Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. február 23.

Példa.

Legyen $L = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ és $g = x^4 - 106x^2 + 1369 \in \mathbb{Q}[x]$.

Példa.

Legyen $L = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ és $g = x^4 - 106x^2 + 1369 \in \mathbb{Q}[x]$.

Példa.

Legyen $L = \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$ és $g = x^4 - 106x^2 + 1369 \in \mathbb{Q}[x]$. A g polnom irreducibilis és van gyöke az L testben, mivel $g(2\sqrt{2}+3\sqrt{5}) = 0$ és $2\sqrt{2}+3\sqrt{5} \in L$.

Példa.

Legyen $L = \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$ és $g = x^4 - 106x^2 + 1369 \in \mathbb{Q}[x]$. A g polnom irreducibilis és van gyöke az L testben, mivel $g(2\sqrt{2}+3\sqrt{5}) = 0$ és $2\sqrt{2}+3\sqrt{5} \in L$. A g polinom elsőfokú tényezők szorzatára bomlik L felett:

Példa.

Legyen $L = \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$ és $g = x^4 - 106x^2 + 1369 \in \mathbb{Q}[x]$. A g polnom irreducibilis és van gyöke az L testben, mivel $g(2\sqrt{2}+3\sqrt{5}) = 0$ és $2\sqrt{2}+3\sqrt{5} \in L$. A g polinom elsőfokú tényezők szorzatára bomlik L felett:

$$g = (x - 2\sqrt{2} + 3\sqrt{5})(x + 2\sqrt{2} - 3\sqrt{5}) \cdot (x + 2\sqrt{2} + 3\sqrt{5})(x - 2\sqrt{2} - 3\sqrt{5}).$$

Tétel.

Legyen L felbontási teste az $f \in K[x]$ polinomnak a K test felett, valamint legyen $g \in K[x]$ irreducibilis polinom. Ekkor g-nek vagy valamennyi gyöke benne van L-ben, vagy nincs gyöke L-ben.

Tétel.

Legyen L felbontási teste az $f \in K[x]$ polinomnak a K test felett, valamint legyen $g \in K[x]$ irreducibilis polinom. Ekkor g-nek vagy valamennyi gyöke benne van L-ben, vagy nincs gyöke L-ben.

Bizonyítás.

Tegyük fel, hogy a g polinomnak van egy β gyöke L-ben. Mivel $L = K(\alpha_1, \ldots, \alpha_n)$, ahol $\alpha_1, \ldots, \alpha_n$ az f polinom gyökei L-ben, ezért β felírható $p(\alpha_1, \ldots, \alpha_n)$ alakban alkalmas $p \in K[x]$ polinomra. A tétel állításának bizonyítása annak igazolásán múlik, hogy g minden gyöke előáll $p(\alpha_{1\sigma}, \ldots, \alpha_{n\sigma})$ alakban alkalmas $\sigma \in S_n$ permutációra.

Definíció: normális bővítés.

Az $L : K$ testbővítés **normális**, ha algebrai bővítés és valahányszor $f \in K[x]$ irreducibilis polinom, mindannyiszor vagy f elsőfokú tényezők szorzatára bomlik L felett, vagy f-nek nincs gyöke L-ben.

Definíció: normális bővítés.

Az $L : K$ testbővítés **normális**, ha algebrai bővítés és valahányszor $f \in K[x]$ irreducibilis polinom, mindannyiszor vagy f elsőfokú tényezők szorzatára bomlik L felett, vagy f-nek nincs gyöke L-ben.

Következmény.

Ha L az $f \in K[x]$ polinom felbontási teste, akkor az $L : K$ bővítés normális.

Definíció: normális bővítés.

Az $L : K$ testbővítés **normális**, ha algebrai bővítés és valahányszor $f \in K[x]$ irreducibilis polinom, mindannyiszor vagy f elsőfokú tényezők szorzatára bomlik L felett, vagy f-nek nincs gyöke L-ben.

Következmény.

Ha L az $f \in K[x]$ polinom felbontási teste, akkor az $L : K$ bővítés normális.

Következmény.

Az $L : K$ algebrai bővítés pontosan akkor normális, ha bármely $\alpha \in L$-re $m_{\alpha,K}$ elsőfokú tényezők szorzatára bontható $L[x]$-ben.

