K-homomorfizmusok, szeparábilis bővítések, Galois-elmélet

Az alábbi jegyzetben bizonyítás nélkül felhasználjuk, hogy minden K testnek létezik $\overline{K}$ algebrai lezártja. Valójában annyi is elég, hogy minden test beágyazható algebrailag zárt testbe. Ez nem fedi le teljesen az előadás anyagát, mert azokat a részeket, melyek megegyeznek a [1]-beli felépítéssel, kihagytam.

1. K-homomorfizmusok, szeparábilis bővítések

1.1. Definíció. *Legyen K egy test, és $K \leq L$, illetve $K \leq L$ két bővítése K-nak. Ekkor K-feletti relatív homomorfizmusnak (röviden K-homomorfizmusnak) nevezünk egy $\tau\colon L \to M$ testhomomorfizmust, melyre $\tau_{|K} = \mathrm{id}_K$. Egy ilyen K-homomorfizmust testbővítések izomorfizmusának nevezünk, ha bijektív.*

Megjegyzés: a testhomomorfizmus megtartja a testnek a 0-változós műveleteit (konstansok kijelölése) is, azaz $\tau(1) = 1$ mindig. Speciálisan minden τ testhomomorfizmus *injektív*, hiszen $1 \notin \mathrm{Ker}(\tau) \lhd L_1$ egy ideál, és L_1-nek csak két ideálja van: $\{0\}$ és L_1.

1.2. Példa. *1.* $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{\mathrm{id}, \bar{\cdot}\}$.

2. $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{2})| = 2$.

3. $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})| = 1$, *de* $|\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})| = 3$.

Megjegyzés: $\mathrm{Hom}_K(L_1, L_2)$ csak egy halmaz, mindenféle extra struktúra nélkül.

1.3. Lemma. *Legyen $\tau \in \mathrm{Hom}_K(L_1, L_2)$ egy K-homomorfizmus, $\alpha \in L_1$, $f(x) \in K[x]$. Ekkor $\tau(f(\alpha)) = f(\tau(\alpha))$.*

Bizonyítás. Legyen $f(x) = a_0 + a_1 x + \ldots a_n x^n$, ekkor $\tau(f(\alpha)) = \tau(a_0 + a_1\alpha + \cdots + a_n\alpha^n) = \tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_n)\tau(\alpha)^n) = a_0 + a_1\tau(\alpha) + \cdots + a_n\tau(\alpha)^n = f(\tau(\alpha))$, hiszen τ egy testhomomorfizmus és a K elemein identikus. □

A következő állítás, és annak egy későbbi általánosítása kulcsfontosságú a felépítésünkben. Ez lényegében a 6.4.7-es állítás [1]-ben.

1.4. Állítás. *Legyen $K \leq K(\alpha)$ és $K \leq L$ két bővítés, α algebrai K felett, $m_\alpha(x) \in K[x]$ a minimálpolinomja. Ekkor a*

$$\begin{array}{rcl} \mathrm{Hom}_K(K(\alpha), L) & \to & \{\beta \in L\colon m_\alpha(\beta) = 0\} \\ \tau & \mapsto & \tau(\alpha) \end{array}$$

leképezés egy bijekció. Speciálisan $|\mathrm{Hom}_K(K(\alpha), L)| \leq \deg(m_\alpha) = |K(\alpha) : K|$.

Bizonyítás. A fenti Lemma miatt minden $\tau \in \mathrm{Hom}_K(K(\alpha), L)$-re $\tau(\alpha)$ gyöke $m_\alpha(x)$-nek, tehát tényleg értelmes a leképezés. Azt kell belátnunk, hogy injektív és szürjektív:

Injektivitás: $K(\alpha)$ minden eleme előáll $g(\alpha)$ alakban, ahol $g(x) \in K[x]$ polinom. Ha $\tau_1(\alpha) = \tau_2(\alpha)$, akkor a fenti Lemma miatt $\tau_1(g(\alpha)) = g(\tau_1(\alpha)) = g(\tau_2(\alpha)) = \tau_2(g(\alpha))$, tehát $\tau_1 = \tau_2$.

