NOVý TEXT O TěLESOVýCH ROZŠířENÍCH

DAVID STANOVSKÝ

1. Algebraické prvky a rozšíření konečného stupně

1.1. **Rozšíření jako vektorový prostor.** Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles. 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 jako operace $S \times S \to S$ uvažujeme pouze restrikci $T \times S \to S$, tj. násobíme prvky většího tělesa $\mathbf{S}$ (vektory) pouze prvky menšího tělesa $\mathbf{T}$ (skaláry). Tento vektorový prostor budeme značit $\mathbf{S_T} = (S, +, -, 0, a\cdot : a \in T)$. Uvědomte si, že jde skutečně o vektorový prostor: sčítání tvoří abelovskou grupu a pro $a, b \in T$ (skaláry), $v, w \in S$ (vektory) platí každý z axiomů: $a(bv) = (ab)v$ plyne z asociativity násobení, $1v = v$ z vlastnosti jednotky a $a(v + w) = av + aw$ a $(a + b)v = av + bv$ z distributivity.

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 jednoznačným 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 $[\mathbb{Q}(\sqrt{s}) : \mathbb{Q}] = 2$, 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 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.
- Buď $\omega = e^{2\pi i/3}$. Pozor, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ a nikoliv 3: prvky $1, \omega, \omega^2$ jsou lineárně závislé, protože $\omega^2 = -1 - \omega$. Bázi tvoří prvky $1, \omega$.
- Je-li u transcendentní číslo, např. $u = e$ nebo $u = \pi$, pak $[\mathbb{Q}(u) : \mathbb{Q}] = \infty$ (viz Věta 1.1).
- $[\mathbb{R} : \mathbb{Q}] = \infty$, stupeň je dokonce nespočetný.

1.2. **Algebraická a transcendentní čísla.**

... definice a počítání VIZ SKRIPTA sekce 10.2 ...

V dalším textu se budeme věnovat algebraickému pohledu na tuto problemtaiku, který dává mnohem více informace, než počítací argument. Dalším cílem bude dokázat následující větu, která dává do souvislosti algebraičnost prvku a stupeň rozšíření.

Věta 1.1. *Číslo a je algebraické právě tehdy, když je rozšíření $\mathbb{Q} \leq \mathbb{Q}(a)$ konečného stupně. Pokud jsou tyto podmínky splněny, pak*

$$[\mathbb{Q}(a) : \mathbb{Q}] = \deg m,$$

Date: 22. února 2018.

kde m je ireducibilní celočíselný polynom takový, že $m(a) = 0$.

Důkaz Věty 1.1. Je-li a transcendentní, pak $1, a, a^2, \dots$ tvoří nekonečnou lineárně nezávislou množinu: kdyby existovala netriviální lineární kombinace $\sum_{i=0}^{n} b_i a^i = 0$, $b_i \in \mathbb{Q}$, ne všechny nulové, pak by prvek a byl kořenem nenulového polynomu $\sum_{i=0}^{n} b_i x^i \in \mathbb{Q}[x]$, a po vynásobení nejmenším společným násobkem jmenovatelů v koeficientech též kořenem nenulového celočíselného polynomu, spor.

Opačná implikace a vztah stupňů plyne z Tvrzení 1.2 a 1.4, které dokážeme v další části. □

Polynom m z Věty 1.1 se nazývá *minimální polynom* prvku a. V další části jej budeme diskutovat podrobně, v obecnějším kontextu libovolných tělesových rozšíření (mj. si dokážeme, že opravdu existuje). Abychom mohli používat tělesová rozšíření, místo celých čísel budeme pracovat s racionálními, resp. s obecnými tělesy. Všimněte si, že číslo a kořenem racionálního polynomu právě tehdy, když je kořenem celočíselného polynomu, viz trik v předchozím důkazu.

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

V této části se budeme zabývat tzv. *jednoduchými rozšířeními*, tj. rozšířeními o jediný prvek.

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 algebraického prvku a nad $\mathbf{T}$ rozumíme monický polynom $m_{a,\mathbf{T}} \in T[x]$ splňující

(1) $m_{a,\mathbf{T}}(a) = 0$;
(2) kdykoliv je a kořenem polynomu $f \in T[x]$, pak $m_{a,\mathbf{T}} \mid f$.

Tvrzení 1.2. *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$ algebraický nad $\mathbf{T}$. Pak existuje minimální polynom $m_{a,T}$ a je v $\mathbf{T}[x]$ ireducibilní. Je-li $m \in T[x]$ ireducibilní monický polynom, jehož je a kořenem, pak $m = m_{a,T}$.*

Důkaz. Buď $m \in T[x]$, nenulový polynom nejmenšího stupně splňující $m(a) = 0$. Uvažujme jiný polynom $f \in T[x]$ splňující $f(a) = 0$. Napišme rovnici pro podíl a zbytek: $f = mq + r$, kde $q, r \in T[x]$ a $\deg(r) < \deg(m)$. Pak $0 = f(a) = m(a)q(a) + r(a) = r(a)$, čili a je kořen r, ale ten má menší stupeň, čili jediná možnost je $r = 0$, a tedy $m \mid f$.