Normális bővítések
Alapvető tulajdonságok

A normális bővítések leírásához ki kell terjesztenünk a felbontási test fogalmát egyetlen polinomról polinomok halmazaira.

A normális bővítések leírásához ki kell terjesztenünk a felbontási test fogalmát egyetlen polinomról polinomok halmazaira.

Definíció: polinomhalmaz felbontási teste.

Legyen K tetszőleges test és $S \subseteq K[x]$. Azt mondjuk, hogy a K test L bővítése **felbontási teste az S polinomhalmaznak**, ha S valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben, és L a legszűkebb ilyen tulajdonságú test.

A normális bővítések leírásához ki kell terjesztenünk a felbontási test fogalmát egyetlen polinomról polinomok halmazaira.

Definíció: polinomhalmaz felbontási teste.

Legyen K tetszőleges test és $S \subseteq K[x]$. Azt mondjuk, hogy a K test L bővítése **felbontási teste az S polinomhalmaznak**, ha S valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben, és L a legszűkebb ilyen tulajdonságú test.

Ha az S halmaz véges, $S = \{f_1, \ldots, f_n\}$, akkor S felbontási teste megegyezik az $f = f_1 \cdots f_n$ polinom felbontási testével.

Tétel.

Az $L : K$ testbővítés pontosan akkor normális, ha L valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.

Tétel.

Az $L : K$ testbővítés pontosan akkor normális, ha L valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.

Bizonyítás.

Tegyük fel, hogy $L : K$ normális, és legyen $S = \{m_{\alpha,K} \mid \alpha \in L\}$.

Tétel.

Az $L : K$ testbővítés pontosan akkor normális, ha L valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.

Bizonyítás.

Tegyük fel, hogy $L : K$ normális, és legyen $S = \{m_{\alpha,K} \mid \alpha \in L\}$.

Tétel.

Az $L : K$ testbővítés pontosan akkor normális, ha L valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.

Bizonyítás.

Tegyük fel, hogy $L : K$ normális, és legyen $S = \{m_{\alpha,K} \mid \alpha \in L\}$. Ekkor S valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben.

Tétel.

Az $L : K$ testbővítés pontosan akkor normális, ha L valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.

Bizonyítás.

Tegyük fel, hogy $L : K$ normális, és legyen $S = \{m_{\alpha,K} \mid \alpha \in L\}$. Ekkor S valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben. Továbbá ezzel a tulajdonsággal nyilván nem rendelkezik L egyetlen valódi részteste sem.

Tétel.

Az $L : K$ testbővítés pontosan akkor normális, ha L valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.

Bizonyítás.

Tegyük fel, hogy $L : K$ normális, és legyen $S = \{m_{\alpha,K} \mid \alpha \in L\}$. Ekkor S valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben. Továbbá ezzel a tulajdonsággal nyilván nem rendelkezik L egyetlen valódi részteste sem.
Tegyük fel, hogy L felbontási teste az $S \subseteq K[x]$ polinomhalmaznak. Legyen R az S-beli polinomok gyökeinek halmaza. Ekkor $L = K(R)$ és az $L : K$ bővítés algebrai, mivel R minden eleme algebrai K felett. Legyen β tetszőleges eleme az L testnek. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_t \in R$ elemek, amelyekre $\beta \in K(\alpha_1, \ldots, \alpha_t)$.

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben.

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben.

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben. Ekkor $K(R_f)$ felbontási teste az f polinomnak K felett.

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben. Ekkor $K(R_f)$ felbontási teste az f polinomnak K felett. Legyen az $m_{\beta,K}$ polinom felbontási teste $K(R_f)$ felett H. Tekintsük $m_{\beta,K}$ egy $\beta' \neq \beta$ gyökét H-ban. Meg fogjuk mutatni, hogy $\beta' \in K(R_f) \subseteq L$.

