

# Testbővítések

Waldhauser Tamás  
2020 őszi félév

## Emlékeztető

A magasabb fokú egyenletek és a geometriai szerkeszthetőség problémájánál is az a feladat, hogy adott számokból (vagy inkább egy adott  $K$  testből) kiindulva, a négy alapművelet és (négyzet)gyökvonások segítségével megkapjunk egy  $\alpha$  célszámot.

Hogy ez megtehető-e, az azon múlik, hogy  $\alpha$  milyen „viszonyban” van  $K$  elemeivel. (Amint látni fogjuk, ezt meghatározza az az információ, hogy  $\alpha$  mely  $K$  feletti polinomoknak gyöke.) Ezt nemcsak számokra, hanem más testek elemeire is lehet vizsgálni.

## Alapfelállítás

Adott egy  $L$  test, és abban egy  $K$  résztest. Ekkor azt mondjuk, hogy  $L$  **bővítése**  $K$ -nak, és ezt így jelöljük:  $L \mid K$ . Azt vizsgáljuk, hogy egy  $\alpha \in L$  elem milyen kölcsönhatásban van  $K$  elemeivel. (A legfontosabb példa:  $L = \mathbb{C}$  és  $K = \mathbb{Q}$ .)

## Definíció

Legyen  $R$  egy gyűrű és  $S \subseteq R$ . Ha  $S$  az  $R$ -ből „örökölt” műveletekkel maga is gyűrű, akkor azt mondjuk, hogy  $S$  **részgyűrűje** az  $R$  gyűrűnek (jelölés:  $S \leq R$ ). Hasonlóan definiálható a **résztest** fogalma is.

## Állítás

Tetszőleges  $R$  gyűrű és  $\{0\} \subseteq S \subseteq R$  esetén  $S$  akkor és csak akkor részgyűrűje  $R$ -nek, ha

- ▶  $S$  zárt az összeadásra:  $\forall a, b \in S : a + b \in S$ ;
- ▶  $S$  zárt a kivonásra:  $\forall a, b \in S : a - b = a + (-b) \in S$ ;
- ▶  $S$  zárt a szorzásra:  $\forall a, b \in S : a \cdot b \in S$ .

## Állítás

Tetszőleges  $L$  test és  $\{0, 1\} \subseteq S \subseteq L$  esetén  $S$  akkor és csak akkor részteste  $L$ -nek, ha

- ▶  $S$  zárt az összeadásra:  $\forall a, b \in S : a + b \in S$ ;
- ▶  $S$  zárt a kivonásra:  $\forall a, b \in S : a - b = a + (-b) \in S$ ;
- ▶  $S$  zárt a szorzásra:  $\forall a, b \in S : a \cdot b \in S$ ;
- ▶  $S$  zárt az osztásra:  $\forall a, b \in S : a/b = a \cdot b^{-1} \in S$ , ha  $b \neq 0$ .

## Definíció

Legyen  $R$  egy gyűrű, és  $H \subseteq R$ . A  $H$  halmaz által **generált részgyűrű**

- ▶ a legszűkebb olyan részgyűrűje  $R$ -nek, ami tartalmazza  $H$ -t;
- ▶ ez nem más, mint a  $H$ -t tartalmazó összes részgyűrűk metszete;
- ▶ vagy, praktikusabban, azon  $R$ -beli elemek halmaza, amelyek megkaphatóak  $H$  elemeiből az első három alapl művelet (összeadás, kivonás, szorzás) véges számú alkalmazásával.

Jelölés:  $[H]_{\text{gy}}$ .

## Definíció

Legyen  $L$  egy test, és  $H \subseteq L$ . A  $H$  halmaz által **generált résztest**

- ▶ a legszűkebb olyan részteste  $L$ -nek, ami tartalmazza  $H$ -t;
- ▶ ez nem más, mint a  $H$ -t tartalmazó összes résztestek metszete;
- ▶ vagy, praktikusabban, azon  $L$ -beli elemek halmaza, amelyek megkaphatóak  $H$  elemeiből az első négy alapl művelet (összeadás, kivonás, szorzás, osztás) véges számú alkalmazásával.

Jelölés:  $[H]_{\text{t}}$ .

## Tétel

Legyen  $L \mid K$  egy testbővítés és  $\alpha \in L$ . Ekkor a  $K \cup \{\alpha\}$  halmaz által generált részgyűrű  $L$ -ben éppen a  $K$  feletti polinomok  $\alpha$  helyen felvett értékeiből áll:

$$K[\alpha] := [K \cup \{\alpha\}]_{\text{gy}} = \{f(\alpha) : f \in K[x]\}.$$

## Bizonyítás.

A **jobb oldali halmaz** részgyűrű, mert zárt az első három alapl műveletre:

$f(\alpha) \pm g(\alpha) = (f \pm g)(\alpha)$  és  $f(\alpha) \cdot g(\alpha) = (f \cdot g)(\alpha)$  minden  $f, g \in K[x]$  esetén.

Ha  $S$  részgyűrű  $L$ -ben és  $S \supseteq K \cup \{\alpha\}$ , akkor  $S$ -nek tartalmaznia kell az összes  $a_n \alpha^n + \dots + a_1 \alpha + a_0$  ( $a_n, \dots, a_1, a_0 \in K$ ) alakú elemet (miért?).

