Pavol Zlatoš

LINEÁRNA ALGEBRA A GEOMETRIA

Kapitoly 0 – 10

Bratislava 2006

Obsah

0. Základné pojmy z logiky a teórie množín

V tejto kapitole zavedieme niektoré základné logické a množinové pojmy a dohodneme sa na štandardnej symbolike, ktorú budeme ďalej používať. Nebudeme však systematicky budovať *axiomatickú teóriu množín*, práve naopak, s množinami budeme narábať skôr intutívne. Čitateľ, ktorý základné množinové pojmy ovláda, môže túto kapitolu vynechať, prípadne ju len letmo prelistovať, aby sa oboznámil s našou terminológiou a symbolikou.

0.1. Logické spojky a kvantifikátory

Kvôli prehľadnosti budeme niektoré matematické tvrdenia zapisovať v symbolickej podobe ako *matematické formuly*. S príkladmi rôznych formúl sa ešte stretneme. V tejto chvíli sa zameriame len na spôsob, ako možno z daných tvrdení či formúl tvoriť nové pomocou *logických spojok* a *kvantifikátorov*.

Nech P, Q sú ľubovoľné tvrdenia.

(a) Tvrdenie, ktoré je pravdivé práve vtedy, keď tvrdenie P je nepravdivé, nazývame *negáciou* tvrdenia P, značíme ho $\neg P$ a čítame ho „nie P“, prípadne „non P“.

(b) Tvrdenie, ktoré je pravdivé práve vtedy, keď sú pravdivé obe tvrdenia P, Q, nazývame *konjunkciou* alebo *logickým súčinom* tvrdení P, Q, značíme ho $P \mathbin{\&} Q$ a čítame „P a zároveň Q“, krátko len „P a Q“, prípadne „P et Q“.

(c) Tvrdenie, ktoré je pravdivé práve vtedy, keď je pravdivé aspoň jedno z tvrdení P, Q, nazývame *alternatívou* alebo *disjunkciou* či *logickým súčtom* tvrdení P, Q, značíme ho $P \vee Q$, a čítame „P alebo Q“, prípadne „P vel Q“.

(d) Tvrdenie $\neg P \vee Q$ skrátene označujeme $P \Rightarrow Q$ a nazývame ho *implikáciou* tvrdení P, Q. Výraz $P \Rightarrow Q$ čítame „ak P, tak Q“ alebo „z P vyplýva Q“, prípadne „P implikuje Q“. Tvrdenie P nazývame *predpokladom* a tvrdenie Q *záverom* implikácie $P \Rightarrow Q$. Uvedomte si, že implikácia $P \Rightarrow Q$ je nepravdivá jedine v tom prípade, ak predpoklad P je pravdivý a záver Q je nepravdivý.

(e) Tvrdenie $(P \Rightarrow Q) \mathbin{\&} (Q \Rightarrow P)$ skrátene označujeme $P \Leftrightarrow Q$ a nazývame ho *ekvivalenciou* tvrdení P, Q. Výraz $P \Leftrightarrow Q$ čítame „P práve vtedy, keď Q“, prípadne „P je ekvivalentné s Q“. Zrejme ekvivalencia $P \Leftrightarrow Q$ je pravdivá vtedy a len vtedy, keď tvrdenia P, Q sú zároveň obe pravdivé alebo zároveň obe nepravdivé.

Znaky $\neg$, $\&$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ nazývame *logickými spojkami*. V literatúre sa možno tiež stretnúť s označením P', $-P$ alebo $\sim P$ pre negáciu, $P \wedge Q$ pre konjunkciu, $P \to Q$ alebo $P \supset Q$ pre implikáciu a $P \leftrightarrow Q$ alebo $P \equiv Q$ pre ekvivalenciu.

