(2. befejező közlemény)

Néhány algebrai fogalom

9. Az előzőkben beláttuk, hogy bizonyos számadatokból azok és csak azok az adatok szerkeszthetők, amelyeket négy alapművelet és négyzetgyökvonás ismételt, véges számú alkalmazásával számíthatunk ki az adott számokból. Ennek a kritériumnak az alkalmazása egy konkrét problémára azonban még nem könnyű. Ezt a következő, déloszi probléma néven ismert, feladaton illusztráljuk: *adott élhosszúságú kockához megszerkesztendő a kétszer akkora térfogatú kocka éle.*

Az adott élhosszúságot választva távolságegységnek, a feladat az

$$x^3 = 2$$

egyenlet egy megoldásának megszerkesztését kívánja. Igaz, hogy a megoldás $x = \sqrt[3]{2}$ alakban írható, és itt köbgyökvonást, tehát a kritérium szerint meg nem engedett műveletet, alkalmaztunk; ez azonban még nem biztosítja a szerkesztés kivihetetlenségét körzővel és vonalzóval, mert nem zárja ki ugyanis eleve azt, hogy más úton ne számíthassuk ki a $\sqrt[3]{2}$-t racionális számokból alapműveletek és négyzetgyökvonások, valamilyen bonyolultabb, ismételt alkalmazásával, ahogy a negyedik gyökvonást pl. visszavezethetjük (nagyon egyszerűen) négyzetgyökvonásra. A továbbiakban azt is be fogjuk látni, hogy nincs olyan ördöngös formula, amely a $\sqrt[3]{2}$ -höz csak négyzetgyökvonás felhasználásával elvezetne.

10. Mivel a szerkeszthetőségre nyert kritérium algebrai, alkalmazása áttekinthetőbb lesz, ha néhány algebrai fogalmat előrebocsátunk. Kitüntetett szerepe van valamilyen adott $a_1, \ldots, a_k$ számokból a négy alapművelettel kiszámítható számok összességének. Egy ilyen összességet *számtestnek* szokás nevezni, közelebbről az $a_1, \ldots, a_k$ számokkal *generált* (vagy származtatott) számtestnek.

Így az 1 szám a racionális számtestet generálja, mert összeadással eljutunk belőle a természetes számokhoz, ezekből kivonással 0-hoz és a negatív egészekhez, végül osztással az összes racionális számokhoz. Ezenkívül más számot nem kapunk, mert két racionális szám összege, különbsége, szorzata és hányadosa is racionális. Könnyen látható, hogy bármely más racionális szám is a racionális számok testét generálja, kivéve a 0-t, mert az az által generált test egyedül a 0-ból áll.

Minden más számtest is tartalmazza a racionális számokat. Ha ugyanis van a testnek egy 0-tól különböző száma, akkor ezt sajátmagával osztva nyerjük, hogy az 1 is benne van a testben, és ezzel együtt, mint láttuk, minden racionális számnak is benne kellene lennie. Vannak számtestek, amelyek határozottan bővebbek a racionális számok testénél, hiszen pl: a $\sqrt{2}$-vel generált test biztosan tartalmazza a racionális számokon kívül a $\sqrt{2}$-t is, amelyről tudjuk, hogy nem racionális.

Bizonyos, $a_1, \ldots, a_k$ számok generálta test legyen T. Legyen t egy olyan T-beli szám, amely nem négyzete valamilyen T-beli számnak,[1] továbbá b és c tetszésszerinti T-beli számok, $c \neq 0$. Ha $a_{k+1} = b + c\sqrt{t}$, képezzük az $a_1, \ldots, a_k$, a_{k+1} által generált testet. Azt állítjuk, hogy ennek a testnek minden száma

$$u + v\sqrt{t} \tag{1}$$

alakban írható, ahol u és v a T testbeli számok. Legyen pl. T a racionális számok teste (amelyet pl. $a_1 = 1$ generál), $t = 3$, és $a_2 = 1 + 2\sqrt{3}$. Az a_1 és a_2 által generált test két száma

$$n_1 = 2a_1 - \frac{1}{2}a_2 = \frac{3}{2} - \sqrt{3}, \qquad n_2 = \frac{5}{3}a_1 + \frac{1}{3}a_2 = 2 + \frac{2}{3}\sqrt{3},$$

akkor ezek összege, különbsége, szorzata, illetőleg hányadosa:

