Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. április 3.

Tétel a primitív elemekről.

Tétel.

Az $L : K$ algebrai bővítés pontosan akkor egyszerű, ha az $L : K$ bővítés közbülső testeinek száma véges.

Tétel a primitív elemekről.

Tétel.

Az $L : K$ algebrai bővítés pontosan akkor egyszerű, ha az $L : K$ bővítés közbülső testeinek száma véges.

Bizonyítás.

Tegyük fel, hogy az $L : K$ testbővítés közbülső testeinek a száma véges. Ekkor L végesen generált K felett. Ha K is véges, akkor $L : K$ is véges. A továbbiakban tegyük fel, hogy K végtelen. Tegyük fel, hogy $r = \min\{|A| \mid L = K(A)\} \geqslant 2$ és $L = K(\alpha_1, \ldots, \alpha_r)$. Legyen $M = K(\alpha_1, \alpha_2)$ és tetszőleges $\beta \in K$-ra legyen $F_\beta = K(\alpha_1 + \beta\alpha_2)$. Legyen $\gamma \in K$ olyan elem, amelyre $F_\beta = F_\gamma$. Ekkor

$$\alpha_2 = (\beta - \gamma)^{-1}\big((\alpha_1 + \beta\alpha_2) - (\alpha_1 + \gamma\alpha_2)\big) \in F_\beta.$$

Valamint $\alpha_1 = (\alpha_1 + \beta\alpha_2) - \beta\alpha_2 \in F_\beta$ is teljesül, így $L = K(\alpha_1 + \beta\alpha_2, \alpha_3, \ldots, \alpha_r)$ ellentmondva az r-re vonatkozó feltevésnek.

Tétel a primitív elemekről.

Bizonyítás (folytatás).

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése K-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az m polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$.

Tétel a primitív elemekről.

Bizonyítás (folytatás).

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése K-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az m polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$.

Tétel a primitív elemekről.

Bizonyítás (folytatás).

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése K-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az m polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$. Ekkor $m_F = d_i$ teljesül valamely $i \in \{1, \ldots, k\}$-ra.

Tétel a primitív elemekről.

Bizonyítás (folytatás).

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése K-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az m polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$. Ekkor $m_F = d_i$ teljesül valamely $i \in \{1, \ldots, k\}$-ra. Legyen $m_F = a_0 + a_x + \cdots + a_r x^r$, valamint legyen $E = K(a_0, \ldots, a_r)$. Ekkor $E \leqslant F$ és m_F irreducibilis E felett.

Tétel a primitív elemekről.

Bizonyítás (folytatás).

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése K-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az m polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$. Ekkor $m_F = d_i$ teljesül valamely $i \in \{1, \ldots, k\}$-ra. Legyen $m_F = a_0 + a_x + \cdots + a_r x^r$, valamint legyen $E = K(a_0, \ldots, a_r)$. Ekkor $E \leqslant F$ és m_F irreducibilis E felett. Mivel $L = E(\alpha)$, ezért $[L : E] = m_F^* = [L : F]$. Azaz $F = E$.

Tétel a primitív elemekről.

Bizonyítás (folytatás).

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése K-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az m polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$. Ekkor $m_F = d_i$ teljesül valamely $i \in \{1, \ldots, k\}$-ra. Legyen $m_F = a_0 + a_x + \cdots + a_r x^r$, valamint legyen $E = K(a_0, \ldots, a_r)$. Ekkor $E \leqslant F$ és m_F irreducibilis E felett. Mivel $L = E(\alpha)$, ezért $[L : E] = m_F^* = [L : F]$. Azaz $F = E$. QED.

Tétel a primitív elemekről.

Tétel.

Ha az $L : K$ testbővítés véges és szeparábilis, akkor egyszerű.

Tétel a primitív elemekről.

Tétel.

Ha az $L : K$ testbővítés véges és szeparábilis, akkor egyszerű.

Bizonyítás.

Tegyük fel, hogy $L = K(\alpha_1, \ldots, \alpha_n)$ és legyen $g = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$. Legyen N a g polinom felbontási teste L felett. Ekkor N a K test felett is felbontási teste g-nek. Így az $N : K$ bővítés Galois-bővítés és $K = \varphi(\mathrm{Gal}(N : K))$.

Tétel a primitív elemekről.

Tétel.

Ha az $L : K$ testbővítés véges és szeparábilis, akkor egyszerű.

Bizonyítás.

Tegyük fel, hogy $L = K(\alpha_1, \ldots, \alpha_n)$ és legyen $g = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$. Legyen N a g polinom felbontási teste L felett. Ekkor N a K test felett is felbontási teste g-nek. Így az $N : K$ bővítés Galois-bővítés és $K = \varphi(\mathrm{Gal}(N : K))$.

Tétel a primitív elemekről.

Tétel.

Ha az $L : K$ testbővítés véges és szeparábilis, akkor egyszerű.

Bizonyítás.

Tegyük fel, hogy $L = K(\alpha_1, \ldots, \alpha_n)$ és legyen $g = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$. Legyen N a g polinom felbontási teste L felett. Ekkor N a K test felett is felbontási teste g-nek. Így az $N : K$ bővítés Galois-bővítés és $K = \varphi(\mathrm{Gal}(N : K))$. Mivel $\mathrm{Gal}(N : K)$ véges, ezért véges sok részcsoportja van, ami a Galoi-elmélet Főtétele szerint azt jelenti, hogy az $N : K$ testbővítés közbülső testeinek a száma is véges. Így az előző tétel szerint $L : K$ egyszerű.

Tétel a primitív elemekről.

Tétel.

Ha az $L : K$ testbővítés véges és szeparábilis, akkor egyszerű.

Bizonyítás.

