Magasabbfokú egyenletek és geometriai szerkeszthetőség

Dormán Miklós

SZTE, Bolyai Intézet

2008. november 7.

Magasabb fokú egyenletek és geometriai szerkeszthetőség

1. ábra: Carl Friedrich Gauss (1777-1855).

Magasabb fokú egyenletek és geometriai szerkeszthetőség

2. ábra: Niels Henrik Abel (1802-1829).

Magasabb fokú egyenletek és geometriai szerkeszthetőség

3. ábra: Évariste Galois (1811-1832).

Tétel (L. Kronecker).

Tetszőleges egész együtthatós polinom véges sok lépésben felbontható $\mathbb{Z}$ felett irreducibilis polinomok szorzatára.

Tétel (L. Kronecker).

Tetszőleges egész együtthatós polinom véges sok lépésben felbontható $\mathbb{Z}$ felett irreducibilis polinomok szorzatára.

Definíció: primitív polinom.

Legyen D integritástartomány, valamint $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ tetszőleges polinom. Azt mondjuk, hogy az f polinom **primitív**, ha az $a_0, \ldots, a_n$ együtthatók relatív prímek.

Tétel (L. Kronecker).

Tetszőleges egész együtthatós polinom véges sok lépésben felbontható $\mathbb{Z}$ felett irreducibilis polinomok szorzatára.

Definíció: primitív polinom.

Legyen D integritástartomány, valamint $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ tetszőleges polinom. Azt mondjuk, hogy az f polinom **primitív**, ha az $a_0, \ldots, a_n$ együtthatók relatív prímek.

Tétel (C. F. Gauss).

Legyen f legalább elsőfokú, egész együtthatós primitív polinom. Az f polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha irreducibilis $\mathbb{Q}$ felett.

Tétel (Schönemann–Eisenstein-tétel).

Legyen

$$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

legalább elsőfokú primitív polinom. Ha létezik olyan p prímszám, amelyre $p \mid a_0, \ldots, a_{n-1}$, de $p \nmid a_n$ és $p^2 \nmid a_0$, akkor f irreducibilis $\mathbb{Z}$ felett.

Tétel (Schönemann–Eisenstein-tétel).

Legyen

$$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

legalább elsőfokú primitív polinom. Ha létezik olyan p prímszám, amelyre $p \mid a_0, \ldots, a_{n-1}$, de $p \nmid a_n$ és $p^2 \nmid a_0$, akkor f irreducibilis $\mathbb{Z}$ felett.

Definíció: polinom eltoltja.

Számos esetben jól alkalmazható tesztet kapunk, ha nem csak az f polinomot, de annak az "eltoltjait" is vizsgáljuk. Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ekkor tetszőleges s egész számra az $f_{\to s} = a_n(x-s)^n + \cdots + a_1(x-s) + a_0$ polinomot az f polinom s-**eltoltjának** nevezzük.

Tétel.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, és $s \in \mathbb{Z}$. Ekkor az f polinom pontosan akkor irreducibilis $\mathbb{Z}$ felett, ha $f_{\to s}$ az.

Tétel.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, és $s \in \mathbb{Z}$. Ekkor az f polinom pontosan akkor irreducibilis $\mathbb{Z}$ felett, ha $f_{\to s}$ az.

Példa.

Tekintsük az $f = x^5 - 7x^4 + 24x^3 - 42x^2 + 39x - 25 \in \mathbb{Z}[x]$ polinomot. Erre a polinomra nem alkalmazható a Schönemann–Eisenstein-tétel. Tekintsük azonban az

$$f_{\to -1} = x^5 - 2x^4 + 6x^3 - 2x^2 + 4x - 10$$

polinomot. Ez a polinom primitív, és a Schönemann–Eisenstein-tételt a $p = 2$ választással alkalmazva kapjuk, hogy irreducibilis. Így a polinom eltoltjára vonatkozó tétel szerint az f polinom is irreducibilis.

A megfelelő eltolt megtalálása azonban nem egyszerű feladat, sőt nem is mindig létezik megfelelő eltolt.

A megfelelő eltolt megtalálása azonban nem egyszerű feladat, sőt nem is mindig létezik megfelelő eltolt.

Tétel (Rolle-tétel).

Legyen $f \in \mathbb{Z}[x]$ tetszőleges polinom. Ha $\frac{p}{q} \in \mathbb{Q}$ tört, ahol $\mathrm{ln.k.o.}(p, q) = 1$, gyöke f-nek, akkor bármely m egész számra $p + mq \mid f(-m)$.

A megfelelő eltolt megtalálása azonban nem egyszerű feladat, sőt nem is mindig létezik megfelelő eltolt.

Tétel (Rolle-tétel).

Legyen $f \in \mathbb{Z}[x]$ tetszőleges polinom. Ha $\frac{p}{q} \in \mathbb{Q}$ tört, ahol $\mathrm{ln.k.o.}(p, q) = 1$, gyöke f-nek, akkor bármely m egész számra $p + mq \mid f(-m)$.

Tétel.

Legyen K test, és $f \in K[x]$ másod- vagy harmadfokú polinom. Ekkor f pontosan akkor irreducibilis K felett, ha nincs gyöke K-ban.