Szürjektivitás: Legyen $\beta \in L$ olyan, amire $m_\alpha(\beta) = 0$. Vegyük észre, hogy $K(\alpha) \cong K[x]/(m_\alpha(x))$. A β behelyettesítése egy $\varphi_\beta\colon K[x] \to L$ $(f(x) \mapsto f(\beta))$ homomorfizmust ad. Mivel $m_\alpha(\beta) = 0$, ezért $m_\alpha(x) \in \mathrm{Ker}(\varphi_\beta)$. Továbbá $(m_\alpha(x))$ egy maximális ideál $K[x]$-ben (és $1 \notin \mathrm{Ker}(\varphi_\beta)$), tehát $(m_\alpha(x)) = \mathrm{Ker}(\varphi_\beta)$. A homomorfizmustétel szerint $\mathrm{Im}(\varphi_\beta) \cong K[x]/(m_\alpha(x)) \cong K(\alpha)$, és ennél az izomorfizmusnál $\beta \in \mathrm{Im}(\varphi_\beta)$ éppen $x + (m_\alpha(x)) \in K[x]/(m_\alpha(x))$-nek, és így $\alpha \in K(\alpha)$-nak felel meg, tehát kapunk egy olyan K-homomorfizmust $K(\alpha)$-ból $\mathrm{Im}(\varphi_\beta) \leq L_1$-be, aminél α képe éppen β. □

1.5. Definíció. *Egy $\alpha (\in M \geq K)$ algebrai elem egy $K \leq L$ bővítésbeli K-feletti konjugáltjainak azokat a $\beta \in L$ elemeket nevezzük, melyek gyökei α minimálpolinomjának. Ezek a fenti tétel szerint nem mások, mint α lehetséges képei a $\tau \in \mathrm{Hom}_K(K(\alpha), L)$ homomorfizmusoknál.*

1.6. Definíció. *Legyen K egy test, $K \leq L$ egy bővebb test. Egy $\alpha \in L$ algebrai elemet szeparábilisnak nevezünk (K felett), ha K feletti m_α minimálpolinomjának nincs többszörös gyöke.*

1.7. Állítás. *Egy $\alpha \in \overline{K}$ elem pontosan akkor szeparábilis K felett, ha $|\mathrm{Hom}_K(K(\alpha), \overline{K})| = |K(\alpha) : K|$.*

Bizonyítás. Triviális az 1.4-es Állításból: m_α-nak pontosan akkor van $\deg(m_\alpha)$ darab különböző gyöke $\overline{K}$-ban, ha nincs többszörös gyöke. □

Megjegyzés: α szeparábilitásához elég, ha van olyan $0 \neq f(x) \in K[x]$ polinom, aminek nincs többszörös gyöke és $f(\alpha) = 0$. Valóban, ekkor $m_\alpha \mid f$-nek sincs többszörös gyöke.

1.8. Következmény. *$K \leq L \leq M$ testek, $\alpha \in M$ szeparábilis K felett $\Rightarrow$ L felett is.*

Bizonyítás. A fenti megjegyzést alkalmazzuk. A K feletti minimálpolinomnak nincs többszörös gyöke, és α gyöke. □

A következő állítás az 1.4-es Állításnak az általánosítása. Ez lényegében a 6.4.8-as tétel [1]-ben.

1.9. Állítás. *Legyenek $K \leq L \leq L(\alpha)$ és $K \leq M$ testbővítések, ahol α algebrai L fölött. Legyen $m_\alpha(x) \in L[x]$ az α minimálpolinomja L felett. Ekkor minden $\tau \in \mathrm{Hom}_K(L, M)$-re a*

$$\begin{array}{rcl} \{\rho \in \mathrm{Hom}_K(L(\alpha), M) \mid \rho_{|L} = \tau\} & \to & \{\beta \in M\colon \tau(m_\alpha)(\beta) = 0\} \\ \rho & \mapsto & \rho(\alpha) \end{array}$$

leképezés egy bijekció. Itt $\tau(m_\alpha)(x) \in \tau(L)[x] \leq M[x]$ az a polinom, amelyet úgy kapunk, hogy m_α együtthatóira ráalkalmazzuk τ-t.