Tegyük fel, hogy $L = K(\alpha_1, \ldots, \alpha_n)$ és legyen $g = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$. Legyen N a g polinom felbontási teste L felett. Ekkor N a K test felett is felbontási teste g-nek. Így az $N : K$ bővítés Galois-bővítés és $K = \varphi(\mathrm{Gal}(N : K))$. Mivel $\mathrm{Gal}(N : K)$ véges, ezért véges sok részcsoportja van, ami a Galoi-elmélet Főtétele szerint azt jelenti, hogy az $N : K$ testbővítés közbülső testeinek a száma is véges. Így az előző tétel szerint $L : K$ egyszerű. QED.

Definíció: diszkrimináns.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Az f polinom gyökei L-ben legyenek $\alpha_1, \ldots, \alpha_n$ (multiplicitással). Továbbá, legyen $\delta(f) = \prod_{1 \leqslant i < j \leqslant n}(\alpha_j - \alpha_i)$. A $\Delta(f) = \delta(f)^2 \in L$ elemet az f polinom **diszkriminánsának** nevezzük.

Definíció: diszkrimináns.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Az f polinom gyökei L-ben legyenek $\alpha_1, \ldots, \alpha_n$ (multiplicitással). Továbbá, legyen $\delta(f) = \prod_{1 \leqslant i < j \leqslant n}(\alpha_j - \alpha_i)$. A $\Delta(f) = \delta(f)^2 \in L$ elemet az f polinom **diszkriminánsának** nevezzük.

Példa.

Definíció: diszkrimináns.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Az f polinom gyökei L-ben legyenek $\alpha_1, \ldots, \alpha_n$ (multiplicitással). Továbbá, legyen $\delta(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i)$. A $\Delta(f) = \delta(f)^2 \in L$ elemet az f polinom **diszkriminánsának** nevezzük.

Példa.

$$\Delta(ax^2 + bx + c) = b^2 - 4ac,$$

Definíció: diszkrimináns.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Az f polinom gyökei L-ben legyenek $\alpha_1, \ldots, \alpha_n$ (multiplicitással). Továbbá, legyen $\delta(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i)$. A $\Delta(f) = \delta(f)^2 \in L$ elemet az f polinom **diszkriminánsának** nevezzük.

Példa.

$$\Delta(ax^2 + bx + c) = b^2 - 4ac,$$
$$\Delta(x^3 + px + q) = -4p^3 - 27q^2,$$

Definíció: diszkrimináns.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Az f polinom gyökei L-ben legyenek $\alpha_1, \ldots, \alpha_n$ (multiplicitással). Továbbá, legyen $\delta(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i)$. A $\Delta(f) = \delta(f)^2 \in L$ elemet az f polinom **diszkriminánsának** nevezzük.

Példa.

$$\Delta(ax^2 + bx + c) = b^2 - 4ac,$$
$$\Delta(x^3 + px + q) = -4p^3 - 27q^2,$$
$$\Delta(x^4 + 2) = 2048,$$

Tétel.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Legyen Δ az f polinom diszkriminánsa. Ekkor teljesülnek a következők.

Tétel.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Legyen Δ az f polinom diszkriminánsa. Ekkor teljesülnek a következők.

(i) Az f polinomnak pontosan akkor van többszörös gyöke L-ben, ha $\Delta = 0$.

Tétel.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Legyen Δ az f polinom diszkriminánsa. Ekkor teljesülnek a következők.

(i) Az f polinomnak pontosan akkor van többszörös gyöke L-ben, ha $\Delta = 0$.

(ii) Ha $\Delta \neq 0$ és $\delta \in K$, akkor $\mathrm{Gal}_K(f) \leqslant A_n$.

Tétel.

Legyen K olyan test, melyre $\mathrm{char}(K) \neq 2$ teljesül, és legyen $f \in K[x]$, melynek felbontási teste K felett L. Legyen Δ az f polinom diszkriminánsa. Ekkor teljesülnek a következők.

(i) Az f polinomnak pontosan akkor van többszörös gyöke L-ben, ha $\Delta = 0$.

(ii) Ha $\Delta \neq 0$ és $\delta \in K$, akkor $\mathrm{Gal}_K(f) \leqslant A_n$.

(iii) Ha $\delta \notin K$, akkor $\mathrm{Gal}_K(f) \not\leqslant A_n$ és $K(\delta) = \varphi(\mathrm{Gal}_K(f) \cap A_n)$.

Legyen K olyan test, amelyre $\mathrm{char}(K) \neq 2, 3$ teljesül, és legyen

$$f = x^3 + px + q$$

irreducibilis főpolinom K felett. Ekkor az f polinom gyökei a következők:

$$\alpha_1 = \frac{1}{3}(\beta + \gamma),$$
$$\alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma),$$
$$\alpha_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma),$$

ahol $\omega \neq 1$ harmadik egységgyök és $\beta\gamma = -3p$, $\beta^3 + \gamma^3 = -27q$.

Legyen K olyan test, amelyre $\mathrm{char}(K) \neq 2, 3$ teljesül, és legyen

$$f = x^4 + px^2 + qx + r$$

irreducibilis főpolinom K felett. Ekkor az f polinom gyökei a következők:

$$\alpha_1 = \frac{1}{2}(\beta + \gamma + \delta), \qquad \alpha_2 = \frac{1}{2}(\beta - \gamma - \delta),$$
$$\alpha_3 = \frac{1}{2}(-\beta + \gamma - \delta), \quad \alpha_4 = \frac{1}{2}(-\beta - \gamma + \delta),$$

ahol $\beta^2 + \gamma^2 + \delta^2 = -2p$, $\beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2 = p^2 - 4r$ és $\beta\gamma\delta = -q$. Azaz β^2, γ^2 és δ^2 a $g = x^3 + 2px^2 + (p^2 - 4r)x - q^2$ polinom gyökei. A g polinomot az f polinom **harmadfokú rezolvensének** nevezzük.

