Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. február 9.

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 $\alpha\beta^{-1}$ is algebrai elemek K felett, melyek foka legfeljebb $\mathrm{gr}_K(\alpha) \cdot \mathrm{gr}_K(\beta)$.

Definíció: több határozatlanrendszerre nézve szimmetrikus polinom.

Legyen R tetszőleges egységelemes gyűrű és $f \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$. Azt mondjuk, hogy az f polinom **szimmetrikus az** $x_1, \ldots, x_m$**, illetve** $y_1, \ldots, y_n$ **határozatlanrendszerekre nézve**, ha bármely $\pi \in S_m$, illetve $\tau \in S_n$ permutációkra

$$f(x_{1\pi}, \ldots, x_{m\pi}, y_{1\tau}, \ldots, y_{n\tau}) = f(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

teljesül.

Tétel.

Legyen R tetszőleges egységelemes gyűrű és $h \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$ tetszőleges olyan polinom, amely szimmetrikus az $x_1, \ldots, x_m$, illetve $y_1, \ldots, y_n$ határozatlanrendszerekre nézve. Ekkor létezik pontosan egy olyan $f \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$ polinom, amelyre

$$h = f(\sigma_1, \ldots, \sigma_m, \tau_1, \ldots, \tau_n),$$

ahol $\sigma_1, \ldots, \sigma_m$, illetve $\tau_1, \ldots, \tau_n$ az $x_1, \ldots, x_m$, illetve $y_1, \ldots, y_n$ határozatlanokból képzett elemi szimmetrikus polinomok.

Következmény.

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

Következmény.

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.

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_i $(0 \leqslant i \leqslant n)$ testeket 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 $K_0, \ldots, K_n$ 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.

Definíció: felbontási test.

Legyen K test, és $f \in K[x] \setminus \{0\}$ tetszőleges polinom. Azt mondjuk, hogy a K test L bővítése **felbontási teste** f**-nek** K **felett**, ha f elsőfokú tényezők szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

Definíció: felbontási test.

Legyen K test, és $f \in K[x] \setminus \{0\}$ tetszőleges polinom. Azt mondjuk, hogy a K test L bővítése **felbontási teste** f**-nek** K **felett**, ha f elsőfokú tényezők szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

A felbontási test definíciójának közvetlen következménye az alábbi állítás.

Definíció: felbontási test.

Legyen K test, és $f \in K[x] \setminus \{0\}$ tetszőleges polinom. Azt mondjuk, hogy a K test L bővítése **felbontási teste** f**-nek** K **felett**, ha f elsőfokú tényezők szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

A felbontási test definíciójának közvetlen következménye az alábbi állítás.

Állítás.

Ha L felbontási teste az $f \in K[x]$ polinomnak K felett, akkor az $L : K$ bővítés véges algebrai bővítés.

Példa.

Tekintsük az $f = x^2 + 1 \in \mathbb{Q}[x]$ polinomot. Mivel f-nek pontosan két gyöke van $\mathbb{C}$-ben, ezért felbontási teste

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Példa.

Tekintsük az $f = x^2 + 1 \in \mathbb{Q}[x]$ polinomot. Mivel f-nek pontosan két gyöke van $\mathbb{C}$-ben, ezért felbontási teste

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Példa.

Legyen $f = x^3 - 2 \in \mathbb{Q}[x]$. Az f polinom gyökei $\mathbb{C}$-ben: $\varepsilon^k \sqrt[3]{2}$ $(k = 0, 1, 2)$, ahol $\varepsilon = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$. Ekkor f felbontási teste $\mathbb{Q}$ felett

$$\mathbb{Q}(\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon).$$

Tétel (A felbontási test létezése).

Legyen K test, és f n-edfokú ($n \in \mathbb{N}$) polinom K felett. Ekkor f-nek van felbontási teste, és az f polinom tetszőleges L felbontási testére $[L : K] \leqslant n!$ teljesül.

