Testbővítések, algebrai számok

A négyelemű test

A $K := \mathbb{Z}_2[x]/(x^2+x+1)$ mardékosztály-gyűrű test, mert $m = x^2+x+1$ irreducibilis $\mathbb{Z}_2$ felett.
Ennek a testnek négy eleme van: $\mathbb{Z}_2[x]/(x^2+x+1) = \{\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1}\}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Ugyanez tömörebben, a $0 := \overline{0}$, $1 := \overline{1}$, $\alpha := \overline{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

A négyelemű test

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Figyeljük meg, hogy

- $\{0,1\} = \{\overline{0},\overline{1}\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban, tehát kis jóindulattal mondhatjuk, hogy $\mathbb{Z}_2 \subseteq K$, vagyis K kibővítése $\mathbb{Z}_2$-nek;
- $\alpha = \overline{x}$ gyöke az $m = x^2 + x + 1 \in K[x]$ polinomnak:
  $\alpha^2 + \alpha + 1 = \overline{x}^2 + \overline{x} + \overline{1} = \overline{x^2 + x + 1} = \overline{m} = \overline{0} = 0.$

Ez azt jelenti, hogy a K testben már van gyöke az $m = x^2 + x + 1$ polinomnak!

A nyolcelemű test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / (x^3 + x + 1)$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Vezessük be az $\alpha = \overline{x}$ jelölést, és hagyjuk el a vonásokat a konstansokról. Ezzel a jelöléssel a K test 8 eleme:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Figyeljük meg, hogy $\{0,1\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban, tehát $\mathbb{Z}_2 \subseteq K$, vagyis K bővítése $\mathbb{Z}_2$-nek.

Számítsuk ki $m(\alpha)$ értékét:

$$m(\alpha) = \alpha^3 + \alpha + 1 = \overline{x}^3 + \overline{x} + \overline{1} = \overline{x^3 + x + 1} = \overline{m} = \overline{0}.$$

Tehát a K testben már van gyöke az $m = x^3 + x + 1$ polinomnak.

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ faktorgyűrű olyan testbővítése T-nek, amelyben az m polinomnak van gyöke (pl. $\alpha = \overline{x}$). A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$. Ezzel a számolási szabállyal már bármit ki tudunk számolni a K testben.

(És ha m nem irreducibilis?)

A komplex számtest újratöltve

Készítsük el a $K = T[x]/(m)$ testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetben.
Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha \quad (a_0, a_1 \in \mathbb{R}).$$

Az α szimbólumra vonatkozó számolási szabály: $m(\alpha) = \alpha^2 + 1 = 0$, vagyis

$$\alpha^2 = -1.$$

Ezzel éppen a komplex számok testét kaptuk (csak α helyett i a szokásos jelölés).

Tehát $\mathbb{C} \cong \mathbb{R}[x]/\left(x^2 + 1\right)$, és ezt tekinthetnénk akár a komplex számok definíciójának is.

Véges testek

Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

A q-elemű testet (mely izomorfia erejéig egyértelműen meghatározott), Galois tiszteletére $\mathrm{GF}(q)$ jelöli (Galois Field).

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / (x^2 + x + 1)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test: $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test: $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] / (x^3 + x + 1) \cong \mathbb{Z}_2[x] / (x^3 + x^2 + 1)$
- kilencelemű test: $\mathrm{GF}(9) \cong \mathbb{Z}_3[x] / (x^2 + 1) = \{a + bi : a, b \in \mathbb{Z}_3\}$
- tízelemű test: nincs!

Egy végtelen maradékosztálytest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}$$

Tehát $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyöktelenníteni.

Megoldóképlet

Legyen $\alpha \in \mathbb{C}$ egy megoldása az $x^5 - 4x + 2 = 0$ egyenletnek.
Ha van megoldóképlete az ötödfokú egyenletnek, akkor azt erre az egyenletre alkalmazva megkapjuk az α számot valami olyan képlettel, amely racionális számokból épül fel a négy alapművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával, pl.

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

Hogy van-e ilyen képlet, annak eldöntésére használhatók a testbővítések: a racionális számok testét lépésenként bővítjük a képletben szereplő gyökökkel:

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2014}\right) \subset \mathbb{Q}\left(\sqrt{2014}\right)\left(\sqrt[17]{323 - \sqrt{2014}}\right) \subset \cdots$$

A cél az, hogy véges sok lépésben eljussunk egy olyan **radikálbővítéshez**, ami már tartalmazza az α számot.

