Magasabb fokú egyenletek és geometriai szerkeszthetőség

Waldhauser Tamás
2020 őszi félév

Bemelegítő feladat

Laci bácsi dolgozatokat javít. Ha nagyon felbosszantják a diákok által írt szamárságok, tízfelé tép egy dolgozatot. Sőt, időnként még a kisebb darabokat is tízfelé 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	

$\longrightarrow \quad \cdots\cdots\cdots \quad \longrightarrow$

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.

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:

$$x = -\frac{a}{4} \pm \frac{1}{2}\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{\sqrt[3]{2}(b^2 - 3ac + 12d)}{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}} + \frac{\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}}{54}} \pm \frac{1}{2}\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{\sqrt[3]{2}(b^2 - 3ac + 12d)}{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}} - \sqrt[3]{\frac{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}{54}} \pm \frac{\sqrt[3]{b^2 - 3ac + 12d}}{6\sqrt{\frac{a^2}{4} - \frac{4b}{3} + \frac{\sqrt[3]{2}(b^2 - 3ac + 12d)}{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}} + \sqrt[3]{\frac{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}{54}}} - \frac{-a^3 + 4ab - 8c}{4\sqrt{\frac{a^2}{4} - \frac{4b}{3} + \frac{\sqrt[3]{2}(b^2 - 3ac + 12d)}{3\sqrt[3]{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}} + \sqrt[3]{\frac{2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + \sqrt{-4(b^2 - 3ac + 12d)^3 + (2b^3 - 9abc + 27c^2 + 27a^2d - 72bd)^2}}{54}}}}$$