Okrem tvrdení zapisujeme formulami aj vlastnosti objektov a vzťahy medzi nimi. Na tento účel používame formuly s *voľnými premennými*. Označujeme ich $P(x)$, $Q(x, y)$, $R(x_1, \ldots, x_n)$ a pod. Dosadením konkrétnych objektov do formúl namiesto voľných premenných dostávame tvrdenia. Napríklad, ak $Q(x, y)$ je formula s voľnými premennými x, y a a, b sú nejaké objekty, tak $Q(a, b)$ je tvrdenie, ktoré je pravdivé práve vtedy, keď sa objekty a, b nachádzajú vo vzťahu označenom formulou Q.

Zrejme aj na formuly s voľnými premennými možno aplikovať logické spojky, ktoré si pritom zachovajú svoj doterajší význam. Popri logických spojkách možno z formúl tvoriť nové formuly či tvrdenia aj pomocou *kvantifikátorov*.

Nech $P(x)$ je ľubovoľná formula.

(a) Tvrdenie „existuje x také, že $P(x)$“ skrátene zapisujeme $(\exists\, x)P(x)$.

(b) Tvrdenie „pre každé (pre všetky) x platí $P(x)$“ skrátene zapisujeme $(\forall\, x)P(x)$.

Znaky $\exists$ resp. $\forall$ sú *kvantifikátory*; $\exists$ nazývame *existenčný* a $\forall$ *univerzálny* alebo tiež *všeobecný kvantifikátor*. Zrejme premenná x už nie je vo formulách $(\forall\, x)P(x)$ a $(\exists\, x)P(x)$ voľná ale *viazaná*; ak x je jediná voľná premenná vo formule $P(x)$, tak $(\forall\, x)P(x)$ a $(\exists\, x)P(x)$ sú tvrdenia. Oba uvedené kvantifikátory sú zviazané pravidlami negácie kvantifikovaných formúl:

$$\begin{aligned} \neg(\exists\, x)P(x) &\Leftrightarrow (\forall\, x)\neg P(x), \\ \neg(\forall\, x)P(x) &\Leftrightarrow (\exists\, x)\neg P(x). \end{aligned}$$

Pomocou existenčného a univerzálneho kvantifikátora už vieme vyjadriť i *kvantifikátor jednoznačnej existencie*. Ak $P(x)$ je nejaká vlastnosť, tak tvrdenie „existuje práve jedno x také, že $P(x)$“, t. j. tvrdenie

$$(\exists\, x)(P(x)\ \&\ (\forall\, y)(P(y) \Rightarrow y = x)),$$

skrátene zapisujeme v tvare $(\exists! x)P(x)$. Toto tvrdenie je zrejme ekvivalentné s tvrdením

$$(\exists\, x)(\forall\, y)(P(y) \Leftrightarrow y = x).$$

0.2. Množiny

Pod *množinou* rozumieme ľubovoľné jednoznačne vymedzené zoskupenie nejakých (často i značne rôznorodých) objektov – *prvkov množiny* – chápané ako jediný objekt. Množiny budeme väčšinou značiť veľkými latinskými písmenami, ich prvky malými písmenami.

Tvrdenie „objekt x je prvkom množiny X“, zapisujeme $x \in X$; hovoríme tiež, že x *patrí* do množiny X. Tvrdenie „objekt x nie je prvkom množiny X“, t. j. x nepatrí do množiny X, zapisujeme $x \notin X$.

Množina je jednoznačne zadaná zoskupením svojich prvkov. Preto dve množiny, nezávisle od spôsobu ich zadania, považujeme za totožné, ak majú tie isté prvky. Pre ľubovoľné množiny X, Y teda platí

$$X = Y \;\Leftrightarrow\; (\forall\, x)(x \in X \;\Leftrightarrow\; x \in Y).$$

Túto vlastnosť množín nazývame *extenzionalitou.*

Hovoríme, že množina X je *podmnožinou* množiny Y, označenie $X \subseteq Y$, ak každý prvok množiny X patrí aj do množiny Y, t. j.

