# 1. Tělesa

Uvažujme například množinu všech racionálních čísel $\mathbf{Q}$ spolu s obvyklými operacemi $+$ a $\cdot$ a všimněme si „běžných" vlastností obou operací (tj. takových, jichž jsme bez rozmýšlení ochotni a schopni používat). Nejprve zaznamenejme takové vlastnosti sčítání:

1. $\forall a, b, c \in \mathbf{Q}$ platí rovnost $(a + b) + c = a + (b + c)$ (této vlastnosti operace se obvykle říká *asociativita*),
2. $\forall a, b \in \mathbf{Q}$ platí, že $a + b = b + a$ (této vlastnosti $+$ říkáme *komutativita*),
3. $\forall a \in \mathbf{Q}$ platí, že $a + 0 = a$ (tedy 0 je tzv. *neutrální prvek* operace $+$),
4. $\forall a \in \mathbf{Q}$ existuje racionální číslo, které označujeme $-a$, pro něž $a + (-a) = 0$ (tedy $-a$ je *opačný prvek* k $a$).

Velmi podobný soubor vlastností splňuje i násobení:

5. $\forall a, b, c \in \mathbf{Q}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*asociativita*),
6. $\forall a, b \in \mathbf{Q}$: $a \cdot b = b \cdot a$ (*komutativita*),
7. $\forall a \in \mathbf{Q}$ platí, že $a \cdot 1 = a$ (tedy 1 je *neutrální prvek* operace $\cdot$),
8. $\forall a \in \mathbf{Q}\setminus\{0\}$ existuje racionální číslo, které označujeme $a^{-1}$, pro něž $a \cdot a^{-1} = 1$ ($a^{-1}$ je tzv. *inverzní prvek* k $a$).

Doposud jsme neuvedli žádnou vlastnost, která by uvažované operace nějak svazovala. Uvědomme si, že velmi silný požadavek na „spolupráci" $+$ a $\cdot$ na racionálních číslech vyjadřuje pravidlo *distributivity*:

9. $\forall a, b, c \in \mathbf{Q}$: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Není těžké nahlédnout, že jsme právě shrnuli důležité vlastnosti uvažovaných operací jako takových a že mnohé další samozřejmé vlastnosti lze z *axiomů* 1.-9. odvodit. Například fakt, že $-(a \cdot b) = (-a) \cdot b$, plyne z axiomů 9. a 4. a z faktu $0 \cdot b = 0$ (konkrétně $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$) a dokonce i fakt, že $0 \cdot b = 0$ můžeme z axiomatiky odvodit (pomocí axiomů 9., 4. a 3.). To samozřejmě v případě racionálních čísel, s nimiž jsme zvyklí počítat, na nic nepotřebujeme, ale může to být velmi užitečné v okamžiku, kdy se zamyslíme, zda stejný (či podobný) soubor vlastností nesplňují i jiné páry operací (a tím ani nevylučujeme ani nezaručujeme, že budou mít stejný zápis) na jiných množinách a zda právě vyjmenované vlastnosti nepostačují k tomu, abychom uměli zodpovědět otázky, které si záhy v rámci kurzu lineární algebry položíme.

Už ve chvíli, kdy jsme sestavovali soupis vlastností 1.– 9., jsme si mohli uvědomit, že jsou samozřejmě splněny pro sčítání a násobení na reálných či komplexních číslech (a že například sčítání a násobení na celých číslech splňuje všechny uvedené axiomy s výjimkou axiomu 8.). Sepišme si tedy tyto vlastnosti ještě jednou, ale uvažujme je pro nějakou obecnou množinu $\mathbf{T}$ s dvojicí binárních operací $+$ a $\cdot$:

1. $\forall a, b, c \in \mathbf{T}$: $(a + b) + c = a + (b + c)$,
2. $\forall a, b \in \mathbf{T}$: $a + b = b + a$,
3. existuje takový prvek $0 \in \mathbf{T}$, že $\forall a \in \mathbf{T}$ platí rovnost $a + 0 = a$,
4. $\forall a \in \mathbf{T}$ existuje $-a \in \mathbf{T}$, pro které $a + (-a) = 0$,
5. $\forall a, b, c \in \mathbf{T}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
6. $\forall a, b \in \mathbf{T}$: $a \cdot b = b \cdot a$,
7. existuje takový prvek $1 \in \mathbf{T}$, že $\forall a \in \mathbf{T}$ platí rovnost $a \cdot 1 = a$,

8. $\forall a \in \mathbf{T} \setminus \{0\}$ existuje $a^{-1} \in \mathbf{T}$, pro které $a \cdot a^{-1} = 1$ ($a^{-1}$ je tzv. *inverzní prvek* k ).
9. $\forall a, b, c \in \mathbf{T}$: $a \cdot (b + c) = a \cdot b + a \cdot c$.

