Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. március 2.

Definíció: szeparábilis irreducibilis polinom.

Legyen K test és f egy irreducibilis n-edfokú polinom K felett, melynek felbontási teste L. Azt mondjuk, hogy az f polinom **szeparábilis (a K teste felett)**, ha f-nek n különböző gyöke van L-ben.

Definíció: szeparábilis irreducibilis polinom.

Legyen K test és f egy irreducibilis n-edfokú polinom K felett, melynek felbontási teste L. Azt mondjuk, hogy az f polinom **szeparábilis (a K teste felett)**, ha f-nek n különböző gyöke van L-ben.

Definíció: szeparábilits polinom.

Legyen K test és f egy tetszőleges polinom K felett. Azt mondjuk, hogy az f polinom **szeparábilis (a K teste felett)**, ha f valamennyi irreducibilis tényezője szeparábilis K felett.

Definíció: szeparábilis elem.

Legyen $L : K$ tetszőleges testbővítés és $\alpha \in L$. Azt mondjuk, hogy az α elem **szeparábilis (a K test felett)**, ha α algebrai K felett és $m_{\alpha,K}$ szeparábilis.

Definíció: szeparábilis elem.

Legyen $L : K$ tetszőleges testbővítés és $\alpha \in L$. Azt mondjuk, hogy az α elem **szeparábilis (a K test felett)**, ha α algebrai K felett és $m_{\alpha,K}$ szeparábilis.

Definíció: szeparábilis bővítés.

Az $L : K$ testbővítést **szeparábilisnek** nevezzük, ha az L test minden eleme szeparábilis K felett.

Definíció: szeparábilis elem.

Legyen $L : K$ tetszőleges testbővítés és $\alpha \in L$. Azt mondjuk, hogy az α elem **szeparábilis (a K test felett)**, ha α algebrai K felett és $m_{\alpha,K}$ szeparábilis.

Definíció: szeparábilis bővítés.

Az $L : K$ testbővítést **szeparábilisnek** nevezzük, ha az L test minden eleme szeparábilis K felett.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés szeparábilis. Ekkor tetszőleges $K \leqslant M \leqslant L$ közbülső testre az $L : M$ és $M : K$ bővítések is szeparábilisak.

Tétel.

Tegyük fel, hogy a $K(\alpha) : K$ testbővítés d-edfokú egyszerű algebrai bővítés, valamint legyen $\mathrm{j}\colon K \to L$ injektív homomorfizmus. Ha α szeparábilis K felett és $\mathrm{j}_{m_{\alpha,K}}$ elsőfokú polinomok szorzatára bomlik L felett, akkor pontosan d darab olyan injektív homomorfizmus van $K(\alpha)$-ból L-be, amely kiterjesztése j-nek. Különben d-nél kevesebb ilyen injektív homomorfizmus van.

Tétel.

Tegyük fel, hogy a $K(\alpha) : K$ testbővítés d-edfokú egyszerű algebrai bővítés, valamint legyen $\mathrm{j}\colon K \to L$ injektív homomorfizmus. Ha α szeparábilis K felett és $\mathrm{j}_{m_{\alpha,K}}$ elsőfokú polinomok szorzatára bomlik L felett, akkor pontosan d darab olyan injektív homomorfizmus van $K(\alpha)$-ból L-be, amely kiterjesztése j-nek. Különben d-nél kevesebb ilyen injektív homomorfizmus van.

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.

Tétel.

Tegyük fel, hogy a $K' : K$ testbővítés d-edfokú véges bővítés, valamint legyen $\mathrm{j}\colon K \to L$ injektív homomorfizmus. Ha a $K' : K$ testbővítés szeparábilis és tetszőleges $\alpha \in K'$-re $\mathrm{j}_{m_{\alpha,K}}$ elsőfokú polinomok szorzatára bomlik L felett, akkor pontosan d darab olyan injektív homomorfizmus van K'-ből L-be, amely kiterjesztése j-nek. Különben d-nél kevesebb ilyen injektív homomorfizmus van.

Következmény.

Tegyük fel, hogy $L : K$ véges bővítés és $L = K(\alpha_1, \ldots, \alpha_r)$. Ha α_i szeparábilis $K(\alpha_1, \ldots, \alpha_{i-1})$ felett minden i-re $(1 \leqslant i \leqslant r)$, akkor $L : K$ szeparábilis.

Következmény.

Tegyük fel, hogy $L : K$ véges bővítés és $L = K(\alpha_1, \ldots, \alpha_r)$. Ha α_i szeparábilis $K(\alpha_1, \ldots, \alpha_{i-1})$ felett minden i-re $(1 \leqslant i \leqslant r)$, akkor $L : K$ szeparábilis.

Következmény.

