1 Binárne operácie

Úloha 1.1. Vypíšte všetky možné binárne operácie na množine $\{0,1\}$. Ktoré z nich sú asociatívne, komutatívne, majú neutrálny prvok? Pre ktoré existuje ku každému prvku aj inverzný?

Úloha 1.2. Dokážte, že ak $\circ$ je binárna operácia na množine A a $\circ$ je asociatívna, tak ľubovoľné uzátvorkovanie výrazu $a \circ b \circ c \circ d$ predstavuje ten istý prvok.[1]

Úloha 1.3. Na $\mathbb{R}$ definujme binárnu operáciu $*$ predpisom $x * y = x \cdot y^2$ (kde $\cdot$ je násobenie reálnych čísel). Má táto operácia neutrálny prvok? Ak má, nájdite ho. Je operácia $*$ asociatívna? Je komutatívna?

Úloha 1.4. Pre dve reálne čísla a, b definujme

$$a * b = \frac{a+b}{2},$$

t.j. výsledkom je ich priemer. Je to binárna operácia na $\mathbb{R}$? Je táto operácia komutatívna? Je asociatívna? Má neutrálny prvok?

Úloha 1.5*. Ak viete, že ide o tabuľku asociatívnej binárnej operácie, doplňte chýbajúce výsledky (ak sa to dá).

	a	b	c
a	b	a	c
b			
c			

2 Grupy

$(G, *)$ je grupa, ak $*$ je binárna operácia na G a ďalej platí: Binárna operácia $*$ je asociatívna (A). V G existuje neutrálny prvok pre túto operáciu (N). Pre každý prvok z G existuje inverzný prvok (I).

$$(\forall a, b, c \in G) a * (b * c) = (a * b) * c \tag{A}$$
$$(\exists e \in G)(\forall a \in G) a * e = e * a = e \tag{N}$$
$$(\forall a \in G)(\exists b \in G) a * b = b * a = e \tag{I}$$

O komutatívnej grupe (abelovskej grupe) hovoríme, ak operácia $*$ je navyše komutatívna.

$$(\forall a, b \in G) a * b = b * a \tag{K}$$

Úloha 2.1. Ktoré z uvedených množín tvoria vzhľadom na dané operácie grupu? V ktorých prípadoch je táto grupa komutatívna?
a) $(\mathbb{Z}, \cdot)$ (celé čísla s obvyklým násobením)
b) $(\mathbb{R}, \cdot)$ (reálne čísla s obvyklým násobením)
c) $(\mathbb{R} \setminus \{0\}, \cdot)$, d) $(\mathbb{C}, +)$, e) $(\mathbb{C}, \cdot)$, f) $(\mathbb{C} \setminus \{0\}, \cdot)$
g) $(\mathbb{R}^2, +)$ (so sčitovaním definovaným po zložkách)
h) $\mathbb{R}$ s operáciou $*$, $a * b = a + b - 1$
i) $\mathbb{R}$ s operáciou $*$, $a * b = ab + a + b$

[1] Máme tu na mysli uzátvorkovania *bez výmeny poradia,* ktoré už jednoznačne určujú výsledok operácie. Aspoň bez dôkazu spomeniem, že to isté platí aj pre ľubovoľný počet prvkov. Počet uzátvorkovaní výrazu s n prvkami je n-té *Catalanove číslo.*

j) $\mathbb{R} \setminus \{-1\}$ s operáciou $*$, $a * b = ab + a + b$
k) Množina všetkých párnych celých čísel vzhľadom na sčitovanie.
l) Množina všetkých nepárnych celých čísel vzhľadom na sčitovanie.
m) $(\mathbb{Z}_5, \oplus)$
(Pozri aj úlohu 2.2 – táto úloha sú v postate inak sformulované časti i) a j).)

Úloha 2.2. Je $(\mathbb{R}, *)$, kde $a * b = ab + a + b$, grupa? Ak nie, vedeli by ste vynechať niektorý prvok a z množiny $\mathbb{R}$ tak, aby $(\mathbb{R} \setminus \{a\}, *)$ bola grupa?

V úlohách 2.3, 2.4 a 2.15 vidíme príklady grúp, ktoré nie sú komutatívne.

Úloha 2.3. Tvoria všetky permutácie na konečnej množine M s operáciou skladania zobrazení grupu? Je táto grupa komutatívna? Urobte tabuľku grupovej operácie v prípade $M = \{1, 2, 3\}$.

Tabuľka grupy $(S_3, \circ)$:

	id	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
id	id	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	id	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	id	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	id	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	id
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	id	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

Úloha 2.4. Nech G je množina všetkých funkcií $f_{a,b} \colon \mathbb{R} \to \mathbb{R}$, ktoré sú tvaru $f_{a,b}(x) = ax + b$ pre nejaké reálne čísla $a, b \in \mathbb{R}$. Tvorí táto množina funkcií s operáciou skladania zobrazení grupu? Je množina $\{f_{a,b}; a, b \in \mathbb{R}, a \neq 0\}$ s operáciou skladania zobrazení grupa? Dostaneme grupu, ak vezmeme len také $a, b \in \mathbb{R}$, že $a = 1$? V tých prípadoch, keď dostaneme grupu, je táto grupa komutatívna?

