MINIMÁLPOLINOM

HF: Biz. be, hogy $\nexists\, a,b \in \mathbb{Q} : \sqrt[3]{2} = a + b\sqrt{2}$

1. megoldás: $\sqrt[3]{2} = a + b\sqrt{2}$

$$2 = a^3 + 3a^2 b\sqrt{2} + 3a(b\sqrt{2})^2 + (b\sqrt{2})^3$$

$$2 = a^3 + 3a^2 b\sqrt{2} + 6ab^2 + 2b^3\sqrt{2}$$

$$(3a^2b + 2b^3)\sqrt{2} = a^3 + 6ab^2 - 2$$

$b = 0$: $\sqrt[3]{2} = a \in \mathbb{Q}$ ↯

$b \neq 0$: $3a^2b + 2b^3 = \overbrace{(3a^2 + 2b^2)}^{>0} \cdot \overset{\neq 0}{b} \neq 0$

$$\sqrt{2} = \frac{a^3 + 6ab^2 - 2}{3a^2b + 2b^3} \in \mathbb{Q} \text{ ↯}$$

X: kétjegyű szám

$\text{lnko}(101, x) = ? = d$

$$\left.\begin{array}{l} d \mid 101 \overset{101 \text{ prím}}{\Longrightarrow} d \sim 1 \vee d \sim 101 \\ d \mid x \end{array}\right\} \Rightarrow d \sim 1$$

2. megoldás $\alpha = \sqrt[3]{2} = a + b\sqrt{2} \quad (a, b \in \mathbb{Q})$

$\alpha^3 = 2 \Rightarrow \alpha^3 - 2 = 0 \Rightarrow \alpha$ gyöke az $m(x) = x^3 - 2 \in \mathbb{Q}[x]$ polinomnak.

$$\alpha = a + b\sqrt{2}$$

$$\alpha - a = b\sqrt{2}$$

$$\alpha^2 - 2a\alpha + a^2 = 2b^2$$

$$\alpha^2 - 2a\alpha + a^2 - 2b^2 = 0$$

$\Rightarrow \alpha$ gyöke az $f(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$ polinomnak.

$$\text{lnko}(m, f) = d$$

$$\left.\begin{array}{l} d \mid m \overset{\uparrow}{\Longrightarrow} d \sim 1 \lor d \sim m \\ d \mid f \end{array}\right\} \Rightarrow d \sim 1$$

m irreducibilis Q felett

$$\left.\begin{array}{l} m(\alpha)=0 \Leftrightarrow x-\alpha \mid m \\ f(\alpha)=0 \Leftrightarrow x-\alpha \mid f \end{array}\right\} \Leftrightarrow x-\alpha \mid d \Leftarrow d(\alpha)=0$$

BÉZOUT-tétel

lnko def.

HF Biz. be, hogy $\nexists a, b \in \mathbb{Q}: \sqrt[3]{4} = a + b\sqrt[3]{2}$

<u>Megoldás.</u> $\alpha = \sqrt[3]{2}$

α gyöke az $m(x) = x^3 - 2 \in \mathbb{Q}[x]$ polinomnak

$\alpha^2 = a + b\alpha$

$\alpha^2 - b\alpha + a = 0$

$\Rightarrow \alpha$ gyöke az $f(x) = x^2 - bx + a \in \mathbb{Q}[x]$ polinomnak

$d := \text{lnko}(m, f)$

$(m(\alpha) = 0$ és $f(\alpha) = 0) \Rightarrow d(\alpha) = 0$

$$\left.\begin{array}{l} m \text{ irr. } \mathbb{Q} \text{ felett} \Rightarrow d \sim 1 \lor d \sim m \\ \deg f = 2 \Rightarrow m \nmid f \Rightarrow d \nsim m \end{array}\right\} \Rightarrow d \sim 1$$

$\alpha = \sqrt[3]{2}$ gyöke az $m = x^3 - 2 \in \mathbb{Q}[x]$ pol.-nak.