$$n_1 + n_2 = \frac{7}{2} - \frac{1}{3}\sqrt{3}, \qquad n_1 - n_2 = -\frac{1}{2} - \frac{5}{3}\sqrt{3},$$

$$n_1 \cdot n_2 = 1 - \sqrt{3}, \qquad \text{és} \qquad \frac{n_1}{n_2} = \frac{\frac{3}{2} - \sqrt{3}}{2 + \frac{2}{3}\sqrt{3}} =$$

$$= \frac{\left(\frac{3}{2} - \sqrt{3}\right)\left(2 - \frac{2}{3}\sqrt{3}\right)}{\left(2 + \frac{2}{3}\sqrt{3}\right)\left(2 - \frac{2}{3}\sqrt{3}\right)} = \frac{5 - 3\sqrt{3}}{4 - \frac{4}{3}} = \frac{15}{8} - \frac{9}{8}\sqrt{3}.$$

Általában is hasonlóan járunk el. Összeadással és kivonással csak (1) alakú számokhoz jutunk. Ha két ilyen alakú számot szorzunk

$$(u_1 + v_1\sqrt{t})(u_2 + v_2\sqrt{t}) = (u_1u_2 + v_1v_2t) + (u_1v_2 + u_2v_1)\sqrt{t},$$

[1] A racionális számok testében ilyen pl. 2, 3 vagy $\frac{1}{2}$, de nem ilyen pl. 4 vagy $\frac{9}{16}$.

ahol a zárójelben álló számok T-ből valók. Végül két (1) alakú szám hányadosa is ilyen alakra hozható a nevező gyöktelenítésével, ha az osztó nem 0:

$$\frac{u_1+v_1\sqrt{t}}{u_2+v_2\sqrt{t}}=\frac{(u_1+v_1\sqrt{t})(u_2-v_2\sqrt{t})}{(u_2+v_2\sqrt{t})(u_2-v_2\sqrt{t})}=$$
$$=\frac{u_1u_2-v_1v_2t}{u_2^2-v_2^2t}+\frac{(u_2v_1-u_1v_2)}{u_2^2-v_2^2t}\sqrt{t}.$$

Itt a nevező továbbra sem 0, mert akkor vagy u_2 is, v_2 is 0 volna, vagy egyik sem. Az előbbi nem lehet, mert eredetileg nem 0-val osztottunk. Az utóbbi esetben

$$t=\left(\frac{u_2}{v_2}\right)^2$$

volna, de t-ről feltettük, hogy nem egyenlő egy T-beli szám négyzetével. Ekkor viszont a fenti utolsó kifejezésben szereplő két tört T-beli szám. Ezzel bebizonyítottuk állításunkat.
Látjuk, hogy ezt az új, és T-nél bővebb testet (hiszen tartalmazza $\sqrt{t}$-t, és ez nincs benne T-ben) $\sqrt{t}$ meghatározza, függetlenül attól, hogy mi volt b és c, csak c nem lehetett 0. Ezt a testet T-nek $\sqrt{t}$-vel való bővítésének nevezzük és így jelöljük: $T(\sqrt{t})$.

11. A fentiekben szerepet játszott még polinomok felbontása alacsonyabbfokú tényezőkre. Egy ilyen felbontás létezése függ attól, hogy milyen számokat engedünk meg együtthatókul. A

$$4x^2-3$$

polinom például a racionális számok R testéből vett együtthatós tényezőkre nem bontható, de felbomlik két elsőfokú $R(\sqrt{3})$-beli együtthatós tényezőre:

$$4x^2-3=(2x-\sqrt{3})(2x+\sqrt{3}).$$

Ha egy polinom együtthatói egy T testből valók, de nem, bonthatók a polinom két alacsonyabbfokú T-beli együtthatós polinom szorzatára, akkor azt mondjuk, hogy *irreducibilis a polinom T fölött.* Ha van ilyen felbontás, akkor a polinomot T fölött reducibilisnek mondjuk.
Az α szög harmadrészének cosinusát szolgáltató

(2) $$4x^3-3x-a=0$$

egyenletben, hol $a=\cos\alpha$ (lásd az 1. pontot az 1. közleményben), a baloldal $\alpha=90°$-ra (tehát $a=0$-ra) reducibilis R fölött.