Úloha 2.5. Ak $(G, \circ)$ je grupa a $a \in G$ je nejaký jej prvok, tak zobrazenie $f_a \colon G \to G$ definované ako $f_a(x) = a \circ x$ je bijekcia.

Úloha 2.6. Nech $(G, \circ)$ je grupa. Dokážte, že zobrazenie $f \colon G \to G$ definované ako $f(x) = x^{-1}$ je bijekcia.

Úloha 2.7*. Nech G je neprázdna množina a $\circ$ je asociatívna binárna operácia na G. Potom G je grupa práve vtedy, keď pre ľubovoľné $a, b \in G$ majú rovnice

$$a \circ x = b$$
$$y \circ a = b$$

riešenie v G (inými slovami, pre ľubovoľné $a, b \in G$ existujú $x, y \in G$, ktoré spĺňajú tieto dve rovnosti.)

Úloha 2.8*. Nech G je konečná množina a $\circ$ je binárna operácia na G taká, že platí asociatívny zákon a zákony o krátení. Dokážte, že G je grupa.

Úloha 2.9*. Dokážte, že v konečnej grupe, ktorá má párny počet prvkov, existuje prvok rôzny od neutrálneho prvku taký, že $a \circ a = e$.

Úloha 2.10. Nech konečná množina $G = \{e, a_1, \ldots, a_n\}$ tvorí s operáciou $*$ komutatívnu grupu a e je jej neutrálny prvok. Dokážte, že $(a_1 * a_2 * \cdots * a_n)^2 = e$.

Úloha 2.11. Nech $*$ je binárna operácia na množine A, taká, že pre každé $a, b, c \in A$ platí $a * (b * c) = (a * c) * b$ a $*$ má neutrálny prvok. Dokážte, že operácia $*$ je komutatívna a asociatívna.

Úloha 2.12. Nech $(G, \circ)$ je grupa. Dokážte, že ak $x \circ x = x$, tak $x = e$.

Úloha 2.13. Overte, že $G \times H$ spolu s operáciou $*$ definovanou ako

$$(a, b) * (a', b') = (a *_G a', b *_H b')$$

tvorí grupu pre ľubovoľné grupy $(G, *_G)$ a $(H, *_H)$.

Úloha 2.14. Zistite, či $(\mathbb{R}^+ \times \mathbb{R}, \square)$, kde pre každé $(a, b), (c, d) \in \mathbb{R}^+ \times \mathbb{R}$ definujeme $(a, b)\square(c, d) = (2ac, b + d)$, je grupa. (Môžete sa zamyslieť aj nad tým, či vám riešenie tejto úlohy nezjednoduší, ak už poznáte výsledok z úlohy 2.13.)

Úloha 2.15. Nech $G = \mathbb{R} \times (\mathbb{R} \setminus \{0\})$. Definujme na tejto množine binárnu operáciu $*$ predpisom $(a, b) * (c, d) = (a + bc, bd)$. Je to skutočne binárna operácia? Je $(G, *)$ grupa? Je to komutatívna grupa?

V súvislosti s úlohami 2.4 a 2.15 sa môžete zamyslieť aj nad tým, či tieto dve grupy nejako nazvájom súvisia.

Úloha 2.16. Doplňte nasledujúcu tabuľku

	a	b	c	d
a				
b				d
c			d	
d				

tak aby ste dostali grupu.

Úloha 2.17. Ak pre každý prvok x grupy $(G, \circ)$ platí $x \circ x = e$, tak táto grupa je komutatívna.

Úloha 2.18. Je množina $\mathbb{Q}$ s operáciou $\triangleleft$ definovanou ako $a \triangleleft b = ab - a$ grupa? Je táto operácia komutatívna? Má ľavý neutrálny prvok? Má pravý neutrálny prvok?

Úloha 2.19. Nech $*$ je asociatívna binárna operácia na množine M, ktorá má neutrálny prvok e. Ak pre nejaké $x \in M$ platí $x * x = x$ a ku x existuje ľavý inverzný prvok, tak $x = e$.

Úloha 2.20*. Nech $*$ je binárna operácia na množine G, ktorá
a) je asociatívna,
b) má ľavý neutrálny prvok t.j. existuje prvok $e \in G$ taký, že $(\forall x \in G)e * x = x$
c) pre každý prvok $x \in G$ existuje $y \in G$ také, že $y * x = e$ (kde e označuje prvok z časti b) t.j.

$$(\forall x \in G)(\exists y \in G)y * x = e$$

(stručne môžeme povedať, že ku každému prvku existuje ľavý inverzný prvok vzhľadom na e).
Dokážte, že potom $(G, *)$ je grupa.

Úloha 2.21. Nech G je konečná grupa, $|G| = n$. Neutrálny prvok tejto grupy označme e a jej prvky označme ako $a_1, \ldots, a_n$ (t.j. $G = \{a_1, \ldots, a_n\}$).
a) Ukážte, že pre ľubovoľné $a \in G$ platí $G = \{aa_1, \ldots, aa_n\}$.
b) Predpokladajme, že G je navyše aj komutatívna grupa. Ukážte, že pre ľubovoľné $a \in G$ platí $a^n = e$.
(Poznámka: Takéto tvrdenie platí aj pre nekomutatívnej grupy – v tom prípade ale treba použiť iný argument. Dá sa to odvodiť napríklad ako dôsledok Lagrangeovej vety.)

