

Magasabb fokú egyenletek és geometriai szerkeszthetőség

Waldhauser Tamás
2021 őszi félév

Bemelegítő feladat

Laci bácsi dolgozatokat javít. Ha nagyon felbosszantják a diákok által írt számárságok, tízfélé tép egy dolgozatot. Sőt, időnként még a kisebb darabokat is tízfélé tépi. Ha 64 dolgozattal kezdte, lehetséges-e, hogy előbb-utóbb 2020 fecni hever előtte?

Megoldás

Nem, mert a fecnik számának 9-es maradéka nem változik, és $64 \not\equiv 2020 \pmod{9}$.

Feladat

Egy szigeten 150 kaméleon él, amelyek közül jelenleg 40 kék, 50 zöld és 60 piros színű. Ha két különböző színű kaméleon találkozik, akkor megijednek, és mindkettő a harmadik színre változik át. Lehetséges-e a találkozások olyan sorozata, hogy azok után minden kaméleon azonos színű legyen?

Megoldás

Nem, mert a kaméleonok számának 3-as maradékai kezdetben mind különbözők $(1,2,0)$ és ez nem változik, ha viszont minden kaméleon ugyanolyan színűvé válna, akkor a 3-as maradékok mind egyformák lennének $(0,0,0)$.

Egy klasszikus feladat

El lehet-e jutni a tizenötös (tili-toli) játékban a bal oldali állásból a jobb oldaliba?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

→ →

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Megoldás

Nem, mert a lépések során az állást leíró permutáció paritása nem változik, és az egyik állás páratlan, a másik páros permutáció.

Helyesebben: a permutáció paritása minden lépésnél megváltozik, de ha az üres mező visszakérült a jobb alsó sarokba, akkor páros sok lépést tettünk, így a paritás megmarad.

Egy másik klasszikus feladat

Ha 7 gyerek fertőzött, és akinek 2 szomszédja fertőzött, az elkapja a betegséget, akkor lehetséges-e, hogy előbb-utóbb mindenki elkapja?



Két még klasszikusabb „feladat”

- ▶ Lehet-e gyökképlettel megoldani az ötöd- és magasabb fokú egyenleteket?
- ▶ Lehet-e euklideszi szerkesztéssel kört négyszögesíteni, kockát kettőzni, szöget harmadolni, . . . ?

Megoldás

Nem lehet. A bizonyítás *elvileg* olyan egyszerű, mint a korábbi feladatoknál:

0. Pontosan megfogalmazzuk, hogy mi a kezdeti és a végállapot, és hogy mik a megengedett lépések.
1. Keresünk egy invariánst, ami a lépések során nem változik, és
2. a kezdeti és a végállapotban nem ugyanaz.

Az invariánsok itt egy *kicsit* bonyolultabbak, mint a korábbi feladatoknál. . .

Az általános harmadfokú egyenlet

Az $x^3 + ax^2 + bx + c = 0$ harmadfokú egyenlet megoldóképlete:

$$x = -\frac{a}{3} + \sqrt[3]{\frac{-2a^3 + 9ab - 27c + \sqrt{(2a^3 - 9ab + 27c)^2 + 4(-a^2 + 3b)^3}}{54}} + \\ + \sqrt[3]{\frac{-2a^3 + 9ab - 27c - \sqrt{(2a^3 - 9ab + 27c)^2 + 4(-a^2 + 3b)^3}}{54}}$$

Az általános negyedfokú egyenlet

Az $x^4 + ax^3 + bx^2 + cx + d = 0$ negyedfokú egyenlet megoldóképlete:



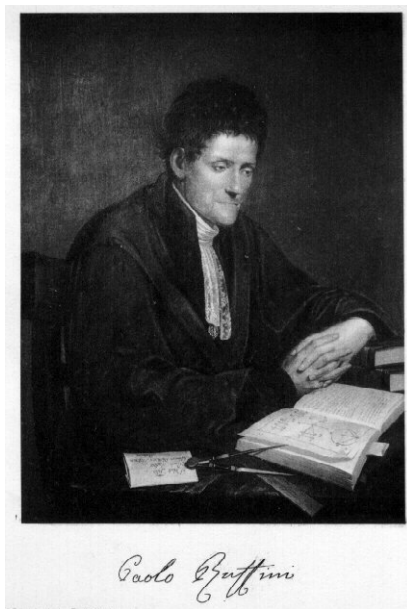
Az általános ötödfokú egyenlet

Az $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ ötödfokú egyenlet megoldóképlete egy olyan képlet *lenne*, ami az a, b, c, d, e betűkből és racionális számokból épül fel, a négy alapművelet és gyökvonások segítségével, és ha a, b, c, d, e helyébe tetszőleges számokat helyettesítünk, akkor megkapjuk az egyenlet egy (összes) megoldását.

