Magasabbfokú egyenletek és geometriai szerkeszthetőség

Dormán Miklós

SZTE, Bolyai Intézet

2010. október 8.

Definíció: felbontási test.

Legyen K test, és $f \in K[x] \setminus \{0\}$ tetszőleges polinom. Azt mondjuk, hogy a K test L bővítése **felbontási teste** f**-nek** K **felett**, ha f elsőfokú tényezők szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

Definíció: felbontási test.

Legyen K test, és $f \in K[x] \setminus \{0\}$ tetszőleges polinom. Azt mondjuk, hogy a K test L bővítése **felbontási teste** f**-nek** K **felett**, ha f elsőfokú tényezők szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

A felbontási test definíciójának közvetlen következménye az alábbi állítás.

Definíció: felbontási test.

Legyen K test, és $f \in K[x] \setminus \{0\}$ tetszőleges polinom. Azt mondjuk, hogy a K test L bővítése **felbontási teste** f**-nek** K **felett**, ha f elsőfokú tényezők szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

A felbontási test definíciójának közvetlen következménye az alábbi állítás.

Állítás.

Ha L felbontási teste az $f \in K[x]$ polinomnak K felett, akkor az $L : K$ bővítés véges algebrai bővítés.

Példa.

Tekintsük az $f = x^2 + 1 \in \mathbb{Q}[x]$ polinomot. Mivel f-nek pontosan két gyöke van $\mathbb{C}$-ben, ezért felbontási teste

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Példa.

Tekintsük az $f = x^2 + 1 \in \mathbb{Q}[x]$ polinomot. Mivel f-nek pontosan két gyöke van $\mathbb{C}$-ben, ezért felbontási teste

$$\mathbb{Q}(i, -i) = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Példa.

Legyen $f = x^3 - 2 \in \mathbb{Q}[x]$. Az f polinom gyökei $\mathbb{C}$-ben: $\varepsilon^k \sqrt[3]{2}$ $(k = 0, 1, 2)$, ahol $\varepsilon = \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}$. Ekkor f felbontási teste $\mathbb{Q}$ felett

$$\mathbb{Q}(\sqrt[3]{2}, \varepsilon\sqrt[3]{2}, \varepsilon^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon).$$

Tétel (A felbontási test létezése).

Legyen K test, és f n-edfokú ($n \in \mathbb{N}$) polinom K felett. Ekkor f-nek van felbontási teste, és az f polinom tetszőleges L felbontási testére $[L : K] \leqslant n!$ teljesül.

Tétel (A felbontási test létezése).

Legyen K test, és f n-edfokú ($n \in \mathbb{N}$) polinom K felett. Ekkor f-nek van felbontási teste, és az f polinom tetszőleges L felbontási testére $[L : K] \leqslant n!$ teljesül.

Bizonyítás.

Az állítást az f polinom fokszáma szerinti indukcióval bizonyítjuk. Ha $f^* \leqslant 1$, akkor az állítás nyilvánvalóan teljesül. Tegyük fel, hogy az állítás igaz tetszőleges K testre és tetszőleges K feletti legfeljebb $(n-1)$-edfokú polinomra. Legyen f egy n-edfokú polinom. A továbbiakban a bizonyítás két esetre bomlik aszerint, hogy f reducibilis vagy irreducibilis.

Bizonyítás (folytatás).

1. eset. Ha f reducibilis $K[x]$-ben, akkor $f = gh$ teljesül valamely $g, h \in K[x]$ polinomokra, ahol $1 \leqslant g^* = s,\ h^* = t < n$. Az indukciós feltevés szerint van a K testnek egy olyan L bővítése, amely felbontási teste az g polinomnak K felett és $[L : K] \leqslant s!$. Ekkor

$$g = \lambda(x - \alpha_1) \cdots (x - \alpha_s),$$

ahol $\alpha_1, \ldots, \alpha_s \in L$, $\lambda \in K$ és $L = K(\alpha_1, \ldots, \alpha_s)$. Tekintsük a $h \in K[x] \subseteq L[x]$ polinomot. Szintén az indukciós feltevés szerint van az L testnek egy olyan M bővítése, amely felbontási teste a h polinomnak az L test felett és $[M : L] \leqslant t!$.

