

Magasabbfokú egyenletek és geometriai szerkeszthetőség

Dormán Miklós

SZTE, Bolyai Intézet

2008. november 14.

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 tényezőik szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \dots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

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

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

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 $\alpha_1, \dots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

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

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

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 tényezőik szorzatára bontható L felett, azaz vannak olyan $\alpha_1, \dots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

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

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

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 $[L : K] \leq n!$ 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 $[L : K] \leq n!$ teljesül.

Bizonyítás.

Az állítást az f polinom fokszáma szerinti indukcióval bizonyítjuk. Ha $f^* \leq 1$, 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 $1 \leq g^* = s, h^* = t < n$. Az indukciós feltevés szerint van a K testnek egy olyan L bővítése, amely felbontási teste az g polinomnak K felett és $[L : K] \leq s!$. Ekkor

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

ahol $\alpha_1, \dots, \alpha_s \in L, \lambda \in K$ és $L = K(\alpha_1, \dots, \alpha_s)$. 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 $[M : L] \leq t!$.

Bizonyítás (folytatás).

Ekkor

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

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

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

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

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

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 $[M : L] \leq (n - 1)!$. Ekkor $h = \mu(x - \beta_1) \cdots (x - \beta_{n-1})$, ahol $\beta_1, \dots, \beta_{n-1} \in M$, $\mu \in L$ és $M = L(\beta_1, \dots, \beta_{n-1})$. Ezért azt kapjuk, hogy

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

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

Felbontási tesztek

Injektív homomorfizmusok kiterjesztése

Most pedig azt mutatjuk meg, hogy a felbontási test lényegében egyértelmű. Legyenek K_1, K_2 testek, és $\eta: K_1 \rightarrow K_2$ izomorfizmus. Tetszőleges $f = \sum_{k=0}^n a_k x^k \in K_1[x]$ polinomra legyen

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

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

Tétel (A felbontási test egyértelmősége.)

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

Felbontási tesztek

Injektív homomorfizmusok kiterjesztése

Tétel (A felbontási test egyértelmősége.)

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

Lemma (Kiterjesztési Lemma).

Legyenek K, K' testek, $\eta: K \rightarrow K'$ 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 $\vartheta: K(\alpha) \rightarrow L'$ injektív homomorfizmussá, ha ηf -nek van gyöke L' -ben, és ebben az esetben η -t annyiféleképpen tudjuk kiterjeszteni ahány gyöke van ηf -nek L' -ben.

Felbontási tesztek

Injektív homomorfizmusok kiterjesztése

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

Felbontási tesztek

Injektív homomorfizmusok kiterjesztése

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

Következmény.

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

Felbontási tesztek

Többszörös gyökök

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 $\alpha_1, \dots, \alpha_r$ 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:

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

A D_x leképezést **(formális) deriválásnak** 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 $D_x(fg) = D_x(f)g + fD_x(g)$ 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 $D_x(fg) = D_x(f)g + fD_x(g)$ teljesül.
- (3) Ha $\text{char}(K) = 0$, 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 $D_x(fg) = D_x(f)g + fD_x(g)$ teljesül.
- (3) Ha $\text{char}(K) = 0$, akkor $\ker(D_x) = K$, és a D_x leképezés szürjektív.

Bizonyítás.

Az állításokat a definíció alapján egyszerűen igazolhatjuk.

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

$$D_x(f) = \ell(x - \alpha)^{\ell-1}g + (x - \alpha)^\ell D_x(g) = (x - \alpha)^{\ell-1} (\ell g + (x - \alpha)D_x(g)).$$

Ekkor $x - \alpha$ osztója az f és $D_x(f)$ polinomoknak $L[x]$ -ben, és így $x - \alpha \mid \text{ln.k.o.}(f, D_x(f))$. Azaz $\text{ln.k.o.}(f, D_x(f))$ 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 $\lambda \in K$, $\alpha_1, \dots, \alpha_s \in M$ 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 $\alpha_1, \dots, \alpha_s \notin L$, akkor $\text{ln.k.o.}(f, D_x(f))$ -nek sem lehet gyöke L -ben.

Tegyük fel, hogy valamely $i \in \{1, \dots, s\}$ -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 $\text{ln.k.o.}(f, D_x(f))$ -nek sem.

Következmény.

Legyen K számtest, f irreducibilis polinom K felett, melynek felbontási teste L . Ekkor az f polinom valamennyi gyöke egyszeres L -ben.

Következmény.

Legyen K számtest, f irreducibilis polinom K felett, melynek felbontási teste L . Ekkor 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 $f = \sum_{j=0}^n \frac{x^j}{j!} \in \mathbb{Q}[x]$ ($n \geq 1$). 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 ($f^* = n \geq 1$). 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.

Magasabb fokú egyenletek

Többszörös gyökök

Példa.

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

Magasabb fokú egyenletek

Többszörös gyökök

Példa.

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

Bizonyítás.

