c_j})$ test elemei is megszerkeszthetők H-ból.
Ezzel a tétel állítását bebizonyítottuk.

Tetszőleges u valós szám esetén a (H, u) szerkesztési feladaton a $(H, (u, 0))$ szerkesztési feladatot értjük.
A 2. Tételben a (2) és (3) feltételek ekvivalenciája mutatja, hogy a szerkeszthetőségre kapott algebrai feltételnél is mindegy, hogy a megfelelő négyzetgyökbővítés létezését a P pontra (azaz mindkét koordinátájára egyidejüleg) vagy a koordinátákra külön-külön követeljük meg. Ezért a 2. Tétel alábbi változata egyenértékű az eredetivel.

Tetszőleges u valós szám esetén a (H, u) szerkesztési feladaton a $(H, (u, 0))$ szerkesztési feladatot értjük.
A 2. Tételben a (2) és (3) feltételek ekvivalenciája mutatja, hogy a szerkeszthetőségre kapott algebrai feltételnél is mindegy, hogy a megfelelő négyzetgyökbővítés létezését a P pontra (azaz mindkét koordinátájára egyidejüleg) vagy a koordinátákra külön-külön követeljük meg. Ezért a 2. Tétel alábbi változata egyenértékű az eredetivel.

4. Tétel.

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

Tetszőleges u valós szám esetén a (H, u) szerkesztési feladaton a $(H, (u, 0))$ szerkesztési feladatot értjük.
A 2. Tételben a (2) és (3) feltételek ekvivalenciája mutatja, hogy a szerkeszthetőségre kapott algebrai feltételnél is mindegy, hogy a megfelelő négyzetgyökbővítés létezését a P pontra (azaz mindkét koordinátájára egyidejüleg) vagy a koordinátákra külön-külön követeljük meg. Ezért a 2. Tétel alábbi változata egyenértékű az eredetivel.

4. Tétel.

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

(1) u megszerkeszthető H-ból;

Tetszőleges u valós szám esetén a (H, u) szerkesztési feladaton a $(H, (u, 0))$ szerkesztési feladatot értjük.
A 2. Tételben a (2) és (3) feltételek ekvivalenciája mutatja, hogy a szerkeszthetőségre kapott algebrai feltételnél is mindegy, hogy a megfelelő négyzetgyökbővítés létezését a P pontra (azaz mindkét koordinátájára egyidejüleg) vagy a koordinátákra külön-külön követeljük meg. Ezért a 2. Tétel alábbi változata egyenértékű az eredetivel.

4. Tétel.

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

(1) u megszerkeszthető H-ból;

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

5. Következmény.

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

A kör négyszögesítése.

A kérdés az, hogy lehetséges-e az egységsugarú körrel azonos területű négyzetet szerkeszteni, amely — az 5. Következményt felhasználva — az algebra nyelvén úgy fogalmazható meg, hogy a π szám foka 2-hatvány-e a a szerkesztés alapteste, azaz $K = \mathbb{Q}$ felett. Azonban a π szám még csak nem is végesfokú, azaz transzcendens, $\mathbb{Q}$ felett, így a kör négyszögesítése euklideszi módon nem végezhető el.

Szögharmadolás.

Lehetséges-e egy adott szög harmadát megszerkeszteni? A válasz általában az, hogy nem; pl. a 60°-os szöget nem lehet harmadolni, azaz nem lehet 20°-os szöget szerkeszteni. A 20°-os szerkesztése azt jelenti, hogy a $P = (\cos 20^\circ, \sin 20^\circ)$ pont szerkeszthető a $O = (0,0)$, $E = (1,0)$, $P = (\cos 60^\circ, \sin 60^\circ) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ pontokból. Ekkor a $Q = (\cos 20^\circ, 0)$ is szerkeszthető, mivel Q nem más mint a P-ból pont OE szakaszra állított merőleges talppontja. Mivel a szerkesztés alapteste $K = \mathbb{Q}(\sqrt{3})$ és $[K : \mathbb{Q}] = 2$, ezért elegendő azt megmutatni, hogy $\cos 20^\circ$ foka nem 2-hatvány $\mathbb{Q}$ felett. Legyen $\alpha = \cos 20^\circ$, ekkor — felhasználva a $\cos 3x = 4\cos^3 x - 3\cos x$ azonosságot — azt kapjuk, hogy α eleget tesz az $\frac{1}{2} = 4x^3 - 3x$ egyenletnek, azaz gyöke a $4x^3 - 3x - \frac{1}{2} \in \mathbb{Q}[x]$ polinomnak.

Szögharmadolás (folytatás).

Tekintsük a $2(4x^3 - 3x - \frac{1}{2}) = 8x^3 - 6x - 1 \in \mathbb{Z}[x]$ polinomot. A Rolle-tétel segítségével gyorsan kideríthető, hogy ez utóbbi polinomnak nincs racionális gyöke, így irreducibilis $\mathbb{Q}$ felett. Ezért a $4x^3 - 3x - \frac{1}{2}$ polinom is irreducibilis $\mathbb{Q}$ felett. Ez azt jelenti, hogy $m_{\cos 20^\circ,\mathbb{Q}} = 4x^3 - 3x - \frac{1}{2}$, azaz $\cos 20^\circ$ foka $\mathbb{Q}$ felett 3, ami nem 2-hatvány. Így a 60°-os szög nem harmadolható euklideszi módon.