Bizonyítás (folytatás).

Ekkor

$$h = \mu(x - \beta_1) \cdots (x - \beta_t),$$

ahol $\beta_1, \ldots, \beta_t \in M$, $\mu \in L$ és $M = L(\beta_1, \ldots, \beta_t)$. Továbbá,

$$f = \lambda\mu(x - \alpha_1) \cdots (x - \alpha_s)(x - \beta_1) \cdots (x - \beta_t)$$

miatt $\lambda\mu \in K$, valamint $M = K(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t)$, azaz M felbontási teste f-nek K felett. Valamint, a Fokszámtétel miatt az

$$[M : K] = [M : L] \cdot [L : K] \leqslant t!s! \leqslant (s + t)! \leqslant n!$$

egyenlőtlenség is teljesül.

Bizonyítás (folytatás).

2. eset. Ha f irreducibilis K felett, akkor tekintsük a K test $L = K[x]/(f)$ bővítését. Tudjuk, hogy $\alpha = x + (f) \in L$ gyöke f-nek, $L = K(\alpha)$ és $[L : K] = n$. A Bézout-tétel szerint $f = (x - \alpha)h$ teljesül valamely $(n-1)$-edfokú $h \in L[x]$ polinomra. Alkalmazzuk az indukciós feltevést h-ra: az L testnek van egy olyan M bővítése, mely felbontási teste h-nak L felett és $[M : L] \leqslant (n-1)!$. Ekkor $h = \mu(x - \beta_1) \cdots (x - \beta_{n-1})$, ahol $\beta_1, \ldots, \beta_{n-1} \in M$, $\mu \in L$ és $M = L(\beta_1, \ldots, \beta_{n-1})$. Ezért azt kapjuk, hogy

$$f = \mu(x - \alpha)(x - \beta_1) \cdots (x - \beta_{n-1})$$

miatt $\mu \in K$, továbbá $M = L(\beta_1, \ldots, \beta_{n-1}) = K(\alpha, \beta_1, \ldots, \beta_{n-1})$, azaz M felbontási teste f-nek K felett. Végül a Fokszámtétel következtében $[M : K] = [M : L] \cdot [L : K] \leqslant (n-1)!n = n!$ is teljesül.

Legyenek K_1, K_2 testek, és $\eta\colon K_1 \to K_2$ izmorfizmus. Tetszőleges $f = \sum_{k=0}^{n} a_i x^i \in K_1[x]$ polinomra legyen

$$\eta_f = \sum_{k=0}^{n} (a_i \eta) x^i \in K_2[x].$$

Egyszerűen igazolható, hogy a $K_1[x] \to K_2[x],\ f \mapsto \eta_f$ leképezés izomorfizmus.

Tétel (A felbontási test egyértelműsége.)

Legyenek K, K' testek, $\eta\colon K \to K'$ izomorfizmus, és $f \in K[x]$ egy n-edfokú polinom ($n \geqslant 1$). Legyenek továbbá rendre L és L' az f és η_f polinomok felbontási testei a K, illetve K' testek felett. Ekkor η kiterjeszthető egy $L \to L'$ izomorfizmussá. Továbbá, az η izomorfizmust legfeljebb $[L : K]$ féleképpen tudjuk kiterjeszteni; a kiterjesztések száma pontosan $[L : K]$, ha η_f gyökei páronként különbözőek L'-ben.

Vizsgáljuk meg azt az esetet, amikor az előző tételben $K = K'$ teljesül, és $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$, és a következőt kapjuk.

Vizsgáljuk meg azt az esetet, amikor az előző tételben $K = K'$ teljesül, és $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$, és a következőt kapjuk.

Következmény.

Legyen K tetszőleges test, $f \in K[x]$, és L, L' az f polinom felbontási testei. Ekkor az L és L' testek izomorfak, sőt olyan $L \to L'$ izomorfizmus is van, amely a $K(\subseteq L, L')$ test elemeit fixen hagyja. Továbbá, pontosan annyi a K test elemeit fixen hagyó $L \to L'$ izomorfizmus van ahány különböző gyöke van f-nek L-ben.

