Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. február 16.

Példa: az $f = x^8 + 2 \in \mathbb{Q}[x]$ polinom felbontási teste.

Mivel az f polinom gyökei a következők:

$$\sqrt[8]{-2} = \sqrt[8]{2}\left(\cos\frac{\pi + 2k\pi}{8} + i\sin\frac{\pi + 2k\pi}{8}\right) \quad (k = 0, 1, \ldots, 7),$$

ezért az f polinom L felbontási teste $\mathbb{Q}$ felett a következő:

$$L = \mathbb{Q}(\alpha_0, \ldots, \alpha_7),$$

ahol $\alpha_k = \sqrt[8]{2}\left(\cos\frac{\pi+2k\pi}{8} + i\sin\frac{\pi+2k\pi}{8}\right) \quad (k = 0, 1, \ldots, 7).$

Példa: az $f = x^8 + 2 \in \mathbb{Q}[x]$ polinom felbontási teste.

Mivel az f polinom gyökei a következők:

$$\sqrt[8]{-2} = \sqrt[8]{2}\left(\cos\frac{\pi + 2k\pi}{8} + i\sin\frac{\pi + 2k\pi}{8}\right) \quad (k = 0, 1, \ldots, 7),$$

ezért az f polinom L felbontási teste $\mathbb{Q}$ felett a következő:

$$L = \mathbb{Q}(\alpha_0, \ldots, \alpha_7),$$

ahol $\alpha_k = \sqrt[8]{2}\left(\cos\frac{\pi+2k\pi}{8} + i\sin\frac{\pi+2k\pi}{8}\right) \quad (k = 0, 1, \ldots, 7).$

Most már tudjuk, hogy mennyi az $L : \mathbb{Q}$ bővítés foka!

Példa: az $f = x^8 + 2 \in \mathbb{Q}[x]$ polinom felbontási teste.

Mivel az f polinom gyökei a következők:

$$\sqrt[8]{-2} = \sqrt[8]{2}\left(\cos\frac{\pi + 2k\pi}{8} + i\sin\frac{\pi + 2k\pi}{8}\right) \quad (k = 0, 1, \ldots, 7),$$

ezért az f polinom L felbontási teste $\mathbb{Q}$ felett a következő:

$$L = \mathbb{Q}(\alpha_0, \ldots, \alpha_7),$$

ahol $\alpha_k = \sqrt[8]{2}\left(\cos\frac{\pi+2k\pi}{8} + i\sin\frac{\pi+2k\pi}{8}\right) \quad (k = 0, 1, \ldots, 7).$

Most már tudjuk, hogy mennyi az $L : \mathbb{Q}$ bővítés foka!

Vagy mégsem!?

Mivel α_0 gyöke az $f \in \mathbb{Q}[x]$ irreducibilis polinomnak, ezért $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 8$. A $\mathbb{Q}(\alpha_0)$ test azonban nem felbontási teste f-nek, az f polinom $\mathbb{Q}(\alpha_0)$ feletti felbontása a következő:

$$(x^2 + \alpha_0^2)(x^2 - \alpha_0^5 x - \alpha_0^2)(x^2 + \alpha_0^5 x - \alpha_0^2)(x + \alpha_0)(x - \alpha_0).$$

Mivel α_0 gyöke az $f \in \mathbb{Q}[x]$ irreducibilis polinomnak, ezért $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 8$. A $\mathbb{Q}(\alpha_0)$ test azonban nem felbontási teste f-nek, az f polinom $\mathbb{Q}(\alpha_0)$ feletti felbontása a következő:

$$(x^2 + \alpha_0^2)(x^2 - \alpha_0^5 x - \alpha_0^2)(x^2 + \alpha_0^5 x - \alpha_0^2)(x + \alpha_0)(x - \alpha_0).$$

Felbontási testek.
Példák.

Mivel α_0 gyöke az $f \in \mathbb{Q}[x]$ irreducibilis polinomnak, ezért $[\mathbb{Q}(\alpha_0) : \mathbb{Q}] = 8$. A $\mathbb{Q}(\alpha_0)$ test azonban nem felbontási teste f-nek, az f polinom $\mathbb{Q}(\alpha_0)$ feletti felbontása a következő:

$$(x^2 + \alpha_0^2)(x^2 - \alpha_0^5 x - \alpha_0^2)(x^2 + \alpha_0^5 x - \alpha_0^2)(x + \alpha_0)(x - \alpha_0).$$