Tétel.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ olyan egész együtthatós primitív polinom. Legyen p olyan prímszám, amely nem osztja a_n-et. Ha $\overline{f} = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}_p[x]$ irreducibilis $\mathbb{Z}_p$ felett, akkor f irreducibilis $\mathbb{Z}$ felett.

Definíció: (test)bővítés.

Legyenek K és L testek. Ha K résztestе L-nek, akkor azt mondjuk, hogy L **(test)bővítése** K-nak, és ezt az $L|K$ szimbólummal jelöljük.

Definíció: (test)bővítés.

Legyenek K és L testek. Ha K résztteste L-nek, akkor azt mondjuk, hogy L **(test)bővítése** K-nak, és ezt az $L|K$ szimbólummal jelöljük.

Tétel.

Ha az L test bővítése a K testnek, akkor L vektortér a K test felett az

$$\oplus\colon L \times L \to L,\ u \oplus v = u + v,$$
$$f_\lambda\colon L \to L,\ uf_\lambda = \lambda u\ (\lambda \in K)$$

műveletekkel.

Példa.

A $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ halmaz számtestet alkot. A $\mathbb{Q}(\sqrt{2})$, mint $\mathbb{Q}$ feletti vektortér 2-dimenziós, melyenk az $1, \sqrt{2}$ elemek bázisát alkotják.

Definíció: testbővítés foka.

Az előző tételt fogjuk felhasználni a testbővítés fokának a definiálására. Az $L|K$ bővítés $[L : K]$ **foka** az L testnek, mint K feletti vektortérnek a dimenziója, azaz $[L : K] = \dim_K L$. Ha $[L : K] < \infty$, akkor azt mondjuk, hogy az $L|K$ bővítés **véges (dimenziós)**, különben $L|K$ **végtelen (dimenziós)**.

Definíció: testbővítés foka.

Az előző tételt fogjuk felhasználni a testbővítés fokának a definiálására. Az $L|K$ bővítés $[L:K]$ **foka** az L testnek, mint K feletti vektortérnek a dimenziója, azaz $[L:K] = \dim_K L$. Ha $[L:K] < \infty$, akkor azt mondjuk, hogy az $L|K$ bővítés **véges (dimenziós)**, különben $L|K$ **végtelen (dimenziós)**.

Példák.

A $\mathbb{C}|\mathbb{R}$ bővítés 2-fokú, mivel $\mathbb{C}$ 2-dimenziós vektortér $\mathbb{R}$ felett; az $1, i \in \mathbb{C}$ vektorok bázist alkotnak. A $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ bővítés szintén 2-fokú. Azonban a $\mathbb{C}|\mathbb{Q}$ és $\mathbb{R}|\mathbb{Q}$ bővítések végtelenek.

Tétel (Fokszámtétel).

Legyenek K, L, M olyan testek, amelyekre $L|K$, $M|L$ teljesül.

Tétel (Fokszámtétel).

Legyenek K, L, M olyan testek, amelyekre $L|K$, $M|L$ teljesül.

(a) Ha az $L|K$ és $M|L$ bővítések valamelyike végtelen, akkor $M|K$ is az.

Tétel (Fokszámtétel).

Legyenek K, L, M olyan testek, amelyekre $L|K$, $M|L$ teljesül.

(a) Ha az $L|K$ és $M|L$ bővítések valamelyike végtelen, akkor $M|K$ is az.

(b) Ha az $L|K$ és $M|L$ bővítések végesek, akkor az $M|K$ bővítés is az, és fennáll az
$$[M : K] = [M : L] \cdot [L : K]$$
egyenlőség.

A Fokszámtétel bizonyítása.

(a) Az állítást kontrapozicióval igazoljuk. Tegyük fel, hogy $M|K$ véges, $[M:K]=n\in\mathbb{N}$. Megmutatjuk, hogy ekkor $[L:K],[M:L]\leqslant n$ teljesül. Legyenek $\lambda_1,\dots,\lambda_{n+1}$, illetve $\mu_1,\dots,\mu_{n+1}$ tetszőleges vektorrendszerek L-ben, illetve M-ben. Mivel az M vektortér n dimenziós K felett, és a $\lambda_1,\dots,\lambda_{n+1}$, illetve $\mu_1,\dots,\mu_{n+1}$ vektorok M-beliek, ezért vannak olyan $a_1,\dots,a_{n+1}$, valamint $b_1,\dots,b_{n+1}$ K-beli skalárok, amelyekre $(a_1,\dots,a_{n+1})\neq\mathbf{0}$ és $(b_1,\dots,b_{n+1})\neq\mathbf{0}$ teljesül és

$$a_1\lambda_1+\cdots+a_{n+1}\lambda_{n+1}=0, \qquad b_1\mu_1+\cdots+b_{n+1}\mu_{n+1}=0.$$

Ez pedig éppen azt bizonyítja, hogy a $\lambda_1,\dots,\lambda_{n+1}$ vektorok lineárisan függők az L (mint K feletti) vektortérben, illetve a $\mu_1,\dots,\mu_{n+1}$ vektorok lineárisan függők az M (mint L feletti) vektortérben.

