IPMPFMF 2025-04-01

$K \subseteq \mathbb{R}$

$\hookrightarrow$ konstruktibilna števila.

$$\mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K = \bigcup_n K_n$$

Trditev: Let $\underbrace{K}$ (to ni več množica konstruktibilnih števil) $\subseteq F$, $a \in F$

$K(a)$ je najmanjši podobseg F, ki vsebuje K in a (= najmanjša razširitev K, ki vsebuje $a \in F$).

Zakaj? Vzemimo vse podobsege F, ki vsebujejo a in K. Njihov presek je obseg in po definiciji najmanjši z istimi lastnostmi.

Primer: $\mathbb{Q}(\sqrt{2})$.

$K(a)$ je enostavna razširitev K z a.

$$K(a) = \left\{ \frac{k_0 + k_1 a + \dots + k_n a^n}{k_0' + k_1' a + \dots + k_n' a^n} \; ; \; k_i, k_i' \in K, \; n \in \mathbb{N}, \; \text{imenovalec} \neq 0 \right\}$$

torej $\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \; ; \; a, b, c, d \in \mathbb{Q} \right\} = \{ a + b\sqrt{2} \; ; \; a, b \in \mathbb{Q} \}$

Opazujemo: $\varphi_a : K[x] \to F$
$p(x) \mapsto p(a)$.

$\underline{\operatorname{Im} \varphi_a} = K[a] = \{ p(a) \; ; \; p(x) \in K[x] \}$

$\hookrightarrow$ podkolobar F, ki v splošnem ni obseg

$\ker \varphi_a = \{ p(x) \in K[x] \; ; \; p(a) = 0 \}$

case $\ker \varphi_a = \{0\}$: a ni ničla nobenega polinoma iz $K[x]$.
a je transcendenten nad K.

case $\ker \varphi_a \neq \{0\}$: $\exists$ netrivialni neničelni polinom $p(x)$ s koef. v K, ki ima v a ničlo.

pravimo a je algebraičen nad K.
(lahko ga dosežemo kot ničlo nad K)

primeri: $\sqrt{2}$ je ničla $p(x) = x^2 - 2 \Rightarrow \sqrt{2}$ je algebraičen nad $\mathbb{Q}$.

Transcendentna števila nad $\mathbb{Q}$. Gotovo obstajajo zaradi kardinalnosti: algebraičnih števil nad $\mathbb{Q}$ je števno, ker $\mathbb{Q}[x]$ je števna, vsak polinom ima končno ničel. $\Rightarrow$ Večina $\mathbb{R}$ števil je transcendentna nad $\mathbb{Q}$.

- i je algebraičen nad $\mathbb{Q}$.
- π je algebraičen nad $\mathbb{R}$: $p(x) = \pi - x$
- π in e sta transcendentna nad $\mathbb{Q}$
ne bomo dokazali.

Def: $K \leq F$. F je algebraična razširitev K, če so vsi elementi F algebraični nad K.
F je transcendentna razširitev K, če $\exists$ vsaj en element F, ki je nad K transcendenten.

Ker $\varphi_a : K[x] \to F$ ni trivialno, tj. $\ker \varphi_a$ je pravi ideal v $K[x]$ (slednji je glavnoidealski).

$\ker \varphi_a = (g_a(x))$, $g_a(x)$ je enolično določen z zahtevo, da je moničen (vodilni koef. 1) in da deli vse polinome, ki imajo a za ničlo.

$\Rightarrow g_a(x)$ je minimalni polinom za a nad K.

Trditev: $g_a(x)$ je nerazcepen

Dokaz: Pdp. $g_a(x) = p(x)\,q(x)$ za p, q nižje stopnje $\Rightarrow g_a(a) = p(a)\,q(a) = 0 \Rightarrow$ $p(a) = 0 \vee q(a) = 0 \Rightarrow$ imamo manjši polinom, ki anhilira a $\times$.

$\Rightarrow (g_a(x)) = \ker \varphi_a$ je maksimalen ideal v $K[x]$.

$\Rightarrow \overline{\varphi_a} : \underbrace{K[x]/(g_a(x))}_{\substack{\text{maksimalen} \\ \Downarrow \\ \text{je obseg}}} \xrightarrow[\operatorname{im}\varphi]{\cong} \underbrace{K[x]}_{\text{je obseg}}$ z OB imamo $\operatorname{im}\varphi$

$K \leq K[a] \leq K(a) \leq F$

$=$ ako a algebraičen nad K

Primeri: $\bullet$ $\underbrace{\{a + b\sqrt{2} ;\ a, b \in \mathbb{Q}\}}_{= \mathbb{Q}[\sqrt{2}]} = \underbrace{\left\{ \frac{a + b\sqrt{2}}{c + d\sqrt{2}} ;\ a, b, c, d \in \mathbb{Q} \right\}}_{= \mathbb{Q}(\sqrt{2})}$

- $a = \sqrt{2} + \sqrt[3]{3}$

$$\mathbb{Q}[a] = \{a + b(\sqrt{2} + \sqrt[3]{3}) + c(\ )^2 + d(\ )^3 + \dots ??\}$$

$$\mathbb{Q}[a] = \mathbb{Q}(a)$$

koliko členov ?