Az f polinom a $\mathbb{Q}(\alpha_0, i)$ test felett már lineáris tényezőkre bomlik:

$$\begin{aligned} f = \frac{1}{16} &\cdot (x + \alpha_0)(x - \alpha_0)(x + i\alpha_0)(x - i\alpha_0) \\ &\cdot (2x - \alpha_0^5 - i\alpha_0^5)(2x - \alpha_0^5 + i\alpha_0^5) \\ &\cdot (2x + \alpha_0^5 + i\alpha_0^5)(2x - i\alpha_0^5 + \alpha_0^5). \end{aligned}$$

Az f polinom felbontási teste $L = \mathbb{Q}(\alpha_0, i)$ és $[L : \mathbb{Q}] = 16$.

Test algebrai lezártja

Definíció: alegbrailag zárt test, algebrai lezárt.

Azt mondjuk, hogy az L test **algebrailag zárt**, ha bármely $f \in L[x]$ polinomnak van gyöke L-ben.
A K test L testbővítése K **algebrai lezártja**, ha az $L : K$ bővítés algebrai és az L test algebrailag zárt.

Test algebrai lezártja

Definíció: alegbrailag zárt test, algebrai lezárt.

Azt mondjuk, hogy az L test **algebrailag zárt**, ha bármely $f \in L[x]$ polinomnak van gyöke L-ben.
A K test L testbővítése K **algebrai lezártja**, ha az $L : K$ bővítés algebrai és az L test algebrailag zárt.

Példa.

Az Algebra Alaptétele éppen azt állítja, hogy a komlex számok $\mathbb{C}$ teste algebrailag zárt, azonban $\mathbb{C}$ nem algebrai lezártja $\mathbb{Q}$-nak, mivel $\mathbb{C}$ nem minden eleme algebrai $\mathbb{Q}$ felett.

Test algebrai lezártja

Tétel.

Tetszőleges $L : K$ testbővítésre ekvivalensek az alábbi állítások.

Test algebrai lezártja

Tétel.

Tetszőleges $L : K$ testbővítésre ekvivalensek az alábbi állítások.

(1) L algebrai lezártja K-nak.

Test algebrai lezártja

Tétel.

Tetszőleges $L : K$ testbővítésre ekvivalensek az alábbi állítások.

(1) L algebrai lezártja K-nak.

(2) az $L : K$ bővítés algebrai és minden irreducibilis $K[x]$-beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$-ben.

Test algebrai lezártja

Tétel.

Tetszőleges $L : K$ testbővítésre ekvivalensek az alábbi állítások.

(1) L algebrai lezártja K-nak.

(2) az $L : K$ bővítés algebrai és minden irreducibilis $K[x]$-beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$-ben.

(3) az $L : K$ bővítés algebrai, és tetszőleges L' testre, ha az $L' : L$ testbővítés algebrai, akkor $L' = L$.

Test algebrai lezártja

Tétel.

Tetszőleges $L : K$ testbővítésre ekvivalensek az alábbi állítások.

(1) L algebrai lezártja K-nak.

(2) az $L : K$ bővítés algebrai és minden irreducibilis $K[x]$-beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$-ben.

(3) az $L : K$ bővítés algebrai, és tetszőleges L' testre, ha az $L' : L$ testbővítés algebrai, akkor $L' = L$.

Bizonyítás.

(1) $\Longrightarrow$ (2): az f irreducibilis polinom fokszámára vonatkozó indukcióval az állítás egyszerűen belátható.

Bizonyítás (folytatás).

(2) $\Longrightarrow$ (3): legyen α az L' test tetszőleges eleme. Mivel az $L : K$ és $L' : L$ bővítések is algebraiak, ezért az $L' : K$ bővítés is algebrai, így α algebrai elem K felett, melynek minimálpolinomja $m_{\alpha,K}$ irreducibilis polinom $K[x]$-ben. Ekkor a (2) pont következtében $m_{\alpha,K}$ lineáris tényezőkre bomlik L felett:

$$m_{\alpha,K} = \lambda(x - \alpha_1) \cdots (x - \alpha_n),$$

ahol $n = \mathrm{gr}_K(\alpha)$, $\lambda \in K$ és $\alpha_1, \ldots, \alpha_n \in L$. Mivel α is gyöke $m_{\alpha,K}$-nak, ezért valamely i-re $(1 \leqslant i \leqslant n)$ $\alpha = \alpha_i \in L$. Azaz $L' = L$.

Test algebrai lezártja

Bizonyítás (folytatás).