— " — $\boxed{\underbrace{(x^3-2)}_{x=\alpha:\,0} \cdot \underbrace{(13x^7 - 4x^5 + 6x - 1)}_{x=\alpha:\ ?}}^{f} \in \mathbb{Q}[x]$ pol.-nak

$\forall f \in \mathbb{Q}[x]: m \mid f \Rightarrow f(\alpha) = 0$

Tfh. $f \in \mathbb{Q}[x]$: $\left.\begin{array}{l} f(\alpha)=0 \\ m(\alpha)=0 \end{array}\right\} \Longrightarrow d(\alpha)=0$ — lko(f,m)

m irr. $\Rightarrow d \sim 1 \vee \boxed{d \sim m} \Rightarrow m \mid f$

$\Downarrow$

$\deg m \leq \deg f$

m mini. fokú

$\{f \in \mathbb{Q}[x] \mid f(\alpha)\} = m$ többszöröseinek halmaza

DEF. K számtest (pl. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \ldots$), $\alpha \in \mathbb{C}$

1) $\forall f \in K[x]$: $f(\alpha)=0 \Rightarrow f=0$

Ekkor α TRANSZCENDENS K felett.

2) $\exists f \in K[x]$, $f \neq 0$: $f(\alpha)=0$

Ekkor α ALGEBRAI K felett.

Legyen $m \in K[x]$ mini. fokú olyan $\neq 0$ pol., amelyre $m(\alpha)=0$.

Ekkor m: α MINIMÁLPOLINOMJA K felett

$m \sim m_{\alpha,K}$

PÉLDA • π transzcendens $\mathbb{Q}$ felett (NEHÉZ!)

• $\sqrt[3]{2}$ algebrai $\mathbb{Q}$ felett $m_{\sqrt[3]{2},\mathbb{Q}} \sim \boxed{x^3-2}$, $\sim 3x^3-6$

TÉTEL $m_{\alpha,K}$ irred. K felett.

Biz. Tfh. nem irr: $m_{\alpha,K} = f_1 \cdot f_2$ $\deg f_1, \deg f_2 < \deg m_{\alpha,K}$

$$\underbrace{m_{\alpha,K}(\alpha)}_{0} = \underbrace{f_1(\alpha)\cdot f_2(\alpha)}_{0[\vee\, 0]} \implies$$

$f_1(\alpha)=0$ és $\deg f_1 < \deg m_{\alpha,K}$ ↯ mini. $\square$

TÉTEL $m\in K[x]$, $m(\alpha)=0$, m irr. K felett

$\implies m \sim m_{\alpha,K}$.

Biz.: Legyen $f\in T[x]$, $f(\alpha)=0$. Cél: $\deg m \leq \deg f$.

$$\left.\begin{array}{l} m(\alpha)=0 \\ f(\alpha)=0 \end{array}\right\} \implies d(\alpha)=0 \quad \text{lnko}(m,f)$$

$$m \text{ irr.} \implies d\sim 1 \vee \boxed{d\sim m} \implies m\,|\,f$$

$$\Downarrow$$

$$\deg m \leq \deg f. \square$$

KÖV. $\{f\in K[x] \mid f(\alpha)=0\} = m$ többszörösei

$$\boxed{f(\alpha)=0 \iff m\,|\,f}$$

$x^2+1=(x+i)\cdot(x-i)$ — x^2+1 nem irr. $\mathbb{C}$ felett

x^2+1 irr $\mathbb{R}$ felett

x^2+1 irr. $\mathbb{Q}$ felett

$x^2-2=(x-\sqrt{2})\cdot(x+\sqrt{2})$ — x^2-2 nem irr $\mathbb{C}$ felett

x^2-2 nem irr $\mathbb{R}$ felett

x^2-2 irr $\mathbb{Q}$ felett

($\mathbb{C} \supseteq \mathbb{R} \supseteq \mathbb{Q}$)

PÉLDA $\quad (x-\sqrt[3]{2})\cdot(\dots)$

$$m_{\sqrt[3]{2},\mathbb{Q}} \sim x^3-2 \qquad m_{\sqrt[3]{2},\mathbb{R}} \sim x-\sqrt[3]{2} \qquad m_{\sqrt[3]{2},\mathbb{C}} \sim x-\sqrt[3]{2}$$

$$m_{\sqrt[100]{2},\mathbb{Q}} \sim x^{100}-2 \qquad m_{\sqrt[100]{2},\mathbb{R}} \sim x-\sqrt[100]{2} \qquad m_{\sqrt[100]{2},\mathbb{C}} \sim x-\sqrt[100]{2}$$