$$X \subseteq Y \;\Leftrightarrow\; (\forall\, x)(x \in X \;\Rightarrow\; x \in Y).$$

Vzťah $\subseteq$ nazývame *vzťahom inklúzie* Extenzionalitu množín teraz možno skrátene vyjadriť v tvare konjunkcie dvoch inklúzií

$$X = Y \;\Leftrightarrow\; X \subseteq Y \;\&\; Y \subseteq X.$$

Kvantifikácie uvedené v predchádzajúcom paragrafe sa nazývajú *neohraničené*, lebo oblasť pôsobnosti kvantifikátorov v nich nebola nijako ohraničená. V matematike (i v bežnom živote) sa však častejšie vyskytujú *ohraničené kvantifikácie*, v ktorých je oblasť pôsobnosti príslušného kvantifikátora ohraničená nejakou množinou X. Ide o kvantifikácie tvaru $(\exists\, x \in X)$, $(\forall\, x \in X)$ a $(\exists!x \in X)$, ktoré čítame postupne „existuje x z množiny X", „pre každé (pre všetky) x z množiny X", resp. „existuje práve jedno (jediné) x z množiny X". Tieto kvantifikácie možno vyjadriť pomocou neohraničených kvantifikácii nasledujúcim spôsobom: Ak $P(x)$ je ľubovoľná vlastnosť a X je množina, kladieme

$$\begin{aligned}
(\exists\, x \in X)P(x) \ &\Leftrightarrow\ (\exists\, x)(x \in X \ \&\ P(x)),\\
(\forall\, x \in X)P(x) \ &\Leftrightarrow\ (\forall\, x)(x \in X \ \Rightarrow\ P(x)),\\
(\exists!x \in X)P(x) \ &\Leftrightarrow\ \big(\exists\, x \in X\big)\big(P(x) \ \&\ (\forall\, y \in X)(P(y) \ \Rightarrow\ y = x)\big).
\end{aligned}$$

V poslednom prípade môžeme tiež použiť vyjadrenie

$$(\exists!x \in X)P(x) \ \Leftrightarrow\ (\exists\, x \in X)(\forall\, y \in X)(P(y) \ \Leftrightarrow\ y = x).$$

Množinu nazývame *konečnou*, ak ju možno zadať vymenovaním všetkých jej prvkov. Ak X je konečná množina a $x_1, x_2, \dots, x_n$ sú všetky jej prvky, píšeme

$$X = \{x_1, x_2, \dots, x_n\}.$$

Z extenzionality potom vyplýva, že nezáleží na poradí vymenovania prvkov množiny X. Taktiež sa môže stať, že X má menej než n prvkov – v takom prípade sa niektoré z prvkov $x_1, \dots, x_n$ opakujú a v zápise množiny X môžeme (no nemusíme) opakujúce sa prvky až na jeden z nich vynechať. Napríklad $\{x,y\} = \{y,x\}$, a ak $x = y$, tak $\{x,y\} = \{x\} = \{y\}$. Okrem množín, ktoré majú nejaké prvky, zavádzame aj tzv. *prázdnu množinu* $\emptyset$, ktorá neobsahuje nijaký prvok. Z extenzionality vyplýva, že prázdna množina je touto podmienkou jednoznačne určená.

Popri konečných množinách však v matematike často pracujeme i s *nekonečnými* množinami, t. j. takými, ktoré nemožno zadať vymenovaním všetkých ich jednotlivých prvkov. Takéto množiny zvykneme zadávať nejakou *charakteristickou vlastnosťou*. Ak $P(x)$ je nejaká vlastnosť, píšeme

$$X = \{x;\ P(x)\},$$

čím myslíme, že pre ľubovoľné x platí $x \in X$ práve vtedy, keď x spĺňa $P(x)$. Z extenzionality vyplýva, že takto definovaná množina X je určená jednoznačne. Napríklad vlastnosťou „x je párne celé číslo“ je určená množina všetkých párnych celých čísel.