Ruffini–Abel-tétel

Az általános ötödfokú egyenletnek nem létezik megoldóképlete (és így a magasabb fokúaknak sem).

Ettől még létezhetne bizonyos fajta egyenletekhez megoldóképlet, de Galois megmutatta, hogy van olyan ötödfokú egyenlet, amelyet még saját „különbejáratú” megoldóképlettel sem lehet megoldani.



Paolo Ruffini (1765–1822)

TEORIA GENERALE
DELLE
EQUAZIONI.

IN CUI SI DIMOSTRA IMPOSSIBILE

LA SOLUZIONE ALGEBRAICA DELLE
EQUAZIONI GENERALI DI GRADO
SUPERIORE AL QUARTO

D I

PAOLO RUFFINI.

P A R T E P R I M A .



BOLOGNA MDCCXCVIII.



NELLA STAMPERIA DI S. TOMMASO D' AQUINO.

(VI)

[illegible]

- 25.^a $f(x''')(x'')(x')(x')(x')$,
- 26.^a $f(x'')(x''')(x')(x')(x')$,
- 27.^a $f(x''')(x'')(x')(x')(x')$,
- 28.^a $f(x'')(x'')(x')(x')(x'')$,
- 29.^a $f(x''')(x'')(x'')(x')(x')$,
- 30.^a $f(x'')(x'')(x'')(x')(x'')$,
- 31.^a $f(x''')(x'')(x'')(x')(x'')$,
- 32.^a $f(x'')(x'')(x'')(x')(x'')$,
- 33.^a $f(x'')(x'')(x'')(x')(x'')$,
- 34.^a $f(x'')(x'')(x'')(x')(x'')$,
- 35.^a $f(x'')(x'')(x'')(x')(x'')$,
- 36.^a $f(x'')(x'')(x'')(x')(x'')$,
- 37.^a $f(x'')(x'')(x'')(x')(x'')$,
- 38.^a $f(x'')(x'')(x'')(x')(x'')$,
- 39.^a $f(x'')(x'')(x'')(x')(x'')$,
- 40.^a $f(x'')(x'')(x'')(x')(x'')$,
- 41.^a $f(x'')(x'')(x'')(x')(x'')$,
- 42.^a $f(x'')(x'')(x'')(x')(x'')$,
- 43.^a $f(x'')(x'')(x'')(x')(x'')$,
- 44.^a $f(x'')(x'')(x'')(x')(x'')$,
- 45.^a $f(x'')(x'')(x'')(x')(x'')$,
- 46.^a $f(x'')(x'')(x'')(x')(x'')$,
- 47.^a $f(x'')(x'')(x'')(x')(x'')$,
- 48.^a $f(x'')(x'')(x'')(x')(x'')$,

- 40.^o $f(x''')(x')(x')(x')(x')$,
- 50.^o $f(x'')(x')(x')(x')(x')$,
- 51.^o $f'(x')(x')(x')(x')(x'')$,
- 52.^o $f(x')(x')(x')(x')(x'')$,
- 53.^o $f(x')(x')(x')(x')(x''')$,
- 54.^o $f'(x')(x'')(x')(x')(x'')$,
- 55.^o $f(x')(x'')(x')(x')(x'')$,
- 56.^o $f(x')(x')(x')(x')(x''')$,
- 57.^o $f'(x')(x'')(x'')(x')(x'')$,
- 58.^o $f(x')(x')(x')(x')(x''')$,
- 59.^o $f(x')(x')(x')(x')(x''')$,
- 60.^o $f(x')(x'')(x'')(x')(x'')$,
- 61.^o $f(x')(x'')(x'')(x')(x'')$,
- 62.^o $f(x'')(x')(x'')(x')(x'')$,
- 63.^o $f(x')(x')(x'')(x')(x'')$,
- 64.^o $f(x')(x'')(x'')(x')(x'')$,
- 65.^o $f(x''')(x')(x')(x')(x'')$,
- 66.^o $f(x')(x')(x')(x')(x'')$,
- 67.^o $f(x')(x')(x')(x')(x'')$,
- 68.^o $f(x')(x'')(x'')(x')(x'')$,
- 69.^o $f(x')(x'')(x'')(x')(x'')$,
- 70.^o $f(x'')(x'')(x'')(x')(x'')$,
- 71.^o $f(x''')(x'')(x'')(x')(x'')$,
- 72.^o $f(x')(x')(x')(x')(x'')$,