A Fokszámtétel bizonyítása (folytatás).

(b) Legyen $[L : K] = m$ és $[M : L] = n$. Válasszunk az L, illetve M vektorterekben bázist:

$$\lambda_1, \dots, \lambda_m \quad \text{bázis } L\text{-ben, mint } K \text{ feletti vektortérben,} \tag{1}$$

$$\mu_1, \dots, \mu_n \quad \text{bázis } M\text{-ben, mint } L \text{ feletti vektortérben.} \tag{2}$$

Megmutatjuk, hogy a $\mu_i\lambda_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ vektorrendszer bázis M-ben, mint K feletti vektortérben. Legyen μ tetszőleges M-beli vektor. Ekkor (2) miatt vannak olyan $b_1, \dots, b_n \in L$ elemek, amelyekre

$$\mu = b_1\mu_1 + \dots + b_n\mu_n.$$

A Fokszámtétel bizonyítása (folytatás).

Mivel $b_1, \ldots, b_n \in L$, ezért (1) miatt vannak olyan $a_{i,j} \in K$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ elemek, amelyekre

$$b_i = a_{i,1}\lambda_1 + \cdots + a_{i,m}\lambda_m \quad (1 \leqslant i \leqslant n)$$

teljesül. Így

$$\mu = \sum_{i=1}^{n} b_i\mu_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{i,j}\lambda_j\right)\mu_i = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\lambda_j\mu_i,$$

azaz a $\mu_i\lambda_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ vektorrendszer generátorrendszer.

A Fokszámtétel bizonyítása (folytatás).

Tegyük fel, hogy

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\lambda_j\mu_i = 0.$$

Ekkor

$$0 = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\lambda_j\mu_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} a_{i,j}\lambda_j\right)\mu_i$$

és (2) miatt $\sum_{j=1}^{m} a_{i,j}\lambda_j = 0$ $(1 \leqslant i \leqslant n)$. Ekkor (1)-et ismét felhasználva azt kapjuk, hogy $a_{i,j} = 0$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$, azaz a $\mu_i\lambda_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ vektorrendszer lineárisan független, így bázisa az M, mint K feletti vektortérnek.

A Fokszámtétel bizonyítása (folytatás).

Mindezeket figyelembevéve azt kapjuk, hogy

$$[L:K]\cdot[M:L]=m\cdot n=\dim_K M=[M:L].$$

Ezzel az állítást igazoltuk.

A Fokszámtétel bizonyítása (folytatás).

Mindezeket figyelembevéve azt kapjuk, hogy

$$[L : K] \cdot [M : L] = m \cdot n = \dim_K M = [M : L].$$

Ezzel az állítást igazoltuk.

Tétel.

A Fokszámtétel állítása teljes indukcióval egyszerűen kiterjeszthető bővítések egymásutánjaira is: ha $K_i : K_{i-1}$ teljesül tetszőleges i-re ($n \in \mathbb{N}$, $1 \leqslant i \leqslant n$), akkor

$$[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1 : K_0].$$

Definíció: generált résztest, egyszerű bővítés.

Legyen L a K test bővítése, és legyen $A \subseteq L$. Ekkor $K(A)$-val jelöljük, és a $K \cup A$ részhalmaz által **generált résztestnek** nevezzük az L test $K \cup A$ részhalmazát tartalmazó legszűkebb résztestét, és azt mondjuk, hogy a $K(A)|K$ bővítés K-nak az A részhalmaz által generált bővítése. Ha A véges részhalmaza L-nek, pl. $A = \{\alpha_1, \dots, \alpha_n\}$, akkor $K(A)$ helyett $K(\alpha_1, \dots, \alpha_n)$-et írunk. Azt mondjuk, hogy az $L|K$ bővítés **egyszerű**, ha van olyan $\alpha \in L$, amelyre $L = K(\alpha)$.

Definíció: generált résztest, egyszerű bővítés.

Legyen L a K test bővítése, és legyen $A \subseteq L$. Ekkor $K(A)$-val jelöljük, és a $K \cup A$ részhalmaz által **generált résztestnek** nevezzük az L test $K \cup A$ részhalmazát tartalmazó legszűkebb résztestét, és azt mondjuk, hogy a $K(A)|K$ bővítés K-nak az A részhalmaz által generált bővítése. Ha A véges részhalmaza L-nek, pl. $A = \{\alpha_1, \ldots, \alpha_n\}$, akkor $K(A)$ helyett $K(\alpha_1, \ldots, \alpha_n)$-et írunk. Azt mondjuk, hogy az $L|K$ bővítés **egyszerű**, ha van olyan $\alpha \in L$, amelyre $L = K(\alpha)$.

Példa.

A $\mathbb{C}|\mathbb{R}$ bővítés egyszerű, mivel $\mathbb{C} = \mathbb{R}(i)$.

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítést.

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítést.