Bizonyítás. A bizonyítás teljesen analóg az 1.4-es Állítás bizonyításához. Először azt látjuk be, hogy $\rho(\alpha)$ valóban gyöke $\tau(m_\alpha)$-nak. Ehhez legyen $m_\alpha(x) = a_0 + a_1 x + \ldots x^n$ és alkalmazzuk ρ-t az $m_\alpha(\alpha) = 0$ azonosságra: $0 = \rho(a_0 + \cdots + \alpha^n) = \rho(a_0) + \cdots + \rho(\alpha)^n = \tau(a_0) + \cdots + \rho(\alpha)^n = \tau(m_\alpha)(\rho(\alpha))$, hiszen $\rho(a_i) = \tau(a_i)$ mivel $a_i \in L$ és $\rho_{|L} = \tau$.

Injektivitás: ha $\rho_{1|L} = \tau = \rho_{2|L}$ és $\rho_1(\alpha) = \rho_2(\alpha)$, akkor ρ_1 és ρ_2 megegyeznek $L(\alpha)$-n is.

Szürjektivitás: vegyük észre, hogy $\tau(m_\alpha) \in \tau(L)[x]$ is irreducibilis polinom, hiszen a $\tau\colon L[x] \to \tau(L)[x]$ egy izomorfizmus. Tehát ha β gyöke $\tau(m_\alpha)$-nak, akkor ez is a minimálpolinomja. Így a kívánt ρ leképezés nem más, mint $\rho := \varphi_\beta \circ \tau \circ \varphi_\alpha^{-1}$, ahol $\varphi_\beta\colon \tau(L)[x]/(\tau(m_\alpha)(x)) \to$

$\tau(L)(\beta) \leq M$ homomorfizmus, amit a β behelyettesítése indukál, $\varphi_\alpha\colon L[x]/(m_\alpha(x)) \to L(\alpha)$ izomorfizmus, amit az α behelyettesítése indukál, τ pedig a $\tau\colon L[x]/(m_\alpha(x)) \to \tau(L)[x]/(\tau(m_\alpha)(x))$ izomorfizmus. □

1.10. Következmény. *Legyenek $K \leq L$ és $K \leq M$ bővítések. Ekkor $|\mathrm{Hom}_K(L, M)| \leq |L : K|$.*

Bizonyítás. Ha $|L : K| = \infty$, akkor az állítás üres. Egyébként legyen $d = |L : K|$ és $L = K(\alpha_1, \ldots, \alpha_n)$. Indukcióval bizonyítunk n-szerint. $n = 1$-re az állítás az 1.4-es Állítás speciális esete. Legyen $n > 1$ és $L_0 = K(\alpha_1, \ldots, \alpha_{n-1})$. Ekkor az indukciós feltevés miatt tetszőleges $\rho \in \mathrm{Hom}_K(L, M)$-re ρ megszorítása L_0-ra legfeljebb $|L_0 : K|$-féle lehet. Továbbá adott $\tau = \rho_{|L_0}$-ra a 1.9-as Állítás miatt ρ csak $|L(\alpha) : L|$-féle lehet. Az állítás a fokszámtételből következik. □

1.11. Következmény. *Legyen $K \leq L$, és $\alpha \in L$ szeparábilis. Ekkor $K(\alpha)$ minden eleme szeparábilis.*

Bizonyítás. Legyen $\beta \in K(\alpha)$. Ekkor α szeparábilis $K(\beta)$ fölött is az 1.8-as Következmény miatt. Tehát adott $\tau \in \mathrm{Hom}_K(K(\beta), \overline{K})$-ra τ éppen $|K(\alpha) : K(\beta)|$-féleképpen terjed ki $\rho\colon K(\alpha) \to \overline{K}$ K-homomorfizmussá. Ezért $|K(\alpha) : K| = |\mathrm{Hom}_K(K(\alpha), \overline{K})| = |\mathrm{Hom}_K(K(\beta), \overline{K})| \cdot |K(\alpha) : K(\beta)|$. Az állítás egyszerű osztással következik a fokszámtételből. □

1.12. Definíció. *Egy (véges) L/K bővítés szeparábilis, ha L minden eleme szeparábilis K felett.*

Tehát a fenti következmény szerint α pontosan akkor szeparábilis K felett, ha a $K(\alpha)/K$ bővítés szeparábilis.