Definíció: primitív egységgyök, körosztási polinom.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Legyen L az $x^m - 1$ polinom felbontási teste K felett, és jelölje R_m e polinom gyökeinek halmazát L-ben. Ekkor $R_m \leqslant L^\times$ ciklikus. Az $\varepsilon \in L$ elemet **primitív m-edik egységgyöknek** nevezzük, ha $R_m = \langle \varepsilon \rangle$. Az **$m$-edik körosztási polinom**:

$$\Phi_m = \prod_{\varepsilon \in R_m} (x - \varepsilon).$$

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

(a) $x^m - 1 = \prod_{d|m} \Phi_d$.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

(a) $x^m - 1 = \prod_{d|m} \Phi_d$.

(b) $\Phi_m \in K_0[x]$.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

(a) $x^m - 1 = \prod_{d|m} \Phi_d$.

(b) $\Phi_m \in K_0[x]$.

Bizonyítás.

(a) Legyen L az $f = x^m - 1$ polinom felbontási teste és $\zeta \in L$ gyöke f-nek.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

(a) $x^m - 1 = \prod_{d|m} \Phi_d$.

(b) $\Phi_m \in K_0[x]$.

Bizonyítás.

(a) Legyen L az $f = x^m - 1$ polinom felbontási teste és $\zeta \in L$ gyöke f-nek.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

(a) $x^m - 1 = \prod_{d|m} \Phi_d$.

(b) $\Phi_m \in K_0[x]$.

Bizonyítás.

(a) Legyen L az $f = x^m - 1$ polinom felbontási teste és $\zeta \in L$ gyöke f-nek. Ekkor pontosan egy olyan $d \mid n$ természetes szám van, amelyre ζ primitív d-edik egységgyök.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Jelölje K_0 a K test prímtestét. Ekkor teljesülnek a következők:

(a) $x^m - 1 = \prod_{d|m} \Phi_d$.

(b) $\Phi_m \in K_0[x]$.

Bizonyítás.

(a) Legyen L az $f = x^m - 1$ polinom felbontási teste és $\zeta \in L$ gyöke f-nek. Ekkor pontosan egy olyan $d \mid n$ természetes szám van, amelyre ζ primitív d-edik egységgyök.

(b) Tudjuk, hogy ha $u, v \in K[x]$, $w \in L[x]$ és $u = wv$, akkor $w \in K[x]$ is teljesül.

Tétel.

Legyen K 0-karakterisztikájú test és m tetszőleges természetes szám. Ekkor

Tétel.

Legyen K 0-karakterisztikájú test és m tetszőleges természetes szám. Ekkor

(a) $\Phi_m \in \mathbb{Z}[x]$.

Tétel.

Legyen K 0-karakterisztikájú test és m tetszőleges természetes szám. Ekkor

(a) $\Phi_m \in \mathbb{Z}[x]$.

(b) Φ_m irreducibilis $\mathbb{Z}$ felett.

Tétel.

Legyen K 0-karakterisztikájú test és m tetszőleges természetes szám. Ekkor

(a) $\Phi_m \in \mathbb{Z}[x]$.

(b) Φ_m irreducibilis $\mathbb{Z}$ felett.

Bizonyítás.

(a) Tudjuk, hogy ha $u, v \in D[x]$, $w \in Q_D[x]$ és $u = wv$, akkor $w \in D[x]$ is teljesül, ahol Q_D a D ntegritástartomány hányadosteste.

Tétel.

Legyen K 0-karakterisztikájú test és m tetszőleges természetes szám. Ekkor

(a) $\Phi_m \in \mathbb{Z}[x]$.

(b) Φ_m irreducibilis $\mathbb{Z}$ felett.

Bizonyítás.

(a) Tudjuk, hogy ha $u, v \in D[x]$, $w \in Q_D[x]$ és $u = wv$, akkor $w \in D[x]$ is teljesül, ahol Q_D a D ntegritástartomány hányadosteste.

Tétel.

Legyen K 0-karakterisztikájú test és m tetszőleges természetes szám. Ekkor

(a) $\Phi_m \in \mathbb{Z}[x]$.

(b) Φ_m irreducibilis $\mathbb{Z}$ felett.

Bizonyítás.

(a) Tudjuk, hogy ha $u, v \in D[x]$, $w \in Q_D[x]$ és $u = wv$, akkor $w \in D[x]$ is teljesül, ahol Q_D a D ntegritástartomány hányadosteste.
(b) Tegyük fel, hogy $\Phi_m = fg$, ahol az $f \in \mathbb{Z}[x]$ főpolinom egy irreducibilis osztója Φ_m-nek. Legyen ζ egy olyan primitív egységgyök Q felett, amely gyöke f-nek és legyen $p \nmid m$ tetszőleges prímszám.

Bizonyítás (folytatás).

Tegyük fel, hogy ζ^p gyöke g-nek. Ekkor ζ gyöke a $g(x^p)$ polinomnak, és így $f \mid g$. Azaz van olyan $h \in \mathbb{Z}[x]$ polinom, amelyre $g(x^p) = f \cdot h$.

Bizonyítás (folytatás).

Tegyük fel, hogy ζ^p gyöke g-nek. Ekkor ζ gyöke a $g(x^p)$ polinomnak, és így $f \mid g$. Azaz van olyan $h \in \mathbb{Z}[x]$ polinom, amelyre $g(x^p) = f \cdot h$.

Bizonyítás (folytatás).

Tegyük fel, hogy ζ^p gyöke g-nek. Ekkor ζ gyöke a $g(x^p)$ polinomnak, és így $f \mid g$. Azaz van olyan $h \in \mathbb{Z}[x]$ polinom, amelyre $g(x^p) = f \cdot h$. Ekkor $\mathbb{Z}_p[x]$-ben teljesül, hogy $\overline{f} \cdot \overline{h} = \overline{g(x^p)} = \overline{g}^p$. Így $\overline{f}$-nek és $\overline{g}$-van közös irreduciblis osztója $\mathbb{Z}_p[x]$-ben.