$$4x^3-3x=x(4x^2-3),$$

hasonlóképpen $\alpha=45°$-ra $\left(a=\frac{1}{\sqrt{2}}\text{-re}\right)$ reducibilis $R\left(\frac{1}{\sqrt{2}}\right)$ fölött:

$$4x^3-3x-\frac{1}{\sqrt{2}}=\left(x+\frac{1}{\sqrt{2}}\right)\left(4x^2-\frac{4}{\sqrt{2}}x-1\right).$$

(R fölötti reducibilitásnak itt értelme sincs, hiszen az együtthatók nem mind racionálisak.)
$\alpha=60°$-ra, tehát, ha $\cos\alpha=\frac{1}{2}$, a

$$4x^3-3x-\frac{1}{2}=0,$$

azaz a

$$8x^3-6x-1=0$$

egyenletet kapjuk. Itt a baloldal a racionális számtest felett irreducibilis. Ha ugyanis felbomlana alacsonyabbfokú, racionális együtthatós tényezőkre, azok egyike elsőfokú volna, és így volna egy racionális gyöke. Tudjuk azonban, hogy csak olyan racionális szám lehet egy egész együtthatós egyenletnek gyöke, amelynek számlálója az állandó tagnak, nevezője pedig a legmagasabbfokú tag együtthatójának osztója. Így esetünkben a $\pm\frac{1}{2}$, $\pm\frac{1}{4}$, $\pm\frac{1}{8}$ számok jönnek számításba, és egy kis számítás mutatja, hogy ezek egyike sem elégíti ki az egyenletet.
Hasonlóan látható, hogy a déloszi problémához tartozó

$$x^3-2=0$$

egyenlet baloldala irreducibilis R fölött, mert különben volna racionális gyöke és ez csak ± 1 vagy ± 2 lehetne, amelyek azonban nem tesznek eleget az egyenletnek.

Harmadfokú egyenlet gyökeinek nem szerkeszthető volta

12. Ezen előkészítések után be fogjuk bizonyítani a következőt:
TÉTEL: *Ha bizonyos szerkesztési alapadatokkal generált* T *testhez adva van egy*

$$x^3 + ax^2 + bx + c = 0 \tag{3}$$

egyenlet, melynek baloldala T *fölött irreducibilis, akkor ezen adatokból az egyenlet egyik gyöke sem szerkeszthető meg.*
A tétel magában foglalja pl. a déloszi probléma megoldhatatlanságát körző és vonalzóval, és a 60° harmadrészének, 20°-nak a nem szerkeszthető voltát. Az egyetlen alapadat ugyanis az első esetben 2, a másodikban $\frac{1}{2}$, ezek mindkét esetben a racionális számtestet generálják, viszont a szerkesztendő adat, amint éppen láttuk, mindkét esetben egy R fölött irreducibilis egyenlet gyöke.

13. A tétel itt következő bizonyítása Edmund Landau híres német matematikustól ered. Indirekt úton fogunk eljárni, azaz feltesszük, hogy ha a tétel nem volna helyes, volna olyan (3) alakú egyenlet, amelyik irreducibilis az alapadatokkal generált test fölött, és mégis megszerkeszthető egy gyöke. Ebből a feltevésből ellentmondásra fogunk jutni.
Feltevésünk szerint a szerkesztés befejeztével eljutunk az egyenlet egy gyökéhez. Beláttuk az 1. közlemény 2 pontjában (lásd a (2) átalakítást), hogy ekkor kiemelhető a baloldalból a gyökhöz tartozó gyöktényező. A visszamaradó tényező együtthatói a gyökből és az eredeti együtthatókból, számítható ki, tehát benne vannak az összes ismert adatok (alap- és megszerkesztett adatok) által generált testben. Ebben a testben tehát a (3) egyenlet már reducibilis.
Kövessük lépésről lépésre a szerkesztést. Az alapadatok generálta test fölött a (3) egyenlet baloldala még irreducibilis, a szerkesztés végén már reducibilis. Kell tehát egy lépésnek lennie, amely előtt az eddig ismert adatok generálta T test fölött a polinom még irreducibilis, de a szerkesztés olyan adatot szolgáltat, amelyet az előzőkhöz hozzávéve az ezek által generált testben már reducibilissá válik.
Ez az adat nem lehet az előzőkből négy alapművelettel kiszámítható, mert akkor benne volna a T testben, és így hozzávétele az előzőkhöz, nem bővítené a testet. Mivel minden egyes szerkesztési lépés a négy alapművelettel vagy a négy alapművelettel és négyzetgyökvonással származó adatot szolgáltat, így csak az a lehetőség marad, hogy ez az adat

