# NOVý TEXT O TěLESOVýCH ROZŠířENÍCH

DAVID STANOVSKÝ

## 1. Algebraické prvky a rozšíření konečného stupně

### 1.1. Rozšíření jako vektorový prostor.

*Rozšířením těles* budeme rozumět libovolnou dvojici těles $\mathbf{T}, \mathbf{S}$ takovou, že $\mathbf{T} \leq \mathbf{S}$. Říkáme, že $\mathbf{T}$ je podtělesem $\mathbf{S}$, nebo že $\mathbf{S}$ je rozšířením $\mathbf{T}$.

Klíčem k pochopení celé kapitoly je myšlenka, že těleso $\mathbf{S}$ lze považovat za vektorový prostor nad tělesem $\mathbf{T}$: sčítání a odčítání ponecháme a místo násobení jakožto operace $S \times S \to S$ uvažujeme pouze restrikci $T \times S \to S$. Neformálně, prvky většího tělesa $\mathbf{S}$ považujeme za vektory, prvky menšího tělesa $\mathbf{T}$ za skaláry a uvažujeme pouze násobení skalár krát vektor. Tento vektorový prostor budeme značit $\mathbf{S_T}$.

Uvědomte si, že jde skutečně o vektorový prostor: aditivní struktura $(S, +, -, 0)$ je abelovskou grupu a pro všechna $a, b \in T$ (skaláry), $v, w \in S$ (vektory) platí každý z axiomů vektorových prostorů: $a(bv) = (ab)v$ plyne z asociativity násobení, $1v = v$ z vlastnosti jednotky a $a(v + w) = av + aw$ a $(a + b)v = av + bv$ z distributivity.

**Definice.** Dimenze vektorového prostoru $\mathbf{S_T}$ se nazývá *stupeň rozšíření* a značí se

$$[\mathbf{S} : \mathbf{T}] = \dim \mathbf{S_T}.$$

Je-li stupeň $[\mathbf{S} : \mathbf{T}]$ konečný, říkáme, že jde o rozšíření *konečného stupně*.

**Příklady.**

- $[\mathbb{C} : \mathbb{R}] = 2$. Každé komplexní číslo lze zapsat právě jedním způsobem jako $a + bi$, $a, b \in \mathbb{R}$, čili prvky $1, i$ tvoří bázi prostoru $\mathbb{C}_\mathbb{R}$.
- Analogicky, pro $s$, které není čtvercem, je stupeň $[\mathbb{Q}(\sqrt{s}) : \mathbb{Q}] = 2$, prvky $1, \sqrt{s}$ tvoří bázi prostoru $\mathbb{Q}(\sqrt{s})_\mathbb{Q}$.
- $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, bázi prostoru $\mathbb{Q}(\sqrt{2}, \sqrt{3})_\mathbb{Q}$ tvoří například prvky $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.
- Pozor, pro $\zeta_3 = e^{2\pi i/3}$ je stupeň $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ a nikoliv 3: prvky $1, \zeta_3, \zeta_3^2$ jsou lineárně závislé, protože $\zeta_3^2 = -1 - \zeta_3$.
- Je-li $u$ transcendentní číslo (např. konstanty $e$ nebo $\pi$), stupeň $[\mathbb{Q}(u) : \mathbb{Q}]$ je nekonečný (spočetný): lineárně nezávislou množinu tvoří třeba prvky $1, u, u^2, \ldots$ (viz Věta 1.5).
- Stupeň $[\mathbb{R} : \mathbb{Q}]$ je dokonce nespočetný: prostory spočetné dimenze nad spočetným tělesem jsou spočetné, zatímco reálných čísel je nespočetně.

Připomeňme pojem prvookruhu. Pro libovolný okruh $\mathbf{R}$ s jednotkou uvažujme zobrazení

$$\mathbb{Z} \to \mathbf{R}, \qquad n \mapsto \underbrace{1 + \ldots + 1}_{n}.$$

*Date*: 3. května 2019.

Je vidět, že jde o homomorfismus, jehož obrazem je tzv. *prvookruh* okruhu $\mathbf{R}$ a jehož jádrem je ideál $n\mathbb{Z}$, kde $n$ je *charakteristika* okruhu $\mathbf{R}$. Použitím 1. věty o izomorfismu dostáváme, že prvookruh libovolného okruhu je izomorfní buď okruhu $\mathbb{Z}$ v případě charakteristiky 0, nebo okruhu $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ v případě charakteristiky $n$.