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben. Ekkor $K(R_f)$ felbontási teste az f polinomnak K felett. Legyen az $m_{\beta,K}$ polinom felbontási teste $K(R_f)$ felett H. Tekintsük $m_{\beta,K}$ egy $\beta' \neq \beta$ gyökét H-ban. Meg fogjuk mutatni, hogy $\beta' \in K(R_f) \subseteq L$.
Mivel $m_{\beta,K}$ a β és β' elemeknek is minimálpolinomja a K test felett, ezért

$$[K(\beta) : K] = [K(\beta') : K]. \tag{1}$$

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben. Ekkor $K(R_f)$ felbontási teste az f polinomnak K felett. Legyen az $m_{\beta,K}$ polinom felbontási teste $K(R_f)$ felett H. Tekintsük $m_{\beta,K}$ egy $\beta' \neq \beta$ gyökét H-ban. Meg fogjuk mutatni, hogy $\beta' \in K(R_f) \subseteq L$.
Mivel $m_{\beta,K}$ a β és β' elemeknek is minimálpolinomja a K test felett, ezért

$$[K(\beta) : K] = [K(\beta') : K]. \tag{1}$$

Legyen $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$ és η kiterjeszthető egy olyan $\vartheta\colon K(\beta) \to K(\beta')$ injektív homomorfizmussá, amelyre $\vartheta(\beta) = \beta'$ teljesül (vö.: Kiterjesztési Lemma).

Bizonyítás (folytatás).

Minden i-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke α_i, és legyen $f = f_1 \cdots f_t$. Jelölje R_f az f polinom gyökeinek a halmazát L-ben. Ekkor $K(R_f)$ felbontási teste az f polinomnak K felett. Legyen az $m_{\beta,K}$ polinom felbontási teste $K(R_f)$ felett H. Tekintsük $m_{\beta,K}$ egy $\beta' \neq \beta$ gyökét H-ban. Meg fogjuk mutatni, hogy $\beta' \in K(R_f) \subseteq L$.
Mivel $m_{\beta,K}$ a β és β' elemeknek is minimálpolinomja a K test felett, ezért

$$[K(\beta) : K] = [K(\beta') : K]. \tag{1}$$

Legyen $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$ és η kiterjeszthető egy olyan $\vartheta\colon K(\beta) \to K(\beta')$ injektív homomorfizmussá, amelyre $\vartheta(\beta) = \beta'$ teljesül (vö.: Kiterjesztési Lemma). Mivel a $K(\beta')$ testet generálja $K \cup \{\beta'\}$, ezért ϑ izomorfizmus. A $K(R_f)$ test felbontási teste f-nek $K(\beta)$ felett és $K(R_f \cup \{\beta'\})$ felbontási teste $\vartheta_f = f$-nek $K(\beta')$ felett.

Bizonyítás (folytatás).

Így a felbontási test egyértelműségéről szóló tétel szerint van olyan $\tau\colon K(R_f) \to K(R_f \cup \{\beta'\})$ izomorfizmus, amelyre $\tau|_{K(\beta)} = \vartheta$. Ez pedig azt jelenti, hogy

$$[K(R_f) : K(\beta)] = [K(R_f \cup \{\beta'\}) : K(\beta')],$$

és így a Fokszámtétel és (1) szerint

$$\begin{aligned}[K(R_f) : K] &= [K(R_f) : K(\beta)][K(\beta) : K] \\ &= [K(R_f \cup \{\beta'\}) : K(\beta)][K(\beta') : K] \\ &= [K(R_f \cup \{\beta'\}) : K].\end{aligned}$$

Mivel $K(R_f) \subseteq K(R_f \cup \{\beta'\})$, ezért $K(R_f) = K(R_f \cup \{\beta'\})$. Ebből pedig már következik, hogy $\beta' \in K(R_f)$.

Következmény.

Az $L : K$ véges testbővítés pontosan akkor normális, ha L valamely $f \in K[x]$ polinom felbontási teste.

Következmény.

Az $L : K$ véges testbővítés pontosan akkor normális, ha L valamely $f \in K[x]$ polinom felbontási teste.

Bizonyítás.

Ha L valamely $f \in K[x]$ polinom felbontási teste, akkor az előző tétel szerint az $L : K$ bővítés normális. Fordítva, tegyük fel, hogy $L : K$ véges és normális. Legyen $[L : K] = k$ és $\alpha_1, \ldots, \alpha_k \in L$ az L, mint K feletti vektortér, bázisa. Ekkor L éppen az $f = m_{\alpha_1,K} \cdots m_{\alpha_k,K} \in K[x]$ polinom felbontási teste.

Tétel.

Ha az $L : K$ bővítés normális és M közbülső teste a bővítésnek, akkor az $L : M$ bővítés is normális.

Tétel.