Legyen f legalább elsőfokú polinom a K test felett, és legyen L az f polinom 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) deriválás.

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** $K[x]$-en, 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** $K[x]$-en, 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) $\ker(D_x) = K$, és a D_x leképezés szürjektív.

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 $\ln.\mathrm{k.o.}(f, D_x(f))$ 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 $\ln.k.o.(f, D_x(f))$ 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 $g \in L[x]$. Így a formális deriválás (2) tulajdonsága szerint

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

Ekkor $x-\alpha$ osztója az f és $D_x(f)$ polinomoknak $L[x]$-ben, és így $x-\alpha \mid \ln.k.o.(f, D_x(f))$. Azaz $\ln.k.o.(f, D_x(f))$ legalább elsőfokú polinom, melynek gyöke az α.

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.

Ha f irreducibilis polinom a K számtest felett, melynek felbontási teste L, akkor az f polinom valamennyi gyöke egyszeres L-ben.

Következmény.

Ha f irreducibilis polinom a K számtest felett, melynek felbontási teste L, akkor az f polinom valamennyi gyöke egyszeres L-ben.

Bizonyítás.

Mivel $D_x(f)^* = n - 1$ és az f polinom irreducibilis, ezért

$$\text{ln.k.o.}(f, D_x(f)) \sim 1,$$

így f-nek nem lehet többszörös gyöke L-ben.

Példa.

Legyen $f = \sum_{j=0}^{n} \frac{x^j}{j!} \in \mathbb{Q}[x]$ $(n \geqslant 1)$. Ekkor $D_x(f) = \sum_{j=0}^{n-1} \frac{x^j}{j!}$.
Legyen $d = \text{ln.k.o.}(f, D_x(f))$. Mivel $d \mid f, D_x(f)$, ezért
$d \mid f - D_x(f) = \frac{x^n}{n!}$. Így d-nek legfeljebb egy gyöke van $\mathbb{C}$-ben, a 0, ami azonban nem gyöke f-nek. Azaz f-nek nincs többszörös gyöke.

Definíció: szeparábilis polinom.

Legyen f irreducibilis polinom a K test felett ($f^* = n \geqslant 1$). Az f polinom **szeparábilis**, ha f-nek n különböző gyöke van L-ben, ahol L az f polinom felbontási teste K felett.
A $g \in K[x]$ polinom **szeparábilis**, ha g minden irreducibilis tényezője szeparábilis.

Definíció: szeparábilis polinom.

Legyen f irreducibilis polinom a K test felett ($f^* = n \geqslant 1$). Az f polinom **szeparábilis**, ha f-nek n különböző gyöke van L-ben, ahol L az f polinom felbontási teste K felett.
A $g \in K[x]$ polinom **szeparábilis**, ha g minden irreducibilis tényezője szeparábilis.

Példa.

Ha K számtest, akkor minden $K[x]$-beli polinom szeparábilis.

Definíció: alegbrailag zárt test, algebrai lezárt.

Azt mondjuk, hogy az L test **algebrailag zárt**, ha bármely $f \in L[x]$ polinomnak van gyöke L-ben.
A K test L testbővítése K **algebrai lezártja**, ha $L : K$ algebrai és L algebrailag zárt.

Definíció: alegbrailag zárt test, algebrai lezárt.

Azt mondjuk, hogy az L test **algebrailag zárt**, ha bármely $f \in L[x]$ polinomnak van gyöke L-ben.
A K test L testbővítése K **algebrai lezártja**, ha $L : K$ algebrai és L algebrailag zárt.

Példa.

Az Algebra Alaptétele éppen azt állítja, hogy a komlex számok $\mathbb{C}$ teste algebrailag zárt, azonban $\mathbb{C}$ nem algebrai lezártja $\mathbb{Q}$-nak, mivel $\mathbb{C}$ nem minden eleme algebrai $\mathbb{Q}$ felett.

Példa.

Legyen $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Q}[x]$ és $\alpha = \sqrt[3]{2}$.

Példa.