$73.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}))$,
 $74.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x')))$,
 $75.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x'')))$,
 $76.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x''')))$,
 $77.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)})))$,
 $78.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x'))))$,
 $79.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x''))))$,
 $80.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x'''))))$,
 $81.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}))))$,
 $82.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x')))))$,
 $83.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x'')))))$,
 $84.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}))))$,
 $85.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x'))))))$,
 $86.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x''))))))$,
 $87.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}))))$,
 $88.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x'))))))$,
 $89.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x''))))))$,
 $90.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}))))$,
 $91.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x'))))))$,
 $92.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x''))))))$,
 $93.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}))))$,
 $94.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x'))))))$,
 $95.^{\circ}f(x^{(v)}(x')(x'')(x''')(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x^{(iv)}(x''))))))$,

$$\begin{aligned}
& 97.^{\circ}f(x')(x')(x')(x''')(x''), \\
& 98.^{\circ}f(x')(x')(x')(x'')(x''), \\
& 99.^{\circ}f(x')(x')(x'')(x'')(x''), \\
& 100.^{\circ}f(x')(x')(x'')(x')(x''), \\
& 101.^{\circ}f(x')(x')(x'')(x')(x''), \\
& 102.^{\circ}f(x')(x'')(x'')(x'')(x''), \\
& 103.^{\circ}f(x')(x'')(x'')(x')(x''), \\
& 104.^{\circ}f(x')(x'')(x'')(x'')(x''), \\
& 105.^{\circ}f(x')(x'')(x'')(x'')(x''), \\
& 106.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 107.^{\circ}f(x'')(x'')(x'')(x')(x''), \\
& 108.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 109.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 110.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 111.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 112.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 113.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 114.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 115.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 116.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 117.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 118.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 119.^{\circ}f(x'')(x'')(x'')(x'')(x''), \\
& 120.^{\circ}f(x'')(x'')(x'')(x'')(x'').
\end{aligned}$$



Niels Henrik Abel (1802–1829)

R 1016

A. 8

Journal

die

reine und angewandte Mathematik.

In zwanglosen Heften.

Herausgegeben

von

A. L. Crelle.



Erster Band.

In 4 Heften.

Mit 5 Kupfertafeln.

Berlin,

im Verlage von Duncker und Humblot.

1826



8.

Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen.

(Von Herrn N. H. Abel.)

Bekanntlich kann man algebraische Gleichungen bis zum vierten Grade allgemein auflösen, Gleichungen von höhern Graden aber nur in einzelnen Fällen, und irre ich nicht, so ist die Frage:

Ist es möglich, Gleichungen von höhern als dem vierten Grade allgemein aufzulösen?

noch nicht befriedigend beantwortet worden. Der gegenwärtige Aufsatz hat diese Frage zum Gegenstande.

Eine Gleichung algebraisch auflösen heist nichts anders, als ihre Wurzeln durch eine algebraische Function der Coefficienten ausdrücken. Man muß also erst die allgemeine Form algebraischer Functionen betrachten und alsdann untersuchen, ob es möglich sei, der gegebenen Gleichung auf die Weise genug zu thun, daß man den Ausdruck einer algebraischen Function statt der unbekannten Größe setzt.

§. I.

Ueber die allgemeine Form algebraischer Functionen.

Wenn $x', x'', x''' \dots$ eine endliche Menge beliebiger Größen sind, so sagt man: φ sei eine algebraische Function dieser Größen, wenn es sich durch $x', x'', x''' \dots$ etc. mittelst folgender Operationen ausdrücken läßt. Erstlich durch die Addition, zweitens durch die Multiplication, sowohl von Größen, die von $x', x'', x''' \dots$ abhängen, als von Größen, die nicht davon abhängen; drittens durch die Division; viertens durch Ausziehen von Wurzeln mit Exponenten, die Primzahlen sind. Wir nennen die Subtraction, Potenzirung und Ausziehung von Wurzeln mit zusammengesetzten Exponenten nicht besonders, weil sie offenbar in den vier vorhin genannten Operationen mit enthalten sind.

Läßt sich die Function φ durch die drei ersten der vier obigen Operationen zusammensetzen, so ist sie algebraisch rational oder bloß rational; und



Évariste Galois (1811–1832)

Je feras imprimer cette lettre dans le *revue Encyclopédique*.

Le ~~fait~~ Je me suis souvent ^{dans ma vie} hasardé à avancer des propositions dont je suis pas sûr. Mais tout ce que j'ai écrit là est depuis longtemps en l'air dans mon tête, et ~~je~~ il est trop de mon intérêt de ne pas me tromper pour que en me trouvant devant des thèses dont je n'aurais pas le courage de m'occuper.