Do istej miery podobnými úvahami ako v predošlej úlohe sa dá prísť aj na takéto tvrdenie:

Úloha 2.22. Nech G je konečná n-prvková množina, jej prvky označme ako $a_1, \ldots, a_n$ (t.j. $G = \{a_1, \ldots, a_n\}$). Nech ďalej $*$ je binárna operácia na G, ktorá má neutrálny prvok e, je asociatívna, komutatívna a platia pre ňu zákony o krátení.
a) Ukážte, že pre ľubovoľné $a \in G$ platí $G = \{aa_1, \ldots, aa_n\}$.
b) Ukážte, že pre ľubovoľné $a \in G$ platí $a^n = e$.
(Poznámka: Z rovnosti $a^n = e$ vieme vyčítať to, že ku e existuje inverzný prvok.)

1 Polia

Množina F s binárnymi operáciami $+$ a $\cdot$ tvorí pole, ak:

(i) $(F, +)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 0;

(ii) $(F \setminus \{0\}, \cdot)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 1;

(iii) pre ľubovoľné $a, b, c \in F$ platí

$$a(b + c) = ab + ac,$$
$$(a + b)c = ac + bc.$$

(Túto vlastnosť nazývame *distributívnosť*.)

Ekvivalentne môžeme túto definíciu prepísať pomocou takýchto podmienok:

(i) pre všetky $a, b, c \in F$ platí $a + (b + c) = (a + b) + c$,

(ii) pre všetky $a, b \in F$ platí $a + b = b + a$,

(iii) existuje prvok $0 \in F$ taký, že pre každé $a \in F$ sa $a + 0 = a$,

(iv) ku každému $a \in F$ existuje $b \in F$ tak, že $a + b = 0$,

(v) pre všetky $a, b, c \in F$ platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

(vi) pre všetky $a, b \in F$ platí $a \cdot b = b \cdot a$,

(vii) existuje prvok $1 \in F$ taký, že $1 \neq 0$ a pre každé $a \in F$ sa $a \cdot 1 = a$,

(viii) ku každému $a \in F$, $a \neq 0$ existuje $b \in F$ tak, že $a \cdot b = 1$,

(ix) pre všetky $a, b, c \in F$ sa $a \cdot (b + c) = a \cdot b + a \cdot c$.

Úloha 1.1. Ktoré z uvedených množín tvoria spolu s obvyklým sčitovaním a násobením pole?
a) $F = \{a + ib; a \in \mathbb{R}, b \in \mathbb{R}, b \geq 0\}$
b) $F = \{a + ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
c) $F = \{a + ib; a \in \mathbb{Z}, b \in \mathbb{Z}\}$
d) $F = \{a + b\sqrt{2}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
e) $F = \{a + b\sqrt{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
f) $F = \{a + \sqrt{3}ib; a \in \mathbb{Q}, b \in \mathbb{Q}\}$
g) $F = \{a + \frac{b}{\sqrt{2}}; a, b \in \mathbb{Q}\}$
h*) $F = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}; a, b, c, d \in \mathbb{Q}\}$ (Hint: Možno pomôže prepísať si túto množinu do tvaru $F = \{a + b\sqrt{3}; a, b \in F'\}$, kde $F' = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$.)
i*) $F = \{a + b\sqrt{2} + c\sqrt{3}; a, b, c \in \mathbb{Q}\}$
j*) $F = \{a + b\sqrt[3]{5}; a \in \mathbb{Q}, b \in \mathbb{Q}\}$

Pri úlohe o $F = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ môže byť užitočné zamyslieť sa najprv nad tým, či vieme zdôvodniť, že pre $a, b \in \mathbb{Q}$ platí:

$$a + b\sqrt{2} = 0 \qquad \Leftrightarrow \qquad a = b = 0.$$

(Platilo by to aj bez predpokladu, že a, b sú racionálne?)

Tiež si môžeme uvedomiť, že potom pre $a, b, a', b' \in \mathbb{Q}$ už ľahko dostaneme

$$a + b\sqrt{2} = a' + b'\sqrt{2} \qquad \Leftrightarrow \qquad a = a' \wedge b = b'.$$

Úloha 1.2. Na $\mathbb{Q} \times \mathbb{Q}$ definujeme operácie + a · takto:
a) $(a,b)+(c,d) = (a+c, b+d)$ a $(a,b)\cdot(c,d) = (ac+3bd, ad+bc)$,
b) $(a,b)+(c,d) = (a+c, b+d)$ a $(a,b)\cdot(c,d) = (ac+2bd, ad+bc)$.
c) $(a,b)+(c,d) = (a+c, b+d)$ a $(a,b)\cdot(c,d) = (ac-5bd, ad+bc)$.
Je potom $(\mathbb{R}\times\mathbb{R}, +, \cdot)$ pole?

Úloha 1.3. V poli $\mathbb{Z}_5$ vyrátajte $2^{-1} \oplus 4$, $(-2) \oplus 4$, $2^{-1} \odot 3$ a $-4 \odot 3^{-1}$.