Tétel (A felbontási test létezése).

Legyen K test, és f n-edfokú ($n \in \mathbb{N}$) polinom K felett. Ekkor f-nek van felbontási teste, és az f polinom tetszőleges L felbontási testére $[L : K] \leqslant n!$ teljesül.

Bizonyítás.

Az állítást az f polinom fokszáma szerinti indukcióval bizonyítjuk. Ha $f^* \leqslant 1$, akkor az állítás nyilvánvalóan teljesül. Tegyük fel, hogy az állítás igaz tetszőleges K testre és tetszőleges K feletti legfeljebb $(n-1)$-edfokú polinomra. Legyen f egy n-edfokú polinom. A továbbiakban a bizonyítás két esetre bomlik aszerint, hogy f reducibilis vagy irreducibilis.

Bizonyítás (folytatás).

1. eset. Ha f reducibilis $K[x]$-ben, akkor $f = gh$ teljesül valamely $g, h \in K[x]$ polinomokra, ahol $1 \leqslant g^* = s,\ h^* = t < n$. Az indukciós feltevés szerint van a K testnek egy olyan L bővítése, amely felbontási teste az g polinomnak K felett és $[L : K] \leqslant s!$. Ekkor

$$g = \lambda(x - \alpha_1) \cdots (x - \alpha_s),$$

ahol $\alpha_1, \ldots, \alpha_s \in L$, $\lambda \in K$ és $L = K(\alpha_1, \ldots, \alpha_s)$. Tekintsük a $h \in K[x] \subseteq L[x]$ polinomot. Szintén az indukciós feltevés szerint van az L testnek egy olyan M bővítése, amely felbontási teste a h polinomnak az L test felett és $[M : L] \leqslant t!$.

Bizonyítás (folytatás).

Ekkor

$$h = \mu(x - \beta_1) \cdots (x - \beta_t),$$

ahol $\beta_1, \ldots, \beta_t \in M$, $\mu \in L$ és $M = L(\beta_1, \ldots, \beta_t)$. Továbbá,

$$f = \lambda\mu(x - \alpha_1) \cdots (x - \alpha_s)(x - \beta_1) \cdots (x - \beta_t)$$

miatt $\lambda\mu \in K$, valamint $M = K(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t)$, azaz M felbontási teste f-nek K felett. Valamint, a Fokszámtétel miatt az

$$[M : K] = [M : L] \cdot [L : K] \leqslant t!s! \leqslant (s + t)! \leqslant n!$$

egyenlőtlenség is teljesül.

Bizonyítás (folytatás).

2. eset. Ha f irreducibilis K felett, akkor tekintsük a K test $L = K[x]/(f)$ bővítését. Tudjuk, hogy $\alpha = x + (f) \in L$ gyöke f-nek, $L = K(\alpha)$ és $[L : K] = n$. A Bézout-tétel szerint $f = (x - \alpha)h$ teljesül valamely $(n-1)$-edfokú $h \in L[x]$ polinomra. Alkalmazzuk az indukciós feltevést h-ra: az L testnek van egy olyan M bővítése, mely felbontási teste h-nak L felett és $[M : L] \leqslant (n-1)!$. Ekkor $h = \mu(x - \beta_1) \cdots (x - \beta_{n-1})$, ahol $\beta_1, \ldots, \beta_{n-1} \in M$, $\mu \in L$ és $M = L(\beta_1, \ldots, \beta_{n-1})$. Ezért azt kapjuk, hogy

$$f = \mu(x - \alpha)(x - \beta_1) \cdots (x - \beta_{n-1})$$

miatt $\mu \in K$, továbbá $M = L(\beta_1, \ldots, \beta_{n-1}) = K(\alpha, \beta_1, \ldots, \beta_{n-1})$, azaz M felbontási teste f-nek K felett. Végül a Fokszámtétel következtében $[M : K] = [M : L] \cdot [L : K] \leqslant (n-1)!n = n!$ is teljesül.

