IPMPFMF2025-03-25

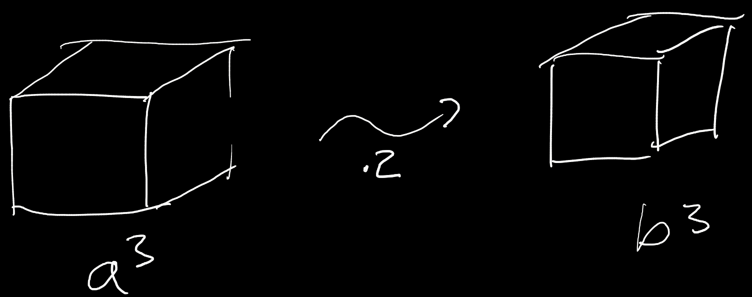
[Konstruktibilna števila]

... števila, ki jih lahko konstruiramo z ravnilom in šestilom.

Ne poznamo splošne konstrukcije za razdelitev danega kota na tretjine. Trisekcija kota.

Dokazano v 1837, da to za poljubni kot ni možno (za specifične seveda je, denimo za 90°). [wikipedia]

Podvojitev kocke (po volumnu)



$$2a^3 = b^3$$

$$b = \underline{\sqrt[3]{2}}\, a$$

Kvadratura kroga

Konstruiraj kvadrat z enako ploščino kot dan krog.

Pravilni mnogokotniki

Pravilne $\{3..6\}$ kotnike je mož narisati.

- sedemkotnika se ne da (dokaže gauss).

· Gauss skonstruira 17kotnik

itd. ne vemo če $\forall n \in \mathbb{N}$ ali se n-kotnik da narisati.

Dopustni operaciji

- skozi dve točki potegnemo premico
- za dani dve točki konstruiramo krožnico s središčem v eni točki, ki gre skozi drugo.

(·) presečišča so nove točke

(·) rišemo v ravnini

(·) ... + ostali evklidovi aksiomi

Konstrukcija števil

1. Fiksiramo enotsko dolžino, tj. 1 je konstruktibilno število.

2. Za konstruktibilni števili a, b je točka (a,b) konstruktibilna in obratno.

3. (a,b), (c,d) konstruktibilni točki tvorita konstruktibilno premico / krožnico.

4. Preseki slednjih so konstruktibilne točke.

Oznaka: let K množica vseh realnih števil, ki jih lahko dobimo kot rezultat končnega števila korakov 2.–4..

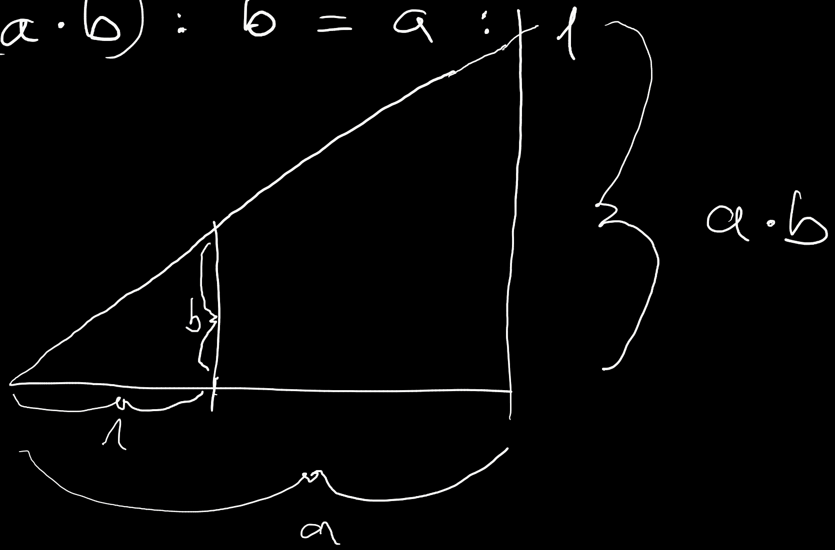
Izrek: K je obseg. $\mathbb{Q} < K < \mathbb{R}$.

strogo

za operacije $+, -, \cdot, /$ iz obsega realnih št.