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítést. Mivel $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$,

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítést. Mivel $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, ezért $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítést. Mivel $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, ezért $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Másrészt, az

$$\sqrt{2} = \frac{1}{2} \cdot ((\sqrt{2} + \sqrt{3})^3 - 9 \cdot (\sqrt{2} + \sqrt{3})),$$
$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2}$$

egyenlőségek következtében

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$ bővítést. Mivel $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, ezért $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$. Másrészt, az

$$\sqrt{2}=\frac{1}{2}\cdot\left((\sqrt{2}+\sqrt{3})^3-9\cdot(\sqrt{2}+\sqrt{3})\right),$$
$$\sqrt{3}=(\sqrt{2}+\sqrt{3})-\sqrt{2}$$

egyenlőségek következtében $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$,

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$ bővítést. Mivel $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, ezért $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$. Másrészt, az

$$\sqrt{2}=\frac{1}{2}\cdot\left((\sqrt{2}+\sqrt{3})^3-9\cdot(\sqrt{2}+\sqrt{3})\right),$$
$$\sqrt{3}=(\sqrt{2}+\sqrt{3})-\sqrt{2}$$

egyenlőségek következtében $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$, azaz $\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Példa.

Tekintsük a $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$ bővítést. Mivel $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, ezért $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$. Másrészt, az

$$\sqrt{2}=\frac{1}{2}\cdot\left((\sqrt{2}+\sqrt{3})^3-9\cdot(\sqrt{2}+\sqrt{3})\right),$$
$$\sqrt{3}=(\sqrt{2}+\sqrt{3})-\sqrt{2}$$

egyenlőségek következtében $\sqrt{2},\sqrt{3}\in\mathbb{Q}(\sqrt{2}+\sqrt{3})$, azaz $\mathbb{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Így azt kapjuk, hogy $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$, azaz a $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$ bővítés egyszerű.

Tétel.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint legyen $\alpha_1, \ldots, \alpha_n \in L$. Ekkor

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

Tétel.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint legyen $\alpha_1, \ldots, \alpha_n \in L$. Ekkor

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

Tegyük fel, hogy $L|K$ teljesül, és legyen $\alpha \in L$. Ekkor két eset lehetséges:

Tétel.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint legyen $\alpha_1, \ldots, \alpha_n \in L$. Ekkor

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

Tegyük fel, hogy $L|K$ teljesül, és legyen $\alpha \in L$. Ekkor két eset lehetséges:

- Van olyan $f \in K[x] \setminus \{0\}$ polinom, amelynek α gyöke, azaz $f(\alpha) = 0$. Ekkor azt mondjuk, hogy az α elem **algebrai elem a K test felett.**

Tétel.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint legyen $\alpha_1, \ldots, \alpha_n \in L$. Ekkor

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

Tegyük fel, hogy $L|K$ teljesül, és legyen $\alpha \in L$. Ekkor két eset lehetséges:

- Van olyan $f \in K[x] \setminus \{0\}$ polinom, amelynek α gyöke, azaz $f(\alpha) = 0$. Ekkor azt mondjuk, hogy az α elem **algebrai elem a K test felett.**
- Nincs olyan $f \in K[x] \setminus \{0\}$ polinom, amelynek α gyöke. Ebben az esetben azt mondjuk, hogy az α elem **transzcendens elem a K test felett.**

Valós transzcendens elemek $\mathbb{Q}$ felett.

Valós transzcendens elemek $\mathbb{Q}$ felett.

- **1844** Joseph **Liouville** megmutatja, hogy bizonyos valós számok, amelyeket ma Liouville-számoknak nevezünk, transzcendensek $\mathbb{Q}$ felett. Ilyan szám pl.: $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$.

Valós transzcendens elemek $\mathbb{Q}$ felett.

- **1844** Joseph **Liouville** megmutatja, hogy bizonyos valós számok, amelyeket ma Liouville-számoknak nevezünk, transzcendensek $\mathbb{Q}$ felett. Ilyan szám pl.: $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$.
- **1873** Charles **Hermite** megmutatja, hogy az e szám transzcendens.

Valós transzcendens elemek $\mathbb{Q}$ felett.

- **1844** Joseph **Liouville** megmutatja, hogy bizonyos valós számok, amelyeket ma Liouville-számoknak nevezünk, transzcendensek $\mathbb{Q}$ felett. Ilyan szám pl.: $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$.
- **1873** Charles **Hermite** megmutatja, hogy az e szám transzcendens.
- **1874** George Ferdinand Ludwig **Cantor** bebizonyítja, hogy azon valós számok halmazának számossága, amelyek algebraiak $\mathbb{Q}$ felett megszámlálhatóan végtelen. Mivel a valós számok halmaza nem megszámlálható, ezért a valós számok többsége transzcendens $\mathbb{Q}$ felett.

Valós transzcendens elemek $\mathbb{Q}$ felett.

- **1844** Joseph **Liouville** megmutatja, hogy bizonyos valós számok, amelyeket ma Liouville-számoknak nevezünk, transzcendensek $\mathbb{Q}$ felett. Ilyan szám pl.: $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$.
- **1873** Charles **Hermite** megmutatja, hogy az e szám transzcendens.
- **1874** George Ferdinand Ludwig **Cantor** bebizonyítja, hogy azon valós számok halmazának számossága, amelyek algebraiak $\mathbb{Q}$ felett megszámlálhatóan végtelen. Mivel a valós számok halmaza nem megszámlálható, ezért a valós számok többsége transzcendens $\mathbb{Q}$ felett.
- **1882** Ferdinand **Lindemann** igazolja, hogy a π szám transzcendens $\mathbb{Q}$ felett.