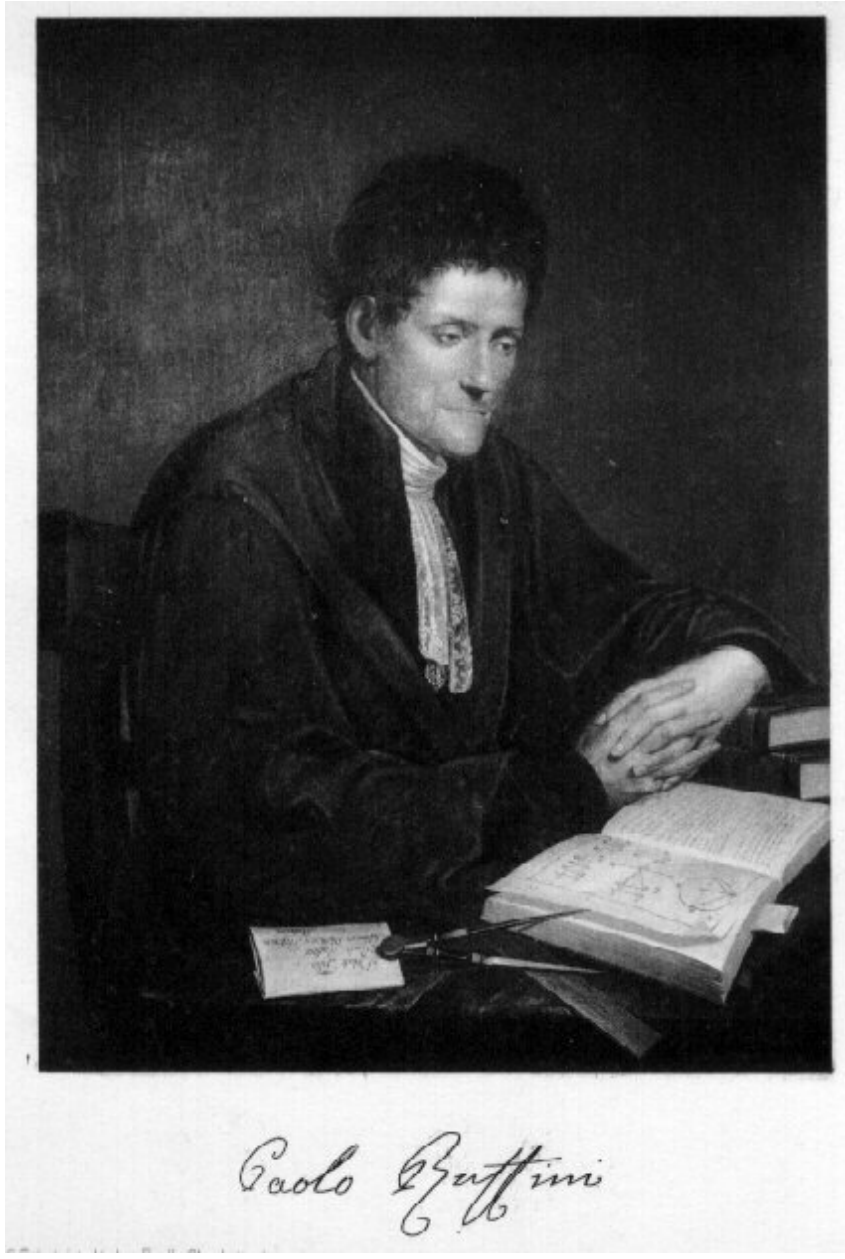
Az általános ötödfokú egyenlet

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, 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

DI

PAOLO RUFFINI.

PARTE PRIMA.

BOLOGNA MDCCXCVIIII.

NELLA STAMPERIA DI S. TOMMASO D' AQUINO.

Pag. 290.

$f(x')(x'')(x''')(x'^{v})(x^{v}),$
$f(x'')(x')(x''')(x'^{v})(x^{v}),$
$f(x'')(x''')(x')(x'^{v})(x^{v}),$
$f(x''')(x')(x'')(x'^{v})(x^{v}),$
$f(x')(x''')(x'')(x'^{v})(x^{v}),$
$f(x''')(x'')(x')(x'^{v})(x^{v}),$
$f(x'')(x''')(x'^{v})(x')(x^{v}),$
$f(x''')(x'^{v})(x')(x'')(x^{v}),$
$f(x'^{v})(x')(x'')(x''')(x^{v}),$
$f(x')(x''')(x'^{v})(x'')(x^{v}),$
$f(x''')(x'^{v})(x'')(x')(x^{v}),$
$f(x'^{v})(x'')(x')(x''')(x^{v}),$
$f(x''')(x')(x'^{v})(x'')(x^{v}),$
$f(x')(x'^{v})(x'')(x''')(x^{v}),$
$f(x'^{v})(x'')(x''')(x')(x^{v}),$
$f(x')(x'')(x'^{v})(x''')(x^{v}),$
$f(x'')(x'^{v})(x''')(x')(x^{v}),$
$f(x'^{v})(x''')(x')(x'')(x^{v}),$
$f(x''')(x'')(x'^{v})(x')(x^{v}),$
$f(x'')(x'^{v})(x')(x''')(x^{v}),$
$f(x'^{v})(x')(x''')(x'')(x^{v}),$
$f(x'')(x')(x'^{v})(x''')(x^{v}),$
$f(x')(x'^{v})(x''')(x'')(x^{v}),$
$f(x'^{v})(x''')(x'')(x')(x^{v}),$

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

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

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

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

Niels Henrik Abel (1802–1829)

Journal

für 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 heifst nichts anders, als ihre Wurzeln durch eine algebraische Function der Coefficienten ausdrücken. Man mufs also erst die allgemeine Form algebraischer Functionen betrachten und alsdann untersuchen, ob es möglich sei, der gegebenen Gleichung auf die Weise genug zu thun, dafs man den Ausdruck einer algebraischen Function statt der unbekannten Gröfse setzt.

§. I.

Ueber die allgemeine Form algebraischer Functionen.

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

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

Évariste Galois (1811–1832)

Je ferai imprimer cette lettre dans la revue Encyclopédique.

Dans ma vie
Il est Je me suis souvent hasardé à avancer des propositions dont je n'étais pas sûr. Mais tout ce que j'ai écrit là est depuis bientôt cinq ans dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour que je me sois exposé de gaieté de cœur à démontrer un théorème dont je n'aurais pas une démonstration complète.

Je prierai publiquement Jacobi de donner leur avis sur la vérité, mais sur l'importance du théorème.

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

Je t'embrasse avec effusion. E Galois Le 29 Mai 1832.

A Galois-elmélet főtétele

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

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

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

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

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

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

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

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

leképezések (amelyek egymás inverzei).