Déloszi probléma vagy kockakettőzés.

Olyan kockát kell szerkeszteni, amely kétszer akkora térfogatú mint egy adott kocka. Legyen az adott kocka élhossza 1 méter, ekkor térfogata 1 m^3. Feladatunk egy 2 m^3-es kocka élének, azaz az $\alpha = \sqrt[3]{2}$ valós számnak a szerkesztése a $H = \{O, E\}$ halmazból. Mivel a $(H, \sqrt[3]{2})$ szerkesztési feladat alapteste $\mathbb{Q}$ és α minimálpolinomja $\mathbb{Q}$ felett a (Schönemann–Eisenstein-Tétel szerint irreducibilis) $x^3 - 2$ polinom, ezért α foka 3 a racionális számtest felett, így nem szerkeszthető az 5. Következmény szerint.

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 $u \in \mathbb{C}$.

6. Állítás.

6. Állítás.

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

6. 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.

6. 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:

6. 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) $z + w$, $-z$,

6. 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 $z \neq 0$),

6. 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.

7. 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.

8. Tétel.

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

8. Tétel.

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

(a) u megszerkeszthető H-ból;

8. 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.

9. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti másodfokú polinomnak, akkor u megszerkeszthető.

9. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti másodfokú polinomnak, akkor u megszerkeszthető.

10. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti harmadfokú polinomnak, akkor az alábbi három feltétel ekvivalens egymással:

9. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti másodfokú polinomnak, akkor u megszerkeszthető.

10. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti harmadfokú polinomnak, akkor az alábbi három feltétel ekvivalens egymással:

(a) u megszerkeszthető,

9. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti másodfokú polinomnak, akkor u megszerkeszthető.

10. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti harmadfokú polinomnak, akkor az alábbi három feltétel ekvivalens egymással:

(a) u megszerkeszthető,

(b) f minden olyan gyöke megszerkeszthető, amely a szerkesztés szempontjából szóba jöhet,

9. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti másodfokú polinomnak, akkor u megszerkeszthető.

10. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy K feletti harmadfokú polinomnak, akkor az alábbi három feltétel ekvivalens egymással:

(a) u megszerkeszthető,

(b) f minden olyan gyöke megszerkeszthető, amely a szerkesztés szempontjából szóba jöhet,

(c) f-nek van gyöke K-ban.

11. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy olyan K feletti negyedfokú polinomnak, amelynek nincs gyöke K-ban, akkor az alábbi három feltétel ekvivalens egymással:

11. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy olyan K feletti negyedfokú polinomnak, amelynek nincs gyöke K-ban, akkor az alábbi három feltétel ekvivalens egymással:

(a) u megszerkeszthető,

11. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy olyan K feletti negyedfokú polinomnak, amelynek nincs gyöke K-ban, akkor az alábbi három feltétel ekvivalens egymással:

(a) u megszerkeszthető,

(b) f minden olyan gyöke megszerkeszthető, amely a szerkesztés szempontjából szóba jöhet,

11. Tétel.

Legyen (H, u) tetszőleges szerkesztési feladat, melynek alapteste legyen K. Ha u gyöke egy olyan K feletti negyedfokú polinomnak, amelynek nincs gyöke K-ban, akkor az alábbi három feltétel ekvivalens egymással:

(a) u megszerkeszthető,

(b) f minden olyan gyöke megszerkeszthető, amely a szerkesztés szempontjából szóba jöhet,

(c) f köbös rezolvensének van gyöke K-ban.

12. 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.

12. 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.

13. 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.

14. 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 $\varepsilon_{p_j^{kj}}$ $(j = 1, \ldots, t)$ 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.

15. Tétel.

Tetszőleges p prímre

15. Tétel.

Tetszőleges p prímre

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

15. 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.

15. 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.

16. Tétel.

Legyen p tetszőleges páratlan prímszám.

16. Tétel.

Legyen p tetszőleges páratlan prímszám.

(1) ε_{p^2} nem szerkeszthető meg.

16. 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.

16. 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.

17. Tétel.

Ha p Fermat-prím, akkor ε_p megszerkeszthető.

18. 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.

18. 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.

19. 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.

A 26. Tétel szerint elegendő az alábbi (tisztán algebrai) tételt igazolni.

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.

A 26. Tétel szerint elegendő az alábbi (tisztán algebrai) tételt igazolni.

20. 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.

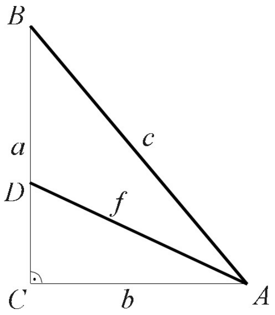
21. Tétel (A szerkeszthetőség szükséges és elegendő feltétele).

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?



3. 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:

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

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

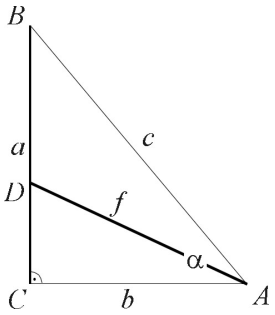
A fenti egyenlőségek felhasználásával azt kapjuk, hogy b gyöke a

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

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?



4. 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.

Geometriai szerkeszthetőség
Hétköznap szerkesztési feladatok.

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 a 10. Tétel szerint b^2 nem szerkeszthető, de a háromszög létezik ($b \approx 0,915$).