Stupeň rozšíření těles

Je-li R podtělesem tělesa T, pak můžeme aditivní grupu $(T, +)$ chápat jako vektorový prostor nad tělesem R: skalárním násobkem vektoru $t \in T$ skalárem $r \in R$ je součin $r \cdot t$ počítaný v tělese T. Axiomy vektorového prostoru jsou splněny:
pro každé skaláry $r_1, r_2 \in R$ a každé vektory $t_1, t_2 \in T$ platí

- $(r_1 + r_2) \cdot t_1 = r_1 \cdot t_1 + r_2 \cdot t_1$,
- $r_1 \cdot (t_1 + t_2) = r_1 \cdot t_1 + r_1 \cdot t_2$,
- $r_1 \cdot (r_2 \cdot t_1) = (r_1 \cdot r_2) \cdot t_1$,
- $1 \cdot t_1 = t_1$,

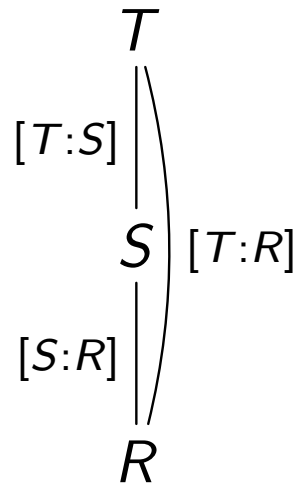
(v T platí distributivní zákony, násobení je asociativní a 1 je jednička). Máme tedy definovánu dimenzi $\dim_R T \in \mathbb{N} \cup \{\infty\}$, zřejmě tato dimenze nemůže být nula.

Definice. Nechť $R \subseteq T$ je rozšířením těles. Jeho stupněm $[T : R]$ rozumíme dimenzi vektorového prostoru T nad tělesem R, tj. $[T : R] = \dim_R T$. Jestliže T není konečněrozměrný vektorový prostor nad R, píšeme $[T : R] = \infty$.

Multiplikativnost stupně rozšíření

Věta. *Nechť $R \subseteq S$, $S \subseteq T$ jsou rozšíření těles. Pak platí*

$$[T : R] = [T : S] \cdot [S : R],$$



kde užíváme konvence $n \cdot \infty = \infty \cdot n = \infty$ pro každé $n \in \mathbb{N} \cup \{\infty\}$.

Důkaz. Je-li $[S : R] = \infty$, pro každé $n \in \mathbb{N}$ v S existuje n lineárně nezávislých prvků nad R, protože $S \subseteq T$, jsou tyto prvky v T a platí $[T : R] = \infty$.

Je-li $[T : S] = \infty$, pro každé $n \in \mathbb{N}$ v T existuje n lineárně nezávislých prvků nad S. Ty jsou lineárně nezávislé i nad R, a proto $[T : R] = \infty$.

Nechť $n = [T : S] \in \mathbb{N}$, $m = [S : R] \in \mathbb{N}$. Nechť $\alpha_1, \ldots, \alpha_n$ je báze T nad S, $\beta_1, \ldots, \beta_m$ báze S nad R. Ukážeme, že $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je bází T nad R. Nechť $\gamma \in T$ je libovolný. Pak existují $\delta_1, \ldots, \delta_n \in S$, že $\gamma = \sum_{i=1}^{n} \delta_i\alpha_i$. Existují tedy $\varepsilon_{ij} \in R$, že $\delta_i = \sum_{j=1}^{m} \varepsilon_{ij}\beta_j$ pro každé i. Dosazením

$$\gamma = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \varepsilon_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j).$$

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je množina generátorů T nad R.

Je-li $\sum_{i=1}^{n} \sum_{j=1}^{m} \varepsilon_{ij}(\alpha_i\beta_j)$ pro nějaké $\varepsilon_{ij} \in R$ nulový vektor, pak z lineární nezávislosti $\alpha_1, \ldots, \alpha_n$ nad S dostaneme, že $\sum_{j=1}^{m} \varepsilon_{ij}\beta_j = 0$ pro každé $i = 1, \ldots, n$ a z lineární nezávislosti $\beta_1, \ldots, \beta_m$ nad R dostaneme, že $\varepsilon_{ij} = 0$ pro každé i, j.

Tedy $\alpha_i\beta_j$ $(1 \leq i \leq n, 1 \leq j \leq m)$ je báze T nad R.

Podokruh generovaný množinou

Připomeňme, že podokruh daného okruhu generovaný danou podmnožinou je definován jako průnik všech podokruhů, které tuto podmnožinu obsahují.

Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ prvek, který je algebraický nad tělesem R. Z algebry víme, že podokruh tělesa T generovaný podmnožinou $R \cup \{c\}$ značíme $R[c]$ a platí

$$R[c] = \{h(c) \mid h(x) \in R[x]\}.$$

Označme $f(x)$ minimální polynom prvku c nad R (je to tedy normovaný polynom s koeficienty z R nejmenšího možného stupně, který má prvek c za kořen).