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

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

a) $[N : E] = |H|$ és $[E : K] = [G : H]$.

b) $E \mid K$ normális $\iff H \lhd G$, és ha ez teljesül, akkor $\mathrm{Gal}(E \mid K) \cong G/H$, azaz

$$\mathrm{Gal}(E \mid K) \cong \mathrm{Gal}(N \mid K) \,/\, \mathrm{Gal}(N \mid E).$$

Definíció

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

Példa

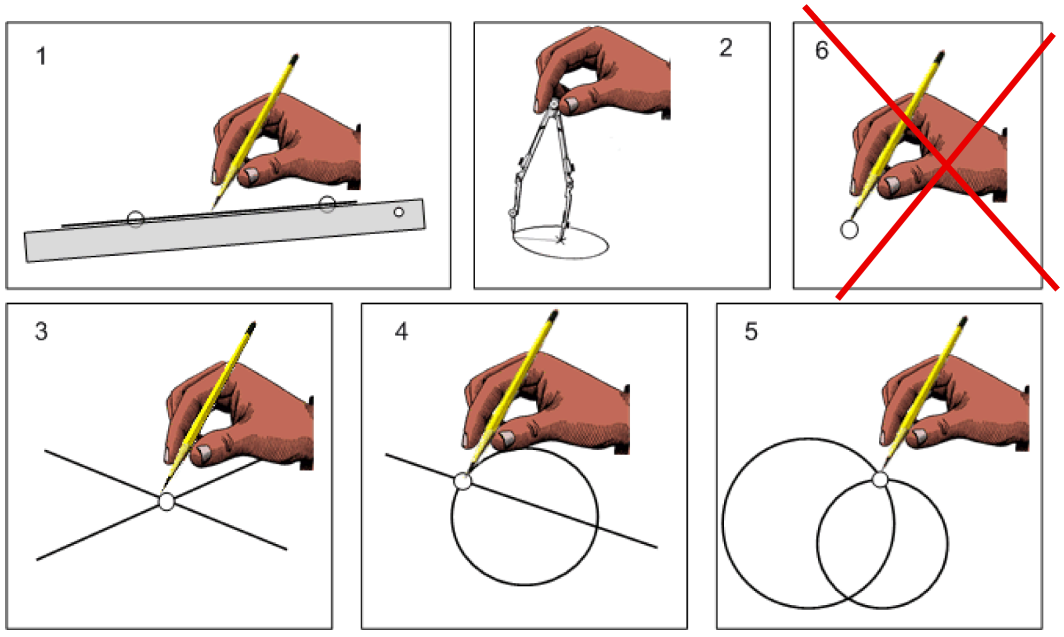
$$\frac{\sqrt[3]{3-\sqrt{\sqrt[4]{2}+\sqrt[5]{\frac{3}{17}}}}+\sqrt[17]{323-\sqrt{2014}}}{\sqrt{2}+\sqrt[3]{3}+\sqrt[5]{5}}$$

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



Szerkesztési lépések

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

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

A szerkesztés menete

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

Megjegyzések

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

Algebraizálás

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

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

Szerkesztési feladat

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

Szerkesztési lépések

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

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

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

A szerkesztés menete

$$\{c_1, c_2, \ldots, c_n\} \rightsquigarrow \{c_1, c_2, \ldots, c_n, \alpha_1\} \rightsquigarrow$$
$$\rightsquigarrow \{c_1, c_2, \ldots, c_n, \alpha_1, \alpha_2\} \rightsquigarrow \cdots$$
$$\rightsquigarrow \{c_1, c_2, \ldots, c_n, \alpha_1, \alpha_2, \ldots, \alpha_\ell\} \quad \alpha_\ell = \alpha.$$

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 $c_1, \ldots, c_n$ számok által generált $K \leq \mathbb{R}$ számtestet a szerkesztés *alaptestének* nevezzük. A K test elemei tehát azok a számok, amelyek megkaphatóak a $c_1, \ldots, c_n$ számokból kiindulva a négy alapművelet 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 szerkeszthetőek, 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 alapművelet (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 négyzetgyökmennyiségen** olyan valós számot értünk, amely megkapható K elemeiből kiindulva a négy alapművelet (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

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

$\Longleftarrow$:

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.

$\Longrightarrow$:

Tfh. α megszerkeszthető ℓ lépésben: $K \rightsquigarrow \alpha_1 \rightsquigarrow \cdots \rightsquigarrow \alpha_\ell = \alpha$.
A lépések száma szerinti indukcióval bizonyítjuk, hogy α négyzetgyökmennyiség K felett.

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

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

Ekkor α megkapható két kögyenes metszéspontjának egyik koordinátájaként, ahol mindkét kögyenest $K \cup \{\alpha_1, \ldots, \alpha_{\ell-1}\}$-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 $a_1, \ldots, d_2 \in K \cup \{\alpha_1, \ldots, \alpha_{\ell-1}\}$. (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:

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

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

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:

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

Állítás

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

Bizonyítás.