Legyen $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Q}[x]$ és $\alpha = \sqrt[3]{2}$.

Példa.

Legyen $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Q}[x]$ és $\alpha = \sqrt[3]{2}$. Ekkor f-nek van gyöke az $L = \mathbb{Q}(\alpha, \varepsilon)$ testben, mivel $f(\alpha + \varepsilon) = 0$.

Példa.

Legyen $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Q}[x]$ és $\alpha = \sqrt[3]{2}$. Ekkor f-nek van gyöke az $L = \mathbb{Q}(\alpha, \varepsilon)$ testben, mivel $f(\alpha + \varepsilon) = 0$. Valamint — első látásra talán meglepő módon — f elsőfokú tényezők szorzatára bomlik L felett:

Példa.

Legyen $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Q}[x]$ és $\alpha = \sqrt[3]{2}$. Ekkor f-nek van gyöke az $L = \mathbb{Q}(\alpha, \varepsilon)$ testben, mivel $f(\alpha + \varepsilon) = 0$. Valamint — első látásra talán meglepő módon — f elsőfokú tényezők szorzatára bomlik L felett:

$$\begin{aligned} f =& (x + 1 + \varepsilon - \alpha) \cdot (x + 1 - \varepsilon\alpha + \varepsilon) \cdot (x + 1 + \alpha + \varepsilon\alpha + \varepsilon) \cdot \\ & (x - \varepsilon + \alpha + \varepsilon\alpha) \cdot (x - \varepsilon - \varepsilon\alpha) \cdot (x - \varepsilon - \alpha). \end{aligned}$$

Példa.

Legyen $f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9 \in \mathbb{Q}[x]$ és $\alpha = \sqrt[3]{2}$. Ekkor f-nek van gyöke az $L = \mathbb{Q}(\alpha, \varepsilon)$ testben, mivel $f(\alpha + \varepsilon) = 0$. Valamint — első látásra talán meglepő módon — f elsőfokú tényezők szorzatára bomlik L felett:

$$\begin{aligned} f =& (x + 1 + \varepsilon - \alpha) \cdot (x + 1 - \varepsilon\alpha + \varepsilon) \cdot (x + 1 + \alpha + \varepsilon\alpha + \varepsilon) \cdot \\ & (x - \varepsilon + \alpha + \varepsilon\alpha) \cdot (x - \varepsilon - \varepsilon\alpha) \cdot (x - \varepsilon - \alpha). \end{aligned}$$

Tétel.

Legyen L felbontási teste az $f \in K[x]$ polinomnam K felett. Ha a $g \in K[x]$ irreducibilis polinom, akkor g-nek vagy valamennyi gyöke benne van L-ben, vagy nincs egyetlen gyöke sem 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.

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.

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.

Következmény.

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

Tétel.

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

Vajon mi a helyzet az $M : K$ bővítéssel? Legyen ε 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. 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.

Definíció: Galois-kapcsolat.

Legyenek A és B tetszőleges halmazok, és $\Delta \subseteq A \times B$. Legyenek φ és γ a következő leképezések:

$$\varphi\colon P(A) \to P(B), \quad U \mapsto \{b \in B \mid (u,b) \in \Delta \text{ minden } u \in U\text{-ra}\},$$
$$\gamma\colon P(B) \to P(A), \quad V \mapsto \{a \in A \mid (a,v) \in \Delta \text{ minden } v \in V\text{-re}\}.$$

A (φ, γ) leképezéspárt a $P(A)$ és $P(B)$ halmazok közötti (a Δ megfeleltetéshez tartozó) **Galois-kapcsolatnak** nevezzük.

Definíció: antimonoton leképezés.

Legyenek A és B tetszőleges halmazok, $\xi\colon P(A) \to P(B)$ tetszőleges leképezések. Ekkor azt mondjuk, hogy a ξ leképezés **antimonoton**, ha bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\xi(U') \subseteq \xi(U)$.

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és
- idempotens, azaz bármely $U \in P(A)$-ra $\omega(\omega(U)) = \omega(U)$.

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és
- idempotens, azaz bármely $U \in P(A)$-ra $\omega(\omega(U)) = \omega(U)$.