Pokud libovolný polynom $h(x) \in R[x]$ vydělíme polynomem $f(x)$ se zbytkem, dostaneme polynomy $q(x), r(x) \in R[x]$ takové, že $h(x) = f(x) \cdot q(x) + r(x)$, přičemž $\operatorname{st} r(x) < \operatorname{st} f(x)$. Protože $f(c) = 0$, platí $h(c) = 0 \cdot q(c) + r(c) = r(c)$. Dostali jsme

$$R[c] = \{r(c) \mid r(x) \in R[x], \operatorname{st} r(x) < \operatorname{st} f(x)\}.$$

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ algebraický prvek nad R, $f(x) \in R[x]$ minimální polynom prvku c nad R. Pak podokruh $R[c]$ je podtěleso tělesa T a platí, že $1, c, c^2, \ldots, c^{n-1}$, kde $n = \operatorname{st} f(x)$, je bází vektorového prostoru $R[c]$ nad R, a tedy stupeň rozšíření $[R[c] : R] = \operatorname{st} f(x)$.*

Důkaz. Víme, že $R[c]$ je podokruh tělesa T. Abychom dokázali, že $R[c]$ je dokonce podtěleso tělesa T, musíme dokázat, že s každým svým nenulovým prvkem obsahuje i k němu inverzní prvek (vzhledem k násobení).
Víme, že libovolný nenulový prvek $\alpha \in R[c]$ je tvaru $\alpha = h(c)$, kde $h(x) \in R[x]$, přičemž $f(x) \nmid h(x)$, protože $h(c) = \alpha \neq 0$. Protože $f(x)$ je ireducibilní, tak jsou $f(x)$ a $h(x)$ nesoudělné. Proto jejich největší společný dělitel 1 lze vyjádřit Bezoutovou rovností, tedy existují polynomy $a(x), b(x) \in R[x]$ tak, že platí
$1 = a(x) \cdot f(x) + b(x) \cdot h(x)$. Dosazením c odtud dostaneme

$$1 = a(c) \cdot f(c) + b(c) \cdot h(c) = b(c) \cdot h(c) = b(c) \cdot \alpha$$

Je tedy $b(c) \in R[c]$ inverzní prvek k prvku α v okruhu $R[c]$.

Protože

$$R[c] = \{r(c) \mid r(x) \in R[x], \operatorname{st} r(x) < \operatorname{st} f(x)\},$$

generují prvky $1, c, c^2, \ldots, c^{n-1}$ vektorový prostor $R[c]$ nad tělesem R. Kdyby tyto prvky nebyly lineárně nezávislé nad R, existovaly by prvky $a_0, a_1, \ldots, a_{n-1} \in R$, ne všechny nulové, tak, že

$$a_0 + a_1 \cdot c + a_2 \cdot c^2 + \cdots + a_{n-1} \cdot c^{n-1} = 0.$$

Ale pak by nenulový polynom $a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ měl kořen c a současně by měl stupeň menší než $\operatorname{st} f(x)$, což by byl spor.

Je tedy $1, c, c^2, \ldots, c^{n-1}$ báze vektorového prostoru $R[c]$ nad tělesem R, a proto stupeň rozšíření $[R[c] : R] = n = \operatorname{st} f(x)$.

(Ne)řešitelnost geometrických úloh pravítkem a kružítkem

Z antiky pocházejí tři problémy, jejichž řešení pravítkem a kružítkem nebylo známo:

- *trisekce úhlu* (rozdělit daný úhel na třetiny),
- *zdvojení krychle* (k dané krychli sestrojit krychli dvojnásobného objemu, tj. k úsečce dané délky najít úsečku $\sqrt[3]{2}$-krát delší),
- *kvadratura kruhu* (k danému kruhu sestrojit čtverec o stejném obsahu).

Abychom mohli dokázat, že žádné řešení těchto úloh neexistuje, musíme přesně specifikovat, co to znamená řešit úlohu pravítkem a kružítkem.

Předpokládejme, že v rovině je zadáno konečně mnoho bodů popisujících zadání úlohy. Těmto bodům budeme říkat význačné. Smíme sestrojit libovolnou přímku procházející dvěma význačnými body a libovolnou kružnici, jejímž středem je význačný bod a poloměrem vzdálenost některých dvou význačných bodů. Libovolný průsečík sestrojených kružnic či přímek můžeme přidat k význačným bodům. Jde o to, jestli po konečně mnoha krocích lze docílit toho, že mezi význačnými body je bod, který popisuje řešení dané úlohy.