Je ~~ne~~ prie publiquement Jacob Ode pour de donner leur avis non sur la vérité, mais sur l'importance de thèses.

Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à débattre tout ce gâchis.

Je t'embrasse avec affection. E. Guichard Le 27 Mai 1832.

A Galois-elmélet főtétele

Legyen $N | K$ Galois-bővítés és $G = \text{Gal}(N | K) = \text{Aut}_K N$.

Tekintsük az $I = \{(\alpha, \sigma) : \alpha\sigma = \alpha\} \subseteq N \times G$ „illeszkedési reláció” által indukált Galois-kapcsolatot:

$$\mathcal{P}(N) \rightarrow \mathcal{P}(G), \quad E \mapsto \{\sigma \in G \mid \forall \alpha \in E : \alpha\sigma = \alpha\} = E' = \text{Gal}(N | E);$$

$$\mathcal{P}(G) \rightarrow \mathcal{P}(N), \quad H \mapsto \{\alpha \in N \mid \forall \sigma \in H : \alpha\sigma = \alpha\} = H' = \text{Fix}(H).$$

$$(1) \quad \forall E \subseteq N : E'' = E \iff K \leq E \leq N \quad (\text{azaz } E \in \text{Sub}_K N).$$

$$(2) \quad \forall H \subseteq G : H'' = H \iff H \leq G \quad (\text{azaz } H \in \text{Sub } G).$$

(3) A $\text{Sub}_K N$ és $\text{Sub } G$ hálók között duális izomorfizmust létesítenek az

$$E \mapsto E' = \text{Gal}(N | E) \quad \text{és} \quad H \mapsto H' = \text{Fix}(H)$$

leképezések (amelyek egymás inverzei).

(4) Legyen $E \in \text{Sub}_K N$ és $H \in \text{Sub } G$ egymásnak megfelelő résztest és részcsoport:

$$E = H' = \text{Fix}(H) \quad \text{és} \quad H = E' = \text{Gal}(N | E).$$

$$a) \quad [N : E] = |H| \quad \text{és} \quad [E : K] = [G : H].$$

b) $E | K$ normális $\iff H \triangleleft G$, és ha ez teljesül, akkor $\text{Gal}(E | K) \cong G/H$, azaz

$$\text{Gal}(E | K) \cong \text{Gal}(N | K) / \text{Gal}(N | E).$$

Definíció

Az α komplex számot **gyökmennyiségnek** nevezzük, ha megkapható racionális számokból kiindulva a négy alpművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával.

Általánosabban, ha K egy számtest, akkor **K feletti gyökmennyiségen** olyan komplex számot értünk, amely megkapható K elemeiből kiindulva a négy alpművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával.

Példa

$$\frac{\sqrt[3]{3 - \sqrt{\sqrt[4]{2} + \sqrt[5]{\frac{3}{17}}}} + \sqrt[17]{323 - \sqrt{2014}}}{\sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}}$$

Példa

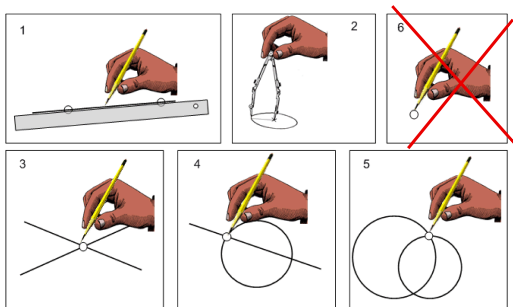
Legyen $\alpha \approx 1,243$ az $x^5 - 4x + 2 = 0$ egyenlet (legnagyobb valós) megoldása.

Gyökmennyiség-e ez a szám, azaz meg lehet-e kapni α -t racionális számokból kiindulva a négy alpművelet és gyökvonások véges számú alkalmazásával?

A Galois-elméletből következik, hogy nem, vagyis az $x^5 - 4x + 2 = 0$ egyenletnek még „ad hoc” megoldóképlete sincs.

Szerkesztési feladat

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



Szerkesztési lépések

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

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

A szerkesztés menete

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

Megjegyzések

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

Algebraizálás

Vegyünk fel egy derékszögű koordinátarendszert, amelynek origója P_1 , és az első tengelyen az egységnek a P_2 pont felel meg. Ezután pontok helyett számokat szerkesztünk: minden valós szám megfelel az első tengely (mint valós számegetes) egy pontjának.

