Normális bővítések, Galois-csoport

Waldhauser Tamás
2015 őszi félév

A továbbiakban (ahogy eddig is) K egy nulla karakterisztikájú testet jelöl.

Definíció

Az $N \mid K$ testbővítés *normális*, ha minden $f \in K[x]$ irreducibilis polinom esetén

$$f\text{-nek van gyöke } N\text{-ben} \implies f \text{ minden gyöke } N\text{-ben van.}$$

(Az utóbbi azt jelenti, hogy $\exists \alpha_1, \ldots, \alpha_n \in N: \ f \sim (x-\alpha_1)\cdots(x-\alpha_n)$.)

A végesfokú normális bővítéseket *Galois-bővítéseknek* nevezzük.

Tétel

Tetszőleges $N \mid K$ végesfokú bővítésre az alábbiak ekvivalensek:

(i) $N \mid K$ normális (azaz Galois);

(ii) N zárt a K feletti konjugáltságra, azaz bármely $\alpha \in N$ elemre $m_{\alpha,K}$ minden gyöke N-ben van;

(iii) $N \mid K$ felbontási test, azaz van olyan $g \in K[x]$ polinom, melyre $N = L_{g,K}$.

Bizonyítás

(i) $\implies$ (ii): Triviális ($f := m_{\alpha,K}$ irreducibilis K felett).

(ii) $\implies$ (iii): Könnyű (legyen $N = K(\vartheta)$ és $g = m_{\vartheta,K}$; ekkor $N = L_{g,K}$).

Bizonyítás (folyt.)

(iii) $\Longrightarrow$ (i): Nem olyan könnyű. Tfh. $\exists g \in K[x] : N = L_{g,K}$, vagyis $N = K(\beta_1, \ldots, \beta_m)$, ahol $g \sim (x - \beta_1) \cdots (x - \beta_m)$.

Legyen $f \in K[x]$ irreducibilis polinom melynek $\alpha \in N$ gyöke, és legyen $\alpha' \in \overline{K}$ egy másik gyöke f-nek. (Cél: $\alpha' \in N$.)

Ekkor $m_{\alpha,K} = m_{\alpha',K} = f$, ezért $K(\alpha) \mid K$ és $K(\alpha') \mid K$ izomorf bővítések (mindkettő izomorf $K[x]/(f) \mid K$-val):

$$\exists\, \varkappa\colon K(\alpha) \to K(\alpha') \text{ izomorfizmus, } \varkappa|_K = \mathrm{id}_K\,.$$

Határozzuk meg g felbontási testét $K(\alpha)$ és $K(\alpha')$ felett:

$$\begin{aligned} L_{g,K(\alpha)} &= K(\alpha)(\beta_1, \ldots, \beta_m) = K(\beta_1, \ldots, \beta_m)(\alpha) = N(\alpha) = N; \\ L_{g,K(\alpha')} &= K(\alpha')(\beta_1, \ldots, \beta_m) = K(\beta_1, \ldots, \beta_m)(\alpha') = N(\alpha')\,. \end{aligned}$$

A felbontási test unicitása (izomorfizmuskiterjesztési tulajdonság) szerint

$$\exists\, \varphi\colon N \to N(\alpha') \text{ izomorfizmus, } \varphi|_{K(\alpha)} = \varkappa.$$

Ekkor $\varphi|_K = \varkappa|_K = \mathrm{id}_K$, tehát $N \mid K \cong N(\alpha') \mid K$.

Emiatt a $K \leq N \leq N(\alpha')$ testtoronyban $[N : K] = [N(\alpha') : K]$, és így $[N(\alpha') : N] = 1$. Tehát $N(\alpha') = N$, azaz $\alpha' \in N$. □

Tétel

Ha $K \leq E \leq N$ és $N \mid K$ Galois-bővítés, akkor $N \mid E$ is Galois-bővítés.

Bizonyítás

$N \mid K$ Galois $\implies \quad \exists g \in K[x] : N = L_{g,K}$, azaz $N = K(\beta_1, \ldots, \beta_m)$, ahol $g \sim (x - \beta_1) \cdots (x - \beta_m)$. Ekkor

$$N = K(\beta_1, \ldots, \beta_m) \subseteq E(\beta_1, \ldots, \beta_m) \subseteq N(\beta_1, \ldots, \beta_m) = N,$$

vagyis $N = E(\beta_1, \ldots, \beta_m)$. Tehát $N = L_{g,E}$ és így $N \mid E$ normális. □

Megjegyzés

Normális bővítés „alsó fele" nem mindig normális, sőt bármilyen végesfokú testbővítés felléphet egy normális bővítés alsó feleként!

