7. TESTBŐVÍTÉS ALGEBRAI ELEMEKKEL

7.A.Definíció. Az $\alpha \in \mathbb{C}$ **komplex számot algebrainak** nevezzük a $K \subseteq \mathbb{C}$ **számtest felett**, ha létezik olyan zérustól különböző $0 \neq f(x) \in K[x]$ polinom, amelynek az α gyöke: $f(\alpha) = 0$. Amennyiben ilyen polinom nem létezik, akkor azt mondjuk, hogy α **transzcendens** a $K \subseteq \mathbb{C}$ **számtest felett**.
Ha $\alpha \in \mathbb{C}$ algebrai a $K \subseteq \mathbb{C}$ számtest felett, akkor egy $f(\alpha) = 0$ tulajdonságú $0 \neq f(x) \in K[x]$ polinom fokszámára nyilvánvalóan teljesül a $\deg(f(x)) \geq 1$ egyenlőtlenség. Mivel a természetes számok $\mathbb{N} = \{1, 2, ..., k, ...\}$ halmazának bármely nem üres részhalamza tartalmaz egy legkisebb elemet, ezért tekinthetjük az

$$n = \min\{\deg(f(x)) \mid 0 \neq f(x) \in K[x] \text{ és } f(\alpha) = 0\}$$

legkisebb fokszámot. Azokat a $p(\alpha) = 0$ tulajdonságú $0 \neq p(x) \in K[x]$ polinomokat nevezzük a K számtest felett **algebrai** $\alpha \in \mathbb{C}$ **szám** K **feletti minimál polinomjainak**, amelyekre $\deg(p(x)) = n$ (a fentiek szerint minden algebrai számnak létezik legalább egy minimál polinomja).♡

7.1.Állítás. *Legyen $K \subseteq \mathbb{C}$ egy számtest és $p(x) \in K[x]$ (az egyik) minimál polinomja a K felett algebrai $\alpha \in \mathbb{C}$ számnak. Ekkor az alábbiak teljesülnek.*

1. *$p(x)$ irreducibilis K felett.*
2. *Ha egy $f(x) \in K[x]$ polinomra $f(\alpha) = 0$, akkor teljesül a $p(x) \mid f(x)$ oszthatóság.*
3. *Ha $q(x) \in K[x]$ irreducibilis polinom a K felett és $q(\alpha) = 0$, akkor $q(x)$ is minimál polinomja α-nak. Tehát egy irreducibilis polinom minden gyökének minimál polinomja.*
4. *Ha $p_1(x) \in K[x]$ és $p_2(x) \in K[x]$ tetszőleges K feletti minimál polinomjai α-nak, akkor teljesül a $p_1(x) \sim p_2(x)$ asszociáltság. Tehát egy algebrai szám minimál polinomja asszociáltságtól eltekintve egyértelműen meghatározott.*

Bizonyítás.

1. Ha $p(x) = u(x)v(x)$ teljesülne a $\deg(u(x)) \geq 1$ és $\deg(v(x)) \geq 1$ tulajdonságú $u(x) \in K[x]$ és $v(x) \in K[x]$ polinomokra, akkor $u(\alpha)v(\alpha) = p(\alpha) = 0$ miatt vagy $u(\alpha) = 0$, vagy $v(\alpha) = 0$ teljesül. Mivel $\deg(u(x)) + \deg(v(x)) = \deg(p(x))$, ezért $\deg(u(x)) < \deg(p(x))$ és $\deg(v(x)) < \deg(p(x))$. Tehát mindkét esetben ellentmondásba kerülünk azzal, hogy $p(x)$ egyike a legkisebb fokszámú olyan $K[x]$-beli polinomoknak, amelyeknek α gyöke.

2. Az 1.részben már láttuk, hogy $p(x)$ irreducibilis $K[x]$-ben. Mivel az $f(x) \in K[x]$ polinomnak és $p(x)$-nek az α közös gyöke, ezért a 4.5.Állítás 4.része szerint $p(x) \mid f(x)$.