1.13. Állítás. *Az L/K véges bővítés pontosan akkor szeparábilis, ha $|\mathrm{Hom}_K(L, \overline{K})| = |L : K|$.*

Bizonyítás. Ha $|\mathrm{Hom}_K(L, \overline{K})| = |L : K|$ és $\alpha \in L$, akkor adott $\tau \in \mathrm{Hom}_K(K(\alpha), \overline{K})$-ra τ a 1.10-es Következmény miatt legfeljebb $|L : K(\alpha)|$-féleképpen terjed ki $L \to \overline{K}$ K-homomorfizmussá. Mivel $|\mathrm{Hom}_K(L, \overline{K})| = |L : K|$, ezért legalább $|L : K|/|L : K(\alpha)| = |K(\alpha) : K|$ darab ilyen τ-nak kell lennie, tehát az állítás következik az 1.4-es Állításból.

Visszafelé, ha L/K szeparábilis, akkor $L = K(\alpha_1, \ldots, \alpha_n)$, ahol az α_i-k szeparábilisek K felett. Ha $n = 1$, akkor az állítás következik az 1.4-es Állításból. Legyen $L_0 = K(\alpha_1, \ldots, \alpha_{n-1})$. Indukcióval ($n$ szerint) feltehetjük, hogy $|\mathrm{Hom}_K(L_0, \overline{K})| = |L_0 : K|$. Jelöljük $m_{\alpha_n}(x)$-szel α_n L_0 feletti minimálpolinomját, és legyen $\tau \in \mathrm{Hom}_K(L_0, \overline{K})$ tetszőleges. Mivel α_n szeparábilis (K fölött a feltevés szerint, így L_0 fölött is az 1.8-as Következmény miatt), és $\overline{K}$ algebrailag zárt, ezért $\tau(m_{\alpha_n})(x)$-nek pontosan $\deg(\tau(m_{\alpha_n})) = \deg(m_{\alpha_n}) = |L : L_0|$ darab gyöke van $\overline{K}$-ban. Tehát az 1.9-es Állítás szerint τ pontosan $|L : L_0|$-féleképpen terjed ki $\rho\colon L \to \overline{K}$ K-homomorfizmussá. Így $|\mathrm{Hom}_K(L, \overline{K})| = |L : L_0||\mathrm{Hom}_K(L_0, \overline{K})| = |L : L_0| \cdot |L_0 : K| = |L : K|$. □

1.14. Állítás. *Legyen $K \leq L \leq M$ véges bővítések egy lánca. M/K akkor és csak akkor szeparábilis, ha L/K és M/L szeparábilis. Speciálisan ha $K \leq M$ tetszőleges bővítés, akkor M azon elemei, melyek szeparábilisek K felett, résztestet alkotnak.*

Bizonyítás. Először belátjuk, hogy ha M/L és L/K szeparábilis, akkor M/K is az. Ehhez legyen $\beta \in M$ tetszőleges, és $m_\beta(x) \in L[x]$ a minimálpolinomja. Ekkor az 1.9-es Állítás miatt minden $\tau \in \mathrm{Hom}_K(L, \overline{K})$ pontosan annyiféleképpen terjed ki $L(\beta)$-ra, ahány gyöke van $\tau(m_\beta)$-nak $\overline{K}$-ban. Mivel M/L szeparábilis, ezért m_β-nak nincsenek többszörös gyökei, így $\tau(m_\beta)$-nak sincsenek. Tehát $\tau(m_\beta)$-nak pontosan $\deg(\tau(m_\beta)) = \deg(m_\beta) = |L(\beta) : L|$ darab gyöke van $\overline{K}$-ban. Így $|\mathrm{Hom}_K(L(\beta), \overline{K})| = |L(\beta) : L| \cdot |\mathrm{Hom}_K(L, \overline{K})| = |L(\beta) : L| \cdot |L : K| = |L(\beta) : K|$, hiszen L/K szeparábilis.