Legyen f tetszőleges $K[x]$ -beli irreducibilis polinom. Tegyük fel, hogy f -nek van többszörös gyöke. Ekkor $\text{ln.k.o.}(f, D_x(f))$ legalább elsőfokú polinom. Mivel f irreducibilis és $\text{ln.k.o.}(f, D_x(f)) \mid f$, ezért $\text{ln.k.o.}(f, D_x(f)) \sim f$. Így $f \mid D_x(f)$, ami azonban a polinomok fokszámai miatt nem lehetséges.

Definíció: algebrailag 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: algebrailag 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 komplex 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.

Tétel.

Tetszőleges $L|K$ testbővítésre ekvivalensek az alábbi állítások.

Tétel.

Tetszőleges $L|K$ testbővítésre ekvivalensek az alábbi állítások.

- (1) L algebrai lezártja K -nak.

Tétel.

Tetszőleges $L|K$ testbővítésre ekvivalensek az alábbi állítások.

- (1) L algebrai lezártja K -nak.
- (2) az $L|K$ bővítés algebrai és minden irreducibilis $K[x]$ -beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$ -ben.

Tétel.

Tetszőleges $L|K$ testbővítésre ekvivalensek az alábbi állítások.

- (1) L algebrai lezártja K -nak.
- (2) az $L|K$ bővítés algebrai és minden irreducibilis $K[x]$ -beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$ -ben.
- (3) az $L|K$ bővítés algebrai, és tetszőleges L' testre, ha a $L'|L$ testbővítés algebrai, akkor $L' = L$.

Tétel.

Tetszőleges $L|K$ testbővítésre ekvivalensek az alábbi állítások.

- (1) L algebrai lezártja K -nak.
- (2) az $L|K$ bővítés algebrai és minden irreducibilis $K[x]$ -beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$ -ben.
- (3) az $L|K$ bővítés algebrai, és tetszőleges L' testre, ha a $L'|L$ testbővítés algebrai, akkor $L' = L$.

Bizonyítás.

(1) \implies (2): az f irreducibilis polinom fokszámára vonatkozó indukcióval az állítás egyszerűen belátható.

Bizonyítás (folytatás).

(2) \implies (3): legyen α az L' test tetszőleges eleme. Mivel az $L|K$ és $L'|L$ bővítések is algebraiak, ezért az $L'|K$ bővítés is algebrai, így α algebrai elem K felett, melynek minimálpolinomja $m_{\alpha,K}$ irreducibilis polinom $K[x]$ -ben. Ekkor a (2) pont következtében $m_{\alpha,K}$ lineáris tényezőkre bomlik L felett:

$$m_{\alpha,K} = \lambda(x - \alpha_1) \cdots (x - \alpha_n),$$

ahol $n = \text{gr}_K(\alpha)$, $\lambda \in K$ és $\alpha_1, \dots, \alpha_n \in L$. Mivel α is gyöke $m_{\alpha,K}$ -nak, ezért valamely i -re ($1 \leq i \leq n$) $\alpha = \alpha_i \in L$. Azaz $L' = L$.

Bizonyítás (folytatás).

(3) \implies (1): csak azt kell megmutatni, hogy L algebrailag zárt. Legyen $f \in L[x]$ tetszőleges legalább elsőfokú polinom, és legyen f_1 az f polinom egy irreducibilis tényezője. Tekintsük az L test $L' = L[x]/(f_1)$ bővítését. Az L' testben f_1 -nek, és így f -nek is van gyöke ($\alpha = x + (f_1)$). Mivel az $L'|L$ bővítés algebrai, ezért (3) szerint $L' = L$, ami éppen azt jelenti, hogy f -nek L -ben is van gyöke.

Bizonyítás (folytatás).

(3) \implies (1): csak azt kell megmutatni, hogy L algebrailag zárt. Legyen $f \in L[x]$ tetszőleges legalább elsőfokú polinom, és legyen f_1 az f polinom egy irreducibilis tényezője. Tekintsük az L test $L' = L[x]/(f_1)$ bővítését. Az L' testben f_1 -nek, és így f -nek is van gyöke ($\alpha = x + (f_1)$). Mivel az $L'|L$ bővítés algebrai, ezért (3) szerint $L' = L$, ami éppen azt jelenti, hogy f -nek L -ben is van gyöke.

Következmény.

Legyen L algebrailag zárt test, és $L|K$ tetszőleges testbővítés. Legyen L_a mindazon L -beli elemek halmaza, amelyek algebraiak K felett. Ekkor az $L_a|K$ testbővítés algebrai lezártja K -nak.

Tétel.

Legyen K test. Ekkor van olyan algebrailag zárt L test, amely tartalmazza K -t.

Tétel.

Legyen K test. Ekkor van olyan algebrailag zárt L test, amely tartalmazza K -t.

Tétel.

Legyen K test. Ekkor van olyan L bővítése a K testnek, amelyre L algebrai lezártja K -nak.

Tétel.

Legyen K test. Ekkor van olyan algebrailag zárt L test, amely tartalmazza K -t.

Tétel.

Legyen K test. Ekkor van olyan L bővítése a K testnek, amelyre L algebrai lezártja K -nak.

Tétel.