Nyní uvažujme těleso $\mathbf{T}$. Jeho *prvotělesem* se rozumí nejmenší podtěleso. To v sobě jistě obsahuje prvookruh, ale navíc musí ke každému nenulovému prvku obsahovat jeho inverz. Podle Tvrzení **??** je charakteristika tělesa 0 nebo prvočíslo $p$. V druhém případě je prvookruh již tělesem (izomorfním $\mathbb{Z}_p$), čili pojmy splývají. V případě charakteristiky 0 prvotěleso sestává ze všech zlomků $ab^{-1}$, kde $a, b$ jsou prvky prvookruhu, čili je izomorfní tělesu $\mathbb{Q}$.

Každé těleso je samozřejmě rozšířením svého prvotělesa. Speciálně, pro konečná tělesa dostáváme velmi zajímavý důsledek vektorového pohledu na tělesová rozšíření.

**Tvrzení 1.1.** *Počet prvků konečného tělesa je mocnina prvočísla.*

*Důkaz.* Konečné těleso $\mathbf{T}$ charakteristiky $p$ je rozšířením svého prvotělesa $\mathbf{P} \simeq \mathbb{Z}_p$. Čili vektorový prostor $\mathbf{T}_\mathbf{P}$ je izomorfní prostoru $(\mathbb{Z}_p)^k$, kde $k = [\mathbf{T} : \mathbf{P}]$, čili má $p^k$ prvků. □

1.2. **Minimální polynom a stupeň jednoduchého rozšíření.**

Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$. Řekneme, že prvek $a$ je *algebraický* nad $\mathbf{T}$, pokud existuje nenulový polynom z $\mathbf{T}[x]$, jehož je $a$ kořenem. V opačném případě se prvek $a$ nazývá *transcendentní* nad $\mathbf{T}$. *Minimálním polynomem* prvku $a$ nad $\mathbf{T}$ rozumíme ireduicibilní monický polynom $m_{a,\mathbf{T}}$ z $\mathbf{T}[x]$, jehož je $a$ kořenem.

**Tvrzení 1.2.** *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$ algebraický nad $\mathbf{T}$. Pak*

(1) *minimální polynom $m_{a,\mathbf{T}}$ existuje a je jednoznačně určený;*
(2) *prvek $a$ je kořenem polynomu $f \in T[x]$ právě tehdy, když $m_{a,\mathbf{T}} \mid f$.*

*Důkaz.* Množina $I = \{f \in T[x] : \ f(a) = 0\}$ tvoří ideál v oboru $\mathbf{T}[x]$, a protože je $\mathbf{T}[x]$ oborem hlavních ideálů (Věta **??**), existuje monický polynom $m \in T[x]$ takový, že $I = mT[x]$. Vidíme, že $f(a) = 0$ právě tehdy, když $m \mid f(a)$. Kdyby polynom $m$ nebyl ireducibilní v $\mathbf{T}[x]$, tj. kdyby $m = fg$, kde $f, g \nmid m$, pak $0 = m(a) = f(a)g(a)$, čili prvek $a$ by byl kořenem alespoň jednoho z polynomů $f, g$, ale $m \nmid f, g$, spor. Čili $m$ je minimální polynom prvku $a$ nad $\mathbf{T}$. Pro jakýkoliv jiný monický ireducibilní polynom $\tilde{m} \in T[x]$, jehož je $a$ kořenem, platí $m \mid \tilde{m}$ a z ireducibility a moničnosti dostáváme $\tilde{m} = m$. □

**Příklad.** Je ihned vidět, že

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

neboť jde o ireducibilní polynomy, které mají daný prvek za kořen.

**Příklad.** Pozor, pro $\zeta_3 = e^{2\pi i/3}$ minimální polynom $m_{\zeta_3,\mathbb{Q}}$ není $x^3 - 1$, neboť tento polynom není ireducibilní. Platí $x^3 - 1 = (x-1)(x^2+x+1)$, $\zeta_3$ je kořenem druhého činitele, ten je ireducibilní, a tedy $m_{\zeta_3,\mathbb{Q}} = x^2 + x + 1$.

