

SZ 1/1
1267

JÓZSEF ATILA TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR
GEOMETRIA TANSZÉK

A GEOMETRIAI SZERKESZTÉSEK
ELMÉLETE

Diplomamunka

Konzulens:
Dr. Kurusa Árpád
egyetemi docens

Készítette:
Cseh Zoltán
V. matematika

Szeged
1998

BEVEZETŐ

Régóta felbukkannak különböző tudományágakban olyan problémák, amelyek nem csupán a tudósok érdeklődését keltik fel, hanem rejtélyes módon izgatják a laikusok fantáziáját évszázadokon, évezredekken át. Talán a problémák látszólagos egyszerűsége a megtévesztő számukra. A középkorban például alkimisták százai próbálkoztak az arany előállításával, sikertelenül.

Századunkban az anyag szerkezetének beható vizsgálata vezetett el oda, hogy meg tudjuk magyarázni az alkimisták kudarcainak okait. Másik ilyen - fizikai jellegű - probléma a perpetuum mobile készítése. Olyan szerkezeté amely állandóan mozog, miközben semmi nem hajtja. Több tudományos intézmény díjat tűzött ki a csodálatos konstrukció megalkotójának. Készültek is szép számmal a különféle szerkezetek, de olyat nem találtak ami valóban megfelelt volna a Kritériumoknak. Mai fizikai ismereteink alapján már tudjuk - bár próbálkozó még mindig akad - hogy ilyen gép nem készíthető.

A matematikában a kör négyszögesítése, a kockakettőzés és a szögharmadolás több mint kétezer éves probléma. Az ókortól kezdve rengeteg tudós szentelte életét valamelyik feladat megoldásának. Próbálkozásaikat ugyan nem koronázta siker, de a kutatások elvezettek már az ókorban a kúpszeletek, harmad- és negyedrendű görbék, sőt néhány transzcendens görbe felfedezéséhez; később pedig hozzájárult a polinomok, algebrai számok elméletének fejlődéséhez, valamint a csoportelmélet, s ezáltal az absztrakt algebra kialakulásához.

Ez a dolgozat a geometriai szerkeszthetőséget veszi nagyító alá, algebrai úton közelítve a problémához. Első része algebrai alapismereteket tartalmaz, ennek megértéséhez nagyon kevés előismeret szükséges. Ezeket részletesen megtalálja az olvasó a szakdolgozat végén lévő számozott irodalomjegyzékben. Ezt követően kerül sor a szerkeszthetőség tárgyalására, a három ókori probléma megoldására, néhány háromszögszerkesztési- szerkeszthetőségi probléma vizsgálatára, valamint a szabályos sokszögek szerkesztésének kérdésére. A

dolgozat végén megemlítek néhány euklideszitől különböző szerkesztési módszert.

Carl Friedrich Gauss -a matematikusok fejedelme- 19 évesen jött rá, hogy a szabályos 17-szög körzővel és vonalzóval megszerkeszthető. A legenda szerint ez a felfedezés juttatta arra az elhatározásra, hogy a matematikának szentelje életét. Hogy mennyire büszke volt erre a felfedezésére, jelzi az a kívánsága, hogy a sírkövére egy szabályos 17-szöget véssenek, s bár ez sohasem teljesült, a szülővárosában, Brunswickban felállított emlékművét valóban szabályos 17 - szög díszíti.

Szakdolgozatom témájának választásánál a matematikának sok szép és érdekes fejezetével találkoztam, ám amikor rábukkantam a szerkesztések elméletére, akárcsak Gauss, én is indíttatást éreztem a témában való elmélkedésre. Nemcsak az vonzott, hogy a három ókori problémát ezen elmélet segítségével meg lehet oldani, hanem az elméletnek az a teljessége is, amellyel megmutatja a matematika dinamikus fejlődését, sokszínűségét, és szépségét.

I. FEJEZET

ALGEBRAI ALAPISMERETEK

1. Alapvető algebrai fogalmak

Bizonyos halmazokat azért vizsgálunk, mert elemei között művelet vagy műveletek vannak értelmezve. Az algebrában külön vizsgálat tárgyát képezik a halmazok a bennük végzett műveletekkel. A következő definíciók alapvető fontosságúak a tárgyaláshoz:

1. 1 Definíció. Az S nem üres halmaz $S \times S$ Descartes - féle szorzatának S be való leképezését az S halmazon értelmezett kétváltozós műveletnek nevezzük.
Szimbólumokkal: $f: S \times S \rightarrow S ((a,b) \rightarrow f(a,b))$

Az $f(a,b)$ jelölés helyett szokás az $a + b$, ab , $a \bullet b$ stb. jelölést is használni.

Példák kétváltozós műveletre:

- az összeadás N -ben,
- a szorzás a páratlan egész számok halmazában,
- A metszetképzés $P(H)$ -ban.

- 1.2 Definíció. Algebrai struktúrának - röviden struktúrának - nevezzük az olyan legalább kéttagú $(S; \bullet, |, *, \dots)$ rendszert, amelynek első eleme egy $S(\neq 0;)$ halmaz, a többi pedig S -en értelmezett algebrai művelet.

Példák:

- $(N; +)$ jelenti a természetes számoknak az összeadás szerinti struktúráját,
 $(R; +, \cdot)$ jelenti a valós számok összeadás és szorzás szerinti struktúráját,
 $(P(H); \cup, \cap,)$ egy H halmaz részhalmazainak halmaza az egyesítés és a metszés művelete szerint.

1.3 Definíció. Az S halmazon értelmezett $\bullet$ műveletről azt mondjuk, hogy
 asszociatív, ha minden $a, b, c (\in S)$ - re : $(a \bullet b) \bullet c = a \bullet (b \bullet c)$,
 kommutatív, ha minden $a, b (\in S)$ elemre : $a \bullet b = b \bullet a$
 invertálható, ha minden $a, b (\in S)$ - re az $x \bullet a = b$, $a \bullet y = b$ egyenleteknek
 mindig van megoldása.

1.4 Definíció. Ha az $(S; \bullet)$ stuktúrának van olyan u eleme, hogy minden
 $a (\in S)$ -re $u \bullet a = a \bullet u = a$, akkor u -t neutrális elemnek, szorzás esetén
 egységelemnek, összeadás esetén additív zérusnak nevezzük.
 Jelölésük általában e , illetve 0 .

1.5 Definíció. Ha az $(S; \bullet)$ struktúrában van olyan z elem, hogy minden
 $a (\in S)$ -re $z \bullet a = a \bullet z = z$, akkor z - t zéruselemnek nevezzük.

1.6 Definíció. Legyen $(S; \bullet, *, \dots)$ legalább kétműveletes struktúra. Ha minden
 $a, b, c (\in S)$ -re: $a * (b \bullet c) = (a * b) \bullet (a * c)$ és $(a \bullet b) * c = (a * c) \bullet (a * b)$ teljesül, akkor a
 $*$ művelet disztributív a $\bullet$ műveletre nézve.

Ezek után rátérek a fontosabb struktúratípusok ismertetésére.

1.7. Definíció.

(1) Az $(S; \bullet)$ félcsoporth, ha a $\bullet$ művelet asszociatív.

(2) Az $(S; \bullet)$ csoport, ha a $\bullet$ művelet asszociatív, és invertálható.

(3) Az $(S; +, \bullet)$ gyűrű, ha $(S; +)$ kommutatív csoport, $(S; \bullet)$ félcsoporth és a $\bullet$
 művelet az összeadásra nézve disztributív.

(4) Az $(S; +, \bullet)$ test, ha S legalább kételemű, $(S; +)$ kommutatív csoport,
 $(S \setminus \{0\}; \bullet)$ kommutatív csoport és a $\bullet$ művelet az összeadásra nézve
 disztributív.

Az algebrai struktúrák kapcsolatára ismereteseek a következők:

1.8 Definíció.

Az $(S; \bullet)$, $(P; \sqcup)$ struktúra esetén a $\varphi: S \rightarrow P$ leképezést homomorfizmusnak nevezzük, ha a $(\bullet; 0)$ műveletpárra :

$\varphi(a \bullet b) = \varphi a \sqcup \varphi b$ ($a, b \in S$) teljesül. Ha a φ leképezés kölcsönösen egyértelmű (bijektív), akkor izomorfizmusnak nevezzük. Két struktúra izomorfizmusát így jelöljük $(S; \bullet) \cong (P; \sqcup)$.

2. A komplex számok teste

Egy adott halmazon egy bizonyos művelet nem mindig végezhető el. Például $\mathbf{Z}$ -ben (egész számok halmazán) az osztás "művelete", hiszen $7/4$ nem egész szám. Ahhoz, hogy a műveletek korlátlanul elvégezhetők legyenek, az alaphalmazt új elemekkel kell bővíteni. Ilyen bővítés révén jött létre $\mathbf{N}$ -ből (természetes számok halmaza) $\mathbf{Z}$, $\mathbf{Z}$ -ből $\mathbf{Q}$ (racionális számok halmaza), $\mathbf{Q}$ -ból $\mathbf{R}$ (valós számok halmaza). A számfogalom fejlődése azonban itt nem állt meg, ugyanis a valós számok halmazán nem oldható meg például az egyszerűnek tűnő $x^2 + 1 = 0$ egyenlet, hiszen $x^2 + 1 > 0$ minden x valós szám esetén. A -1 valós számból nem tudunk négyzetgyököt vonni. A gyökvonás korlátlan elvégezhetőségének igénye vezetett el a komplex számokhoz.

2.1 Definíció. $\mathbf{R} \times \mathbf{R}$ -ben értelmezzünk összeadást és szorzást a következőképpen:

$$(a, b) + (c, d) := (a + c, b + d)$$

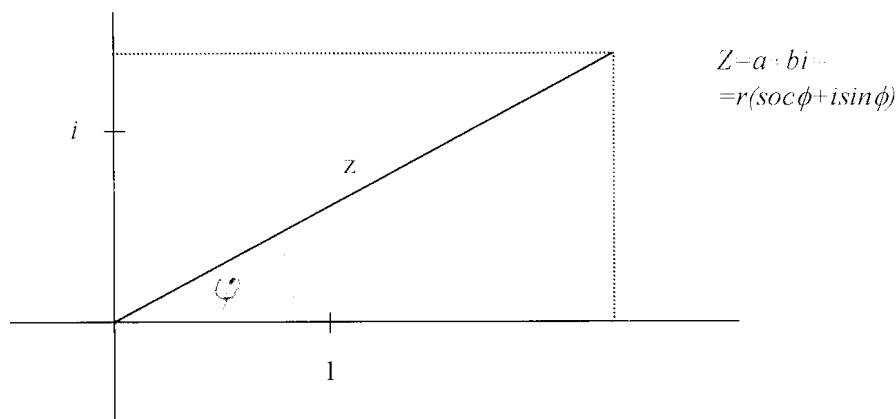
$$(a, b)(c, d) := (ac - bd, ad + bc).$$

Könnyen igazolható, hogy az $(\mathbf{R} \times \mathbf{R}; +, \cdot)$ struktúra test. Ennek bizonyítása [9] -ben megtalálható.