Tegyük fel, hogy $L : K$ véges bővítés és $L = K(\alpha_1, \ldots, \alpha_r)$. Ha α_i szeparábilis K felett minden i-re $(1 \leqslant i \leqslant r)$, akkor $L : K$ szeparábilis.

Következmény.

Tegyük fel, hogy $L : K$ véges bővítés és $L = K(\alpha_1, \ldots, \alpha_r)$. Ha α_i szeparábilis $K(\alpha_1, \ldots, \alpha_{i-1})$ felett minden i-re $(1 \leqslant i \leqslant r)$, akkor $L : K$ szeparábilis.

Következmény.

Tegyük fel, hogy $L : K$ véges bővítés és $L = K(\alpha_1, \ldots, \alpha_r)$. Ha α_i szeparábilis K felett minden i-re $(1 \leqslant i \leqslant r)$, akkor $L : K$ szeparábilis.

Következmény.

Tegyük fel, hogy $f \in K[x]$ szeparábilis K felett és L az f polinom egy felbontási teste. Ekkor az $L : K$ testbővítés szeparábilis.

Következmény.

Tegyük fel, hogy az K, L, M testekre $L : M$ és $M : K$ teljesül. Ha az $L : M$ és $M : K$ testbővítések szeparábilisek, akkor az $L : K$ bővítés is szeparábilis.

Következmény.

Tegyük fel, hogy az K, L, M testekre $L : M$ és $M : K$ teljesül. Ha az $L : M$ és $M : K$ testbővítések szeparábilisek, akkor az $L : K$ bővítés is szeparábilis.

Definíció: Galois-bővítés.

A véges, normális és szeparábilis bővítéseket **Galois-bővítéseknek** nevezzük.

Következmény.

Tegyük fel, hogy az K, L, M testekre $L : M$ és $M : K$ teljesül. Ha az $L : M$ és $M : K$ testbővítések szeparábilisek, akkor az $L : K$ bővítés is szeparábilis.

Definíció: Galois-bővítés.

A véges, normális és szeparábilis bővítéseket **Galois-bővítéseknek** nevezzük.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges. Ha $L : K$ Galois-bővítés, akkor $|\mathrm{Gal}(L : K)| = [L : K]$, különben $|\mathrm{Gal}(L : K)| < [L : K]$.

Polinomok többszörös gyökei
(Formális) deriválás

Legyen $f \neq 0$ tetszőleges polinom a K test felett, és legyen L az f polinom egy felbontási teste. Ekkor az f polinom felírható

$$f = \lambda(x - \alpha_1)^{\ell_1} \cdots (x - \alpha_r)^{\ell_r}$$

alakban, ahol $\alpha_1, \ldots, \alpha_r$ az f polinom páronként különböző gyökei L-ben. Az $\ell_i \in \mathbb{N}$ egészet az α_i gyök multiplicitásának nevezzük. Ha $\ell_i = 1$, akkor α_i **egyszeres gyök**, különben pedig **többszörös gyök**. Megjegyezzük, hogy az f polinom gyökeinek multiplicitása független a felbontási test választásától.

Definíció: (formális) deriváltak

Legyen K tetszőleges test, és legyen D_x a következő leképezés:

$$D_x\colon K[x] \to K[x],\ \sum_{k=0}^{n} a_k x^k \mapsto \begin{cases} 0, & \text{ha } f \in K, \\ \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k, & \text{ha } f^* = n \geqslant 1. \end{cases}$$

A D_x leképezést **(formális) driválásnak** nevezzük a $K[x]$ halmazon.

A következő tétel a formális deriválás tulajdonságait foglalja össze.

Tétel.

Legyen K tetszőleges test, ekkor a D_x formális deriválásra teljesülnek a következők.

Tétel.

Legyen K tetszőleges test, ekkor a D_x formális deriválásra teljesülnek a következők.

(1) D_x lineáris transzformációja a K test feletti $K[x]$ vektortérnek.

Tétel.

Legyen K tetszőleges test, ekkor a D_x formális deriválásra teljesülnek a következők.

(1) D_x lineáris transzformációja a K test feletti $K[x]$ vektortérnek.

(2) D_x **deriváció** a $K[x]$ halmazon, azaz tetszőleges $f, g \in K[x]$-re $D_x(f \cdot g) = D_x(f) \cdot g + f \cdot D_x(g)$ teljesül.

Tétel.

Legyen K tetszőleges test, ekkor a D_x formális deriválásra teljesülnek a következők.

(1) D_x lineáris transzformációja a K test feletti $K[x]$ vektortérnek.

(2) D_x **deriváció** a $K[x]$ halmazon, azaz tetszőleges $f, g \in K[x]$-re $D_x(f \cdot g) = D_x(f) \cdot g + f \cdot D_x(g)$ teljesül.