Bizonyítás (folytatás).

Tegyük fel, hogy ζ^p gyöke g-nek. Ekkor ζ gyöke a $g(x^p)$ polinomnak, és így $f \mid g$. Azaz van olyan $h \in \mathbb{Z}[x]$ polinom, amelyre $g(x^p) = f \cdot h$. Ekkor $\mathbb{Z}_p[x]$-ben teljesül, hogy $\overline{f} \cdot \overline{h} = \overline{g(x^p)} = \overline{g}^p$. Így $\overline{f}$-nek és $\overline{g}$-van közös irreduciblis osztója $\mathbb{Z}_p[x]$-ben. Ez azonban ellentmondásra vezet. Így ζ^p is gyöke f-nek.

Bizonyítás (folytatás).

Tegyük fel, hogy ζ^p gyöke g-nek. Ekkor ζ gyöke a $g(x^p)$ polinomnak, és így $f \mid g$. Azaz van olyan $h \in \mathbb{Z}[x]$ polinom, amelyre $g(x^p) = f \cdot h$. Ekkor $\mathbb{Z}_p[x]$-ben teljesül, hogy $\overline{f} \cdot \overline{h} = \overline{g(x^p)} = \overline{g}^p$. Így $\overline{f}$-nek és $\overline{g}$-van közös irreduciblis osztója $\mathbb{Z}_p[x]$-ben. Ez azonban ellentmondásra vezet. Így ζ^p is gyöke f-nek. Legyen ξ egy tetszőleges gyöke Φ_m-nek. Ekkor van olyan m-hez relatív prím r egész, amelyre $\xi = \zeta^r$. Ebből pedig már következik, hogy ξ gyöke f-nek is. Azaz $f = \Phi_m$ is irreducibilis.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Ekkor $\mathrm{Gal}_K(\Phi_m)$ olyan Abel-csoport, amely izomorf R_m egy részcsoportjával. A Φ_m polinom pontosan akkor irreducibilis K felett, ha $\mathrm{Gal}_K(\Phi_m) \cong R_m$.

Tétel.

Legyen K tetszőleges test és m olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Ekkor $\mathrm{Gal}_K(\Phi_m)$ olyan Abel-csoport, amely izomorf R_m egy részcsoportjával. A Φ_m polinom pontosan akkor irreducibilis K felett, ha $\mathrm{Gal}_K(\Phi_m) \cong R_m$.

Bizonyítás.

Legyen L a Φ_m polinom felbontási teste K felett, és $\varepsilon \in L$ egy primitív m-edik egységgyök. Ekkor Φ_m gyökei L-ben:

$$\varepsilon^{n_1}, \ldots, \varepsilon^{n_k},$$

ahol $k = \varphi(m)$, és feltehető, hogy $n_1 = 1$.

Bizonyítás (folytatás).

Mivel $\ln.k.o.(n_i, m) = 1$ teljesül minden i-re $(1 \leqslant i \leqslant k)$, ezért $\{\overline{n_1}, \ldots, \overline{n_k}\} \leqslant \mathbb{Z}_m^\times = R_m$.

Bizonyítás (folytatás).

Mivel $\ln.k.o.(n_i, m) = 1$ teljesül minden i-re $(1 \leqslant i \leqslant k)$, ezért $\{\overline{n_1}, \ldots, \overline{n_k}\} \leqslant \mathbb{Z}_m^\times = R_m$.

Bizonyítás (folytatás).

Mivel $\ln.k.o.(n_i, m) = 1$ teljesül minden i-re $(1 \leqslant i \leqslant k)$, ezért $\{\overline{n_1}, \ldots, \overline{n_k}\} \leqslant \mathbb{Z}_m^\times = R_m$. Legyen σ a Φ_m polinom K feletti Galois-csoportjának egy tetszőleges eleme. Ekkor $\sigma(\varepsilon) = \varepsilon^{n_{i_\sigma}}$ teljesül valamely $1 \leqslant i_\sigma \leqslant k$-ra.

Bizonyítás (folytatás).

Mivel $\ln.k.o.(n_i, m) = 1$ teljesül minden i-re $(1 \leqslant i \leqslant k)$, ezért $\{\overline{n_1}, \ldots, \overline{n_k}\} \leqslant \mathbb{Z}_m^\times = R_m$. Legyen σ a Φ_m polinom K feletti Galois-csoportjának egy tetszőleges eleme. Ekkor $\sigma(\varepsilon) = \varepsilon^{n_{i_\sigma}}$ teljesül valamely $1 \leqslant i_\sigma \leqslant k$-ra. Definiáljuk a $\mathrm{j}\colon \mathrm{Gal}_K(\Phi_m) \to R_m$ leképezést úgy, hogy $\sigma \mapsto \overline{n_{i_\sigma}}$.

Bizonyítás (folytatás).

Mivel $\ln.k.o.(n_i, m) = 1$ teljesül minden i-re $(1 \leqslant i \leqslant k)$, ezért $\{\overline{n_1}, \ldots, \overline{n_k}\} \leqslant \mathbb{Z}_m^\times = R_m$. Legyen σ a Φ_m polinom K feletti Galois-csoportjának egy tetszőleges eleme. Ekkor $\sigma(\varepsilon) = \varepsilon^{n_{i_\sigma}}$ teljesül valamely $1 \leqslant i_\sigma \leqslant k$-ra. Definiáljuk a $\mathrm{j}\colon \mathrm{Gal}_K(\Phi_m) \to R_m$ leképezést úgy, hogy $\sigma \mapsto \overline{n_{i_\sigma}}$. Mivel tetszőleges $\sigma, \tau \in \mathrm{Gal}_K(\Phi_m)$-re

$$(\sigma\tau)(\varepsilon) = \varepsilon^{n_{i_\tau} \cdot n_{i_\sigma}} = \varepsilon^{n_{i_\sigma} \cdot n_{i_\tau}} = (\tau\sigma)(\varepsilon),$$

ezért j (injektív) homomorfizmus és $\mathrm{Gal}_K(\Phi_m)$ Abel-csoport.