Úloha 1.4. V $\mathbb{Z}_5$ vyrátajte 2^3, $(2^{-1})^4$, $2 \odot (4^{-1})^3$, $(4 \odot 2^{-1})^3$, $(-1)^5 \odot (4 \odot 3^{-1})^2$.

Úloha 1.5. V ľubovoľnom poli F platí:

$$a+b = a+c \Rightarrow b = c$$
$$(a+b)(c+d) = ac+ad+bc+bd$$
$$-(-a) = a$$
$$-0 = 0$$
$$-(a+b) = (-a)+(-b)$$
$$(a-b)c = ac-bc$$
$$1 \neq 0$$
$$a\cdot a = 1 \Leftrightarrow a = 1 \vee a = -1$$
$$a^2 = b^2 \Leftrightarrow a = b \vee a = -b$$
$$a\cdot(b_1+\ldots+b_n) = a\cdot b_1+\ldots+a\cdot b_n$$

Úloha 1.6. Na množine $\mathbb{R}^+$ všetkých kladných reálnych čísel zadefinujme operácie $\oplus$ a $\odot$ tak, že $x \oplus y = x \cdot y$ a $x \odot y = x^y$. Ktoré z axióm poľa spĺňa $(\mathbb{R}^+, \oplus, \odot)$? (Pričom $x \cdot y$ označuje obvyklé násobenie a x^y obvyklé umocňovanie.)

Úloha 1.7. Nech F je pole a $a \in F$. Definujeme zobrazenie $f_a \colon F \to F$ tak, že $f_a(b) = a+b$. Je f_a bijekcia? Ak áno, ako vyzerá zobrazenie f_a^{-1}? Čomu sa rovná $f_a \circ f_b$?

Ďalej definujeme $g_a \colon F \to F$ pre $a \neq 0$ tak, že $g_a(b) = a \cdot b$. Je to bijekcia?

Úloha 1.8. Nech na množine $M = \{0,1\}$ sú operácie + a · dané tabuľkami

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	1	1

Ukážte, že $(M,+)$ a $(M\setminus\{0\}, \cdot)$ sú komutatívne grupy a že platí distributívny zákon $(a+b)c = ac+bc$. Je $(M,+,\cdot)$ pole?

Úloha 1.9. Zistite, či $(\mathbb{R}, +, *)$, kde + je obvyklé sčitovanie reálnych čísel a pre každé $a, b \in \mathbb{R}$ $a * b = -2ab$, je pole.

Úloha 1.10*. Pre ktoré prvky a poľa $\mathbb{Z}_7$ má riešenie rovnica $x^2 = a$? Koľko je takých prvkov v poli $\mathbb{Z}_{109}$?

Úloha 1.11*. Dokážte, že:
a) V ľubovoľnom poli platí $(a+b)^m = a^m + \binom{m}{1} \times a^{m-1}b + \binom{m}{2} \times a^{m-2}b^2 + \ldots + \binom{m}{m-1} ab^{m-1} + b^m$. (Súčet na pravej strane sa zvykne označovať takto: $\sum_{k=0}^{m} \binom{m}{k} \times a^{m-k}b^k$.)
b) V poli $\mathbb{Z}_p$ platí: $(a \oplus b)^p = a^p \oplus b^p$.

Úloha 1.12*. Pomocou úlohy 1.11 dokážte matematickou indukciou vzhľadom na a, že v $\mathbb{Z}_p$ platí rovnosť $a^p = a$ (pre ľubovoľné $a \in \mathbb{Z}_p$). (Toto je vlastne iná formulácia malej Fermatovej vety.)

Úloha 1.13. Nech F je konečné pole a platí $|F| = n$. Ukážte, že potom pre každý prvok $a \in F \setminus \{0\}$ platí $a^{n-1} = 1$. (Týmto sme súčasne získali aj iné odvodenie malej Fermatovej vety.)

Úloha 1.14. Majme štvorprvkovú množinu $F = \{0, 1, a, b\}$ a binárne operácie $+, \cdot$ na tejto množine. Ak viete, že $(F, +, \cdot)$ je pole, tak doplňte zvyšok zadaných tabuliek:

$+$	0	1	a	b
0	0	1	a	b
1		0		
a			0	
b				0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a				
b				

T.j. v tabuľkách máme zadané, že $0 + x = x$ a $x + x = 0$ pre všetky $x \in F$. A tiež to, že $0 \cdot x = 0$ a $1 \cdot x = 1$ pre všetky $x \in F$.

Zdôvodnite, prečo váš výsledok je jediná možnosť, ako sa tieto tabuľky dajú doplniť. (To, či na konci naozaj vyšlo pole, overovať nemusíte.)

Poznámka. Jeden z dôvodov, prečo som pridal takýto príklad, je ukázať, že existuje aj štvorprvkové pole. (Z konečných polí ste sa zatiaľ stretli s poľami, ktoré majú prvočíselný počet prvkov. Neskôr sa na Algebre 3 dozviete, že existujú aj iné konečné polia a aj to ako všetky také polia vyzerajú. Z toho, čo sa naučíte tam, sa štvorprkové pole bude dať dostať oveľa jednoduchšie – tu vlastne máme zadanú tabuľku sčitovania a násobenia, ale nevieme, prečo sme ich zobrali akurát takéto.)