**Příklad.** Spočteme minimální polynom prvku $a = \sqrt{2} + \sqrt{3}$. Platí

$$a^2 = 5 + 2\sqrt{6}, \quad a^3 = 11\sqrt{2} + 9\sqrt{3}, \quad a^4 = 49 + 20\sqrt{6}$$

a vidíme, že $a^4 = 10a^2 - 1$. Čili $a$ je kořenem polynomu $x^4 - 10x^2 + 1$. Tento polynom je ireducibilní: díky Tvrzení **??** nemá racionální kořen a na součin dvou polynomů stupňů 2 se rozkládat nemůže, neboť $\sqrt{2} + \sqrt{3}$ není řešením žádné kvadratické rovnice.

**Tvrzení 1.3.** *Buď* $\mathbf{T} \leq \mathbf{S}$ *rozšíření těles a* $a \in S$ *algebraický prvek nad* $\mathbf{T}$. *Pak*

$$\mathbf{T}(a) = \mathbf{T}[a].$$

*Důkaz.* Podle Tvrzení **??** je

$$T[a] = \{f(a) : \ f \in T[x]\}.$$

Dokážeme, že tyto prvky tvoří podtěleso. Mějme tedy nějaký prvek $0 \neq f(a) \in T[a]$, hledáme jeho inverz, tedy polynom $g \in T[x]$ takový, že $f(a)g(a) = 1$. Protože $f(a) \neq 0$, polynom $m_{a,\mathbf{T}}$ nedělí $f$. Z ireducibility $m_{a,\mathbf{T}}$ plyne $\mathrm{NSD}(m_{a,\mathbf{T}}, f) = 1$, čili podle Bézoutovy rovnosti existují polynomy $u, g \in T[x]$ takové, že $1 = um_{a,\mathbf{T}} + gf$. Dosazením prvku $a$ dostáváme

$$1 = u(a)m_{a,\mathbf{T}}(a) + g(a)f(a) = u(a) \cdot 0 + g(a)f(a) = f(a)g(a),$$

čili $g(a)$ je inverzní prvek k $f(a)$. □

**Příklad.** Číslo $\sqrt{s}$, $s \in \mathbb{Z}$, je algebraické nad $\mathbb{Q}$, tedy $\mathbb{Q}(\sqrt{s}) = \mathbb{Q}[\sqrt{s}]$. A skutečně,

$$(a + b\sqrt{s})^{-1} = \frac{a}{a^2 - b^2 s} - \frac{b}{a^2 - b^2 s}\sqrt{s} \in \mathbb{Q}[\sqrt{s}].$$

Pro rozšíření vyšších stupňů vycházejí vzorce ošklivě (zkuste si to!) a Tvrzení 1.3 má svoji cenu.

**Poznámka.** Je-li $a$ transcendentní prvek nad $\mathbf{T}$, pak $\mathbf{T}[a] \neq \mathbf{T}(a)$. Kdyby $\frac{1}{a} \in \mathbf{T}[a]$, pak by existoval polynom $f \in \mathbf{T}[x]$ takový, že $f(a) = a^{-1}$, čili $af(a) = 1$, a tedy $a$ by bylo kořenem polynomu $xf - 1 \in T[x]$, spor.

**Tvrzení 1.4.** *Buď* $\mathbf{T} \leq \mathbf{S}$ *rozšíření těles a* $a \in S$ *algebraický prvek nad* $\mathbf{T}$. *Pak*

$$[\mathbf{T}(a) : \mathbf{T}] = \deg m_{a,\mathbf{T}}.$$

*Důkaz.* Označme $n = \deg m_{a,\mathbf{T}}$. Dokážeme, že prvky $1, a, a^2, \ldots, a^{n-1}$ tvoří bázi vektorového prostoru $\mathbf{T}(a)_{\mathbf{T}}$, a tedy že jeho dimenze je $n$.

Kdyby byly prvky $1, a, a^2, \ldots, a^{n-1}$ lineárně závislé, pak by platilo $\sum_{i=0}^{n-1} t_i a^i = 0$ pro nějaká $t_i \in T$, z nichž by aspoň jedno bylo nenulové. Prvek $a$ by tedy byl kořenem (nenulového) polynomu $\sum_{i=0}^{n-1} t_i x^i \in T[x]$ s menším stupněm než $m_{a,\mathbf{T}}$, což by byl spor s minimalitou.