V novém souboru axiomů jsme do 3. a 7. axiomu přidali formulaci „existuje takový prvek”, která byla v případě racionálních, reálných či komplexních čísel zbytečná (0 a 1 tam označují zcela konkrétní čísla a my jen zaznamenali jejich charakteristické vlastnosti), ale ve chvíli, kdy nemáme k dispozici nic víc než dvě operace na abstraktní množině $\mathbf{T}$, je nezbytná. Rovněž si všimněme, že jsme v nové axiomatice převzali značení obvyklé u zmiňovaných konkrétních číselných struktur (kromě symbolů pro neutrální prvky také – a $^{-1}$), které v obecné situaci nemá konkrétní obsah (je okamžitě srozumitelné, jaké konkrétní racionální čísl máme na mysli, napíšeme-li $-5$ nebo $\frac{2}{3}^{-1}$, ovšem v jiných konkrétních příkladech struktur splňujících danou axiomatiku budou symboly – a $^{-1}$ teprve výzvou k následnému výpočtu).

Než shrneme naší axiomatiku pod pojem těleso, ujasněme si, co by znamenalo, kdyby oba výjimečné prvky (tj. 0 a 1) splývaly (tj. $0 = 1$). Potom by pro libovolné $a \in \mathbf{T}$ platilo $a = a \cdot 1 = a \cdot 0 = 0$, tedy množina $\mathbf{T}$ by byla pouze jednoprvková. Pro jednoprvkovou množinu a jednoznačně určené (a zjevně totožné) operace + a $\cdot$ by všechny axiomy sice platily, ale počítání by v takovém případě nebylo vůbec zajímavé a při budování vektorových prostorů by připuštění jednoprvkových těles přinášelo potíže. Proto přidáme k axiomatice požadavek, aby množina $\mathbf{T}$ byla aspoň dvouprvková (nebo ekvivalentně, aby $0 \neq 1$).

Nyní ukážeme, že dobře známé struktury $\mathbf{Q}$, $\mathbf{R}$ či $\mathbf{C}$ nejsou zdaleka jediné, které splňují aximatiku tělesa. Pomineme na tomto místě velké množství příkladů těles, která bychom mohli najít jako podtělesa reálných čísel a zaměříme se na tělesa s konečným počtem prvků.

Buď v následujícím $p$ prvočíslo a položme $\mathbf{Z}_p = \{0, 1, \dots, p-1\}$. Nyní definujme na $\mathbf{Z}_p$ operace $+_p$ a $\cdot_p$ předpisem $a +_p b = (a + b)\text{mod}p$ a $a \cdot_p b = (a \cdot b)\text{mod}p$, kde mod$p$ znamená zbytek po celočíselném dělení hodnotou $p$

**1.1.** Ověřte, že pro všechna celá $a$, $b$ a libovolné přirozené $n$ platí, že $((a)\text{mod}n + (b)\text{mod}n)\text{mod}n = (a + b)\text{mod}n$ a $((a)\text{mod}n \cdot (b)\text{mod}n)\text{mod}n = (a \cdot b)\text{mod}n$.

Zvolme libovolě celá $a$, $b$ a přirozené $n$. Předně si rozmyslíme význam zbytku po celočíselném dělení, tedy, že existují (jednoznačně určená) celá $q$ a $r$, pro něž $(a)\text{mod}n + qn = a$ a $(b)\text{mod}n + rn = b$. Navíc připomeňme, že $0 \leq (a)\text{mod}n < n$ a $0 \leq (b)\text{mod}n < n$. Nyní počítejme: $(a + b)\text{mod}n = ((a)\text{mod}n + qn + (b)\text{mod}n + rn)\text{mod}n = ((a)\text{mod}n+(b)\text{mod}n+(q+r)n)\text{mod}n = ((a)\text{mod}n+(b)\text{mod}n)\text{mod}n$. $\square$

**1.2.** Dokažte, že $\mathbf{Z}_p$ spolu s operacemi $+_p$ a $\cdot_p$ splňuje axiomy 1.– 7. a 9.

Platnost axiomů 2.,3.,6.,7. plyne okamžitě z definice operací a odpovídající vlastnosti pro celá čísla, axiomy 1., 5. a 9. platí díky pozorování z 1.1. Konečně $-0 = 0$ a $-a = p - a$ pro všechna $a \in \mathbf{Z}_p \setminus \{0\}$, protože $(a + p - a)\text{mod}p = (p)\text{mod}p = 0$. $\square$

**1.3.** Najděte inverzní prvky pro všechny nenulové prvky tělesa $\mathbf{Z}_5$.

V daném případě můžeme postupovat zkusmo. Snadno zjistíme, že $1^{-1} = 1$ (to platí ostatně v každém tělese), z pozorování, že $2 \cdot_5 3 = 1$, plyne, že $2^{-1} = 3$ i že $3^{-1} = 2$, a konečně $4^{-1} = 4$, protože $4 \cdot_5 4 = 1$. $\square$