Valós transzcendens elemek $\mathbb{Q}$ felett (folytatás).

Valós transzcendens elemek $\mathbb{Q}$ felett (folytatás).

- **1934** A.J. **Gelfond** igazolja, hogy ha $\alpha, \beta \in \mathbb{R}$ olyan algebrai elemek $\mathbb{Q}$ felett, amelyekre $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ teljesül, akkor az α^β valós szám transzcendens $\mathbb{Q}$ felett. (Pl.: $2^{\sqrt{2}}$ transzcendens $\mathbb{Q}$ felett.)

Valós transzcendens elemek $\mathbb{Q}$ felett (folytatás).

- **1934** A.J. **Gelfond** igazolja, hogy ha $\alpha, \beta \in \mathbb{R}$ olyan algebrai elemek $\mathbb{Q}$ felett, amelyekre $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ teljesül, akkor az α^β valós szám transzcendens $\mathbb{Q}$ felett. (Pl.: $2^{\sqrt{2}}$ transzcendens $\mathbb{Q}$ felett.)

Problémák.

Valós transzcendens elemek $\mathbb{Q}$ felett (folytatás).

- **1934** A.J. **Gelfond** igazolja, hogy ha $\alpha, \beta \in \mathbb{R}$ olyan algebrai elemek $\mathbb{Q}$ felett, amelyekre $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ teljesül, akkor az α^β valós szám transzcendens $\mathbb{Q}$ felett. (Pl.: $2^{\sqrt{2}}$ transzcendens $\mathbb{Q}$ felett.)

Problémák.

- Igaz-e, hogy $e + \pi$ transzcendens $\mathbb{Q}$ felett?

Valós transzcendens elemek $\mathbb{Q}$ felett (folytatás).

- **1934** A.J. **Gelfond** igazolja, hogy ha $\alpha, \beta \in \mathbb{R}$ olyan algebrai elemek $\mathbb{Q}$ felett, amelyekre $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ teljesül, akkor az α^{β} valós szám transzcendens $\mathbb{Q}$ felett. (Pl.: $2^{\sqrt{2}}$ transzcendens $\mathbb{Q}$ felett.)

Problémák.

- Igaz-e, hogy $e + \pi$ transzcendens $\mathbb{Q}$ felett?
- Igaz-e, hogy a $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right) \approx 0.5772156649015328606065120\,9$ transzcendens $\mathbb{Q}$ felett?

Tétel.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül. Legyen $\alpha \in L$, valamint ε_α a következő leképezés:

$$\varepsilon_\alpha\colon K[x] \to K(\alpha),\ f \mapsto f(\alpha).$$

Ekkor az alábbi két állítás közül pontosan az egyik teljesül.

Tétel (folytatás).

Tétel (folytatás).

(a) Az ε_α leképezés injektív homomorfizmus, és ε_α-t kiterjesztve $K[x]$ hányadostestére, a kapott $\widetilde{\varepsilon_\alpha}\colon K(x) \to K(\alpha)$ leképezés izomorfizmus. Ekkor a $K(\alpha)|K$ bővítés végtelen, és az α elem transzcendens K felett.

Tétel (folytatás).

(a) Az ε_α leképezés injektív homomorfizmus, és ε_α-t kiterjesztve $K[x]$ hányadostestére, a kapott $\widetilde{\varepsilon_\alpha}\colon K(x) \to K(\alpha)$ leképezés izomorfizmus. Ekkor a $K(\alpha)|K$ bővítés végtelen, és az α elem transzcendens K felett.

(b) Az ε_α leképezés homomorfizmus, amely nem injektív, így magja $\ker(\varepsilon_\alpha) \neq \{0\}$. Ekkor $\ker(\varepsilon_\alpha) = (m_{\alpha,K})$ teljesül valamely (egyért. meghat.) $m_{\alpha,K} \in K[x]$ irreducibilis főpolinomra, és az $\widehat{\varepsilon_\alpha}\colon K[x]/(m_{\alpha,K}) \to K(\alpha)$ homomorfizmus izomorfizmus. Ekkor $K(\alpha)|K$ véges, és az α elem algebrai K felett.

Definíció: minimálpolinom, algebrai elem foka.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint $\alpha \in L$ algebrai elem K felett. Ekkor az előző tétel (b) részében kapott $m_{\alpha,K}$ polinomot az α elem **minimálpolinomjának** nevezzük. Az α **algebrai elem foka** minimálpolinomjának a foka, amit $\mathrm{gr}_K(\alpha)$-val jelölünk.

Definíció: minimálpolinom, algebrai elem foka.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint $\alpha \in L$ algebrai elem K felett. Ekkor az előző tétel (b) részében kapott $m_{\alpha,K}$ polinomot az α elem **minimálpolinomjának** nevezzük. Az α **algebrai elem foka** minimálpolinomjának a foka, amit $\mathrm{gr}_K(\alpha)$-val jelölünk.