Visszafelé ha M/K szeparábilis, akkor az 1.10-es Következmény szerint $|\mathrm{Hom}_K(L, \overline{K})| \leq |L : K|$, és $|\mathrm{Hom}_L(M, \overline{L})| \leq |M : L|$. Feltehetjük, hogy $L \leq \overline{K}$, és azt is, hogy $\overline{L} = \overline{K}$. Viszont adott (fix) $\tau \in \mathrm{Hom}_K(L, \overline{K})$-ra L-et azonosíthatjuk $\tau(L)$-lel, tehát τ pontosan annyiféleképpen terjed ki egy $\rho\colon M \to \overline{K}$ K-homomorfizmussá, amennyi eleme van $\mathrm{Hom}_L(M, \overline{L})$-nak. Azt kaptuk, hogy $|M : K| = |\mathrm{Hom}_K(M, \overline{K})| = |\mathrm{Hom}_K(L, \overline{K})| \cdot |\mathrm{Hom}_L(M, \overline{L})| \leq |L : K| \cdot |M : L| = |M : K|$, azaz végig egyenlőség van. Speciálisan $|\mathrm{Hom}_K(L, \overline{K})| = |L : K|$ és $|\mathrm{Hom}_L(M, \overline{L})| = |M : L|$, másszóval mindkettő szeparábilis.

A másik állításhoz legyen $\alpha, \beta \in M$ szeparábilis K fölött. Ekkor $K(\alpha)(\beta)$ is szeparábilis az első állítás szerint K fölött. Tehát minden eleme szeparábilis, speciálisan $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is. □

A következő tétel a [1] 6.3.8-as (és a 6.3.11-es) tétel általánosítása.

1.15. Tétel. *Minden véges szeparábilis bővítés egyszerű, azaz minden L/K véges szeparábilis bővítésre van olyan $\alpha \in L$, melyre $L = K(\alpha)$.*

Bizonyítás. Az állítást csak akkor bizonyítjuk, ha K végtelen. Ha K véges és $\alpha \in L^\times$ a multiplikatív csoportnak egy generátoreleme, akkor $L = K(\alpha)$.

Legyen $L = K(\alpha_1, \ldots, \alpha_n)$, $|L : K| = d$ és $\mathrm{Hom}_K(L, \overline{K}) = \{\tau_1, \ldots, \tau_d\}$ (lsd. 1.13-as Állítás). Ha találunk olyan $\alpha \in L$-et, melyre a $\tau_1(\alpha), \ldots, \tau_d(\alpha) \in \overline{K}$ elemek mind különbözők, akkor készen vagyunk: Valóban, ha $m_\alpha(x) \in K[x]$-szel jelöljük α minimálpolinomját, akkor $\tau_1(\alpha), \ldots, \tau_d(\alpha)$ mind gyöke m_α-nak, speciálisan $|K(\alpha) : K| = \deg(m_\alpha) \geq d = |L : K|$, így $L = K(\alpha)$, hiszen $K(\alpha) \leq L$.

Az α-t $\alpha = \sum_{i=1}^n \alpha_i \beta^i$ alakban keressük, ahol $\beta \in K$. Legyen $f(x) = \sum_{i=1}^n \alpha_i x^i \in L[x]$ polinom. Ha $1 \leq j \neq k \leq d$, akkor nem lehet, hogy minden $i = 1, \ldots, n$-re $\tau_j(\alpha_i) = \tau_k(\alpha_i)$, hiszen akkor τ_j és τ_k az α_i-k által generált testen, azaz L-en is megegyezne, holott különbözők. Tehát a $\tau_j(f)(x) = \sum_{i=1}^n \tau_j(\alpha_i) x^i \in \overline{K}[x]$ polinomok ($j = 1, \ldots, d$) páronként különbözők. Ez azt jelenti, hogy a $P(x) := \prod_{1 \leq j < k \leq d} (\tau_j(f)(x) - \tau_k(f)(x)) \in \overline{K}[x]$ polinom nem a 0 polinom. Mivel K végtelen, ezért van olyan $\beta \in K$, ami nem gyöke $P(x)$-nek. Tehát

$$\tau_j(f(\beta)) = \tau_j\left(\sum_{i=1}^n a_i \beta^i\right) = \sum_{i=1}^n \tau_j(a_i)\beta^i = \tau_j(f)(\beta) \neq \tau_k(f)(\beta) = \tau_k(f(\beta)) \quad (j \neq k)$$

(hiszen $\beta \in K$ miatt $\tau_j(\beta) = \beta = \tau_k(\beta)$), így az $\alpha := f(\beta)$ választás megfelel. □

2. Galois-bővítések

2.1. Definíció. *Legyen L/K véges bővítés.* $\mathrm{Gal}(L/K) := \mathrm{Hom}_K(L, L)$ *a bővítés* Galois-csoportja*, azaz a relatív automorfizmusok csoportja.*

Vegyük észre, hogy $\mathrm{Gal}(L/K)$ valóban csoport a kompozícióra nézve. A kompozícióra való zártság és az asszociativitás nyilvánvaló, az identitás az egységelem. Inverz azért létezik, mert minden $\tau \in \mathrm{Hom}_K(L, L)$ szürjektív is (nemcsak injektív), hiszen L végesdimenziós vektortér K felett. Könnyű számolás mutatja, hogy τ^{-1} is művelettartó, tehát eleme $\mathrm{Hom}_K(L, L)$-nek.

