Számológéppel gyökök ellen

dr. Szalkai István
Pannon Egyetem, Veszprém,
SZALKAI@ALMOS.UNI-PANNON.HU

2019.12.30.

Kivonat

Köztudottan "nem illik" irracionális egyenlőségeket, mint pl. $\sqrt{2}+\sqrt{5-2\sqrt{6}} \stackrel{?}{=} \sqrt{3}$ csak zsebszámológéppel kiszámolva "*bebizonyítani*". Az alábbiakban megmutatjuk, hogy bizonyos esetekben (mint a fenti példában) mégis "DE", vagyis *matematikai precízség* is elérhető zsebszámológépek (véges) számításaival, sőt már megvalósult (komoly) alkalmazásokat is mutatunk a cikk végén.

HALADVANY-KIADVANY, 2019.12.30.
http://www.math.bme.hu/~hujter/halad

1. Bemelegítés

Racionális számok esetén működik-e a "zsebszámológép" módszer, például, az

$$\frac{5+\frac{2}{3}}{\frac{4}{7}-\frac{1}{11}} \stackrel{?}{=} 11+\frac{17}{37}+\frac{1}{3}\ . \tag{1}$$

egyenlőségnél? Hiszen ezek a törtek is végtelen tizedestörtek. Azonban az egyenlőség mindkét oldala *periodikus* tizedes tört, ezért számológéppel biztosan elég

$$2\cdot lkkt\,(nevezok)+2 \tag{2}$$

tizedesjegyig számolnunk (lehet, hogy kevesebb is elég) - ennek végiggondolása házi feladat.

Tekintsük most a bevezető példát:

$$\sqrt{2}+\sqrt{5-2\sqrt{6}} \stackrel{?}{=} \sqrt{3}\ . \tag{3}$$

Legelső ötletünk, hogy tekintjük a két oldal különbségét: legyen

$$\beta := \sqrt{2}+\sqrt{5-2\sqrt{6}}-\sqrt{3} \qquad \stackrel{?}{=}\ 0 \tag{4}$$

és tüntessük el a gyököket:

$$\begin{aligned}
&\beta-\sqrt{5-2\sqrt{6}}=\sqrt{2}-\sqrt{3} \qquad /\ (\ )^2\\
&\beta^2+\left(5-2\sqrt{6}\right)-2\beta\sqrt{5-2\sqrt{6}}=2+3-2\sqrt{6}\ ,\\
&\beta^2-2\beta\sqrt{5-2\sqrt{6}}=0\ ,\\
&\beta^2=2\beta\sqrt{5-2\sqrt{6}} \qquad /\ (\ )^2\\
&\beta^4=4\beta^2\cdot\left(5-2\sqrt{6}\right)=20\beta^2-8\beta^2\sqrt{6}\ ,\\
&\beta^4-20\beta^2=-8\beta^2\sqrt{6} \qquad /\ (\ )^2\\
&\beta^8-40\beta^6+400\beta^4=64\cdot 6\beta^4\\
&\beta^8-40\beta^6+16\beta^4=0\ .
\end{aligned}$$

Tehát: β gyöke egy egész együtthatójú polinomnak! Márpedig egy polinomnak véges sok gyöke van. Ha pedig a (nemnulla) gyökök 0 -tól való távolságaira tudnánk egy ε alsó becslést adni (a polinom együtthatóinak ismeretében), akkor a számológépes módszer a következő lenne: kiszámoljuk β értékét (zseb)számológéppel, ε -nál pontosabban (több tizedesjegyre). Ha ez a numerikus érték ε alatt van, akkor biztosan állíthatjuk, hogy $\beta = 0$, és ez a módszer valóban matematikailag precíz! Az alábbiakban látni fogjuk, hogy ez valóban (már) járt út, tehát a valóság!

Kérjük az Olvasó türelmét és kitartását!

2. Algebrai számok

Mint láttuk, β speciális irracionális szám. Ebben a fejezetben pontosan meghatározzuk, hogy milyen (speciális) számokkal is foglalkozunk ebben a cikkben.

1. Definíció. $\mathbb{Z}$ *= egész -,* $\mathbb{Q}$ *= racionális -,* $\mathbb{R}$ *= valós -,* $\mathbb{C}$ *= komplex számok halmaza. Legyen továbbá*

$\mathbb{A}_{\mathbb{Z},\sqrt{}} := [\mathbb{Z}\ ;\ +,-,\cdot,\sqrt[y]{x}]$ *azon komplex számok halmaza, amelyek felírhatók egész számok,* három *alapművelet (osztás nélkül) és tetszőleges gyökjelek segítségével,*

$\mathbb{A}_{\mathbb{Q},\sqrt{}} := [\mathbb{Q}\ ;\ +,-,\cdot,\div,\sqrt[y]{x}]$ *azon komplex számok halmaza, amelyek felírhatók racionális számok,* négy *alapművelet (osztás megengedett) és tetszőleges gyökjelek segítségével; ezeket a számokat* ***konstruálható számok*** *-nak hívjuk,*

$$\mathbb{A}_{\mathbb{Z}[x]} := \left\{ p(x)\ \ \textit{gyökei}: p(x) \in \mathbb{Z}[x]\ \ ,\ \text{főegyüttható}^{1)} = \pm 1 \right\}$$

a ± 1 *főegyütthatójú,* egész *együtthatós polinomok (komplex) gyökeinek halmaza,*