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$ algebrai elem K felett, melynek minmálpolinomja f. Ekkor tetszőleges $g \in K[x]$, $g \neq 0$ polinomra $g(\alpha) = 0$ pontosan akkor teljesül, ha $f \mid g$.

Példa.

Példa.

- $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2,$

Példa.

- $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2,$
- $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1,$

Példa.

- $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2,$
- $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1,$
- $m_{\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3},\mathbb{Q}} = x^2 + x + 1,$

Példa.

- $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$,
- $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1$,
- $m_{\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3},\mathbb{Q}} = x^2 + x + 1$,
- $m_{\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p},\mathbb{Q}} = x^{p-1} + \cdots + x + 1$ (p prímszám).

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$. Ekkor az α elem pontosan akkor algebrai K felett, ha $[K(\alpha) : K] < \infty$. Ha α algebrai elem K felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$. Ekkor az α elem pontosan akkor algebrai K felett, ha $[K(\alpha) : K] < \infty$. Ha α algebrai elem K felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Bizonyítás.

Tegyük fel, hogy a $K(\alpha)|K$ testbővítés véges, azaz $[K(\alpha) : K] = n$ teljesül valamely n természetes számra.

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$. Ekkor az α elem pontosan akkor algebrai K felett, ha $[K(\alpha) : K] < \infty$. Ha α algebrai elem K felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Bizonyítás.

Tegyük fel, hogy a $K(\alpha)|K$ testbővítés véges, azaz $[K(\alpha) : K] = n$ teljesül valamely n természetes számra.

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$. Ekkor az α elem pontosan akkor algebrai K felett, ha $[K(\alpha) : K] < \infty$. Ha α algebrai elem K felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Bizonyítás.

Tegyük fel, hogy a $K(\alpha)|K$ testbővítés véges, azaz $[K(\alpha) : K] = n$ teljesül valamely n természetes számra. Az $1, \alpha, \ldots, \alpha^n \in K(\alpha)$ vektorok lineárisan függő vektorrendszert alkotnak, mivel számuk $n + 1 > \dim_K K(\alpha) = n$.

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$. Ekkor az α elem pontosan akkor algebrai K felett, ha $[K(\alpha) : K] < \infty$. Ha α algebrai elem K felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Bizonyítás.

Tegyük fel, hogy a $K(\alpha)|K$ testbővítés véges, azaz $[K(\alpha) : K] = n$ teljesül valamely n természetes számra. Az $1, \alpha, \ldots, \alpha^n \in K(\alpha)$ vektorok lineárisan függő vektorrendszert alkotnak, mivel számuk $n + 1 > \dim_K K(\alpha) = n$. Így vannak olyan $a_0, \ldots, a_n \in K$ skalárok, amelyek nem mind 0-ák és amelyekre $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ teljesül.

Tétel.

Legyen $L|K$ testbővítés, és $\alpha \in L$. Ekkor az α elem pontosan akkor algebrai K felett, ha $[K(\alpha) : K] < \infty$. Ha α algebrai elem K felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Bizonyítás.

Tegyük fel, hogy a $K(\alpha)|K$ testbővítés véges, azaz $[K(\alpha) : K] = n$ teljesül valamely n természetes számra. Az $1, \alpha, \ldots, \alpha^n \in K(\alpha)$ vektorok lineárisan függő vektorrendszert alkotnak, mivel számuk $n + 1 > \dim_K K(\alpha) = n$. Így vannak olyan $a_0, \ldots, a_n \in K$ skalárok, amelyek nem mind 0-ák és amelyekre $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ teljesül. Ekkor α gyöke az $f = a_nx^n + \cdots + a_1x + a_0$ polinomnak. Mivel $f \neq 0$, ezért α algebrai elem K felett.

Bizonyítás (folytatás).

Tegyük fel, hogy α algebrai elem K felett. Ekkor az

$$\widehat{\varepsilon_\alpha}\colon K[x]/(m_{\alpha,K}) \to K(\alpha),\ f + (m_{\alpha,K}) \mapsto f(\alpha)$$

homomorfizmus izomorfizmus. Mivel tetszőleges $f \in K[x]$ polinomhoz pontosan egy olyan $h \in K[x]$, $h^* < (m_{\alpha,K})^*$ polinom van, amelyre $f + (m_{\alpha,K}) = h + (m_{\alpha,K})$, ezért $K(\alpha)$ tetszőleges eleme egyértelműen írható fel $h(\alpha)$ alakban, ahol $h^* < (m_{\alpha,K})^*$. Ez pedig azt jelenti, hogy a $K(\alpha)$ (mint K feletti) vektortérnek bázisa az $1, \alpha, \ldots, \alpha^{n-1}$ vektorrendszer, ahol $n = (m_{\alpha,K})^*$. Azaz $[K(\alpha) : K]$ véges és $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.

Tétel.

Ha $L|K$ véges bővítés, és $\alpha \in L$, akkor α algebrai elem K felett, és $\mathrm{gr}_K(\alpha)$ osztója $[L:K]$-nak.

Tétel.

Ha $L|K$ véges bővítés, és $\alpha \in L$, akkor α algebrai elem K felett, és $\mathrm{gr}_K(\alpha)$ osztója $[L:K]$-nak.