1 Vektorové priestory

Definícia 1.1. Nech F je pole a $V \neq \emptyset$ je množina. Nech $+$ je binárna operácia na V a každej dvojici $c \in F$, $\vec{\alpha} \in V$ je priradený prvok $c \cdot \vec{\alpha} \in V$, pričom platí pre ľubovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$:

(i) $(V, +)$ je komutatívna grupa,

(ii) $c \cdot (\vec{\alpha} + \vec{\beta}) = c \cdot \vec{\alpha} + c \cdot \vec{\beta}$,

(iii) $(c + d) \cdot \vec{\alpha} = c \cdot \vec{\alpha} + d \cdot \vec{\alpha}$,

(iv) $(c \cdot d) \cdot \vec{\alpha} = c \cdot (d \cdot \vec{\alpha})$,

(v) $1 \cdot \vec{\alpha} = \vec{\alpha}$.

Potom hovoríme, že V je *vektorový priestor* nad poľom F.

Označenie: $\vec{0}$ = nulový vektor, $-\vec{x}$ = opačný vektor

Príklady vektorových priestorov, ktoré poznáme z prednášky: F^n (usporiadané n-ties) aj F^M (zobrazenia z M do F) sú vektorové priestory nad poľom F.

Úloha 1.2. Koľko prvkov má vektorový priestor $(\mathbb{Z}_3)^n$? Čomu sa v tomto priestore rovná $\vec{\alpha} + \vec{\alpha} + \vec{\alpha}$?

Úloha 1.3. Nech V je množina všetkých postupností reálnych čísel. Pre postupnosti $a = (a_n)_{n=1}^{\infty}$ a $b = (b_n)_{n=1}^{\infty}$ definujeme $a + b = (a_n + b_n)_{n=1}^{\infty}$ a $c \cdot a = (c \cdot a_n)_{n=1}^{\infty}$. Overte, že V s týmito operáciami tvorí vektorový priestor nad poľom $\mathbb{R}$.

Úloha 1.4. Overte, že všetky zobrazenia $f\colon \langle 0, 1\rangle \to \mathbb{R}$ so sčitovaním a násobením skalárom definovaným po bodoch tvoria vektorový priestor nad poľom $\mathbb{R}$.

Úloha 1.5. Overte, že $\mathbb{R}$ je vektorový priestor nad $\mathbb{Q}$, $\mathbb{C}$ je vektorový priestor nad $\mathbb{R}$, $\mathbb{C}$ je vektorový priestor nad $\mathbb{Q}$. Je $\mathbb{C}$ vektorový priestor nad $\mathbb{Z}$?

Úloha 1.6. Zistite, či $\mathbb{R} \times \mathbb{R}$ s operáciami $+$ a $\cdot$ definovanými tak, že $(a, b) + (c, d) = (a + c, b + d)$ pre ľubovoľné $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$ a $r \cdot (a, b) = (ra, 2rb)$ pre ľubovoľné $r \in \mathbb{R}$, je vektorový priestor nad $\mathbb{R}$.

Úloha 1.7. Zistite, či $(\mathbb{R}^+, \oplus, \odot)$ je vektorový priestor nad $\mathbb{R}$, ak definujeme $x \oplus y = xy$, $c \odot x = x^c$ pre $x, y \in \mathbb{R}^+$, $c \in \mathbb{R}$.

2 Podpriestory

Ak V je vektorový priestor nad poľom F, $S \neq \emptyset$ a $S \subseteq V$, tak S je *vektorovým podpriestorom* priestoru V, ak

(i) pre ľubovoľné $\vec{\alpha}, \vec{\beta} \in S$ platí $\vec{\alpha} + \vec{\beta} \in S$,

(ii) pre ľubovoľné $\vec{\alpha} \in S$ a $c \in F$ platí $c\vec{\alpha} \in S$.

Kritérium vektorového podpriestoru: Namiesto uvedených dvoch podmienok stačí overiť, že pre ľubovoľné $c, d \in F$ a $\vec{\alpha}, \vec{\beta} \in V$ platí

$$\vec{\alpha}, \vec{\beta} \in S \qquad \Rightarrow \qquad c\vec{\alpha} + d\vec{\beta} \in S. \tag{1}$$

(A ďalšia ekvivalentná charakterizácia podpriestorov je uvedená v úlohe 2.6.)

Podpriestor vektorového priestoru tiež tvorí vektorový priestor.

Každý podpriestor obsahuje nulový vektor.