$\mathbb{A}_{int} := \mathbb{A}_{\mathbb{Z}[x]}$, *amely számokat* ***algebrai egész számok*** *-nak hívunk,*

$\mathbb{A}_{\mathbb{Q}[x]} := \{q(x)\ \ \textit{gyökei}: q(x) \in \mathbb{Q}[x]\}$

a racionális *együtthatós polinomok (komplex) gyökeinek halmaza,*

$\mathbb{A} := \mathbb{A}_{\mathbb{Q}[x]}$, *amely számokat* ***algebrai számok*** *-nak hívunk.* $\square$

2. Megjegyzés. *i) Könnyen látható, hogy*

$$\mathbb{A}_{\mathbb{Q},\sqrt{}} = \left[\mathbb{Z}\ ;\ +,-,\cdot,\div,\sqrt[y]{x}\right]\ , \tag{5}$$

vagyis csak egész számokból *is fel tudjuk építeni a konstruálható számokat, az osztás felhasználásával.*

ii) Az is nyilvánvaló, hogy bármely $q(x) \in \mathbb{Q}[x]$ *racionális együtthatójú polinomot az együtthatók nevezőinek* c *legkisebb többszörösével szorozva a kapott polinom,* $p(x) = c \cdot q(x)$ *már egész együtthatójú, vagyis* $\mathbb{Z}[x]$ *-nek eleme. Ez azt jelenti, hogy a* $\mathbb{Q}[x]$ *-beli polinomok gyökeinek halmaza megegyezik a* $\mathbb{Z}[x]$ *-beli polinomok gyökeinek halmazával:*

$$\mathbb{A}_{\mathbb{Q}[x]} = \{p(x)\ \ \textit{gyökei}: p(x) \in \mathbb{Z}[x]\ \ \textit{(bármilyen főegyüttható)}\}\ .$$

A lényeges különbség $\mathbb{A}_{\mathbb{Q}[x]}$ *és* $\mathbb{A}_{\mathbb{Z}[x]}$ *között az, hogy az* $\mathbb{A}_{\mathbb{Z}[x]}$ *-beli (egész együtthatójú) polinomok főegyütthatójáról megköveteljük, hogy pontosan* ± 1 *legyen. Később látni fogjuk, hogy ez nem öncélú megkülönböztetés. Az olyan polinomokat, melyek főegyütthatója éppen* ± 1*, angolul* ***monic*** *polinomoknak nevezzük. (Nyilván* $\mathbb{A}_{\mathbb{Q}[x]}$ *-beli polinomok főegyütthatóira bármilyen egész vagy racionális számot előírhatunk, vagyis* $\mathbb{A}_{\mathbb{Q}[x]}$ *-ben ez lényegtelen kérdés.)*

A fentiek szerint $\mathbb{A}_{\mathbb{Z}[x]} \subsetneqq \mathbb{A}_{\mathbb{Q}[x]}$ *(lásd még az 3. Tételt), és a bevezetésben említett* β *szám* $\mathbb{A}_{\mathbb{Z}[x]}$ *-nak eleme. Továbbá* [w A hu] *és* [w A en] *-ben bőséges listákat találunk* $\mathbb{A}_{\mathbb{Z}[x]}$ *és* $\mathbb{A}_{\mathbb{Q}[x]}$ *elemeiről (algebrai és algebrai egész számokról), valamint* $\mathbb{A}_{\mathbb{Q}[x]}$ *-ba* nem *tartozó számokról. Például, bármely* $r \in \mathbb{Q}$ *racionális számra* $\sin(r\pi)$ *és* $\cos(r\pi)$ *is algebrai számok (elemei* $\mathbb{A}_{\mathbb{Q}[x]}$ *-nak).*

iii) A fent definiált $\mathbb{A}_{\mathbb{Q},\sqrt{\ }}$ *"konstruálható" számok halmaza nem azonos a "**kiszámítható**", vagy más néven "**rekurzív**" számok* $\mathbb{K}$ *halmazával. Ez utóbbi olyan valós számokat tartalmaz, amelyek valamely algoritmussal (számítógép programmal) tetszőleges pontossággal megadhatóak. Például* π *és* e *rekurzív de nem konstruálható számok, és nyilván* $\mathbb{A}_{\mathbb{Q},\sqrt{\ }} \subsetneqq \mathbb{K}$ *.*

3. Tétel. *i)* $\mathbb{Z} \subsetneqq \mathbb{A}_{\mathbb{Z},\sqrt{\ }} \subsetneqq \mathbb{A}_{\mathbb{Z}[x]} \subsetneqq \mathbb{A}_{\mathbb{Q}[x]} = \mathbb{A} \subsetneqq \mathbb{K} \subsetneqq \mathbb{C}$,