Most pedig azt mutatjuk meg, hogy a felbontási test lényegében egyértelmű. Legyenek K_1, K_2 testek, és $\eta\colon K_1 \to K_2$ izmorfizmus. Tetszőleges $f = \sum_{j=0}^{n} a_j x^j \in K_1[x]$ polinomra legyen

$$\eta_f = \sum_{j=0}^{n} (a_j\eta) x^j \in K_2[x].$$

Egyszerűen igazolható, hogy a $K_1[x] \to K_2[x],\ f \mapsto \eta_f$ leképezés izomorfizmus.

Tétel (A felbontási test egyértelműsége.)

Legyenek K, K' testek, $\eta\colon K \to K'$ izomorfizmus, és $f \in K[x]$ egy n-edfokú polinom ($n \geqslant 1$). Legyenek továbbá rendre L és L' az f és η_f polinomok felbontási testei a K, illetve K' testek felett. Ekkor η kiterjeszthető egy $L \to L'$ izomorfizmussá. Továbbá, az η izomorfizmust legfeljebb $[L : K]$ féleképpen tudjuk kiterjeszteni; a kiterjesztések száma pontosan $[L : K]$, ha η_f gyökei páronként különbözőek L'-ben.

Lemma (Kiterjesztési Lemma).

Legyenek K, K' testek, $\eta\colon K \to K'$ izomorfizmus, és $L : K$, $L' : K'$. Tegyük fel, hogy az $\alpha \in L$ elem algebrai K felett, és legyen $f = m_{\alpha,K} \in K[x]$. Ekkor η pontosan akkor terjeszthető ki egy $\vartheta\colon K(\alpha) \to L'$ injektív homomorfizmussá, ha η_f-nek van gyöke L'-ben, és ebben az esetben η-t annyiféleképpen tudjuk kiterjeszteni ahány gyöke van η_f-nek L'-ben.

A Kiterjesztési Lemma bizonyítása.

Tegyük fel, hogy $\vartheta\colon K(\alpha) \to L'$ injektív homomorfizmus, amely kiterjesztése η-nak. Ekkor

$$\eta_f(\vartheta(\alpha)) = \vartheta(f(\alpha)) = \vartheta(0) = 0,$$

azaz $\vartheta(\alpha) \in L'$ gyöke η_f-nek.

A Kiterjesztési Lemma bizonyítása (folytatás).

Tegyük fel, hogy $\omega \in L'$ gyöke η_f-nek. Tekintsük a

$$\kappa\colon K[x] \to L',\ h \mapsto \eta_h(\omega)$$

homomorfizmust. Mivel $\kappa(f) = \eta_f(\omega) = 0$, ezért $(f) \subseteq \ker(\kappa)$, és így κ indukál egy

$$\widehat{\kappa}\colon K[x]/(f) \to L',\ h + (f) \mapsto \eta_h(\omega)$$

homomorfizmust. Az f polinom irreducibilitása miatt $K[x]/(f)$ test, ezért $\widehat{\kappa}$ injektív homomorfizmus.

A Kiterjesztési Lemma bizonyítása (folytatás).

Legyen

$$\vartheta = \widehat{\kappa} \circ (\widehat{\varepsilon_\alpha})^{-1} \colon K(\alpha) \to L',\ h(\alpha) \mapsto \eta_h(\omega).$$

Ekkor ϑ injektív homomorfizmus, valamint tetszőleges $u \in K$-ra

$$\vartheta(u) = \widehat{\kappa}((\widehat{\varepsilon_\alpha})^{-1}(u)) = \widehat{\kappa}(u + (f)) = \eta_u(\omega) = \eta(u),$$

azaz ϑ kiterjesztése η-nak. Abból a tényből, hogy $K \cup \{\alpha\}$ generálja a $K(\alpha)$ testet következik, hogy a fent definiált ϑ az egyetlen olyan injektív homomorfizmus, amelyre $\vartheta(\alpha) = \omega$ teljesül. Így már az is világos, hogy η annyiféleképpen terjeszthető ki $K(\alpha) \to L'$ injektív homomorfizmussá, ahány gyöke van η_f-nek L'-ben.