Tehát a **jobb oldali halmaz** a legszűkebb mindazon részgyűrűk között, amelyek tartalmazzák a  $K \cup \{\alpha\}$  halmazt. □

## Tétel

Legyen  $L \mid K$  egy testbővítés, és  $\alpha \in L$ . Ekkor a  $K \cup \{\alpha\}$  halmaz által generált résztest  $L$ -ben éppen a  $K$  feletti racionális törtek  $\alpha$  helyen felvett értékeiből áll:

$$K(\alpha) := [K \cup \{\alpha\}]_{\text{t}} = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}.$$

## Bizonyítás.

Hasonló az előző tételhez, csak itt osztani is kell. □

## Példák

- ▶  $[\mathbb{Q} \cup \{\sqrt{2}\}]_{\text{gy}} = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
- ▶  $[\mathbb{Q} \cup \{\sqrt{2}\}]_{\text{t}} = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
- ▶  $[\mathbb{Q} \cup \{\sqrt[3]{2}\}]_{\text{gy}} = \mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$
- ▶  $[\mathbb{Q} \cup \{\sqrt[3]{2}\}]_{\text{t}} = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$
- ▶  $[\mathbb{Q} \cup \{\pi\}]_{\text{gy}} = \mathbb{Q}[\pi] = \{f(\pi) : f \in \mathbb{Q}[x]\}$
- ▶  $[\mathbb{Q} \cup \{\pi\}]_{\text{t}} = \mathbb{Q}(\pi) = \left\{ \frac{f(\pi)}{g(\pi)} : f, g \in \mathbb{Q}[x], g(\pi) \neq 0 \right\}$

## Definíció

Ha van olyan *nemnulla*  $f \in K[x]$  polinom, amelyre  $f(\alpha) = 0$ , akkor azt mondjuk, hogy  $\alpha$  **algebrai  $K$  felett**. A legkisebb fokszámú ilyen *főpolinomot*  $\alpha$   **$K$  feletti minimálpolinomjának** nevezzük. Jelölése:  $m_{\alpha, K}$ .

Ha  $\alpha$  nem gyöke semmilyen nemnulla  $K$  feletti polinomnak, akkor azt mondjuk, hogy  $\alpha$  **transzcendens  $K$  felett**.

Az  $L = \mathbb{C}$ ,  $K = \mathbb{Q}$  esetben **algebrai számokról** és **transzcendens számokról** beszélünk.

## Példák

- ▶  $\sqrt{2}$  algebrai  $\mathbb{Q}$  felett (vagyis algebrai szám):  $m_{\sqrt{2}, \mathbb{Q}} = x^2 - 2$
- ▶  $\sqrt{2}$  algebrai  $\mathbb{R}$  felett:  $m_{\sqrt{2}, \mathbb{R}} = x - \sqrt{2}$
- ▶  $\sqrt{2}$  algebrai  $\mathbb{C}$  felett:  $m_{\sqrt{2}, \mathbb{C}} = x - \sqrt{2}$
- ▶  $\pi$  transzcendens  $\mathbb{Q}$  felett (vagyis transzcendens szám)
- ▶  $\pi$  algebrai  $\mathbb{R}$  felett:  $m_{\pi, \mathbb{R}} = x - \pi$
- ▶  $\pi$  algebrai  $\mathbb{C}$  felett:  $m_{\pi, \mathbb{C}} = x - \pi$
- ▶  $\pi$ ,  $e$ ,  $2\sqrt{2}$ ,  $\sqrt{2}\sqrt{2}$ ,  $i^i = e^{-\pi/2}$  transzcendens számok

## Példák

$\alpha$	$m_{\alpha, \mathbb{Q}}$	$m_{\alpha, \mathbb{R}}$	$m_{\alpha, \mathbb{C}}$
$\frac{2}{3}$	$x - \frac{2}{3}$	$x - \frac{2}{3}$	$x - \frac{2}{3}$
$\sqrt[3]{2}$	$x^3 - 2$	$x - \sqrt[3]{2}$	$x - \sqrt[3]{2}$
$\sqrt[100]{2}$	$x^{100} - 2$	$x - \sqrt[100]{2}$	$x - \sqrt[100]{2}$
$i$	$x^2 + 1$	$x^2 + 1$	$x - i$
$2 + 3i$	$x^2 - 4x + 13$	$x^2 - 4x + 13$	$x - (2 + 3i)$



## Tétel

Legyen  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal. Tetszőleges  $f \in K[x]$  főpolinom esetén az alábbi három állítás ekvivalens:

- (1)  $f = m$ ;
- (2)  $f(\alpha) = 0$  és  $f$  irreducibilis  $K$  felett;
- (3) egy  $K$  feletti  $g$  polinomnak pontosan akkor gyöke  $\alpha$ , ha  $g$  többszöröse  $f$ -nek:

$$\forall g \in K[x]: g(\alpha) = 0 \iff f \mid g.$$

## Bizonyítás.

(1)  $\implies$  (2): Azt kell belátnunk, hogy  $m$  irreducibilis  $K$  felett.

Tfh. nem, azaz létezik  $m = g \cdot h$  *nemtriviális*  $K$  feletti felbontás főpolinomok szorzatára.

Ekkor  $0 = m(\alpha) = g(\alpha) \cdot h(\alpha)$ , így  $g(\alpha) = 0$  vagy  $h(\alpha) = 0$ . (miért?)