Tegyük fel, hogy a K és K' testek izomorfak, $\eta: K \rightarrow K'$ izomorfizmus. Legyenek L , illetve L' a K , illetve K' testek algebrai lezártjai. Ekkor van olyan $\psi: L \rightarrow L'$ izomorfizmus, amely kiterjesztése η -nek, azaz $\psi|_K = \eta$.

Következmény.

Legyen K tetszőleges test. Ha L és L' is a K test algebrai lezártja, akkor van olyan $\psi: L \rightarrow L'$ izomorfizmus, amely kiterjesztése K elemeit fixen hagyja.

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:

$$f = (x + 1 + \varepsilon - \alpha) \cdot (x + 1 - \varepsilon\alpha + \varepsilon) \cdot (x + 1 + \alpha + \varepsilon\alpha + \varepsilon) \cdot \\ (x - \varepsilon + \alpha + \varepsilon\alpha) \cdot (x - \varepsilon - \varepsilon\alpha) \cdot (x - \varepsilon - \alpha).$$

Normális bővítések

Alapvető tulajdonságok

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:

$$f = (x + 1 + \varepsilon - \alpha) \cdot (x + 1 - \varepsilon\alpha + \varepsilon) \cdot (x + 1 + \alpha + \varepsilon\alpha + \varepsilon) \cdot \\ (x - \varepsilon + \alpha + \varepsilon\alpha) \cdot (x - \varepsilon - \varepsilon\alpha) \cdot (x - \varepsilon - \alpha).$$

Tétel.

Legyen L felbontási teste az $f \in K[x]$ polinomnak 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.

Normális bővítések

Alapvető tulajdonságok

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.

Normális bővítések

Alapvető tulajdonságok

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.

Normális bővítések

Alapvető tulajdonságok

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.

Normális bővítések

Alapvető tulajdonságok

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.

Normális bővítések

Alapvető tulajdonságok

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, $S = \{f_1, \dots, f_n\}$, 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.

Normális bővítések

Alapvető tulajdonságok

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.

Normális bővítések

Alapvető tulajdonságok

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 $\alpha_1, \dots, \alpha_k \in L$ 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.

Normális bővítések

Alapvető tulajdonságok

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 $K \leq M \leq L$. Vajon mi a helyzet az $M|K$ bővítéssel? Például 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.

Normális bővítések

Injektív homomorfizmusok és automorfizmusok

Definíció: testbővítés Galois-csoportja.

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

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

Nyilvánvaló, hogy $\text{Aut}_K(L)$ részcsoportha $\text{Aut}(L)$ -nek. Az L test automorfizmuscsoportjának $\text{Aut}_K(L)$ részcsoporthát az $L|K$ **testbővítés Galois-csoportjának** nevezzük, és $\text{Gal}(L|K)$ -val jelöljük.

Tétel.

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

Tétel.

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

- (1) az $M|K$ bővítés normális;

Tétel.

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

- (1) az $M|K$ bővítés normális;
- (2) ha $\sigma \in \text{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;

Tétel.

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

- (1) az $M|K$ bővítés normális;
- (2) ha $\sigma \in \text{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;
- (3) ha $\sigma \in \text{Aut}_K(L)$, akkor $\sigma(M) = M$.

Tétel.

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

- (1) az $M|K$ bővítés normális;
- (2) ha $\sigma \in \text{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;
- (3) ha $\sigma \in \text{Aut}_K(L)$, akkor $\sigma(M) = M$.

Bizonyítás.

(1) \implies (2): Tegyük fel, hogy az $M|K$ bővítés normális, és legyen $\sigma \in \text{Aut}_K(L)$. 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) \implies (3): Az állítás következik abból, hogy $\sigma^{-1} \in \text{Aut}_K(L)$.

(3) \implies (1): Tegyük fel, hogy tetszőleges $\sigma \in \text{Aut}_K(L)$ -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 $\eta = \text{id}_K$ izomorfizmus kiterjeszthető egy $\vartheta: K(\alpha) \rightarrow K(\beta)$ 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 $\sigma: L \rightarrow L$ izomorfizmussá. Ekkor $\sigma \in \text{Aut}_K(L)$, és így (3) miatt $\sigma(M) = M$. Ebből pedig azt kapjuk, hogy $\beta = \vartheta(\alpha) = \sigma(\alpha) \in M$. Ezzel a bizonyítást befejeztük.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Definíció: Galois-kapcsolat.

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

$$\varphi: P(A) \rightarrow P(B), \quad U \mapsto \{b \in B \mid (u, b) \in \Delta \text{ minden } u \in U\text{-ra}\},$$

$$\gamma: P(B) \rightarrow P(A), \quad V \mapsto \{a \in A \mid (a, v) \in \Delta \text{ minden } v \in V\text{-re}\}.$$

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, $\xi: P(A) \rightarrow P(B)$ 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, $\omega: P(A) \rightarrow P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega: P(A) \rightarrow P(A)$ 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, $\omega: P(A) \rightarrow P(A)$ 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, $\omega: P(A) \rightarrow P(A)$ 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, $\omega: P(A) \rightarrow P(A)$ 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, $\omega: P(A) \rightarrow P(A)$ 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 $U = \gamma(V)$.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Bizonyítás.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

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

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

Bizonyítás (folytatás).