Bizonyítás (folytatás).

Mivel $\ln.k.o.(n_i, m) = 1$ teljesül minden i-re $(1 \leqslant i \leqslant k)$, ezért $\{\overline{n_1}, \ldots, \overline{n_k}\} \leqslant \mathbb{Z}_m^\times = R_m$. Legyen σ a Φ_m polinom K feletti Galois-csoportjának egy tetszőleges eleme. Ekkor $\sigma(\varepsilon) = \varepsilon^{n_{i_\sigma}}$ teljesül valamely $1 \leqslant i_\sigma \leqslant k$-ra. Definiáljuk a $\mathrm{j}\colon \mathrm{Gal}_K(\Phi_m) \to R_m$ leképezést úgy, hogy $\sigma \mapsto \overline{n_{i_\sigma}}$. Mivel tetszőleges $\sigma, \tau \in \mathrm{Gal}_K(\Phi_m)$-re

$$(\sigma\tau)(\varepsilon) = \varepsilon^{n_{i_\tau} \cdot n_{i_\sigma}} = \varepsilon^{n_{i_\sigma} \cdot n_{i_\tau}} = (\tau\sigma)(\varepsilon),$$

ezért j (injektív) homomorfizmus és $\mathrm{Gal}_K(\Phi_m)$ Abel-csoport. Végül,

$$\begin{aligned} \mathrm{Gal}_K(\Phi_m) \cong R_m &\iff |\mathrm{Gal}_K(\Phi_m)| = \varphi(m) \\ &\iff |\{\sigma(\varepsilon) \mid \sigma \in \mathrm{Gal}_K(\Phi_m)\}| = \varphi(m) \\ &\iff \mathrm{Gal}_K(\Phi_m) \text{ tranzitív.} \end{aligned}$$

Ciklikus bővítések.

Tétel.

Legyen K tetszőleges test, $\vartheta \in K$ és n olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Legyen L az $^f = x^n - \vartheta \in K[x]$ polinom felbontási teste. Ekkor L tartalmaz egy ε primitív n-edik egységgyököt, és a $\mathrm{Gal}(L : K(\varepsilon))$ csoport ciklikus, melynek rendje n osztója. Valamint, az f polinom pontosan akkor irreducibilis $K(\varepsilon)$ felett, ha $[L : K(\varepsilon)] = n$.

Ciklikus bővítések.

Tétel.

Legyen K tetszőleges test, $\vartheta \in K$ és n olyan természetes szám, amelyre $\mathrm{char}(K) > 0$ esetén $\mathrm{char}(K) \nmid m$ teljesül. Legyen L az $^f = x^n - \vartheta \in K[x]$ polinom felbontási teste. Ekkor L tartalmaz egy ε primitív n-edik egységgyököt, és a $\mathrm{Gal}(L : K(\varepsilon))$ csoport ciklikus, melynek rendje n osztója. Valamint, az f polinom pontosan akkor irreducibilis $K(\varepsilon)$ felett, ha $[L : K(\varepsilon)] = n$.

Bizonyítás.

Legyen $\varepsilon \in L$ primitív n-edik egységgyök és $\beta \in L$ az f polinom egyik gyöke L-ben. Ekkor $x^n - \vartheta$ gyökei L-ben $\beta, \beta\varepsilon, \ldots, \beta\varepsilon^{n-1}$. Ekkor $L = K(\varepsilon, \beta)$ és a $\sigma \in \mathrm{Gal}(L : K(\varepsilon))$ automorfizmust egyértelműen meghatározza $\sigma(\beta)$: $\sigma(\beta) = \beta\varepsilon^{i_\sigma}$ valamely $i_\sigma \in \{0, 1, \ldots, n-1\}$-re.

Ciklikus bővítések.

Bizonyítás (folytatás).

Tekintsük a $\mathrm{j}\colon \mathrm{Gal}(L : K(\varepsilon)) \to \mathbb{Z}_n,\ \sigma \mapsto \overline{i_\sigma}$ leképezést.

Ciklikus bővítések.

Bizonyítás (folytatás).

Tekintsük a $\mathrm{j}\colon \mathrm{Gal}(L : K(\varepsilon)) \to \mathbb{Z}_n,\ \sigma \mapsto \overline{i_\sigma}$ leképezést.

Ciklikus bővítések.

Bizonyítás (folytatás).

Tekintsük a $\mathrm{j}\colon \mathrm{Gal}(L : K(\varepsilon)) \to \mathbb{Z}_n,\ \sigma \mapsto \overline{i_\sigma}$ leképezést. Ha $x^n - \vartheta$ irreducibilis $K(\varepsilon)$ felett, akkor $n = [L : K(\varepsilon)] = |\mathrm{Gal}(L : K(\varepsilon))|$. Ha $x^n - \vartheta$ nem irreducibilis $K(\varepsilon)$ felett, akkor legyen g egy irreducibilis osztója $K(\varepsilon)[x]$-ben.

Ciklikus bővítések.

Bizonyítás (folytatás).