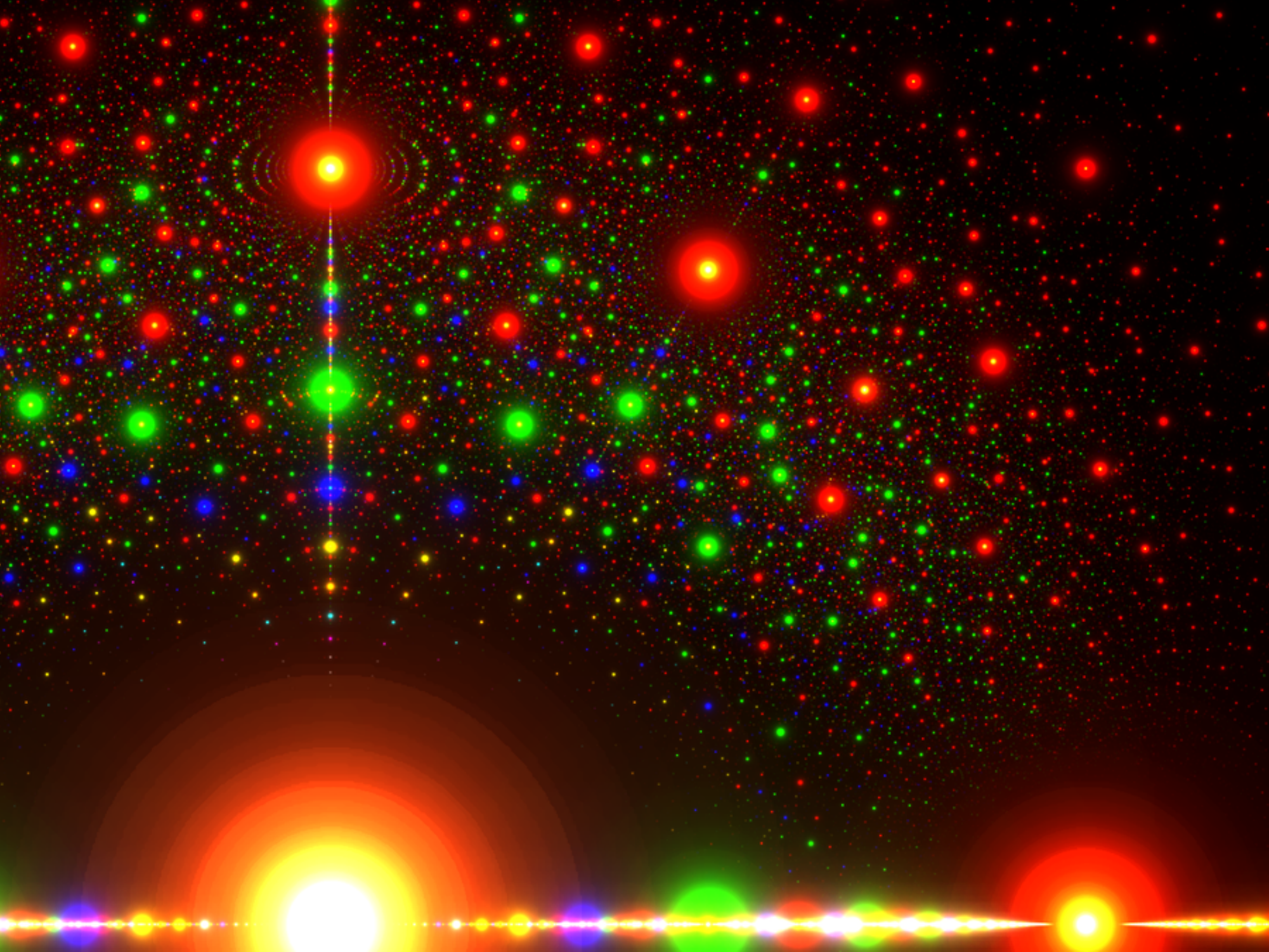
Algebrai számok és gyökmennyiségek

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.
- Az α komplex számot **algebrai számnak** nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak.
- A legkisebb fokszámú ilyen polinomot (asszociáltság erejéig egyértelmű) az α algebrai szám **minimálpolinomjának** nevezzük.
- A nem algebrai számokat **transzcendens számoknak** nevezzük.

Tétel.

Minden gyökmennyiség algebrai szám, de van olyan algebrai szám, ami nem gyökmennyiség.



Algebrai és transzcendens számok

Tétel.

Létezik transzcendens szám.

Példa.

- $\sqrt{2}$ algebrai szám, minimálpolinomja: $x^2 - 2$.
- $\sqrt[n]{2}$ algebrai szám, minimálpolinomja: $x^n - 2$.
- i algebrai szám, minimálpolinomja: $x^2 + 1$.
- π és e transzcendens számok.
- A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- Gelfond–Schneider-tétel: Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám.

  Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $i^i = e^{-\pi/2}$ transzcendens számok.

Diofantoszi approximáció

Megjegyzés.

A transzcendenciabizonyítások egy fontos eszköze, az a megfigyelés, hogy algebrai számokat nem lehet nagyon jól közelíteni racionális számokkal. Ez a **diofantoszi approximáció** témaköre: adott α valós számhoz szeretnénk olyan $\frac{p}{q}$ közelítő törtet találni ($p, q \in \mathbb{Z}, q > 0, p \perp q$), amelyre $\left|\alpha - \frac{p}{q}\right|$ kicsi, és q nem túl nagy.

Tétel (Dirichlet approximációs tétele).

Minden α valós szám és minden N természetes szám esetén van α-nak olyan $\frac{p}{q}$ közelítése, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq} \quad \text{és} \quad q \leq N.$$

Következmény.

Ha $\alpha \notin \mathbb{Q}$, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Állítás.

Ha $\alpha \in \mathbb{Q}$, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Diofantoszi approximáció

Tétel (Hurwitz tétele).

Ha α irracionális szám, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Ha $\alpha = \frac{1+\sqrt{5}}{2}$, akkor az állítás nem javítható: nem írhatunk a nevezőbe semmilyen $\sqrt{5}$-nél nagyobb számot.

Tétel (Liouville, Thue, Siegel, Roth).

Ha α irracionális algebrai szám és $\varepsilon > 0$, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$