Így azonban γ definíciója miatt azt kapjuk, hogy

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

ami ellentmond az előzőeknek. Ezzel igazoltuk, hogy $\varphi\gamma$ extenzív ($\gamma\varphi$ extenzív). Legyen V tetszőleges részhalma 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, $\gamma\varphi$ extenzivitása miatt $\gamma(V) \subseteq \gamma\varphi(\gamma(V)) = \gamma\varphi\gamma(V)$, így azt kapjuk, hogy

$$\gamma(V) = \gamma\varphi\gamma(V). \quad (1)$$

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.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Példa.

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

$$\varphi(U) = \{a \in L \mid (\tau, a) \in \Delta \text{ minden } \tau \in U\text{-ra}\},$$

$$= \{a \in L \mid \tau(a) = a \text{ minden } \tau \in U\text{-ra}\},$$

$$\gamma(V) = \{\sigma \in \text{Aut}(L) \mid (\sigma, v) \in \Delta \text{ minden } v \in V\text{-re}\},$$

$$= \{\sigma \in \text{Aut}(L) \mid \sigma(v) = v \text{ minden } v \in V\text{-re}\},$$

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.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Tétel.

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

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Tétel.

Legyen L tetszőleges test és $U \subseteq \text{Aut}(L)$. 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 részcsoporthja $\text{Aut}(L)$ -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.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\text{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\text{Aut}(L)$ -nek.

Tetszőleges $\alpha \in L$ -re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha: G \rightarrow L, \quad \sigma \mapsto \sigma(\alpha).$$

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

Tétel.

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

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\text{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\text{Aut}(L)$ -nek.

Tetszőleges $\alpha \in L$ -re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha: G \rightarrow L, \quad \sigma \mapsto \sigma(\alpha).$$

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

Tétel.

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

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

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\text{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\text{Aut}(L)$ -nek.

Tetszőleges $\alpha \in L$ -re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha: G \rightarrow L, \quad \sigma \mapsto \sigma(\alpha).$$

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

Tétel.

Legyen G részcsoportja $\text{Aut}(L)$ -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;

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Az előző állítás éppen azt mondja, hogy általában elegendő csupán $\text{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\text{Aut}(L)$ -nek.

Tetszőleges $\alpha \in L$ -re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha: G \rightarrow L, \quad \sigma \mapsto \sigma(\alpha).$$

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

Tétel.

Legyen G részcsoportja $\text{Aut}(L)$ -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: szeparábilis bővítés.

Legyen $L|K$ testbővítés. Azt mondjuk, hogy **az $\alpha \in L$ elem szeparábilis** (K felett), ha $m_{\alpha,K}$ szeparábilis K felett, illetve azt mondjuk, hogy **az $L|K$ bővítés szeparábilis** (K felett), ha minden $\alpha \in L$ elem szeparábilis.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Definíció: szeparábilis bővítés.

Legyen $L|K$ testbővítés. Azt mondjuk, hogy **az $\alpha \in L$ elem szeparábilis** (K felett), ha $m_{\alpha,K}$ szeparábilis K felett, illetve azt mondjuk, hogy **az $L|K$ bővítés szeparábilis** (K felett), ha minden $\alpha \in L$ elem szeparábilis.

Definíció: Galos-bővítés.

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

Tétel (A Galois-bővítések Tétele).

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

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Tétel (A Galois-bővítések Tétele).

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

Lemma.

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

Tétel.

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

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Tétel.

Legyen G véges részcsoportha $\text{Aut}(L)$ -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.

Automorfizmusok és fixtestek

Polinom Galois-csoportja

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 $\text{Gal}(L|K)$ Galois-csoportját az f polinom Galois-csoportjának nevezzük, és $\text{Gal}_K(f)$ -val fogjuk jelölni.

Automorfizmusok és fixtestek

Polinom Galois-csoportja

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 $\text{Gal}(L|K)$ Galois-csoportját az f polinom Galois-csoportjának nevezzük, és $\text{Gal}_K(f)$ -val fogjuk jelölni.

A $\text{Gal}_K(f)$ 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. Ha f szeparábilis, akkor $|\text{Gal}_K(f)| = [L : K]$ és $K = \varphi(\text{Gal}_K(f))$; különben $|\text{Gal}_K(f)| < [L : K]$ és K valódi részteste $\varphi(\text{Gal}_K(f))$ -nek.

Automorfizmusok és fixtestek

Polinom Galois-csoportja.

A $\text{Gal}_K(f)$ 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 veszünk információt, ha csak ezt a hatást vizsgáljuk.

Automorfizmusok és fixtestek

Polinom Galois-csoportja.

A $\text{Gal}_K(f)$ 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 veszünk 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 $\sigma \in \text{Gal}_K(f)$ -ra $\sigma|_R \in S_R$, és a

$$\text{Gal}_K(f) \rightarrow S_R, \sigma \mapsto \sigma|_R$$

leképezés injektív homomorfizmus.

Automorfizmusok és fixtestek

Polinomok Galois-csoportjai

Ha f irreducibilis, akkor $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \text{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$.