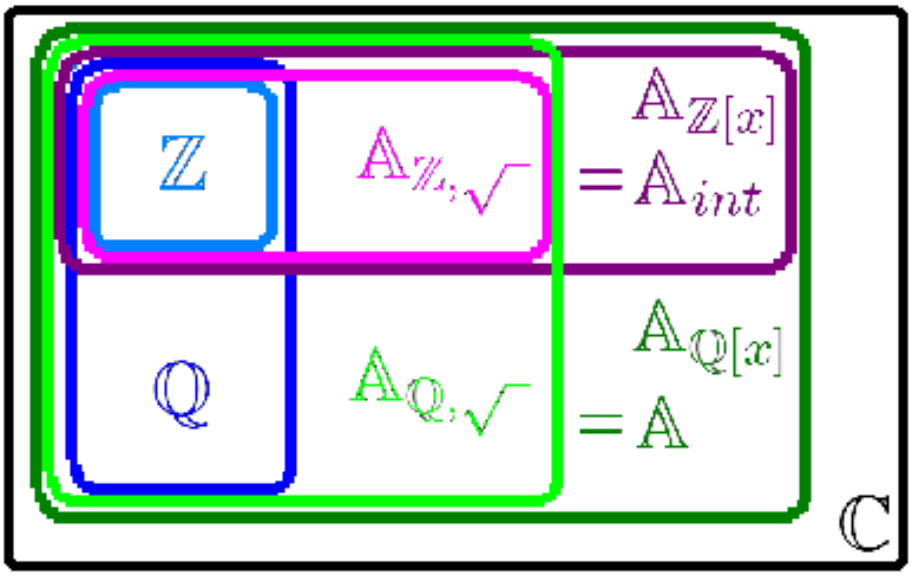
ii) $\mathbb{A}_{\mathbb{Z},\sqrt{\ }} \subsetneqq \mathbb{A}_{\mathbb{Q},\sqrt{\ }} \subsetneqq \mathbb{A}_{\mathbb{Q}[x]} = \mathbb{A}$,

iii) $\mathbb{Z}$ *,* $\mathbb{A}_{\mathbb{Z},\sqrt{\ }}$ *és* $\mathbb{A}_{\mathbb{Z}[x]}$ gyűrűk *(azaz zártak az összeadásra, kivonásra és szorzásra),*

iv) $\mathbb{Q}$ *,* $\mathbb{A}_{\mathbb{Q},\sqrt{\ }}$ *,* $\mathbb{A}_{\mathbb{Q}[x]}$ *és* $\mathbb{K}$ testek *(azaz zártak a négy alapműveletre).* □

4. Megjegyzés. *A fenti i) és ii) összefüggéseket az alábbi ábra szemlélteti, sajnos* $\mathbb{K}$ *nem szerepel rajta. Az ábra nem "méretarányos", mert mindegyik* $\mathbb{A}_*$ *halmaz és* $\mathbb{K}$ *is* megszámlálhatóak *(vagyis ugyanannyi elemük van, mint* $\mathbb{N}$ *-nek),* $\mathbb{C}$ *pedig* kontinuum *számosságú.*

A továbbiakban elsősorban az <u>*algebrai egészekkel*</u> ($\mathbb{A}_{int} = \mathbb{A}_{\mathbb{Z}[x]}$) foglalkozunk!



3. Mátrixok

Az egész- és racionális együtthatójú polinomok (kissé bonyolult) elmélete megoldja a gyök-számológép problémánkat, de érdekes módon az alábbi, mátrixos megközelítés kevesebb új elmélet megismerését igényli (de így is még egy kis figyelmet kérünk az Olvasótól). A legtöbb tétel bizonyítása is nagyon egyszerű, alább le is írjuk őket. Azonban az Olvasónak mégis azt javasoljuk, hogy első olvasatban hagyja ki ezeket a bizonyításokat, és ugorjon a következő fejezetre.

5. Állítás. *Minden, csak egész számokat tartalmazó mátrix (vagyis* $A \in \mathbb{Z}^{n\times n}$*)* karakterisztikus polinomja[2)] *egy egész együtthatós és főegyütthatója* ± 1 *(ú.n.* ***"monic"*** *polinom).* $\square$

[2)] **Definíció:** Egy (tetszőleges) $A \in \mathbb{R}^{n\times n}$ (vagy $A \in \mathbb{C}^{n\times n}$) mátrix **sajátértéke** $\lambda \in \mathbb{C}$ és **sajátvektora** $\overrightarrow{v} \in \mathbb{R}^n$, ha $\overrightarrow{v} \neq \overrightarrow{0}$ és $A\overrightarrow{v} = \lambda\overrightarrow{v}$. $\square$

Könnyen látható, hogy $\overrightarrow{v} \neq \overrightarrow{0}$ esetén szükségképpen $\det(A - \lambda \cdot E) = 0$, ahol E az egységmátrix. Továbbá $\det(A - \lambda \cdot E)$ egy n -edfokú polinomja λ -nek, amit A **karakterisztikus polinomjának** nevezünk: $kar_A(\lambda) := \det(A - \lambda \cdot E)$. $\square$

6. Megjegyzés. *Sajnos a* ***karakterisztikus polinom*** *pontos definíciója nem egyértelmű a szakirodalomban. Legtöbbször a*

$$kar_A(x) := \det(A - x \cdot E) \tag{6}$$

definícióval találkozunk, ahol $A, E \in \mathbb{R}^{n\times n}$ *és* E *az* egységmátrix *(pl.* [w S hu], [w S en], [m Ch]*), de nagyon sokszor a*

$$kar^*_A(x) := \det(x \cdot E - A) \tag{7}$$

képlettel ([w Ch en], [w CM en], [m CM], [SE 2000]*). A két definíció között nincs lényeges különbség, hiszen*

$$kar^*_A(x) = (-1)^n \cdot kar_A(x) \ , \tag{8}$$

tehát a két polinom együtthatói (előjeltől eltekintve) és gyökei (A sajátértékei) ugyanazok*. A kétféle képlet keveredése, különösen egymásra hivatkozó honlapokon eléggé zavaró (pl.* [m Ch] *és* [m CM]*).*

Az alábbiakban mindig jelöljük, hogy a "$kar_A(x)$*" vagy "*$kar^*_A(x)$*" polinommal dolgozunk.*