HF: Bizonyítsuk be, hogy egy $Q = (x, y)$ pont akkor és csak akkor szerkeszthető meg, ha az x, y számok (illetve a nekik megfelelő pontok az első tengelyen) megszerkeszthetők.

Szerkesztési feladat

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

Szerkesztési lépések

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

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

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

A szerkesztés menete

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

Megjegyzés

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

A szerkesztés alapteste

A kiindulásul megadott $c_1, \dots, c_n$ számok által generált $K \leq \mathbb{R}$ számtestet a szerkesztés *alaptestének* nevezzük. A K test elemei tehát azok a számok, amelyek megkaphatóak a $c_1, \dots, c_n$ számokból kiindulva a négy alpművelet véges sokszori alkalmazásával.

HF: Mutassuk meg, hogy ha $0, 1, a, b$ adottak, akkor $a \pm b, a \cdot b, a/b$ ($b \neq 0$) megszerkeszthető.

Következmény

A K test elemei szerkeszthetők, ezért AÁMNTFH kiindulási adatunk ez a test.

Tétel

Az alaptest nem függ a koordinátarendszer választásától.

Definíció

Az α valós számot **négyzetgyökmennyiségnek** nevezzük, ha megkapható racionális számokból kiindulva a négy alpművelet (összeadás, kivonás, szorzás, osztás) és négyzetgyökvonás véges számú alkalmazásával. (Csak valós számokkal dolgozunk, ezért csak nemnegatív számból szabad négyzetgyököt vonni.)

Általánosabban, ha $K \leq \mathbb{R}$ egy számtest, akkor **K feletti négyzetgyökmennyiség** olyan valós számot értünk, amely megkapható K elemeiből kiindulva a négy alpművelet (összeadás, kivonás, szorzás, osztás) és négyzetgyökvonás véges számú alkalmazásával.

Példa

$$\cos \frac{2\pi}{17} = \frac{1}{16} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \right)$$

Tétel

Az α valós szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α négyzetgyökmennyiség K felett.

Bizonyítás

α szerkeszthető $\overset{?}{\iff} \alpha$ négyzetgyökmennyiség K felett

$\Leftarrow$:

Elég belátni, hogy ha a, b megszerkeszthető, akkor $a \pm b, a \cdot b, a/b$ ($b \neq 0$) és $\sqrt{a}$ ($a \geq 0$) is megszerkeszthető. **HF: Mutassuk meg, hogy ha $a > 0$ megszerkeszthető, akkor $\sqrt{a}$ ($a \geq 0$) is megszerkeszthető.**

$\Rightarrow$:

Tfh. α megszerkeszthető ℓ lépésben: $K \rightsquigarrow \alpha_1 \rightsquigarrow \dots \rightsquigarrow \alpha_\ell = \alpha$.

A lépések száma szerinti indukcióval bizonyítjuk, hogy α négyzetgyökmennyiség K felett.

Kezdőlépés: $\ell = 0$ esetén $\alpha \in K$. ✓

Indukciós lépés: tfh. $\alpha_1, \dots, \alpha_{\ell-1}$ négyzetgyökmennyiségek K felett. (IH)

Ekkor α megkapható két kögyenes metszéspontjának egyik koordinátájaként, ahol mindkét kögyenest $K \cup \{\alpha_1, \dots, \alpha_{\ell-1}\}$ -beli koordinátákkal rendelkező pontok határozzák meg.

Pl. legyen α az A kp.-ú B -n átmenő és a C kp.-ú, D -n átmenő kör metszéspontjának első koordinátája, ahol $A = (a_1, a_2)$, $B = (b_1, b_2)$, $C = (c_1, c_2)$, $D = (d_1, d_2)$ és $a_1, \dots, d_2 \in K \cup \{\alpha_1, \dots, \alpha_{\ell-1}\}$. (A másik öt eset hasonló, de könnyebb.)

Bizonyítás (folyt.)

A két kör egyenlete:

$$(x - a_1)^2 + (y - a_2)^2 = (b_1 - a_1)^2 + (b_2 - a_2)^2 =: r^2$$

$$(x - c_1)^2 + (y - c_2)^2 = (d_1 - c_1)^2 + (d_2 - c_2)^2 =: s^2.$$

Vonjuk ki a két egyenletet egymásból:

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

Fejezzük ki ebből y -t: $y = px + q$ (itt p és q négyzetgyökmennyiségek K felett), majd helyettesítsük ezt be valamelyik kör egyenletébe.

Így egy másodfokú egyenletet kapunk:

$$ux^2 + vx + w = 0 \quad (u, v, w \text{ négyzetgyökmennyiségek } K \text{ felett}).$$

A másodfokú egyenlet megoldóképletét alkalmazva kapjuk, hogy α négyzetgyökmennyiség K felett.