A komplex számok halmazát $\mathbf{C}$ -vel jelöljük, egy tetszőleges elemét $z = a + bi$ alakban adjuk meg ($a, b \in \mathbf{R}$), i pedig $\sqrt{-1}$ -gyel egyenlő.

Ha adott a síkon egy derékszögű koordináta-rendszer, akkor a sík pontjai és a komplex számok között kölcsönösen egyértelmű megfeleltetés létesíthető. Emiatt lesz hasznos a komplex számok használata a szerkeszthetőség vizsgálatánál.

Szokás még a komplex számot $z = r(\cos\varphi + i\sin\varphi)$, úgynevezett trigonometrikus alakban megadni. A két felírás közötti kapcsolatot az alábbi ábra szemlélteti:



Az ábrából világos, hogy $a = r\cos\varphi$, $b = r\sin\varphi$, valamint $|z| = r = \sqrt{a^2 + b^2}$.

Egy komplex szám hatványozása trigonometrikus alakban egyszerűbb. Moivre-képlete alapján a $z = r(\cos\varphi + i\sin\varphi)$ komplex szám k -adik hatványa:

$$z^k = r^k (\cos k\varphi + i \sin k\varphi), \quad (k \text{ egész szám}).$$

A sokszögek szerkesztésének vizsgálatakor szükség lesz a komplex szám n -edik gyökére. A fentiek alapján belátható, hogy a $z = r(\cos\varphi + i\sin\varphi)$ komplex számnak az n -edik gyökét az $\sqrt[n]{r}(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n})$ alakban felírt komplex számok adják ($k = 0, 1, \dots, n-1$). Egy adott számnak n különböző n -edik gyöke van, a számsíkon ezek egy $\sqrt[n]{r}$ sugarú körívet osztanak fel n egyenlő részre.

2.2 Definíció. Egy T részhalmazát számtestnek (testnek) nevezzük, ha $0, 1 \in T$,

és bármely $a, b \in T$ elemekre $a+b, -a, ab \in T$ és $a \neq 0$ esetén $1/a \in T$ is teljesül.

Ez a definíció megkönnyíti a II. fejezet tárgyalását.

3. A polinomok

3.1 Definíció.

- (1) Az $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ alakú (formális) összeget a T test fölötti polinomnak nevezzük. ($a_n, a_{n-1}, \dots, a_0 \in T$)
- (2) Ha $a_n \neq 0$, akkor n -et a polinom fokszámának nevezzük.
- (3) Ha $a_n = 1$ akkor főpolinomról beszélünk.
- (4) Ha van olyan $c \in T$ szám, hogy $f(c) = 0$, akkor c -t a polinom gyökének nevezzük.

3.2 Definíció. Két polinom $f(x)$ és $g(x)$ akkor és csak akkor egyenlő, ha a megfelelő együtthatóik rendre egyenlők.

3.3 Definíció.

A T test fölötti polinomok halmazát $T[x]$ -szel jelöljük $T[x]$ -ben definiáljuk

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \text{ és } g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

összeget és szorzatát a következőképpen: (feltehetjük, hogy $n \geq m$)

$$f(x) + g(x) := (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \dots + (a_1 + b_1)x + (a_0 + b_0)$$

$$f(x)g(x) := a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)x^{n+m-1} + \dots + (a_1 b_0 + a_0 b_1)x + a_0 b_0$$

3.4. Tétel. A $(T[x]; +, \cdot)$ struktúra olyan gyűrű, amelyben a szorzás kommutatív, egységelemes (egységeleme az 1), és bármely két $f(x) \neq 0$ és $g(x) \neq 0$ polinom szorzata 0-tól különböző (zérusosztómentes).

A már ismert definíciók alapján a bizonyítás elvégezhető (például [9]-ben megtalálható).

3.5 Definíció. Legyen T tetszőleges számtest, $f(x), g(x), d(x) \in T[x]$ tetszőleges polinomok. Azt mondjuk, hogy:

- (1) f osztója g -nek (jelölése $f \mid g$), ha van olyan $h \in T[x]$ polinom, hogy $g = fh$,
- (2) d legnagyobb közös osztója f -nek és g -nek, ha $d \mid f$ és $d \mid g$, továbbá minden olyan $d^* \in T[x]$ -re, amelyre $d^* \mid f, g$, fennáll $d^* \mid d$ is,
- (3) irreducibilis, ha f legalább elsőfokú, és f -nek nincs más osztója, mint a c illetve cf alakú polinomok ahol $c \in T, c \neq 0$.

Bizonyítás nélkül tárgyaljuk a következő két tételt:

3.6 Tétel Legyen T tetszőleges számtest. Bármely $f, g (\neq 0) \in T[x]$ polinomokra:

- (1) léteznek olyan $q, r \in T[x]$ polinomok, hogy $f = gq + r$ és r vagy azonosan 0, vagy fokszáma kisebb q fokszámánál; q és r egyértelműen meghatározott,
- (2) létezik olyan $d \in T[x]$ polinom amely legnagyobb közös osztója f -nek és g -nek; d egy nemnulla konstans szorzó erejéig egyértelműen meghatározott,
- (3) léteznek olyan $u, v \in T[x]$ polinomok, hogy: $fu + gv = d$.

3.7 Tétel Tetszőleges T számtest esetén minden $T[x]$ -beli, legalább elsőfokú polinom felbontható egy T -beli nemnulla konstans polinom, valamint $T[x]$ -beli irreducibilis főpolinomok szorzatára, s ez a felbontás a tényezők sorrendjétől eltekintve egyértelműen meghatározott.

3.8 Definíció. Legyen T tetszőleges számtest és $a \in \mathbb{C}$ komplex szám.

- (1) Azt mondjuk, hogy a algebrai elem T fölött, ha a egy $T[x]$ -beli nemzéró polinom gyöke.
- (2) Ha nincs olyan $T[x]$ -beli (nem azonosan zéró) polinom amelynek a gyöke, akkor a -t transzcendens számnak nevezzük.
- (3) Ha a algebrai elem T fölött, akkor azt a $T[x]$ -beli irreducibilis főpolinomot, aminek a gyöke, az a szám T fölötti minimálpolinomjának nevezzük.

A következőkben a polinomoknak testek ($\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$) fölötti irreducibilitásáról lesz szó.

A $\mathbb{C}$ fölötti polinomok tárgyalásához segítségül hívjuk a klasszikus algebra alaptételét.

3.9 Tétel Minden komplex együtthatós, legalább elsőfokú polinomnak van gyöke a komplex számtestben,

Ebből következik, hogy a komplex együtthatós polinomok között pontosan az elsőfokú polinomok az irreducibilisek.

Az $\mathbf{R}$ fölötti polinomokra érvényes az alábbi:

3.10 Tétel A valós együtthatós polinomok közül az elsőfokúak és néhány másodfokú polinom irreducibilis. A magasabb fokszámú polinomok mindig felbonthatóak.

A bizonyítás azon alapszik, hogy ha egy $z = a + bi$ komplex szám gyöke a polinomnak, akkor a konjugáltja, $z^* = a - bi$ is gyöke, és zz^* pedig mindig valós szám.

3.11 Tétel $\mathbf{Q}$ fölötti polinomok közül tetszőlegesen nagy fokszámúak lehetnek irreducibilisek.

A bizonyításhoz elég megmutatni, hogy az $f(x) = x^n - 2$ polinom minden n -re irreducibilis, nincsen racionális gyöke.

A tárgyaláshoz szükség lesz még az egész együtthatós polinomok vizsgálatára, ugyanis sok szerkeszthetőségi probléma visszavezethető $\mathbf{Z}(x)$ -beli polinomok irreducibilitásának az eldöntésére. Másrészt pedig a $\mathbf{Z}[x]$ -beli polinomok felbonthatatlanságára több elegendő feltétel is létezik, ezeket viszonylag egyszerűbb vizsgálni.

3.12 Definíció. Az egész együtthatós polinomot primitívnek nevezzük, ha együtthatóinak legnagyobb közös osztója 1.

$\mathbf{Q}[x]$ -beli és $\mathbf{Z}[x]$ -beli polinomok kapcsolatáról szól a következő:

3.13 Tétel Minden $\mathbf{Q}[x]$ -beli $f(x) (\neq 0)$ polinom előjeltől eltekintve egyértelműen felírható egy racionális szám és egy $\mathbf{Z}[x]$ -beli primitív polinom szorzataként.

A fenti tétel bizonyítása konstruktív, az unicitásé indirekt.

3.14 Tétel, Ahhoz, hogy egy $f(x) (\in \mathbf{Z}[x])$ polinom irreducibilis legyen, szükséges és elegendő, hogy $f(x)$ primitív és $f(x)$ irreducibilis $\mathbf{Q}[x]$ -ben.

Megjegyzés. Primitív polinomokra tehát $\mathbf{Z}$, illetve $\mathbf{Q}$ feletti irreducibilitás ekvivalens egymással.

A már említett elegendő feltételek a $\mathbf{Z}[x]$ -beli felbonthatatlanságra:

3.15 Tétel (Schönemann-Eisenstein)

Ha az egész együtthatós $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ polinom együtthatóira, valamint egy p prímszámra teljesül, hogy $p \mid a_n, p \mid a_{n-1}, \dots, p \mid a_0$, és $p^2 \nmid a_n$, akkor $f(x)$ irreducibilis $\mathbf{Q}[x]$ -ben, és ha $f(x)$ primitív, akkor $\mathbf{Z}[x]$ -ben is az.

3.16 Tétel (Rolle-tétele) Ha egy p/q racionális szám ($p, q \in \mathbf{Z}$ és $(p, q) = 1$) gyöke az $f(x) (\in \mathbf{Z}[x])$ polinomnak, akkor $p \mid a_0$, és $q \mid a_n$.

4. *A vektorterek*

4.1 Definíció. Az elemeknek egy $\mathbf{V}$ halmaza vektortér a T test fölött, ha $\mathbf{V}$ a benne értelmezett összeadás szerint kommutatív csoportot alkot, valamint minden $a, b (\in T)$ és $\mathbf{v}, \mathbf{w} (\in \mathbf{V})$ elemhez hozzá van rendelve egy $a\mathbf{v} (\in \mathbf{V})$ elem, amelyekre:

$$(1) \quad a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}.$$

$$(2) \quad (a+b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$$

$$(3) \quad (ab)\mathbf{v} = a(b\mathbf{v})$$

$$(4) \quad 1\mathbf{v} = \mathbf{v}$$

teljesül. A vektortér elemeit vektoroknak, a T test elemeit skalároknak nevezzük. A zérusvektort $\mathbf{0}$ -val jelöljük.