Tekintsük a $\mathrm{j}\colon \mathrm{Gal}(L : K(\varepsilon)) \to \mathbb{Z}_n,\ \sigma \mapsto \overline{i_\sigma}$ leképezést. Ha $x^n - \vartheta$ irreducibilis $K(\varepsilon)$ felett, akkor $n = [L : K(\varepsilon)] = |\mathrm{Gal}(L : K(\varepsilon))|$. Ha $x^n - \vartheta$ nem irreducibilis $K(\varepsilon)$ felett, akkor legyen g egy irreducibilis osztója $K(\varepsilon)[x]$-ben. Ha γ gyöke g-nek, akkor $L = K(\gamma, \varepsilon)$ miatt

$$|\mathrm{Gal}(L : K(\varepsilon))| = [L : K(\varepsilon)] = [K(\gamma, \varepsilon) : K(\varepsilon)] = g^* < n.$$

QED.

Ciklikus bővítések.

Tétel (Abel-tétel).

Legyen K tetszőleges test, $\vartheta \in K$ és q olyan prímszám, amelyre $q \neq \mathrm{char}(K)$ teljesül. Ekkor $f = x^q - \vartheta$ vagy irreducibilis K felett vagy van gyöke K-ban. Ez utóbbi esetben $x^q - \vartheta$ pontosan akkor bomlik elsőfokú polinomok szorzatára K felett, ha K tartalmaz primitív q-adik egységgyököt.

Ciklikus bővítések.

Tétel (Abel-tétel).

Legyen K tetszőleges test, $\vartheta \in K$ és q olyan prímszám, amelyre $q \neq \mathrm{char}(K)$ teljesül. Ekkor $f = x^q - \vartheta$ vagy irreducibilis K felett vagy van gyöke K-ban. Ez utóbbi esetben $x^q - \vartheta$ pontosan akkor bomlik elsőfokú polinomok szorzatára K felett, ha K tartalmaz primitív q-adik egységgyököt.

Bizonyítás.

Tegyük fel, hogy $f \in K[x]$ nem irreducibilis. Legyen a $g \in K[x]$ irreducibilis főpolinom egy osztója f-nek. Legyen γ a g polinom egy gyöke az f polinom L felbontási testében.

Ciklikus bővítések.

Tétel (Abel-tétel).

Legyen K tetszőleges test, $\vartheta \in K$ és q olyan prímszám, amelyre $q \neq \mathrm{char}(K)$ teljesül. Ekkor $f = x^q - \vartheta$ vagy irreducibilis K felett vagy van gyöke K-ban. Ez utóbbi esetben $x^q - \vartheta$ pontosan akkor bomlik elsőfokú polinomok szorzatára K felett, ha K tartalmaz primitív q-adik egységgyököt.

Bizonyítás.

Tegyük fel, hogy $f \in K[x]$ nem irreducibilis. Legyen a $g \in K[x]$ irreducibilis főpolinom egy osztója f-nek. Legyen γ a g polinom egy gyöke az f polinom L felbontási testében.

Ciklikus bővítések.

Tétel (Abel-tétel).

Legyen K tetszőleges test, $\vartheta \in K$ és q olyan prímszám, amelyre $q \neq \mathrm{char}(K)$ teljesül. Ekkor $f = x^q - \vartheta$ vagy irreducibilis K felett vagy van gyöke K-ban. Ez utóbbi esetben $x^q - \vartheta$ pontosan akkor bomlik elsőfokú polinomok szorzatára K felett, ha K tartalmaz primitív q-adik egységgyököt.

Bizonyítás.

Tegyük fel, hogy $f \in K[x]$ nem irreducibilis. Legyen a $g \in K[x]$ irreducibilis főpolinom egy osztója f-nek. Legyen γ a g polinom egy gyöke az f polinom L felbontási testében. Ekkor

$$g = (x - \gamma\varepsilon^{n_1})(x - \gamma\varepsilon^{n_2}) \cdots (x - \gamma\varepsilon^{n_d}),$$

ahol $1 = n_1 < n_2 < \cdots < n_d \leqslant q - 1$ és ε primitív q-adik gyök.

Ciklikus bővítések.

Bizonyítás (folytatás).

Ekkor $g(0) = (-1)^d \gamma^d \varepsilon^k$, ahol $k = n_1 \cdots + n_d$. Legyen $g_0 = g(0)/(-1)^d = \gamma^d \varepsilon^k$.

Ciklikus bővítések.

Bizonyítás (folytatás).

Ekkor $g(0) = (-1)^d \gamma^d \varepsilon^k$, ahol $k = n_1 \cdots + n_d$. Legyen $g_0 = g(0)/(-1)^d = \gamma^d \varepsilon^k$.

Ciklikus bővítések.

Bizonyítás (folytatás).

Ekkor $g(0) = (-1)^d \gamma^d \varepsilon^k$, ahol $k = n_1 \cdots + n_d$. Legyen $g_0 = g(0)/(-1)^d = \gamma^d \varepsilon^k$. Ekkor azt kapjuk, hogy

$$g_0^q = \gamma^{dq} \varepsilon^{kq} = \gamma^{dq} = \vartheta^d.$$

Legyenek u és v olyan egészek, amelyekre $du + qv = 1$ teljesül.

Ciklikus bővítések.

Bizonyítás (folytatás).

Ekkor $g(0) = (-1)^d \gamma^d \varepsilon^k$, ahol $k = n_1 \cdots + n_d$. Legyen $g_0 = g(0)/(-1)^d = \gamma^d \varepsilon^k$. Ekkor azt kapjuk, hogy

$$g_0^q = \gamma^{dq} \varepsilon^{kq} = \gamma^{dq} = \vartheta^d.$$

Legyenek u és v olyan egészek, amelyekre $du + qv = 1$ teljesül. Ekkor $\vartheta = \vartheta^{du} \vartheta^{qv} = (g_0^u \vartheta^v)^q$, azaz $g_0^u \vartheta^v \in K$ gyöke f-nek.
Ha $x^q - \vartheta$ nem irreducibilis, akkor az előző tétel szerint $[L : K(\varepsilon)] < q$ és $[L : K(\varepsilon)] \mid q$, ezért $[L : K(\varepsilon)] = 1$, azaz $L = K(\varepsilon)$.