2.2. Állítás. *A fenti definíció akkor is értelmes, ha L/K nem feltétlenül véges, de algebrai bővítés.*

Bizonyítás. Azt kell belátnunk, hogy minden $\tau\colon L \to L$ K-homomorfizmus szürjektív (a fenti érvelésben csak itt használtuk L/K végességét). Vegyünk egy $\alpha \in L$-et és legyen $m_\alpha(x) \in K[x]$ a minimálpolinomja. Ennek véges sok gyöke lehet csak L-ben: $\{\alpha = \alpha_1, \ldots, \alpha_n\}$. Ekkor minden $i \in \{1, \ldots, n\}$-re $\tau(\alpha_i)$ is gyöke m_α-nak az 1.3-as Lemma miatt. Tehát τ permutálja az $\{\alpha = \alpha_1, \ldots, \alpha_n\}$ véges halmazt (hiszen injektív), így α is benne van a képében. □

Megjegyzés: Ha $K \leq L \leq \overline{K}$ (mivel L-nek is van algebrai lezártja, ezt minden további nélkül feltehetjük), akkor minden $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L)$-beli elemet tekinthetünk $\overline{K}$-ba menő homomorfizmusnak is. Tehát $|\mathrm{Gal}(L/K)| \leq |\mathrm{Hom}_K(L, \overline{K})| \leq |L : K|$ mindig teljesül.

2.3. Definíció. *Az L/K véges bővítésről azt mondjuk, hogy Galois-bővítés, ha $|\mathrm{Gal}(L/K)| = |L : K|$. (Bizonyos forrásokban a $\mathrm{Gal}(L/K)$ csoportot csak akkor hívják Galois-csoportnak, ha az L/K bővítés Galois.)*

2.4. Állítás. *Minden Galois-bővítés szeparábilis, speciálisan egyszerű.*

Bizonyítás. Valóban, a fenti megjegyzés miatt ha L/K Galois, akkor $|\mathrm{Hom}_K(L, \overline{K})|$ is egyenlő $|L : K|$-val. □

2.5. Állítás. *Legyen $K \leq L (\leq \overline{K})$ egy véges szeparábilis bővítés. A következők ekvivalensek:*

(i) L/K Galois.

(ii) Minden $\tau\colon L \to \overline{K}$ K-homomorfizmusra $\tau(L) = L$. (Ha nem tesszük fel, hogy L eleve részteste $\overline{K}$-nak, akkor azt kell mondani, hogy minden τ-nak ugyanaz a képtere.)

(iii) Minden $\alpha \in L$-re α összes $\overline{K}$-beli K fölötti konjugáltja L-ben van. (Azaz az $m_\alpha(x) \in K[x]$ minimálpolinom L felett gyöktényezők szorzatára bomlik.)

(iv) $L = K(\alpha_1, \ldots, \alpha_n)$ és minden α_i minden $\overline{K}$-beli K-feletti konjugátlja L-ben van.

Bizonyítás. $(i) \iff (ii)$, hiszen $L \leq \overline{K}$ miatt minden $\tau \in \mathrm{Hom}_K(L, L)$ tekinthető $L \to \overline{K}$ K-homomorfizmusnak is.

$(ii) \Rightarrow (iii)$: Legyen $\beta \in \overline{K}$ az α egyik konjugáltja. Ekkor az 1.4-es Állítás miatt van olyan $\tau \in \mathrm{Hom}_K(K(\alpha), \overline{K})$, melyre $\tau(\alpha) = \beta$. Továbbá (mivel $L/K(\alpha)$ is szeparábilis) van olyan $\alpha' \in L$, melyre $L = K(\alpha)(\alpha')$. Az 1.9-es Állítás szerint így τ kiterjed egy $\rho\colon L \to \overline{K}$ K-homomorfizmussá, melyre $\rho(\alpha) = \tau(\alpha) = \beta$. (ii) szerint viszont $\rho(L) = L$, azaz $\beta \in L$.