3. Az előbb igazolt 2.rész szerint $p(x) \mid q(x)$. Mivel $q(x)$ irreducibilis $K[x]$-ben, ezért a 4.5.Állítás 1.része alapján $q(x)$-nek csak triviális osztói léteznek $K[x]$-ben. Tehát a $K[x]$-beli $p(x)$ polinomra vagy $p(x) \sim 1$, vagy $p(x) \sim q(x)$. A $p(x) \sim 1$ asszociált viszony nem teljesülhet, mert $p(x)$ irreducibilis (K felett). Így $p(x) \sim q(x)$, ami azt jelenti, hogy $\deg(p(x)) = \deg(q(x))$, azaz $q(x) \in K[x]$ is minimál polinomja α-nak.

4. A már igazolt 2.rész szerint teljesülnek a $p_1(x) \mid p_2(x)$ és $p_2(x) \mid p_1(x)$ oszthatóságok, ami a $p_1(x) \sim p_2(x)$ asszociált viszonyt jelenti.

□□□

7.2.Állítás. *Legyenek $K \subseteq L \subseteq \mathbb{C}$ számtestek és $\alpha \in L$. Ha $K \subseteq L$ véges bővítés, akkor α algebrai a K számtest felett és α-nak a K feletti $p(x) \in K[x]$ minimál polinomjára a*

$$\deg(p(x)) \leq [L : K]$$

egyenlőtlenség teljesül.

Bizonyítás. Ha $m = [L : K]$, akkor L-nek akárhogyan kiválasztva $m+1$ darab elemét, azok lineárisan összefüggőek lesznek K felett (lásd a 2.6.Állítás 2.részét). Tehát α-nak az L-ben található $1, \alpha, \alpha^2, ..., \alpha^m$ hatványai lineárisan összefüggenek K felett, azaz

$$u_0 1 + u_1\alpha + u_2\alpha^2 + ... + u_m\alpha^m = 0$$

teljesül alkalmas $u_0, u_1, u_2, ..., u_m \in K$ számokkal úgy, hogy valamelyik $u_i \neq 0$. Tehát

$$f(x) = u_0 + u_1 x + u_2 x^2 + ... + u_m x^m$$

olyan zérustól különböző $K[x]$-beli polinom, amelynek α gyöke: $f(\alpha) = 0$. Az α-ról így látjuk, hogy algebrai a K számtest felett és azt is, hogy a K feletti minimál polinomjának a fokszáma a fenti $f(x)$ fokszámától nem lehet nagyobb:

$$\deg(p(x)) \leq \deg(f(x)) \leq m = [L : K].$$

□□□

7.3.Tétel. *Legyen $p(x) \in K[x]$ a minimál polinomja a $K \subseteq \mathbb{C}$ számtest felett algebrai $\alpha \in \mathbb{C}$ számnak és $n = \deg(p(x))$. Ekkor α-nak az $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ hatványai K-ra nézve bázisát alkotják a $K(\alpha)$ bővített számtestnek. Tehát $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ lineárisan függetlenek K felett és*

$$K(\alpha) = [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K = \{f(\alpha) \mid f(x) \in K[x] \text{ és } \deg(f(x)) \leq n-1\},$$

továbbá a $K(\alpha) \subseteq \mathbb{C}$ számtest K feletti dimenziójára

$$[K(\alpha) : K] = n = \deg(p(x))$$

teljesül.

Bizonyítás. Amennyiben α-nak az $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ hatványai lineárisan összefüggenek K felett, akkor

$$u_0 1 + u_1\alpha + u_2\alpha^2 + ... + u_{n-1}\alpha^{n-1} = 0$$

teljesül alkalmas $u_0, u_1, u_2, ..., u_{n-1} \in K$ számokkal úgy, hogy valamelyik $u_i \neq 0$. Tehát

$$f(x) = u_0 + u_1 x + u_2 x^2 + ... + u_{n-1} x^{n-1}$$

olyan zérustól különböző $K[x]$-beli polinom, amelynek α gyöke: $f(\alpha) = 0$. Így ellentmondáshoz jutottunk, hiszen $\deg(f(x)) \leq n-1$ és α-nak a K feletti $p(x) \in K[x]$ minimál polinomjára $\deg(p(x)) = n$.
Az alábbi

$$[1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K = \{f(\alpha) \mid f(x) \in K[x] \text{ és } \deg(f(x)) \leq n-1\} \subseteq K(\alpha)$$