$[K(a):K]$

$$K(a) = K[a] \cong K[x]/(g_a(x))$$

baza: $1 + (g_a(x)),\ x + (g_a(x)), \dots, x^{\deg g_a - 1} + (g_a(x))$

$\downarrow$ izomorfizem: vstavi a

baza: $1, \quad a, \quad a^2, \quad \dots, \quad a^{d-1}$

<u>Izrek:</u> Let $a \in F$ algebraičen nad $K \leq F$

a.) $\exists!$ monični polinom $g_a(x)$, ki deli vse polinome, ki imajo a za ničlo $\hookrightarrow$ minimalni polinom za a nad K.

b.) minimalna razširitev $K(a) = K[a] \cong K[x]/(g_a(x))$

c.) stopnja razširitve := stopnja minimalnega polinoma

zadatno: baza za $K(a)$ nad K: $1, a, \dots, a^{\deg g_a - 1}$

<u>Oznaka:</u> $\deg_K(a) := [K(a):K]$ oz. $\deg g_a(x)$

$\hookrightarrow$ stopnja a nad K

Posledica: če je F končna razširitev K, potem

$$\forall a \in F: \deg_K a \mid [F:K]$$

deli

Dokaz: $K \subseteq K(a) \subseteq F \rightsquigarrow [F:K] = [F:K(a)] \cdot \underbrace{[K(a):K]}_{\deg_K a}$

□

Vsako konstruktibilno število dobimo s končnim zaporedjem operacij, kjer bodisi ostanemo v istem obsegu bodisi dodamo kvadratni koren nekega elementa. $\Rightarrow$ vsako konstruktibilno število je v neki razširitvi stopnje 2^k obsega $\mathbb{Q}$.

Posledica: Stopnja vsakega konstruktibilnega števila nad $\mathbb{Q}$ je potenca št. 2. ZDB

a konstruktibilno $\Rightarrow \deg_{\mathbb{Q}} a = 2^k$

(velja tudi $\Leftarrow$ a ne bomo dokazali niti potrebovali)

Primeri:
- $\sqrt[3]{2}$ ni konstruktibilno. $x^3 - 2$ je nerazcepen, moničen in ima $\sqrt[3]{2}$ za ničlo.
- Kvadratura kroga.
  $\sqrt{\pi}$ ni algebraično število.
  (ne bomo dokazali)

- trisekcija kota:

dan je konstruktibilen kot

kot α je konstruktibilen $:\Leftrightarrow$ $\cos\alpha$ in $\sin\alpha$ sta konstruktibilni števili.

α velja $\cos\alpha$ konstr. $\Rightarrow \cos\frac{\alpha}{3}$ konstr.?

velja $\cos\alpha = 4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3}$

$\rightarrow$ za $\alpha = 60°$: $\rightsquigarrow \cos\alpha = 1/2$

$$4\cos^3\frac{\alpha}{3} - 3\cos\frac{\alpha}{3} - \frac{1}{2} = 0$$

$$\deg_{\mathbb{Q}} \cos\frac{\alpha}{3} = 3 = \deg_{\mathbb{Q}} \cos 20°$$

$\hookrightarrow \neq 2^k \Rightarrow$ kot $20°$ ni konstruktibilen.

$$4x^3 - 3x = \frac{1}{2}$$

$8x^3 - 6x - 1$ nerazcepen

$\rightarrow$ za $\alpha = 90°$, $\cos\alpha = 0$

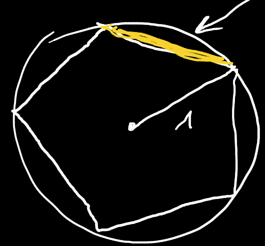
$$4x^3 - 3x = x\underline{(4x^2 - 3)}$$

$2^k \Rightarrow$ je konstrukt.

Sklep: $\cos\frac{\alpha}{3}$ konstruktibilno $\iff 4x^3 - 3x - \cos\alpha$ razcepen nad $\mathbb{Q}$ $\iff$ ima racionalno ničlo.

- pravilni n-kotniki
  - trikotnik, štirikotnik, petkotnik, šestkotnik, osemkotnik.

$$\deg_{\mathbb{Q}} \sqrt{\frac{5-\sqrt{5}}{2}} = 4$$



× sedemkotnik ima stranico z min. polinomom $x^3 + x^2 - 2x - 1$

<u>Izrek (Gauss-Wantzel)</u>: pravilni n-kotnik je konstruktibilen z ravnilom in šestilom $\Leftrightarrow$

$\Leftrightarrow$ $n = 2^k \cdot$ (produkt različnih Fermatovih praštevil)

Fermatova števila so oblike $2^{(2^n)} - 1 =: F_n$

Fermatova praštevila so Fermatova števila, ki so praštevila

prvih nekaj Fermatovih števil:

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

$F_5 - F_{32}$ so vsa sestavljena.

za F_{33} in dalje so števila prevelika, da bi preverili. domnevajo, da so vsa nadaljnja sestavljena.