Nyní dokážeme, že prvky $1, a, a^2, \ldots, a^{n-1}$ generují vektorový prostor $\mathbf{T}(a)_{\mathbf{T}}$. Uvažujme prvek $f(a)$ tělesa $\mathbf{T}(a) = \mathbf{T}[a]$, vyjádříme jej jako lineární kombinaci. Buď $q, r \in T[x]$ takové, že $f = q \cdot m_{a,\mathbf{T}} + r$ a $\deg r < \deg m_{a,\mathbf{T}} = n$. Pak

$$f(a) = q(a) \cdot m_{a,\mathbf{T}}(a) + r(a) = q(a) \cdot 0 + r(a) = r(a),$$

a protože je stupeň $r$ menší než $n$, máme $f(a) = r(a) = \sum_{i=0}^{n-1} t_i a^i$, kde $t_i \in T$ jsou koeficienty polynomu $r$. □

**Příklad.** Pomocí Tvrzení 1.4 lze určit stupeň jednoduchého rozšíření.

- $[\mathbb{C} : \mathbb{R}] = [\mathbb{R}(i) : \mathbb{R}] = \deg m_{i,\mathbb{R}} = \deg(x^2 + 1) = 2$.
- $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \deg(x^n - p) = n$ pro libovolné $n \in \mathbb{N}$ a prvočíslo $p$, protože uvedený polynom je podle Eisensteinova kritéria ireducibilní. (Pokud $p$ není prvočíslo, situace je složitější.)
- $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$ (hodnota Eulerovy funkce), což ale není snadné dokázat, používá se k tomu teorie cyklotomických polynomů. Je-li $n$ prvočíslo, minimálním polynomem je $x^{n-1} + x^{n-2} + \ldots + 1 = \frac{x^n - 1}{x - 1}$, jehož ireducibilitu lze po substituci ukázat z Eisensteinova kritéria.

**Důsledek 1.5.** *Buď* $\mathbf{T} \leq \mathbf{S}$ *rozšíření těles a* $a \in S$*. Prvek* $a$ *je algebraický nad* $\mathbf{T}$ *právě tehdy, když je stupeň* $[\mathbf{T}(a) : \mathbf{T}]$ *konečný.*

*Důkaz.* Je-li $a$ transcendentní, pak $1, a, a^2, \dots$ tvoří nekonečnou lineárně nezávislou množinu: kdyby $\sum_{i=0}^{n} t_i a^i = 0$ pro nějaké koeficienty $t_i \in T$, aspoň jeden nenulový, bylo by $a$ kořenem nenulového polynomu $\sum_{i=0}^{n} t_i x^i$ z $\mathbf{T}[x]$, spor. Opačná implikace plyne z Tvrzení 1.4. □

1.3. **Vícenásobná rozšíření.**

K výpočtu stupně vícenásobného rozšíření slouží následující obecné pravidlo. (Platí i pro nekonečné stupně, viz poznámka nad Větou **??**.)

**Tvrzení 1.6.** *Buď* $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ *rozšíření těles. Pak*

$$[\mathbf{U} : \mathbf{T}] = [\mathbf{U} : \mathbf{S}] \cdot [\mathbf{S} : \mathbf{T}].$$

*Důkaz.* Zvolme bázi $A$ vektorového prostoru $\mathbf{S_T}$ a bázi $B$ vektorového prostoru $\mathbf{U_S}$. Dokážeme, že

$$C = \{ab : \ a \in A, \ b \in B\}$$

je bází vektorového prostoru $\mathbf{U_T}$. Z toho ihned plyne, že

$$[\mathbf{U} : \mathbf{T}] = |C| = |A \times B| = |A| \cdot |B| = [\mathbf{S} : \mathbf{T}] \cdot [\mathbf{U} : \mathbf{S}].$$

Nejprve dokážeme, že $C$ generuje prostor $\mathbf{U_T}$. Je-li $u \in U$, pak $u = \sum_j s_j b_j$ pro nějaká $s_j \in S$ a $b_j \in B$. Každé $s_j$ lze napsat jako $s_j = \sum_i t_{ij} a_i$ pro nějaká $t_{ij} \in T$ a $a_i \in A$, a dosazením druhé rovnosti do první dostaneme

$$u = \sum_j \big( \sum_i t_{ij} a_i \big) b_j = \sum_{i,j} t_{ij} \cdot a_i b_j.$$

Tedy $u$ je lineární kombinací prvků $C$ s koeficienty z tělesa $\mathbf{T}$.