Tétel (A felbontási test egyértelműsége.)

Legyenek K, K' testek, $\eta\colon K \to K'$ izomorfizmus, és $f \in K[x]$ egy n-edfokú polinom ($n \geqslant 1$). Legyenek továbbá rendre L és L' az f és η_f polinomok felbontási testei a K, illetve K' testek felett. Ekkor η kiterjeszthető egy $L \to L'$ izomorfizmussá. Továbbá, az η izomorfizmust legfeljebb $[L : K]$ féleképpen tudjuk kiterjeszteni; a kiterjesztések száma pontosan $[L : K]$, ha η_f gyökei páronként különbözőek L'-ben.

Tétel (A felbontási test egyértelműsége.)

Legyenek K, K' testek, $\eta\colon K \to K'$ izomorfizmus, és $f \in K[x]$ egy n-edfokú polinom ($n \geqslant 1$). Legyenek továbbá rendre L és L' az f és η_f polinomok felbontási testei a K, illetve K' testek felett. Ekkor η kiterjeszthető egy $L \to L'$ izomorfizmussá. Továbbá, az η izomorfizmust legfeljebb $[L : K]$ féleképpen tudjuk kiterjeszteni; a kiterjesztések száma pontosan $[L : K]$, ha η_f gyökei páronként különbözőek L'-ben.

Bizonyítás.

Az állítást $[L : K]$-ra vonatkozó indukcióval bizonyítjuk. Ha $[L : K] = 1$, akkor $L = K$ és $f = \lambda(x - \alpha_1) \cdots (x - \alpha_n)$, ahol $\lambda, \alpha_1, \ldots, \alpha_n \in K$. Ekkor $\eta_f = \eta(\lambda)(x - \eta(\alpha_1)) \cdots (x - \eta(\alpha_n))$ teljesül $K'[x]$-ben, így $L' = K'$ és η-nak pontosan egy kiterjesztése van.

Bizonyítás (folytatás).

Tegyük fel, hogy $[L : K] > 1$, azaz f nem bomlik fel lineáris tényezők szorzatára K felett. Legyen g egy legalább elsőfokú irreducibilis tényezője f-nek. Ekkor $g \mid f$ miatt $\eta_g \mid \eta_f$. Az általánosság megszorítása nélkül feltehető, hogy

$$f = \lambda(x-\alpha_1)\cdots(x-\alpha_n), \eta_f = \kappa(x-\omega_1)\cdots(x-\omega_n),$$
$$g = \mu(x-\alpha_1)\cdots(x-\alpha_m), \eta_g = \nu(x-\omega_1)\cdots(x-\omega_m).$$

Legyen $M = K(\alpha_1)$. Mivel g irreducibilis K felett, ezért $m_{\alpha_1,K} = g$, és $[M : K] = g^* = m$. A Kiterjesztési Lemma szerint η-nak pontosan k kiterjesztése van $M \to L'$ injektív homomorfizmussá: $\vartheta_1, \ldots, \vartheta_k$, ahol $k = |\{\omega_1, \ldots, \omega_m\}|$.

Bizonyítás (folytatás).

Világos, hogy L felbontási teste M felett az $f \in M[x]$ polinomnak és L' felbontási teste a $\vartheta_i(M)$ test felett az η_f polinomnak $(1 \leqslant i \leqslant k)$.

Bizonyítás (folytatás).

Világos, hogy L felbontási teste M felett az $f \in M[x]$ polinomnak és L' felbontási teste a $\vartheta_i(M)$ test felett az η_f polinomnak $(1 \leqslant i \leqslant k)$.

Bizonyítás (folytatás).