Kdyby se polynom $m_{a,\mathbf{T}}$ rozkládal na součin $f \cdot g$, pak by byl prvek a kořenem f nebo g, což by bylo ve sporu s minimalitou. Naopak, je-li a kořen monického ireducibilního polynomu $m \in T[x]$, pak $m_{a,\mathbf{T}} \mid m$, a z ireducibility a monicity plyne $m = m_{a,\mathbf{T}}$. □

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

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 $\mathbb{Q}(\sqrt{s}) = \mathbb{Q}[\sqrt{s}]$. Skutečně,

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

Poznámka. Buď 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 $\sum_{i=0}^{n-1} b_i a^i = 0$ pro nějaká $b_i \in T$, z nichž by aspoň jedno bylo nenulové. Prvek a by tedy byl kořenem (nenulového) polynomu $\sum_{i=0}^{n-1} b_i x^i \in T[x]$ s menším stupněm než $m_{a,\mathbf{T}}$, což by byl spor s minimalitou $m_{a,\mathbf{T}}$.

Nyní dokážeme, že prvky $1, a, \ldots, a^{n-1}$ 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 $f(a) = r(a) = \sum_{i=0}^{n-1} b_i a^i$, kde $b_i \in T$ 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, minilmálním polynomem je $x^{n-1} + x^{m-2} + \ldots + x + 1$, jehož ireducibilitu lze po substitutci ukázat z Eisensteinova kritéria.

1.4. **Vícenásobná rozšíření.**

K výpočtu stupně rozšíření o více prvků se hodí následující obecné pravidlo.

Tvrzení 1.5. *Buď* $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ *rozšíření těles. Pak*

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

Abychom zjednodušili zápis, důkaz tvrzení provedeme pouze pro případ, kdy jde o rozšíření konečného stupně. V nekonečném případě lze postupovat analogicky a čtenář zběhlý v práci s prostory nekonečné dimenze si důkaz snadno sám upraví (v dalším textu nebudeme nekonečná rozšíření potřebovat).

Důkaz. Označme $m = [\mathbf{U} : \mathbf{S}]$, $n = [\mathbf{S} : \mathbf{T}]$ a zvolme bázi $a_1, \ldots, a_n$ vektorového prostoru $\mathbf{S_T}$ a bázi $b_1, \ldots, b_m$ vektorového prostoru $\mathbf{U_S}$. Dokážeme, že prvky

$$a_1b_1, \ldots, a_1b_m,\ a_2b_1, \ldots, a_2b_m,\ \ldots,\ a_nb_1, \ldots, a_nb_m$$

tvoří bázi vektorového prostoru $\mathbf{U_T}$.

Nejprve dokážeme, že tyto prvky generují $\mathbf{U_T}$. Je-li $u \in U$, pak $u = \sum_i s_i b_i$ pro nějaká $s_i \in S$. Každé s_i lze napsat jako $s_i = \sum_j t_{ij} a_j$ pro nějaká $t_{ij} \in T$ a dosazením druhé rovnosti do první dostáváme

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

Tedy u je lineární kombinací uvedených prvků 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 $t_{ij} \in T$. 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 $b_1, \ldots, b_m$ nad tělesem $\mathbf{S}$ nám dává $\sum_i t_{ij} a_i = 0$ pro každé j a z lineární nezávislosti $a_1, \ldots, a_n$ nad tělesem $\mathbf{T}$ dostáváme $t_{ij} = 0$ pro všechna i, j. □

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

2. Konstrukce pravítkem a kružítkem

... úvod VIZ SKRIPTA, sekce 26.

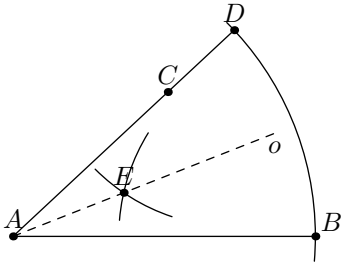
Předně musíme upřesnit, co vlastně rozumíme konstrukcí pomocí pravítka a kružítka. Na začátku je daná jistá konečná množina $\mathcal{M}_0$ bodů v rovině. Z ní můžeme zkonstruovat nový bod jako průsečík přímek nebo kružnic určených již zkonstruovanými body; a tento postup lze několikrát opakovat. Formálně, 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 1.5 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.