irr. $\mathbb{Q}$ felett
S-E, $p=2$

$$m_{i,\mathbb{Q}} \sim x^2+1 \qquad m_{i,\mathbb{R}} \sim x^2+1 \qquad m_{i,\mathbb{C}} \sim x-i$$

irr $\mathbb{Q}$ felett
nincs gyöke $\mathbb{Q}$ fa
és 2-odfokú

irr $\mathbb{R}$ felett
nincs gyöke $\mathbb{R}$ fa
és 2-odfokú

TRIVI. $\quad \alpha \in K \iff m_{\alpha,K} = x-\alpha$

$\alpha \notin K \iff \deg m_{\alpha,K} \geq 2$

PÉLDA $\quad \alpha = 2+3i \qquad K = \mathbb{C}, \mathbb{R}, \mathbb{Q}$

$$m_{\alpha,\mathbb{C}} \sim x-\alpha = x-(2+3i)$$

$$\alpha - 2 = 3i$$

$$\alpha^2 - 4\alpha + 4 = -9$$

$\alpha^2 - 4\alpha + 13 = 0 \Rightarrow \alpha$ gyöke az $x^2-4x+13 \in \mathbb{R}[x]$ pol.-nak.

$$\Rightarrow m_{\alpha,\mathbb{R}} \mid \underbrace{x^2-4x+13}_{\substack{\text{irr. } \mathbb{R} \text{ felett:} \\ \text{nincs gyöke } \mathbb{R}\text{-ben} \\ \text{és csak 2-odfokú}}} \Rightarrow m_{\alpha,\mathbb{R}} \sim x^2-4x+13$$

$\mathbb{Q} \subseteq \mathbb{R}$

$$\Rightarrow m_{\alpha,\mathbb{Q}} \sim x^2-4x+13$$

PÉLDA $\alpha = \sqrt{3} + i \qquad K = \mathbb{C}, \mathbb{R}, \mathbb{Q}$

$$m_{\alpha,\mathbb{C}} = x - \alpha = x - \sqrt{3} - i$$

$$\alpha - \sqrt{3} = i$$

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

$$\alpha^2 - 2\sqrt{3}\alpha + 4 = 0$$

$$f = x^2 - 2\sqrt{3}x + 4 \in \mathbb{R}[x] \qquad f(\alpha) = 0$$

$\Rightarrow m_{\alpha,\mathbb{R}} \mid f$ ← irr. $\mathbb{R}$ felett (nincs valós gyöke és csak 2-odfokú)
$(\sqrt{3} \pm i)$

$$\Rightarrow m_{\alpha,\mathbb{R}} \sim f = x^2 - 2\sqrt{3}x + 4$$

$$\alpha^2 + 4 = -2\sqrt{3}\alpha$$

$$\boxed{m_{\alpha,\mathbb{R}} \mid m_{\alpha,\mathbb{Q}}}$$

$$\alpha^4 + 8\alpha^2 + 16 = 12\alpha^2$$

$$\alpha^4 - 4\alpha^2 + 16 = 0$$

$$g = x^4 - 4x^2 + 16 \in \mathbb{Q}[x] \qquad g(\alpha) = 0$$

$\Rightarrow m_{\alpha,\mathbb{Q}} \mid g$ irr. $\mathbb{Q}$ felett?

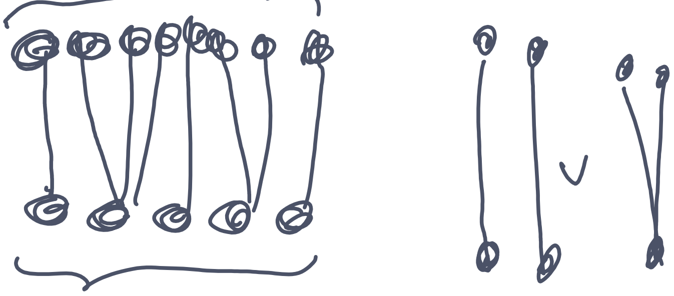
$$x^4 - 4x^2 + 16 = \underbrace{(x^2 - 2\sqrt{3}x + 4)\cdot(x^2 + 2\sqrt{3}x + 4)}_{g \text{ irr. fell. } \mathbb{R} \text{ felett}}$$

