Tělesa

Alexander „Olin“ Slávik

Úvod

Tělesa jsou algebraické struktury, které mají velmi příjemné vlastnosti – jsou „šité na míru“ tak, aby se s nimi dalo počítat podobně jako třeba s reálnými čísly. I přes to, jak je jejich struktura striktně zadána, lze u nich pozorovat zajímavé odlišnosti a jevy.

Definice. Množinu $\mathbb{F}$ spolu s binárními operacemi $+$ a $\cdot$ a „význačnými“ prvky 0 a 1 nazveme *(komutativním) tělesem*, pokud pro všechna $x, y, z \in \mathbb{F}$ platí následující vztahy:

(i) $x + (y + z) = (x + y) + z$,
(ii) $x + y = y + x$,
(iii) $x + 0 = x$,
(iv) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
(v) $x \cdot y = y \cdot x$,
(vi) $x \cdot 1 = x$,
(vii) $x \cdot (y + z) = x \cdot y + x \cdot z$,
(viii) existuje prvek $-x \in \mathbb{F}$ takový, že $x + -x = 0$,
(ix) je-li $x \neq 0$, pak existuje prvek $x^{-1} \in \mathbb{F}$ takový, že $x \cdot x^{-1} = 1$.

Příklady. Uveďme pár (více či méně obvyklých) příkladů těles:

(i) reálná čísla $\mathbb{R}$,
(ii) komplexní čísla $\mathbb{C}$,
(iii) racionální čísla $\mathbb{Q}$,
(iv) zbytky modulo p s operacemi modulo p $\mathbb{Z}_p$,
(v) čtyřprvkové těleso (množina $\{0, 1, a, b\}$ s operacemi danými vztahy $0 = 1 + 1 = a + a = b + b$, $a + b = 1$, $a \cdot b = 1$, $a \cdot a = b$, $b \cdot b = a$),
(vi) racionální funkce (tj. podíly polynomů),
(vii) Laurentovy řady (tj. formální sumy tvaru $\sum_{k=n}^{\infty} a_k x^k$, kde $n \in \mathbb{Z}$ a a_k jsou prvky nějakého předem zvoleného tělesa).

Vlastnosti těles

Definice. *Charakteristika tělesa* $\mathbb{F}$ je nejmenší přirozené číslo n takové, že v $\mathbb{F}$ platí rovnost

$$\underbrace{1+1+\cdots+1}_{n}=0.$$

Pokud takové $n \in \mathbb{N}$ neexistuje, říkáme, že $\mathbb{F}$ má charakteristiku 0.

Cvičení. Je-li charakteristika tělesa nenulová, pak je to již nutně prvočíslo.

Cvičení. Zřejmě má každé konečné těleso nenulovou charakteristiku. Ukažte, že opačná implikace nemusí platit, tj. najděte nekonečné těleso s nenulovou charakteristikou.

Definice. Řekneme, že těleso $\mathbb{F}$ je algebraicky uzavřené, pokud každý nekonstantní polynom s koeficienty z $\mathbb{F}$ má v $\mathbb{F}$ aspoň jeden kořen.

Věta. (Základní věta algebry) *Těleso $\mathbb{C}$ je algebraicky uzavřené.*

Pozorování. *Na rozdíl od reálných čísel není možné komplexní čísla „přirozeně“ uspořádat, tj. není možné na nich zavést nějaké uspořádání $\preceq$ takové, že by pro všechna $x, y, z \in \mathbb{C}$ platilo:*

(i) *je-li $x \preceq y$, pak také $x + z \preceq y + z$,*
(ii) *platí-li $0 \preceq x$ a $0 \preceq y$, pak také $0 \preceq xy$.*

Cvičení. Ukažte, že žádné konečné těleso není algebraicky uzavřené.

Konstrukce těles

Cvičení. Mějme strukturu podobnou tělesu, ve které platí všechny podmínky z úvodní definice kromě poslední (existence inverzních prvků)[1] – takovou strukturou jsou například celá čísla. Je možné tuto strukturu doplnit o další prvky (a dodefinovat na této větší množině operace $+$, $\cdot$) tak, aby výsledná množina byla tělesem?

Cvičení. Ukažte, že racionální funkce je možné vnořit jakožto podtěleso do Laurentových řad.

Cvičení. Představme si, že máme těleso $\mathbb{F}$ a někdo nám „přinese“ úplně nový prvek x, který chce do tělesa „přidat“. Co všechno ještě musíme k $\mathbb{F} \cup \{x\}$ přidat, abychom dostali zase těleso?

Cvičení. Situace jako v předchozím cvičení, ale požadavek navíc je, aby x splňovalo $x^2 + 1 = 0$, případně nějakou jinou polynomiální rovnici. Která známá tělesa takto umíme získat?

[1] Takové struktury se nazývají *okruhy*.

Definice. Mějme těleso $\mathbb{F}$ a jeho podtěleso $\mathbb{T}$. Prvek $x \in \mathbb{F}$ se nazývá *algebraický nad* $\mathbb{T}$, pokud je kořenem nějakého polynomu s koeficienty z $\mathbb{T}$, v opačném případě je *transcendentní nad* $\mathbb{T}$.

Příklad. $\sqrt{2}$ je algebraická nad $\mathbb{Q}$, ovšem například π není.

Věta. *Pro každé těleso $\mathbb{F}$ existuje nadtěleso $\overline{\mathbb{F}}$ s následujícími vlastnostmi:*

(i) *$\overline{\mathbb{F}}$ je algebraicky uzavřené,*

(ii) *pokud těleso $\mathbb{T}$ splňuje $\mathbb{F} \subseteq \mathbb{T} \subseteq \overline{\mathbb{F}}$ a je algebraicky uzavřené, pak $\mathbb{T} = \mathbb{F}$ (neboli $\overline{\mathbb{F}}$ je „nejmenší“ algebraicky uzavřené nadtěleso $\mathbb{F}$),*

(iii) *je-li $\mathbb{S}$ nadtěleso $\mathbb{F}$ splňující body (i) a (ii), pak jsou $\mathbb{S}$ a $\overline{\mathbb{F}}$ isomorfní (tj. algebraicky „stejná“).*

Výše uvedené těleso $\overline{\mathbb{F}}$ se nazývá algebraický uzávěr $\mathbb{F}$.

Příklad. $\overline{\mathbb{R}} = \mathbb{C}$. $\overline{\mathbb{Q}}$ je tvořeno právě všemi komplexními čísly algebraickými nad $\mathbb{Q}$.