A következő összefüggés önmagában is érdekes, és a továbbiakban fontos lesz:

7. Állítás. *Tetszőleges* $c_0, ..., c_{n-1}$ *valós (vagy komplex) számok esetén az*

$$A_{\overrightarrow{c}} := \begin{bmatrix} 0 & 0 & ... & 0 & 0 & -c_0 \\ 1 & 0 & ... & 0 & 0 & -c_1 \\ 0 & 1 & ... & 0 & 0 & -c_2 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & ... & 1 & 0 & -c_{n-2} \\ 0 & 0 & ... & 0 & 1 & -c_{n-1} \end{bmatrix} \in \mathbb{R}^{n\times n} \tag{9}$$

mátrix $kar^*_A(x)$ *karakterisztikus polinomja éppen a*

$$p_{\overrightarrow{c}}(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + c_1 x + c_0 \tag{10}$$

monic *polinom, vagyis*

$$kar^*_{A_{\overrightarrow{c}}}(x) = \det(x \cdot E - A_{\overrightarrow{c}}) = p_{\overrightarrow{c}}(x) \ . \tag{11}$$

□

A (11) összefüggés miatt nevezik az $A_{\overrightarrow{c}}$ mátrixot a $p_{\overrightarrow{c}}(\lambda)$ polinom **kísérő mátrixának** (*companion matrix*, ld. pl. [m CM], [w CM en]). Az állítás igazolása teljes indukcióval nem nehéz (hasonló a Horner elrendezéshez).

Vegyük észre, hogy a csak egész számokból álló ($\mathbb{Z}^{n\times n}$ -beli) mátrixok karakterisztikus polinomjai is egész együtthatójúak, és a fenti állítás szerint *minden* monic polinom valamely $\mathbb{Z}^{n\times n}$ -beli mátrix karakterisztikus polinomja, és hasonló összefüggés igaz a racionális elemű mátrixok és polinomok között. Ezt a két észrevételt fogalmazzuk meg precízebben az alábbi definícióban és tételben.

8. Definíció. *Legyen*

$$\begin{aligned}\mathbb{A}_{\mathbb{Z},karpol} &= \left\{kar\,(A)\ \ gyökei:\ A\in\mathbb{Z}^{n\times n}\right\} \\ &= \left\{A\ sajátértékei:\ \ A\in\mathbb{Z}^{n\times n}\right\}\end{aligned} \tag{12}$$

és

$$\begin{aligned}\mathbb{A}_{\mathbb{Q},karpol} &= \left\{kar\,(B)\ \ gyökei:\ B\in\mathbb{Q}^{n\times n}\right\} \\ &= \left\{B\ sajátértékei:\ \ B\in\mathbb{Q}^{n\times n}\right\}\end{aligned} \tag{13}$$

ahol $\mathbb{Z}^{n\times n}$ és $\mathbb{Q}^{n\times n}$ az egész- illetve racionális elemű mátrixok halmaza. □

9. Tétel.

$$\mathbb{A}_{\mathbb{Z},karpol}=\mathbb{A}_{\mathbb{Z}[x]}\quad \text{és}\quad \mathbb{A}_{\mathbb{Q},karpol}=\mathbb{A}_{\mathbb{Q}[x]}\ .\qquad \square \tag{14}$$

A továbbiakban szükségünk lesz az alábbi technikai jelölésekre.

10. Definíció. *Legyen tetszőleges $n,b\in\mathbb{N}$ esetén*

$$\mathcal{M}(n,b):=\left\{A\in\mathbb{Z}^{n\times n}\ :\ |a_{i,j}|\le b\right\} \tag{15}$$

az olyan $n\times n$ méretű mátrixok halmaza, amelyeknek minden eleme (abszolút értékben) legfeljebb b , és

$$\Lambda(n,b):=\{A\ sajátértékei:\ \ A\in\mathcal{M}(n,b)\} \tag{16}$$

a fenti mátrixok (összes) sajátértékeinek (véges) halmazai. □

Nyilván minden $n \in \mathbb{N}$ esetén

$$\bigcup_{b \in \mathbb{N}} \mathcal{M}(n,b) = \mathbb{Z}^{n \times n} \ , \tag{17}$$

és

11. Tétel.

$$\bigcup_{n,b \in \mathbb{N}} \Lambda(n,b) = \mathbb{A}_{\mathbb{Z},karpol} = \mathbb{A}_{\mathbb{Z}[x]} \ . \qquad \square \tag{18}$$

Fontos megjegyzés: Előrebocsájtjuk, hogy az alábbi 12., 14. és 15. Tételekben mindössze n és b , azaz a mátrix *mérete* és elemeinek *felső korlátja* szerepelnek, sőt azok is nagyon egyszerű képletekben, vagyis a kérdéses algebrai számhoz tartozó mátrix semmilyen további, bonyolultabb szerkezete vagy tulajdonsága nem szükséges, sőt maga a mátrix sem! Ez az elmélet egyik fő erénye!