egyenlőség és tartalmazás nyilvánvaló, mert $K(\alpha)$ zárt az összeadásra és a szorzásra nézve, továbbá $K \subseteq K(\alpha)$ és $\alpha \in K(\alpha)$. Mivel $K \subseteq [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$ és $\alpha \in [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$, ezért $K(\alpha)$ definíciójára való tekintettel a $K(\alpha) \subseteq [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$ tartalmazáshoz elegendő azt megmutatni, hogy $[1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K \subseteq \mathbb{C}$ számtest.
Az összeadásra és kivonásra a $[1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$ részhalmaz nyilvánvalóan zárt (lásd a 2.3.Állítás 1.részét). Tekintsük most a $[1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$ lineáris generátumnak két tetszőleges

$$a = u_0 1 + u_1\alpha + u_2\alpha^2 + ... + u_{n-1}\alpha^{n-1} = f(\alpha) \text{ és } b = v_0 1 + v_1\alpha + v_2\alpha^2 + ... + v_{n-1}\alpha^{n-1} = g(\alpha)$$

elemét, ahol $u_0, u_1, u_2, ..., u_{n-1} \in K$, $v_0, v_1, v_2, ..., v_{n-1} \in K$ és

$$f(x) = u_0 + u_1 x + u_2 x^2 + ... + u_{n-1}x^{n-1} \in K[x] \ , \ g(x) = v_0 + v_1 x + v_2 x^2 + ... + v_{n-1}x^{n-1} \in K[x].$$

Ha az $r(x)$ polinom az $f(x)g(x)$ szorzatnak a $p(x)$-el való maradékos osztásánál keletkező osztási maradék, akkor

$$f(x)g(x) = p(x)h(x) + r(x)$$

és $\deg(r(x)) \leq \deg(p(x)) - 1 = n - 1$. Így $p(\alpha) = 0$ miatt

$$ab = f(\alpha)g(\alpha) = p(\alpha)h(\alpha) + r(\alpha) = r(\alpha),$$

ahol $f(x)g(x) \in K[x]$ és $p(x) \in K[x]$ miatt

$$r(x) = w_0 + w_1 x + w_2 x^2 + ... + w_{n-1}x^{n-1} \in K[x],$$

$$ab = r(\alpha) = w_0 + w_1\alpha + w_2\alpha^2 + ... + w_{n-1}\alpha^{n-1} \in [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K.$$

Ha $a \neq 0$, akkor $f(x)$ nem lehet a zérus polinom. Mivel $\deg(f(x)) \leq n-1 < \deg(p(x))$, ezért most $p(x) \nmid f(x)$. A 4.5.Állítás 3.részét alkalmazva a $K[x]$-ben irreducibilis $p(x)$ polinomra az

$$\text{lnko}(p(x), f(x)) = 1$$

egyenlőséget kapjuk. A 3.6.Tétel és az utána következő megjegyzések értelmében léteznek olyan $s(x), t(x) \in K[x]$ polinomok, amelyekre

$$1 = p(x)t(x) + f(x)s(x).$$

A fenti egyenlőségből α behelyettesítésével és $p(\alpha) = 0$ figyelembe vételével kapjuk, hogy

$$1 = f(\alpha)s(\alpha) = as(\alpha),$$

ahol $s(x) = s_0 + s_1 x + s_2 x^2 + ... + s_m x^m$. Mivel azt már igazoltuk, hogy $[1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$ zárt az összeadásra és szorzásra, ezért $s_i \in K$ $(0 \leq i \leq m)$ valamint $\alpha \in [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K$ miatt megkapjuk azt is, hogy

$$\frac{1}{a} = s(\alpha) = s_0 + s_1\alpha + s_2\alpha^2 + ... + s_m\alpha^m \in [1, \alpha, \alpha^2, ..., \alpha^{n-1}]_K.$$

□□□

7.4.Állítás. *Legyenek $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{C}$ algebrai számok a $K \subseteq \mathbb{C}$ számtest felett. Ekkor a $K(\alpha_1, \alpha_2, ..., \alpha_m)$ bővítés bármely eleme $f(\alpha_1, \alpha_2, ..., \alpha_m)$ alakban írható valamilyen m változós $f(x_1, x_2, ..., x_m) \in K[x_1, x_2, ..., x_m]$ polinommal, azaz*

$$K(\alpha_1, \alpha_2, ..., \alpha_m) = \{f(\alpha_1, \alpha_2, ..., \alpha_m) \mid f(x_1, x_2, ..., x_m) \in K[x_1, x_2, ..., x_m]\}.$$

A dimenziókra teljesül az alábbi

$$[K(\alpha_1, \alpha_2, ..., \alpha_m) : K] \leq [K(\alpha_1) : K] \cdot [K(\alpha_2) : K] \cdot ... \cdot [K(\alpha_m) : K]$$

egyenlőtlenség.