Zavedeme v této rovině soustavu souřadnic, rovinu tedy ztotožňujeme s kartézským součinem $\mathbb{R} \times \mathbb{R}$. Označme T_0 podtěleso tělesa $\mathbb{R}$ generované x-ovými a y-ovými souřadnicemi všech zadaných bodů. Pokud bylo přidáno celkem n význačných bodů, definujeme tělesa $T_1, \ldots, T_n$ takto: těleso T_i je generováno tělesem T_{i-1} a souřadnicemi i-tého význačného bodu.

Naším cílem je dokážat, že rozšíření těles $T_0 \subseteq T_n$ je konečné a jeho stupeň $[T_n : T_0] \mid 2^n$.

Označme $[x_i, y_i]$ souřadnice i-tého význačného bodu. Tento bod byl získán jako průsečík sestrojených přímek či kružnic, rovnice takové přímky je tvaru $ax + by = c$, kde $a, b, c \in T_{i-1}$, rovnice takové kružnice tvaru $(x - m)^2 + (y - n)^2 = u$, kde $m, n, u \in T_{i-1}$. Proto $[x_i, y_i]$ je řešením soustavy dvou lineárních rovnic anebo soustavy jedné lineární a jedné kvadratické rovnice s koeficienty v T_{i-1} (případ dvou kružnic vede sice na soustavu dvou kvadratických rovnic, jejich odečtením však dostaneme rovnici lineární).

Dosazením z lineární rovnice do druhé rovnice získáme rovnici lineární nebo kvadratickou pro jednu ze souřadnic $[x_i, y_i]$ s koeficienty v T_{i-1}. Minimální polynom získaného řešení nad tělesem T_{i-1} má stupeň 1 nebo 2, druhou ze souřadnic dopočítáme z lineární rovnice. Proto $[T_i : T_{i-1}] \leq 2$.

Z věty o násobení stupňů rozšíření dostáváme $[T_n : T_0] \mid 2^n$.

Neřešitelnost úlohy zdvojení krychle

Jsou dány dva body o souřadnicích $[0,0]$ a $[0,1]$, cílem je získat bod $[0,\sqrt[3]{2}]$.

Je tedy $T_0 = \mathbb{Q}$.

Protože $x^3 - 2$ je minimální polynom čísla $\sqrt[3]{2}$ nad $\mathbb{Q}$, platí $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Jestliže tedy $\sqrt[3]{2} \in T_n$, pak $3 \mid [T_n : T_0]$.

$$\begin{array}{c} T_n \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \\ T_0 = \mathbb{Q} \end{array}$$

To spolu s odvozenou dělitelností $[T_n : T_0] \mid 2^n$ dává spor $3 \mid 2^n$.

Neřešitelnost úlohy trisekce úhlu

Ukážeme, že nemůžeme sestrojit pravítkem a kružítkem úhel $\frac{\pi}{9}$. Vzhledem k tomu, že umíme sestrojit úhel $\frac{\pi}{3}$ jako vnitřní úhel rovnostranného trojúhelníka, bude to znamenat, že nelze rozdělit na třetiny libovolný zadaný úhel.

Jsou dány dva body o souřadnicích $[0,0]$ a $[0,1]$, cílem je získat bod $[\cos\frac{\pi}{9}, \sin\frac{\pi}{9}]$. Opět máme $T_0 = \mathbb{Q}$.

K nalezení minimálního polynomu čísla $\cos\frac{\pi}{9}$ využijeme vzorec $\cos 3\alpha = \cos^3\alpha - 3\cos\alpha\sin^2\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Pro $\alpha = \frac{\pi}{9}$ dostáváme, že $c = 2\cos\frac{\pi}{9}$ je kořenem polynomu $x^3 - 3x - 1$. Tento kubický polynom nemá racionální kořen (± 1 kořen není), a tedy je ireducibilní nad $\mathbb{Q}$.

Odtud $[\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$ a stejně jako v předchozím případě dostáváme spor.

Neřešitelnost úlohy kvadratury kruhu

V tomto případě využijeme toho, že π je transcendentní číslo (tento fakt zde nebudeme dokazovat).

Jsou dány dva body o souřadnicích $[0, 0]$ a $[0, 1]$. Kruh jednotkového poloměru má obsah π. Cílem je získat bod $[0, \sqrt{\pi}]$. Opět máme $T_0 = \mathbb{Q}$.

Předpokládejme, že $\sqrt{\pi} \in T_n$, pak $\pi \in T_n$. Protože T_n je těleso, plyne odtud $1, \pi, \pi^2, \pi^3, \ldots \in T_n$.

Protože π je transcendentní nad $\mathbb{Q}$, tak pro libovolné $m \in \mathbb{N}$ platí, že čísla $1, \pi, \pi^2, \pi^3, \ldots, \pi^m$ jsou lineárně nezávislá nad $\mathbb{Q}$, a tedy konečněrozměrný vektorový prostor T_n nemůže všechna tato čísla obsahovat.