*7.10.*

Nechť $a_0 \geq a_1$ jsou dvě přirozená čísla. Připomeňme Euklidův algoritmus hledání největšího společného dělitele (NSD) čísel $a_0$ a $a_1$:

Známe-li $a_{i-1}$ a $a_i$ spočteme $a_{i+1} = (a_{i-1})\text{mod } a_i$. Tedy víme, že existuje takové $q_i \in \mathbf{N}$ že $a_{i-1} = q_i a_i + a_{i+1}$ a $a_{i+1} < a_i$. Algoritmus skončí, když $a_{n+1} = 0$, potom $a_n = \text{NSD}(a_0, a_1)$.

**1.4.** Najděte pomocí Euklidova algoritmu taková celá čísla $x$ a $y$, aby $30x + 101y = 1$.

Nejprve si všimněme, že číslo 101 je prvočíslo, tedy největší společný dělitel čísel 30 a 101 je zcela jistě roven jedné. Euklidův algoritmus na nalezení největšího společného dělitele čísel 30 a 101 nám tedy samozřejmě musí dát výsledek 1. Přesto ho použijeme a budeme věnovat pozornost vztahu předchozích a následujících prvků:

$a_0 = 101$,
$a_1 = 30$,
$a_2 = 101 - 3 \cdot 30 = 11$,
$a_3 = 30 - 2 \cdot 11 = 8$,
$a_4 = 11 - 8 = 3$,
$a_5 = 8 - 2 \cdot 3 = 2$,
$a_6 = 3 - 2 = 1 = \text{NSD}(101, 30)$.

Vidíme, že každé $a_{i+1}$ je celočíselnou lineární kombinací prvků $a_i$ a $a_{i-1}$, budeme-li postupně dosazovat předchozí vyjádření do následujících výrazů, dostaneme každé $a_{i+1}$ jako celočíselnou lineární kombinací prvků $a_0$ a $a_1$:

$a_2 = 11 = 101 - 3 \cdot 30$,
$a_3 = 8 = 30 - 2 \cdot 11 = 30 - 2 \cdot (101 - 3 \cdot 30) = 7 \cdot 30 - 2 \cdot 101$,
$a_4 = 3 = 11 - 8 = (101 - 3 \cdot 30) - (7 \cdot 30 - 2 \cdot 101) = 3 \cdot 101 - 10 \cdot 30$,
$a_5 = 2 = 8 - 2 \cdot 3 = (7 \cdot 30 - 2 \cdot 101) - 2 \cdot (3 \cdot 101 - 10 \cdot 30) = 27 \cdot 30 - 8 \cdot 101$,
$a_6 = 1 = 3 - 2 = (3 \cdot 101 - 10 \cdot 30) - (27 \cdot 30 - 8 \cdot 101) = 11 \cdot 101 - 37 \cdot 30$.

Zjistili jsme, že $x = -37$ a $y = 11$. □

**1.5.** Najděte inverzní prvek k prvku 30 v tělese $\mathbf{Z}_{101}$.

Potřebujeme najít číslo $x \in \mathbf{Z}_{101}$, které by řešilo rovnici $(30 \cdot x)\text{mod } 101 = 1$, což můžeme reformulovat tak, že hledáme celá $x$ a $y$, z nichž $x$ má ležet v $\mathbf{Z}_{101}$, aby $30x + 101y = 1$. Podobnou úlohu už jsme řešili v předchozím příkladu, nyní si stačí uvědomit, že nalezené $x$, které neleží v požadovaném intervalu můžeme posunout pomocí vhodného násobku čísla 101. Dostaneme tedy zbytek po celočíselném dělení číslem 101, tj. $30^{-1} = (-37)\text{mod}101 = 101 - 37 = 64$, protože

$$1 = 11 \cdot 101 - 37 \cdot 30 = 11 \cdot 101 - 30 \cdot 101 + 101 \cdot 30 - 37 \cdot 30 = (11 - 30) \cdot 101 + (101 - 37) \cdot 30.$$

Tedy jsme našli další a pro nás zajímavější řešení řešení $1 = 64 \cdot 30 - 19 \cdot 101$ rovnice z 1.4.

**1.6.** Najděte v tělese $\mathbf{Z}_{101}$ prvky $63^{-1}$, $20^{-1}$, $2^{-1}$, $(20 \cdot 63)^{-1}$ a vyřešte nad ním rovnici $20 \cdot_{101} x = 7$

U prvních dvou hodnot postupujme stejně jako v předchozích úvahách, tedy využijeme Euklidův algoritmus:

$38 = 101 - 63$,

$25 = 63 - 38 = 2 \cdot 63 - 101,$
$13 = 38 - 25 = 2 \cdot 101 - 3 \cdot 63,$
$12 = 25 - 13 = 5 \cdot 63 - 3 \cdot 101,$
$1 = 13 - 12 = 5 \cdot 101 - 8 \cdot 63.$
Zjistili jsme, že $63^{-1} = (-8) \bmod 101 = 93$.