Poznamenajme, že z rovnosti $X = \{x;\ P(x)\}$ ešte nijako nevyplýva, že množina X je nekonečná – rovnako dobre môže byť aj konečná, dokonca prázdna.

Na tomto mieste je potrebné poznamenať, že uvedený princíp, ktorý nám umožňuje zadávať množiny akýmikoľvek vlastnosťami ich prvkov, vedie k logickým sporom, a je preto v uvedenej intuitívnej a neobmedzenej podobe nepoužiteľný. Keďže sa však nehodláme púšťať do jeho upresňovania, čo by si vyžiadalo vybudovať základy axiomatickej teórie množín, nezostáva nám než čitateľovi vopred zaručiť, že všetky prípady použitia tohto princípu, ktoré sa v tomto texte vyskytnú, budú plne legálne z hľadiska teórie množín, a požiadať ho o dôveru. Zatiaľ stačí, ak prezradíme, že všetky množiny netvoria množinu, t. j. neexistuje množina všetkých množín. To znamená, že vlastnosťou „x je množina“ nie je vymedzená nijaká množina.

Najčastejšie budeme spomínaný princíp používať na vymedzovanie podmnožín nejakej vopred danej *množiny* pomocou vlastností popísaných *matematickými formulami*. Ak M je množina a $P(x)$ je nejaká (matematická) vlastnosť, tak existuje množina X všetkých tých prvkov x množiny M, ktoré majú vlastnosť $P(x)$, t. j. množina

$$X = \{x \in M;\ P(x)\} = \{x;\ x \in M \ \&\ P(x)\}.$$

Nech X, Y sú ľubovoľné množiny. *Prienikom*, *zjednotením*, a *rozdielom* množín X, Y nazývame porade nasledujúce množiny:

$$\begin{aligned} X \cap Y &= \{x;\ x \in X \ \&\ x \in Y\}, \\ X \cup Y &= \{x;\ x \in X \vee x \in Y\}, \\ X \smallsetminus Y &= \{x;\ x \in X \ \&\ x \notin Y\}. \end{aligned}$$

Množiny X, Y nazývame *disjunktné*, ak $X \cap Y = \emptyset$. Čitateľovi prenechávame, aby si sám premyslel základné vlastnosti uvedených množinových operácií.

Pod usporiadanou dvojicou objektov x, y rozumieme objekt označovaný (x, y), taký, že pre všetky x, y, u, v platí:

$$(x, y) = (u, v) \ \Leftrightarrow\ (x = u \ \&\ y = v).$$

Uvedomme si, že nepotrebujeme vedieť, čo je „naozaj“ usporiadaná dvojica (x, y), dôležitá je len uvedená vlastnosť. Analogicky zavádzame pre ľubovoľné celé číslo $n \geq 2$ usporiadanú n-ticu $(x_1, \ldots, x_n)$ tak, že pre všetky $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ platí

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n) \ \Leftrightarrow\ (x_1 = y_1 \ \& \ \ldots \ \& \ x_n = y_n).$$

Množiny

$$X \times Y = \{(x, y);\ x \in X\ \&\ y \in Y\},$$
$$X_1 \times \ldots \times X_n = \{(x_1, \ldots, x_n);\ x_1 \in X_1\ \&\ \ldots\ \&\ x_n \in X_n\}$$

nazývame *karteziánskym súčinom* množín X, Y, resp. množín $X_1, \ldots, X_n$. V prípade, že $X_1 = \cdots = X_n = X$, píšeme

$$X_1 \times \ldots \times X_n = X^n.$$

Pre úplnosť ešte kladieme

$$X^1 = X, \qquad X^0 = \{\emptyset\}.$$

X^n nazývame *n-tou karteziánskou mocninou* množiny X. *Počet prvkov* konečnej množiny X budeme značiť $\# X$. Taktiež prázdna množina je konečná a platí $\# \emptyset = 0$. Pre nekonečnú množinu X píšeme $\# X = \infty$. Zrejme pre ľubovoľné konečné množiny X, Y platí

$$\# (X \cup Y) = \# X + \# Y - \# (X \cap Y),$$
$$\# (X \times Y) = \# X \cdot \# Y.$$

Z poslednej rovnosti vyplýva, že

$$\# \big(X^n\big) = (\# X)^n$$

pre každé celé číslo $n \geq 0$ a konečnú množinu X.