Automorfizmusok és fixtestek

Polinomok Galois-csoportjai

Ha f irreducibilis, akkor $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \text{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$.

Automorfizmusok és fixtestek

Polinomok Galois-csoportjai

Ha f irreducibilis, akkor $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \text{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Tegyük fel, hogy $f \in K[x]$ egy n -edfokú polinom, amelynek n különböző gyöke van egy L felbontási testében és $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán.

Automorfizmusok és fixtestek

Polinomok Galois-csoportjai

Ha f irreducibilis, akkor $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \text{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Tegyük fel, hogy $f \in K[x]$ egy n -edfokú polinom, amelynek n különböző gyöke van egy L felbontási testében és $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán. Legyen m az f polinom α gyökének minimálpolinomja K felett, valamint $\beta \in L$ az f polinom egy tetszőleges gyöke.

Automorfizmusok és fixtestek

Polinomok Galois-csoportjai

Ha f irreducibilis, akkor $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \text{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Tegyük fel, hogy $f \in K[x]$ egy n -edfokú polinom, amelynek n különböző gyöke van egy L felbontási testében és $\text{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán. Legyen m az f polinom α gyökének minimálpolinomja K felett, valamint $\beta \in L$ az f polinom egy tetszőleges gyöke. Ekkor van olyan $\sigma \in \text{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Ezért

$$m(\beta) = m(\sigma(\alpha)) = \sigma(m)(\sigma(\alpha)) = \sigma(m(\alpha)) = 0,$$

és így m -nek legalább n gyöke van. Mivel $m \mid f$, ezért $m = f$. Azaz f irreducibilis.

Automorfizmusok és fixtestek

Egy példa.

Legyen G permutációcsoport az X véges halmazon. Az X halmazon definiáljuk a \sim relációt a következőképpen:

$$x \sim y \iff x = y \text{ vagy } (x y) \in G.$$

Automorfizmusok és fixtestek

Egy példa.

Legyen G permutációcsoport az X véges halmazon. Az X halmazon definiáljuk a \sim relációt a következőképpen:

$$x \sim y \iff x = y \text{ vagy } (x y) \in G.$$

Automorfizmusok és fixtestek

Egy példa.

Legyen G permutációcsoport az X véges halmazon. Az X halmazon definiáljuk a \sim relációt a következőképpen:

$$x \sim y \iff x = y \text{ vagy } (x y) \in G.$$

A $\sim \subseteq X \times X$ reláció nyilván reflexív és szimmetrikus. Tegyük fel, hogy az $x, y, z \in X$ elemekre teljesül, hogy $x \sim y$ és $y \sim z$. Ekkor $(x y), (y z) \in G$. Mivel G csoport, ezért $(x z) = (x y) \cdot (y z) \cdot (x y) \in G$. Azaz $(x z) \in G$, és így $x \sim z$. Ezzel igazoltuk, hogy \sim ekvivalenciareláció.

Automorfizmusok és fixtestek

Egy példa.

Tegyük fel, hogy G tranzitív, és legyen rendre E_x , illetve E_y az x , illetve y elemeket tartalmazó ekvivalenciaosztály. Mivel G tranzitív, ezért van olyan $\sigma \in G$, amelyre $y = \sigma(x)$ teljesül. Ha $x' \in E_x$, akkor $x \sim x'$ miatt $(x x') \in G$. Így

$$G \ni \sigma^{-1}(x x')\sigma = (\sigma(x) \sigma(x')) = (y \sigma(x'))$$

miatt $\sigma(x') \in E_y$. Azaz $\sigma(E_x) \subseteq E_y$. Ez pedig éppen azt jelenti, hogy $|E_x| \leq |E_y|$. Az x és y elemek szerepét felcserélve azt kapjuk, hogy $|E_x| = |E_y|$. Ezzel megmutattuk, hogy bármely két ekvivalenciaosztály elemszáma megegyezik.

Automorfizmusok és fixtestek

Egy példa.

Tegyük fel, hogy G tranzitív, és legyen rendre E_x , illetve E_y az x , illetve y elemeket tartalmazó ekvivalenciaosztály. Mivel G tranzitív, ezért van olyan $\sigma \in G$, amelyre $y = \sigma(x)$ teljesül. Ha $x' \in E_x$, akkor $x \sim x'$ miatt $(x x') \in G$. Így

$$G \ni \sigma^{-1}(x x')\sigma = (\sigma(x) \sigma(x')) = (y \sigma(x'))$$

miatt $\sigma(x') \in E_y$. Azaz $\sigma(E_x) \subseteq E_y$. Ez pedig éppen azt jelenti, hogy $|E_x| \leq |E_y|$. Az x és y elemek szerepét felcserélve azt kapjuk, hogy $|E_x| = |E_y|$. Ezzel megmutattuk, hogy bármely két ekvivalenciaosztály elemszáma megegyezik.

Ha X elemszáma prímszám és G tartalmaz legalább egy transzpozíciót, akkor G tranzitivitása miatt G az összes transzpozíciót tartalmazza, amelyek azonban generálják S_X -et, így $G = S_X$.

Automorfizmusok és fixtestek

Egy példa.

