Kapitola 3

Tělesa

Definice 3.1 *Předpokládáme, že* $\mathbf{T}$ *je množina, na které jsou definované dvě operace – sčítání a násobení. Pokud tyto dvě operace splňují následující podmínky (axiomy), říkáme že množina* $\mathbf{T}$ *spolu s těmito operacemi tvoří* těleso. *Jsou to podmínky*

(A0) *součet* $a + b \in \mathbf{T}$ *pro libovolné* $a, b \in \mathbf{T}$,

(A1) *platí* $(a + b) + c = a + (b + c)$ *pro libovolné* $a, b, c \in \mathbf{T}$,

(A2) $a + b = b + a$ *pro libovolné dva prvky* $a, b \in \mathbf{T}$,

(A3) *existuje prvek* $0 \in \mathbf{T}$ *takový, že* $0 + a = a$ *pro každé* $a \in \mathbf{T}$,

(A4) *ke každému prvku* $a \in \mathbf{T}$ *existuje prvek* $-a \in \mathbf{T}$, *pro který platí, že* $(-a) + a = 0$.

To jsou všechny axiomy pro sčítání. Axiom (A0) říká, že množina $\mathbf{T}$ *je* uzavřená *na sčítání. Axiom (A1) je* asociativita *sčítání, axiom (A2) je* komutativita *sčítání. Axiomu (A3) říkáme existence* nulového prvku *nebo také* neutrálního prvku *vzhledem ke sčítání a axiomu (A4) pak existence* opačného prvku *vzhledem ke sčítání.*

Následují axiomy pro násobení:

(M0) *součin* $ab \in \mathbf{T}$ *pro libovolné* $a, b \in \mathbf{T}$,

(M1) *platí* $(ab)c = a(bc)$ *pro libovolné* $a, b, c \in \mathbf{T}$,

(M2) $ab = ba$ *pro libovolné dva prvky* $a, b \in \mathbf{T}$,

(M3) *existuje prvek* $1 \in \mathbf{T}$ *takový, že* $1a = a$ *pro každé* $a \in \mathbf{T}$,

(M4) *ke každému prvku* $0 \neq a \in \mathbf{T}$ *existuje prvek* $a^{-1} \in \mathbf{T}$*, pro který platí* $a^{-1}a = 1$.

Axiom (M0) vyjadřujeme slovy, že množina $\mathbf{T}$ *je* uzavřená *vzhledem k násobení, axiomy (M1) a (M2) říkají, že násobení je* asociativní *a* komutativní. *Axiom (M3) je existence* jednotkového prvku *nebo také* neutrálního prvku *vzhledem k násobení a axiom (M4) je axiom existence* inverzního prvku *vzhledem k násobení.*

Obě operace pak spojuje axiom distributivity

(D) *platí* $a(b + c) = ab + ac$ *pro libovolné tři prvky* $a, b, c \in \mathbf{T}$.

A nakonec axiom netriviality

(N) $0 \neq 1$.

Tvrzení 3.1 *V každém tělese* $\mathbf{T}$ *platí*

1. *nulový prvek je určený jednoznačně,*
2. *opačný prvek* $-a$ *je prvkem* $a \in \mathbf{T}$ *určený jednoznačně,*
3. *jednotkový prvek je určený jednoznačně,*
4. *prvek* a^{-1} *inverzní k prvku* $0 \neq a \in \mathbf{T}$*, je prvkem a určený jednoznačně,*
5. $0a = 0$ *pro libolný prvek* $a \in \mathbf{T}$*,*
6. *je-li* $ab = 0$*, pak buď* $a = 0$ *nebo* $b = 0$*,*
7. $(-1)a = -a$ *pro každý prvek* $a \in \mathbf{T}$*,*
8. *rovnice* $ax = b$*,* $a \neq 0$*, má vždy právě jedno řešení,*
9. *rovnice* $c + x = d$ *má vždy právě jedno řešení,*
10. *z rovnosti* $ab = ac$ *a předpokladu* $a \neq 0$*, vyplývá* $b = c$*,*
11. *z rovnosti* $a + b = a + c$ *plyne* $b = c$*,*
12. $(-a)(-b) = ab$ *pro každé dva prvky* $a, b \in \mathbf{T}$.

Všechny dosavadní poznatky o maticích a řešení soustav lineárních rovnic platí v libovolném tělese $\mathbf{T}$. Soustavou lineárních rovnic v tělese $\mathbf{T}$ rozumíme soustavu

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &= b_2, \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m, \end{aligned}$$

kde jsou všechny koeficienty $a_{ij}, b_k \in \mathbf{T}$. Z axiomů tělesa a jejich bezprostředních důsledků pak vyplývá, že Gaussova eliminace a zpětná substituce vedou k řešením této soustavy, která všechna opět leží v tělese $\mathbf{T}$.

Podobně matice s prvky z tělesa $\mathbf{T}$ je matice $\mathbf{A} = (a_{ij})$, kde $a_{ij} \in \mathbf{T}$. Elementární řádkové úpravy matice s prvky z libovolného tělesa $\mathbf{T}$ můžeme provádět beze změny. Je-li $\mathbf{A}$ regulární matice, pak pomocí elementárních řádkových úprav použitých na jednotkovou matici dostaneme inverzní matici $\mathbf{A}^{-1}$, která má také všechny prvky z tělesa $\mathbf{T}$. Podobně zůstávají v platnosti i všechny ostatní vlastnosti matic. Stačí pouze vždy na začátku říct, v jakém tělese leží prvky matic, se kterými počítáme. Tak například faktory $\mathbf{L}, \mathbf{U}$ v LU-rozkladu matice $\mathbf{A}$, která má prvky z tělesa $\mathbf{T}$, jsou oba také matice s prvky z tělesa $\mathbf{T}$.