Valóban, legyen $E \mid K$ végesfokú, és legyen $\vartheta \in E$ primitív elem: $E = K(\vartheta)$. Legyen $N = L_{m_{\vartheta,K},K}$; ekkor $K \leq E \leq N$ és $N \mid K$ normális.

Vegyük észre, hogy $E \mid K$ minden normális kiterjesztése tartalmazza N-et (miért?), ezért N-et az $E \mid K$ bővítés normális lezártjának nevezzük.

Definíció

Az $E \mid K$ testbővítés *normális lezártján* a legszűkebb olyan N testet értjük, melyre $K \leq E \leq N$ és $N \mid K$ normális.

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés normális lezártja:

$N = L_{x^3-2,\mathbb{Q}} = \mathbb{Q}(\sqrt[3]{2},\ \sqrt[3]{2}\varepsilon,\ \sqrt[3]{2}\varepsilon^2) = \mathbb{Q}(\sqrt[3]{2},\ \varepsilon)$, ahol $\varepsilon = \text{cis}\,\frac{2\pi}{3}$.

Példa

Normális-e a $\mathbb{Q}(\sqrt{2}, i) \mid \mathbb{Q}$ testbővítés?

A $\vartheta = \sqrt{2} + i$ primitív elem minimálpolinomja $f := m_{\vartheta,\mathbb{Q}} = x^4 - 2x^2 + 9$, és ennek gyökei $\pm\sqrt{2} \pm i$. Tehát $L_{f,\mathbb{Q}} = \mathbb{Q}(\pm\sqrt{2} \pm i) = \mathbb{Q}(\sqrt{2}, i)$, azaz a bővítés normális (normális lezártja saját maga).

HF: Határozza meg a $\mathbb{Q}(\sqrt[4]{3}) \mid \mathbb{Q}$ bővítés normális lezártját.

HF: Bizonyítsa be, hogy minden másodfokú bővítés normális.

Definíció

Az $N \mid K$ testbővítés *Galois-csoportja* azon $N \to N$ automorfizmusok csoportja, melyek pontonként fixen hagyják K-t:

$$\mathrm{Gal}\,(N \mid K) = \mathrm{Aut}_K N = \{\sigma \colon N \to N \text{ izom.}, \ \sigma|_K = \mathrm{id}_K\}\,.$$

Tétel

Legyen $N \mid K$ Galois-bővítés, és legyen $G = \mathrm{Gal}\,(N \mid K)$. Bármely $\alpha, \alpha' \in N$ esetén

$$\exists \sigma \in G : \ \alpha\sigma = \alpha' \iff m_{\alpha,K} = m_{\alpha',K} \text{ (azaz } \alpha \text{ és } \alpha' \text{ konjugáltak).}$$

Bizonyítás

$\Longrightarrow$: Legyen $f = m_{\alpha,K} = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ \ (a_i \in K)$.

Tfh. $\alpha\sigma = \alpha'$ valamely $\sigma \in G$-re. Számítsuk ki $f\,(\alpha')$ értékét:

$$\begin{aligned} f\,(\alpha') = f\,(\alpha\sigma) &= a_n\,(\alpha\sigma)^n + a_{n-1}\,(\alpha\sigma)^{n-1} + \cdots + a_1\,(\alpha\sigma) + a_0 \\ &= a_n\sigma \cdot (\alpha\sigma)^n + a_{n-1}\sigma \cdot (\alpha\sigma)^{n-1} + \cdots + a_1\sigma \cdot (\alpha\sigma) + a_0\sigma \\ &= \left(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right)\sigma \\ &= (f\,(\alpha))\,\sigma = 0\,\sigma = 0. \end{aligned}$$

Tehát α' gyöke f-nek, és így $f = m_{\alpha',K}$, hiszen f irreducibilis K felett.

Tétel

Legyen $N \mid K$ Galois-bővítés, és legyen $G = \mathrm{Gal}(N \mid K)$. Bármely $\alpha, \alpha' \in N$ esetén

$$\exists \sigma \in G : \ \alpha\sigma = \alpha' \iff m_{\alpha,K} = m_{\alpha',K} \text{ (azaz } \alpha \text{ és } \alpha' \text{ konjugáltak).}$$

Bizonyítás (folyt.)

$\Longleftarrow$: Ha $m_{\alpha,K} = m_{\alpha',K}$, akkor $K(\alpha) \mid K$ és $K(\alpha') \mid K$ izomorf bővítések:

$$\exists\, \varkappa\colon K(\alpha) \to K(\alpha') \text{ izomorfizmus, } \varkappa|_K = \mathrm{id}_K \text{ és } \alpha\varkappa = \alpha'.$$

Mivel $N \mid K$ Galois-bővítés, $\exists g \in K[x] : N = L_{g,K}$, vagyis $N = K(\beta_1, \ldots, \beta_m)$, ahol $g \sim (x - \beta_1) \cdots (x - \beta_m)$.