Nyní dokážeme lineární nezávislost. Předpokládejme, že $\sum_{i,j} t_{ij} \cdot a_i b_j = 0$ pro nějaká $t_{ij} \in T$ a $a_i b_j \in C$. Rozepíšeme

$$0 = \sum_{i,j} t_{ij} a_i b_j = \sum_j \underbrace{\big( \sum_i t_{ij} a_i \big)}_{\in S} b_j.$$

Lineární nezávislost prvků $b_j$ nad tělesem $\mathbf{S}$ nám dává $\sum_i t_{ij} a_i = 0$ pro každé $j$ a z lineární nezávislosti prvků $a_i$ nad tělesem $\mathbf{T}$ dostáváme $t_{ij} = 0$ pro všechna $i, j$. □

Tvrzení 1.4 a 1.6 můžeme aplikovat na výpočet stupně vícenásobných rozšíření typu $\mathbf{T}(a_1, a_2, \dots)$. Dvojité rozšíření $\mathbf{T} \leq \mathbf{T}(a, b)$ můžeme rozbít na dvě jednoduchá rozšíření $\mathbf{T} \leq \mathbf{T}(a) \leq \mathbf{T}(a, b)$ a spočteme

$$\begin{aligned}[\mathbf{T}(a, b) : \mathbf{T}] = [\mathbf{T}(a, b) : \mathbf{T}(a)] \cdot [\mathbf{T}(a) : \mathbf{T}] &= \deg m_{b,\mathbf{T}(a)} \cdot \deg m_{a,\mathbf{T}} \\ &\leq \deg m_{b,\mathbf{T}} \cdot \deg m_{a,\mathbf{T}}.\end{aligned}$$

Pozor, při vyjádření stupně $[\mathbf{T}(a, b) : \mathbf{T}(a)]$ musíme použít minimální polynom prvku $b$ nad tělesem $\mathbf{T}(a)$, který může být menšího stupně, než minimální polynom nad tělesem $\mathbf{T}$. Vícenásobným použitím popsaného postupu snadno dokážeme následující důsledek.

**Důsledek 1.7.** *Buď* $\mathbf{T} \leq \mathbf{S}$ *rozšíření těles a* $a_1, \dots, a_n \in S$ *prvky algebraické nad* $\mathbf{T}$*. Pak* $\mathbf{T}(a_1, \dots, a_n)$ *je rozšířením konečného stupně nad* $\mathbf{T}$*.*

**Příklad.** Pomocí výpočtu dimenze předvedeme, že

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Zřejmě $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \leq \mathbb{Q}(\sqrt{2},\sqrt{3})$. Pokud tedy dokážeme, že oba prostory mají stejnou dimenzi, musí být totožné. Spočteme minimální polynomy:

- $m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1$;
- $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$;
- $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})} = x^2 - 3$ (ověřte, že je opravdu ireducibilní v $\mathbb{Q}(\sqrt{2})[x]$ !).

Podle Tvrzení 1.4 a 1.6 dostáváme $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$ a $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

Je-li $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a každý prvek tělesa $\mathbf{S}$ je algebraický nad $\mathbf{T}$, hovoříme o *algebraickém rozšíření*. Tuto vlastnost mají všechna rozšíření konečného stupně.

**Tvrzení 1.8.** *Rozšíření konečného stupně jsou algebraická.*

*Důkaz.* Označme $n = [\mathbf{S} : \mathbf{T}]$. Pro libovolný prvek $a \in S$ dokážeme, že je algebraický nad $\mathbf{T}$. Prvky $1, a, a^2, \ldots, a^{n-1}, a^n$ jsou lineárně závislé, protože jich je více než je dimenze vektorového prostoru $\mathbf{S_T}$. Tedy existují koeficienty $t_i \in T$, aspoň jeden z nich nenulový, kterými lze lineárně nakombinovat nulu, tj. $\sum_{i=0}^{n} t_i a^i = 0$. Čili prvek $a$ je kořenem nenulového polynomu $\sum_{i=0}^{n} t_i x^i \in T[x]$. □

Tvrzení 1.8 je principem nekonstruktivních důkazů algebraičnosti: k důkazu, že je prvek $a$ algebraický nad $\mathbf{T}$, stačí najít rozšíření $\mathbf{S} \geq \mathbf{T}$ konečného stupně, v němž $a$ leží. Typickým příkladem je důkaz, že součet, rozdíl, součin a podíl algebraických prvků je algebraický prvek.

