1. Čísla a tělesa

Definice 1.1. Buď X neprázdná množina. Binární operací na množině X rozumíme libovolnou funkci $f : X \times X \to X$.

Vlastnosti sčítání a násobení reálných (komplexních, racionálních) čísel:
A: Každé dvojici čísel a, b odpovídá číslo $a + b$, nazývané součet čísel a, b a platí

- (A1) sčítání je komutativní, tj. platí $a + b = b + a$ pro každá dvě čísla a, b,
- (A2) sčítání je asociativní, tj. platí $(a + b) + c = a + (b + c)$ pro každá tři čísla a, b, c,
- (A3) existuje neutrální (nulový) prvek vzhledem ke sčítání, tj. číslo 0 takové, že platí $a + 0 = 0 + a = a$ pro každé číslo a,
- (A4) ke každému číslo a existuje opačné číslo $-a$, pro které platí $a+(-a) = (-a)+a = 0$.

B: Každé dvojici čísel a, b odpovídá číslo ab nazývané součin čísel a, b a platí

- (B1) násobení je komutativní, tj. platí $ab = ba$ pro každá dvě čísla a, b,
- (B2) násobení je asociativní, tj. platí $a(bc) = (ab)c$ pro každá třo čísla a, b, c,
- (B3) existuje neutrální (jednotkový) prvek vzhledem k operaci násobení, tj. číslo 1 takové, že platí $1a = a1 = a$ pro každé číslo a,
- (B4) pro každé číslo $a \neq 0$ existuje inverzní prvek a^{-1} takový, že $aa^{-1} = a^{-1}a = 1$.

C: Násobení je distributivní vzhledem ke sčítání, tj. platí $a(b+c) = (ab) + (ac)$, $(b+c)a = (ba) + (ca)$ pro každá tři čísla a, b, c.
D: $0 \neq 1$.

Definice 1.2. Buď $\mathbf{T}$ libovolná množina (její prvky budeme nazývat čísla nebo skaláry) a sčítání $(+)$ a násobení $(\cdot)$ dvě binární operace definované na $\mathbf{T}$. Splňují-li tyto dvě operace podmínky (A1)-(A4), (B1)-(B4), C, D, pak nazýváme množinu $\mathbf{T}$ spolu s příslušnými operacemi sčítání a násobení *těleso.*

Příklad 1.1. Známá tělesa. a) Obvyklé operace sčítání a násobení racionálních čísel mají uvedených 10 vlastností. Množina všech racionálních čísel s obvyklým sčítáním a násobením je tedy těleso. Budeme mu říkat těleso racionálních čísel a označovat ho $\mathbf{Q}$.
b) Těleso reálných čísel $\mathbf{R}$.
c) Těleso komplexních čísel $\mathbf{C}$.

Příklad 1.2. Některá konečná tělesa. a) Na množině $\{0, 1\}$ definujeme operace sčítání a násobení takto:

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1,$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Jsou to vlastně sčítání a násobení modulo 2. Ověřte si, že množina $\{0, 1\}$ s takto definovaným sčítáním a násobením splňuje všech 10 podmínek a je tedy tělesem. Označujeme ho $\mathbf{Z}_2$.

Typeset by $\mathcal{AMS}$-TEX

b) Podobně na množině $\{0, 1, 2\}$ definujeme operace sčítání a násobení takto:

$$0 + 0 = 1 + 2 = 2 + 1 = 0,\; 0 + 1 = 1 + 0 = 2 + 2 = 1,\; 0 + 2 = 2 + 0 = 1 + 1 = 2,$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 2 = 2 \cdot 0 = 0,\; 1 \cdot 1 = 2 \cdot 2 = 1,\; 1 \cdot 2 = 2 \cdot 1 = 2.$$

V tomto případě jde o sčítání a násobení modulo 3. Ověřte, že jde o těleso. (V případě asociativity nebo distributivity je nutné ověřit 27 rovností.) Toto těleso označujeme $\mathbf{Z}_3$.

c) Množina $\{0, 1, 2, 3\}$ spolu se sčítáním a násobením modulo 4 **není** těleso, protože prvek 2 nemá žádný inverzní prvek. Přesto čtyřprvkové těleso existuje, operace sčítání a násobení je ale třeba definovat jinak.

d) Množina $\{0, 1, 2, 3, 4\}$ spolu s operacemi sčítání a násobení modulo 5 **je** těleso.