12. Tétel. *Minden* $n, b \in \mathbb{N}$ *és* $\lambda \in \Lambda(n,b)$ *esetén*

$$|\lambda| \leq n \cdot b \ . \tag{19}$$

Bizonyítás. Legyen λ az A mátrix sajátértéke a $\overrightarrow{v}$ sajátvektorral. Tegyük fel, hogy

$$\|\overrightarrow{v}\|_2 = |\overrightarrow{v}| = \sqrt{\sum_{i=1}^{n} |v_i|^2} = 1 \ , \tag{20}$$

ekkor

$$\overrightarrow{v} \cdot (A\overrightarrow{v}) = \overrightarrow{v} \cdot \lambda \overrightarrow{v} = \lambda \tag{21}$$

és

$$|\lambda| \ = \ (\overrightarrow{v} \cdot A\overrightarrow{v}) = \left| \sum_{i=1}^{n} \sum_{j=1}^{n} a_{i,j} v_i v_j \right| \leq b \cdot \sum_{i=1}^{n} \sum_{j=1}^{n} |v_i v_j| \tag{22}$$

$$= \ b \cdot \left(\sum_{i=1}^{n} |v_i| \right) \cdot \left(\sum_{j=1}^{n} |v_j| \right) = b \cdot \left(\|\overrightarrow{v}\|_1 \right)^2 \leq b \cdot \left(\sqrt{n} \cdot \|\overrightarrow{v}\|_2 \right)^2 = b \cdot n \ . \tag{23}$$

mivel (a számtani és a négyzetes közepek közötti összefüggés alapján)

$$\frac{\|\overrightarrow{v}\|_1}{n} = \frac{1}{n}\sum_{i=1}^{n}|v_i| \leq \sqrt{\frac{1}{n}\sum_{i=1}^{n}|v_i|^2} = \frac{1}{\sqrt{n}}\|\overrightarrow{v}\|_2 \tag{24}$$

vagyis

$$\|\overrightarrow{v}\|_1 \leq \sqrt{n}\cdot\|\overrightarrow{v}\|_2 \ . \tag{25}$$

■

13. Megjegyzés. *A becslés éles, mert ha A összes eleme b , akkor az $\mathbf{1} := [1,...,1]$ sajátvektorral $A\mathbf{1} = nb\mathbf{1}$ teljesül.*

14. Tétel. ***(Gyök-szétválasztási tétel)*** *Tetszőleges $n, b \in \mathbb{N}$ és $\lambda \in \Lambda(n,b)$, $\lambda \neq 0$ esetén*

$$|\lambda| \geq (n\cdot b)^{1-n} = \frac{1}{(nb)^{n-1}} \quad . \tag{26}$$

Bizonyítás. Ha A többi nemnulla sajátértékei $\lambda_2, ..., \lambda_t$ $(t \leq n-1)$, akkor a karakterisztikus polinom legutolsó nemnulla együtthatója éppen $\lambda\cdot\lambda_2\cdot...\cdot\lambda_t$, de $A \in \mathbb{Z}^{n\times n}$ miatt ez az együttható egész szám, vagyis

$$|\lambda\cdot\lambda_2\cdot...\cdot\lambda_t| \geq 1 \tag{27}$$

ahonnan 12. Tétel alapján

$$|\lambda| \geq \frac{1}{|\lambda_2\cdot...\cdot\lambda_t|} \geq \frac{1}{(nb)^{n-1}} \ .$$

■

A fenti (26) alapján (elméletben) már meg is tudjuk oldani a bevezetésben említett "*gyök vs. számológép*" problémánkat: *ha* adott $\lambda \in \mathbb{A}_{\mathbb{Z}[x]}$ algebrai *egész* (!) számhoz meg tudjuk határozni n és b értékét, akkor (26) alapján kicsivel több, mint $\varepsilon = \frac{1}{(nb)^{n-1}} + 1$ (tizedesjegy) pontossággal kell kiszámolnunk λ értékét ahhoz, hogy eldöntsük: $\lambda = 0$ avagy $\lambda \neq 0$.

Már "csak" az a kérdés, hogy hogyan találunk λ -hoz megfelelő n -et és b -t ? (Sajnos az (26) egyenlőtlenségben szereplő alsó becslés általában nagyon kicsi, vagyis a $\frac{1}{(nb)^{n-1}} + 1$ -nál nagyobb pontosságú számolás várhatólag nem zsebszámológéppel, hanem számítógép-programokkal, néhány percnyi-órai futással fog történni.)

15. Tétel. *Legyenek* $n, n_1, n_2, k, b, b_1, b_2 \in \mathbb{N}\setminus\{0\}$ *tetszőleges nemnulla természetes számok,* $\alpha, \beta \in \mathbb{C}$ *komplex számok. Ekkor*

o) ha $k \in \mathbb{Z}$ *(egész) akkor* $k \in \Lambda(1, |k|)$,

i) ha α *gyöke egy egész együtthatós* monic *polinomnak (főegyütthatója* 1*), melynek minden együtthatója abszolút értékben legfeljebb* b *, akkor* $\alpha \in \Lambda(n, b)$,

ii) ha $n_1 \leq n_2$ *és* $b_1 \leq b_2$ *akkor* $\Lambda(n_1, b_1) \subseteqq \Lambda(n_2, b_2)$,

iii) ha $\alpha \in \Lambda(n, b)$ *akkor* $-\alpha, \overline{\alpha} \in \Lambda(n, b)$ *("mínusz"* α *és* α *komplex konjugáltja),*

iv) ha $k \in \mathbb{N}\setminus\{0\}$ *(pozitív egész) és* $\gamma \in \Lambda(n, b)$ *akkor* $\sqrt[k]{\gamma} \in \Lambda(k \cdot n, b)$,

v) ha $\alpha_1 \in \Lambda(n_1, b_1)$ *és* $\alpha_2 \in \Lambda(n_2, b_2)$ *akkor* $\alpha_1 \cdot \alpha_2 \in \Lambda(n_1 \cdot n_2, b_1 \cdot b_1)$,

vi) ha $\alpha_1 \in \Lambda(n_1, b_1)$ *és* $\alpha_2 \in \Lambda(n_2, b_2)$ *akkor* $\alpha_1 + \alpha_2 \in \Lambda(n_1 \cdot n_2, b_1 + b_1)$.