$\mathbb{R}$

$\cup$

$\mathbb{Q}$

irr. fel. $\mathbb{R}$ felett



irr. fel. $\mathbb{Q}$ felett

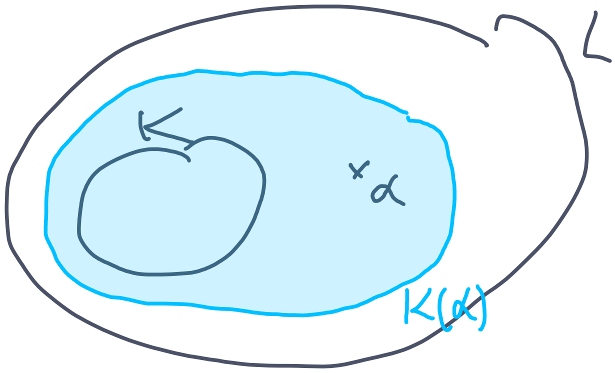
$$\underbrace{\boxed{x^4 - 4x^2 + 16}}_{g \text{ irr. fell. } \mathbb{Q} \text{ felett?}}$$

$\Rightarrow g$ irr. $\mathbb{Q}$ felett $\Rightarrow m_{\alpha,\mathbb{Q}} \sim g = x^4 - 4x^2 + 16$

TESTBŐVÍTÉSEK

$K \leq L \leq \mathbb{C}$

résztest



PÉLDA $K=\mathbb{Q}$ $\quad \alpha=\pi$

$$[\mathbb{Q}\cup\{\pi\}]_{gy} = \mathbb{Q}[\pi] \qquad +,-,\cdot$$

$$\mathbb{Q}[\pi] \ni \pi,\ \pi+\frac{2}{3},\ \pi^2,\ \pi^2-\pi-\frac{2}{3},\ \dots$$

$$\in$$

$$\underbrace{a_n\cdot\pi^n + a_{n-1}\cdot\pi^{n-1} + \dots + a_1\pi + a_0}_{f(\pi),\ \text{ahol}\ f = a_nx^n+\dots+a_1x+a_0} \quad (n\in\mathbb{N},\ a_i\in\mathbb{Q})$$

$$\mathbb{Q}[\pi] \supseteq \{f(\pi) \mid f\in\mathbb{Q}[x]\} \leftarrow \text{zárt } +,-,\cdot\text{-ra}$$

$$[\mathbb{Q}\cup\{\pi\}]_t = \mathbb{Q}(\pi) \qquad +,-,\cdot,/$$

$$\mathbb{Q}(\pi) \supseteq \left\{\frac{f(\pi)}{g(\pi)} \,\middle|\, f,g\in\mathbb{Q}[x],\ g(\pi)\neq 0\right\} \leftarrow \text{zárt } +,-,\cdot,/\text{-re}$$

PÉLDA $\alpha=\sqrt{2}$ $\quad K=\mathbb{Q}$

$$[\mathbb{Q}\cup\{\sqrt{2}\}]_{gy} = \mathbb{Q}[\sqrt{2}] \qquad +,-,\cdot$$

$$\mathbb{Q}[\sqrt{2}] \ni a_n\sqrt{2}^n + a_{n-1}\sqrt{2}^{n-1} + \dots + a_1\sqrt{2} + a_0 \quad (n \in \mathbb{N},\ a_i \in \mathbb{Q})$$

$$3\cdot(\sqrt{2})^3 - 7(\sqrt{2})^2 + 5\cdot\sqrt{2} + 3 =$$

$$= 6\cdot\sqrt{2} - 14 + 5\cdot\sqrt{2} + 3 =$$

$$= -11 + 11\sqrt{2}$$

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \{f(\sqrt{2}) \mid f \in \mathbb{Q}[x]\}$$

$$[\mathbb{Q} \cup \{\sqrt{2}\}]_t = \mathbb{Q}(\sqrt{2}) \qquad +, -, \cdot, /$$

$$\mathbb{Q}(\sqrt{2}) \ni \frac{1}{\sqrt{2}} = \underbrace{0}_{\in\mathbb{Q}} + \underbrace{\tfrac{1}{2}}_{\in\mathbb{Q}} \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\mathbb{Q}(\sqrt{2}) \ni \frac{1}{3+5\sqrt{2}} = \underbrace{\frac{-3}{41}}_{\in\mathbb{Q}} + \underbrace{\frac{5}{41}}_{\in\mathbb{Q}} \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\frac{1}{3+5\sqrt{2}} \cdot \frac{3-5\sqrt{2}}{3-5\sqrt{2}} = \frac{3-5\sqrt{2}}{9-50} = \frac{3-5\sqrt{2}}{-41} \in \mathbb{Q}[\sqrt{2}]$$

