Těleso racionálních funkcí

Poznámka. V minulém semestru jsme libovolnému oboru integrity sestrojili podílové těleso. Pro libovolné těleso R je okruh polynomů $R[x]$ oborem integrity, máme tedy podílové těleso i pro něj.

Definice. Nechť R je libovolné těleso. Podílové těleso oboru integrity $R[x]$ nazýváme těleso racionálních funkcí nad tělesem R, značíme jej $R(x)$.

Libovolný prvek tělesa racionálních funkcí je tedy zlomek, který má ve jmenovateli i čitateli polynomy s koeficienty z tělesa R, tedy

$$R(x) = \left\{ \frac{f}{g};\ f, g \in R[x],\ g \neq 0 \right\}.$$

Operace sčítání a násobení jsou v $R(x)$ definovány tak, jak jsme zvyklí pracovat se zlomky. Přitom okruh polynomů $R[x]$ je podokruhem tělesa $R(x)$, neboť libovolný polynom f je ztotožněn se zlomkem $\frac{f}{1}$.

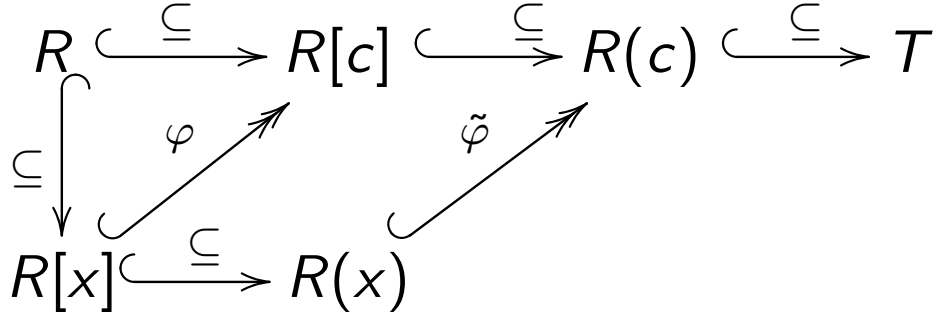
Těleso $R(c)$ pro prvek c, který je transcendentní nad R

Věta. *Nechť $R \subseteq T$ je rozšířením těles, $c \in T$ transcendentní prvek nad R. Pak platí*

1. $R[c] \subsetneq R(c)$ *v* T,
2. $R[c] \cong R[x]$, $R(c) \cong R(x)$,
3. *stupeň rozšíření* $[R(c) : R] = \infty$.

Důkaz. Zobrazení φ přiřazující každému polynomu $h \in R[x]$ jeho hodnotu v c, tj. $\varphi(h) = h(c)$, je homomorfismus okruhů $\varphi : R[x] \to T$, obrazem je $\varphi(R[x]) = \{h(c);\ h \in R[x]\} = R[c]$. Protože c je transcendentní nad R, je $\ker \varphi = \{0\}$ a φ je injekce.

Tedy $R[x] \cong R[c]$.



Homomorfismus φ lze rozšířit na injektivní homomorfismus $\tilde{\varphi} : R(x) \to T$ předpisem $\tilde{\varphi}\left(\frac{h}{g}\right) = h(c)g(c)^{-1}$, obrazem je podtěleso $R(c)$ tělesa T. Zřejmě je $\dim_R R[x] = \infty$, a proto $[R(c) : R] = \infty$.

Jednoduchá, konečná a algebraická rozšíření

Definice. Nechť $R \subseteq T$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, existuje-li prvek $c \in T$, který je algebraický nad R, takový, že $T = R(c)$;
- *konečné*, je-li stupeň $[T : R] < \infty$;
- *algebraické*, je-li každý prvek $c \in T$ algebraický nad R.

Věta. Každé jednoduché rozšíření těles je konečné.

Důkaz. Je-li $T = R(c)$ pro $c \in T$, který je algebraický nad R, pak víme, že $[T : R] = [R(c) : R] = \operatorname{st} f$, kde $f \in R[x]$ je minimální polynom prvku c nad R.