Úloha 2.1. Ktoré z týchto množín tvoria vektorový podpriestor priestoru $\mathbb{R}^3$?
a) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 \in \mathbb{Z}\}$
b) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 = 0\}$
c) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 = 0 \vee x_2 = 0\}$
d) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; 3x_1 + 4x_2 = 1\}$
e) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; 7x_1 - x_2 = 0\}$
f) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 = x_3\}$
g) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; |x_1| = |x_2|\}$
h) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 + x_3 \geq 0\}$
i) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; 2x_1 = -x_2 = x_3\}$
j) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + x_2 + x_3 = 0\}$
k) $M = \{(x_1, x_2, x_3) \in \mathbb{R}^3; x_1 + 2x_2 + 3x_3 = 0, 3x_1 + 2x_2 + x_3 = 0\}$

Úloha 2.2. Ktoré z týchto podmnožín tvoria vektorový podpriestor priestoru reálnych funkcií $\mathbb{R}^{\mathbb{R}}$?
a) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ s vlastnosťou $2f(0) = f(1)$
b) nezáporné funkcie
c) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ s vlastnosťou $f(1) = 1 + f(0)$
d) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ s vlastnosťou $(\forall x \in \langle 0, 1\rangle) f(x) = f(1 - x)$
e) ohraničené funkcie $f\colon \mathbb{R} \to \mathbb{R}$
f) spojité funkcie $f\colon \mathbb{R} \to \mathbb{R}$
h) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ také, že existuje konečná $\lim\limits_{x\to\infty} f(x)$
i*) funkcie $f\colon \mathbb{R} \to \mathbb{R}$ také, že existuje konečná alebo nekonečná $\lim\limits_{x\to\infty} f(x)$.

Úloha 2.3. Overte, či
a) množina všetkých polynómov s reálnymi koeficientami,
b) množina všetkých polynómov s reálnymi koeficientami stupňa najviac n,
c) množina všetkých polynómov párneho stupňa,
d) množina všetkých polynómov stupňa práve n
sú vektorové priestory. Sčitovanie a násobenie skalárom definujeme rovnako ako pre reálne funkcie.

Úloha 2.4. Dokážte, že množina všetkých funkcií $f\colon \mathbb{R} \to \mathbb{R}$, ktoré sú tvaru $a+b\cos x+c\sin x$ pre nejaké $a, b, c \in \mathbb{R}$ tvoria vektorový podpriestor priestoru všetkých reálnych funkcií $\mathbb{R}^{\mathbb{R}}$.

Úloha 2.5. Nech S, T sú podpriestory vektorového priestoru V nad poľom F. Ukážte, že $S \cup T$ je podpriestor priestoru V práve vtedy, keď $S \subseteq T$ alebo $T \subseteq S$.

Úloha 2.6. Nech V je vektorový priestor nad poľom F a $S \neq \emptyset$ je podmnožina V. Ukážte, že S je podpriestor V práve vtedy, keď pre ľubovoľné $c \in F$ a $\vec{\alpha}, \vec{\beta} \in S$ platí $c\vec{\alpha} + \vec{\beta} \in S$.

[1]

1 Lineárne kombinácie, lineárny obal

$$[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] = \{c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n; c_i \in F \text{ pre } i = 1, 2 \ldots, n\}$$

Je užitočné si uvedomiť, že:

- Lineárny obal $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n]$ je najmenší podpriestor daného vektorového priestoru, ktorý obsahuje vektory $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n$.
- Teda ak S je podpriestor taký, že $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n \in S$, tak $[\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_n] \subseteq S$. (Toto je vlastne trochu inak sformulovaný fakt, že podpriestory sú uzavreté vzhľadom na lineárne kombinácie.)

Úloha 1.1. Nech $\vec{\alpha}, \vec{\beta}, \vec{\gamma}$ sú ľubovoľné vektory z vektorového priestoru V nad poľom $\mathbb{R}$. Potom $[\vec{\alpha}, \vec{\beta}, \vec{\gamma}] = [\vec{\alpha} + \vec{\beta}, \vec{\alpha} - \vec{\beta}, \vec{\gamma}]$.

Úloha 1.2. Nech $M = \{(x, y, z) \in \mathbb{R}^3; 2x + 3y + 5z = 0\}$. Ukážte, že M je vektorový podpriestor $\mathbb{R}^3$ a nájdite vektory, ktoré ho generujú.

2 Lineárna nezávislosť

Lineárne závislé vektory: Existujú $c_1, c_2, \ldots, c_n \in F$, ktoré nie sú všetky nulové a platí pre ne:

$$c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n = \vec{0}.$$

Lineárne nezávislé vektory:

$$c_1\vec{\alpha}_1 + c_2\vec{\alpha}_2 + \cdots + c_n\vec{\alpha}_n = \vec{0} \qquad \Rightarrow \qquad c_1 = c_2 = \ldots = c_n = 0$$

Nie je zlé si uvedomiť, ako to je s lineárnou závislosťou a nezávislosťou, ak máme jeden vektor resp. dva vektory.

Úloha 2.1. Množina $\{\vec{\alpha}\}$ je lineárne nezávislá práve vtedy, keď $\vec{\alpha} \neq \vec{0}$. Dva vektory $\vec{\alpha}, \vec{\beta}$ sú lineárne závislé práve vtedy, keď jeden z nich je násobkom druhého (t.j. existuje $c \in F$ tak, že $c.\vec{\alpha} = \vec{\beta}$), alebo jeden z nich je $\vec{0}$.

Ak vektory $\vec{\alpha}, \vec{\beta}$ sú lineárne nezávislé, tak $\vec{\alpha}, \vec{\beta}, \vec{\gamma}$ sú lineárne závislé práve vtedy, keď $\vec{\gamma}$ je lineárna kombinácia vektorov $\vec{\alpha}, \vec{\beta}$.