$$b + c\sqrt{t}$$

alakú, ahol t olyan T-beli szám, amelynek a négyzete nincs T-ben, c pedig nem 0. Ennek hozzávétele az előző adatokhoz a $T(\sqrt{t})$ testhez vezet. Ebben (3) bal-oldala már felbontható alacsonyabbfokú tényezőkre.
Ekkor az egyik tényező elsőfokú, s így gyöke az együtthatók hányadosaként adódik, tehát benne van a $T(\sqrt{t})$ testben. Legyen ez

$$x_1 = u_1 + v_1\sqrt{t}.$$

Itt $v_1 \neq 0$, mert T-ben még nem bomlik fel a polinom, s így gyöke sem lehet. Behelyettesítve x_1-et (3)-ba, azt kapjuk, hogy

$$\begin{aligned} 0 = x_1^3 + ax_1^2 + bx_1 + c = (u_1^3 + 3u_1v_1^2t + au_1^2 + av_1^2t + bu_1 + c) + \\ + (3u_1^2v_1 + v_1^3t + 2au_1v_1 + bv_1)\sqrt{t} = m + n\sqrt{t}, \end{aligned}$$

ahol m, és n T-beli számok. Megmutatjuk, hogy m és n külön-külön 0.
Ha $n = 0$, akkor nyilván m is 0. Ha viszont n a 0-tól különböző szám volna, akkor

$$\sqrt{t} = -\frac{m}{n}, \qquad t = \left(\frac{m}{n}\right)^2$$

volna, holott t nem négyzete T-beli számnak.
Ha viszont $m = n = 0$, akkor

$$\begin{aligned} &(u_1 - v_1\sqrt{t})^3 + a(u_1 - v_1\sqrt{t})^2 + b(u_1 - v_1\sqrt{t}) + c = \\ &= (u_1^3 + 3u_1v_1^2t + au_1^2 + av_1^2t + bu_1 + c) - (3u_1^2v_1 + v_1^3t + 2au_1v_1)\sqrt{t} = \\ &= m - n\sqrt{t} = 0, \end{aligned}$$

tehát

$$x_2 = u_1 - v_1\sqrt{t}$$

is gyöke a (3) egyenletnek, és x_1-től különböző gyök, mert $v_1 \neq 0$. Így x_2 az $x - x_1$ gyöktényező kiemelése után maradó másodfokú polinomnak gyöke, tehát abból még kiemelhető az $x - x_2$ gyöktényező, és visszamarad egy elsőfokú tényező. Az x együtthatója ebben is 1, mert a szorzatban is együtthatóval szerepel x^3. Így (3) bal oldala így alakítható át:

$$x^3 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3),$$

ahol x_1 és x_2 a fenti értékek, x_3 pedig alkalmas szám, amit éppen a nyert összefüggésből határozhatunk meg, ha összehasonlítjuk pl. a másodfokú tag együtthatóját a két oldalon:

$$a = -x_1 - x_2 - x_3, \qquad \text{ahonnan} \qquad x_3 = -x_1 - x_2 - a = -2u_1 - a.$$

Ez azonban T-beli szám, másrészt

$$(x - x_1)(x - x_2) = [(x - u_1) - v_1\sqrt{t}][(x - u_1) + v_1\sqrt{t}] = (x - u_1)^2 - v_1^2 t =$$
$$= x^2 - 2u_1 x + (u_1^2 - v_1^2 t)$$

szintén T-beli együtthatós polinom. A (3) baloldala tehát felbomlana két T-beli együtthatós polinomra, holott T olyan test volt, amiben (3) baloldala még irreducibilis.
Ezzel ellenmondásra jutottunk, s így helytelen volt az a feltevés, amiből kiindultunk. Azt nyertük tehát, hogy a (3) egyenlet egyik gyöke sem lehet szerkeszthető, amint azt a tétel állítja.
Megjegyezzük, hogy igaz a következő tétel, amelynek a fenti speciális esete:
Ha egy

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$$

egyenlet bizonyos alapadatok által generált test fölött irreducibilis, és n nem 2 valamilyen hatványa, akkor az egyenlet egyetlen gyöke sem szerkeszthető.