Příklad 3.1 Příklady těles $\mathbf{Q}, \mathbf{R}, \mathbf{C}$, netěleso $\mathbf{Z}$, pro které nicméně řada poznatků také platí, jsou to všechny, které nezávisí na existenci inverzního prvku.

Příklad 3.2 Dvouprvková množina $\{0, 1\}$ spolu s operacemi sčítání

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

a násobení

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

je také těleso. Je to vlastně počítání *modulo* 2. Výsledek operace získáme tak, že uděláme napřed obvyklý součet dvou čísel a za výsledek pak vezmeme zbytek při dělení obvyklého součtu číslem 2. Podobně pro součin. Platnost všech axiomů tělesa můžeme pak ověřit přímo. Toto těleso budeme označovat $\mathbf{Z}_2$.

Příklad 3.3 Jiné konečné těleso dostaneme, když čísla $\{0,1,2\}$ sčítáme a násobíme *modulo* 3. Operace sčítání je potom

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

a operace násobení je

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

Můžete si sami ověřit, že množina $\{0,1,2\}$ s takto definovanými operacemi je těleso. V případě asociativity obou operací a distributivity je třeba vždy ověřit 27 rovností.

Příklad 3.4 Množina $\{0,1,2,3\}$ spolu s operacemi sčítání a násobení *modulo* 4 **není** těleso. Platí v ní totiž $2\cdot 2=0$ a přitom $2\neq 0$. To se v žádném tělese nemůže stát podle Tvrzení 3.1.6.

Příklad 3.5 Čtyřprvkové těleso ale existuje. Nejlépe je počítat s polynomy $\mathbf{GF}(4)=\{0,1,x,x+1\}$ jedné proměnné s koeficienty $0,1$. Koeficienty považujeme za prvky tělesa $\mathbf{Z}_2$. Tyto polynomy pak můžeme sčítat a násobit obvyklým způsobem. Množina $\mathbf{GF}(4)$ je uzavřená na sčítání polynomů, není ale uzavřená na jejich násobení, neboť $(x+1)(x+1)=x^2+(1+1)x+1=x^2+1$. Operaci násobení proto definujeme *modulo* polynom x^2+x+1. To znamená, že obvyklý součin dvou polynomů vydělíme se zbytkem polynomem x^2+x+1 a jako výsledek součinu vezmeme tento zbytek. Potom platí např.

$$x(x+1)=(x+1)x=1 \quad \text{a} \quad (x+1)(x+1)=x.$$

Zkuste si sami ověřit axiomy tělesa a dokázat, že množina $\mathbf{GF}(4)$ je skutečně těleso.

Příklad 3.6 Množina $\mathbf{Z}_n=\{0,1,2,\ldots,n-1\}$ pro $n\geq 2$ spolu s operacemi sčítání a násobení *modulo* n je těleso právě když je n prvočíslo. Toto tvrzení si nebudeme dokazovat. Pokud někdo zná Euklidův algoritmus, tak to zvládne sám. Jediný problém spočívá v důkazu existence inverzního prvku k libovolnému číslu $0\neq x<n$, pokud je n prvočíslo. Pokud n není prvočíslo, tak $\mathbf{Z}_n$ není tělesem ze stejného důvodu, kvůli kterému není $\mathbf{Z}_4$ těleso.

Příklad 3.7 Pro každé prvočíslo p a každý exponent $n \geq 1$ existuje právě jedno těleso, které má p^n prvků a žádná jiná tělesa s konečným počtem prvků neexistují. Žádné šestiprvkové těleso tedy neeistuje. Tělesa s počtem prvků p^n pro $n \geq 2$ se konstruují podobně, jako jsme sestrojili čtyřprvkové těleso v Příkladu 3. Vezmeme všechny polynomy (včetně konstantních) stupně menšího než n s koeficienty v tělese $\mathbf{Z}_p$. Těch je celkem p^n. Na této množině sčítáme obvyklým způsobem a násobíme *modulo* **vhodný** polynom stupně n.

Vidíme, že tělesa mohou být značně odlišná. jejich vlastnosti hodně závisí na následujícím číselném parametru.

Definice 3.2 *Existuje-li kladné celé číslo n takové, že v tělese $\mathbf{T}$ platí*

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

pak nejmenší takové kladné číslo nazýváme charakteristika *tělesa* $\mathbf{T}$.

Pokud žádné takové kladné celé číslo n neexistuje, tak říkáme, že těleso $\mathbf{T}$ *má* charakteristiku 0.

Věta 3.2 *Charakteristika každého tělesa je buď 0 nebo prvočíslo.*

Důkaz. Jestliže charakteristika tělesa $\mathbf{T}$ není rovná 0, pak existuje nějaké kladné celé číslo $n \geq 2$, pro které platí

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

Jestliže je n složené číslo, platí $n = kl$ pro nějaká kladná celá čísla $k, l < n$. V důsledku axiomu distributivity (D) platí

$$(\underbrace{1+1+\cdots+1}_{k})(\underbrace{1+1+\cdots+1}_{l})=\underbrace{1+1+\cdots+1}_{n}=0.$$

Podle Tvrzení 3.1.6 může být součin dvou prvků v tělese rovný 0 pouze pokud je aspoň jeden z činitelů rovný 0. Proto je buď

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

nebo

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

V každém případě nemůže být složené číslo $n \geq 2$ nejmenším kladným celým číslem, pro které platí

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

Protože je $1 \neq 0$ podle axiomu netriviality (N), musí být nejmenší takové číslo prvočíslo. $\square$

Úloha 3.1 Zjistěte charakteristiky těles $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Q}$, $\mathbf{R}$ a $\mathbf{C}$. Jakou má charakteristiku konečné těleso, které má p^n prvků?