Úloha 2.2. Zistite, či dané vektory sú lineárne závislé v príslušnom vektorovom priestore:
a) (1,2,3), (1,3,2), (2,1,5) v $\mathbb{R}^3$,
b) (1,2,3), (1,3,2), (2,1,5), (1,127,3) v $\mathbb{R}^3$,
c) (1,3,4), (2,1,3), (3,1,4) v $\mathbb{Z}_5^3$
d) (1,3,4), (2,1,3), (3,1,4) v $\mathbb{Z}_7^3$.

V niektorých častiach nasledujúcej úlohye budeme využívať fakt, že polynóm sa rovná nule práve vtedy, keď všetky koeficienty sú nulové.[2] (Ale mali by sme ju vedieť vyriešiť aj bez neho.)

[1] TODO dám do tohto istého súboru aj veci na bázu a dimenziu?
[2] `https://msleziak.com/forum/viewtopic.php?t=1349`

Úloha 2.3. Zistite, či sú nasledujúce funkcie lineárne závislé vo vektorovom priestore všetkých funkcií z $\mathbb{R}$ do $\mathbb{R}$:
a) $x+1$, x^2, x^3,
b) 1, $x+a$, x^2+bx+c (a, b, c môžu byť ľubovoľné reálne čísla),
c*) 1, $\cos x$, $\cos^2(\frac{x}{2})$,
d) x, $x(x-1)$, $x(x-1)(x-2)$,
e) 1, $\cos x$, $\cos 2x$.

Úloha 2.4. Ak $\vec{\alpha}$, $\vec{\beta}$, $\vec{\gamma}$ sú lineárne nezávislé vo vektorovom priestore V nad poľom $\mathbb{R}$, tak aj $\vec{\alpha}+\vec{\beta}$, $\vec{\alpha}+\vec{\gamma}$, $\vec{\beta}+\vec{\gamma}$ sú lineárne nezávislé. (Platilo by to aj vo vektorovom priestore nad poľom $\mathbb{Z}_2$?)

Úloha 2.5*. Overte, že $\mathbb{R}$ je vektorový priestor nad poľom $\mathbb{Q}$. Dokážte, že v tomto priestore sú 1, $\sqrt{2}$ a $\sqrt{3}$ lineárne nezávislé. [3]

Úloha 2.6. Ukážte, že vo vektorovom priestore $\mathbb{R}$ nad $\mathbb{Q}$ (z predošlej úlohy) sú lineárne nezávislé vektory $1+3\sqrt{2}$ a $2-\sqrt{2}$.

Úloha 2.7*. Sú 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ lineárne nezávislé vo vektorovom priestore $\mathbb{R}$ nad poľom $\mathbb{Q}$? (Hint: Úlohu môže o niečo zjednodušiť, ak sa pozriete na 1 a $\sqrt{3}$ ako prvky priestoru $\mathbb{R}$ nad poľom $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{3}; a, b \in \mathbb{Q}\}$.) [4]

Úloha 2.8. Nech $\vec{\alpha}, \vec{\beta}, \vec{\gamma}$ sú ľubovoľné vektory. Zistite, či sú tieto systémy vektorov lineárne závislé:
a) $\vec{\alpha}, \vec{\beta}, \vec{\alpha}+\vec{\beta}, \vec{\gamma}$, b) $\vec{\alpha}, \vec{\beta}, \vec{0}$, c) $\vec{\alpha}, \vec{\alpha}, \vec{\beta}, \vec{\gamma}$, d) $\vec{\alpha}+\vec{\beta}+\vec{\gamma}, \vec{\alpha}+\vec{\beta}, \vec{\alpha}+\vec{\gamma}, \vec{\beta}+\vec{\gamma}$.

Úloha 2.9. Nech vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé vektory v nejakom vektorovom priestore nad poľom $\mathbb{R}$. Sú aj vektory $\vec{\alpha}_1, \vec{\alpha}_1+2\vec{\alpha}_2, \ldots, \vec{\alpha}_1+2\vec{\alpha}_2+\ldots+n\vec{\alpha}_n$ lineárne nezávislé?

[3] http://math.stackexchange.com/questions/557976/show-that-1-sqrt2-sqrt3-is-linearly-independent-over-mathbbq
[4] https://math.stackexchange.com/questions/96946/how-to-prove-1-sqrt2-sqrt3-and-sqrt6-are-linearly-independent-ove/

Báza a dimenzia

Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ tvoria bázu vektorového priestoru V, ak sú *lineárne nezávislé* a *generujú celý priestor*. Ekvivalentná podmienka: Každý vektor $\vec{\beta} \in V$ sa dá *jednoznačne* vyjadriť ako

$$\vec{\beta} = c_1\vec{\alpha}_1 + \cdots + c_n\vec{\alpha}_n.$$

(T.j. máme jednoznačnosť vyjadrenia ľubovoľného vektora v tvare lineárnej kombinácie bázových vektorov.)

Ľubovoľné dve bázy vektorového priestoru majú rovnaký počet prvkov. Počet prvkov bázy priestoru V nazývame *dimenzia priestoru* V. Označujeme $\dim(V)$ alebo $d(V)$.