Podobně už v prvním kroku Euklidova algoritmu zjistíme, že $1 = 101 - 5 \cdot 20$, tedy $20^{-1} = (-5) \bmod 101 = 96$

Při určování hodnoty $2^{-1}$ můžeme udělat jednoduchou obecnou úvahu pro $\mathbf{Z}_p$, kde $p$ je liché prvočíslo, že $\frac{p+1}{2} \in \mathbf{Z}_p$ a že $(2 \cdot \frac{p+1}{2}) \bmod p = (p+1) \bmod p = 1$, tedy $2^{-1} = \frac{101+1}{2} = 51$ v tělese $\mathbf{Z}_{101}$.

Uvážíme-li, že z axiomatiky tělesa plyne $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ a $(-a)^{\cdot}(-b) = a \cdot b$ pro všechny jeho prvky $a$ a $b$ (zkuste podrobně dokázat!), a využijeme-li vypočítaných hodnot, pak

$$(20 \cdot_{101} 63)^{-1} = 20^{-1} \cdot_{101} 63^{-1} = (-5) \cdot_{101} (-8) = 40.$$

Protože obvyklý způsob upravovaní rovnic je ekvivalentní (tj. vratný) i pro rovnice nad obecným tělesem, zjišťujeme, že hledané $x$ je tvaru $x = 20^{-1} \cdot_{101} 7 = 96 \cdot_{101} 7 = 66$. □

**1.7.** Dokažte, pomocí Euklidova algoritmu, že $\mathbf{Z}_p$ spolu s operacemi $+_p$ a $\cdot_p$ splňuje axiom 8.

Uvažujeme stejným způsobem jako v předchozích úlohách. Zvolme libovolně nenulové $a \in \mathbf{Z}_p$. Protože $p$ je prvočíslo, jsou $a$ a $p$ nesoudělná, tedy pomocí Euklidova algoritmu lze najít celá $x$ a $y$, pro něž $ax + py = \mathrm{NSD}(a, p) = 1$. Nyní stačí vzít $a^{-1} = (x) \bmod p$. □

Nadále budeme sčítání a násobení v tělese $\mathbf{Z}_p$ psát bez indexu $_p$ (tj. jen $+$ a $\cdot$).

**1.8.** Spočítejte v tělesech $\mathbf{Z}_5$ a $\mathbf{Z}_7$ hodnotu výrazu $(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3$.

Postupujeme podle definice operací na $\mathbf{Z}_5$ i $\mathbf{Z}_7$, nejprve počítejme nad $\mathbf{Z}_5$:

$$(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3 = 3^{-1} \cdot (1 \cdot 3^{-1}) + 3 = 2 \cdot 2 + 3 = 2.$$

Podobně dostáváme nad $\mathbf{Z}_7$:

$$(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3 = 5^{-1} \cdot (6 \cdot 1^{-1}) + 3 = 3 \cdot 6 + 3 = 0.$$

□

**1.9.** Spočítejte v tělese komplexních čísel $\mathbf{C}$ hodnotu výrazů $(3+i)^{-1}$ a $(1-2i)^{-1} \cdot (2+3i)$.

Obvyklým způsobem rozšíříme zlomky komplexně sdruženou hodnotou a dostaneme

$$(3+i)^{-1} = \frac{1}{3+i} = \frac{1}{3+i} \cdot \frac{3-i}{3-i} = \frac{3}{10} - \frac{1}{10}i$$

a

$$(1-2i)^{-1} \cdot (2+3i) = \frac{2+3i}{1-2i} = \frac{2+3i}{1-2i} \cdot \frac{1+2i}{1+2i} = -\frac{4}{5} + \frac{7}{5}i.$$

□

*21.10.*

**1.10.** Najděte všechna reálná rešení soustavy rovnic:

$$\begin{array}{rcrcrcl} x & + & 2y & + & z & = & 1 \\ -2x & + & y & + & 2z & = & 2 \end{array}$$

Nejprve si soustavu zapíšeme do matice a poté ji pomocí přičtení vhodného násobku jedné rovnice k rovnici druhé upravíme (na střední škole se tento způsob upravování obvykle nazývá „sčítací metoda"):

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ -2 & 1 & 2 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 5 & 4 & 4 \end{array}\right),$$