Tétel.

Legyen p prímszám, és tegyük fel, hogy $f \in \mathbb{Q}[x]$ olyan p -edfokú irreducibilis polinom, amelynek pontosan $p - 2$ darab valós gyöke van. Ekkor $\text{Gal}_{\mathbb{Q}}(f) \cong S_p$.

Automorfizmusok és fixtestek

Egy példa.

Bizonyítás.

Legyen $L \subseteq \mathbb{C}$ az f polinom felbontási teste \mathbb{Q} felett. Mivel f irreducibilis, ezért $\text{Gal}_{\mathbb{Q}}(f)$ tranzitívan hat f (L -beli) gyökeinek R halmazán. Az $\xi: L \rightarrow L, z \rightarrow \bar{z}$ leképezés nyilván eleme f Galois-csoportjának, és $\xi|_R \in S_R$ transzpozíció. Így a

$$\{\sigma|_R \mid \sigma \in \text{Gal}_K(f)\} \leq S_R$$

permutációcsoport tranzitív és tartalmaz transzpozíciót. Ekkor az előzőek szerint $\{\sigma|_R \mid \sigma \in \text{Gal}_K(f)\} = S_R$. Továbbá,

$$\text{Gal}_K(f) \cong S_R \cong S_p.$$

Automorfizmusok és fixtestek

Egy példa.

Példa.

Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot.

Automorfizmusok és fixtestek

Egy példa.

Példa.

Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot.

Automorfizmusok és fixtestek

Egy példa.

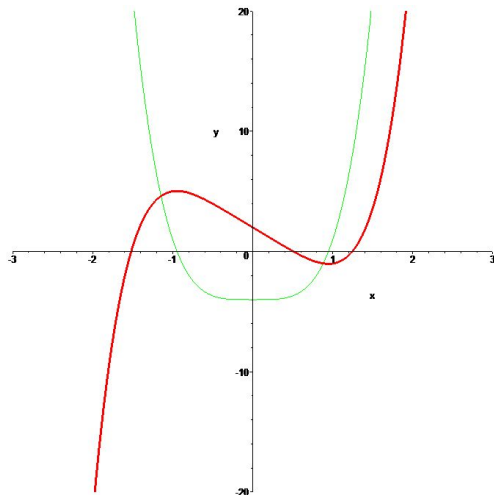
Példa.

Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot. A

Schönemann–Eisenstein-tétel szerint az f polinom irreducibilis.

Automorfizmusok és fixtestek

Egy példa.



1. ábra: Az f és $D_x(f)$ polinomok grafikonja.

Automorfizmusok és fixtestek

Egy példa.

A polinomnak pontosan 3 darab valós gyöke van. Az előző tétel szerint $\text{Gal}_{\mathbb{Q}}(f) \cong S_5$.

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

A Galois-elmélet főtétele részleteiben írja le a fejezet elején bevezetett polaritást.

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

A Galois-elmélet főtétele részleteiben írja le a fejezet elején bevezetett polaritást.

Tétel (A Galois-elmélet Főtétele).

Legyen $L|K$ véges bővítés, $G = \text{Gal}(L|K)$ és $K_0 = \varphi(G)$. Az $L|K_0$ bővítés tetszőleges M közbülső testére legyen $\gamma(M) = \text{Gal}(L|M)$. Ekkor teljesülnek a következők.

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

Tétel (A Galois-elmélet Főtétele).

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

Tétel (A Galois-elmélet Főtétele).

(a) A

$\text{Sub}(G) \rightarrow \{M \mid M \text{ közbülső teste az } L|K_0 \text{ bővítésnek}\}, G \mapsto \varphi(G)$
leképezés rendezéstartó bijekció, melynek inverze

$\{M \mid M \text{ közbülső teste az } L|K_0 \text{ bővítésnek}\} \rightarrow \text{Sub}(G), M \mapsto \gamma(M).$

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

Tétel (A Galois-elmélet Főtétele).

(a) A

$\text{Sub}(G) \rightarrow \{M \mid M \text{ közbülső teste az } L|K_0 \text{ bővítésnek}\}, G \mapsto \varphi(G)$
leképezés rendezéstartó bijekció, melynek inverze

$\{M \mid M \text{ közbülső teste az } L|K_0 \text{ bővítésnek}\} \rightarrow \text{Sub}(G), M \mapsto \gamma(M).$

(b) A G csoport H részcsoportja pontosan akkor normális, ha a $\varphi(H)|K_0$ bővítés normális.

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

Tétel (A Galois-elmélet Főtétele).

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

Tétel (A Galois-elmélet Főtétele).

- (c) Tegyük fel, hogy H normális részcsoport G -ben. Ha $\sigma \in G$, akkor $\sigma|_{\varphi(H)} \in \text{Gal}(\varphi(H)|K_0)$. A

$$G \rightarrow \text{Gal}(\varphi(H)|K_0), \sigma \mapsto \sigma|_{\varphi(H)}$$

leképezés szürjektív homomorfizmus, melynek magja H . Így

$$\text{Gal}(\varphi(H)|K_0) \cong G/H.$$

Automorfizmusok és fixtestek

A Galois-elmélet főtétele.