$\Longrightarrow$: 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.

$\Longleftarrow$: 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:

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

Bizonyítás.

$\Longrightarrow$: 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

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

akkor így épül fel egy alkalmas négyzetgyökbővítés:

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

Tétel

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

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

Bizonyítás (folyt.).

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

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

Megmutatjuk i szerinti indukcióval, hogy T_i elemei mind négyzetgyökmennyiségek K felett, tehát megszerkeszthetőek (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 szerkeszthetőek 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 $\alpha = \sqrt[3]{2}$. Node $m_{\alpha,K} = x^3 - 2$ 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 $\alpha = \sqrt{\pi}$. Node $\sqrt{\pi}$ 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.

□

Ikerfeladatok

1. Adott az egyenlő szárú háromszög beírt körének sugara és
   (a) az alapja, vagy
   (b) a szára.

   Megszerkeszthető-e a háromszög?

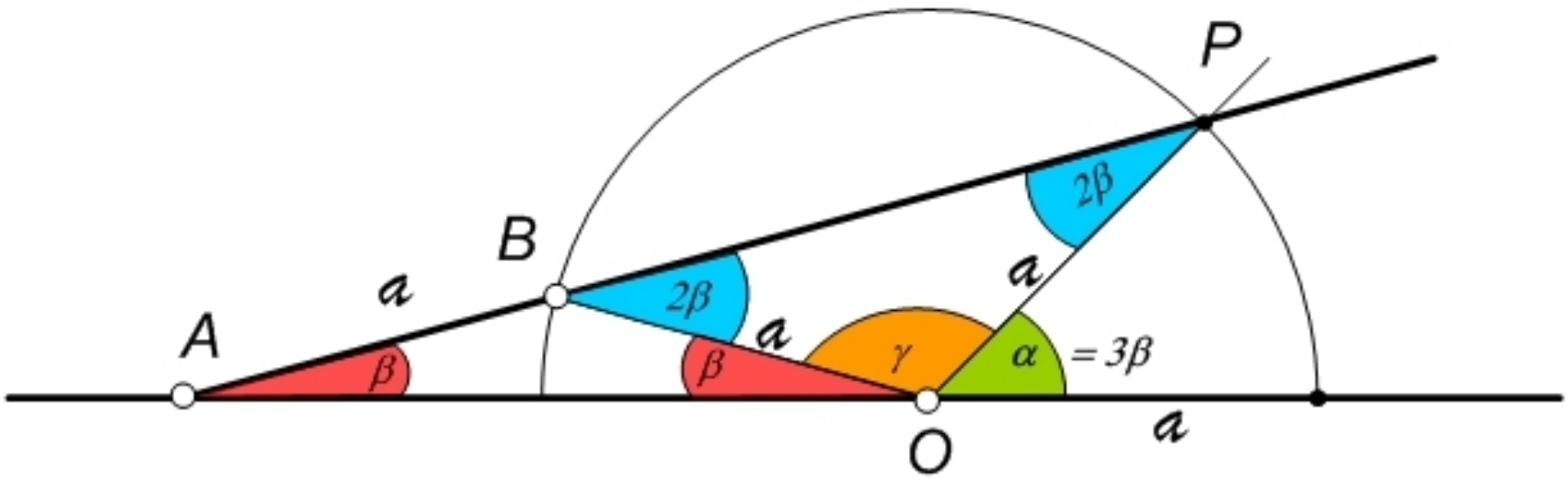
2. Adott a derékszögű háromszög derékszögű csúcsból induló magassága és
   (a) a derékszögű csúcsból induló szögfelezője, vagy
   (b) egy másik csúcsból induló szögfelezője.

   Megszerkeszthető-e a háromszög?