Druhý řádek upravené matice, který odpovídá rovnici $5y + 4z = 4$, jsme dostali přičtením dvojnásobku rovnice $x + 2y + z = 1$ k rovnici $-2x + y + 2z = 2$ (tedy přičtením dvojnásobku řádku $\left(1 \quad 2 \quad 1 \,\middle|\, 1\right)$ k řádku $\left(-2 \quad 1 \quad 2 \,\middle|\, 2\right)$). Snadno si uvědomíme, že dosadíme-li za $z$ libovolnou hodnotu, pak jednoznačně dopočítáme $y$ a $x$. Položíme-li například $z = 0$, pak z rovnice $5y + 4 \cdot 0 = 4$ dostáváme, že $y = \frac{4}{5}$ a z rovnice $x + 2 \cdot \frac{4}{5} + 0 = 1$ spočítáme, že $x = -\frac{3}{5}$. Našli jsme tedy jedno řešení dané soustavy, které můžeme zapsat do trojice $(-\frac{3}{5}, \frac{4}{5}, 0)$.

Nyní si uvědomíme geometrický význam řešení dané soustavy: každou z rovnic chápeme jako rovinu v $\mathbf{R}^3$ (tvořenou všemi trojicemi $(x, y, z)$, které rovnici řeší) a množina řešení celé soustavy je průnik těchto dvou rovin. Všimneme-li si navíc, že roviny zjevně nejsou rovnoběžné, musí množinu všech řešení tvořit přímka, jejíž jeden bod $(-\frac{3}{5}, \frac{4}{5}, 0)$ už jsme našli. Nyní tedy zbývá najít „směrový vektor" této přímky, tedy vektor $\mathbf{v} = (v_1, v_2, v_3)$, pro nějž jsou právě body tvaru $(-\frac{3}{5}, \frac{4}{5}, 0) + t \cdot \mathbf{v}$, kde $t$ je libovolné reálné, všechny body hledané přímky. Připomeňme, že vektor $\mathbf{v}$ musí pro $(x, y, z) = (v_1, v_2, v_3)$ nutně řešit (homogenní) soustavu

$$\begin{array}{rcrcrcl} x & + & 2y & + & z & = & 0 \\ -2x & + & y & + & 2z & = & 0 \end{array}$$

Abychom to nahlédli, stačí uvážit jedno řešení $(x_0, y_0, z_0)$ původní (nehomogenní) soustavy, a potom další řešení tvaru $(x_0, y_0, z_0) + (v_1, v_2, v_3) = ((x_0 + v_1, y_0 + v_2, z_0 + v_3)$. Dosadíme-li obě řešení dostaneme

$$\begin{array}{rcrcrcl} x_0 & + & 2y_0 & + & z_0 & = & 1 \\ -2x_0 & + & y_0 & + & 2z_0 & = & 2 \end{array}$$

a

$$\begin{array}{rcrcrcl} x_0 + v_1 & + & 2(y_0 + v_2) & + & z_0 + v_3 & = & 1 \\ -2(x_0 + v_1) & + & y_0 + v_2 & + & 2(z_0 + v_3) & = & 2 \end{array}$$

Odečteme-li od sebe první rovnice a druhé rovnice, dostáváme

$$\begin{array}{rcrcrcl} v_1 & + & 2v_2 & + & v_3 & = & 0 \\ -2v_1 & + & v_2 & + & 2v_3 & = & 0 \end{array}$$

Budeme-li v maticovém zápisu řešit homogenní variantu naší rovnice, hodnoty levých stran se nezmění, zatímco pravé strany budou vždy nulové:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ -2 & 1 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 5 & 4 & 0 \end{array}\right),$$

I tentokrát stačí najít jedno řešení, jehož jsou všechna další násobkem, ovšem tentokrát nemůžeme za $z$ volit nulu, abychom našli nenulový směrový vektor. Položíme-li například $z = 1$, pak z rovnice $5y + 4 \cdot 1 = 0$ dostáváme, že $y = -\frac{4}{5}$ a z rovnice $x - 2 \cdot \frac{4}{5} + 1 = 0$ spočítáme, že $x = \frac{3}{5}$. Našli jsme tedy jedno řešení homogenní soustavy, které můžeme opět zapsat do trojice $(\frac{3}{5}, -\frac{4}{5}, 1)$.