Példa: az $x^4 - 2 \in \mathbb{Q}[x]$ polinom vizsgálata.

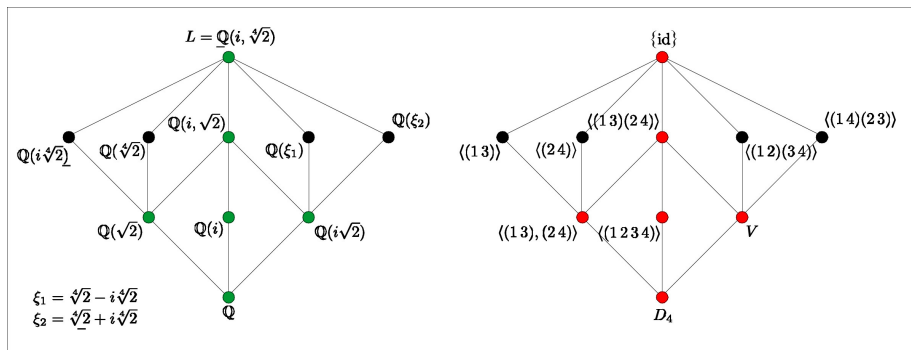
Az $x^4 - 2$ polinom \mathbb{Q} feletti felbontási teste $F = \mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} + i)$:

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Mivel $\sqrt[4]{2} + i$ minimálpolinomja \mathbb{Q} felett: $x^8 + 4x^6 + 2x^4 + 28x^2 + 1$, ezért $[F : \mathbb{Q}] = 8 = |\text{Gal}(F|\mathbb{Q})| = |\text{Gal}_{\mathbb{Q}}(x^4 - 2)|$. Ha $\varphi \in \text{Gal}_{\mathbb{Q}}(x^4 - 2)$, akkor $\varphi(\sqrt[4]{2}) \in \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$ és $\varphi(i) \in \{-i, i\}$. Az $x^4 - 2$ (\mathbb{Q} felett irreducibilis) polinom Galois-csoportja izomorf D_4 -gyel. A Galois-elmélet főtételét a következő ábra szemlélteti.

Automorfizmusok és fixtestek

Egy példa.



2. ábra: Az $L|\mathbb{Q}$ bővítés és közbülső teste.

Tétel.

Legyen K számtest, $\alpha \in K$ és p prímszám. Ekkor az $x^p - \alpha$ polinom vagy irreducibilis K felett, vagy van gyöke K -ban. Ha legalább két gyöke van K -ban, akkor elsőfokú polinomok szorzatára bomlik K felett.

Tétel.

Legyen K számtest, $\alpha \in K$ és p prímszám. Ekkor az $x^p - \alpha$ polinom vagy irreducibilis K felett, vagy van gyöke K -ban. Ha legalább két gyöke van K -ban, akkor elsőfokú polinomok szorzatára bomlik K felett.

Tétel.

Legyen K számtest, $\alpha \in K$, és p prímszám. Ha K tartalmazza a p -edik egységgyököket, akkor a $K(\beta)|K$ bővítés normális, ahol $\beta^p = \alpha$. A bővítés foka 1 vagy p . Ez utóbbi esetben $x^p - \alpha$ irreducibilis K felett.

Definíció: normállánc, faktor, feloldható csoport

A G csoport **normálláncának** nevezzük G részcsoportjainak egy G_0, \dots, G_n sorozatát, amelyre

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

teljesül. A G_i/G_{i-1} faktorcsoportokat e normállánc **faktorainak** nevezzük; n a normállánc **hossza**.

Azt mondjuk, hogy a G csoport **feloldható**, ha G -nek van olyan normállánca, amelynek faktorai Abel-csoportok.

Példák feloldható csoportokra.

Az S_3 csoport feloldható, mivel a

$$\{\text{id}\} \triangleleft A_3 \triangleleft S_3$$

normállánc faktorai Abel-csoportok, sőt ciklikus csoportok:

$$A_3/\{\text{id}\} \cong A_3 = \langle (1\ 2\ 3) \rangle, \quad S_3/A_3 \cong C_2.$$

Az S_4 csoport is feloldható, az

$$\{\text{id}\} \triangleleft \{\text{id}, (1\ 2)(3\ 4)\} \triangleleft \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \triangleleft A_4 \triangleleft S_4$$

normállánc faktorai Abel-csoportok.

Tétel.

Az A_n alternáló csoport $n \geq 5$ esetén nem feloldható.

Tétel.

Az A_n alternáló csoport $n \geq 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leq G$ és $N \triangleleft G$. Ekkor igazak a következők:

Tétel.

Az A_n alternáló csoport $n \geq 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leq G$ és $N \triangleleft G$. Ekkor igazak a következők:

(a) ha G feloldható, akkor H is feloldható;

Tétel.

Az A_n alternáló csoport $n \geq 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leq G$ és $N \triangleleft G$. Ekkor igazak a következők:

- (a) ha G feloldható, akkor H is feloldható;
- (b) a G csoport pontosan akkor feloldható, ha N és G/N is feloldható.

Tétel.