(3) Ha $\mathrm{char}(K) = 0$, akkor $\ker(D_x) = K$, és a D_x leképezés szürjektív.

Tétel.

Legyen K tetszőleges test, ekkor a D_x formális deriválásra teljesülnek a következők.

(1) D_x lineáris transzformációja a K test feletti $K[x]$ vektortérnek.

(2) D_x **deriváció** a $K[x]$ halmazon, azaz tetszőleges $f, g \in K[x]$-re $D_x(f \cdot g) = D_x(f) \cdot g + f \cdot D_x(g)$ teljesül.

(3) Ha $\mathrm{char}(K) = 0$, akkor $\ker(D_x) = K$, és a D_x leképezés szürjektív.

(4) Ha $\mathrm{char}(K) = p$ prímszám, akkor

$$\ker(D_x) = \{h(x^p) \mid h \in K[x]\},$$

és D_x képterét generálják az x^k monomok ($k \in \mathbb{N}_0$, $p \nmid k+1$).

Tétel.

Legyen f a K test feletti polinom, és $\alpha \in L$ az f polinom gyöke a K test valamely L bővítésében. Ekkor α pontosan akkor többszörös gyöke f-nek, ha $\mathrm{ln.k.o.}(f, D_x(f))$ legalább elsőfokú polinom, amelynek gyöke α.

Tétel.

Legyen f a K test feletti polinom, és $\alpha \in L$ az f polinom gyöke a K test valamely L bővítésében. Ekkor α pontosan akkor többszörös gyöke f-nek, ha $\mathrm{ln.k.o.}(f, D_x(f))$ legalább elsőfokú polinom, amelynek gyöke α.

Bizonyítás.

Tegyük fel, hogy $\alpha \in L$ többszörös gyöke f-nek a K test L bővítésében. Ekkor $f = (x-\alpha)^\ell g$, ahol $\ell \geqslant 2$ és $g \in L[x]$.

Tétel.

Legyen f a K test feletti polinom, és $\alpha \in L$ az f polinom gyöke a K test valamely L bővítésében. Ekkor α pontosan akkor többszörös gyöke f-nek, ha $\mathrm{ln.k.o.}(f, D_x(f))$ legalább elsőfokú polinom, amelynek gyöke α.

Bizonyítás.

Tegyük fel, hogy $\alpha \in L$ többszörös gyöke f-nek a K test L bővítésében. Ekkor $f = (x-\alpha)^\ell g$, ahol $\ell \geqslant 2$ és $g \in L[x]$.

Tétel.

Legyen f a K test feletti polinom, és $\alpha \in L$ az f polinom gyöke a K test valamely L bővítésében. Ekkor α pontosan akkor többszörös gyöke f-nek, ha $\ln.k.o.(f, D_x(f))$ legalább elsőfokú polinom, amelynek gyöke α.

Bizonyítás.

Tegyük fel, hogy $\alpha \in L$ többszörös gyöke f-nek a K test L bővítésében. Ekkor $f = (x-\alpha)^\ell g$, ahol $\ell \geqslant 2$ és $g \in L[x]$. Továbbá az is teljesül, hogy

$$\begin{aligned} D_x(f) &= \ell(x-\alpha)^{\ell-1} g + (x-\alpha)^\ell D_x(f) \\ &= (x-\alpha)^{\ell-1} \left(\ell g + (x-\alpha) D_x(f)\right). \end{aligned}$$

Tétel.

Legyen f a K test feletti polinom, és $\alpha \in L$ az f polinom gyöke a K test valamely L bővítésében. Ekkor α pontosan akkor többszörös gyöke f-nek, ha $\ln.k.o.(f, D_x(f))$ legalább elsőfokú polinom, amelynek gyöke α.

Bizonyítás.

Tegyük fel, hogy $\alpha \in L$ többszörös gyöke f-nek a K test L bővítésében. Ekkor $f = (x-\alpha)^\ell g$, ahol $\ell \geqslant 2$ és $g \in L[x]$. Továbbá az is teljesül, hogy

$$\begin{aligned} D_x(f) &= \ell(x-\alpha)^{\ell-1} g + (x-\alpha)^\ell D_x(f) \\ &= (x-\alpha)^{\ell-1} \left(\ell g + (x-\alpha) D_x(f)\right). \end{aligned}$$

Ekkor $x-\alpha$ osztója az f és $D_x(f)$ polinomoknak $L[x]$-ben, és így $x-\alpha \mid \ln.k.o.(f, D_x(f))$.

Bizonyítás (folytatás).