Poznámka. Pro tělesa charakteristiky nula platí i opačná implikace, tuto větu však budeme dokazovat až v předmětu Galoisova teorie: *Každé konečné rozšíření těles charakteristiky nula je jednoduché.*

Jednoduchá, konečná a algebraická rozšíření

Věta. *Každé konečné rozšíření těles je algebraické.*

Důkaz. Nechť $R \subseteq T$ je konečné rozšíření těles, pak stupeň $[T : R] = m$ je přirozené číslo.

Pro libovolný prvek $c \in T$ jsou prvky $1, c, c^2, \ldots, c^m$ lineárně závislé nad R, neboť je jich více než $\dim_R T = m$.

Existují tedy $r_0, r_1, \ldots, r_m \in R$, ne všechny nulové, tak, že $r_0 \cdot 1 + r_1 \cdot c + r_2 \cdot c^2 + \cdots + r_m \cdot c^m = 0$.

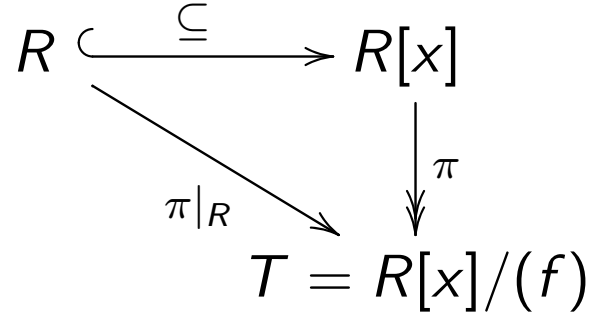
Proto je c kořenem nenulového polynomu $r = r_m x^m + \cdots + r_1 x + r_0 \in R[x]$, a tedy c je algebraický nad R.

Důsledek. *Nechť $R \subseteq T$ je rozšíření těles. Jestliže těleso T obsahuje prvek transcendentní nad R, pak $[T : R] = \infty$.*

Konstrukce jednoduchého rozšíření

Věta. *Nechť R je těleso, $f \in R[x]$ normovaný ireducibilní polynom. Pak $R[x]/(f)$ je těleso, které je jednoduché rozšíření tělesa R. Přesněji: ztotožníme libovolný prvek $r \in R$ s třídou $r + (f)$ obsahující konstantní polynom r a označíme $c = x + (f)$ třídu obsahující polynom x, pak $R[x]/(f) = R(c)$ a f je minimální polynom prvku c nad R.*

Důkaz. Protože f je ireducibilní polynom nad tělesem R, hlavní ideál $(f) \subseteq R[x]$ je maximálním ideálem okruhu polynomů $R[x]$. Protože $R[x]$ je komutativní okruh, je faktorokruh $T = R[x]/(f)$ těleso.



Protože $\pi|_R : R \to T$ je homomorfismus okruhů mezi tělesy, je injektivní. Proto můžeme ztotožnit libovolný prvek $r \in R$ s jeho obrazem $r + (f)$ v T. Po tomto ztotožnění je R podtělesem tělesa T, máme tedy rozšíření těles $R \subseteq T$.

Označme $c = x + (f)$ třídu obsahující lineární polynom x. Pak pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= (g_m + (f))(x + (f))^m + \cdots + (g_1 + (f))(x + (f)) + (g_0 + (f)) = \\ &= (g_m x^m + \cdots + g_1 x + g_0) + (f) = g + (f). \end{aligned}$$

Odtud $T = R(c)$. Speciálně $f(c) = f + (f) = 0 + (f) = 0$, a tedy c je kořenem polynomu f. Protože f je normovaný a ireducibilní nad R, je f minimálním polynomem prvku c.

Poznámka. Je-li $\operatorname{st} f > 1$, nemá polynom f v tělese R žádný kořen. Konstrukcí z předchozí věty jsme těleso R „rozšířili“ na těleso $R(c)$, přičemž minimální polynom prvku c je právě f. Porovnáním s důkazem věty o minimálním polynomu vidíme, že takové rozšíření je jediné až na izomorfismus, je totiž izomorfní s faktorokruhem $R[x]/(f)$.