Példák :

- a sík összes vektora ($\mathbf{R}_2$)

a komplex számok $\mathbf{R}$ fölött,

- a tér összes vektora ($\mathbf{R}_3$),

- a T test fölötti összes polinomok $T[x]$ halmaza vektorteret alkot T fölött, ha az összeadást és a T -beli elemmel való szorzást a 3. pontban leírtak szerint definiáljuk.

4.2. Definíció.

Legyen T egy tetszőleges test, $\mathbf{V}$ pedig T fölötti vektortér.

(1) Tetszőleges $\mathbf{v}_1, \dots, \mathbf{v}_m (\in \mathbf{V})$ vektorokra és $c_1, \dots, c_m (\in T)$ számokra $\mathbf{v} = c_1 \mathbf{v}_1 + \dots + c_m \mathbf{v}_m$ alakú vektorokat a $\mathbf{v}_1, \dots, \mathbf{v}_m$ vektorok lineáris kombinációinak nevezzük.

(2) $c_1 = \dots = c_m = 0$ esetén triviális lineáris kombinációról beszélünk. (ekkor nyilván $\mathbf{v} = 0$).

(3) A $\mathbf{v}_1, \dots, \mathbf{v}_m (\in \mathbf{V})$ vektorrendszert lineárisan függetlennek nevezzük, ha a 0 vektort $\mathbf{v}_1, \dots, \mathbf{v}_m$ lineáris kombinációi közül csak a triviális lineáris kombináció állítja elő.

(4) Azt mondjuk, hogy a $\mathbf{V}$ vektortér véges dimenziós, ha valamely m természetes számra léteznek olyan $\mathbf{v}_1, \dots, \mathbf{v}_m (\in \mathbf{V})$ vektorok, hogy minden $\mathbf{V}$ -beli vektor előáll $\mathbf{v}_1, \dots, \mathbf{v}_m$ lineáris kombinációjaként. Az ilyen $\mathbf{v}_1, \dots, \mathbf{v}_m$ vektorrendszert $\mathbf{V}$ generátorrendszerének hívjuk. Úgy is mondják, hogy $\mathbf{v}_1, \dots, \mathbf{v}_m$ generálja $\mathbf{V}$ -t.

(5) A $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbf{V}$ vektorrendszert a $\mathbf{V}$ bázisának nevezzük, ha $\mathbf{v}_1, \dots, \mathbf{v}_m$ lineárisan független, és minden $\mathbf{V}$ -beli vektor előáll $\mathbf{v}_1, \dots, \mathbf{v}_m$ lineáris kombinációjaként.

A fentiekből következik, hogy egy $\mathbf{v}_1, \dots, \mathbf{v}_m$ vektorrendszer akkor és csak akkor bázisa $\mathbf{V}$ -nek, ha minden $\mathbf{V}$ -beli vektor egyértelműen előáll $\mathbf{v}_1, \dots, \mathbf{v}_m$ lineáris kombinációjaként,

4.3 Tétel Legyen T tetszőleges test, $\mathbf{V}$ pedig T fölötti vektortér. Ha $\mathbf{V}$ véges dimenziós, akkor

- (1) $\mathbf{V}$ -nek létezik bázisa, és bármely két bázisának elemszáma egyenlő;
- (2) $\mathbf{V}$ -ben bármely lineárisan független vektorrendszer kiegészíthető bázissá, s bármely generátorrendszerből kiválasztható bázis.

4.4. Definíció.

A $\mathbf{V}$ véges dimenziós vektortér bázisainak közös elemszámát dimenziójának nevezzük.

A 4.3 tételből következik, hogy ha $\mathbf{V}$ n -dimenziós, akkor $\mathbf{V}$ -ben bármely, lineárisan független vektorrendszer legfeljebb n , és bármely, generátorrendszer legalább n vektorból áll.

II. FEJEZET

Algebrai testbővítések

1. Tétel Tetszőleges $H \subseteq \mathbb{C}$ számhalmazra létezik legszűkebb olyan számtest, amely H -t tartalmazza; ez a számtest egyértelműen meghatározott, és pontosan azokból a számokból áll, amelyek a $H \cup \{1\}$ számhalmaz elemeiből az összeadás, additív inverzképzés, szorzás és 0-tól különböző elemből történő reciprokképzés véges számú alkalmazásával megkaphatók.

Bizonyítás. Egyrészt a test definíciójából következik, hogy a leírt elemekből álló K számhalmaz test, másrészt pedig minden olyan K^* számtestre, amelyre $H \subseteq K^*$, a K definíciója miatt fennáll, hogy $K \subseteq K^*$.

2. Definíció. A fenti tételben leírt számtestet H által generált számtestnek nevezzük.

3. Definíció. Az $(S; +, \cdot)$ testet a $(T; +, \cdot)$ test résztestének nevezzük, ha:

(1) $(0) \subset S \subseteq T$, és

(2) az $\tau: (S; +, \cdot) \rightarrow (T; +, \cdot)$ leképezés homomorfizmus.

Megjegyzés. Tetszőleges S, T számtestekre $S \subseteq T$ esetén azt mondjuk, hogy T bővítése S -nek. Jelölése: $S|T$.

4. Definíció. Ha K egy számtest és $a \notin K$, akkor a $K \cup \{a\}$ által generált testet a K test a -val való bővítésének hívjuk, és $K(a)$ -val jelöljük.

Megjegyzés. Abban a speciális esetben, ha $a = \sqrt{c}$ ($c \in K$) könnyen igazolható:

1. $K(\sqrt{c}) = K$ ha $\sqrt{c} \in K$

2. $K(\sqrt{c}) = \{a + b\sqrt{c}; a, b \in K\}$ ha $\sqrt{c} \notin K$.

A fenti állítás azt mondja, hogy az $a + b\sqrt{c}$ alakú számok összege, szorzata, különbsége, hányadosa is ugyanilyen alakú szám.

A $\sqrt{c}$ a c komplex szám valamelyik négyzetgyökét jelöli. Mivel a $K(\sqrt{c})$ test nem függ attól, hogy a két négyzetgyök közül melyikről van szó, ez nem okoz félreértést.

5. Definíció.

Legyen L a K test egy bővítése. Az L -et a K négyzetgyökbővítésének nevezzük, ha van K bővítéseinek egy olyan $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{t-1} \subseteq K_t = L$ sorozata hogy minden j -re $K_j = K_{j-1}(\sqrt{c_j})$ valamely $c_j \in K_{j-1}$ számra ($1 \leq j \leq t$) $L \subseteq \mathbf{R}$ esetén (ekkor $K \subseteq \mathbf{R}$ is teljesül) L -et a K valós négyzetgyökbővítésének nevezzük.

Megjegyzés. Az előző fejezetben láttuk, hogy a komplex számok vektortérnek tekinthetők a valós számtest fölött. Ugyanígy bármely $L|K$ testbővítés esetén L vektortér lesz K fölött, ha vektortér összeadásnak a testbeli összeadást, K -beli elemekkel való szorzásnak pedig az ezen elemekkel való testbeli szorzást tekintjük.

6. Definíció. Azt mondjuk, hogy az $L|K$ testbővítés végesfokú, ha L mint K fölötti vektortér véges dimenziós. E vektortér dimenzióját az $L|K$ bővítés fokának nevezzük, és $[L:K]$ -val jelöljük.

7. Tétel Fokszám-tétel. Ha az $L|K$ és az $M|L$ testbővítések végesfokúak, akkor az $M|K$ bővítés is végesfokú, és $[M:K] = [M:L] \cdot [L:K]$.

Bizonyítás. Legyenek $r_1, \dots, r_n$ az L -nek K feletti, és $s_1, \dots, s_k$ az M -nek L feletti bázisa. Kimutatjuk, hogy az $r_i s_j$ elemek ($1 \leq i \leq n, 1 \leq j \leq k$) az L -nek egy K feletti bázisát alkotják. Tekintsük az M egy tetszőleges s elemét. A feltétel szerint ez felírható $s = a_1 s_1 + \dots + a_k s_k$ alakban, ahol $a_1, \dots, a_k \in L$. Ekkor viszont ezek bármelyike - pl. a_i - felírható $a_i = c_{i1} r_1 + \dots + c_{in} r_n$ alakban, alkalmas K -beli c_{ij} elemekkel. Ez éppen azt jelenti, hogy a fenti $r_i s_j$ elemek generátorrendszert alkotnak.

Lineáris függetlenségük a következőképp látható be. Tegyük fel, hogy valamelyik K -beli d_{ij} együtthatókkal képzett lineáris kombinációjuk 0. Tekintsük ekkor az $e_j = d_{1j} r_1 + \dots + d_{nj} r_n$ elemeket. Ezek - mint L -beli elemek szorzatainak az összegei - maguk is L -beliek; s a disztributivitás alapján teljesül rájuk az $e_1 s_1 + \dots + e_k s_k = 0$ feltétel. Az s -ek L feletti lineáris függetlensége miatt ebből következik, hogy minden $e_i = 0$; s az r -ek K feletti függetlenségét figyelembe véve kapjuk, hogy minden egyes d_{ij} is 0-val

egyenlő. Így valóban bázist kaptunk, s mivel a bázis elemszáma megegyezik a vektortér dimenziójával, ezért a fokszámtételt igazoltuk. $\square$

8. Tétel (az előző tétel következménye): Ha L négyzetgyökbővítése K -nak, akkor $[L : K]$ 2-hatvány.

Bizonyítás. Tegyük fel, hogy a feltétel teljesül. A $K(\sqrt{c})$ ($c \in K$) alakú testek

leírásából (lásd fent) adódik, hogy minden j -re ($1 \leq j \leq t$)

$$[K_j : K_{j-1}] = [K_{j-1}(\sqrt{c_j}) : K_{j-1}] = 1 \text{ vagy } 2$$

A fokszám-tétel szerint $[L : K]$ ezek szorzata, tehát 2-hatvány. $\square$

9. Tétel Legyen K egy tetszőleges számtest, $a \in \mathbb{C}$ pedig az, $f(x) \in K[x]$

irreducibilis főpolinom egy gyöke. Ekkor:

(1) bármely, $h(x) \in K[x]$ -re $h(a) = 0 \Leftrightarrow f(x) \mid h(x)$

(2) $f(x)$ az a elem minimálpolinomja $K[x]$ fölött,

(3) $K(a) = \{g(a) : g(x) \in K[x]\}$,

(4) $K(a)$ minden eleme egyértelműen előáll $r(a)$ alakban, ahol $r(x) \in K[x]$, és $r(x)$ vagy a zérópolinom vagy fokszáma kisebb $f(x)$ fokszámánál.

(5) $[K(a) : K]$ megegyezik $f(x)$ fokszámával.

Bizonyítás.

(1) - (2) a feltételekből és a polinomokból tanultakból (lásd előző fejezet) nyilvánvaló.