$(iii) \Rightarrow (iv)$ triviális. $(iv) \Rightarrow (ii)$: Minden $\alpha \in L$-re van olyan $f \in K[x_1, \ldots, x_n]$ polinom, melyre $\alpha = f(\alpha_1, \ldots, \alpha_n)$, tehát $\tau(\alpha) = \tau(f(\alpha_1, \ldots, \alpha_n)) = f(\tau(\alpha_1), \ldots, \tau(\alpha_n)) \in L$. Tehát $\tau(L) \leq L$, és mivel $\dim_K \tau(L) = \dim_K L$, ezért $\tau(L) = L$.

□

2.6. Példa. *(a)* $\mathbb{C}/\mathbb{R}$ *Galois.*

(b) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *Galois.*

(c) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ *nem Galois.*

(d) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ *és* $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *Galois, de* $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ *mégsem Galois.*

2.7. Definíció. *Legyen* $f(x) \in K[x]$ *polinom, legyenek* f *gyökei* $\overline{K}$*-ban* $\{\alpha_1, \ldots, \alpha_n\}$*. Ekkor a* $K_f := K(\alpha_1, \ldots, \alpha_n)(\leq \overline{K})$ *testet* f K *feletti felbontási testének nevezzük.*

2.8. Példa. *1.* $x^2 - 2$ *felbontási teste* $\mathbb{Q}$ *fölött* $\mathbb{Q}(\sqrt{2})$*.*

2. $x^3 - 2$ *felbontási teste* $\mathbb{Q}$ *fölött* $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$*, ahol* ε *primitív harmadik egységgyök.*

3. Ha $K(\alpha)/K$ *Galois, akkor* $K(\alpha)$ *az* α *minimálpolinomjának felbontási teste.*

2.9. Következmény. *Ha* f *szeparábilis polinom (azaz nincs többszörös gyöke), akkor* K_f/K *Galois. Speciálisan minden véges szeparábilis bővítés beágyazható egy véges Galois-bővítésbe.*

Bizonyítás. Mivel f szeparábilis, ezért $K_f = K(\alpha_1, \ldots, \alpha_n)$ szeparábilis K felett, tehát alkalmazhatjuk a 2.5-ös Állítást, melynek (iv)-es feltétele triviálisan teljesül. Továbbá ha L/K véges szeparábilis, akkor az 1.15-ös Tétel szerint $L = K(\alpha)$ valamilyen $\alpha \in L$-re, és α minimálpolinomjának felbontási teste tartalmazza L-et (vagy legalábbis egy L-lel izomorf résztestet, ha nem tettük fel, hogy $L \leq \overline{K}$). □

2.10. Lemma. *Legyen* F/K *tetszőleges szeparábilis bővítés és* $G := \mathrm{Gal}(F/K)$*.*

(i) Ha $K \leq L \leq F$ *közbülső test, akkor* $\mathrm{Gal}(F/L) \leq G$*.*

(ii) Ha $H \leq G$*, akkor* $F^H := \{\alpha \in F \mid \tau(\alpha) = \alpha \forall \tau \in H\}$ *egy* K*-t tartalmazó résztest* F*-ben. (Definíció: a* H fixteste F^H*.) Továbbá* $K \leq F^G \leq F^H \leq F$ *és* $H \leq \mathrm{Gal}(F/F^H)$*.*

Bizonyítás. Mindkettő triviális: (i)-nél $\mathrm{Gal}(F/L)$ éppen azon $F \to F$ automorfizmusokból áll, amiknek L-re való megszorítása az identitás, speciálisan a K-ra való megszorítása is az. (ii)-nél pedig azt kell ellenőrizni, hogy ha $\alpha, \beta \in F^H$, akkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is benne van F^H-ban. Ez közvetlenül látszik a definícióból, hiszen H minden eleme testhomomorfizmus. A további két tartalmazás nyilvánvaló. □

2.11. Állítás. *Legyen* $F = K(\alpha)$*, ahol* α *algebrai* K *felett.*

(i) Ha F/K *Galois és* $G = \mathrm{Gal}(F/K)$*, akkor* $F^G = K$*.*

(ii) Ha $F^G = K$ *valamilyen* $G \leq \mathrm{Gal}(F/K)$ *részcsoportra, akkor* F/K *Galois és* $G = \mathrm{Gal}(F/K)$*.*

Bizonyítás. (i): Nyilván $K \leq F^G \leq F$, és $G \leq \mathrm{Gal}(F/F^G)$ miatt $|G| \leq |\mathrm{Gal}(F/F^G)| \leq |F : F^G| \leq |F : K| = |G|$, tehát mindenütt egyenlőség áll.