Határozzuk meg g felbontási testét $K(\alpha)$ és $K(\alpha')$ felett:

$$L_{g,K(\alpha)} = K(\alpha)(\beta_1, \ldots, \beta_m) = K(\beta_1, \ldots, \beta_m)(\alpha) = N(\alpha) = N;$$
$$L_{g,K(\alpha')} = K(\alpha')(\beta_1, \ldots, \beta_m) = K(\beta_1, \ldots, \beta_m)(\alpha') = N(\alpha') = N.$$

A felbontási test unicitása (izomorfizmuskiterjesztési tulajdonság) szerint

$$\exists\, \sigma\colon N \to N \text{ izomorfizmus, } \sigma|_{K(\alpha)} = \varkappa.$$

Ekkor $\sigma|_K = \varkappa|_K = \mathrm{id}_K$, tehát $\sigma \in \mathrm{Gal}(N \mid K)$ és $\alpha\sigma = \alpha'$. □

Következmény

Galois-bővítés Galois-csoportjának elemszáma megegyezik a bővítés fokszámával:

$$|\mathrm{Gal}\,(N \mid K)| = [N : K]\,.$$

Bizonyítás

Legyen $N \mid K$ Galois-bővítés, $\vartheta = \vartheta_1 \in N$ primitív elem ($N = K\,(\vartheta)$) és legyen $f = m_{\vartheta,K} = (x - \vartheta_1) \cdots (x - \vartheta_n)$. Ekkor $n = [N : K]$ és $\vartheta_1, \ldots, \vartheta_n \in N$ (miért?).

Ha $\sigma \in \mathrm{Gal}\,(N \mid K)$, akkor ϑ és $\vartheta\sigma$ konjugáltak: $\exists k : \ \vartheta\sigma = \vartheta_k$. Ez az információ (és az, hogy $\sigma|_K = \mathrm{id}_K$) már egyértelműen meg is határozza a σ leképezést. Valóban, az N test minden eleme egyértelműen felírható

$$\alpha = a_{n-1}\vartheta^{n-1} + \cdots + a_1\vartheta + a_0 \ \ (a_i \in K)$$

alakban, és ekkor

$$\alpha\sigma = a_{n-1}\sigma \cdot (\vartheta\sigma)^{n-1} + \cdots + a_1\sigma \cdot (\vartheta\sigma) + a_0\sigma = a_{n-1}{\vartheta_k}^{n-1} + \cdots + a_1\vartheta_k + a_0.$$

Jelölje σ_k a fenti leképezést, vagyis $\sigma_k \colon N \to N$, $\sum a_i\vartheta^i \mapsto \sum a_i\vartheta_k^i$.

Beláttuk, hogy $\mathrm{Gal}\,(N \mid K) \subseteq \{\sigma_1, \ldots, \sigma_n\}$. Még azt kellene igazolni, hogy mindegyik σ_k valóban izomorfizmus. Node ez következik az egyszerű algebrai bővítés unicitásáról szóló tételből: $N = K\,(\vartheta) = K\,(\vartheta_k)$ miatt létezik $\varphi \colon N \to N$ izomorfizmus, amelyre $\vartheta\varphi = \vartheta_k$ és $\varphi|_K = \mathrm{id}_K$. Ekkor a fentiek szerint $\varphi = \sigma_k$. $\square$

Definíció

Egy $f \in K[x]$ polinom *Galois-csoportján* a K feletti felbontási testének a Galois-csoportját értjük: $\mathrm{Gal}(f) = \mathrm{Gal}(N \mid K)$, ahol $N = L_{f,K}$.

Tétel

Legyen $f \in K[x]$ többszörös gyökök nélküli n-edfokú polinom. Ekkor $\mathrm{Gal}(f)$ izomorf S_n egy részcsoportjával. Konkrétabban, ha Gy a gyökök halmaza, akkor a

$$\mu\colon\ \mathrm{Gal}(f) \to S_{Gy},\ \sigma \mapsto \sigma|_{Gy}$$

„megszorító leképezés" beágyazza a $\mathrm{Gal}(f)$ csoportot $S_{Gy} \cong S_n$-be.

Bizonyítás

Legyen $N = L_{f,K}$ és $\sigma \in \mathrm{Gal}(f)$. Ha $\alpha \in Gy$, akkor $f(\alpha\sigma) = f(\alpha)\,\sigma = 0\sigma = 0$, vagyis $\alpha\sigma \in Gy$. Tehát $\sigma(Gy) \subseteq Gy$, ezért van értelme megszorítani a σ leképezést a Gy halmazra, és így egy $\sigma|_{Gy} \in S_{Gy}$ permutációt kapunk.