(3) jelöljük az egyenlőség jobb oldalán álló számhalmazt L -l. Ekkor

$K(a) \supseteq L$, továbbá $K \subseteq L$ és $a \in L$. Ha belátjuk, hogy L test, akkor $K(a)$

definíciója alapján következik a $K(a) \subseteq L$, tartalmazás is. Az L definíciójából nyilvánvaló, hogy bármely $c, d \in L$ elemekre $c + d, -c, cd \in L$.

Legyen $c = g(a) \in L, c \neq 0$. Ekkor $f(x) \nmid g(x)$, azaz $f(x)$ irreducibilitása miatt $f(x)$ és $g(x)$ relatív prímek, így vannak olyan alkalmas $u(x), v(x) \in K[x]$ polinomok, hogy $f(x)u(x) + g(x)v(x) = 1$. Behelyettesítve az a elemet kapjuk, hogy

$1 = f(a)u(a) + g(a)v(a) = cv(a)$, ahonnan $1/c = v(a) \in L$, tehát L test.

(4) Az előállítás létezése (3)-ból adódik, hiszen ha $g(x)$ polinom $f(x)$ -szel osztva a maradék $r(x)$, akkor $g(a) = r(a)$. Az egyértelműség igazolásához

feltesszük, hogy legalább két előállítás létezik. Alkalmazzuk (1)-et e két polinom különbségére. (5) Az $f(x)$ fokszámát n -nel jelölve a (4) azt állítja -vektorterekre átfogalmazva-, hogy $K(a)$ -ban mint K fölötti vektortérben bázist alkotnak az $1, a, a^2, \dots, a^{n-1}$ elemek. $\square$

10. Tétel Legyen K tetszőleges számtest. Ekkor bármely $a \in \mathbb{C}$ komplex számra ekvivalensek a következő állítások :

- (1) a $K(a)|K$ bővítés végesfokú,
- (2) a egy $K[x]$ -beli nem zéró polinom gyöke,
- (3) létezik olyan $f(x) \in K[x]$ irreducibilis főpolinom, amelynek a gyöke.

Bizonyítás.

(1) $\Rightarrow$ (2). Legyen a $K(a)|K$ bővítés foka n . Ekkor a $K(a)$ (K fölötti) vektortérben lineárisan összefüggő rendszert alkotnak az $1, a, a^2, \dots, a^n$ elemek, így alkalmas $c_0, c_1, c_2, \dots, c_n \in K$, nem csupa 0 elemekre:

$$c_n a^{n+1} + \dots + c_2 a^2 + c_1 a + c_0 = 0.$$

(2) $\Rightarrow$ (3). A polinomoknál tanultakból következik, hogy ha a gyöke egy $g(x) \in K[x]$ nem zéró polinomnak, akkor a gyöke a $g(x)$ irreducibilis felbontásában szereplő valamelyik irreducibilis tényezőnek.

(3) $\Rightarrow$ (1). Az előző (9.) tételből következik. $\square$

III. FEJEZET

Szerkesztések elmélete

Alexandriában, Kr.e.300 körül alkotta meg Euklidész görög matematikus főművét. az Elemek-et. A könyv az akkori ismereteket foglalta össze, rendszerezte, legnagyobb érdeme mégis a geometria axiomatikus felépítése volt. Olyan axiómarendszert alkotott Euklidész, amelynél tökéletesebbet a XIX. század végéig nem sikerült összeállítani. A definíciók mellett kilenc axióma (sarkigazság, melyet a logikus gondolkodás érdekében kényszerülünk elfogadni, tehát kényszerítő erejűek), és öt posztulátum (nem a gondolkodásnak alappillérei, tehát elfogadásuk nem kötelező) található. A posztulátumok közül az alábbiak (az első három) fektetik le az euklideszi szerkesztések alapjait:

- »(1) Követeltessék, **hag**y minden pontból minden ponthoz legyen egyenes húzható.
- (2) És hogy véges egyenes vonal egyenesben folytatólag meghosszabbítható legyen.
- (3) És hogy minden középponttal és távolsággal legyen kör rajzolható.«

Az euklideszi szerkesztésekhez tehát csak két eszközt, a körzőt és a vonalzót használhatjuk. A megengedett szerkesztési lépések a következők:

- (1) két egyenes metszéspontjának kijelölése,
- (2) egyenes és kör metszéspontjának kijelölése.
- (3) két kör metszéspontjainak kijelölése.

Ezeket alapszerkesztéseknek nevezzük. Egy pontot akkor tekintünk megszerkesztettnek, ha a fenti három lépés valamelyikeként kapjuk. A szerkesztés tehát olyan eljárás, amely során előre megadott pontokból kiindulva körök és egyenesek metszéspontjaként - lépésről lépésre - újabb és újabb pontokat szerkesztünk.

Megjegyzés: szükséges megemlíteni, hogy az iskolában tanult szerkesztések nem szigorú értelemben vett euklideszi szerkesztések; hiszen például a szakaszfelező-merőleges szerkesztésénél úgy tanítják, hogy a két végpontból tetszőleges (a

szakasz felénél hosszabb) sugarú köröket rajzolva a metszéspontjaikat összekötő egyenes lesz a szakaszfelező. Euklideszi szerkesztéseknél viszont csak az adott, vagy a már megszerkesztett pontok távolságát vehetem körzőnyílásba, illetve csak ilyen pontokba szűrhetem a körzőt.

Belátható azonban, hogy az ún. »megengedő« szerkesztések (vonalzó csúsztatás, billentés merőleges-állítás, stb. ...) ekvivalensek az euklideszi szerkesztéssel. Lényeges még, hogy a vonalzon nincs semmilyen jelölés; ha például megengednénk egy adott szakasz bejelölését a vonalzóra, akkor belátható, hogy így olyan pontok is megszerkeszthetők lennének, amelyek euklideszi úton nem. Az euklideszi szerkesztés látszólag egy egyszerű «játék» adott játékszabályokkal. Az, hogy mitől olyan izgalmasak ezek a szerkesztések, talán annak köszönhető, hogy kiderült egyes problémákról, hogy megoldhatatlanok, sőt ennek az oka nem geometriai, hanem algebrai természetű. A szerkeszthetőség tárgyalását néhány, jelölés bevezetésével kezdjük:

Legyen H a sík pontjainak egy halmaza. A legalább két H -beli pontra illeszkedő egyenesek halmazát e_H , a H -beli középpontú és két H -beli pont távolságával megegyező sugarú körök halmazát k_H jelöli.

1. Definíció. Legyen H a sík pontjainak egy halmaza. A sík: egy P pontja

közvetlenül szerkeszthető H -ból, ha P :

- (1) két e_H -beli egyenes metszéspontja, vagy
- (2) egy e_H -beli egyenes és egy k_H -beli kör metszéspontja, vagy,
- (3) két k_H -beli kör metszéspontja.

2. Definíció. Legyen H a sík pontjainak egy halmaza, H -ból kiindulva definiáljuk ponthalmazok egy végtelen sorozatát a következőképpen :

$$H_0 = H$$

$$H_{i+1} = H_i \cup \{P; \text{ minden olyan pont, amely közvetlenül szerkeszthető } H \text{-ből}\}$$

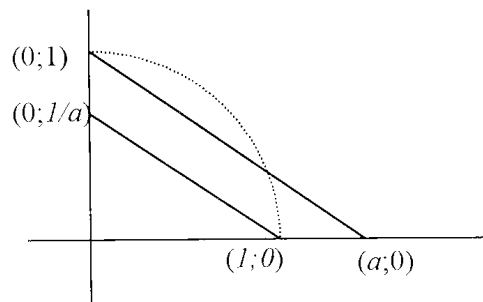
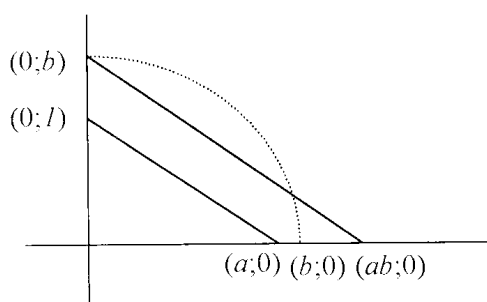
$$(i = 0, 1, 2, \dots)$$

Akkor mondjuk, hogy P megszerkeszthető H -ból, ha $P \in H_i$ valamelyik i -re.

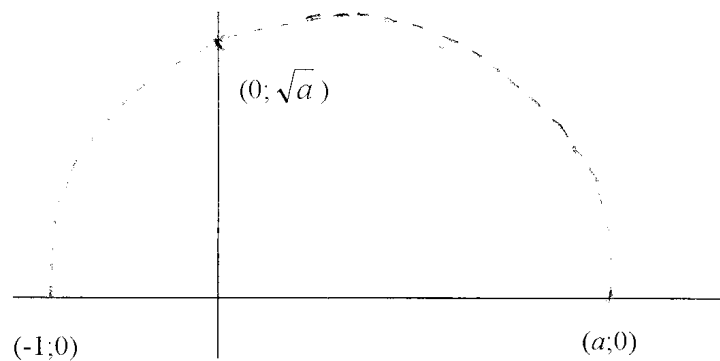
Ha az első H halmaz üres, vagy egy eleme van, akkor további pontok a fenti módszerrel nem szerkeszthetők. Ezért feltehetjük, hogy H legalább kételemű. Ahhoz, hogy a szerkeszthetőség problémáját (azaz egy bizonyos pont megszerkeszthetőségét lefordíthassuk az algebra nyelvére felvesszünk a síkon derékszögű (Descartes-féle) koordináta-rendszert. A pontokat itt valós szám-párokkal adjuk meg. A tengelyeket az általánosság megszorítása nélkül felvehetjük úgy, hogy az origó $O = (0;0)$ és az egyik egységpont $E = (1;0)$ H -beli legyen.

Ekkor világos, hogy:

- O és E pontokból a két tengely megszerkeszthető [az egyik éppen az OE egyenes, a másikat megkaphatjuk például a $(-1;0)$ és E pontok szakaszfelezőjének ismert szerkesztésével),
- egy $P(a; b)$ pont akkor és csak akkor szerkeszthető, ha az $A(a;0)$ és $B(0;b)$ pontok szerkeszthetők,
- egy tetszőleges α szög szerkesztése ekvivalens a $(\cos \alpha ; \sin \alpha)$ pont megszerkesztésével,
- valahányszor az $A(a,0)$ és $B(0;b)$ pontok szerkeszthetők, mindannyiszor megszerkeszthetők a következő pontok is :
- $(-a;0)$ [O -ba szúrom a körzót és: $A(a;0)$ -ból elmetszem OE tengelyt]
- $(-a+b;0)$ [$A(a;0)$ -ba szúrok és $r = OB$ sugárral elmetszem a tengelyt] (ez nem szigorú értelemben vett euklideszi szerkesztés)
- $(ab;0)$ [hasonlósággal, az alábbi (bal oldali) ábra alapján]
- $(1/a;0)$ ($a \neq 0$) [szintén hasonlóság alapján, a jobboldali ábra szerint]



$-(\sqrt{a}; 0)$ ($a \geq 0$) [Thalesz-kör segítségével]



A fentiekből kitűnik, hogy a H pontjainak koordinátái olyan K számtestet generálnak, amely részteste a valós számoknak. ($K \subseteq \mathbf{R}$)

Ezek után kimondjuk és bebizonyítjuk a szerkeszthetőség algebrai átfogalmazására vonatkozó tételt:

3. Tétel Legyen H egy tetszőleges ponthalmaz a síkban. Vegyük fel a koordináta-rendszert a már ismertetett módon. Legyen K a H -beli pontok koordinátái által generált számtest ($K \subseteq \mathbf{R}$) Ekkor a következő két állítás egyenértékű:
- (1) P megszerkeszthető H -ból;
 - (2) K -nak létezik olyan valós négyzetgyökbővítése, amely P mindkét koordinátáját tartalmazza.