**Věta 1.9.** *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. Prvky $\mathbf{S}$, které jsou algebraické nad $\mathbf{T}$, tvoří podtěleso tělesa $\mathbf{S}$.*

*Důkaz.* Uvažujme prvky $a, b \in S$ algebraické nad $\mathbf{T}$. Rozšíření $\mathbf{T} \leq \mathbf{T}(a,b)$ je konečného stupně (Důsledek 1.7), a tedy algebraické (Tvrzení 1.8). Čili všechny prvky $\mathbf{T}(a,b)$ jsou algebraické nad $\mathbf{T}$, speciálně také prvky $a+b$, $a \cdot b$, $-a$ i $a^{-1}$ (pro $a \neq 0$). Tedy algebraické prvky tvoří podtěleso tělesa $\mathbf{S}$. □

## 2. Konstrukce pravítkem a kružítkem

… úvod VIZ SKRIPTA, sekce 26.

Předně musíme upřesnit, co vlastně rozumíme konstrukcí pomocí pravítka a kružítka. Na začátku je daná jistá konečná množina $\mathcal{M}_0$ bodů v rovině. Z ní můžeme zkonstruovat nový bod jako průsečík přímek nebo kružnic určených již zkonstruovanými body; a tento postup lze několikrát opakovat. Formálně, konstrukce pomocí pravítka a kružítka je posloupnost $\mathcal{M}_0 \subseteq \mathcal{M}_1 \subseteq \ldots \subseteq \mathcal{M}_n$ konečných množin bodů v rovině taková, že $\mathcal{M}_{i+1} = \mathcal{M}_i \cup \{X\}$, kde $X$ vznikne jako

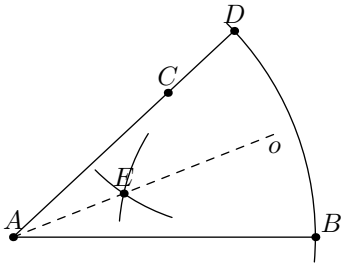
(1) průsečík přímky $AB$ a přímky $CD$;
(2) průsečík přímky $AB$ a kružnice $k(C, |DE|)$ se středem $C$ a poloměrem $|DE|$;
(3) průsečík kružnic $k(A, |BC|)$ a $k(D, |EF|)$

pro nějaké body $A, B, C, D, E, F \in \mathcal{M}_i$.

Princip Wantzelovy metody je převedení konstrukcí pravítkem a kružítkem do jazyka algebry. Zvolme v rovině souřadnice a uvažujme nejmenší těleso $\mathbf{T}_i \leq \mathbb{R}$, které obsahuje $x$-ové i $y$-ové souřadnice všech bodů z $\mathcal{M}_i$. Čili, pokud $\mathcal{M}_i$ obsahuje body

$A_1, \ldots, A_k$ se souřadnicemi $(a_1, b_1), \ldots, (a_k, b_k)$, pak $\mathbf{T}_i = \mathbb{Q}(a_1, b_1, \ldots, a_k, b_k)$. Přidáním bodu $X$ se souřadnicemi $(u, v)$ dostaneme $\mathbf{T}_{i+1} = \mathbf{T}_i(u, v)$. Výsledkem je řetězec rozšíření těles $\mathbf{T}_0 \leq \mathbf{T}_1 \leq \mathbf{T}_2 \leq \ldots \leq \mathbf{T}_n$.

**Příklad** (Půlení úhlu)**.** Podívejme se, jak se formalizuje úloha k danému úhlu sestrojit poloviční úhel. Mějme dán úhel třemi body $A, B, C$ (kde $A$ je vrchol).




Sestrojíme body

$$D = k(A, |AB|) \cap AC \quad \text{a} \quad E = k(B, |BD|) \cap k(D, |BD|),$$

výsledkem bude úhel daný body $A, B, E$. Tedy

$$\mathcal{M}_0 = \{A, B, C\}, \quad \mathcal{M}_1 = \mathcal{M}_0 \cup \{D\}, \quad \mathcal{M}_2 = \mathcal{M}_1 \cup \{E\}.$$

Zvolme souřadnice tak, že $A = (0, 0)$, $B = (1, 0)$ a $C = (a, b)$. Není těžké spočítat, že $D = (\frac{a}{\sqrt{a^2+b^2}}, \frac{b}{\sqrt{a^2+b^2}})$ a $E = (\frac{1}{2} + \frac{a-b\sqrt{3}}{2\sqrt{a^2+b^2}}, \frac{\sqrt{3}}{2} + \frac{b+a\sqrt{3}}{2\sqrt{a^2+b^2}})$, tedy

$$\mathbf{T}_0 = \mathbb{Q}(a, b), \quad \mathbf{T}_1 = \mathbf{T}_0(\sqrt{a^2 + b^2}), \quad \mathbf{T}_2 = \mathbf{T}_0(\sqrt{a^2 + b^2}, \sqrt{3}).$$

Stěžejním krokem Wantzelovy metody je následující vlastnost.