(3) $\Longrightarrow$ (1): csak azt kell megmutatni, hogy L algebrailag zárt. Legyen $f \in L[x]$ tetszőleges legalább elsőfokú polinom, és legyen f_1 az f polinom egy irreducibilis tényezője. Tekintsük az L test $L' = L[x]/(f_1)$ bővítését. Az L' testben f_1-nek, és így f-nek is van gyöke ($\alpha = x + (f_1)$). Mivel az $L' : L$ bővítés algebrai, ezért (3) szerint $L' = L$, ami éppen azt jelenti, hogy f-nek L-ben is van gyöke.

Test algebrai lezártja

Bizonyítás (folytatás).

(3) $\Longrightarrow$ (1): csak azt kell megmutatni, hogy L algebrailag zárt. Legyen $f \in L[x]$ tetszőleges legalább elsőfokú polinom, és legyen f_1 az f polinom egy irreducibilis tényezője. Tekintsük az L test $L' = L[x]/(f_1)$ bővítését. Az L' testben f_1-nek, és így f-nek is van gyöke ($\alpha = x + (f_1)$). Mivel az $L' : L$ bővítés algebrai, ezért (3) szerint $L' = L$, ami éppen azt jelenti, hogy f-nek L-ben is van gyöke.

Következmény.

Legyen L algebrailag zárt test, és $L : K$ tetszőleges testbővítés. Legyen L_a mindazon L-beli elemek halmaza, amelyek algebraiak K felett. Ekkor az $L_a : K$ testbővítés algebrai lezártja K-nak.

Test algebrai lezártja

Tétel.

Legyen K test. Ekkor van olyan L test, amelyre $L : K$ algebrai lezártja K-nak.

Test algebrai lezártja

Tétel.

Legyen K test. Ekkor van olyan L test, amelyre $L : K$ algebrai lezártja K-nak.

Bizonyítás.

Legyen $U = \{(f, j) \mid f \in K[x],\ f^* \geqslant 1,\ f$ főpolinom és $1 \leqslant j \leqslant f^*\}$, valamint legyen $X_U = \{x_j(f) \mid (f, j) \in U\}$. Tegyük fel, hogy $f \in K[x]$ egy n-edfokú főpolinom. Írjuk fel f-et

$$f = x^n + \sum_{k=1}^{n} (-1)^k a_k(f) x^{n-k}$$

alakban.

Bizonyítás (folytatás).

Legyen

$$\begin{aligned} g(f) &= (x - x_1(f)) \cdots (x - x_n(f)) \\ &= x^n + \sum_{k=1}^{n} (-1)^k s_k(f) x^{n-k} \in K[X_U][x], \end{aligned}$$

ahol $s_k(f) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1}(f) \cdots x_{i_k}(f)$ $(k = 1, \ldots, n)$. Továbbá jelölje $\mathcal{I}$ a $K[X_U]$ polinomgyűrű $t_i(f) := s_i(f) - a_i(f)$ alakú elemei által generált ideált, ahol $(f, i) \in U$.

Bizonyítás (folytatás): $\mathcal{I}$ valódi ideál.

Tegyük fel, hogy $\mathcal{I}$ nem valódi ideálja $K[X_U]$-nak, azaz $1 \in \mathcal{I}$. Ekkor van olyan $N \in \mathbb{N}$, valamint vannak olyan $r_1, \ldots, r_N \in K[X_U]$ elemek, $f_1, \ldots, f_N \in K[x]$ legalább elsőfokú főpolinomok és $1 \leqslant i_k \leqslant f_k^*$ $(k = 1, \ldots, N)$, amelyekre

$$1 = r_1 t_{i_1}(f_1) + \cdots + r_N t_{i_N}(f_N)$$

teljesül. Legyen a $h = f_1 \cdots f_N \in K[x]$ polinom felbontási teste K felett L, valamint

$$f_k = (x - \alpha_1(k)) \cdots (x - \alpha_{n_k}(k)),$$

ahol $n_k = f_k^*$ és $k = 1, \ldots, N$.

Bizonyítás (folytatás): $\mathcal{I}$ valódi ideál.

Tekintsük az alábbiakban definiált $E\colon K[X_U] \to L$ leképezést:

$$E(x_i(f)) = \begin{cases} \alpha_i(k), & \text{ha } f = f_k \text{ és } 1 \leqslant i \leqslant f_k^*, \\ 0, & \text{különben.} \end{cases}$$

Ekkor

$$\begin{aligned} E(s_j(f_k)) &= E\left(\sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n_k} x_{i_1}(f_k) \cdots x_{i_j}(f_k) \right) \\ &= \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n_k} \alpha_{i_1}(k) \cdots \alpha_{i_j}(k) \\ &= a_j(f_k). \end{aligned}$$

Bizonyítás (folytatás): $\mathcal{I}$ valódi ideál.