Bizonyítás. $(1) \Rightarrow (2)$. A koordináta-rendszerben az egyeneseket és a köröket egyenleteikkel határozzuk meg. Bármely két ilyen alakzat metszéspontjai olyan pontok, melyek koordinátái mindkét alakzat egyenletét kielégítik.

Egy e_H -beli egyenes egyenlete: $\mathbf{Ax} + \mathbf{By} + \mathbf{C} = 0$ ($\mathbf{A}, \mathbf{B}, \mathbf{C} \in K$).

Egy k_H -beli kör egyenlete: $x^2 + y^2 + \mathbf{Dx} + \mathbf{Ey} + \mathbf{F} = 0$ ($\mathbf{D}, \mathbf{E}, \mathbf{F} \in K$).

Attól függően, hogy P koordinátáit melyik alapszerkesztésből kaptuk, három esetet különböztetünk meg:

1. két e_H -beli egyenes metszéspontjaként; ekkor a metszéspont koordinátái benne vannak K -ban (ez az elsőfokú kétismeretlenes egyenletrendszer megoldásából következik)

2. egy e_H -beli egyenes és egy k_H -beli kör metszéspontjaként; a koordináták ekkor vagy K -beli elemek, vagy benne vannak K valamelyik valós négyzetgyökbővítésében (a másodfokú egyenlet megoldóképletéből közvetlenül adódik)

3. két k_H -beli kör metszéspontjaként; ekkor ugyanazt mondhatjuk el, mint a 2. esetben.

Az előbbieket alapján világos a következő:

Ha egy F pont a H pontthalmazból közvetlenül szerkeszthető és a H -beli pontok koordinátái által generált számtest K , akkor a $H \cup \{P\}$ pontthalmazbeli pontok koordinátái által generált számtest vagy K , vagy $K(\sqrt{c})$ valamely $c \in K$ nemnegatív valós számra.

A fentiekből, valamint abból a tényből, hogy az alapszerkesztéseket véges sokszor alkalmaztuk (a szerkesztés definíciója miatt) következik az állítás.

(2) $\Rightarrow$ (1) Tegyük fel, hogy a P koordinátái benne vannak a K számtest egy valós négyzetgyökbővítésében, ahol: $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{t-1} \subseteq K_t = L$,

$K_j = K_{j-1}(\sqrt{c_j})$ minden $1 \leq j \leq t$ -re.

A koordináta-rendszer bevezetésekor tett megfigyeléseket felhasználva egyszerűen igazolható j szerinti teljes indukcióval, hogy minden j -re ($1 \leq j \leq t$) a K_j test bármely a eleme esetén az $(a; 0)$ pont H -ból megszerkeszthető. $\square$

4. Tétel Legyen H egy tetszőleges pontthalmaz a síkban, s vegyünk fel egy koordináta-rendszert a meghatározott módon. Legyen K a H -beli pontok koordinátái által generált számtest ($K \subseteq \mathbf{R}$). A sík egy $P = (a; b)$ pontja akkor és csak akkor szerkeszthető meg H -ból, ha:

(1) a és b algebrai elem K fölött, és

(2) a és b minimálpolinomjának fokszáma 2-hatvány.

Bizonyítás. Ha F megszerkeszthető H -ból, akkor van K -nak olyan L

négyzetgyökbővítése, hogy $a, b \in L$ (lásd előző tétel). Ekkor $K(a) \subseteq L$, másrészt az előző fejezetből tudjuk, hogy $[L:K]$ 2-hatvány. Ezért a $K(a)|K$ bővítés végesfokú, így a algebrai elem K fölött. Figyelembe véve, hogy:

$$[L:K] = [L:K(a)] \cdot [K(a):K],$$

a $[K(a);K]$ is 2-hatvány. Ez utóbbi viszont megegyezik az a szám K fölötti minimálpolinomjának fokszámával. Mivel a b koordinátára ugyanez az okoskodás alkalmazható, a tétel állítását beláttuk. $\square$

Megjegyzés.

1. A fenti tételben szereplő (1) , (2) feltételek teljesülése önmagában általában nem elegendő a P pont megszerkesztéséhez.

2. Az előző tételeket koordináták helyett komplex számos megközelítésre analóg módon lehet tárgyalni. Például a 4. tétel megfelelője a következőképpen szól:

4(b) Tétel Legyen H tetszőleges ponthalmaz a síkban, és tekintsük az I. fejezetben említett komplex számsíkot. Legyen K^* a H -beli pontoknak megfelelő komplex számok és konjugáltjaik által generált számtest. A sík egy P pontja csak akkor szerkeszthető meg H -ból, ha a p -nek megfelelő z komplex számra:

(1) z algebrai K^* fölött, és

(2) K^* fölötti minimálpolinomjának fokszáma 2-hatvány.

3. Abban a speciális esetben, ha $K = \mathbf{Q}$, a szerkeszthetőség vizsgálata -a polinomokról tanultak alapján - visszavezethető egész együtthatós polinomok vizsgálatára.

Ezek után a következő fejezetekben alkalmazzuk az eddigi eredményeket konkrét szerkesztési problémák vizsgálatára.

IV. FEJEZET

Nevezetes szerkesztési feladatok

Ebben a fejezetben kerül sor a bevezetőben említett ókori szerkesztési problémák megoldhatatlanságának bizonyítására.

1. A kör négyszögesítése

A feladat közismert: szerkesztendő adott r sugarú kör területével megegyező területű négyzet. Az ókorban e téren a legnagyobb eredményt Hippokratész érte el, aki két különböző sugarú körív által határolt rész (ún. holdacska) területével egyező háromszöget szerkesztett. Lényeges előrelépés ezután majd csak a XIX. század elején született. De mielőtt rátérnénk, hogy mi volt ez a matematikatörténeti szempontból kiemelkedő felfedezés, vizsgáljuk meg a problémát algebrai szempontból.

Az r sugarú kör területe $t_k = r^2\pi$ egy a élű négyzeté $t_a = a^2$. A feladat a $t_k = t_a$ egyenlőséggel ekvivalens. Ekkor nyilván $r^2\pi = a^2$, amiből $a = r\sqrt{\pi}$

A kört a középpontjával, és egy tetszőleges pontjával tekintünk adottnak (lásd előző fejezet). Vegyük fel a tárgyaláshoz szükséges koordináta-rendszer tengelyeit úgy, hogy a kör középpontja az $O(0;0)$, az adott pont pedig $E(1;0)$ legyen! Ekkor a kiindulásul megadott pontok koordinátái $\{0,1\}$ által generált számtest éppen $\mathbf{Q}$. A feladat tehát mivel most $r=1-a/\sqrt{\pi}$ pont megszerkesztését kívánja. Nyilvánvaló tény, hogy $\sqrt{\pi}$ szerkesztése ekvivalens π megszerkesztésével. A kérdést az eddig tanultak alapján feltehetjük úgy is, hogy π algebrai-e $\mathbf{Q}$ fölött, azaz van-e olyan racionális együtthatós polinom, amelynek π gyöke. Erre a kérdésre adott nemleges választ 1882-ben F. Lindemann német matematikus, megoldva ezzel a körnégyszögesítés évezredes problémáját. $\square$

2. A kör kiegyenesítése

A feladat az előző "kistestvére": szerkesztendő adott r sugarú kör kerületével egyenlő hosszúságú szakasz.

Az r sugarú kör kerülete $k=2r\pi$. Ha a koordináta-rendszert az előző pontban meghatározott módon vesszük fel, akkor a generált számtest ismét $\mathbf{Q}$. A feladat, 2π a pont megszerkesztése egyenértékű π szerkesztésével, ami Lindemann tétele miatt lehetetlen. Tehát sem a kör négyszögesítése, sem a kör kiegyenesítése euklideszi úton nem oldható meg. $\square$

3. Kockakettőzés (Délósi probléma)

A feladat keletkezését Plutarkhosz görög történetíró jegyezte fel. Egyszer Délósi szigetén pestis tombolt. A délósiak elkeseredettségükben a Delphoi-i jósdához fordultak tanácsért. Ott azt mondták nekik, hogy ha meg akarnak szabadulni a járványtól, akkor cseréljék ki Apolló Delphoi-i kocka alakú oltárkövét kétszer akkora kocka alakú oltárkövel. Ez az aránylag könnyűnek látszó feladat a görögöknek legyőzhetetlen nehézséget okozott. Azt felismerték, hogy ha a az eredeti kocka élének hossza és x a keresett élhossz, akkor az

$$a:x = x:y = y:2a$$

alapján a feladat ekvivalens a és $2a$ közötti középarányosok szerkesztésével. Sokan próbálkoztak a megoldással, de - a sokat ígérő felfedezések (kúpszeletek, konkhoisz, cisszoisz és más transzcendens görbék) ellenére - ez megnyugtató módon senkinek sem sikerült.

Az algebrai tárgyalás végett vegyük az eredeti kocka élét egységnyi hosszúságúnak, és a koordináta - tengelyt vegyük fel úgy, hogy O és E a szakasz két végpontja legyen. A megadott pontoknak megfelelő $(0$ és $1)$ számok által generált számtest ismét a racionális számok $\mathbf{Q}$ teste. A feladat tehát a két térfogategységnyi kocka élhosszának, azaz a $\sqrt[3]{2}$ pontnak a megszerkesztése. A $\sqrt[3]{2}$ az $x^3-2 \in \mathbf{Q}[x]$ polinomnak a gyöke. Ez a polinom azonban irreducibilis $\mathbf{Q}$ fölött (ezt a Rolle - tétel vagy a Schönemann – Eisenstein - tétel segítségével

ellenőrizhetjük, ezért ez éppen a $\sqrt[3]{2}$ minimálpolinomja $\mathbf{Q}$ fölött. Mivel a fokszáma nem 2 - hatvány, ezért $\sqrt[3]{2}$ nem szerkeszthető meg euklideszi úton.□

4. Szögharmadolás

Tetszőleges szög fele a közismert módon mindig megszerkeszthető. A kérdés az, hogy létezik-e olyan általános eljárás, amellyel tetszőleges szög harmadát meg tudjuk szerkeszteni.