Tehát  $g$  vagy  $h$  egy  $m$ -nél kisebb fokú  $K$  feletti polinom, ami „annullálja”  $\alpha$ -t.  $\nexists \square$

## Tétel

Legyen  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal. Tetszőleges  $f \in K[x]$  főpolinom esetén az alábbi három állítás ekvivalens:

- (1)  $f = m$ ;
- (2)  $f(\alpha) = 0$  és  $f$  irreducibilis  $K$  felett;
- (3) egy  $K$  feletti  $g$  polinomnak pontosan akkor gyöke  $\alpha$ , ha  $g$  többszöröse  $f$ -nek:

$$\forall g \in K[x]: g(\alpha) = 0 \iff f \mid g.$$

## Bizonyítás.

(2)  $\implies$  (3): Tfh.  $f(\alpha) = 0$  és  $f$  irreducibilis  $K$  felett.

Az világos, hogy  $f \mid g \implies g(\alpha) = 0$  (ugye?).

A másik irányhoz tfh.  $g(\alpha) = 0$ , és legyen  $d = \text{Inko}(f, g)$ .

$$\left. \begin{array}{l} d(\alpha) = 0 \text{ (miért?)} \\ d \sim 1 \text{ vagy } d \sim f \text{ (miért?)} \end{array} \right\} \begin{array}{l} \xrightarrow{\text{miért?}} d \sim f \\ \xrightarrow{\text{miért?}} f \mid g \end{array}$$



## Tétel

Legyen  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal. Tetszőleges  $f \in K[x]$  főpolinom esetén az alábbi három állítás ekvivalens:

- (1)  $f = m$ ;
- (2)  $f(\alpha) = 0$  és  $f$  irreducibilis  $K$  felett;
- (3) egy  $K$  feletti  $g$  polinomnak pontosan akkor gyöke  $\alpha$ , ha  $g$  többszöröse  $f$ -nek:

$$\forall g \in K[x]: g(\alpha) = 0 \iff f \mid g.$$

## Bizonyítás.

(3)  $\implies$  (1): Ez könnyű: tetszőleges  $g \in K[x]$  polinom esetén, ha  $g(\alpha) = 0$ , akkor (3) szerint  $f \mid g$ , és így  $\deg f \leq \deg g$  (kivéve, ha  $g = 0$ ).

Tehát  $f$  valóban a lehető legkisebb fokszámú az  $\alpha$ -t annulláló nemzérő polinomok között. □

## Definíció

A  $K(\alpha) \mid K$  alakú testbővítéseket (ahol  $\alpha$  tetszőleges elem egy  $K$ -nál bővebb  $L$  testben), **egyszerű testbővítéseknek** nevezzük, és azt mondjuk, hogy  $K(\alpha)$  az  $\alpha$  elem **adjungálásával** keletkezik  $K$ -ból.

Ha  $\alpha$  transzcendens  $K$  fölött, akkor **egyszerű transzcendens bővítésről**, ha pedig  $\alpha$  algebrai  $K$  fölött, akkor **egyszerű algebrai bővítésről** beszélünk.

## Emlékeztető

Az  $\alpha$  elem adjungálása nem csupán annyit jelent, hogy ezt az egy elemet hozzávesszük  $K$ -hoz (így nem kapnánk testet!), hanem a  $K \cup \{\alpha\}$  halmazt még le is kell zárni a négy alapműveletre.

$$K(\alpha) := [K \cup \{\alpha\}]_t = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}$$

$$K[\alpha] := [K \cup \{\alpha\}]_{gy} = \{f(\alpha) : f \in K[x]\}.$$

Meg fogjuk mutatni, hogy algebrai esetben  $K(\alpha) = K[\alpha]$ , és ennek a testnek a szerkezetét teljesen meghatározza  $\alpha$  minimálpolinomja.

## Tétel

Ha  $\alpha \in L \mid K$  transzcendens elem, akkor  $K(\alpha)$  izomorf a  $K$  feletti racionális törtek testével. Az izomorfizmust a racionális törtek  $\alpha$  helyen történő kiértékelése szolgáltatja:

$$\varphi: K(x) \rightarrow K(\alpha), \quad \frac{f}{g} \mapsto \frac{f(\alpha)}{g(\alpha)}.$$

## Bizonyítás.

- ▶ Mivel  $\alpha$  transzcendens  $K$  felett,  $g(\alpha) \neq 0$  ha  $g$  nem a konstans nulla polinom, így a  $\varphi$  leképezés mindenütt értelmezett.
- ▶ Különböző racionális törtek  $\alpha$  helyen különböző értékeket adnak:

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)} \implies (f_1g_2 - f_2g_1)(\alpha) = 0 \implies f_1g_2 - f_2g_1 = 0 \implies \frac{f_1}{g_1} = \frac{f_2}{g_2}.$$

Tehát  $\varphi$  injektív leképezés.