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és
- idempotens, azaz bármely $U \in P(A)$-ra $\omega(\omega(U)) = \omega(U)$.

Azt mondjuk, hogy az $U \subseteq A$ halmaz **zárt ω-ra vonatkozóan**, ha $\omega(U) = U$.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

(1) A φ és γ leképezések antimonotonok.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

(1) A φ és γ leképezések antimonotonok.

(2) A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás a B, illetve az A halmazon.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

(1) A φ és γ leképezések antimonotonok.

(2) A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás a B, illetve az A halmazon.

(3) Az $U \subseteq A$ halmaz pontosan akkor zárt $\gamma\varphi$-re vonatkozóan, ha van olyan $V \subseteq B$, amelyre $U = \gamma(V)$.

Bizonyítás.

Bizonyítás.

Bizonyítás.

(1) Az állítás nyilvánvaló.

Bizonyítás.

(1) Az állítás nyilvánvaló.
(2) Az állítást $\varphi\gamma$-ra igazoljuk, $\gamma\varphi$-re az állítás hasonlóan igazolható. Legyen $U, U' \in P(A)$, $U \subseteq U'$. Ekkor (1) felhasználva azt kapjuk, hogy $\gamma(U') \subseteq \gamma(U)$, és így szintén (1) szerint:

$$\varphi\gamma(U) = \varphi(\gamma(U)) \subseteq \varphi(\gamma(U')) = \varphi\gamma(U'),$$

azaz $\varphi\gamma$ monoton ($\gamma\varphi$ monoton).
Legyen V tetszőleges részhalmaza B-nek. Tegyük fel, hogy van olyan $v \in V$, amely nem eleme $\varphi\gamma(V)$-nek. Ekkor

$$v \notin \varphi\gamma(V) \Longleftrightarrow \text{van olyan } u_0 \in \gamma(V), \text{ amelyre } (u_0, v) \notin \Delta.$$

Bizonyítás (folytatás).

Így azonban γ definíciója miatt azt kapjuk, hogy

$$u_0 \in \gamma(V) \Longleftrightarrow \text{minden } v \in V\text{-re, } (u_0, v) \in \Delta,$$

ami ellentmond az előzőeknek. Ezzel igazoltuk, hogy $\varphi\gamma$ extenzív ($\gamma\varphi$ extenzív). Legyen V tetszőleges részhalmaza B-nek. Ekkor $\varphi\gamma$ extenzivitása miatt $V \subseteq \varphi\gamma(V)$, és így felhasználva, hogy γ antimonoton azt kapjuk, hogy $\gamma(V) \supseteq \gamma(\varphi\gamma(V)) = \gamma\varphi\gamma(V)$. Másrészt, $\gamma\varphi$ extenzitvitása miatt $\gamma(V) \subseteq \gamma\varphi(\gamma(V)) = \gamma\varphi\gamma(V)$, így azt kapjuk, hogy

$$\gamma(V) = \gamma\varphi\gamma(V). \tag{1}$$

Bizonyítás (folytatás).

Ebből pedig már következik, hogy

$$\varphi\gamma\varphi\gamma(V) = \varphi\gamma(V),$$

azaz $\varphi\gamma$ idempotens ($\gamma\varphi$ idempotens). Ezzel igazoltuk, hogy a $\varphi\gamma$ és $\gamma\varphi$ leképezések polaritások.
(3) Tegyük fel, hogy $U \subseteq A$ zárt $\gamma\varphi$-re vonatkozóan, azaz $\gamma\varphi(U) = U$. Ekkor $V = \varphi(U) \subseteq B$-re teljesül, hogy $U = \gamma\varphi(U) = \gamma(\varphi(U)) = \gamma(V)$. Fordítva, tegyük fel, hogy $U = \gamma(V)$ valamely $V \subseteq B$-re. Ekkor (1) miatt

$$U = \gamma(V) = \gamma\varphi\gamma(V) = \gamma\varphi(\gamma(V)) = \gamma\varphi(U),$$

azaz U zárt $\gamma\varphi$-re vonatkozóan. Ezzel a tétel állításait igazoltuk.

Példa.