Be fogjuk bizonyítani, hogy ilyen általános módszer nem létezik. Természetesen vannak olyan szögek (90° , 180° , stb.), amelyek harmadolhatók. Azt kell megmutatnunk, hogy a harmadolásra nem adható meg minden szög esetében ilyen érvényes eljárás. Ehhez elég egyetlen olyan szöget találni, amelyik nem harmadolható. Így tehát ha ki tudjuk mutatni, hogy például a 60° -os szög nem harmadolható körző és vonalzó egyedüli használatával, akkor bebizonyosodna a sejtésünk.

A 60° -os szög két pontból kiindulva közismert módon szerkeszthető. Azt kell megmutatnunk, hogy a 20° -os szög nem szerkeszthető. A koordináta tengelyeket vegyük fel ismét úgy, hogy a kiindulási két pont O illetve E legyen. A 20° -os szög szerkesztése ekvivalens az $u = 2\cos 20^\circ$ hosszúságú szakasz szerkesztésével. Ismert trigonometrikus összefüggések alapján :

$$\cos 3\phi = 4\cos^3 \phi - 3\cos \phi$$

ahonnan $\phi = 20^\circ$ -ra azt kapjuk, hogy $u = 2\cos 20^\circ$ gyöke az $f(x) = x^3 - 3x - 1 \in \mathbf{Q}[x]$ polinomnak. Mivel $f(x)$ -nek nincs racionális gyöke (ez a már említett Schönemann -Eisenstein tétellel ellenőrizhető), ezért $f(x)$ irreducibilis $\mathbf{Q}$ fölött, s így $f(x)$ éppen $u = 2\cos 20^\circ$ minimálpolinomja $\mathbf{Q}$ fölött. Mivel $f(x)$ fokszáma nem 2-hatvány, ezért $u = 2\cos 20^\circ$ nem szerkeszthető meg, azaz a 60° -os szög nem harmadolható.□

Megjegyzés.

1. Arkhimédész a szögharmadolásra olyan vonalzót használt, amelyre bizonyos szakaszt előre bejelölt (ez nem euklideszi szerkesztőeszköz). Az eredeti szögnek az egyik szárát meghosszabbította, majd a szög csúcsából

egy tetszőleges r sugárral kört rajzolt. A vonalzóra bejelölte A és B pontokat úgy, hogy $AB = r$ legyen, majd a vonalzót addig mozgatta, míg B mindvégig a körön mozogva az A rá nem került a meghosszabbított szögszárra, s átment a kör és a másik szögszár metszéspontján.

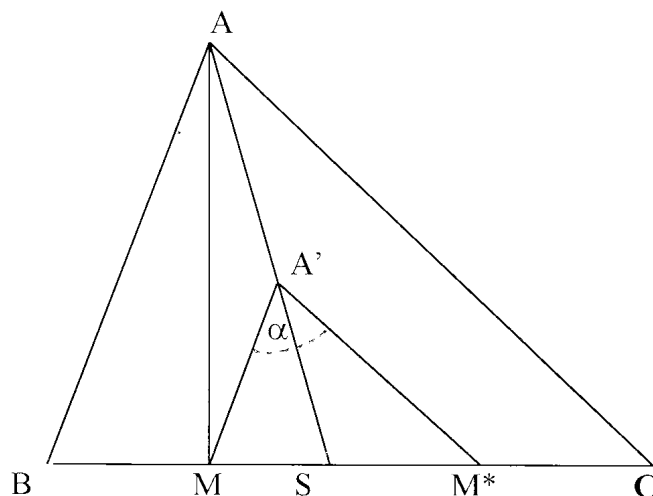
2. Ide kívánczik még egy elemi geometriából ismert, a fentiek ismeretében meghökkentő tétel:

Morley-tétele. Bármely háromszög szomszédos szögharmadolóinak három metszéspontja szabályos háromszöget határoz meg.

5. Háromszögszerkesztések

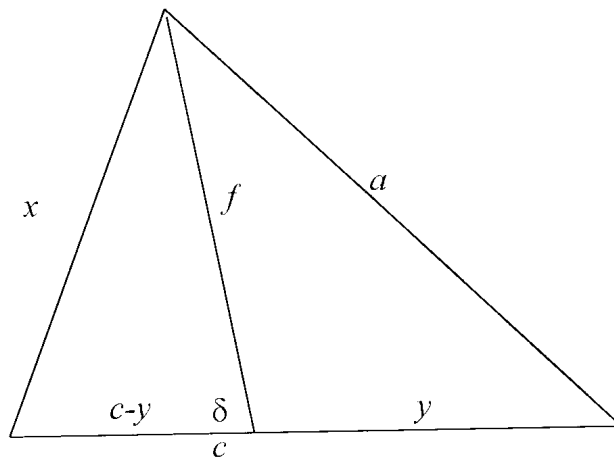
A szerkesztési feladatok közül a háromszögek szerkesztése tűnik a legegyszerűbbnek, hiszen már általános iskolában megtanítják, hogy egy háromszög megszerkesztéséhez elég három - egymástól független – adat. Azt gondolnánk, hogy bármely három adatból meg is szerkeszthető az általuk meghatározott háromszög. Be fogjuk bizonyítani, hogy ez nincs így, azaz tudunk olyan három adatot mondani amelyekből nem szerkeszthető meg a háromszög. Vizsgáljuk meg a következő két példát!

(1) Szerkesszünk háromszöget, ha adott egy szöge(α), valamint ebből a csúcsból kiinduló magassága (AM), és súlyvonala (AS)! (nyilván $AM < AS$)



Megoldás: felezzük meg a súlyvonalat és rajzoljunk fölé Thalesz-kört! A - ből a magassággal elmetszem a kört, a metszéspont (bármelyik a kettő közül) M. Húzzuk meg az S, M pontokra illeszkedő egyenest (ez a háromszög egyik oldalegyenese)! S-be szúrva a körzött tükrözzük M-et S-re (M*)! Ezután MM* szakasz fölé az ismert módon szerkesszünk α szögű látókört! A súlyvonal és a látókör metszéspontja A'. Könnyen ellenőrizhető, hogy az így kapott A'MM* háromszög az eredetihez hasonló, a hasonlóság centruma S. Ha A-n keresztül párhuzamosokat húzunk A'M-mel és A'M*-gal, akkor ezeknek az ismert oldalegyenessel való metszéspontjai lesznek a B és C csúcsok. Mivel minden szerkesztési lépést a kiindulási adatokból alapszerkesztések véges számú egymás utáni végrehajtása után kaptuk, ezért a fenti feladat mindig megoldható és általános esetben két megoldása van. $\square$

(2) Szerkesszünk háromszöget, ha adott két oldala a és c, valamint a c-vel szemközi szög felezője f!



Az ábra jelöléseit használva, a szögfelező tételből következik, hogy:

$$x : a = c-y : y \text{ innen } y = \frac{ac}{a+x} \text{ és } c-y = \frac{cx}{a+x}$$

$$\text{Az } x\text{-re felírva a cosinus-tételt kapjuk, hogy } x^2 = \frac{c^2 x^2}{(a+x)^2} + f^2 - \frac{2cx}{a+x} f \cos \delta$$

Ezután felírjuk a cosinus-tételt az a oldalra (az a, y, f háromszögben), majd kifejezve $\cos \delta$ -t ($\cos(180^\circ - \delta) = -\cos \delta$ azonosság alapján ezt megtehetjük), és visszaírva a fenti egyenletbe kapjuk, hogy : $a(a+x) = \frac{c^2}{(a+x)^2} a(a+x) + \frac{a+x}{x} f^2$, egyszerűsítés és $x(a+x)$ -szel való beszorzás után az $ax(a+x)^2 - ac^2x + (a+x)^2 f^2$ egyenlethez jutunk.

Ha a kiindulási adatokat úgy választjuk, hogy $a = c = f = 1$ legyen (ilyen háromszög létezik!), ekkor a generált számtest ismét $\mathbf{Q}$, így azt kapjuk, hogy a harmadik oldal (x) gyöke az $x^3 + x^2 - 2x - 1 = 0$ irreducibilis harmadfokú egyenletnek, ezért ez x minimálpolinomja $\mathbf{Q}$ fölött. Mivel a fokszáma nem 2-hatvány, ezért x nem szerkeszthető.!!

Megjegyzés. Egy háromszöget általában az oldalak (a, b, c) , szögek (α, β, χ) magasságok (m_a, m_b, m_c) , súlyvonalak (s_a, s_b, s_c) , és a szögfelezők (f_a, f_b, f_c) közül hárommal adnak meg. Ez $\binom{15}{3} = 455$ esetet határoz meg. Ezek közül 95 lényegileg különböző eset van (nem tekintjük különbözőnek a háromszög szerkesztését például az a, b, m_c , és b, c, m_a adatokból). A 95 eset közül kettő (α, β, χ) és (a, m_b, χ) nem határozza meg egyértelműen a háromszöget. A fennmaradó 93 esetből 63 szerkeszthető, 30 pedig nem, noha a háromszög minden esetben létezik.

V. FEJEZET

Szabályos sokszögek szerkesztése

Egyik legfontosabb és legérdekesebb szerkesztési feladat, szokták még körosztás néven említeni. A feladat megvizsgálni, hogy milyen n -ekre szerkeszthető meg a szabályos n -szög. Nyilván a feladat ekvivalens n olyan pont szerkesztésével, amely egy kört n egyenlő ívre bont. A körosztást az ókorban az n páratlan értékei közül a 3, 5 és 15 számokra tudták csak elvégezni körző és vonalzó segítségével. Mivel körívet tudtak felezni, így még ismerték a $3 \cdot 2^k$, $5 \cdot 2^k$, $15 \cdot 2^k$ oldalú szabályos sokszögek szerkesztési eljárását is. Az ókori eredmények után a körosztásban az első jelentős lépést Gauss tette, amikor felfedezte a szabályos 17-szög szerkesztését. Később ő adott szükséges és elegendő feltételt a körosztás elvégezhetőségére.

1. Tétel (Gauss) Ahhoz, hogy a körnek n egyenlő ívre ($n > 2$) osztását körzővel és vonalzóval el lehessen végezni, szükséges és elegendő, hogy n prímtényezőss felbontása $n = 2^k p_1 \dots p_r$ ($k, r \geq 0$) alakú legyen ahol $p_1 \dots p_r$ páronként különböző páratlan prímelek, és $p_1 - 1, \dots, p_r - 1$ mindegyike 2-hatvány.

Megjegyzés.

1. Ha egy p páratlan prímszámra $p-1$ 2 hatvány, mondjuk $p=2^m+1$, akkor m maga is 2-hatvány (különben m bármely $v > 1$ páratlan prímosztójára $2^{m/v}+1$ valódi osztója lenne 2^m+1 -nek). A $p(n)=2^{2^n}+1$ alakú prímszámokat Fermat-prímeknek nevezzük. Az első öt ilyen alakú szám mindegyike prím (3, 5, 17, 257, 65537) $n=5$ esetén már összetett számot kapunk. A felsoroltakon kívül jelenleg nem ismerünk több Fermat-prímet, s az sem eldöntött, hogy véges sok ilyen szám van-e.