Csak akkor olvass tovább, ha már tanultál a végesfokú testbővítésekről!

Definíció

Az $L|K$ testbővítés **egyszerű négyzetgyökbővítés**, ha $\exists a \in K: L = K(\sqrt{a})$.

Az $L|K$ testbővítés **négyzetgyökbővítés**, ha megkapható véges sok egyszerű négyzetgyökbővítés egymásutánjaként:

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

Állítás

$L|K$ egyszerű négyzetgyökbővítés $\iff [L : K] \leq 2$.

Bizonyítás.

$\implies$: Ha $L = K(\sqrt{a})$, ahol $a \in K$, akkor $[L : K] = \deg m_{\alpha, K} \in \{1, 2\}$, aszerint, hogy $\sqrt{a} \in K$ vagy sem.

$\impliedby$: Fordítva, ha $[L : K] = 1$, akkor $L = K = K(\sqrt{0})$.

Ha pedig $[L : K] = 2$, akkor bármely $\alpha \in L \setminus K$ esetén $L = K(\alpha)$ (miért?), és persze $\deg m_{\alpha, K} = 2$. Legyen $m_{\alpha, K} = x^2 + bx + c$; ekkor $L = K(\alpha) = K(\sqrt{b^2 - 4c})$ (miért?).



Következmény

Négyzetgyökbővítés foka kettőhatvány.

Tétel

Az α valós szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α benne van K valamely négyzetgyökbővítésében:

$$\alpha \text{ szerkeszthető} \iff \exists L: L|K \text{ négyzetgyökbővítés és } \alpha \in L.$$

Bizonyítás.

$\Rightarrow$: Tfh. α megszerkeszthető. Tudjuk, hogy ekkor α négyzetgyökmennyiség K felett. Az α négyzetgyökmennyiségként való felírásában szereplő gyökjelek száma szerinti indukcióval bizonyítható, hogy létezik K -nak olyan négyzetgyökbővítése, ami tartalmazza α -t. Ehhez csak megfelelő sorrendben kell adjungálnunk az α -ban fellépő négyzetgyököket. Például, ha $K = \mathbb{Q}$ és

$$\alpha = \frac{1}{16} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \right),$$

akkor így épül fel egy alkalmas négyzetgyökbővítés:

$$\begin{aligned} \mathbb{Q} &\leq \mathbb{Q}(\sqrt{17}) \leq \mathbb{Q}(\sqrt{17})(\sqrt{34 - 2\sqrt{17}}) \leq \mathbb{Q}(\sqrt{17})(\sqrt{34 - 2\sqrt{17}})(\sqrt{34 + 2\sqrt{17}}) \\ &\leq \mathbb{Q}(\sqrt{17})(\sqrt{34 - 2\sqrt{17}})(\sqrt{34 + 2\sqrt{17}})\left(\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}\right) \end{aligned}$$

Tétel

Az α valós szám akkor és csak akkor szerkeszthető meg a K alaptestből kiindulva, ha α benne van K valamely négyzetgyökbővítésében:

$$\alpha \text{ szerkeszthető} \iff \exists L: L|K \text{ négyzetgyökbővítés és } \alpha \in L.$$

Bizonyítás (folyt.).

$\Leftarrow$: Tfh. létezik olyan L négyzetgyökbővítése K -nak, ami tartalmazza α -t:

$$K = T_0 \leq T_1 \leq \dots \leq T_\ell = L \ni \alpha \quad (T_{i+1} = T_i(\sqrt{a_i}), \text{ ahol } a_i \in T_i).$$

Megmutatjuk i szerinti indukcióval, hogy T_i elemei mind négyzetgyökmennyiségek K felett, tehát megszerkeszthetők (és így $i = \ell$ esetén $\alpha \in T_\ell$ is az).

Kezdőlépés: $T_0 = K$ elemei nyilván négyzetgyökmennyiségek K felett.

Indukciós lépés: tfh. T_i elemei mind négyzetgyökmennyiségek K felett (és $i < \ell$).

Mivel $T_{i+1} = [T_i \cup \{\sqrt{a_i}\}]_t$, és az indukciós feltevés szerint a **piros** halmaz elemei négyzetgyökmennyiségek K felett, így T_{i+1} elemei is négyzetgyökmennyiségek K felett. □

Következmény

Ha az α valós szám megszerkeszthető a K alaptestből kiindulva, akkor α algebrai K felett, és minimálpolinomjának foka kettőhatvány.

Bizonyítás.