(ii): Legyen m_α az α minimálpolinomja és definiáljuk az $f_\alpha(x) := \prod_{\tau \in G}(x - \tau(\alpha)) \in F[x]$ polinomot. Ekkor ha $\sigma \in G$, akkor $\sigma(f_\alpha)(x) = \prod_{\tau \in G}(x - \sigma\tau(\alpha)) = \prod_{\tau \in G}(x - \tau(\alpha)) = f_\alpha(x)$, hiszen ha τ végigfut G összes elemén, akkor $\sigma\tau$ is végigfut ugyanezeken az elemeken. Tehát

az $f_\alpha(x)$ polinom együtthatóit minden $\sigma \in G$ fixálja, azaz $f_\alpha(x) \in F^G[x] = K[x]$. Nyilván $f_\alpha(\alpha) = 0$, ezért $m_\alpha \mid f_\alpha$. Speciálisan $|F : K| = \deg(m_\alpha) \leq \deg(f_\alpha) = |G| \leq |\mathrm{Gal}(F/K)| \leq |F : K|$, ezért mindenhol egyenlőség van, azaz $G = \mathrm{Gal}(F/K)$ és $|\mathrm{Gal}(F/K)| = |F : K|$, másszóval F/K Galois. □

2.12. Tétel (Galois-elmélet főtétele)**.** *Legyen F/K egy véges Galois-bővítés $G = \mathrm{Gal}(F/K)$ Galois-csoporttal. Ekkor a*

$$\begin{aligned} \{K \leq L \leq F \text{ közbülsőtestek}\} &\leftrightarrow \{H \leq G \text{ részcsoportok}\} \\ \psi\colon L &\mapsto \mathrm{Gal}(F/L) \\ F^H &\mapsfrom H\colon \varphi \end{aligned}$$

leképezések egymás inverzei (speciálisan mindkettő bijekció). Továbbá ha $L \leftrightarrow H$ a fenti megfeleltetésben, akkor $|F : L| = |H|$ (azaz F/L is Galois) és $|L : K| = |G : H|$.

Bizonyítás. Először belátjuk, hogy tetszőleges L közbülsőtestre F/L egy Galois-bővítés. Mivel F/K Galois, ezért szeparábilis is, így az 1.15-ös Tétel szerint $F = K(\alpha)$ valamilyen $\alpha \in F$-re. A 2.5-ös Állítás (iii) része szerint α K feletti $m_\alpha(x) \in K[x]$ minimálpolinomja gyöktényezők szorzatára bomlik F felett. Viszont α L fölötti f_α minimálpolinomja nyilván osztója m_α-nak, ezért az is gyöktényezők szorzatára bomlik L felett, tehát a 2.5 Állítás (iv) része miatt F/L is Galois-bővítés. (Vegyük észre, hogy F/L szeparábilis az 1.8-as Következmény szerint és ez kell ahhoz, hogy a 2.5-ös Állítást alkalmazhassuk.)

Ha már tudjuk, hogy F/L Galois, akkor legyen $H := \mathrm{Gal}(F/L)$. A $2.11(i)$ szerint $L = F^H$, tehát $\varphi \circ \psi = \mathrm{id}$.

Megfordítva legyen $H \leq G$ tetszőleges, és legyen $L = F^H$. Ekkor $2.11(ii)$ szerint F/L Galois-bővítés és $H = \mathrm{Gal}(F/L)$, azaz $\psi \circ \varphi = \mathrm{id}$. Tehát ψ és φ egymás kétoldali inverzei. Az $|L : K| = |G : H|$ állítás következik a fokszámtételből. □

Hivatkozások

[1] Kiss Emil, *Bevezetés az algebrába*, Typotex, Budapest, 2007.