Az világos (?), hogy a megszorítás és a leképezésszorzás felcserélhető egymással: $(\sigma \circ \tau)|_{Gy} = \sigma|_{Gy} \circ \tau|_{Gy}$, ezért μ homomorfizmus. Azt kell még belátnunk, hogy μ injektív.

Ha $\sigma, \tau \in \mathrm{Gal}(f)$ és $\sigma|_{Gy} = \tau|_{Gy}$, akkor σ és τ megegyezik a $K \cup Gy$ halmazon. Ez a halmaz generálja az N testet (hiszen $N = L_{f,K} = K(Gy)$), ezért $\sigma = \tau$.

□

A Galois-elmélet főtétele

Legyen $N \mid K$ Galois-bővítés és $G = \mathrm{Gal}(N \mid K) = \mathrm{Aut}_K N$.

Tekintsük az $I = \{(\alpha, \sigma) : \alpha\sigma = \alpha\} \subseteq N \times G$ „illeszkedési reláció" által indukált Galois-kapcsolatot:

$$\mathcal{P}(N) \to \mathcal{P}(G), \quad E \mapsto \{\sigma \in G \mid \forall \alpha \in E : \alpha\sigma = \alpha\} = E' = \mathrm{Gal}(N \mid E);$$
$$\mathcal{P}(G) \to \mathcal{P}(N), \quad H \mapsto \{\alpha \in N \mid \forall \sigma \in H : \alpha\sigma = \alpha\} = H' = \mathrm{Fix}(H).$$

(1) $\forall E \subseteq N: \; E'' = E \iff K \leq E \leq N$ (azaz $E \in \mathrm{Sub}_K N$).

(2) $\forall H \subseteq G: \; H'' = H \iff H \leq G$ (azaz $H \in \mathrm{Sub}\, G$).

(3) A $\mathrm{Sub}_K N$ és $\mathrm{Sub}\, G$ hálók között duális izomorfizmust létesítenek az

$$E \mapsto E' = \mathrm{Gal}(N \mid E) \quad \text{és} \quad H \mapsto H' = \mathrm{Fix}(H)$$

leképezések (amelyek egymás inverzei).

(4) Legyen $E \in \mathrm{Sub}_K N$ és $H \in \mathrm{Sub}\, G$ egymásnak megfelelő résztest és részcsoport:

$$E = H' = \mathrm{Fix}(H) \quad \text{és} \quad H = E' = \mathrm{Gal}(N \mid E).$$

a) $[N : E] = |H|$ és $[E : K] = [G : H]$.

b) $E \mid K$ normális $\iff H \lhd G$, és ha ez teljesül, akkor $\mathrm{Gal}(E \mid K) \cong G/H$, azaz

$$\mathrm{Gal}(E \mid K) \cong \mathrm{Gal}(N \mid K) \,/\, \mathrm{Gal}(N \mid E).$$

Bizonyítás

(1) $E'' = E \overset{?}{\iff} K \leq E \leq N$

$\Longrightarrow$: Ha $E'' = E$, akkor $E = (E')'$, és így közbülső test (HF).

$\Longleftarrow$: Tfh. $E \in \mathrm{Sub}_K N$ és legyen $F = E''$. (Cél: $E = F$.) Ekkor $E \subseteq F$ és

$$\mathrm{Gal}(N \mid F) = F' = E''' = E' = \mathrm{Gal}(N \mid E).$$

Mivel $N \mid F$ és $N \mid E$ normális bővítések,

$$[N : F] = |\mathrm{Gal}(N \mid F)| = |\mathrm{Gal}(N \mid E)| = [N : E].$$

Tehát a $K \subseteq E \subseteq F \subseteq N$ testtoronyban $[N : F] = [N : E]$, és így $[F : E] = 1$.

(2) $H'' = H \overset{?}{\iff} H \leq G$

$\Longrightarrow$: Ha $H'' = H$, akkor $H = (H')'$, és így részcsoport (HF).

$\Longleftarrow$: Nem bizonyítjuk.

(3) Következik a fentiekből és a Galois-kapcsolatokról tanultakból.

(4) Legyen $H = E' = \mathrm{Gal}(N \mid E)$. Mivel $N \mid K$ és $N \mid E$ normális bővítések,

$$[N : K] = |\mathrm{Gal}(N \mid K)| = |G| \quad \text{és} \quad [N : E] = |\mathrm{Gal}(N \mid E)| = |H|.$$

Ebből következik, hogy

$$[E : K] = [N : K] \,/\, [N : E] = |G| \,/\, |H| = [G : H].$$

A többit nem bizonyítjuk. □