Legyen L test, $A = \mathrm{Aut}(L)$, $B = L$, valamint legyen Δ az alábbi megfeleltetés A-ból B-be: $\Delta = \{(\sigma, a) \in \mathrm{Aut}(L) \times L \mid \sigma(a) = a\}$. Ekkor tetszőleges $U \subseteq \mathrm{Aut}(L)$, $V \subseteq L$ halmazokra azt kapjuk, hogy

$$\begin{aligned}
\varphi(U) &= \{a \in L \mid (\tau, a) \in \Delta \text{ minden } \tau \in U\text{-ra}\}, \\
&= \{a \in L \mid \tau(a) = a \text{ minden } \tau \in U\text{-ra}\}, \\
\gamma(V) &= \{\sigma \in \mathrm{Aut}(L) \mid (\sigma, v) \in \Delta \text{ minden } v \in V\text{-re}\}, \\
&= \{\sigma \in \mathrm{Aut}(L) \mid \sigma(v) = v \text{ minden } v \in V\text{-re}\},
\end{aligned}$$

azaz $\varphi(U)$ azon L-beli elemek halmaza, melyeket U valamennyi eleme fixen hagy, illetve $\gamma(V)$ az L test automorfizmuscsoportjának azon elemeit tartalmazza, amelyek minden V-beli elemet fixen hagynak.

A továbbiakban rögzítsük az L testet és a (φ, γ) Galois-kapcsolatot.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Bizonyítás.

Az, hogy $\varphi(U)$ test, azaz részteste L-nek, nyilvánvaló. Mivel $U \subseteq \langle U \rangle$, ezért φ antimonotonitása miatt $\varphi(\langle U \rangle) \subseteq \varphi(U)$. Felhasználva, hogy $\gamma\varphi(U)$ olyan részcsoportja $\mathrm{Aut}(L)$-nek, amely tartalmazza U-t, azt kapjuk, hogy $U \subseteq \langle U \rangle \subseteq \gamma\varphi(U)$. A Galois-kapcsolatok tulajdonságait alkalmazva azt kapjuk, hogy

$$\varphi(U) = \varphi\gamma\varphi(U) = \varphi(\gamma\varphi(U)) \subseteq \varphi(\langle U \rangle) \subseteq \varphi(U),$$

azaz $\varphi(U) = \varphi(\langle U \rangle)$. Ezzel az állítást igazoltuk.

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\mathrm{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\mathrm{Aut}(L)$-nek. Tetszőleges $\alpha \in L$-re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha \colon G \to L, \quad \sigma \mapsto \sigma(\alpha).$$

Mivel L^G vektortér L felett, ezért L^G a $\varphi(G) \leqslant L$ test felett is vektortér.

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\mathrm{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\mathrm{Aut}(L)$-nek. Tetszőleges $\alpha \in L$-re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha \colon G \to L, \quad \sigma \mapsto \sigma(\alpha).$$

Mivel L^G vektortér L felett, ezért L^G a $\varphi(G) \leqslant L$ test felett is vektortér.

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

(1) A lineárisan független $\varphi(G)$ felett;

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\mathrm{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\mathrm{Aut}(L)$-nek. Tetszőleges $\alpha \in L$-re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha \colon G \to L, \quad \sigma \mapsto \sigma(\alpha).$$

Mivel L^G vektortér L felett, ezért L^G a $\varphi(G) \leqslant L$ test felett is vektortér.

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

(1) A lineárisan független $\varphi(G)$ felett;

(2) $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett;

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\mathrm{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\mathrm{Aut}(L)$-nek. Tetszőleges $\alpha \in L$-re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha \colon G \to L, \quad \sigma \mapsto \sigma(\alpha).$$

Mivel L^G vektortér L felett, ezért L^G a $\varphi(G) \leqslant L$ test felett is vektortér.

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

(1) A lineárisan független $\varphi(G)$ felett;

(2) $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett;

(3) $\{T_\alpha \mid \alpha \in A\}$ lineárisan független L felett.

Definíció: Galos-bővítés.

Az $L : K$ testbővítést **Galois-bővítésnek** hívjuk, ha véges és normális.