Tegyük fel, hogy az $f \in K[x]$ polinomnak ($f^* = n \in \mathbb{N}$) nincs többszörös gyöke a K test L bővítésében. Legyen $f = g_1 \cdots g_t$ az f polinom irreducibilis felbontása L felett, valamint legyen M az f polinom felbontási teste L felett:

$$f = \lambda(x - \alpha_1)^{\ell_1} \cdots (x - \alpha_s)^{\ell_s},$$

ahol $\lambda \in K$, $\alpha_1, \ldots, \alpha_s \in M$ páronként különböző elemek és $\ell_1 + \cdots + \ell_s = n$. Ekkor

$$D_x(f) = D_x(g_1) \cdot g_2 \cdots g_t + \cdots + g_1 \cdots g_{t-1} \cdot D_x(g_t).$$

Bizonyítás (folytatás).

Ha $\alpha_1, \ldots, \alpha_s \notin L$, akkor $\ln.k.o.(f, D_x(f))$-nek sem lehet gyöke L-ben. Tegyük fel, hogy valamely $i \in \{1, \ldots, s\}$-re $\alpha_i \in L$. Ekkor $g_j = x - \alpha_i$ irreducibilis tényezője f-nek, és $x - \alpha_i$-től különböző irreducibilis tényezőnek nem gyöke α_i. Így
$D_x(f)(\alpha_i) = g_1(\alpha_i) \cdots g_{j-1}(\alpha_i) \cdot D_x(x - \alpha_i)(\alpha_i) \cdot g_{j+1}(\alpha_i) \cdots g_t(\alpha_i) \neq 0$
miatt α_i nem lehet gyöke $\ln.k.o.(f, D_x(f))$-nek sem.

Következmény.

Legyen K olyan test, melynek karakterisztikája 0, valamint legyen f irreducibilis polinom K felett, melynek egy felbontási teste L. Ekkor az f polinom valamennyi gyöke egyszeres L-ben.

Következmény.

Legyen K olyan test, melynek karakterisztikája 0, valamint legyen f irreducibilis polinom K felett, melynek egy felbontási teste L. Ekkor az f polinom valamennyi gyöke egyszeres L-ben.

Következmény.

Ha a K testre $\mathrm{char}(K) = 0$ teljesül, akkor minden K feletti polinom szeparábilis.

Tétel.

Legyen K test és tegyük fel, hogy $f \in K[x]$ irreducibilis polinom. Ekkor az f polinom pontosan akkor nem szeparábilis, ha $\mathrm{char}(K) = p > 0$ és

$$f = a_n x^{np} + \cdots + a_1 x^p + a_0.$$

.

Tétel.

Tegyük fel, hogy a K testre $\mathrm{char}(K) = p > 0$ teljesül. Ekkor a $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ leképezés injektív homomorfizmus, valamint az $\alpha \in K$ elemre pontosan akkor teljesül, hogy $\mathfrak{F}(\alpha) = \alpha$, ha α a K test prímtestében van.

Tétel.

Tegyük fel, hogy a K testre $\mathrm{char}(K) = p > 0$ teljesül. Ekkor a $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ leképezés injektív homomorfizmus, valamint az $\alpha \in K$ elemre pontosan akkor teljesül, hogy $\mathfrak{F}(\alpha) = \alpha$, ha α a K test prímtestében van.

Definíció: Frobenius-endomorfizmus.

A fenti $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ leképezést Frobenius-endomorfizmusnak nevezzük.

Tétel.

Tegyük fel, hogy a K testre $\mathrm{char}(K) = p > 0$ teljesül. Ekkor a $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ leképezés injektív homomorfizmus, valamint az $\alpha \in K$ elemre pontosan akkor teljesül, hogy $\mathfrak{F}(\alpha) = \alpha$, ha α a K test prímtestében van.

Definíció: Frobenius-endomorfizmus.

A fenti $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ leképezést Frobenius-endomorfizmusnak nevezzük.

Következmény.

Ha $\mathrm{char}(K) = p > 0$ és a K test algebrai a prímteste felett, akkor a Frobenius-endomorfizmus automorfizmus.

Tétel.

Tegyük fel, hogy $\mathrm{char}(K) = p > 0$ és legyen

$$f = x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1x^p + a_0 \in K[x].$$

Ekkor az f polinom pontosan akkor irreducibilis K felett, ha a

$$g = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

polinom irreducibilis $K[x]$-ben és van olyan $i \in \{1, \ldots, n-1\}$ index, amelyre a_i nem p-hatvány K-ban.

Tétel.

Tegyük fel, hogy $\mathrm{char}(K) = p > 0$ és legyen

$$f = x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1x^p + a_0 \in K[x].$$

Ekkor az f polinom pontosan akkor irreducibilis K felett, ha a

$$g = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

polinom irreducibilis $K[x]$-ben és van olyan $i \in \{1, \ldots, n-1\}$ index, amelyre a_i nem p-hatvány K-ban.

Következmény.

Ha a p karakterisztikájú K test algebrai bővítése prímtestének, akkor minden K feletti polinom szeparábilis.