e) Množina $\{0, 1, 2, 3, 4, 5\}$ spolu s operacemi sčítání a násobení modulo 6 **není** těleso, čísla $2, 3, 4$ nemají žádný inverzní prvek. Žádné šestiprvkové těleso neexistuje, na množině $\{0, 1, 2, 3, 4, 5\}$ nelze definovat sčítání a násobení tak, aby měly všech 10 vlastností, které musí těleso mít.

f) Platí, že počet prvků jakéhokoliv konečného tělesa musí být roven p^k, kde p je nějaké prvočíslo, a $k \geq 1$ je přirozené číslo. A naopak, je-li p prvočíslo a $k \geq 1$ přirozené číslo, existuje "právě jedno" konečné těleso, které má p^k prvků.

Věta 1.1. Základní vlastnosti sčítání a násobení v tělesech. Buď $\mathbf{T}$ libovolné těleso. Potom platí:

a) nulový prvek (neutrální prvek vzhledem ke sčítání) je určený jednoznačně,
b) prvek $-a$ je určený jednoznačně prvkem a,
c) jednotkový prvek (neutrální prvek vzhledem k násobení) je určený jednoznačně,
d) prvek a^{-1} je určený jednoznačně prvkem $a \neq 0$,
e) $0 \cdot a = 0$ pro každé $a \in \mathbf{T}$,
f) je-li $a \cdot b = 0$, pak buď $a = 0$ nebo $b = 0$,
g) $(-1)a = -a$ pro každé $a \in \mathbf{T}$,
h) rovnice $ax = b$, $a \neq 0$, má právě jedno řešení,
i) rovnice $c + x = d$ má právě jedno řešení,
j) z rovnosti $ab = ac$, $a \neq 0$, plyne $b = c$,
k) $(-a) \cdot (-b) = ab$,
l) z rovnosti $a + b = a + c$ plyne $b = c$.

Důkaz. a) Předpokládejme, že dva prvky 0_1 a 0_2 jsou neutrální vzhledem k operaci sčítání. Potom platí

$$0_1 = 0_1 + 0_2 = 0_2.$$

b) Buď x libovolný prvek tělesa $\mathbf{T}$, který je opačný k prvku a, tj. pro který platí $a + x = x + a = 0$. Pak platí

$$x = 0 + x = ((-a) + a) + x = (-a) + (a + x) = (-a) + 0 = -a.$$

c),d) za domácí úkol.

e) Platí $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. K oběma stranám rovnosti $0 \cdot a = 0 \cdot a + 0 \cdot a$ připočteme prvek $-(0 \cdot a)$ opačný k $0 \cdot a$. Dostaneme tak

$$-(0 \cdot a) + 0 \cdot a = -(0 \cdot a) + 0 \cdot a + 0 \cdot a,$$

a tedy také $0 = 0 \cdot a$.

f) Je-li $a \cdot b = 0$ a $a \neq 0$, pak vynásobíme obě strany rovnosti prvkem a^{-1}, který existuje díky předpokladu $a \neq 0$. Potom platí

$$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

g) Platí $0 = 0a = (-1+1)a = (-1)a + 1a = (-1)a + a$ a rovněž $0 = (1 + (-1))a = 1a + (-1)a = a + (-1)a$. Prvek $(-1)a$ je tedy opačným prvkem k prvku a a z jednoznačnosti opačného prvku (tvrzení b) plyne $(-1)a = -a$.

h) Vynásobením rovnice $a \cdot x = b$ zleva prvkem a^{-1} dostaneme postupně $a^{-1}(ax) = a^{-1}b$, tj. $(a^{-1}a)x = a^{-1}b$, $1x = a^{-1}b$, $x = a^{-1}b$.

i), j), k), l) za domácí úkol. □

V nějakém tělese **T** je definováno sčítání pouze **dvou** prvků **T**. Chceme-li sečíst více prvků, musíme pomocí závorek určit, jaké dvojice prvků postupně sčítáme. V případě součtu $a + b + c$ jsou pouze dvě možnosti a axiom (A3) říká, že obě možnosti vedou k témuž výsledku, neboť

$$a + (b + c) = (a + b) + c.$$

V případě součtu $a + b + c + d$ existuje celkem pět různých uzávorkování (jakých?) a opět s použitím axiomu asociativity sčítání v **T** lze dokázat, že všech pět možností vede k jednomu a témuž výsledku.