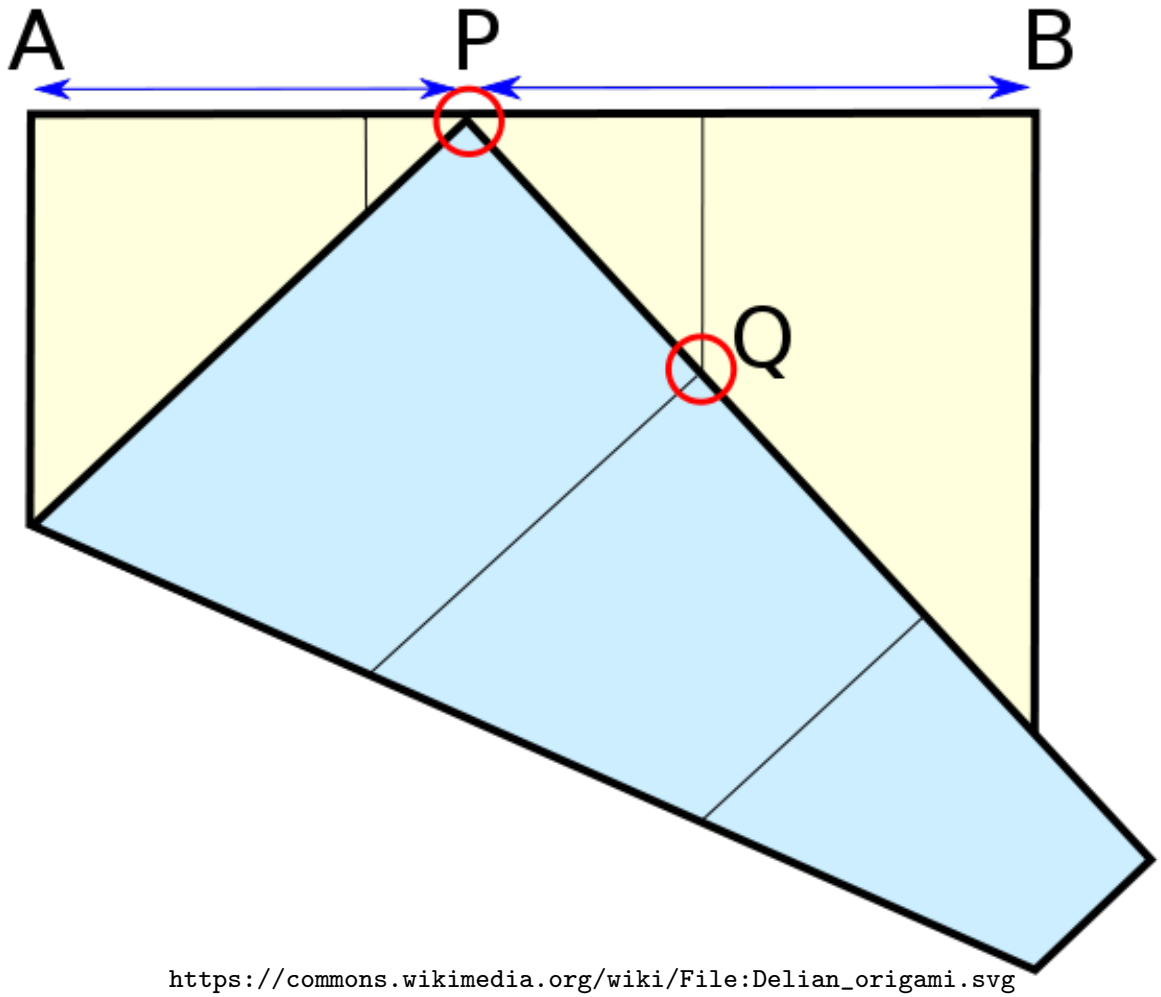
Nemeuklideszi szerkesztések

- 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 (fok$=2^k3^\ell$)
  betolóvonalzó, papírhajtogatás

Szögharmadolás betolóvonalzóval



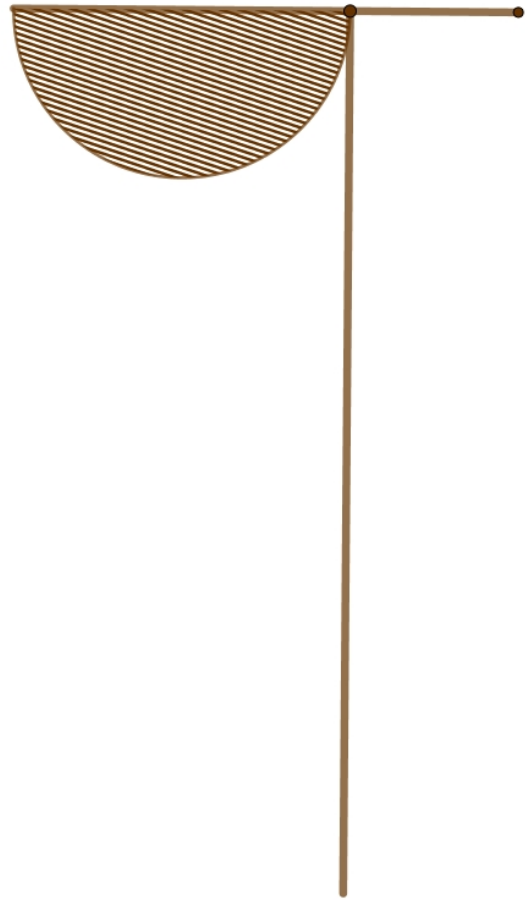
Kockakettőzés papírhajtogatással



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:

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

Tétel

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

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

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

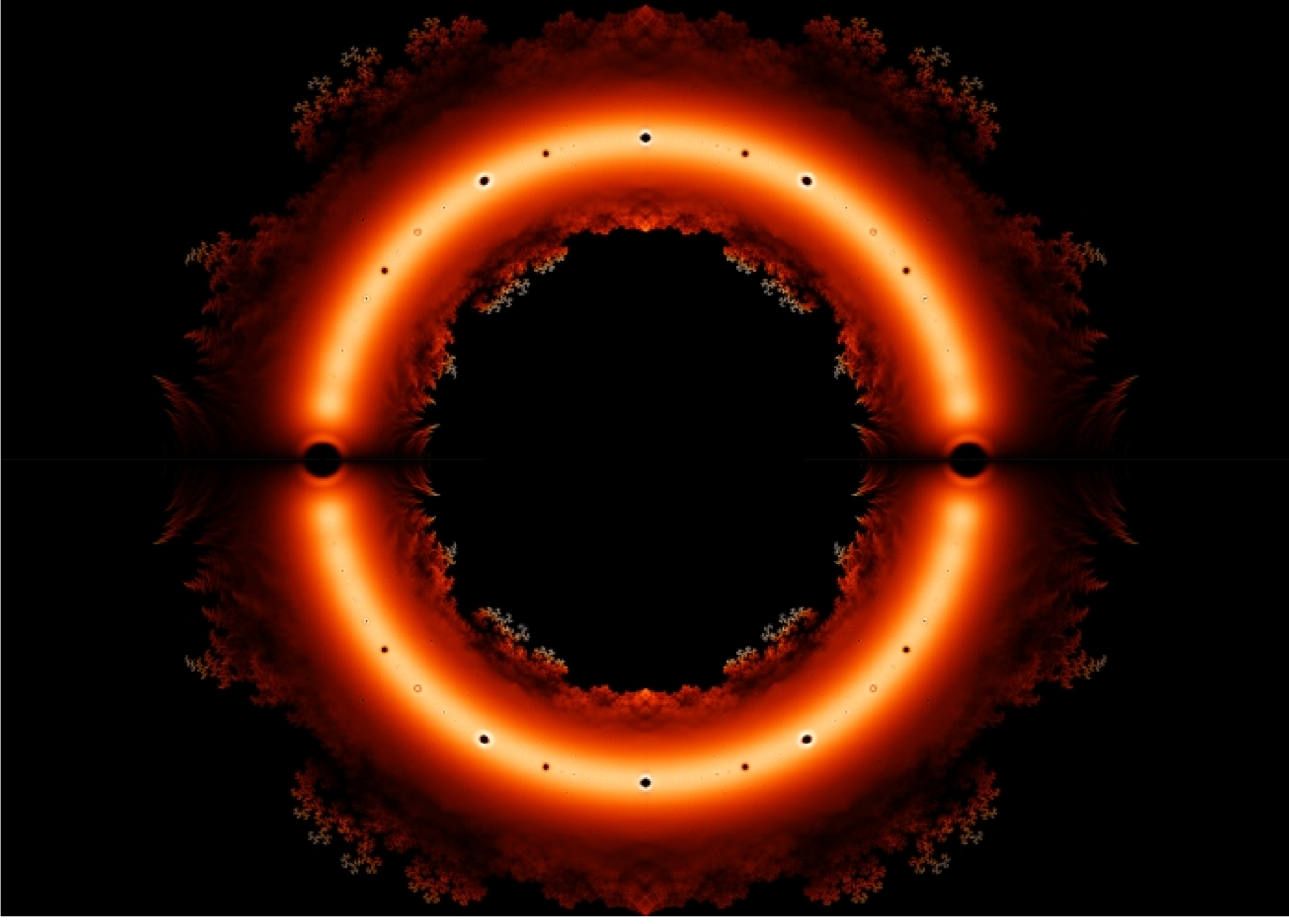
Minden gyökmennyiség algebrai szám.

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).



https://math.ucr.edu/home/baez/roots/