Magasabbfokú egyenletek és geometriai szerkeszthetőség

Dormán Miklós

SZTE, Bolyai Intézet

2010/2011. őszi félév, 2010. szeptember 17.

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

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

3. ábra: Évariste Galois (1811-1832).

Definíció: (test)bővítés.

Legyenek K és L testek. Ha K részteste 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 részteste 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.

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. $A = \{\alpha_1, \ldots, \alpha_n\}$, 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 $L = K(\alpha)$.

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

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

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

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

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

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

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 $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right) \approx 0.57721566490153286060651209$ 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.

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.

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

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.

Tétel.

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