Ha α megszerkeszthető, akkor benne van egy $L \mid K$ négyzetgyökbővítésben. Tudjuk, hogy $[L : K]$ kettőhatvány, és azt is tudjuk, hogy $\deg m_{\alpha, K} \mid [L : K]$. □

Megjegyzés

A tétel megfordítása nem igaz, pl. az $x^4 + 7x + 7$ polinom gyökei nem szerkeszthetők meg a $K = \mathbb{Q}$ alaptestből.

Tétel (kockakettőzés)

Nem lehet adott kockához kétszer akkora térfogatú kockát szerkeszteni.

Bizonyítás.

Legyen a kocka oldalhosszúsága 1. Ekkor $K = \mathbb{Q}$, és a megszerkesztendő szám $\alpha = \sqrt[3]{2}$. Mivel $m_{\alpha, K} = x^3 - 2$ foka nem kettőhatvány. □

Tétel (körnégyszögesítés)

Nem lehet adott körhöz vele azonos területű négyzetet szerkeszteni.

Bizonyítás.

Legyen a kör sugara 1. Ekkor $K = \mathbb{Q}$, és a megszerkesztendő szám $\alpha = \sqrt{\pi}$.
Mivel $\sqrt{\pi}$ még csak nem is algebrai K fölött.



Tétel (szögharmadolás)

Nem lehet adott szöghöz harmadakkora szöget szerkeszteni.

Bizonyítás.

Legyen a szög 60° . Ekkor $K = \mathbb{Q}$, és a megszerkesztendő szám $\alpha = \cos(20^\circ)$.
A minimálpolinom meghatározásához fejezzük ki $\cos 3x$ -et $\cos x$ segítségével:

$$\cos 3x = \cos^3 x - 3 \cos x \cdot \sin^2 x = 4 \cos^3 x - 3 \cos x.$$

Az $x = 20^\circ$ értékre azt kapjuk, hogy $\cos 60^\circ = 4 \cos^3 20^\circ - 3 \cos 20^\circ$, azaz $\frac{1}{2} = 4\alpha^3 - 3\alpha$. Tehát α gyöke a $8x^3 - 6x - 1$ polinomnak, és ez a polinom irreducibilis $\mathbb{Q}$ felett (ugye?). Ebből következik, hogy $m_{\alpha, K} = x^3 - \frac{3}{4}x - \frac{1}{8}$, és így α nem szerkeszthető.



Tétel (Gauss 1801, Wantzel 1837)

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

Bizonyítás.

Szükségesség: $\cos \frac{2\pi}{n}$ minimálpolinomjának foka $\varphi(n)$. □

Fermat-prímelek

Fermat-prímeleknek a $2^k + 1$ alakú prímszámokat nevezzük. Nem nehéz belátni, hogy ha $2^k + 1$ prím, akkor k kettőhatvány. Fermat azt sejtette, hogy $F_n = 2^{2^n} + 1$ mindig prím, de ez nem igaz: Euler észrevette, hogy $F_5 = 641 \cdot 6700417$. Minden további Fermat-szám, amit megvizsgáltak szintén összetettnek bizonyult. Tehát csak öt Fermat-prímet ismerünk:

► $F_0 = 2^1 + 1 = 3$ (szerk.: ókori görögök)

► $F_1 = 2^2 + 1 = 5$ (szerk.: ókori görögök)

► $F_2 = 2^4 + 1 = 17$ (szerk.: Gauss 1796, Erchinger ~1800)

$$\cos \frac{2\pi}{17} = \frac{1}{16} \left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}} \right)$$

► $F_3 = 2^8 + 1 = 257$ (szerk.: Richelot 1832)

► $F_4 = 2^{16} + 1 = 65537$ (szerk.: Hermes 1894; 10 év, 200 oldal)

Ikerfeladatok

1. Adott az egyenlő szárú háromszög beírt körének sugara és

(a) az alapja, vagy

(b) a szára.

Megszerkeszthető-e a háromszög?

2. Adott a derékszögű háromszög derékszögű csúcsból induló magassága és

(a) a derékszögű csúcsból induló szögfelezője, vagy

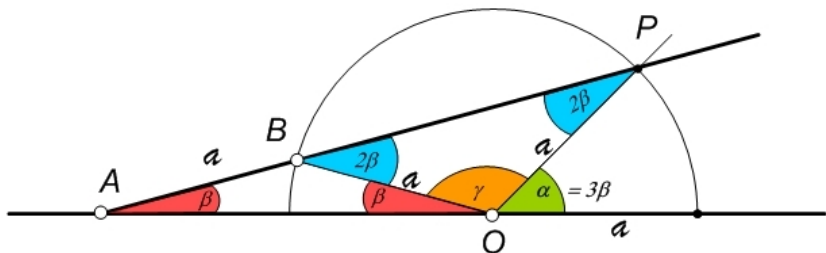
(b) egy másik csúcsból induló szögfelezője.