Így $E(t_j(f_k)) = E(s_j(f_k) - a_j(f_k)) = E(s_j(f_k)) - E(a_j(k)) = 0$ teljesül tetszőleges j-re és k-ra ($1 \leqslant j \leqslant n_k$, $1 \leqslant k \leqslant N$). Ekkor a következő ellentmondást kapjuk:

$$\begin{aligned} 1 &= E(1) \\ &= E(r_1 t_{i_1}(f_1) + \cdots + r_N t_{i_N}(f_N)) \\ &= E(r_1)E(t_{i_1}(f_1)) + \cdots + E(r_N)E(t_{i_N}(f_N)) \\ &= 0. \end{aligned}$$

Ezzel igazoltuk, hogy $\mathcal{I}$ valódi ideálja $K[X_U]$-nak. Legyen $\mathcal{J}$ egy $\mathcal{I}$-t tartalmazó maximális ideálja $K[X_U]$-nak. Ekkor $M = K[X_U]/\mathcal{J}$ test.

Bizonyítás (folytatás).

Tekintsük a $\mathfrak{j} = \mathfrak{q} \circ \mathfrak{i}$ leképezést, ahol $\mathfrak{i}\colon K \to K[X_U]$ a természetes homomorfizmus és $\mathfrak{q}\colon K[X_U] \to M,\ f \mapsto f + \mathcal{J}$. Ekkor $\mathfrak{j}\colon K \to M$ injektív homomorfizmus, és így az M test bővítése $\mathfrak{j}(K)$-nak. Tetszőleges $(f, j) \in U$-ra legyen $\beta_j(f) = \mathfrak{q}(x_j(f))$.
Tegyük fel, hogy

$$f = x^n + \sum_{k=1}^{n} (-1)^k a_k(f) x^{n-k}$$

egy nemkonstans $K[x]$-beli főpolinom. Ekkor
$\mathfrak{j}_f = x^n + \sum_{k=1}^{n} (-1)^k \mathfrak{j}(a_k(f)) x^{n-k}$ az f-hez tartozó polinom $M[x]$-ben.
Mivel $s_k(f) - \mathfrak{i}(a_k(f)) = t_k(f) \in \mathcal{I} \subseteq \mathcal{J}$, ezért
$\mathfrak{j}(a_k(f)) = \mathfrak{q}(\mathfrak{i}(a_k(f))) = \mathfrak{q}(s_k(f))$.

Bizonyítás (folytatás).

Így azt kapjuk, hogy

$$\begin{aligned}
\mathfrak{j}_f &= x^n + \sum_{k=1}^{n} (-1)^k \mathfrak{j}(a_k(f)) x^{n-k} \\
&= x^n + \sum_{k=1}^{n} (-1)^k \mathfrak{q}(s_k(f)) x^{n-k} \\
&= \mathfrak{q}(x^n + \sum_{k=1}^{n} (-1)^k s_k(f) x^{n-k}) \\
&= \mathfrak{q}((x - x_1(f)) \cdots (x - x_n(f))) \\
&= (x - \beta_1(f)) \cdots (x - \beta_n(f)),
\end{aligned}$$

Test algebrai lezártja

Bizonyítás (folytatás).

azaz $\mathfrak{j}_f$ elsőfokú polinomok szorzatára bomlik M felett, és $\beta_k(f)$ algebrai $\mathfrak{j}(K)$ felett. Mivel a $\beta_k(f)$ elemek generálják M-et K felett, ezért az $M : K$ bővítés algebrai. Ez pedig már maga után vonja, hogy M algebrai lezártja K-nak.

Test algebrai lezártja

Tétel.

Legyenek K, K' és L testek. Tegyük fel, hogy van egy $\eta\colon K \to K'$ injektív homomorfizmus, $L : K$ algebrai bővítés és K' algebrailag zárt. Ekkor van olyan $\psi\colon L \to K'$ injektív homomorfizmus, amely kiterjesztése η-nak, azaz, amelyre $\psi|_K = \eta$ teljesül.

Test algebrai lezártja

Tétel.