- ▶ Azt, hogy  $\varphi$  szürjektív, már [tudjuk](#).
- ▶ Világos, hogy  $\varphi$  felcserélhető a műveletekkel: tetszőleges  $t_1, t_2 \in K(x)$  esetén

$$(t_1 + t_2)(\alpha) = t_1(\alpha) + t_2(\alpha) \quad \text{és} \quad (t_1 \cdot t_2)(\alpha) = t_1(\alpha) \cdot t_2(\alpha). \quad \square$$

## Példa

Legyen  $K = \mathbb{Q}$ ,  $L = \mathbb{C}$  és  $\alpha = \sqrt[3]{2}$ . Láttuk, hogy ekkor

$$K[\alpha] = \mathbb{Q}[\sqrt[3]{2}] = \{a\sqrt[3]{4} + b\sqrt[3]{2} + c : a, b, c \in \mathbb{Q}\}.$$

Nézzük meg, hogy pl. a  $\beta = \sqrt[3]{4} - 2\sqrt[3]{2} + 1 = \alpha^2 - 2\alpha + 1$  elemnek van-e multiplikatív inverze ebben a gyűrűben:

$$\beta^{-1} = \frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = ?$$

Oldjuk meg az  $(x^3 - 2) \cdot u + (x^2 - 2x + 1) \cdot v = 1$  „diofantoszi” egyenletet a  $\mathbb{Q}[x]$  polinomgyűrűben:

$$u = -3x + 2, \quad v = 3x^2 + 4x + 5.$$

Tehát

$$(x^3 - 2) \cdot (-3x + 2) + (x^2 - 2x + 1) \cdot (3x^2 + 4x + 5) = 1.$$

Írjunk mindenütt  $x$  helyébe  $\alpha$ -t:

$$(\alpha^3 - 2) \cdot (-3\alpha + 2) + (\alpha^2 - 2\alpha + 1) \cdot (3\alpha^2 + 4\alpha + 5) = 1.$$

Következésképp

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = \beta^{-1} = (\alpha^2 - 2\alpha + 1)^{-1} = 3\alpha^2 + 4\alpha + 5 = 3\sqrt[3]{4} + 4\sqrt[3]{2} + 5.$$

## Példa (folyt.)

Hasonlóan lehet a  $\mathbb{Q}[\sqrt[3]{2}]$  gyűrű bármely nemnulla elemének multiplikatív inverzét kiszámolni (nevezőt gyökteleníteni). Tehát  $\mathbb{Q}[\sqrt[3]{2}]$  test, és így  $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$ .

Összefoglalva: a  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$  testről a következő két dolgot kell tudni:

- ▶ elemei **egyértelműen** felírhatók  $a\alpha^2 + b\alpha + c$  ( $a, b, c \in \mathbb{Q}$ ) alakban („kanonikus alak”);
- ▶ az  $\alpha$  szimbólum azt tudja, hogy  $\alpha^3 = 2$  („számolási szabály”).
- ▶ Hab a tortán:  $\mathbb{Q}(\alpha)$  háromdimenziós vektortér  $\mathbb{Q}$  fölött.

## Ismerősebb példa

A komplex számtest egyszerű algebrai bővítése a valós számtestnek:

$$\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i).$$

- ▶ elemei **egyértelműen** felírhatók  $ai + b$  ( $a, b \in \mathbb{R}$ ) alakban (kanonikus alak);
- ▶ az  $i$  szimbólum azt tudja, hogy  $i^2 = -1$  („számolási szabály”).
- ▶ Hab a tortán:  $\mathbb{C}$  kétdimenziós vektortér  $\mathbb{R}$  fölött.

**Megjegyzés:** A számolási szabály mindkét esetben leírható a minimálpolinommal:

$$m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2 \text{ és } m_{i, \mathbb{R}} = x^2 + 1.$$

## Tétel

Ha  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal, akkor  $K(\alpha)$  izomorf a  $K[x]$  polinomgyűrű modulo  $m$  maradékosztálytestével. Az izomorfizmust a polinomok  $\alpha$  helyen történő kiértékelése szolgáltatja:

$$\varphi: K[x]/(m) \rightarrow K(\alpha), \quad \bar{f} \mapsto f(\alpha).$$

## Bizonyítás.

- ▶ Mikor veszi fel két polinom ugyanazt az értéket az  $\alpha$  helyen?

$$\begin{aligned} f_1(\alpha) = f_2(\alpha) &\iff (f_1 - f_2)(\alpha) = 0 &\iff m \mid f_1 - f_2 \\ &&\iff f_1 \equiv f_2 \pmod{m} \\ &&\iff \bar{f}_1 = \bar{f}_2. \end{aligned}$$

Tehát  $\varphi$  injektív leképezés.

- ▶ Világos, hogy  $\varphi$  felcserélhető a műveetekkel: tetszőleges  $f_1, f_2 \in K[x]$  esetén

$$(f_1 + f_2)(\alpha) = f_1(\alpha) + f_2(\alpha) \quad \text{és} \quad (f_1 \cdot f_2)(\alpha) = f_1(\alpha) \cdot f_2(\alpha).$$



## Tétel

Ha  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal, akkor  $K(\alpha)$  izomorf a  $K[x]$  polinomgyűrű modulo  $m$  maradékosztálytestével. Az izomorfizmust a polinomok  $\alpha$  helyen történő kiértékelése szolgáltatja:

$$\varphi: K[x]/(m) \rightarrow K(\alpha), \quad \bar{f} \mapsto f(\alpha).$$

## Bizonyítás. (folyt.)

- ▶ Tudjuk, hogy  $\varphi$  értékészlete  $K[\alpha]$ . Tehát eddig azt láttuk be, hogy

$$K[x]/(m) \cong K[\alpha].$$

Még azt kellene igazolni, hogy  $K[\alpha] = K(\alpha)$ , vagyis azt, hogy  $K[\alpha]$ -ban minden nemnulla elemnek van multiplikatív inverze.