0.3. Zobrazenia

Zobrazením alebo tiež *funkciou* z množiny X do množiny Y rozumieme ľubovoľný predpis, ktorý každému prvku x množiny X priradí jednoznačne určený prvok y množiny Y. Zápis $f: X \to Y$ označuje, že f je zobrazenie (funkcia) z X do Y. Ten jednoznačne určený prvok $y \in Y$, ktorý zobrazenie f priradí prvku $x \in X$, budeme značiť $f(x)$, prípadne len fx alebo f_x. Vo vzťahu $y = f(x)$ nazývame x *nezávisle premennou* alebo *argumentom* a y *závisle premennou* alebo *funkčnou hodnotou* funkcie f. Píšeme tiež $f: x \mapsto y$.

Dve zobrazenia $f, g: X \to Y$ *sa rovnajú*, ak pre každé $x \in X$ platí $f(x) = g(x)$.

Množinu všetkých zobrazení z množiny X do množiny Y budeme označovať Y^X; teda

$$Y^X = \{f;\ f: X \to Y\}.$$

Toto označenie je motivované vzorcom pre počet prvkov množiny Y^X. Pre konečné množiny X, Y totiž platí

$$\#\left(Y^X\right) = (\# Y)^{(\# X)}.$$

(Samostatne si rozmyslite prečo!)

Zobrazenie $f: X \to X$ sa nazýva *transformáciou* množiny X alebo tiež *unárnou* (t. j. jednomiestnou) *operáciou* na množine X.

Zobrazenie $f: X \to Y$ sa nazýva *prosté* alebo tiež *injektívne* či *injekcia*, ak rôznym prvkom $x_1, x_2 \in X$ priraďuje rôzne prvky $f(x_1), f(x_2) \in Y$, t. j. ak platí

$$(\forall x_1, x_2 \in X)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)).$$

Uvedenú podmienku možno ekvivalentne vyjadriť v tvare

$$(\forall\, x_1, x_2 \in X)(f(x_1) = f(x_2) \;\Rightarrow\; x_1 = x_2).$$

Zobrazenie $f : X \to Y$ sa nazýva zobrazenie *na množinu* Y alebo tiež *surjektívne* či *surjekcia*, ak na každý prvok množiny Y sa zobrazí nejaký prvok množiny X, t. j. ak platí

$$(\forall\, y \in Y)(\exists\, x \in X)(y = f(x)).$$

Hovoríme, že $f : X \to Y$ je *prosté zobrazenie* X *na* Y alebo tiež *bijektívne zobrazenie* či *bijekcia*, ak f je zároveň prosté a na, t. j. injektívne i surjektívne. Ešte inak to môžeme vyjadriť podmienkou

$$(\forall\, y \in Y)(\exists!x \in X)(y = f(x)).$$

Namiesto uvedených pojmov niekedy tiež hovoríme, že f je *vzájomne jednoznačné zobrazenie množiny* X *na množinu* Y.

Ak $f : X \to Y$ je bijekcia, tak existuje jednoznačne určené zobrazenie $g : Y \to X$, ktoré každému $y \in Y$ priradí ten jediný prvok $x \in X$, pre ktorý platí $y = f(x)$. Toto zobrazenie nazývame *inverzným zobrazením* k zobrazeniu f a označujeme ho f^{-1}. Zrejme $f^{-1} : Y \to X$ je tiež bijekcia a pre všetky $x \in X$, $y \in Y$ platí