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
$$= \{f(\sqrt{2}) \mid f \in \mathbb{Q}[x],\ \deg f \le 1\}$$

PÉLDA $\alpha = \sqrt[3]{2},\ K = \mathbb{Q}$

$$a + bx + cx^2 = f$$

$$\mathbb{Q}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) \mid f \in \mathbb{Q}[x]\} = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$
$$= \{f(\sqrt[3]{2}) \mid f \in \mathbb{Q}[x],\ \deg f \le 2\}$$

$$(\sqrt[3]{2})^1 = \sqrt[3]{2},\ (\sqrt[3]{2})^2 = \sqrt[3]{4},\ (\sqrt[3]{2})^3 = 2,\ (\sqrt[3]{2})^4 = 2\sqrt[3]{2},\ (\sqrt[3]{2})^5 = 2\sqrt[3]{4}$$

$$\mathbb{Q}(\sqrt[3]{2}) \ni \frac{1}{\sqrt[3]{2}} = \underbrace{0}_{\in\mathbb{Q}} + \underbrace{0}_{\in\mathbb{Q}}\cdot\sqrt[3]{2} + \underbrace{\tfrac{1}{2}}_{\in\mathbb{Q}}\cdot\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$$

$$\frac{1}{\sqrt[3]{2}}\cdot\frac{\sqrt[3]{4}}{\sqrt[3]{4}} = \frac{\sqrt[3]{4}}{2} \in \mathbb{Q}[\sqrt[3]{2}]$$

$$\mathbb{Q}(\sqrt[3]{2}) \ni \frac{1}{\sqrt[3]{4}-2\sqrt[3]{2}+1} = \underbrace{\qquad}_{\in\mathbb{Q}} + \underbrace{\qquad}_{\in\mathbb{Q}}\cdot\sqrt[3]{2} + \underbrace{\qquad}_{\in\mathbb{Q}}\cdot\sqrt[3]{4}$$

$\alpha = \sqrt[3]{2} \qquad \alpha^3 = 2 \qquad \alpha^3 - 2 = 0 \qquad m_{\alpha,\mathbb{Q}} = x^3 - 2$

$$\mathbb{Q}[\alpha] = \{ g(\alpha) \mid g \in \mathbb{Q}[x],\ \deg g \le 2 \} =$$
$$= \{ a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q} \}$$

$$\frac{1}{\sqrt[3]{4}-2\sqrt[3]{2}+1} = \frac{1}{\alpha^2 - 2\alpha + 1} = \frac{1}{f(\alpha)}, \text{ ahol } f = x^2 - 2x + 1$$

Cél: $\dfrac{1}{f(\alpha)} = v(\alpha)$, ahol $v \in \mathbb{Q}[x]$, $\deg v \le 2$

$$\underbrace{\overset{0}{\widetilde{m(\alpha)}}\cdot u(\alpha)}_{0} + f(\alpha)\cdot v(\alpha) = 1 \qquad\qquad m = x^3 - 2$$

$$\Uparrow$$

$m(x)\cdot u(x) + f(x)\cdot v(x) = 1$ adott: m, f keressük: $u, v \in \mathbb{Q}[x]$

$m \cdot u + f \cdot v = 1$ kétismeretlenes lineáris „diofantoszi" egyenlet

$$\overbrace{(x^3-2)}^{m} : \overbrace{(x^2-2x+1)}^{f} = \overbrace{x+2}^{\text{hányados}}$$

$$\begin{array}{l} x^3-2x^2+x \\ \hline 2x^2-x-2 \\ 2x^2-4x+2 \\ \hline \underbrace{3x-4}_{\text{maradék}} \end{array}$$

$$m = f\cdot(x+2) + (3x-4)$$

$$3x-4 = m - f\cdot(x+2) \quad (1)$$

$$\cancel{= (x^3-2) - (x^2-2x+1)\cdot(x+2) =}$$

$$\cancel{= \ldots 3x-4}$$

$$\overbrace{(x^2-2x+1)}^{f} : (3x-4) = \overbrace{\frac{1}{3}x - \frac{2}{9}}^{\text{hányados}}$$