2. A körosztás lehetőségének vizsgálatánál elég azokra az esetekre szorítkoznunk, amikor n páratlan prímszám, vagy ilyen szám négyzete. Ezt a következőképp láthatjuk be: legyen n a páratlan n_1 és n_2 relatív prímszámok szorzata. Ekkor a kör $n_1 n_2$ ívre való osztását vissza tudjuk vezetni n_1 és n_2 ívre való osztására. Mivel n_1 és n_2 relatív prímelek, ezért létezik olyan k_1 és k_2

egész szám, hogy $k_1 n_2 - k_2 n_1 = 1$ teljesül. Szorozzuk meg az egyenletet $\frac{2\pi}{n_1 n_2}$ -

vel! Ekkor a $\frac{2\pi}{n_1} k_1 - \frac{2\pi}{n_2} k_2 = \frac{2\pi}{n_1 n_2}$ egyenlőség szerint a körosztást úgy

végezhetjük, hogy közös kezdőpontból n_1 illetve n_2 ívre osztjuk a kört, majd kijelölve ugyanazon irányba a k_1 -edik, illetve k_2 -edik osztópontot, e két pont által meghatározott körív a körnek $n_1 n_2$ -ed része.

Bizonyítás. Az általánosság megszorítása nélkül feltehető, hogy a kör, amelybe a szabályos sokszöget szerkesztjük, egységnyi sugarú és a középpontjával $(0;0)$ s az $(1;0)$ pontjával van megadva. A koordináták által generált számtest ismét $\mathbf{Q}$. A körbe írt szabályos n -szög szerkeszthetősége - a komplex

számokról tanultak alapján - ekvivalens $\varepsilon_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ az

megszerkeszthetőségével.

A megjegyzések alapján elég a prímszámú oldalú szabályos sokszögekkel foglalkoznunk.

2. Definíció. Tetszőleges p prímre a p -edik körosztási polinom

$$\chi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1, \text{ a } p^2\text{-edik körosztási polinom pedig}$$

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

Nyilvánvalóan ε_p gyöke χ_p -nek, ε_{p^2} pedig χ_{p^2} -nek.

3. Tétel Tetszőleges p prímre ε_p $\mathbf{Q}$ fölötti minimálpolinomja χ_p , ε_{p^2} $\mathbf{Q}$ fölötti minimálpolinomja pedig χ_{p^2} .

Bizonyítás. Elegendő megmutatni, hogy a $\chi_p, \chi_{p^2} \in \mathbf{Z}[x]$ polinomok

irreducibilisek $\mathbf{Q}$ fölött. Ezek a polinomok pontosan akkor irreducibilisek, ha az $f(y) = \chi_p(y+1)$, illetve $g(y) = \chi_{p^2}(y+1)$ polinomok irreducibilisek.

$$\text{Az } f(y) = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{p-1} y^{p-2} + \dots + \binom{p}{2} y + p \text{ polinom irreducibilitása}$$

a Schönemann- Eisenstein - tétel alkalmazásával belátható.

A g polinomra vonatkozó számolás leegyszerűsítése céljából vezessük be a következő jelölést: tetszőleges $h, h' \in \mathbb{Z}[y]$ polinomokra $h \approx h'$ jelentse azt, hogy a h, h' polinomok főegyütthatója megegyezik, különbségük pedig $pyH(y)$ alakú, alkalmas $H(y) \in \mathbb{Z}[y]$ polinomra. Az előbbieket miatt például $(y+1)^p \approx y^p + 1$. Ezt felhasználva kapjuk, hogy

$$g(y) = \sum_{k=0}^{p-1} ((y+1)^p)^k \approx \sum_{k=0}^{p-1} (y^p + 1)^k = f(y^p), \text{ ezért felhasználva a Schönemann-}$$

Eisenstein tételt adódik $g(y)$ irreducibilitása. $\square$

Következmény.

1. Ha p páratlan prímszám nem Fermat-prím, akkor ε_p nem szerkeszthető meg.
2. ε_{p^2} egyetlen p páratlan prímre sem szerkeszthető meg.

Mivel szabályos p^2 -szög nem szerkeszthető, ezért a fejezet elején tett megjegyzés miatt szabályos p^k -szög sem szerkeszthető semmilyen $k > 2$ egészre és p páratlan prímre. Ezzel beláttuk, hogy a tételben leírt feltétel szükséges. Rátérhetünk az elegendőség bizonyítására. Azt kell igazolnunk, hogy ha p Fermat-prím, akkor ε_p megszerkeszthető.

A bizonyításhoz szükség lesz egy számelméleti fogalomra és tételre.

4. Definíció. Legyen p tetszőleges prímszám. Azt mondjuk, hogy $q \in \mathbb{Z}$ primitív gyök modulo p , ha $p \nmid q$ és a $q^0=1, q, q^2, \dots, q^{p-2}$ számok páronként különböző maradékot adnak p -vel osztva, azaz e számok maradékai - sorrendtől eltekintve - éppen az $1, 2, \dots, p-1$ számok.
5. Tétel Minden p prímszámhoz létezik primitív gyök modulo p . A bizonyítást nem végezzük el. Útmutatásként: Fermat tétele szerint $q^{p-1} \equiv 1 \pmod{p}$, azaz q^{p-1} p -vel osztva 1 maradékot ad, a q hatványainak maradékai a $(p-1)$ -edikétől kezdve ciklikusan ismétlődnek. A bizonyítás azon alapszik, hogy megmutatjuk $q^{(p-1)/2} \not\equiv 1 \pmod{p}$ -ről, hogy $p-1$ maradékot ad p -vel osztva.

Bizonyítás. Legyen $p=2^m+1$ Fermat-prím. A tétel állítása $p=3$ esetére közismert, ezért feltesszük, hogy $p \geq 5$. Az ε_p számot ezentúl ε -al jelöljük. Látható, hogy $\varepsilon \in \mathbb{Q}$ fölötti. minimálpolinomjának - χ_p -nek a gyökei éppen az $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ komplex

számok, azaz az 1-től különböző p-edik komplex egységgyökök. Rögzítsünk egy q primitív gyököt modulo p. A $\mathbf{Q}(\varepsilon_p)$ test elemeinek leírását (lásd II. Fejezet) felhasználva látható, hogy $\gamma: \mathbf{Q}(\varepsilon) \rightarrow \mathbf{Q}(\varepsilon), f(\varepsilon) \rightarrow f(\varepsilon^q)$ ($f \in \mathbf{Q}[x]$) megfeleltetés leképezés. A γ ismételt végrehajtásával keletkező γ^j ($j=1, 2, \dots$) leképezések:

$$\gamma^j: \mathbf{Q}(\varepsilon) \rightarrow \mathbf{Q}(\varepsilon), f(\varepsilon) \rightarrow f(\varepsilon^{q^j}) \quad (f \in \mathbf{Q}[x])$$

Mivel $\varepsilon^{q^{p-1}}$ identikus leképezés. Ebből az is adódik, hogy γ^j ($j=1, 2, \dots$)

mindegyike bijektív. Könnyen ellenőrizhető, hogy tetszőleges $a, b \in \mathbf{Q}(\varepsilon)$ elemekre és $j \geq 1$ egészre:

$$(a-b) \gamma^j = a\gamma^j + b\gamma^j, \text{ és } (ab) \gamma^j = (a\gamma^j)(b\gamma^j).$$

Tekintsük azokat a komplex számokat, amelyek ε -ból kiindulva γ egymás utáni alkalmazásával kaphatók:

$$\varepsilon = \varepsilon \gamma^0 = \varepsilon^{q^0}, \varepsilon \gamma = \varepsilon^q, \varepsilon \gamma^2 = \varepsilon^{q^2}, \dots, \varepsilon \gamma^{p-2} = \varepsilon^{q^{p-2}} \quad (\varepsilon \gamma^{p-1} = \varepsilon).$$

Mivel q primitív gyök modulo p, ezek a számok - sorrendtől eltekintve - éppen az $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$ számok

Speciálisan: $\varepsilon^{-1} = \varepsilon^{p-1} = \varepsilon^{q^{(p-1)/2}}$, ezért az inverz párok, azaz $\varepsilon \gamma^j$ és $\varepsilon^{-1} \gamma^j = \varepsilon \gamma^{j+(p-1)/2}$ ($0 \leq j < (p-1)/2$), a körön a középpontra szimmetrikusan helyezkednek el.

Képezzünk két összeget a körön szereplő számokból úgy, hogy minden második kerül ugyanabba az összegbe:

$$a_0 = \varepsilon + \varepsilon \gamma^2 + \dots + \varepsilon \gamma^{p-3} \qquad a_1 = \varepsilon \gamma + \varepsilon \gamma^3 + \dots + \varepsilon \gamma^{p-2}.$$

Nyilvánvalóan $a_0 + a_1 = \varepsilon + \varepsilon^2 + \dots + \varepsilon^{p-1} = \chi_p(\varepsilon) - 1 = -1$. Az $a_0 a_1$ szorzatban

minden tag ε hatványa, s mivel az inverz párok ugyanabban az összegben vannak, 1 nincs a tagok között. Így vannak olyan $m_0, \dots, m_{p-2}$ nemnegatív egészek, hogy:

$$a_0 a_1 = m_0 \varepsilon + m_1 (\varepsilon \gamma) + \dots + m_{p-2} (\varepsilon \gamma^{p-2}) \text{ és } m_0 + m_1 + \dots + m_{p-2} = ((p-1)/2)^2.$$

Észrevéve, hogy $a_0 \gamma = a_1$ és $a_1 \gamma = a_0$, az $a_0 a_1$ szorzatra másik előállítás adódik:

$$a_0 a_1 = (a_1 \gamma)(a_0 \gamma) = (a_1 a_0) \gamma = m_0 (\varepsilon \gamma^j) + m_1 (\varepsilon \gamma^2) + \dots + m_{p-2} \varepsilon.$$

A kettő különbségéből $0 = (m_0 - m_{p-2}) \varepsilon + (m_1 - m_0) (\varepsilon \gamma) + \dots + (m_{p-2} - m_{p-3}) (\varepsilon \gamma^{p-2})$.