$$f^{-1}\bigl(f(x)\bigr) = x, \qquad f\bigl(f^{-1}(y)\bigr) = y.$$

Nech $f : X \to Y$, $g : Y \to Z$ sú zobrazenia. *Kompozíciou* zobrazení f, g alebo aj *zloženým zobrazením* z f a g rozumieme zobrazenie označené ako $g \circ f : X \to Z$, dané pre každé $x \in X$ predpisom

$$(g \circ f)(x) = g(f(x)).$$

Zložené zobrazenie možno znázorniť pomocou tzv. *komutatívneho diagramu*

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, "g \circ f"'] & Y \arrow[d, "g"] \\ & Z \end{tikzcd}$$

(Všimnite si, že zobrazenie $g \circ f$ zapisujeme „v obrátenom poradí“ – najprv totiž na prvok x aplikujeme f a až potom g. Núti nás k tomu zaužívaná konvencia, podľa ktorej argument x píšeme napravo od funkcie f. Poznamenajme, že niektorí autori dávajú prednosť „prirodzenému poradiu“ a kompozíciu zobrazení $f : X \to Y$, $g : Y \to Z$, zapisujú ako $f \circ g$. Kvôli tomu však opúšťajú spomínanú konvenciu a namiesto $f(x)$ píšu xf. V tomto duchu fungujú napr. niektoré kalkulačky.)

Skladanie zobrazení je *asociatívne* v nasledujúcom zmysle: ak $f : X \to Y$, $g : Y \to Z$ a $h : Z \to W$ sú zobrazenia, tak

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Ľahko totiž nahliadneme, že obe zobrazenia priradia prvku $x \in X$ prvok $h(g(f(x))) \in W$.

Na každej množine X máme definované *identické zobrazenie* $\mathrm{id}_X : X \to X$, nazývané tiež *identita na* X, také, že

$$\mathrm{id}_X(x) = x$$

pre každé $x \in X$. Zrejme id_X je bijekcia pre každé X, a pre ľubovoľné zobrazenie $f : X \to Y$

platí

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$

Pre $f : X \to X$ kladieme $f^2 = f \circ f$, $f^3 = f \circ f \circ f$, atď. Kvôli úplnosti definujeme aj $f^1 = f$, $f^0 = \mathrm{id}_X$. Zobrazenie f^n nazývame n-tou *iteráciou zobrazenia* f.

Ak $f : X \to Y$ je bijekcia, tak k nej inverzné zobrazenie $f^{-1} : Y \to X$ teraz môžeme charakterizovať rovnosťami

$$f^{-1} \circ f = \mathrm{id}_X, \qquad f \circ f^{-1} = \mathrm{id}_Y .$$

Čitateľ sám ľahko nahliadne, že pre ľubovoľné zobrazenia $f : X \to Y$, $g : Y \to Z$ platí:

(a) Ak f, g sú injektívne, tak aj $g \circ f$ je injektívne.
(b) Ak f, g sú surjektívne, tak aj $g \circ f$ je surjektívne.
(c) Ak f, g sú bijektívne, tak aj $g \circ f$ je bijektívne.
(d) Ak $g \circ f$ je injektívne, tak aj f je injektívne.
(e) Ak $g \circ f$ je surjektívne, tak aj g je surjektívne.
(f) Ak $g \circ f$ je bijektívne, tak f je injektívne a g je surjektívne.

Podmienka (c) nás oprávňuje zaviesť pre bijekcie $f : X \to X$ aj záporné iterácie

$$f^{-n} = \left(f^{-1}\right)^n = \left(f^n\right)^{-1}.$$

Nech $f : X \to Y$ je nejaké zobrazenie a $A \subseteq X$. *Zúžením zobrazenia* f na množinu A nazývame zobrazenie $f \restriction A : A \to Y$ také, že

$$(f \restriction A)(x) = f(x)$$

pre každé $x \in A$. *Obrazom množiny* A v zobrazení f nazývame množinu

$$f(A) = \{f(x);\, x \in A\} \subseteq Y.$$

Špeciálne, množinu $f(X)$ nazývame *obrazom zobrazenia* f a značíme ju

$$\operatorname{Im} f = f(X) = \{f(x);\, x \in X\}.$$

Pre $f : X \to Y$ a $A \subseteq X$ platí $\operatorname{Im}(f \restriction A) = f(A)$; zrejme f je surjekcia práve vtedy, keď $\operatorname{Im} f = Y$,