Megszerkeszthető-e a háromszög?

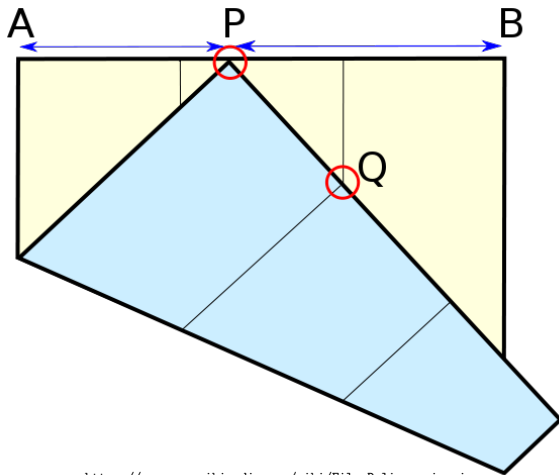
Nemeuklideszi szerkesztések

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

Szögharmadolás betolóvonalzóval



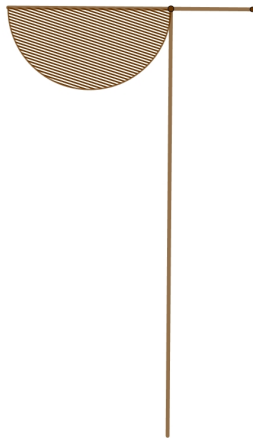
Kockakettőzés papírhajtogatással



https://commons.wikimedia.org/wiki/File:Delian_origami.svg

$$\frac{PB}{PA} = \sqrt[3]{2}$$

Szögharmadolás tomahawkkal



https://commons.wikimedia.org/wiki/File:Tomahawk-BHM_Ethno_1894.410.37-P8260256-white.jpg

Definíció

Az $L|K$ testbővítés **egyszerű radikálbővítés**, ha $\exists a \in K \exists n \in \mathbb{N}: L = K(\sqrt[n]{a})$.

Az $L|K$ testbővítés **radikálbővítés**, ha ha megkapható véges sok egyszerű radikálbővítés egymásutánjaként:

$$K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L \quad (T_{i+1} = T_i(\sqrt[n_i]{a_i}), \text{ ahol } a_i \in T_i, n_i \in \mathbb{N}).$$

Tétel

Az α komplex szám akkor és csak akkor gyökmennyiség K felett, ha α benne van K valamely radikálbővítésében:

$$\exists L: L|K \text{ radikálbővítés és } \alpha \in L.$$

Tétel

Algebrai számok összege, különbsége, szorzata, hányadosa is algebrai szám, vagyis az algebrai számok testet alkotnak.

Bizonyítás.

Tfh. α, β algebrai számok, és tekintsük az alábbi kétlépcsős testbővítést:

$$\mathbb{Q} =: K \leq K(\alpha) \leq K(\alpha)(\beta) =: L.$$

Ekkor $L \mid K$ végesfokú bővítés:

$$\begin{aligned} [L : K] &= [K(\alpha) : K] \cdot [K(\alpha)(\beta) : K(\alpha)] \\ &= \deg m_{\alpha, K} \cdot \deg m_{\beta, K(\alpha)} \\ &\leq \deg m_{\alpha, K} \cdot \deg m_{\beta, K} < \infty. \end{aligned}$$

Tudjuk, hogy végesfokú bővítés minden eleme algebrai, így $\alpha + \beta, \alpha - \beta, \alpha \cdot \beta, \alpha / \beta$ (ha $\beta \neq 0$) $\in K(\alpha)(\beta)$ mind algebraiak K felett.



Tétel

Algebrai szám gyöke is algebrai szám.

Bizonyítás.

Ha α gyöke a nemzéró $f(x) \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke az $f(x^n)$ polinomnak. □

Következmény

Minden gyökmennyiség algebrai szám.

Bizonyítás.

A gyökmennyiségek racionális számokból (amik nyilván algebraiak) épülnek fel a négy alapművelet és gyökvonások véges számú alkalmazásával, és láttuk, hogy az algebrai számok halmaza zárt ezekre a műveletekre. □

Megjegyzés

A fenti állítás megfordítása nem igaz: van olyan algebrai szám, ami nem gyökmennyiség (pl. az $x^5 - 4x + 2$ polinom gyökei).