Legyenek K, K' és L testek. Tegyük fel, hogy van egy $\eta\colon K \to K'$ injektív homomorfizmus, $L : K$ algebrai bővítés és K' algebrailag zárt. Ekkor van olyan $\psi\colon L \to K'$ injektív homomorfizmus, amely kiterjesztése η-nak, azaz, amelyre $\psi|_K = \eta$ teljesül.

Bizonyítás.

Legyen S azon (M, ϑ) párok halmaza, amelyekre M az L test K-t tartalmazó részteste és $\vartheta\colon M \to K'$ olyan injektív homomorfizmus, amely kiterjesztése η-nak.

Test algebrai lezártja

Bizonyítás.

Definiáljuk S-en a $\leqslant$ relációt a következőképpen: $(M_1, \vartheta_1), (M_2, \vartheta_2) \in S$,

$$(M_1, \vartheta_1) \leqslant (M_2, \vartheta_2) \iff M_1 \subseteq M_2 \text{ és } \vartheta_2|_K = \vartheta_1.$$

Egyszerűen látható, hogy $\leqslant$ részbenrendezés az S (nemüres) halmazon. Tegyük fel, hogy $\mathcal{C} \subseteq \mathcal{S}$ lánc. Legyen $N = \bigcup_{(M,\vartheta)\in\mathcal{C}} M$. Ha $n \in N$, akkor van olyan $(M, \vartheta) \in \mathcal{C}$, amelyre $n \in M$ teljesül. A $\varphi\colon N \to K'$ leképezést definiáljuk úgy, hogy ekkor $\varphi(n) = \vartheta(n)$ teljesüljön. Ekkor φ jóldefiniált és $(N, \varphi) \in S$ felső korlátja $\mathcal{C}$-nek. Így a Zorn-lemma szerint S-ben van maximális elem: (M, ϑ). Meg fogjuk mutatni, hogy $M = L$.

Test algebrai lezártja

Bizonyítás.

Tegyük fel, hogy $M \neq L$, és legyen $\alpha \in L \setminus M$. Az α elem algebrai M felett, melynek minimálpolinomja legyen m. Mivel K' algebrailag zárt, ϑ_m elsőfokú polinom szorzatára bomlik K' felett:

$$\vartheta_m = (x - \beta_1) \cdots (x - \beta_r).$$

Mivel $\vartheta_m(\beta_1) = 0$, a Kiterjesztési Lemma szerint van olyan injektív $\vartheta_1 \colon M(\alpha) \to K'$ homomorfizmus, amelyre $\vartheta_1|_M = \vartheta$. Ez azonban ellentmond (M, ϑ) maximalitásának.

Test algebrai lezártja

Tétel.

Legyen K tetszőleges test. Ha $(\mathfrak{i}, K, L)$ és $(\mathfrak{i}', K, L')$ is algebrai lezártja K-nak, akkor van olyan $\mathfrak{j}\colon L \to L'$ izomorfizmus, amelyre $\mathfrak{i}' = \mathfrak{j}\mathfrak{i}$ teljesül.

Test algebrai lezártja

Tétel.

Legyen K tetszőleges test. Ha $(\mathfrak{i}, K, L)$ és $(\mathfrak{i}', K, L')$ is algebrai lezártja K-nak, akkor van olyan $\mathfrak{j}\colon L \to L'$ izomorfizmus, amelyre $\mathfrak{i}' = \mathfrak{j}\mathfrak{i}$ teljesül.

Bizonyítás.

Mivel $\mathfrak{i}'\colon K \to L'$ injektív homomorfizmus, $L : K$ algebrai bővítés és L' algebrailag zárt, ezért az előző tétel szerint van olyan $\mathfrak{j}\colon L \to L'$ injektív homomorfizmus, amelyre $\mathfrak{j}|_K = \mathfrak{i}'$, azaz $\mathfrak{i}' = \mathfrak{j}\mathfrak{i}$.
Legyen $f \in K[x]$ irreducibilis polinom. Ekkor $\mathfrak{i}_f$ lineáris tényezőkre bomlik L felett, illetve $\mathfrak{i}'_f$ lineáris tényezőkre bomlik $\mathfrak{j}(L)$ felett. Mivel $(\mathfrak{i}', K, \mathfrak{j}(L))$ algebrai bővítés, $(\mathfrak{i}', K, \mathfrak{j}(L))$ algebrai lezártja K-nak. Az $L' : \mathfrak{j}(L)$ bővítés algebrai bővítés, mivel $(\mathfrak{i}', K, L')$ az. Így azonban $L' = \mathfrak{j}(L)$ adódik.