Rozkladové těleso polynomu

Věta. *Nechť R je těleso a $f \in R[x]$ nekonstantní polynom. Pak existuje rozšíření T tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.*

Důkaz. Větu dokážeme indukcí vzhledem ke $\operatorname{st} f$.

Je-li $\operatorname{st} f = 1$, stačí vzít $T = R$.

Nechť tedy $\operatorname{st} f > 1$ a věta byla dokázána pro všechny nekonstantní polynomy stupně menšího než $\operatorname{st} f$ nad libovolným tělesem (tj. nejen nad naším R). Rozložme polynom f v $R[x]$ na součin ireducibilních činitelů (to lze, neboť R je těleso)

$$f = a \cdot g_1 \cdots g_k,$$

kde a je vedoucí koeficient polynomu f a $g_1, \ldots, g_k \in R[x]$ jsou normované ireducibilní polynomy. Pak podle předchozí věty je $K = R[x]/(g_1)$ rozšíření tělesa R, ve kterém má polynom g_1 kořen $\alpha = x + (g_1)$. Existuje proto normovaný polynom $q \in K[x]$ takový, že $g_1 = (x - \alpha) \cdot q$. Označme $g = a \cdot q \cdot g_2 \cdots g_k \in K[x]$, pak $f = (x - \alpha) \cdot g$ a $\operatorname{st} g = \operatorname{st} f - 1$.

Proto podle indukčního předpokladu existuje rozšíření T tělesa K takové, že g se v $T[x]$ rozkládá na součin lineárních činitelů. Pak T je také rozšíření tělesa R takové, že f se v $T[x]$ rozkládá na součin lineárních činitelů.

Definice. Podle předchozí věty pro libovolný nekonstantní polynom $f \in R[x]$, kde R je těleso, existuje rozšíření $R \subseteq T$ takové, že

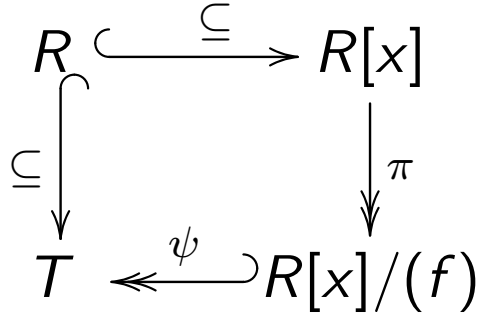
$$f = a \cdot (x - \alpha_1) \cdots (x - \alpha_n),$$

kde $a \in R$, $\alpha_1, \ldots, \alpha_n \in T$. Pak těleso $R(\alpha_1, \ldots, \alpha_n)$ nazýváme rozkladové těleso polynomu f nad tělesem R.

Poznámka. Je možné dokázat, že rozkladové těleso polynomu f nad tělesem R je určeno jednoznačně až na izomorfismus: jsou-li K, L obě rozkladová tělesa polynomu f nad tělesem R, pak existuje izomorfismus $\varphi : K \to L$ takový, že $\varphi(r) = r$ pro každé $r \in R$.

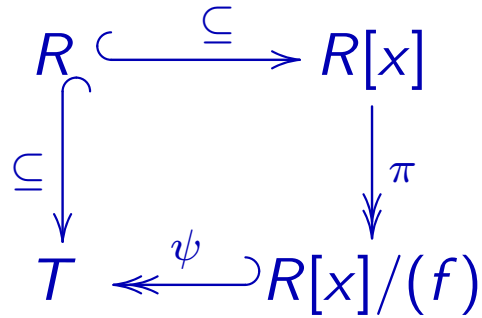
Popis jednoduchých rozšíření

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Pak platí: $R \subseteq T$ je jednoduché rozšíření, právě když existuje polynom $f \in R[x]$, který je ireducibilní nad R, a izomorfismus okruhů $\psi : R[x]/(f) \to T$ tak, že následující diagram komutuje*



Poznámka. Tato věta je ve skriptech nepřesně formulovaná (jde o větu 11.12 na straně 114). V jejím důkaze sice chyba není, ale nedokazuje se zde přesně to, co je ve znění věty.