Bizonyítás.

A Fokszámtételt alkalmazva az $K(\alpha)|K$ és $L|K(\alpha)$ bővítésekre azt kapjuk, hogy a $K(\alpha)|K$ bővítés véges, így α algebrai elem K felett, valamint

$$[L:K] = [L:K(\alpha)][K(\alpha):K] = [L:K(\alpha)] \cdot \mathrm{gr}_K(\alpha),$$

azaz $\mathrm{gr}_K(\alpha) \mid [L:K]$.

Tétel.

Legyen $L|K$ tetszőleges testbővítés, és $\alpha \in L$ algebrai elem K felett, valamint legyen $k \in \mathbb{N}$. Ekkor $\sqrt[k]{\alpha}$ is algebrai K felett, és $\mathrm{gr}_K(\sqrt[k]{\alpha}) \leqslant k \cdot \mathrm{gr}_K(\alpha)$.

Tétel.

Legyen $L|K$ tetszőleges testbővítés, és $\alpha \in L$ algebrai elem K felett, valamint legyen $k \in \mathbb{N}$. Ekkor $\sqrt[k]{\alpha}$ is algebrai K felett, és $\mathrm{gr}_K(\sqrt[k]{\alpha}) \leqslant k \cdot \mathrm{gr}_K(\alpha)$.

Tétel.

Legyenek $L|K$ és $M|L$ tetszőleges testbővítések, és $\alpha \in M$ algebrai elem K felett. Ekkor α algebrai L felett is, és $\mathrm{gr}_L(\alpha) \leqslant \mathrm{gr}_K(\alpha)$.

Tétel.

Legyen $L|K$ tetszőleges testbővítés, és $\alpha \in L$ algebrai elem K felett, valamint legyen $k \in \mathbb{N}$. Ekkor $\sqrt[k]{\alpha}$ is algebrai K felett, és $\mathrm{gr}_K(\sqrt[k]{\alpha}) \leqslant k \cdot \mathrm{gr}_K(\alpha)$.

Tétel.

Legyenek $L|K$ és $M|L$ tetszőleges testbővítések, és $\alpha \in M$ algebrai elem K felett. Ekkor α algebrai L felett is, és $\mathrm{gr}_L(\alpha) \leqslant \mathrm{gr}_K(\alpha)$.

Tétel.

Legyenek K és L olyan testek, amelyekre $L|K$ teljesül, valamint legyen $\alpha, \beta \in L$. Ekkor

$$K(\alpha, \beta) = K(\alpha)(\beta) = K(\beta)(\alpha).$$

Tétel.

Legyen $L|K$ tetszőleges testbővítés, és $\alpha, \beta \in L$ algebrai elemek K felett. Ekkor $\alpha \pm \beta$, $\alpha\beta$, valamint $\beta \neq 0$ esetén α/β is algebrai elemek K felett, melyek foka legfeljebb $\mathrm{gr}_K(\alpha) \cdot \mathrm{gr}_K(\beta)$.

Tétel.

Legyen $L|K$ tetszőleges testbővítés, és $\alpha, \beta \in L$ algebrai elemek K felett. Ekkor $\alpha \pm \beta$, $\alpha\beta$, valamint $\beta \neq 0$ esetén α/β is algebrai elemek K felett, melyek foka legfeljebb $\mathrm{gr}_K(\alpha) \cdot \mathrm{gr}_K(\beta)$.

Tétel.

Legyen $L|K$ tetszőleges testbővítés. Ekkor az L test K felett algebrai elemei L egy résztestét alkotják.

Tétel.

Legyen $L|K$ tetszőleges testbővítés, és $\alpha, \beta \in L$ algebrai elemek K felett. Ekkor $\alpha \pm \beta$, $\alpha\beta$, valamint $\beta \neq 0$ esetén α/β is algebrai elemek K felett, melyek foka legfeljebb $\mathrm{gr}_K(\alpha) \cdot \mathrm{gr}_K(\beta)$.

Tétel.

Legyen $L|K$ tetszőleges testbővítés. Ekkor az L test K felett algebrai elemei L egy résztestét alkotják.

Definíció: algebrai szám.

A z komplex számot **algebrai számnak** nevezzük, ha z algebrai $\mathbb{Q}$ felett. Az előző tétel szerint az algebrai számok a komplex számtest egy résztestét alkotják, melyet $\mathbb{A}$-val jelölünk.

Definíció: algebrai (test)bővítés.

Azt mondjuk, hogy az $L|K$ testbővítés **algebrai testbővítés**, ha L minden eleme algebrai K felett.

Definíció: algebrai (test)bővítés.

Azt mondjuk, hogy az $L|K$ testbővítés **algebrai testbővítés**, ha L minden eleme algebrai K felett.

Tétel.

Legyen $L|K$ tetszőleges testbővítés. Ekkor a következők ekvivalensek:

Definíció: algebrai (test)bővítés.

Azt mondjuk, hogy az $L|K$ testbővítés **algebrai testbővítés**, ha L minden eleme algebrai K felett.

Tétel.

Legyen $L|K$ tetszőleges testbővítés. Ekkor a következők ekvivalensek:

(1) $[L:K] < \infty$;

Definíció: algebrai (test)bővítés.