- ▶ Legyen tehát  $K[\alpha] \ni \beta = f(\alpha) \neq 0$ , ahol  $f \in K[x]$ . Ekkor  $m \nmid f$  (miért?), és így  $\text{Ink}(f, m) \sim 1$  (miért?). Ezért az  $mu + fv = 1$  „diofantoszi egyenletnek” van megoldása a  $K[x]$  polinomgyűrűben (miért?). Értékeljük ki ezt az  $\alpha$  helyen:

$$1 = m(\alpha) \cdot u(\alpha) + f(\alpha) \cdot v(\alpha) = 0 \cdot u(\alpha) + f(\alpha) \cdot v(\alpha) = \beta \cdot v(\alpha).$$

Tehát  $\beta$  multiplikatív inverze  $v(\alpha)$ .



## Következmény

Ha  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal és  $\deg m = n$ , akkor  $K(\alpha)$  elemei egyértelműen felírhatóak

$$a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \quad (a_{n-1}, \dots, a_1, a_0 \in K)$$

alakban. Az ezen elemekkel való számoláshoz elég annyit tudni, hogy  $m(\alpha) = 0$ .

## Bizonyítás.

Láttuk, hogy  $K(\alpha)$  elemei kölcsönösen egyértelműen megfelelnek a  $K$  feletti polinomok modulo  $m$  maradékosztályainak. Mivel a modulus  $n$ -edfokú, minden maradékosztály egyértelműen reprezentálható egy  $n$ -nél kisebb fokú polinommal:

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} \quad (a_{n-1}, \dots, a_1, a_0 \in K).$$

Ennek a maradékosztálynak az előző tételbeli  $\varphi$  izomorfizmusnál éppen az  $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$  elem felel meg.

A tétel másik állítása csak egy informális megfogalmazása a  $K(\alpha) \cong K[x]/(m)$  izomorfíának. □

## Állítás

Ha  $K$  részteste  $L$ -nek, akkor  $L$  vektortér  $K$  felett.

## Bizonyítás.

A vektortéraxiómák mind következnek a testaxiómákból (ugye?). □

## Definíció

Ha  $K$  részteste  $L$ -nek, és  $L$  véges dimenziós vektortér  $K$  felett, akkor azt mondjuk, hogy  $L \mid K$  **végesfokú testbővítés**. Ennek a vektortérnek a dimenzióját a **testbővítés fokszámának** nevezzük. Jelölés:  $[L : K] := \dim_K L$ .

## Következmény

Ha  $\alpha \in L \mid K$  algebrai elem  $m = m_{\alpha, K}$  minimálpolinommal és  $\deg m = n$ , akkor

$$[K(\alpha) : K] = n.$$

## Bizonyítás.

Láttuk, hogy  $K(\alpha)$  elemei egyértelműen felírhatóak az  $\alpha^{n-1}, \dots, \alpha, 1$  elemek lineáris kombinációjaként, tehát ez az  $n$ -elemű „vektorrendszer” bázis, következésképp  $\dim_K K(\alpha) = n$ . □

## Példa

Legyen  $K = \mathbb{Q}$  és  $\alpha = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ . Ekkor  $m_{\alpha, K} = x^4 + 1$ , és így  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ , továbbá a  $\mathbb{Q}(\alpha)$  vektortérnek ( $\mathbb{Q}$  felett) bázisa  $\alpha^3, \alpha^2, \alpha, 1$ , azaz minden elem egyértelműen felírható  $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$  ( $a_3, a_2, a_1, a_0 \in \mathbb{Q}$ ) alakban.

Határozzuk meg az  $\alpha^2 + 2\alpha + 2$  elem multiplikatív inverzét.

## Megoldás

Megoldjuk az  $(x^4 + 1) \cdot u + (x^2 + 2x + 2) \cdot v = 1$  „diofantoszi” egyenletet:

$$u = -\frac{1}{3}, \quad v = \frac{1}{3}x^2 - \frac{2}{3}x + \frac{2}{3}.$$

Tehát

$$\begin{aligned}(x^4 + 1) \cdot \left(-\frac{1}{3}\right) + (x^2 + 2x + 2) \cdot \left(\frac{1}{3}x^2 - \frac{2}{3}x + \frac{2}{3}\right) &= 1 \\ (\alpha^4 + 1) \cdot \left(-\frac{1}{3}\right) + (\alpha^2 + 2\alpha + 2) \cdot \left(\frac{1}{3}\alpha^2 - \frac{2}{3}\alpha + \frac{2}{3}\right) &= 1 \\ (\alpha^2 + 2\alpha + 2) \cdot \left(\frac{1}{3}\alpha^2 - \frac{2}{3}\alpha + \frac{2}{3}\right) &= 1.\end{aligned}$$

A keresett inverz:

$$(\alpha^2 + 2\alpha + 2)^{-1} = \left(\frac{1}{3}\alpha^2 - \frac{2}{3}\alpha + \frac{2}{3}\right).$$

## Másik megoldás

$$\alpha^4 + 1 = 0$$

$$\alpha^4 + 4 = 3$$

$$\alpha^4 + 4\alpha^2 + 4 - 4\alpha^2 = 3$$

$$(\alpha^2 + 2)^2 - (2\alpha)^2 = 3$$

$$(\alpha^2 + 2 - 2\alpha) \cdot (\alpha^2 + 2 + 2\alpha) = 3$$

$$\frac{\alpha^2 - 2\alpha + 2}{3} = \frac{1}{\alpha^2 + 2\alpha + 2}$$

## Keresztkérdés

Adott egy tetszőleges  $f \in K[x]$  polinom. Van-e olyan  $\alpha$  elem, aminek éppen  $f$  a minimálpolinomja?