Ak $\vec{\alpha}_1, \ldots, \vec{\alpha}_n \in V$ a $\dim(V) = n$, tak tieto podmienky sú ekvivalentné:

- $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ je báza priestoru V.
- Vektory $\vec{\alpha}_1, \ldots, \vec{\alpha}_n$ sú lineárne nezávislé.
- Platí $[\vec{\alpha}_1, \ldots, \vec{\alpha}_n] = V$, t.j. tieto vektory generujú celý priestor.

Inak povedané: Ak už viem, že mám „správny počet vektorov“ – toľko, koľko je dimenzia celého priestoru – tak vlastne stačí overiť jednu z dvoch podmienok, ktoré sa vyskytujú v definícii bázy. Tá druhá je potom splnená „zadarmo“.

Úloha 1. Zistite, či dané vektory tvoria bázu v $\mathbb{R}^3$:
a) $(1,2,3)$, $(1,-2,3)$, $(1,2,-3)$
b) $(1,1,1)$, $(1,1,0)$, $(1,0,1)$
c) $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,1)$

Úloha 2. Zistite, či dané vektory tvoria bázu v $\mathbb{Z}_5^3$:
a) $(1,2,3)$, $(2,3,4)$, $(0,3,1)$
b) $(1,0,0)$, $(0,1,2)$, $(2,1,3)$
c) $(0,1,2)$, $(3,0,1)$, $(1,0,2)$.

Úloha 3. Nájdite dimenziu zadaných podpriestorov priestoru $\mathbb{R}^4$. Nájdite pre každý z nich aspoň jednu bázu.
a) $S_1 = \{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4; x_1+x_2+x_3+x_4 = 0\}$
b) $S_2 = \{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4; x_1+x_2+x_3+x_4 = 0, x_1+x_2-x_3+2x_4 = 0\}$
c) $S_3 = \{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4; x_1+x_2+x_3+x_4 = 0, x_1+x_2-x_3+2x_4 = 0, x_1+2x_3-x_4 = 0\}$

Úloha 4. Určte dimenziu podpriestoru $[\vec{\alpha}, \vec{\beta}, \vec{\gamma}]$, ak $\vec{\alpha} = (1,3,2,1)$, $\vec{\beta} = (4,9,5,4)$ a $\vec{\gamma} = (3,7,4,3)$ v $\mathbb{R}^4$.

Úloha 5. Ako P_n označme priestor všetkých polynómov stupňa najviac n. Overte, že $d(P_n) = n+1$ a že $1, x-1, \ldots (x-1)^n$ je báza tohoto priestoru.

Úloha 6. Ak sa to dá, doplňte dané vektory na bázu príslušného vektorového priestoru:
a) (1,1,2), (2,1,3) v $\mathbb{R}^3$,
b) x^2-1, x^2+1 v priestore polynómov stupňa najviac 3,
c) (1,2,3,0), (3,4,1,2) v $\mathbb{Z}_5^4$.

Úloha 7. Máme dané vektory $\vec{\alpha}_1 = (1,1,2,0)$, $\vec{\alpha}_2 = (0,0,3,1)$ v priestore $\mathbb{Z}_5^4$. Koľko existuje možností na výber vektorov $\vec{\alpha}_3, \vec{\alpha}_4 \in \mathbb{Z}_5^4$ tak, aby tieto štyri vektory tvorili bázu?

Úloha 8. Ak každý z vektorov $\vec{\beta}_1, \ldots, \vec{\beta}_k$ je lineárnou kombináciou vektorov $\vec{\alpha}_1, \ldots, \vec{\alpha}_m$, tak $d([\vec{\beta}_1, \ldots, \vec{\beta}_k]) \leq d([\vec{\alpha}_1, \ldots, \vec{\alpha}_m])$.

Úloha 9. Overte, že množina $S = \{f\colon \mathbb{R} \to \mathbb{R} : (\exists a,b \in \mathbb{R})(\forall x \in \mathbb{R}) f(x) = ax+b\}$ je podpriestor priestoru všetkých funkcií z $\mathbb{R}$ do $\mathbb{R}$. Nájdite funkcie $g, h \in S$ také, že $S = [g,h]$.

Úloha 10. Zistite, či $S = \{f\colon \mathbb{R} \to \mathbb{R}; f(x) = ax^2 + bx + c, a, b, c \in \mathbb{R}\}$ je vektorový podpriestor priestoru reálnych funkcií. Ak áno, nájdite, $g_1, g_2, g_3 \in S$ také, že $S = [g_1, g_2, g_3]$.

Úloha 11*. a) Nech $p_1, \ldots, p_k$ sú navzájom rôzne prvočísla. Ukážte, že čísla $\ln p_1, \ln p_2, \ldots, \ln p_k$ sú lineárne nezávislé ako prvky vektorového priestoru $\mathbb{R}$ nad poľom $\mathbb{Q}$.
b) Ukážte, že vektorový priestor $\mathbb{R}$ nad poľom $\mathbb{Q}$ je nekonečnorozmerný.[1]

[1]Keď budeme vedieť nejaké veci o lineárnych izomorfizmoch a tiež o spočítateľných a nespočítateľných množinách, tak by sme mali byť schopní nájsť jednoduchšie zdôvodnenie, že ide o nekonečnorozmerný priestor. Dá sa to však zdôvodniť aj takýmto spôsobom – budeme tu potrebovať využiť nejaké veci o prvočíslach.