Důkaz. „$\Rightarrow$“ Je-li $T = R(c)$, kde c je algebraický prvek nad R, pak jsme izomorfismus ψ získali v důkaze věty o minimálním polynomu (tam se jmenoval $\tilde{\varphi}$).



„⇐“ Označme $c = \psi(x + (f)) \in T$. Pro libovolný polynom $g = g_m x^m + \cdots + g_1 x + g_0 \in R[x]$ platí

$$\begin{aligned} g(c) &= g_m c^m + \cdots + g_1 c + g_0 = \\ &= \psi(g_m + (f)) \cdot (\psi(x + (f)))^m + \cdots + \\ &\quad + \psi(g_1 + (f)) \cdot \psi(x + (f)) + \psi(g_0 + (f)) = \\ &= \psi(g_m x^m + \cdots + g_1 x + g_0 + (f)) = \psi(g + (f)). \end{aligned}$$

Libovolný prvek tělesa T je tedy tvaru $g(c)$ pro vhodný $g \in R[x]$, proto $T = R(c)$. Volbou $g = f$ dostaneme

$$f(c) = \psi(f + (f)) = \psi(0 + (f)) = 0,$$

a tudíž c je algebraický nad R.

Podtěleso algebraických prvků

Věta. *Nechť $R \subseteq T$ je rozšíření těles. Označme A množinu všech prvků $t \in T$, které jsou algebraické nad R. Pak A je podtěleso tělesa T obsahující těleso R.*

Důkaz. Zřejmě $R \subseteq A$, neboť každý $r \in R$ je kořenem nenulového polynomu $x - r \in R[x]$. Musíme dokázat, že pro každé $\alpha, \beta \in A$ platí $-\alpha, \alpha + \beta, \alpha \cdot \beta \in A$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in A$. Protože α je algebraický nad R, platí $[R(\alpha) : R] < \infty$. Zřejmě $(R(\alpha))(\beta)$ je nejmenší podtěleso tělesa T obsahující $(R(\alpha)) \cup \{\beta\}$, a tedy nejmenší podtěleso tělesa T obsahující $R \cup \{\alpha, \beta\}$. Proto $(R(\alpha))(\beta) = R(\alpha, \beta)$. Protože β je algebraický nad R, je také algebraický nad $R(\alpha)$ a platí $[R(\alpha, \beta) : R(\alpha)] < \infty$. Dohromady $[R(\alpha, \beta) : R] = [R(\alpha, \beta) : R(\alpha)] \cdot [R(\alpha) : R] < \infty$. Protože každé konečné rozšíření těles je algebraické, platí, že $-\alpha, \alpha + \beta, \alpha \cdot \beta \in R(\alpha, \beta)$, a pokud $\alpha \neq 0$, tak také $\alpha^{-1} \in R(\alpha, \beta)$ jsou algebraické prvky nad R.

Příklad nekonečného algebraického rozšíření

Aplikujme předchozí větu na rozšíření $\mathbb{Q} \subseteq \mathbb{C}$. Pak A je těleso všech algebraických čísel. Proto je $\mathbb{Q} \subseteq A$ algebraické rozšíření.

Ukážeme, že $\mathbb{Q} \subseteq A$ není konečné. Pro libovolné $n \in \mathbb{N}$ je polynom $x^n - 2$ je ireducibilní nad $\mathbb{Q}$ podle Eisensteinova kriteria, a tedy je minimálním polynomem algebraického čísla $\sqrt[n]{2}$, odkud $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Proto vektorový prostor A nad $\mathbb{Q}$ obsahuje n-rozměrný vektorový podprostor pro každé $n \in \mathbb{N}$, nemůže být tedy konečněrozměrný.

(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 π je transcendentní nad $\mathbb{Q}$, plyne odtud $[T_n : \mathbb{Q}] = \infty$, což je spor s tím, že $\mathbb{Q} \subseteq T_n$ je konečné rozšíření.