## Válasz

- ▶ Ha  $f$  nem irreducibilis, akkor biztosan nincs.
- ▶ Ha  $f$  irreducibilis, akkor van: legyen  $T = K[x]/(f)$  (miért test?). Nem nehéz ellenőrizni, hogy az  $\alpha = \bar{x} \in T$  elemre  $m_{\alpha, K} = f$  és  $T = K(\alpha)$ .

## Megjegyzés

- ▶ Ha  $f \in K[x]$  nem irreducibilis, akkor vegyük egy  $m$  irreducibilis osztóját, és alkalmazzuk arra a fenti konstrukciót. Így olyan  $T = K[x]/(m)$  testet kapunk, amelyben  $\alpha = \bar{x}$  gyöke  $f$ -nek (de most  $K(\alpha) \subsetneq T$ ). Így minden polinomnak lehet „gyököt csinálni”.
- ▶ Sőt, az eljárást ismételve olyan  $L$  testet is kaphatunk, amelyben  $f$ -nek annyi gyöke van (multiplicitással), amennyi a fokszáma, azaz  $f$  gyöktényezők szorzatára bomlik  $L$  felett. Ezt nevezzük  $f$  **felbontási testének**.
- ▶ Sőt, az eljárást végtelen sokáig ismételve olyan  $\bar{K}$  testet is kaphtatunk, amelyben már *minden*  $K$  feletti polinomnak van gyöke. Ezt a testet nevezzük  $K$  **algebrai lezártjának**. Pl.  $\bar{\mathbb{R}} = \mathbb{C}$  és  $\bar{\mathbb{Q}} = \bar{\mathbb{A}}$  (az algebrai számok teste).

## Példa

Legyen  $m = x^2 + x + 1 \in \mathbb{Z}_2[x]$  (miért irreducibilis?).

A  $T := \mathbb{Z}_2[x]/(m)$  testnek négy eleme van:  $\bar{0}$ ,  $\bar{1}$ ,  $\bar{x}$ ,  $\overline{x+1}$ .

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Ugyanez tömörebben, a  $0 := \bar{0}$ ,  $1 := \bar{1}$ ,  $\alpha := \bar{x}$ ,  $\beta := \overline{x+1}$  jelöléssel:

+	0	1	$\alpha$	$\beta$	·	0	1	$\alpha$	$\beta$
0	0	1	$\alpha$	$\beta$	0	0	0	0	0
1	1	0	$\beta$	$\alpha$	1	0	1	$\alpha$	$\beta$
$\alpha$	$\alpha$	$\beta$	0	1	$\alpha$	0	$\alpha$	$\beta$	1
$\beta$	$\beta$	$\alpha$	1	0	$\beta$	0	$\beta$	1	$\alpha$

Figyeljük meg, hogy

▶  $\{0, 1\} = \{\bar{0}, \bar{1}\}$  egy  $\mathbb{Z}_2$ -vel izomorf résztestet alkot  $T$ -ben;

▶  $\alpha = \bar{x}$  gyöke az  $x^2 + x + 1 \in T[x]$  polinomnak:

$$\alpha^2 + \alpha + 1 = \overline{x^2 + x + 1} = \overline{x^2 + x + 1} = \bar{0} = 0.$$

## Emlékeztető

Az  $L | K$  testbővítés

- ▶ egyszerű algebrai bővítés, ha  $L = K(\alpha) = [K \cup \{\alpha\}]_t$  és  $\alpha$  algebrai  $K$  felett;
- ▶ végesfokú bővítés, ha  $[L : K] := \dim_K L < \infty$ .

## Definíció

Azt mondjuk, hogy  $L | K$  **algebrai testbővítés**, ha  $L$  minden eleme algebrai  $K$  felett. Ha ez nem teljesül (azaz létezik olyan  $L$ -beli elem, ami transzcendens  $K$  felett), akkor **transzcendens bővítésről** beszélünk.

## Tétel

Tetszőleges  $L | K$  testbővítés esetén

$$L | K \text{ egyszerű algebrai} \xrightarrow{(1)} L | K \text{ végesfokú} \xrightarrow{(2)} L | K \text{ algebrai.}$$

## Bizonyítás.

(1) Ezt már láttuk:  $[K(\alpha) : K] = \deg m_{\alpha, K}$ .

(2) Tfh.  $[L : K] = n$  és  $\alpha \in L$ . Ekkor az  $1, \alpha, \dots, \alpha^n$  „vektorrendszer” lineárisan függő  $K$  felett (miért?), így léteznek olyan  $a_0, a_1, \dots, a_n \in K$  „skalárok” (nem mind nulla), amelyekre  $a_0 \cdot 1 + a_1 \cdot \alpha + \dots + a_n \cdot \alpha^n = 0$ .  
Tehát  $\alpha$  gyöke a nemnulla  $a_0 + a_1x + \dots + a_nx^n \in K[x]$  polinomnak. □



## Megjegyzés

A tételben szeplő két állítás megfordítása nem igaz.

- (1) Van olyan végesfokú bővítés, ami nem egyszerű algebrai. Csak „csúnya” ellenpéldát lehetne mutatni, mert számtestekre igaz a megfordítás. (Ez egyáltalán nem triviális, az ún. **primitív elem tételen** múlik.)
- (2) Van olyan algebrai bővítés, ami nem végesfokú. Például az **algebrai számok teste** nyilván algebrai bővítése  $\mathbb{Q}$ -nak, de nem végesfokú (miért?).