Az A_n alternáló csoport $n \geq 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leq G$ és $N \triangleleft G$. Ekkor igazak a következők:

- (a) ha G feloldható, akkor H is feloldható;
- (b) a G csoport pontosan akkor feloldható, ha N és G/N is feloldható.

Tétel.

Az S_n csoport $n \geq 5$ esetén nem feloldható.

Tétel.

Legyen K számtest, és ε primitív n -edik egységgyök. Ekkor a $K(\varepsilon)|K$ bővítés normális, és $\text{Gal}(K(\varepsilon)|K)$ izomorf \mathbb{Z}_n^\times egy részcsoportjával.

Tétel.

Legyen K számtest, és ε primitív n -edik egységgyök. Ekkor a $K(\varepsilon)|K$ bővítés normális, és $\text{Gal}(K(\varepsilon)|K)$ izomorf \mathbb{Z}_n^\times egy részcsoportjával.

Tétel.

Legyen K számtest és $f \in K[x]$ irreducibilis polinom. Ha f valamelyik komplex gyöke felírható egy olyan képlettel, amely f együtthatóiból a négy alapművelet és gyökvonások felhasználásával keletkezik, akkor az f polinom K feletti Galois-csoportja feloldható csoport.

Egyenletek gyökjelekkel való megoldása

Tétel.

Legyen K számtest, és ε primitív n -edik egységgyök. Ekkor a $K(\varepsilon)|K$ bővítés normális, és $\text{Gal}(K(\varepsilon)|K)$ izomorf \mathbb{Z}_n^\times egy részcsoportjával.

Tétel.

Legyen K számtest és $f \in K[x]$ irreducibilis polinom. Ha f valamelyik komplex gyöke felírható egy olyan képlettel, amely f együtthatóiból a négy alapművelet és gyökvonások felhasználásával keletkezik, akkor az f polinom K feletti Galois-csoportja feloldható csoport.

Példa.

Az $x^5 - 4x + 2$ polinom egyik gyöke sem gyökkifejezés \mathbb{Q} felett.

Tétel.

Legyenek y_1, \dots, y_n határozatlanok, K a $\mathbb{Q}[y_1, \dots, y_n]$ hányadosteste, és

$$f = x^n + y_1x^{n-1} + \dots + y_{n-1}x + y_n \in K[x].$$

Legyen F egy felbontási teste f -nek. Ekkor $\text{Gal}(F|K)$ izomorf S_n -nel.

Tétel.

Legyenek y_1, \dots, y_n határozatlanok, K a $\mathbb{Q}[y_1, \dots, y_n]$ hányadosteste, és

$$f = x^n + y_1x^{n-1} + \dots + y_{n-1}x + y_n \in K[x].$$

Legyen F egy felbontási teste f -nek. Ekkor $\text{Gal}(F|K)$ izomorf S_n -nel.

Tétel (Ruffini–Abel).

Ha $n \geq 5$, akkor az általános n -edfokú egyenletre nem létezik gyökképlet.

Definíció: gyökkifejezés.

Legyen K számtest. Azt mondjuk, hogy a $z \in \mathbb{C}$ komplex szám **gyökkifejezés** K felett, ha van olyan $n \in \mathbb{N}_0$ és egy

$$K = K_0 < K_1 < \dots < K_{n-1} < K_n \subseteq \mathbb{C}$$

testlánc, amelyre $z \in K_n$, és minden $0 \leq i \leq n-1$ -re $K_{i+1} = K_i(\beta_i)$, ahol $\beta_i^{p_i} \in K_i$, p_i prímszám, és az $x^{p_i} - \beta_i$ polinom irreducibilis K_i felett.

Lemma.

Legyen K számtest és p prímszám. Tegyük fel, hogy a K számtest tartalmazza a p -edik egységgyököket. Ha az $L|K$ bővítés egy p -edfokú normális bővítés, akkor van olyan $\alpha \in K$, hogy az L test az $x^p - \alpha \in K[x]$ irreducibilis polinom felbontási teste K felett.

Lemma.

Legyen K számtest és p prímszám. Tegyük fel, hogy a K számtest tartalmazza a p -edik egységgyököket. Ha az $L|K$ bővítés egy p -edfokú normális bővítés, akkor van olyan $\alpha \in K$, hogy az L test az $x^p - \alpha \in K[x]$ irreducibilis polinom felbontási teste K felett.

Tétel.

Legyen K olyan számtest, amelynek minden eleme gyökkifejezés egy $K_0 \leq K$ számtest felett. Ha ε primitív n -edik egységgyök, akkor $K(\varepsilon)$ minden eleme gyökkifejezés K_0 felett.

Tétel.

Legyen K számtest, és $L|K$ véges normális bővítés, amelynek Galois-csoportja feloldható. Ekkor L minden eleme gyökkifejezés K felett.

Tétel.

Legyen K számtest, és $L|K$ véges normális bővítés, amelynek Galois-csoportja feloldható. Ekkor L minden eleme gyökkifejezés K felett.

Következmény.

Ha az $f \in K[x]$ polinom egyik gyöke gyökkifejezés, akkor mindegyik gyöke az.