Ha az $L : K$ bővítés normális és M közbülső teste a bővítésnek, akkor az $L : M$ bővítés is normális.

Példa.

Az előző tétel szerint, ha az $L : K$ testbővítés normális, akkor az $L : M$ testbővítés is normális, ahol $K \leqslant M \leqslant L$. Vajon mi a helyzet az $M : K$ bővítéssel?
Legyen $\varepsilon \notin \mathbb{R}$ egy komplex harmadik egységgyök. Ekkor a $\mathbb{Q}(\sqrt[3]{2}, \varepsilon) : \mathbb{Q}$ bővítés normális, mivel $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ az $f = x^3 - 2$ polinom felbontási teste $\mathbb{Q}$ felett. Azonban a $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ bővítés nem normális, mivel f-nek van gyöke a $\mathbb{Q}(\sqrt[3]{2})$ testben, de f nem bomlik fel elsőfokú polinomok szorzatára $\mathbb{Q}(\sqrt[3]{2})[x]$-ben.

Definíció: testbővítés Galois-csoportja.

Legyenek K és L testek úgy, hogy $K \leqslant L$. Ekkor $\mathrm{Aut}(L)$-lel jelöljük az L test automorfizmusainak csoportját, valamint

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(k) = k \text{ minden } k \in K\text{-ra}\}\,.$$

Nyilvánvaló, hogy $\mathrm{Aut}_K(L)$ részcsoportja $\mathrm{Aut}(L)$-nek. Az L test automorfizmuscsoportjának $\mathrm{Aut}_K(L)$ részcsoportját **az $L : K$ testbővítés Galois-csoportjának** nevezzük, és $\mathrm{Gal}(L : K)$-val jelöljük.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:

(1) az $M : K$ bővítés normális;

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:

(1) az $M : K$ bővítés normális;

(2) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:

(1) az $M : K$ bővítés normális;

(2) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;

(3) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) = M$.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:

(1) az $M : K$ bővítés normális;

(2) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;

(3) ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) = M$.

Bizonyítás.

(1)$\Longrightarrow$(2): Tegyük fel, hogy az $M : K$ bővítés normális, és legyen $\sigma \in \mathrm{Aut}_K(L)$. Legyen α az M test tetszőleges eleme, melynek minimálpolinomja $f = m_{\alpha,K} \in K[x]$. Ekkor $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, azaz $\sigma(\alpha)$ is gyöke f-nek. Mivel f lineáris tényezőkre bomlik $M[x]$-ben, ezért $\sigma(\alpha) \in M$. Így $\sigma(M) \subseteq M$.

Bizonyítás (folytatás).

(2)$\Longrightarrow$(3): Az állítás következik abból, hogy $\sigma^{-1} \in \mathrm{Aut}_K(L)$.
(3)$\Longrightarrow$(1): Tegyük fel, hogy tetszőleges $\sigma \in \mathrm{Aut}_K(L)$-ra $\sigma(M) = M$ teljesül. Legyen α az M test tetszőleges eleme, melynek minimálpolinomja $f = m_{\alpha,K} \in K[x]$. Legyen β az f polinom α-tól különböző gyöke L-ben (mivel az $L : K$ bővítés normális, ezért f valamennyi gyöke L-ben van). Azt kell igazolnunk, hogy $\beta \in M$. A Kiterjesztési Lemma szerint az $\eta = \mathrm{id}_K$ izomorfizmus kiterjeszthető egy $\vartheta\colon K(\alpha) \to K(\beta)$ injektív homomorfizmussá, amelyre $\vartheta(\alpha) = \beta$ is teljesül.

Bizonyítás (folytatás).

Mivel $L : K$ véges és normális bővítés, ezért L valamely $g \in K[x]$ polinom felbontási testével egyezik meg. Az L test a $\vartheta_g = g$ polinom felbontási teste mind a $K(\alpha)$, mind a $K(\beta)$ testek felett, ezért a felbontási test egyértelműsége szerint ϑ kiterjeszthető egy $\sigma\colon L \to L$ izomorfizmussá. Ekkor $\sigma \in \mathrm{Aut}_K(L)$, és így (3) miatt $\sigma(M) = M$. Ebből pedig azt kapjuk, hogy $\beta = \vartheta(\alpha) = \sigma(\alpha) \in M$. Ezzel a bizonyítást befejeztük.