## A testbővítések fokszámtétele

Ha  $K \leq L \leq M$  (végesfokú bővítések), akkor

$$[M : K] = [M : L] \cdot [L : K].$$

## Bizonyítás.

Legyen  $\alpha_1, \dots, \alpha_\ell$  bázisa az  ${}_K L$  vektortérnek (tehát  $[L : K] = \ell$ ), és legyen  $\beta_1, \dots, \beta_m$  bázisa az  ${}_L M$  vektortérnek (tehát  $[M : L] = m$ ).

Ekkor  $\alpha_1\beta_1, \dots, \alpha_\ell\beta_m$  bázisa az  ${}_K M$  vektortérnek, és így  $[M : K] = \ell \cdot m$ .

## Bizonyítás. (folyt.)

Tfh.  $\alpha_1, \dots, \alpha_\ell$  bázisa az  ${}_K L$  vektortérnek,  $\beta_1, \dots, \beta_m$  bázisa az  ${}_L M$  vektortérnek.

Cél:  $\alpha_1\beta_1, \dots, \alpha_\ell\beta_m$  bázisa az  ${}_K M$  vektortérnek.

### ► Generálás:

Bármely  $\mu \in M$  elem felírható  $\mu = \sum_{j=1}^m \lambda_j \cdot \beta_j$  alakban alkalmas  $\lambda_j \in L$  elemekkel (miért?).

Mindegyik  $\lambda_j$  felírható  $\lambda_j = \sum_{i=1}^{\ell} a_{ij} \cdot \alpha_i$  alakban alkalmas  $a_{ij} \in K$  elemekkel (miért?).

Helyettesítsük be ezeket  $\mu$  fenti felírásába:

$$\mu = \sum_{j=1}^m \lambda_j \cdot \beta_j = \sum_{j=1}^m \left( \sum_{i=1}^{\ell} a_{ij} \cdot \alpha_i \right) \cdot \beta_j = \sum_{i,j} a_{ij} \cdot \alpha_i \beta_j.$$

Tehát  $\mu$  valóban előáll az  $\alpha_i\beta_j$  elemek  $K$  feletti lineáris kombinációjaként.

### ► Függetlenség: (zanzásítva)

$$0 = \sum_{i,j} a_{ij} \cdot \alpha_i \beta_j = \sum_{j=1}^m \left( \sum_{i=1}^{\ell} a_{ij} \cdot \alpha_i \right) \cdot \beta_j \implies \sum_{i=1}^{\ell} a_{ij} \cdot \alpha_i = 0 \implies a_{ij} = 0.$$



## Következmény

Ha  $[L : K] = \ell$  és  $\alpha \in L$ , akkor  $\alpha$  algebrai  $K$  fölött, és  $\deg m_{\alpha, K} \mid \ell$ .

## Bizonyítás.

Tekintsük a  $K \leq K(\alpha) \leq L$  kétlépcsős bővítést. A fokszámtétel szerint

$$\ell = [L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K].$$

Másrészt tudjuk, hogy  $[K(\alpha) : K] = \deg m_{\alpha, K}$ . □

## Példa

- ▶  $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$ , mert  $3 = \deg m_{\sqrt[3]{2}, \mathbb{Q}} \nmid [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ .  
Következésképp  $\sqrt[3]{2}$  nem áll elő  $a + b\sqrt{2}$  ( $a, b \in \mathbb{Q}$ ) alakban.
- ▶  $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$ , mert  $2 = \deg m_{\sqrt{2}, \mathbb{Q}} \nmid [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ .  
Következésképp  $\sqrt{2}$  nem áll elő  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$  ( $a, b, c \in \mathbb{Q}$ ) alakban.

## Példa

Legyen  $M = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})(\sqrt{2}) = [\mathbb{Q} \cup \{\sqrt{2}, \sqrt[3]{2}\}]_t$ .  
Határozzuk meg az  $[M : \mathbb{Q}]$  fokszámot, és adjunk meg egy bázist.

## Megoldás

Nézzük két lépcsőben a bővítést:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) = L \leq L(\sqrt{2}) = M.$$

1. Az első lépcső fokszáma:  $[L : \mathbb{Q}] = \deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3$ ; egy bázis:  $1, \sqrt[3]{2}, \sqrt[3]{4}$ .
2. A második lépcső fokszáma:  $[M : L] = \deg m_{\sqrt{2}, L} \stackrel{?}{=} 2$ .

Az világos, hogy  $m_{\sqrt{2}, L} \mid x^2 - 2$  ( $= m_{\sqrt{2}, \mathbb{Q}}$ ).

Ha ez valódi oszthatóság lenne, akkor  $m_{\sqrt{2}, L}$  elsőfokú lenne, vagyis  $\sqrt{2} \in L = \mathbb{Q}(\sqrt[3]{2})$ , de láttuk, hogy ez nem igaz.

Tehát  $m_{\sqrt{2}, L} = x^2 - 2$ , és így  $[M : L] = 2$ ; egy bázis:  $1, \sqrt{2}$ .