Zjistili jsme, že množina všech řešení je přímka tvaru

$$\{(-\frac{3}{5}, \frac{4}{5}, 0) + t \cdot (\frac{3}{5}, -\frac{4}{5}, 1) |\ t \in \mathbf{R}\}.$$

□

**1.11.** Najděte všechna racionální rešení soustavy rovnic z úlohy 1.10.

Stačí si rozmyslet, že z množiny všech řešení předchozí úlohy musíme vybrat ta, která jsou ve všech složkách racionální. Zřejmě má řešení $(-\frac{3}{5}, \frac{4}{5}, 0)$ všechny složky racionální a hodnota $(-\frac{3}{5}, \frac{4}{5}, 0) + t \cdot (\frac{3}{5}, -\frac{4}{5}, 1)$ je racionální právě tehdy, když je racionální $t$. To znamená, že množina všech řešení je tentokrát tvaru

$$\{(-\frac{3}{5}, \frac{4}{5}, 0) + t \cdot (\frac{3}{5}, -\frac{4}{5}, 1) |\ t \in \mathbf{Q}\}.$$

□

**1.12.** Najděte rešení soustavy rovnic z úlohy 1.10 nad tělesem $\mathbf{Z}_5$.

Budeme postupovat stejným formalizmem jako v úloze 1.10. Snadno si uvědomíme, že ve skutečnosti stačí výslenou matici upravit modulo 5:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ -2 & 1 & 2 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 0 & 4 & 4 \end{array}\right),$$

Nyní nejprve opět najdeme jedno řešení nehomogenní soustavy. Z druhé rovnice nutně plyne, že $z = 0$ a dosadíme-li tentokrát $y = 0$ dopočítáme z první rovnice $x = 1$.

Nyní najdeme řešení homogenní soustavy s maticí

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ -2 & 1 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 0 \\ 0 & 0 & 4 & 0 \end{array}\right).$$

Vidíme, že nutně $z = 0$. Položímeli $y = 1$, potom z první rovnice dostaneme $x = 3$, protože $3+2\cdot 1+0 = 0$. Tedy množina všech řešení je tvaru $\{(1, 0, 0)+t\cdot(3, 1, 0) |\ t \in \mathbf{Z}_5\}$. □

## 2. Vektorové prostory a lineární nezávislost

**2.1.** Dokažte, že množina reálných polynomů jedné neurčité $\mathbf{R}[x]$ tvoří nad tělesem $\mathbf{R}$ vektorový prostor.

Stačí přímočaře ověřit platnost axiomatiky vektorového prostoru pro sčítání polynomů a pro násobení polynomu reálným číslem. □

**2.2.** Dokažte, že vektorový prostor $\mathbf{R}[x]$ není nad tělesem $\mathbf{R}$ konečné dimenze.

Předpokládejme, že $M$ je nějaká konečná množina polynomů a označme $m$ maximum ze stupňů polynomů v $M$. Potom polynom $x^{m+1}$ neleží v $\langle M\rangle$, tedy $\mathbf{R}[x]$ nemůže být konečné dimenze. □

**2.3.** Ověřte, že množina $X = \{x^i |\ i \geq 0\}$ tvoří bázi reálného vektorového prostoru $\mathbf{R}[x]$.

Zřejmě je každý polynom lineární kombinací (konečně mnoha) polynomů z $X$. Položíme-li nule nějakou lineární kombinaci $a_0x^0 + a_1x^1 + \cdots + a_nx^n = 0$, pak všechna $a_i = 0$, tedy přímo z definice vidíme, že $X$ je lineárně nezávislá množina. □

*4.11.*

**2.4.** Rozhodněte, zda je posloupnost vektorů $(1,1,0,1)$, $(2,1,1,1)$, $(3,1,2,1)$ z vektorového prostoru $\mathbf{R}^4$ nad tělesem $R$ lineárně závislá či nezávislá.

Potřebujeme zjistit, zda existuje nějaké netriviální (tj. nenulové) řešení vektorové rovnice

$$x_1 \cdot (1,1,0,1) + x_2 \cdot (2,1,1,1) + x_3 \cdot (3,1,2,1) = (0,0,0,0)$$

Snadno nahlédneme, že řešení dané vektorové rovnice jsou právě řešení homogenní soustavy rovnic s maticí levých stran $\mathbf{A}$ (pravé strany jsou nulové, u matice homogenní soustavy rovnic vynecháváme sloupec nulových pravých stran, který se žádnými úpravami nemění). Tu následně obvyklým způsobem upravujeme:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 1 & 2 \\ 0 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Aniž musíme nenulové řešení dopočítávat, ale zjevně jím jsou všechny násobky vektoru $(1,-2,1)$, zjišťujeme, že homogenní soustava rovnic s maticí $\mathbf{A}$, a tudíž i výše uvedená vektorová rovnice mají netriviální řešení, a proto jsou přímo podle definice vektory $(1,1,0,1)$, $(2,1,1,1)$, $(3,1,2,1)$ lineárně závislé. □

**2.5.** Rozhodněte, zda je posloupnost vektorů $(1,0,2,1)$, $(2,0,1,1)$, $(1,0,1,-1)$ ve vektorovém prostoru $\mathbf{Q}^4$ nad tělesem $\mathbf{Q}$ lineárně závislá či nezávislá.