Azt mondjuk, hogy az $L|K$ testbővítés **algebrai testbővítés**, ha L minden eleme algebrai K felett.

Tétel.

Legyen $L|K$ tetszőleges testbővítés. Ekkor a következők ekvivalensek:

(1) $[L:K] < \infty$;

(2) az $L|K$ bővítés algebrai, és L végesen generált K felett;

Definíció: algebrai (test)bővítés.

Azt mondjuk, hogy az $L|K$ testbővítés **algebrai testbővítés**, ha L minden eleme algebrai K felett.

Tétel.

Legyen $L|K$ tetszőleges testbővítés. Ekkor a következők ekvivalensek:

(1) $[L : K] < \infty$;

(2) az $L|K$ bővítés algebrai, és L végesen generált K felett;

(3) $L = K(\alpha_1, \dots, \alpha_n)$, ahol $\alpha_1, \dots, \alpha_n \in L$ algebrai elemek K felett.

Bizonyítás.

(1) $\Longrightarrow$ (2): legyen $[L:K]=n$, és $\alpha_1,\ldots,\alpha_n \in L$ az L vektortér bázisa. Ekkor $L=[\alpha_1,\ldots,\alpha_n]$ miatt $L=K(\alpha_1,\ldots,\alpha_n)$, azaz L végesen generált. Legyen α az L test tetszőleges eleme. Ekkor a Fokszámtétel szerint a $K(\alpha)|K$ testbővítés végesfokú, így α algebrai elem K felett. Ezért az $L|K$ testbővítés algebrai.

(2) $\Longrightarrow$ (3): Az állítás triviálisan teljesül.

Bizonyítás (folytatás).

(3) $\Longrightarrow$ (1): Definiáljuk az L_0 $(1 \leqslant i \leqslant n)$ testeseket a következőképpen:

$$L_0 = K, \qquad L_i = L_{i-1}(\alpha_i) \quad (1 \leqslant i \leqslant n).$$

Mivel $\alpha_i \in L$ algebrai elem K felett, ezért α_i algebrai elem L_{i-1} felett is, így

$$[L_i : L_{i-1}] = [L_{i-1}(\alpha_i) : L_{i-1}] < \infty.$$

Ekkor a Fokszámtételt alkalmazva azt kapjuk, hogy

$$[L : K] = [L_n : L_0] = \prod_{i=1}^{n} [L_i : L_{i-1}] < \infty.$$

Ezzel a tétel bizonyítását befejeztük.

Következmény.

Ha $\alpha \in L$ az $L|K$ bővítés algebrai eleme, akkor a $K(\alpha)|K$ bővítés algebrai.

Következmény.

Ha $\alpha \in L$ az $L|K$ bővítés algebrai eleme, akkor a $K(\alpha)|K$ bővítés algebrai.

Következmény.

Legyen $L|K$ testbővítés, és $S \subseteq L$. Ha S minden eleme algebrai K felett, akkor a $K(S)|K$ bővítés algebrai.

Következmény.

Ha $\alpha \in L$ az $L|K$ bővítés algebrai eleme, akkor a $K(\alpha)|K$ bővítés algebrai.

Következmény.

Legyen $L|K$ testbővítés, és $S \subseteq L$. Ha S minden eleme algebrai K felett, akkor a $K(S)|K$ bővítés algebrai.

Bizonyítás

Legyen α tetszőleges eleme a $K(S)$ testnek. Ekkor van olyan véges S' részhalmaza S-nek, amelyre $\alpha \in K(S')$. Ekkor az előző tétel szerint a $K(S')$ bővítés algebrai, így α is algebrai elem K felett. Azaz a $K(S)|K$ bővítés algebrai.

Tétel.

Ha az $M|L$ és $L|K$ testbővítések algebraiak, akkor az $M|K$ bővítés is algebrai.

Tétel.

Ha az $M|L$ és $L|K$ testbővítések algebraiak, akkor az $M|K$ bővítés is algebrai.

Bizonyítás.

Legyen α tetszőleges eleme M-nek. Mivel az $M|L$ bővítés algebrai, ezért α algebrai elem L felett. Legyen $m_{\alpha,L} = \sum_{i=0}^{n} \lambda_i x^i$. Definiáljuk a $K_0, \dots, K_n$ testeket a következő módon:

$$K_0 = K, \qquad K_i = K_{i-1}(\lambda_i) \quad (1 \leqslant i \leqslant n).$$

Mivel λ_i algebrai elem K felett, ezért a $K_i|K_{i-1}$ bővítések végesek $(1 \leqslant i \leqslant n)$. Így a Fokszámtétel szerint a $K_n|K$ bővítés is véges.

Bizonyítás (folytatás).

Tekintsük a $K_n(\alpha)|K$ bővítést. Mivel α algebrai elem K_n felett, ezért $K_n(\alpha)|K_n$ véges, ezért ismét a Fokszámtétel szerint azt kapjuk, hogy

$$[K_n(\alpha) : K] = [K_n(\alpha) : K_n] \cdot [K_n : K] < \infty,$$

azaz α a K test felett is algebrai elem.