A fokszám-tétel szerint  $[M : \mathbb{Q}] = 6$ , és az  ${}_Q M$  vektortér egy bázisa:

$$1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{2}, \sqrt[3]{2}\sqrt{2}, \sqrt[3]{4}\sqrt{2}.$$

Tehát  $M$  elemei így festenek („kanonikus alak”):

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\sqrt{2} + e\sqrt[3]{2}\sqrt{2} + f\sqrt[3]{4}\sqrt{2} \quad (a, b, c, d, e, f \in \mathbb{Q}).$$

## Példa

Legyen  $M = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})(\sqrt{2}) = [\mathbb{Q} \cup \{\sqrt{2}, \sqrt[3]{2}\}]_t$ .  
Határozzuk meg az  $[M : \mathbb{Q}]$  fokszámot, és adjunk meg egy bázist.

## Másik megoldás

Tekintsük az  $N = \mathbb{Q}(\sqrt[6]{2})$  testet. Az  $N | \mathbb{Q}$  bővítés fokszámát könnyű megállapítani:  $[N : \mathbb{Q}] = 6$ . Cél:  $N = M$ .

$$\blacktriangleright \mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt[6]{2}): \sqrt[3]{2} = (\sqrt[6]{2})^2 \text{ és } \sqrt{2} = (\sqrt[6]{2})^3$$

$$\blacktriangleright \mathbb{Q}(\sqrt[6]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{2}): \sqrt[6]{2} = \sqrt{2} / \sqrt[3]{2}$$

Tehát  $N = M$ , és így  $[M : \mathbb{Q}] = 6$ , egy bázis:  $1, \sqrt[6]{2}, \sqrt[6]{4}, \sqrt[6]{8}, \sqrt[6]{16}, \sqrt[6]{32}$ .

## Megjegyzés

Két különböző bázist találtunk ugyanabban a testbővítésben:

$$1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{2}, \sqrt[3]{2}\sqrt{2}, \sqrt[3]{4}\sqrt{2} \quad \text{és} \quad 1, \sqrt[6]{2}, \sqrt[6]{4}, \sqrt[6]{8}, \sqrt[6]{16}, \sqrt[6]{32}.$$

Ilyenkor az egyik bázis elemeit biztosan ki lehet fejezni a másik bázis elemeinek lineáris kombinációjaként, és viszont. Hogyan?

## Példa

Legyen  $M = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = [\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\}]_t$ .  
Határozzuk meg az  $[M : \mathbb{Q}]$  fokszámot, és adjunk meg egy bázist.

## Megoldás

Nézzük két lépcsőben a bővítést:

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) = L \leq L(\sqrt{3}) = M.$$

1. Az első lépcső fokszáma:  $[L : \mathbb{Q}] = \deg m_{\sqrt{2}, \mathbb{Q}} = 2$ ; egy bázis:  $1, \sqrt{2}$ .

2. A második lépcső fokszáma:  $[M : L] = \deg m_{\sqrt{3}, L} \stackrel{?}{=} 2$ .

Az világos, hogy  $m_{\sqrt{3}, L} \mid x^2 - 3$  ( $= m_{\sqrt{3}, \mathbb{Q}}$ ).

Ha ez valódi oszthatóság lenne, akkor  $m_{\sqrt{3}, L}$  elsőfokú lenne, vagyis  $\sqrt{3} \in L = \mathbb{Q}(\sqrt{2})$ , de ez nem igaz:  $\nexists a, b \in \mathbb{Q}: \sqrt{3} = a + b\sqrt{2}$  (HF).

Tehát  $m_{\sqrt{3}, L} = x^2 - 3$ , és így  $[M : L] = 2$ ; egy bázis:  $1, \sqrt{3}$ .

A fokszám-tétel szerint  $[M : \mathbb{Q}] = 4$ , és az  ${}_Q M$  vektortér egy bázisa:

$$1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}.$$

Tehát  $M$  elemei így festenek („kanonikus alak”):

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \quad (a, b, c, d \in \mathbb{Q}).$$

## Példa

Legyen  $M = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2}) = [\mathbb{Q} \cup \{\sqrt{2}, \sqrt{3}\}]_t$ .  
Határozzuk meg az  $[M : \mathbb{Q}]$  fokszámot, és adjunk meg egy bázist.

## Másik megoldás

Tekintsük az  $N = \mathbb{Q}(\alpha)$  testet, ahol  $\alpha = \sqrt{2} + \sqrt{3}$ . Cél:  $N = M$ .

$$\blacktriangleright \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha): \sqrt{2} = -\frac{9}{2}\alpha + \frac{1}{2}\alpha^3 \text{ és } \sqrt{3} = \frac{11}{2}\alpha - \frac{1}{2}\alpha^3$$

$$\blacktriangleright \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}): \alpha = \sqrt{2} + \sqrt{3}$$

Ekkor  $[N : \mathbb{Q}] = 4$ , mert  $m_{\alpha, \mathbb{Q}} = x^4 - 10x^2 + 1$  (miért irreducibilis?).  
Tehát  $N = M$ , és így  $[M : \mathbb{Q}] = 4$ ; egy bázis:  $1, \alpha, \alpha^2, \alpha^3$ .

## Megjegyzés

Két különböző bázist találtunk ugyanabban a testbővítésben:

$$1, \sqrt{2}, \sqrt{3}, \sqrt{6} \quad \text{és} \quad 1, \alpha, \alpha^2, \alpha^3.$$

Ilyenkor az egyik bázis elemeit biztosan ki lehet fejezni a másik bázis elemeinek lineáris kombinációjaként, és viszont. Hogyan?