**Tvrzení 2.1.** $[\mathbf{T}_n : \mathbf{T}_0]$ *je mocnina čísla 2.*

*Důkaz.* Podle Tvrzení **??** je

$$[\mathbf{T}_n : \mathbf{T}_0] = [\mathbf{T}_n : \mathbf{T}_{n-1}] \cdot \ldots \cdot [\mathbf{T}_2 : \mathbf{T}_1] \cdot [\mathbf{T}_1 : \mathbf{T}_0].$$

Ukážeme, že

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] \in \{1, 2\}.$$

Probereme postupně všechny tři možnosti, jak se konstruuje nový bod.

(1) Jde-li o průsečík dvou různoběžných přímek, získáme souřadnice nového bodu řešením soustavy dvou lineárních rovnic o dvou neznámých nad tělesem $\mathbf{T}_i$. Konkrétně, přímka určená body $A, B$ se souřadnicemi $(a, b)$, $(c, d)$, kde $a, b, c, d \in T_i$, má rovnici

$$(b - d)x + (c - a)y = bc - ad$$

a vidíme, že všechny tři koeficienty jsou v tělese $\mathbf{T}_i$. Řešením soustavy lineárních rovnic dvou proměnných nad tělesem $\mathbf{T}_i$ je dvojice $(u, v)$ prvků tělesa $\mathbf{T}_i$, takže $\mathbf{T}_{i+1} = \mathbf{T}_i(u, v) = \mathbf{T}_i$ a

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] = 1.$$

(2) Jde-li o průsečík přímky a kružnice, získáme souřadnice nového bodu řešením soustavy jedné lineární a jedné kvadratické rovnice o dvou neznámých nad tělesem $\mathbf{T}_i$. Přímku jsme si rozebrali výše, a kružnice $k(A, |BC|)$ určená body $A, B, C$ se souřadnicemi $(a, b)$, $(c, d)$, $(e, f)$, kde $a, b, c, d, e, f \in T_i$, má rovnici

$$(x - a)^2 + (y - b)^2 = (c - e)^2 + (d - f)^2$$

a vidíme, že všechny koeficienty jsou v tělese $\mathbf{T}_i$. Vyjádříme-li z rovnice přímky $y$ a dosadíme jej do kvadratické, dostaneme kvadratickou rovnici pro $x$, jejíž koeficienty jsou z $\mathbf{T}_i$ a řešením je $x = u + v\sqrt{s}$ pro nějaká $u, v, s \in T_i$. Dosazením do lineární rovnice zjistíme, že $y = u' + v'\sqrt{s}$ pro nějaká $u', v' \in T_i$. Čili $\mathbf{T}_{i+1} = \mathbf{T}_i(u, v) = \mathbf{T}_i(\sqrt{s})$, z čehož plyne, že

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] \in \{1, 2\}$$

v závislosti na tom, zda je $\sqrt{s} \in T_i$ nebo ne. (Proveďte popsaný výpočet podrobně a ověřte, že skutečně obě řešení náleží $\mathbf{T}_i(\sqrt{s})$ !)

(3) Jde-li o průsečík dvou kružnic, získáme souřadnice nového bodu řešením soustavy dvou kvadratických rovnic o dvou neznámých nad tělesem $\mathbf{T}_i$. Odečtením rovnic od sebe se zbavíme se kvadratických členů (všechny mají koeficient 1) a získáme tak ekvivalentní soustavu sestávající z jedné lineární a jedné kvadratické rovnice, vše nad tělesem $\mathbf{T}_i$. Stejným argumentem jako v (2) dostaneme

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] \in \{1, 2\}.$$

(Proveďte popsaný výpočet podrobně sami!) □

... PŘÍKLADY VIZ SKRIPTA, sekce 26.