Bizonyítás. o) Nyilván a $[k]$ $(1 \times 1$ mátrix) karakterisztikus polinomja $x - k$, amelynek gyöke k .

i) következik a 7. Állítás (9) mátrixából.

ii) Könnyen igazolható, hogy tetszőleges $A \in \mathbb{R}^{n_1 \times n_1}$ mátrix összes sajátértéke az $\begin{bmatrix} A & \mathbf{0}_1 \\ \mathbf{0}_2 & \mathbf{0}_3 \end{bmatrix} \in \mathbb{R}^{n_2 \times n_2}$ négyzetes mátrixnak is sajátértéke, ahol $\mathbf{0}_1, \mathbf{0}_2, \mathbf{0}_3$ megfelelő méretű mátrixok, b növelésének hatása pedig nyilvánvaló.

iii) Könnyen belátható, hogy ha α gyöke a

$$p(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + ... + c_1 x + c_0$$

polinomnak, akkor

$$(-1)^n(-\alpha)^n + (-1)^{n-1}c_{n-1}(-\alpha)^{n-1} + (-1)^{n-2}c_{n-2}(-\alpha)^{n-2} + ... - c_1(-\alpha) + c_0 = 0$$

és

$$\overline{\alpha}^n + \overline{c_{n-1}} \cdot \overline{\alpha}^{n-1} + \overline{c_{n-2}} \cdot \overline{\alpha}^{n-2} + ... + \overline{c_1} \cdot \overline{\alpha} + \overline{c_0} = \overline{0} .$$

iv) Ha γ gyöke a fenti $p(x)$ polinomnak, akkor $\left(\sqrt[k]{\gamma}\right)^k = \gamma$ miatt

$$\left(\sqrt[k]{\gamma}\right)^{k \cdot n} + c_{n-1}\left(\sqrt[k]{\gamma}\right)^{k \cdot (n-1)} + c_{n-2}\left(\sqrt[k]{\gamma}\right)^{k \cdot (n-2)} + ... + c_1\left(\sqrt[k]{\gamma}\right)^k + c_0 = 0 . \qquad (28)$$

v) és **vi)** bizonyítása sajnos igényli a mátrixok *Kronecker (tenzor) szorzatát* (lásd például [m K], [w K hu] vagy [SE 2000]). A bizonyítás vázlatát a Függelékben közöljük. ■

Mint nemsokára látni fogjuk, a fenti tételben kapott n és b számok eléggé nagyok, és a (26) egyenlőtlenség is nagyon nagy pontosságot igényel, ezért hasznos lesz még a következő kis eredmény is:

16. Állítás. *Tetszőleges $a, b \in \mathbb{N}$ számokra*

$$\sqrt{a \cdot b} \ \in \ \Lambda\left(2, \max\left\{|a|, |b|\right\}\right) \tag{29}$$

Bizonyítás. Az $A := \begin{bmatrix} 0 & b \\ a & 0 \end{bmatrix}$ mátrix eleme $\mathcal{M}\left(2, \max\left\{|a|, |b|\right\}\right)$ -nak, karakterisztikus polinomja $kar_A(x) = \det(A - x \cdot E) = \det\begin{bmatrix} -x & b \\ a & -x \end{bmatrix} = x^2 - ab$, melynek gyökei $\pm\sqrt{a \cdot b}$, tehát valóban $\pm\sqrt{a \cdot b} \in \Lambda\left(2, \max\left\{|a|, |b|\right\}\right)$. ■

17. Megjegyzés. *$k = -1$ esetén a (28) polinomot x^n -el megszorozva ismét egy egész együtthatós polinomot kapunk, azonban a főegyüttható c_0 lesz, ami nem feltétlenül 1. Ez azt mutatja, hogy ha γ algebrai szám vagy akár algebrai egész ($\gamma \in \mathbb{A}_{\mathbb{Q}[x]}$ vagy $\gamma \in \mathbb{A}_{\mathbb{Z}[x]}$), akkor $\frac{1}{\gamma} \in \mathbb{A}_{\mathbb{Q}[x]}$ de* nem feltétlenül *$\frac{1}{\gamma} \in \mathbb{A}_{\mathbb{Z}[x]}$, és ugyanez igaz γ bármely* racionális *kitevőjű hatványára.*

4. Egy-két példa

Kezdjük régi ismerősünkkel:

$$\beta = \sqrt{2} + \sqrt{5 - 2\sqrt{6}} - \sqrt{3} \ \in \ \Lambda\left(?, ?\right) \tag{30}$$

A (15) tételt többször alkalmazzuk:

$2 \in \Lambda(1, 2)$, így $\sqrt{2} \in \Lambda(2, 2)$, hasonlóan $\sqrt{3} \in \Lambda(2, 3)$ és $\sqrt{6} \in \Lambda(2, 6)$, tehát $2\sqrt{6} \in \Lambda(2, 12)$ és $5 - 2\sqrt{6} \in \Lambda(2, 17)$ és $\sqrt{5 - 2\sqrt{6}} \in \Lambda(4, 17)$, végül

$$\beta \in \Lambda(2 \cdot 4 \cdot 2 \ , \ 2 + 17 + 3) = \Lambda(16, 22) \ . \tag{31}$$

Tehát a 14.Tétel (26) egyenlőtlensége alapján: ha $\beta \neq 0$, akkor

$$|\beta| \geq (16 \cdot 22)^{-15} \approx 6.3 * 10^{-39} \ , \tag{32}$$

vagyis $40-45$ (pontos) tizedesjegy már matematikailag is precízen dönti el a $\beta=0$ kérdést! (A számításokat az Olvasókra hagyjuk.)