Bizonyítás. Az $m \geq 1$ egészre vonatkozó teljes indukciót alkalmazunk.
Ha $m = 1$, akkor az előbbi 7.3.Tétel pontosan azt mondja ki, amire itt szükségünk van és az egyenlőtlenség helyett most nyilvánvalóan egyenlőség teljesül: $[K(\alpha_1) : K] = [K(\alpha_1) : K]$.
Tételezzük fel most állításunk igazságát egy bizonyos $m \geq 1$ egészre és tekintsük az $\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1} \in \mathbb{C}$ algebrai számokat a $K \subseteq \mathbb{C}$ számtest felett. Mivel

$$K(\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}) = (K(\alpha_1, \alpha_2, ..., \alpha_m))(\alpha_{m+1})$$

és a $K \subseteq \mathbb{C}$ számtest felett algebrai $\alpha_{m+1} \in \mathbb{C}$ szám nyilvánvalóan algebrai lesz a K-nál bővebb $K(\alpha_1, \alpha_2, ..., \alpha_m) \subseteq \mathbb{C}$ számtest felett is, ezért ismét a 7.3.Tételt alkalmazva kapjuk, hogy

$$(K(\alpha_1, \alpha_2, ..., \alpha_m))(\alpha_{m+1}) = [1, \alpha_{m+1}, \alpha_{m+1}^2, ..., \alpha_{m+1}^{n-1}]_{K(\alpha_1, \alpha_2, ..., \alpha_m)},$$

ahol $n = \deg(p(x))$ az $\alpha_{m+1} \in \mathbb{C}$ szám $K(\alpha_1, \alpha_2, ..., \alpha_m)$ feletti $p(x) \in K(\alpha_1, \alpha_2, ..., \alpha_m)[x]$ minimál polinomjának a fokszáma. A $[1, \alpha_{m+1}, \alpha_{m+1}^2, ..., \alpha_{m+1}^{n-1}]_{K(\alpha_1, \alpha_2, ..., \alpha_m)}$ lineáris generátumnak bármely a eleme az

$$a = \lambda_0 1 + \lambda_1 \alpha_{m+1} + \lambda_2 \alpha_{m+1}^2 + ... + \lambda_{n-1} \alpha_{m+1}^{n-1}$$

alakban írható, ahol minden $\lambda_i \in K(\alpha_1, \alpha_2, ..., \alpha_m)$ együttható $(0 \leq i \leq n-1)$ az indukciós feltevés szerint

$$\lambda_i = g_i(\alpha_1, \alpha_2, ..., \alpha_m)$$

alakban írható valamilyen m változós $g_i(x_1, x_2, ..., x_m) \in K[x_1, x_2, ..., x_m]$ polinommal. Tehát

$$a = g_0(\alpha_1, \alpha_2, ..., \alpha_m)1 + g_1(\alpha_1, \alpha_2, ..., \alpha_m)\alpha_{m+1} + ... + g_{n-1}(\alpha_1, \alpha_2, ..., \alpha_m)\alpha_{m+1}^{n-1} =$$

$$= f(\alpha_1, \alpha_2, ..., \alpha_m, \alpha_{m+1}),$$

ahol az

$$f(x_1, x_2, ..., x_m, x_{m+1}) = g_0(x_1, x_2, ..., x_m) + g_1(x_1, x_2, ..., x_m)x_{m+1} + ... + g_{n-1}(x_1, x_2, ..., x_m)x_{m+1}^{n-1}$$

polinomra nyilvánvalóan teljesül, hogy $f(x_1, x_2, ..., x_m, x_{m+1}) \in K[x_1, x_2, ..., x_m, x_{m+1}]$.
Ha $q(x) \in K[x]$ jelöli az $\alpha_{m+1} \in \mathbb{C}$ szám K feletti minimál polinomját, akkor
$q(x) \in K(\alpha_1, \alpha_2, ..., \alpha_m)[x]$ és $q(\alpha_{m+1}) = 0$ miatt a 7.3.Tétel figyelembe vételével adódik, hogy

$$[(K(\alpha_1, \alpha_2, ..., \alpha_m))(\alpha_{m+1}) : K(\alpha_1, \alpha_2, ..., \alpha_m)] = \deg(p(x)) = n \leq \deg(q(x)) = [K(\alpha_{m+1}) : K].$$