Ciklikus bővítések.

Bizonyítás (folytatás).

Ekkor $g(0) = (-1)^d \gamma^d \varepsilon^k$, ahol $k = n_1 \cdots + n_d$. Legyen $g_0 = g(0)/(-1)^d = \gamma^d \varepsilon^k$. Ekkor azt kapjuk, hogy

$$g_0^q = \gamma^{dq} \varepsilon^{kq} = \gamma^{dq} = \vartheta^d.$$

Legyenek u és v olyan egészek, amelyekre $du + qv = 1$ teljesül. Ekkor $\vartheta = \vartheta^{du} \vartheta^{qv} = (g_0^u \vartheta^v)^q$, azaz $g_0^u \vartheta^v \in K$ gyöke f-nek.
Ha $x^q - \vartheta$ nem irreducibilis, akkor az előző tétel szerint $[L : K(\varepsilon)] < q$ és $[L : K(\varepsilon)] \mid q$, ezért $[L : K(\varepsilon)] = 1$, azaz $L = K(\varepsilon)$. QED.

Ciklikus bővítések.

Definíció: karakter.

Legyen G csoport és K test. A $\chi\colon G \to K^\times$ leképezést **(K-értékű) karakternek** nevezzük G-**n**, ha χ homomorfizmus.

Ciklikus bővítések.

Definíció: karakter.

Legyen G csoport és K test. A $\chi\colon G \to K^\times$ leképezést **(K-értékű) karakternek** nevezzük G-**n**, ha χ homomorfizmus.

Tétel.

Legyen G csoport és K test, valamint S K-értékű karakternek egy halmaza G-n. Ekkor S lineárisan független K felett.

Ciklikus bővítések.

Definíció: karakter.

Legyen G csoport és K test. A $\chi\colon G \to K^\times$ leképezést **(K-értékű) karakternek** nevezzük G-**n**, ha χ homomorfizmus.

Tétel.

Legyen G csoport és K test, valamint S K-értékű karakternek egy halmaza G-n. Ekkor S lineárisan független K felett.

Bizonyítás.

Tegyük fel, hogy S nem lineárisan független K felett. Legyenek $\gamma_1, \ldots, \gamma_n \in S$ olyan karakterek, amelyek lineárisan függők K felet, de bármely valódi részrendszerük már lineárisan független. Ekkor $n \geqslant 2$ és

Ciklikus bővítések.

Definíció: karakter.

Legyen G csoport és K test. A $\chi\colon G \to K^\times$ leképezést **(K-értékű) karakternek** nevezzük G-**n**, ha χ homomorfizmus.

Tétel.

Legyen G csoport és K test, valamint S K-értékű karakternek egy halmaza G-n. Ekkor S lineárisan független K felett.

Bizonyítás.

Tegyük fel, hogy S nem lineárisan független K felett. Legyenek $\gamma_1, \ldots, \gamma_n \in S$ olyan karakterek, amelyek lineárisan függők K felet, de bármely valódi részrendszerük már lineárisan független. Ekkor $n \geqslant 2$ és

Ciklikus bővítések.

Definíció: karakter.

Legyen G csoport és K test. A $\chi\colon G \to K^\times$ leképezést **(K-értékű) karakternek** nevezzük G-**n**, ha χ homomorfizmus.

Tétel.

Legyen G csoport és K test, valamint S K-értékű karakternek egy halmaza G-n. Ekkor S lineárisan független K felett.

Bizonyítás.

Tegyük fel, hogy S nem lineárisan független K felett. Legyenek $\gamma_1, \ldots, \gamma_n \in S$ olyan karakterek, amelyek lineárisan függők K felet, de bármely valódi részrendszerük már lineárisan független. Ekkor $n \geqslant 2$ és van olyan $(\lambda_1, \ldots, \lambda_n) \in K^n \setminus \mathbf{0}$, amelyre minden $g \in G$ esetén $\lambda_1\gamma_1(g) + \cdots \lambda_n\gamma_n(g) = 0$.

Ciklikus bővítések.

Bizonyítás (folytatás).

Mivel $\gamma_1 \neq \gamma_n$, ezért van olyan $h \in G$, amelyre $\gamma_1(h) \neq \gamma_n(h)$.

Ciklikus bővítések.

Bizonyítás (folytatás).

Mivel $\gamma_1 \neq \gamma_n$, ezért van olyan $h \in G$, amelyre $\gamma_1(h) \neq \gamma_n(h)$.

Ciklikus bővítések.

Bizonyítás (folytatás).

Mivel $\gamma_1 \neq \gamma_n$, ezért van olyan $h \in G$, amelyre $\gamma_1(h) \neq \gamma_n(h)$. Ekkor bármely $g \in G$-re:

$$\begin{aligned} 0 &= \lambda_1\gamma_1(hg) + \cdots + \lambda_n\gamma_n(hg) \\ &= \lambda_1\gamma_1(h)\gamma_1(g) + \cdots + \lambda_n\gamma_n(h)\gamma_n(g) \end{aligned}$$

és

$$\lambda_1\gamma_n(h)\gamma_1(g) + \cdots + \lambda_n\gamma_n(h)\gamma_n(g) = 0$$

miatt $\lambda_1(\gamma_1(h) - \gamma_n(h))\gamma_1(g) + \cdots + \lambda_{n-1}(\gamma_{n-1}(h) - \gamma_n(h))\gamma_{n-1}(g) = 0$. Ez pedig ellentmondás.

Következmény.

Ha $\tau_1, \ldots, \tau_n$ a K test különböző automorfizmusai és $k_1, \ldots, k_n \in K \setminus \{0\}$, akkor van olyan $k \in K$, amelyre $k_1\tau_1(k) + \cdots + k_n\tau_n(k) \neq 0$ teljesül.