A 16. állítást is felhasználva javíthatjuk a fenti becsléseket (a részletek házi feladat): $\beta\in\Lambda\,(16,16)$, ami által megkövetelt pontosság (32) helyett $|\beta|\geq(16\cdot 16)^{-15}\approx 7.5*10^{-37}$. Ha még azt is észrevesszük, hogy $5-2\sqrt{6}$ gyöke az $x^2-10x+1$ polinomnak (lásd az alábbi 18. állítást), akkor kapjuk, hogy $5-2\sqrt{6}\in\Lambda\,(2,10)$, amivel megint csökkenthetjük a megkövetelt pontosságot:

$$|\beta|\geq(16\cdot 15)^{-15}\approx 2*10^{-36}\ . \tag{33}$$

Gyakorlásképpen kiszámolhatjuk még, hogy például

$$\gamma:=\sqrt{7}\cdot\sqrt[3]{5-\sqrt{2}}\in\Lambda\,(12,49)\ . \tag{34}$$

A MATHEMATICA programcsomag "*Recognize*" parancsa bármilyen γ algebrai számhoz (gyökös kifejezéshez) megkeres egy egész együtthatójú polinomot, amelynek γ gyöke (a cikkünk elején ismertetett "gyök-eltüntető" számításhoz hasonlóan), persze nem mindig a legkisebb fokszámmal és a legkisebb abszolút értékű együtthatókkal. A legegyszerűbb esetre mi is találhatunk egy megfelelő ilyen polinomot:

18. Állítás. *Tetszőleges $a,b,c\in\mathbb{Z}$ egészszámok esetén a $\delta=a-b\sqrt{c}$ szám kielégíti a*

$$\delta^2-2a\delta+\left(a^2-b^2c\right)=0 \tag{35}$$

egyenletet.

Bizonyítás. $\delta-a=-b\sqrt{c}$ miatt $(\delta-a)^2=b^2c$, rendezés után (35) teljesül. ■

5. Alkalmazások

A számítógépek elterjedésével, a nagypontosságú közelítő számítások mindennapossá válásával egyidőben mind a matematikai, mind a mérnöki munkában szükséges nem csak a közelítés pontossága, hanem a tényleges matematikai egyenlőség kérdése is.

Elsősorban a kiszámítható geometriában (computable geometry) használják, aminek (számomra) legszebb példája Bozóki Sándor - Tsung-Lin Lee - Rónyai Lajos

[BLR 2015] cikke, amiben John Edensor Littlewood 1968-ban megjelent sejtését igazolták: lehetséges *hét* (elegendően hosszú) azonos átmérőjű hengert elhelyezni a térben úgy, hogy mindegyik érintse mindegyiket.

További alkalmazásokat és kutatásokat találunk még a [BFMS 1999], [LPT 1997], [L 1992a], [L 1992b], [L 1994], [S] és [Y] művekben, még komolyabb művek [HS 2012] és [S 1986], de ismételten kiemeljük, hogy a (jelenlegi) módszerek exponenciálisan ("rettenetesen") sok tizedes jegy pontosságot követelnek.

Lovász László [LL 1986] klasszikus művének 37-40. oldalain is foglalkozik az algebrai számok közelítésének problémájával.

Ingyenes programokat találunk a [BBBO] és [GMP] címeken.

6. Irodalom

[BBBO] **Batut,C., Belabas,K., Bernardi,D., Cohen,H., Olivier,M.:** *PARI-GP*, http://hasse.mathematik.tu-muenchen.de/ntsw/pari/Welcome

[BFMS 1999] **Burnikel,C., Fleischer,R., Mehlhorn,K., Schirra,S.:** *Efficient exact geometric computation made easy*, Proc. 15'th Annual Symp. Comp. Geom, ACM Press, 1999, 341-350.

[BLR 2015] **Bozóki Sándor, Tsung-Lin Lee, Rónyai Lajos:** *Seven mutually touching infinite cylinders*, Computational Geometry 48 (2015), 87 - 93.

[F 1996] **Fallat,S.:** *Algebraic integers and tensor products of matrices*, Crux. Math. 22 (1996), 341-343.

[GMP] GMP home page: http://www.gnu.org/software/gmp/gmp.html

[HS 2012] **Hauenstein,J.D., Sottile,F.:** *Algorithm 921: "alphaCertified", Certifying Solutions to Polynomial Systems*, ACM Trans. Math. Softw. 38, 4, Article 28 (August 2012), DOI = 10.1145/2331130.2331136 ,
http://doi.acm.org/10.1145/2331130.2331136

[m Ch] **Weisstein, Eric W:** *Characteristic Polynomial*, From MathWorld - A Wolfram Web Resource,
http://mathworld.wolfram.com/CharacteristicPolynomial.html

[m CM] **Rowland, Todd**: *Companion Matrix*, From MathWorld - A Wolfram Web Resource, created by Eric W. Weisstein,
http://mathworld.wolfram.com/CompanionMatrix.html

[m K] **Weisstein, Eric W.:** *Kronecker Product*, From MATHWORLD - A Wolfram Web Resource, http://mathworld.wolfram.com/KroneckerProduct.html

[L 1992a] **Landau,Susan:** *A note on Zipple denesting*, J.Symb.Comput. 13(1992), 41-45.