Stejně jako v předchozí úloze se ptáme, zda existuje, a v takovém případě půjde o lineárně závislé vektory, či neexistuje, což by znamenalo, že dané vektory by byli lineárně nezávislé, netriviální řešení vektorové rovnice

$$x_1 \cdot (1,0,2,1) + x_2 \cdot (2,0,1,1) + x_3 \cdot (1,0,1,-1) = (0,0,0,0)$$

Úlohu převedeme na otázku, zda existuje jednoznačné (tedy pouze triviální) řešení homogenní soustavy rovnic s maticí $\mathbf{A}$:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & -3 & -1 \\ 0 & -1 & -2 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{pmatrix}$$

Z upravené soustavy dostáváme jednoznačné řešení $x_1 = x_2 = x_3 = 0$, tedy vektory $(1,0,2,1)$, $(2,0,1,1)$, $(1,0,1,-1)$ jsou lineárně nezávislé. □

**2.6.** Najděte nějakou bázi podprostoru $V$ vektorového prostoru $\mathbf{R}^4$ generovaného vektory $(1,1,0,1)$, $(2,1,1,1)$, $(-1,1,2,0)$, $(0,1,3,0)$, $(3,1,2,1)$ a určete dimenzi $V$.

Připomeňme, že elementární úpravy provedené na posloupnost vektorů nezmění podprostor jimi generovaný. Sepíšeme-li si tedy generátory prostoru V do řádků matice a matici budeme obvyklým způsobem upravovat, budou řádky upravené matice generovat stejný vektorový prostor V. Upravíme-li řádky matice tak, aby výsledné nenulové řádky (které můžeme v souladu s pozorováním o podprostorech generovaných řádky vypustit) byly zjevně lineárně nezávislé, budou tyto nenulové řádky tvořit bázi daného prostoru. Tedy upravujme:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 1 \\ -1 & 1 & 2 & 0 \\ 0 & 1 & 3 & 0 \\ 3 & 1 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -1 \\ 0 & 2 & 2 & 1 \\ 0 & 1 & 3 & 0 \\ 0 & -2 & 2 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -1 \\ 0 & 0 & 4 & -1 \\ 0 & 0 & 4 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & -1 & 1 & -1 \\ 0 & 0 & 4 & -1 \end{pmatrix}.$$

Vektory $(1,1,0,1)$, $(0,-1,1,-1)$, $(0,0,4,-1)$ jsou lineárně nezávislé, protože jsou uspořádány do odstupňované matice, a navíc generují celý prostor $V$, proto je posloupnost $(1,1,0,1)$, $(0,-1,1,-1)$, $(0,0,4,-1)$ bází $V$.

Protože je dimenze definována jako počet prvků (libovolné) báze, máme $\dim(V) = 3$. □

**2.7.** Vyberte z množiny $X = \{(2,4,0,1,4), (4,3,0,2,3), (1,2,3,4,0), (3,1,1,1,2), (4,3,4,0,2)\}$ bázi podprostoru $U = \langle X \rangle$ vektorového prostoru $\mathbf{Z}_5^5$ nad tělesem $\mathbf{Z}_5$.

Stačí si uvědomit, které vektory z daného seznamu jsou lineární kombinací předchozích. Seřadíme-li si vektory postupně do řádků matice, kterou upravíme posloupností elementárních úprav na ostupňovaný tvar (například nejprve přičteme vhodné násobky prvního řádku k ostatním a poté přehodíme druhý a třetí řádek, jímž stejným způsobem vynulujeme pátý a šestý řádek), stačí zjistit, kterým řádkům původní matice odpovídají nenulové řádky odstupňované matice. Řádky původní matice si označíme římskými číslicemi a budeme zaznamenávat všechna přehazování řádků:

$$\left(\begin{array}{ccccc|c} 2 & 4 & 0 & 1 & 4 & i \\ 4 & 3 & 0 & 2 & 3 & ii \\ 1 & 2 & 3 & 4 & 0 & iii \\ 3 & 1 & 1 & 1 & 2 & iv \\ 4 & 3 & 4 & 0 & 2 & v \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 4 & 0 & 1 & 4 & i \\ 0 & 0 & 0 & 0 & 0 & ii \\ 0 & 0 & 3 & 1 & 3 & iii \\ 0 & 0 & 1 & 2 & 1 & iv \\ 0 & 0 & 4 & 3 & 4 & v \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 4 & 0 & 1 & 4 & i \\ 0 & 0 & 3 & 1 & 3 & iii \\ 0 & 0 & 0 & 0 & 0 & ii \\ 0 & 0 & 0 & 0 & 0 & iv \\ 0 & 0 & 0 & 0 & 0 & v \end{array}\right).$$

Ukázalo se, že řádek ii je násobkem řádku i a řádky iv a v jsou lineární kombinací řádků i a iii. Naopak řádek iii není lineární kombinací řádku i. Hledanou bázi tvoří například první a třetí vektor množiny $X$, tedy množina $\{(2,4,0,1,4), (1,2,3,4,0)\}$. □

**2.8.** Doplňte lineárně nezávislou posloupnost $B = ((2,4,0,1,4), (1,2,1,0,3))$ na bázi aritmetického vektorového prostoru $\mathbf{Z}_5^5$.