$$\begin{array}{l} x^2 - \frac{4}{3}x \\ \hline -\frac{2}{3}x + 1 \\ -\frac{2}{3}x + \frac{8}{9} \\ \hline \underbrace{\frac{1}{9}}_{\text{maradék}} \sim 1 \end{array}$$

$$f = (3x-4)\cdot\left(\frac{1}{3}x - \frac{2}{9}\right) + \frac{1}{9}$$

$$\frac{1}{9} = f - \underbrace{(3x-4)}_{(1)}\cdot\left(\frac{1}{3}x - \frac{2}{9}\right) \quad (2)$$

$$(2):\ \frac{1}{9} = f - \underbrace{(3x-4)}_{m-f\cdot(x+2)}\cdot\left(\frac{1}{3}x - \frac{2}{9}\right) \overset{(1)}{=} f - (m - f(x+2))\cdot\left(\frac{1}{3}x - \frac{2}{9}\right)$$

$$1 = 9f - (m - f\cdot(x+2))\cdot(3x-2) =$$

$$= 9f - m\cdot(3x-2) + f\cdot(x+2)\cdot(3x-2) =$$

$$= m\cdot(-3x+2) + f\cdot((x+2)\cdot(3x-2)+9)$$

$$= m\cdot\underbrace{(-3x+2)}_{u} + f\cdot\underbrace{(3x^2+4x+5)}_{v} = 1$$

$$\Downarrow\ x = \alpha$$

$$\underbrace{\overset{0}{m(\alpha)}\cdot(-3\alpha+2)}_{0} + f(\alpha)\cdot\underbrace{(3\alpha^2+4\alpha+5)}_{1/f(\alpha)} = 1$$

$$\frac{1}{f(\alpha)} = \frac{1}{\alpha^2 - 2\alpha + 1} = v(\alpha) = 3\alpha^2 + 4\alpha + 5$$

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = 3 \cdot \sqrt[3]{4} + 4\sqrt[3]{2} + 5$$

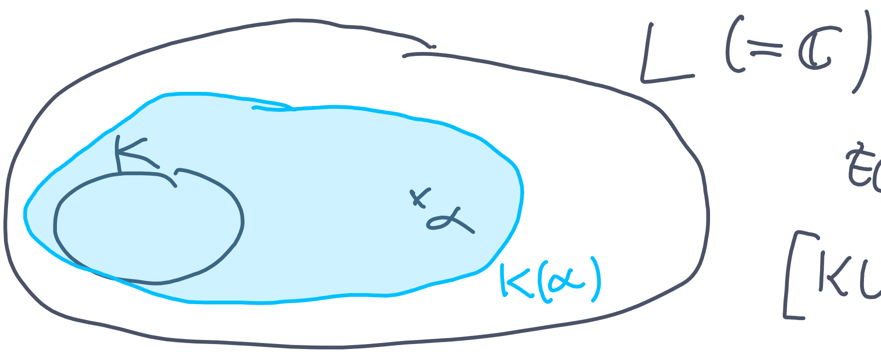
TÉTEL K α algebrai K felett $m := m_{\alpha,K}$ $\deg m = n$.

$$K[\alpha] = K(\alpha) = \{f(\alpha) \mid f \in K[x],\ \deg f \leq n-1\}$$
$$= \{a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$$

$$f(\alpha) \pm g(\alpha) = (f \pm g)(\alpha)$$

$$f(\alpha) \cdot g(\alpha) = (f \cdot g \bmod m)(\alpha)$$

$$\frac{1}{f(\alpha)} = v(\alpha) \qquad mu + f \cdot v = 1 \text{ (eukl. alg.)}$$



EGYSZERŰ ALGEBRAI BŐVÍTÉS

$$[K \cup \{\alpha\}]_t = K(\alpha)$$

$$m = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

$$0 = \alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0$$

$$\boxed{\alpha^n = -b_{n-1}\alpha^{n-1} - \ldots - b_1\alpha - b_0}$$

[$\alpha = \sqrt[3]{2} : \alpha^3 = 2$

$\alpha = i \ : \ i^2 = -1$]