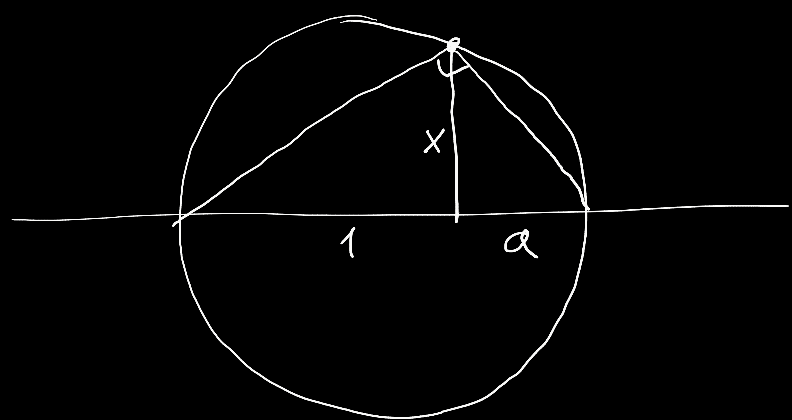
Dokaz: Zaprtost za $+$ je očitna (šestilo).

množenje: $(a \cdot b) : b = a : 1$



deljenje: podobno.

mimogrede: $\sqrt{a}$:



$$\frac{a}{x} = \frac{x}{1}$$

$$\Rightarrow x = \sqrt{a}.$$

$\Rightarrow \quad K \neq \mathbb{Q}$.

$K \neq \mathbb{R}$, ker je kardinalnost K števna, $\mathbb{R}$ pa ne. (KONČNO mnogo korakov za konstrukcijo).

Vemo, da $\pi \notin K$. Pokazje žalo dolg.

$e \notin K$.

Še danes ne vemo, a je $\pi + e \in K$.

$$\mathbb{Q} = K_0 \leq K_1 \leq K_2 \leq K_3 \leq \cdots \leq K = \bigcup_{n \geq 1}^{\infty} K_n$$

K_{n+1} je najmanjši podobseg $\mathbb{R}$, ki vsebuje vse kvadratne točke pozitivnih elementov K_n.

Razširitve obsegov

za $K \leq F$ rečemo F je razširitev obsega K.

podobseg, a ne rečemo „nadobseg"

$\rightsquigarrow$ F je vektorski prostor nad K.

če je $\underbrace{[F:K]}_{F \text{ glede na } K} = \dim_K F$ $\begin{cases} \to \text{končna} \ldots \text{gre za končno razširitev} \\ \to \text{neskončna} \ldots \text{gre za neskončno razširitev} \end{cases}$

Primeri: $[\mathbb{R} : \mathbb{Q}]$ neskončna razširitev

$[\mathbb{C} : \mathbb{R}]$ končna razširitev stopnje 2.

$a + bi$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ končna razširitev stopnje 2

$a + \sqrt{2}\, b$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ končna razširitev stopnje 3.

$a \cdot 1 + b \cdot \sqrt[3]{2} + c \cdot \sqrt[3]{4}$

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

<u>Izrek:</u> če je $K \leq F \leq E$, je
($\leq$: podobseg)

$$[E:K] = [E:F] \cdot [F:K].$$

<u>Dokaz:</u> privzemimo, da $[F:K], [E:F]$ končni.
($[F:K] = m$, $[E:F] = n$)

$\Rightarrow \exists \{x_1, \dots, x_m\}$ baza za F nad K.

zdb vsak element f lahko napišemo kot linearno kombinacijo m elementov iz obsega K.

$\exists \{y_1, \dots, y_n\}$ baza za E nad F.

$\{\underset{\in F \subseteq E}{x_i} \cdot \underset{\in E}{y_j} ; \forall i \in \{1..m\}, j \in \{1..n\}\}$ je baza za E nad K

<u>• razpenja:</u> vzemimo element $e \in E$ poljuben.

$e = f_1 y_1 + \dots + f_n y_n$, $\underline{f_i \in F}$ $\rightarrow$ vsih zapišemo kot LK. el. iz K:

$$\forall i \in \{1..n\} : f_i = k_{i1} x_1 + \dots + k_{im} x_m$$

$$e = \sum_{i=1}^{n} (f_i) y_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} k_{ij} x_j \right) y_i =$$

$$= \sum_{i,j} k_{ij} (x_j y_i).$$

• LN: $\sum_{i,j} k_{ij} x_j y_i = 0$

$$0 = \sum_i \underbrace{\left(\sum_j k_{ij} x_j \right)}_{\in F} \underbrace{y_i}_{\text{el. baze}} \Rightarrow$$

$$\sum_j k_{ij} \underbrace{x_j}_{\text{el. baze}} = 0 \quad \forall i$$

$$\Rightarrow k_{ij} = 0 \quad \forall i,j.$$

$$\Rightarrow \dim_K E = m \cdot n \qquad \square$$

Posledica: $\nexists K \ni: \mathbb{R} < K < \mathbb{C}$

strogi