[L 1992b] **Landau,Susan:** *Simplification of nested radicals*, SIAM J.Comput. 21 (1992), 85-110.

[L 1994] **Landau,Susan:** *How to tangle with a nested radical*, Math. Intelligencer, 16 (1994), 49-55.

[LL 1986] **László Lovász:** *An Algorithmic Theory of Numbers*, SIAM 1986.

[LPT 1997] **Liotta,G., Preparata,F.P., Tamassia,R.:** *Robust proximity queries: An illustration of degree-driven algorithm design*, Proc. 13'th Annual Symp. comp. Geom., ACM Press, 1997, 156-165.

[S] **Seel,M.:** LEDA, http://www.mpi-sb.mpg.de/LEDA/

[S 1986] **Smale,S.:** *Newton's method estimates from data at one point*, in R.E. Ewing, K.I. Gross, C.F. Martin (Eds.): The Merging of Disciplines: New Directions in Pure, Applied, and Computational Mathematics, Springer, New York, 1986, pp. 185-196.

[SE 2000] **Edward R. Scheinerman:** *When close enough is close enough*, American Math. Monthly 2000, June-July, 489-499.

[w A hu] **Wikipédia:** *Algebrai szám*, https://hu.wikipedia.org/wiki/Algebrai_szám

[w A en] **Wikipedia:** *Algebraic number*,
https://en.wikipedia.org/wiki/Algebraic_number

[w Ch en] **Wikipedia:** *Characteristic_polynomial*,
https://en.wikipedia.org/wiki/Characteristic_polynomial

[w CM en] **Wikipedia:** *Companion matrix*,
https://en.wikipedia.org/wiki/Companion_matrix

[w K hu] **Wikipédia:** *Kronecker szorzat*,
https://hu.wikipedia.org/wiki/Kronecker-szorzat

[w K en] **Wikipedia:** *Kronecker product*,
https://en.wikipedia.org/wiki/Kronecker_product

[w S hu] **Wikipédia:** *Sajátvektor_és_sajátérték*,
https://hu.wikipedia.org/wiki/Sajátvektor_és_sajátérték

[w S en] **Wikipedia:** *Eigenvalues and Eigenvectors,*
https://en.wikipedia.org/wiki/Eigenvalues_and_eigenvectors

[17] [Y] **Yap,C.:** *Exact geometric computation* page: http://cs.nyu.edu/exact/

7. Függelék

A 15.Tétel **v)** és **vi)** pontjainak bizonyítása.

19. Definíció. *Az* $A = [a_{i,j}] \in \mathbb{R}^{m\times n}$ *és* $B \in \mathbb{R}^{k\times \ell}$ *mátrixok* ***Kronecker (tenzor) szorzata*** *([m K], [w K hu])*

$$A \otimes B := \begin{bmatrix} a_{1,1}B & a_{1,2}B & ... & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & ... & a_{2,n}B \\ ... & ... & ... & ... \\ a_{m,1}B & a_{m,2}B & ... & a_{m,n}B \end{bmatrix} \in \mathbb{R}^{mk\times n\ell} \ . \quad \square \tag{36}$$

Könnyen ellenőrizhető, hogy $\mathbf{v} \in \mathbb{R}^n$ és $\mathbf{w} \in \mathbb{R}^\ell$ esetén

$$(A \otimes B)(\mathbf{v} \otimes \mathbf{w}) = (A\mathbf{v}) \otimes (B\mathbf{w}) \ . \tag{37}$$

Legyen $\alpha \in \Lambda(n_1, b_1)$ és $\beta \in \Lambda(n_2, b_2)$, azaz $A\mathbf{v} = \alpha\mathbf{v}$ és $B\mathbf{w} = \beta\mathbf{w}$ (és $A \in \mathcal{M}(n_1, b_1)$, $B \in \mathcal{M}(n_2, b_2)$).

v) (37) alapján

$$(A \otimes B)(\mathbf{v} \otimes \mathbf{w}) = (A\mathbf{v}) \otimes (B\mathbf{w}) = \alpha\mathbf{v} \otimes \beta\mathbf{w} = \alpha\beta(\mathbf{v} \otimes \mathbf{w}) \tag{38}$$

vagyis $\alpha\beta \in \Lambda(n_1n_2, b_1b_2)$.

vi) Legyen

$$C := A \otimes E_{n_2} + E_{n_1} \otimes B \tag{39}$$

ahol $E_{n_1} \in \mathbb{R}^{n_1\times n_1}$ és $E_{n_2} \in \mathbb{R}^{n_2\times n_2}$ egységmátrixok, tehát $C \in \mathcal{M}(n_1n_2, b_1 + b_2)$. Ekkor

$$C(\mathbf{v} \otimes \mathbf{w}) = (A\mathbf{v})\otimes\mathbf{w} + \mathbf{v}\otimes(B\mathbf{w}) = \alpha(\mathbf{v} \otimes \mathbf{w}) + \beta(\mathbf{v} \otimes \mathbf{w}) = (\alpha + \beta)(\mathbf{v} \otimes \mathbf{w}) \tag{40}$$

vagyis $\alpha\beta \in \Lambda(n_1n_2, b_1 + b_2)$.

$\square$