Az itteni ε - hatványok helyett a megfelelő ε_l ($1 \leq l \leq p-1$) hatványokat írva, majd ε -t kiemelve adódik, hogy ε gyöke egy olyan legfeljebb $(p-2)$ -edfokú polinomnak, amelynek együtthatói - valamilyen sorrendben – az m_0 - m_{p-2} , m_1 - m_0 , ... m_{p-2} - m_{p-3} egészek. Minthogy azonban $\varepsilon \in \mathbf{Q}$ fölötti minimálpolinomjának, χ_p -nek a fokszáma $p-1$, ez csak úgy lehet, ha m_0 - $m_{p-2} = m_1$ - $m_0 = \dots = m_{p-2}$ - $m_{p-3} = 0$. Innen $m_0 = m_1 = \dots = m_{p-2} = (p-1)/4$, s így

$$a_0 a_l = ((p-1)/4) (\varepsilon + \varepsilon^2 + \dots + \varepsilon^{p-1}) = -(p-1)/4.$$

Tehát a_0 és a_l az $x^2 + x - (p-1)/4 \in \mathbf{Q}[x]$ polinom két gyöke, s ily módon a_0, a_l benne van $\mathbf{Q}$ egy K_1 négyzetgyökbővítésében.

Ezután az a_0, a_l összegeket újra osszuk szét két részösszegre úgy, hogy minden második tag kerül ugyanabba a részösszegbe:

$$\begin{aligned} a_{00} &= \varepsilon + \varepsilon^4 + \dots + \varepsilon^{p-5}, & a_{01} &= \varepsilon^2 + \varepsilon^6 + \dots + \varepsilon^{p-3}, \text{ illetve} \\ a_{10} &= \varepsilon\gamma + \varepsilon\gamma^5 + \dots + \varepsilon\gamma^{p-4}, & a_{11} &= \varepsilon\gamma^3 + \varepsilon\gamma^7 + \dots + \varepsilon\gamma^{p-3}. \end{aligned}$$

Nyilvánvalóan $a_{t0} + a_{tl} = a_t \in K_1$ ($t = 0, 1$). Az $a_{t0}a_{tl}$ ($t = 0, 1$) szorzat most is az $\varepsilon\gamma^j$ ($j = 0, 1, \dots, p-2$) számok nemnegatív egész együtthatós lineáris kombinációja. Felhasználva, hogy $a_{t0}\gamma^2 = a_{tl}$ és $a_{tl}\gamma^2 = a_{t0}$, a korábbihoz hasonló gondolatmenettel látható, hogy alkalmas n_{t0}, n_{tl} nemnegatív egészekre,

$$a_{t0} a_{tl} = n_{t0} a_0 + n_{tl} a_l \in K_1.$$

Igy $t=0$ -ra és $t=1$ -re is az a_{t0}, a_{tl} számpár egy $K_1[x]$ -beli másodfokú polinom két gyöke, s ily módon létezik $\mathbf{Q}$ -nak olyan $K_2 (\supseteq K_1)$ négyzetgyökbővítése, amelyre

$$a_{00}, a_{01}, a_{10}, a_{11} \in K_2.$$

Ezt ismételve, az utolsó előtti $((m-1)$ -edik) lépésben eljutunk odáig, hogy az inverz párokat tartalmazó kéttagú részösszegek mindegyike benne van $\mathbf{Q}$ egy alkalmasan választott K_{m-1} négyzetgyökbővítésében. Speciálisan $\varepsilon + \varepsilon^{-1} \in K_{m-1}$. Mivel $\varepsilon\varepsilon^{-1} = 1$, az ε és ε^{-1} egy K_{m-1} fölötti másodfokú polinom gyöke, tehát ε is benne van $\mathbf{Q}$ egy négyzetgyökbővítésében. Ezzel beláttuk, hogy ε megszerkeszthető. $\square$

VI Fejezet

Szerkesztések euklideszitől különböző feltételekkel

Ebben az utolsó fejezetben rátérek a különféle szerkesztési módszerek és szerkesztési eszközök ismertetésére.

1. Egységátrakó vonalzó

Szokás még normavonalzónak is nevezni, ez olyan vonalzó, amelynek élén két pont - alappont - meg van jelölve. A két alappont távolsága a vonalzó egysége vagy normája, de ez nem szükségképpen a hosszúságegység. Ezt az eszközt kétféleképp használjuk:

- (1) közösleges vonalzóként két adott ponton át egyenes húzására,
- (2) az alapszakasznak egy félegyenesre a kezdőpontjából való felmérésére.

Ezzel az eszközzel a következő szerkesztési lépéseket lehet elvégezni.

1. Adott két ponton át egyenes húzása, és két metsző egyenes metszéspontjának kijelölése,
2. Adott szakasz fölrakása adott félegyenesre a kezdőpontjából,
3. Adott szögnek adott félegyeneshez való átrakása a kijelölt oldalra.
4. Egy ponton át adott egyenessel párhuzamos húzása
5. Egy ponton át adott egyenesre merőleges szerkesztése.

A normavonalzóval végzett szerkesztéseket Hilbert - féle szerkesztésnek nevezzük. Belátható, hogy ilyen vonalzóval az euklideszi alapszerkesztések közül általános esetben a körrel való metszéspontok nem szerkeszthetők. Adott pontokból (koordinátákból) Hilbert - féle szerkesztéssel csak olyan pontokat kaphatunk, amelyeknek koordinátái olyan számtest számai, amely m számával együtt a $\sqrt{1+m^2}$ számot is magában foglalja.

Megjegyzés : Ha megengedjük, hogy a normavonalzó egyik alappontját egy, adott O pontba helyezzük és a vonalzót O körül addig forgassuk, míg másik alappontja egy adott e egyenes egy pontjába essék, akkor minden euklideszi alapszerkesztés végrehajtható.

2. Szerkesztések csak körző használatával

Az euklideszi eszközök kiterjesztésével végzett szerkesztések vizsgálatával párhuzamosan folytak a kutatások a másik irányban is, nevezetesen mi történik akkor, ha korlátozzuk a körző és a vonalzó használatát. Az első - elég meglepő eredményt G. Mohr dán matematikus érte el amikor bebizonyította, hogy minden euklideszi szerkesztés elvégezhető vonalzó nélkül, csak körző használatával. Nyilvánvalóan azt kell igazolni, hogy az 1. és 2. alapszerkesztés (lásd III. fejezet) csak körzővel végrehajtható. A bizonyítás azon múlik, hogy olyan k körre vonatkozó inverzióval, amelynek középpontja a szóban forgó egyenesekre, illetve körre nem illeszkedik:

- (1) az egyenesek, illetve a kör is körbe megy át, s e körök csak körzővel megszerkeszthetők az eredeti egyenesekből, illetve körből továbbá
- (2) a kapott metszéspont(ok) csak körző segítségével visszainvertálhatót(k) a k körre - így megadva az eredeti metszéspont(ka)t.

Az inverzióról és a bizonyításról bővebben [1] és [10] könyvekben található leírás.

Megjegyzés: K. Yanagihara japán matematikus azt is bebizonyította, hogy körzővel végezhető bármely szerkesztés akkor is elvégezhető, ha körzővel nem lehet akármilyen nagy és akármilyen kicsiny sugarú kört rajzolni, hanem csak olyan ω sugarú köröket, amelyeknek sugarára az $r \leq \omega \leq R$ egyenlőtlenség áll fenn, ahol r és R előre megadott hosszúságú szakasz és $R > r$.

3. Szerkesztések csak vonalzó használatával

Az előző pontban láthattuk, hogy a vonalzó nélkülözhető az euklideszi szerkesztéseknél. Kérdés, hogy a körző nélkülözhető-e, vagyis a három alapszerkesztés mindegyike elvégezhető-e vonalzó kizárólagos használatával. A válasz nemleges, hiszen két egyenes metszéspontjának a koordinátáit lineáris kétismeretlenes egyenletből kapjuk, így ha a kiindulásul választott pontok Q -t

generálják, akkor vonalzóval nem juthatunk el például a $\sqrt{2}$ számhoz. A matematikusok azonban nem nyugodtak bele ebbe, s kimutatták, hogy gyengébb feltételekkel ugyan, de lehetséges euklideszi szerkesztés csak vonalzóval. Poncelet 1822-ben és tőle függetlenül Steiner 1833-ban a. következő tételt bizonyította:

Ha a síkon meg van adva egy kör a középpontjával, akkor mindazok a geometriai szerkesztések amelyek körzővel és vonalzóval elvégezhetők, egyedül vonalzóval is elvégezhetők.

Megjegyzés.

1. A fenti tétel bizonyítása igen nehéz, projektív geometriai előismereteket igényel.
2. A kör középpontja nélkülözhetetlen.
3. A tétel fokozása Weiss német matematikustól származik: ha meg van adva egy kör a középpontjával, akkor bármely körzővel és vonalzóval elvégezhető szerkesztést vonalzóval úgy is el lehet végezni, hogy csak olyan egyeneseket húzunk, amelynek a síknak négy meghatározott pontja közül valamelyiken átmennek.

FELHASZNÁLT IRODALOM

- [1] R Courant-H Robbins: Mi a matematika? Gondolat Könyvkiadó, Budapest, 1996
- [2] H.S.M. Coxeter: A geometriák alapjai (fordította Sztókay Kálmán), Műszaki Könyvkiadó, Budapest, 1973
- [3] Csákány Béla: Algebra, Tankönyvkiadó, Budapest, 1973.
- [4] Euklidesz: elemek (fordította Mayer Gyula), Gondolat Könyvkiadó, Budapest, 1983.
- [5] Fuchs László: algebra, Tankönyvkiadó, Budapest, 1989
- [6] Rozgonyi-Borus Ferenc: Ram-ba zárt világ, Mozaik Oktatási Kiadó, Szeged, 1996.
- [7] A. G. Kuros: Felsőbb algebra, Tankönyvkiadó, Budapest, 1968.
- [8] Szendrei Ágnes: A geometriai szerkeszthetőség algebrai elmélete, Polygon III. kötet 1. Szám, Szeged, 1993.
- [9] Dr Szendrei János: Algebra és számelmélet, Tankönyvkiadó, Budapest, 1989.
- [10] Szőkefalvi-Nagy Gyula: A geometriai szerkesztések elmélete, Akadémia Kiadó, Budapest, 1968.

**Köszönetet mondok Dr. Kurusa Árpádnak a szakdolgozatom
elkészítéséhez nyújtott támogatásáért!**

Tartalomjegyzék

Bevezető.....	2
I. Algebrai alapismeretek	4
1. Alapvető algebrai fogalmak.....	4
2. A komplex számok teste.....	6
3. A polinomok	8
4. A vektorterek.....	11
II. Algebrai testbővítések	13
III. Szerkesztések elmélete	17
IV. Nevezetes szerkesztési feladatok.....	23
1. A kör négyszögesítése	23
2. A kör kiegyenesítése.....	24
3. Kockakettőzés	24
4. Szögharmadolás	25
5. Háromszögszerkesztés.....	26
V. Szabályos sokszögek szerkesztése.....	29
VI. Szerkesztések euklideszitől különböző feltételekkel.....	34
1. Egységátrakó vonalzó.....	34
2. Szerkesztések csak körző használatával	35
3. Szerkesztések csak vonalzó használatával.....	35
Felhasznált irodalom.....	37
Köszönetnyilvánítás.....	38