Nejprve najdeme bázi podprostoru $\langle B \rangle$ tak, aby její vektory uspořádané do matice daly Gaussovu (tj. odstupňovanou) matici.

$$\begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 1 & 2 & 1 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix}.$$

Nyní snadno doplníme matici na odstupňovanou čtvercovou matici, jejíž všechny řádky jsou nenulové, například vektory kanonické báze (i-tý přidáme, právě když i-tý sloupec matice neobsahuje pivot) a přitom si všimneme, že:

$$\begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 1 & 2 & 1 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \mathbf{A}.$$

Zřejmě má podprostor generovaný řádky matice $\mathbf{A}$ dimenzi 5, proto je podle Věty 2.22 z přednášky roven $\mathbf{Z}_5^5$. Tedy posloupnost $((2,4,0,1,4),(1,2,1,0,3),(0,1,0,0,0),$ $(0,0,0,1,0),(0,0,0,0,1))$ tvoří bázi $\mathbf{Z}_5^5$ rozšiřující posloupnost $B$.

$\square$

**Další úlohy**

(1) Spočítejte v tělese $\mathbf{Z}_{83}$ hodnoty $15^{-1}$ a $(3^{-1} + 6 \cdot 53^{-1})^{-1}$.

(2) Vyřešte v tělese $\mathbf{Z}_{97}$ rovnici $7^{-1} \cdot x = 51^{-1}$.

(3) Dokažte, že pro všechny prvky $a$, $b$ obecného tělesa platí $-(a \cdot b) = -a \cdot b = a \cdot (-b)$, $-(a)^{-1} = (-a)^{-1}$, $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ a $(-a)^{\cdot}(-b) = a \cdot b$.

(4) Najděte nad tělesy $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{Z}_3$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$ všechna rešení soustavy rovnic:

$$\begin{array}{rcrcrcl} 2x & - & y & + & 2z & = & 1 \\ x & + & y & - & z & = & 1 \end{array}$$

(5) Najděte všechna komplexní řešení soustavy rovnic:

$$\begin{array}{rcrcrcl} ix & - & 2y & + & z & = & 1-i \\ x & + & (1+i)y & - & (2+3i)z & = & i \end{array}$$

(6) Najděte nad tělesy $\mathbf{Z}_5$ a $\mathbf{Z}_7$ aspoň tři řešení soustavy rovnic:

$$\begin{array}{rcrcrcrcl} x & + & y & + & z & + & u & = & 3 \\ x & + & 2y & + & 3z & + & 4u & = & 0 \\ x & + & 4y & & & & & = & 0 \end{array}$$

(7) Určete dimenzi vektorového prostoru komplexních čísel $\mathbf{C}$ nad tělesem $\mathbf{R}$.

(8) Dokažte, že vektorový prostoru reálných čísel $\mathbf{R}$ nad tělesem racionálních čísel $\mathbf{Q}$ není konečné dimenze.

(9) Rozhodněte, zda je posloupnost vektorů $(1,3,2,1)$, $(3,0,1,1)$, $(1,4,2,4)$ lineárně závislá ve vektorovém prostorech $\mathbf{R}^4$, $\mathbf{C}^4$, $\mathbf{Z}_5^4$ a $\mathbf{Z}_7^4$.

(10) Najděte nějakou bázi a určete dimenzi podprostoru $\langle(1,3,2,1)$, $(3,0,1,1)$, $(1,4,2,4)\rangle$ vektorových prostorů $\mathbf{R}^4$, $\mathbf{C}^4$, $\mathbf{Z}_5^4$ a $\mathbf{Z}_7^4$.

(11) Najděte všechny podmnožiny množiny vektorů $X = \{(1,2,1,1,1),(3,1,3,3,3),$ $(2,4,2,2,2)$, $(1,0,1,3,2)\}$, které tvoří bázi podprostoru $U = \langle X\rangle$ vektorových prostorů $\mathbf{Q}^5$, $\mathbf{Z}_5^5$, $\mathbf{Z}_7^5$.

(12) Kolik existuje bází podprostoru $\langle(1,1,2,0)$, $(4,1,3,1)$, $(1,3,2,1)\rangle$ vektorových prostorů $\mathbf{Z}_5^4$ a $\mathbf{Z}_7^4$?

(13) Kolika způsoby lze lineárně nezávislou posloupnost $((1,2,2,1)$, $(2,1,1,0))$ doplnit na bázi (chapanou jako posloupnost, tj. záleží na pořadí prvků) vektorového prostoru $\mathbf{Z}_3^4$?