Definíció: Galos-bővítés.

Az $L : K$ testbővítést **Galois-bővítésnek** hívjuk, ha véges és normális.

Lemma.

Legyenek K, L és L' testek. Tegyük fel, hogy az $L : K$ bővítés d-edfokú és $\eta\colon K \to L'$ injektív homomorfizmus. Ekkor ha tetszőleges $\alpha \in L$-re $\eta_{m_{\alpha,K}}$ lineáris tényezőkre bomlik L' felett, akkor pontosan d darab injektív $L \to L'$ homomorfizmus van, amely kiterjesztése η-nak; ellenkező esetben d-nél kevesebb kiterjesztése van.

Tétel (A Galois-bővítések Tétele).

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

Tétel.

Legyen G véges részcsoportja $\mathrm{Aut}(L)$-nek. Ekkor $[L : \varphi(G)] = |G|$, és így az $L : \varphi(G)$ testbővítés Galois-bővítés.

Tétel.

Legyen G véges részcsoportja $\mathrm{Aut}(L)$-nek. Ekkor $[L : \varphi(G)] = |G|$, és így az $L : \varphi(G)$ testbővítés Galois-bővítés.

Tétel.

Ha az $L : K$ testbővítés Galois-bővítés, akkor $|\gamma(K)| = [L : K]$ és $K = \varphi\gamma(K)$. Másrészt, ha az $L : K$ bővítés nem Galois-bővítés, akkor $|\gamma(K)| < [L : K]$ és K valódi részteste $\varphi\gamma(K)$-nek.

A testbővítések elméletének legfontosabb célja a polinomok és felbontási testeiknek vizsgálata.

A testbővítések elméletének legfontosabb célja a polinomok és felbontási testeiknek vizsgálata.

Definíció: polinom Galois-csoportja.

Tegyük fel, hogy $f \in K[x]$ és L az f polinom felbontási teste a K számtest felett. Ekkor az $L : K$ testbővítés $\mathrm{Gal}(L : K)$ Galois-csoportját az f polinom Galois-csoportjának nevezzük, és $\mathrm{Gal}_K(f)$-val fogjuk jelölni.

A testbővítések elméletének legfontosabb célja a polinomok és felbontási testeiknek vizsgálata.

Definíció: polinom Galois-csoportja.

Tegyük fel, hogy $f \in K[x]$ és L az f polinom felbontási teste a K számtest felett. Ekkor az $L : K$ testbővítés $\mathrm{Gal}(L : K)$ Galois-csoportját az f polinom Galois-csoportjának nevezzük, és $\mathrm{Gal}_K(f)$-val fogjuk jelölni.

A $\mathrm{Gal}_K(f)$ csoport természetesen függ f-től és K-tól, de nem függ a felbontási test választásától.

Tétel.

Legyen L az $f \in K[x]$ polinom felbontási teste K felett. Ekkor $|\mathrm{Gal}_K(f)| = [L : K]$ és $K = \varphi(\mathrm{Gal}_K(f))$.

A $\mathrm{Gal}_K(f)$ csoport egy tetszőleges σ eleme az L test automorfizmusa. Számunkra a legfontosabb az lesz, hogy σ hogyan hat az f polinom gyökeinek halmazán. A következő tétel szerint nem vesztünk információt, ha csak ezt a hatást vizsgáljuk.

A $\mathrm{Gal}_K(f)$ csoport egy tetszőleges σ eleme az L test automorfizmusa. Számunkra a legfontosabb az lesz, hogy σ hogyan hat az f polinom gyökeinek halmazán. A következő tétel szerint nem vesztünk információt, ha csak ezt a hatást vizsgáljuk.

Tétel.

Legyen L az $f \in K[x]$ polinom felbontási teste K felett, és jelölje R az f polinom L-beli gyökeinek halmazát. Ekkor tetszőleges $\sigma \in \mathrm{Gal}_K(f)$-ra $\sigma|_R \in S_R$, és a

$$\mathrm{Gal}_K(f) \to S_R,\ \sigma \mapsto \sigma|_R$$

leképezés injektív homomorfizmus.