Ciklikus bővítések.

Tétel.

Legyen $L : K$ olyan n-edfokú ciklikus bővítés, amelyre $\mathrm{char}(K) \nmid n$ teljesül és K tartalmaz egy ε n-edik primitív egységgyököt. Ekkor van olyan $\vartheta \in K$, amelyre az $x^n - \vartheta$ polinom irreducibilis K felett és felbontási teste L. Ha $\beta \in L$ gyöke $x^n - \vartheta$-nak, akkor $L = K(\beta)$.

Ciklikus bővítések.

Tétel.

Legyen $L : K$ olyan n-edfokú ciklikus bővítés, amelyre $\mathrm{char}(K) \nmid n$ teljesül és K tartalmaz egy ε n-edik primitív egységgyököt. Ekkor van olyan $\vartheta \in K$, amelyre az $x^n - \vartheta$ polinom irreducibilis K felett és felbontási teste L. Ha $\beta \in L$ gyöke $x^n - \vartheta$-nak, akkor $L = K(\beta)$.

Bizonyítás.

Legyen $\mathrm{Gal}(L : K) = \langle \sigma \rangle$. Ekkor van olyan $\alpha \in L$, amelyre $\beta = \alpha + \varepsilon\sigma(\alpha) + \cdots + \varepsilon^{n-1}\sigma^{n-1}(\alpha) \neq 0$. Mivel $\sigma(\beta) = \varepsilon^{-1}\beta$, ezért $\beta \notin K$, valamint $\sigma(\beta^n) = \beta^n$ miatt $\beta^n \in K$.

Ciklikus bővítések.

Tétel.

Legyen $L : K$ olyan n-edfokú ciklikus bővítés, amelyre $\mathrm{char}(K) \nmid n$ teljesül és K tartalmaz egy ε n-edik primitív egységgyököt. Ekkor van olyan $\vartheta \in K$, amelyre az $x^n - \vartheta$ polinom irreducibilis K felett és felbontási teste L. Ha $\beta \in L$ gyöke $x^n - \vartheta$-nak, akkor $L = K(\beta)$.

Bizonyítás.

Legyen $\mathrm{Gal}(L : K) = \langle \sigma \rangle$. Ekkor van olyan $\alpha \in L$, amelyre $\beta = \alpha + \varepsilon\sigma(\alpha) + \cdots + \varepsilon^{n-1}\sigma^{n-1}(\alpha) \neq 0$. Mivel $\sigma(\beta) = \varepsilon^{-1}\beta$, ezért $\beta \notin K$, valamint $\sigma(\beta^n) = \beta^n$ miatt $\beta^n \in K$.

Ciklikus bővítések.

Tétel.

Legyen $L : K$ olyan n-edfokú ciklikus bővítés, amelyre $\mathrm{char}(K) \nmid n$ teljesül és K tartalmaz egy ε n-edik primitív egységgyököt. Ekkor van olyan $\vartheta \in K$, amelyre az $x^n - \vartheta$ polinom irreducibilis K felett és felbontási teste L. Ha $\beta \in L$ gyöke $x^n - \vartheta$-nak, akkor $L = K(\beta)$.

Bizonyítás.

Legyen $\mathrm{Gal}(L : K) = \langle \sigma \rangle$. Ekkor van olyan $\alpha \in L$, amelyre $\beta = \alpha + \varepsilon\sigma(\alpha) + \cdots + \varepsilon^{n-1}\sigma^{n-1}(\alpha) \neq 0$. Mivel $\sigma(\beta) = \varepsilon^{-1}\beta$, ezért $\beta \notin K$, valamint $\sigma(\beta^n) = \beta^n$ miatt $\beta^n \in K$. Mivel $\varepsilon \in K$, ezért $K(\beta)$ felbontási teste az $x^n - \beta^n \in K[x]$ polinomnak. Továbbá $\sigma^0|_{K(\beta)}, \ldots, \sigma^{n-1}|_{K(\beta)} \in \mathrm{Gal}(K(\beta) : K)$, ezért $[K(\beta) : K] = |\mathrm{Gal}(K(\beta) : K)| \geqslant n$. Így $L = K(\beta)$ és $x^n - \beta^n$ irreducibilis.

Tétel.

Legyen $L : K$ olyan Galois-bővítés, amelynek Galois-csoportja d-exponensű Abel-csoport és az $x^d - 1$ polinomnak d különböző gyöke van K-ban. Ekkor vannak olyan $\vartheta_1, \ldots, \vartheta_r \in K$ elemek, amelyekre L az $(x^d - \vartheta_1) \cdots (x^d - \vartheta_r)$ polinom felbontási teste K felett.

Tétel.

Legyen $L : K$ olyan Galois-bővítés, amelynek Galois-csoportja d-exponensű Abel-csoport és az $x^d - 1$ polinomnak d különböző gyöke van K-ban. Ekkor vannak olyan $\vartheta_1, \ldots, \vartheta_r \in K$ elemek, amelyekre L az $(x^d - \vartheta_1) \cdots (x^d - \vartheta_r)$ polinom felbontási teste K felett.

Definíció: Kummer-bővítés.

Az $L : K$ testbővítést d-**exponensű Kummer-bővítésnek** nevezzük, ha L egy $(x^d - \vartheta_1) \cdots (x^d - \vartheta_r)$ alakú polinom felbontási teste K felett $(\vartheta_1, \ldots, \vartheta_r \in K)$ és az $x^d - 1$ polinomnak d különböző gyöke van K-ban.

Tétel.

Ha az $L : K$ testbővítés d-exponensű Kummer-bővítés, akkor $\mathrm{Gal}(L : K)$ olyan Abel-csoport, melynek exponense osztja d-t.