Az indukciós feltevésünket és a

$$K \subseteq K(\alpha_1, \alpha_2, ..., \alpha_m) \subseteq (K(\alpha_1, \alpha_2, ..., \alpha_m))(\alpha_{m+1})$$

számtestekre a dimenziók szorzási szabályát (2.7.Tétel) használva jutunk a kívánt egyenlőtlenséghez:

$$[(K(\alpha_1, \alpha_2,...,\alpha_m))(\alpha_{m+1}) : K] = [(K(\alpha_1, \alpha_2,...,\alpha_m))(\alpha_{m+1}) : K(\alpha_1, \alpha_2,...,\alpha_m)][K(\alpha_1, \alpha_2,..., \alpha_m) : K] \leq$$

$$\leq [K(\alpha_{m+1}) : K] \cdot ([K(\alpha_1) : K] \cdot [K(\alpha_2) : K] \cdot ... \cdot [K(\alpha_m) : K]) .$$

□□□

7.5.Tétel. *Legyenek $\alpha, \beta \in \mathbb{C}$ algebrai számok a $K \subseteq \mathbb{C}$ számtest felett. Ekkor véges sok $c \in K$ elemtől eltekintve teljesül a $K(\alpha, \beta) = K(\alpha + c\beta)$ egyenlőség, pontosabban*

$$|\{c \in K \mid c \neq 0 \text{ és } K(\alpha, \beta) \neq K(\alpha + c\beta)\}| \leq ([K(\alpha) : K] - 1)([K(\beta) : K] - 1).$$

Bizonyítás. Legyen $p(x) \in K[x]$ az α-nak és $q(x) \in K[x]$ a β-nak a K feletti minimál polinomja és tekintsük ezeknek a $K[x]$-ben irreducibilis polinomoknak az 5.8.Következményben leírt alakú

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \text{ és } q(x) = b_m(x - \beta_1)(x - \beta_2)...(x - \beta_m)$$

gyöktényezős felbontását, ahol $\alpha = \alpha_1$, $\beta = \beta_1$ és

$$n = \deg(p(x)) = [K(\alpha) : K] \ , \ m = \deg(q(x)) = [K(\beta) : K].$$

Ha egy $0 \neq c \in K$ számra

$$\alpha + c\beta = \alpha_1 + c\beta_1 \neq \alpha_i + c\beta_j$$

teljesül minden $2 \leq i \leq n$ és $2 \leq j \leq m$ indexre, akkor alkalmazzuk a $\gamma = \alpha + c\beta$ jelölést és tekintsük a

$$d(x) = \text{lnko}(p(\gamma - cx), q(x))$$

legnagyobb közös osztóját a $p(\gamma - cx) \in K(\gamma)[x]$ és $q(x) \in K[x] \subseteq K(\gamma)[x]$ polinomoknak. A 3.6.Tétel és az utána következő megjegyzések értelmében $d(x) \in K(\gamma)[x]$, továbbá a 3.5.Állítás 9.része alapján $d(x)$-nek pontosan azok a komplex számok a gyökei, amelyek $p(\gamma - cx)$-nek és $q(x)$-nek is gyökei.
A $p(\gamma - cx)$-nek és $q(x)$-nek egyetlen közös gyöke a $\beta = \beta_1$, hiszen a $2 \leq j \leq m$ esetben $p(\gamma - c\beta_j) = 0$ csak akkor teljesül, ha valamilyen $1 \leq i \leq n$ indexre $\alpha_i = \gamma - c\beta_j = (\alpha_1 + c\beta_1) - c\beta_j$, ami ellentétes az $\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$ feltételezésünkel (az $i = 1$ esetben sem lehet egyenlőség, hiszen $c \neq 0$). Mivel $d(x)$ főegyütthatója 1, ezért a fentiek alapján $d(x)$ gyöktényezős felbontása $d(x) = (x - \beta_1)^k$ alakú valamilyen $k \geq 1$ kitevővel. Az 5.4.Állítás szerint a $d(x) \mid q(x)$ oszthatóságból $k = 1$ következik, azaz $d(x) = x - \beta_1$. A $d(x) \in K(\gamma)[x]$ tartalmazás azt eredményezi, hogy $\beta = \beta_1 \in K(\gamma)$. Innen $c \in K$ figyelembe vételével kapjuk, hogy $\alpha = \gamma - c\beta \in K(\gamma)$. A fentiekből a $K(\alpha, \beta)$ definíciójára való tekintettel előbb a