Věta 1.2. Obecná asociativita pro sčítání. V každém tělese **T** platí, že součet

$$a_1 + a_2 + \cdots + a_n$$

libovolného nenulového počtu prvků nezávisí na uzávorkování, které k jeho výpočtu použijeme.

Důkaz. Indukcí podle n. Začátek indukce je snadný, pro $n = 1, 2$ není co dokazovat. Pro $n = 3$ to platí podle axiomu (A2). Předpokládejme, že tvrzení platí pro všechna přirozená čísla menší než $n \geq 4$. Uvažujme nyní dvě možná uzávorkování součtu $a_1 + \cdots + a_n$. Při výpočtu podle jednoho uzávorkování je poslední krok součet

$$(a_1 + \cdots + a_k) + (a_{k+1} + \cdots + a_n)$$

pro nějaké $0 < k < n$. V každé závorce je součet méně než n prvků tělesa **T** a jsme tedy oprávněni použít indukční předpoklad a pro součty v závorkách už nemusíme konkrétní uzávorkování vypisovat, neboť všechny vedou k témuž součtu.

Při druhém výpočtu je poslední krok součet

$$(a_1 + \cdots + a_l) + (a_{l+1} + \cdots + a_n),$$

kde $0 < l < n$.

Oba součty se rovnají, je-li $k = l$. Je-li $k \neq l$, můžeme předpokládat, že $k < l$. Opět použijeme indukční předpoklad a napíšeme si první součet jako

$$(a_1 + \cdots + a + k) + ((a_{k+1} + \cdots + a_l) + (a_{l+1} + \cdots + a_n)).$$

Podobně druhý součet můžeme vyjádřit ve tvaru

$$((a_1 + \cdots + a + k) + (a_{k+1} + \cdots + a_l)) + (a_{l+1} + \cdots + a_n).$$

Oba součty se potom rovnají podle axiomu ($A2$). $\square$

V celém důkazu jsme nepoužili žádný jiný axiom než ($A2$). Pokud bychom všude nahradili sčítání násobením a axiom (A2) axiomem (B2), dostali bychom důkaz obecné asociativity i pro násobení v tělese **T**.

Definice 1.3. Charakteristika tělesa. Existuje-li v tělese **T** nějaké kladné přirozené číslo n takové, že platí

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

pak nejmenší takové kladné čísla nazýváme *charakteristika* tělesa **T**. Pokud žádné takové kladné n neexistuje, říkáme, že těleso **T** má charakteristiku 0.

Věta 1.3. Charakteristika každého tělesa **T** je buď 0 nebo prvočíslo.

Důkaz. Jestliže charakteristika **T** není rovna 0, je rovna nějakému kladnému přirozenému číslu n. Pokud n není prvočíslo, existují kladná přirozená čísla p, q, obě menší než n, pro která platí $pq = n$. Potom platí

$$(\underbrace{1 + 1 + \cdots + 1}_{p})(\underbrace{1 + 1 + \cdots + 1}_{q}) = \underbrace{1 + 1 + \cdots + 1}_{n=pq} = 0.$$

V tělese ale může být součin dvou prvků roven 0 pouze je-li jeden z těchto prvků roven 0 (Věta 2f). Proto platí buď

$$\underbrace{1 + 1 + \cdots + 1}_{p} = 0$$

nebo

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

V obou případech to je ve sporu s předpokladem, že n bylo nejmenší kladné přirozené číslo takové, že

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

□

V tělese s nenulovou charakteristikou nejsou obsažena přirozená čísla, protože součet p jednotek se rovná 0. Naproti tomu každé těleso charakteristiky 0 "obsahuje" nejenom přirozená čísla, ale i čísla racionální. Obsahuje-li totiž přirozená čísla, musí na základě axiomu (A4) obsahovat i celá čísla, a v důsledku axiomu (B4) také podíly celých čísel neboli čísla racionální.

Příklad 1.3. Charakteristiky těles $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$.

Problémy k přemýšlení. a) Sestrojte čtyřprvkové těleso.

b) Dokažte, že množina $\mathbf{Z}_p=\{0,1,\ldots,p-1\}$ spolu s operacemi sčítání a násobení modulo p je těleso právě když je p prvočíslo.