Világos, hogy L felbontási teste M felett az $f \in M[x]$ polinomnak és L' felbontási teste a $\vartheta_i(M)$ test felett az η_f polinomnak ($1 \leqslant i \leqslant k$). Mivel $[L : M] = [L : K]/[M : K] = [L : K]/m < [L : K]$, ezért az indukciós feltevés alkalmazva azt kapjuk, hogy ϑ_i kiterjeszthető egy $L \to L'$ izomorfizmussá, és ezen kiterjesztések száma $\leqslant [L : M]$ (egyenlőség pontosan akkor van, ha η_f gyökei páronként különbözők L'-ben).

Bizonyítás (folytatás).

Világos, hogy L felbontási teste M felett az $f \in M[x]$ polinomnak és L' felbontási teste a $\vartheta_i(M)$ test felett az η_f polinomnak ($1 \leqslant i \leqslant k$). Mivel $[L : M] = [L : K]/[M : K] = [L : K]/m < [L : K]$, ezért az indukciós feltevés alkalmazva azt kapjuk, hogy ϑ_i kiterjeszthető egy $L \to L'$ izomorfizmussá, és ezen kiterjesztések száma $\leqslant [L : M]$ (egyenlőség pontosan akkor van, ha η_f gyökei páronként különbözők L'-ben). Mivel ezen izomorfizmusok mindegyike az η-nak is kiterjesztése, ezért ezen a módon η-nak legfeljebb $k[L : M] \leqslant m[L : M] = [L : K]$ kiterjesztését kapjuk (pontosan $[L : K]$ kiterjesztést kapunk, ha η_f gyökei páronként különbözők).

Bizonyítás (folytatás).

Világos, hogy L felbontási teste M felett az $f \in M[x]$ polinomnak és L' felbontási teste a $\vartheta_i(M)$ test felett az η_f polinomnak ($1 \leqslant i \leqslant k$). Mivel $[L : M] = [L : K]/[M : K] = [L : K]/m < [L : K]$, ezért az indukciós feltevés alkalmazva azt kapjuk, hogy ϑ_i kiterjeszthető egy $L \to L'$ izomorfizmussá, és ezen kiterjesztések száma $\leqslant [L : M]$ (egyenlőség pontosan akkor van, ha η_f gyökei páronként különbözők L'-ben). Mivel ezen izomorfizmusok mindegyike az η-nak is kiterjesztése, ezért ezen a módon η-nak legfeljebb $k[L : M] \leqslant m[L : M] = [L : K]$ kiterjesztését kapjuk (pontosan $[L : K]$ kiterjesztést kapunk, ha η_f gyökei páronként különbözők). A bizonyítás befejezéséhez csak azt kell meggondolnunk, hogy η-nak más kiterjesztései nem is lehetnek. Tegyük fel, hogy a $\vartheta\colon L \to L'$ izomorfizmus kiterjesztése η-nak. Ekkor $\vartheta|_M$ egy $M \to L'$ injektív homomorfizmus, azaz $\vartheta = \vartheta_i$ valamely i-re ($1 \leqslant i \leqslant k$), és így a ϑ izomorfizmus is a fenti módon keletkezik.

Vizsgáljuk meg azt az esetet, amikor az előző tételben $K = K'$ teljesül, és $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$, és a következőt kapjuk.

Vizsgáljuk meg azt az esetet, amikor az előző tételben $K = K'$ teljesül, és $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$, és a következőt kapjuk.

Következmény.

Legyen K tetszőleges test, $f \in K[x]$, és L, L' az f polinom felbontási testei. Ekkor az L és L' testek izomorfak, sőt olyan $L \to L'$ izomorfizmus is van, amely a $K(\subseteq L, L')$ test elemeit fixen hagyja. Továbbá, pontosan annyi a K test elemeit fixen hagyó $L \to L'$ izomorfizmus van ahány különböző gyöke van f-nek L-ben.