$$K(\alpha, \beta) \subseteq K(\gamma) = K(\alpha + c\beta)$$

tartalmazás, majd a nyilvánvalóan teljesülő $K(\alpha + c\beta) \subseteq K(\alpha, \beta)$ fordított tartalmazást is felhasználva a $K(\alpha, \beta) = K(\alpha + c\beta)$ egyenlőség adódik.

Tehát minden olyan $0 \neq c \in K$ számra teljesül $K(\alpha, \beta) = K(\alpha + c\beta)$, amelyre

$$c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}.$$

□□□

7.6.Tétel. *A $K \subseteq L \subseteq \mathbb{C}$ számtestekre az alábbiak ekvivalensek.*

1. *$K \subseteq L$ véges bővítés, azaz létezik L-nek bázisa K felett (az $[L : K]$ dimenzió véges).*
2. *Létezik olyan K felett algebrai $\alpha \in \mathbb{C}$ szám, amelyre $K(\alpha) = L$ (ilyenkor $\alpha \in L$).*

Bizonyítás. 2. $\Longrightarrow$ 1. A 7.3.Tétel szerint α-nak az $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ hatványai K-ra nézve bázisát alkotják a $K(\alpha) = L$ számtestnek (itt $n = \deg(p(x))$ a $K \subseteq \mathbb{C}$ számtest felett algebrai $\alpha \in \mathbb{C}$ szám $p(x) \in K[x]$ minimál polinomjának a fokszáma).
1. $\Longrightarrow$ 2. Az $n = [L : K]$ dimenzióra vonatkozó teljes indukciót alkalmazunk.
Ha $n = 1$, akkor a 2.8.Állítás 1.részére való tekintettel $L = K$, ezért $L = K(\alpha)$, ahol $\alpha \in L$ tetszőleges. Tételezzük fel most, hogy állításunk igaz minden olyan véges $K' \subseteq L'$ (itt $L' \subseteq \mathbb{C}$) bővítésre, amelyre $[L' : K'] \leq n$ és tekintsünk egy olyan véges $K \subseteq L$ (itt $L \subseteq \mathbb{C}$) bővítést, amelynél $[L : K] = n + 1$. Legyen $\alpha \in L$ tetszőleges elem, ekkor a 7.2.Állítás miatt α algebrai K felett. Ha $K(\alpha) = L$, akkor készen vagyunk. Ha $K(\alpha) \neq L$, akkor a $K \subseteq K(\alpha) \subseteq L$ számtestekre $[L : K(\alpha)] \leq n$ teljesül, hiszen a 2.8.Állítás szerint az $[L : K(\alpha)] = n + 1 = [L : K]$ egyenlőségből $K(\alpha) = L$ következne. Az indukciós feltevésünket a $K(\alpha) \subseteq L$ bővítésre alkalmazva kapjuk olyan $\beta \in L$ létezését, amelyre $L = (K(\alpha))(\beta) = K(\alpha, \beta)$. Mivel $\beta \in L$ és $K \subseteq L$ véges bővítés, ezért a 7.2.Állítás miatt β is algebrai K felett, így a 7.5.Tétel szerint van olyan $c \in K$ elem, amire $K(\alpha, \beta) = K(\alpha + c\beta)$ (K-nak csak véges sok c elemére nem teljesül ez). Tehát $L = K(\alpha + c\beta)$ teljesül az $\alpha + c\beta \in L$ elemre.

□□□