Podobne, *vzorom množiny* $B \subseteq Y$ v zobrazení $f : X \to Y$ nazývame množinu

$$f^{-1}(B) = \{x \in X;\, f(x) \in B\} \subseteq X.$$

Pre ľubovoľné $A \subseteq X$, $B \subseteq Y$ možno jednoducho overiť inklúzie

$$A \subseteq f^{-1}\big(f(A)\big), \qquad f\big(f^{-1}(B)\big) \subseteq B.$$

0.4. Binárne operácie

Ak X, Y, Z sú množiny, tak zobrazenie $f : X \times Y \to Z$ nazývame *binárnou* (t. j. dvojmiestnou) *operáciou na množinách* X, Y *s hodnotami v množine* Z. Binárne operácie väčšinou označujeme znakmi umiestňovanými medzi hodnoty argumentov, ako napr $+$, $\cdot$, $\circ$, $*$ a pod. Hodnotu takej operácie na dvojici prvkov $x \in X$, $y \in Y$ potom označujeme $x + y$, $x \cdot y$ (prípadne len xy), $x \circ y$, $x * y$ a pod.

Podobným spôsobom možno zaviesť aj n-miestne operácie $X_1 \times \ldots \times X_n \to Y$, prípadne $X^n \to Y$, či $X^n \to X$ pre ľubovoľné celé číslo $n \geq 0$.

Najčastejšie budeme pracovať s binárnymi operáciami tvaru $f : X \times X \to X$, ktoré nazývame jednoducho *binárnymi operáciami na množine* X.

Binárna operácia $*$ na množine X sa nazýva *asociatívna*, ak pre všetky $x, y, z \in X$ platí

$$x * (y * z) = (x * y) * z.$$

Asociativita operácie nám dovoľuje vynechávať zátvorky a písať len $x * y * z$. Podobne si možno počínať i v prípade viacerých argumentov.

Binárna operácia $*$ na množine X sa nazýva *komutatívna*, ak pre všetky $x, y \in X$ platí

$$x * y = y * x.$$

Prvok $e \in X$ sa nazýva *neutrálny prvok* binárnej operácie $*$ na množine X, ak pre všetky $x \in X$ platí

$$x * e = e * x = x.$$

Zrejme neutrálny prvok operácie $*$ (ak existuje) je určený jednoznačne. Keby totiž $e_1, e_2 \in X$ boli dva neutrálne prvky, tak nevyhnutne

$$e_1 = e_1 * e_2 = e_2.$$

Ak binárna operácia $*$ na množine X má neutrálny prvok e a k danému prvku $x \in X$ existuje prvok $y \in X$ taký, že

$$x * y = y * x = e,$$

hovoríme, že y je *inverzný prvok* k prvku x. Ak $*$ je *asociatívna* binárna operácia na X, tak aj inverzný prvok k danému prvku $x \in X$ (pokiaľ existuje) je určený jednoznačne. Keby totiž y_1, y_2 boli dva inverzné prvky k x, tak

$$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2.$$

Napríklad pre ľubovoľnú množinu X kompozícia $\circ$ je asociatívna binárna operácia na množine X^X všetkých transformácií množiny X. Zrejme ak $\# X \geq 2$, tak táto operácia nie je komutatívna. Identické zobrazenie $\mathrm{id}_X \in X^X$ je neutrálnym prvkom operácie $\circ$. K danému zobrazeniu $f \in X^X$ existuje inverzný prvok práve vtedy, keď f je bijekcia; v tom prípade je ním inverzné zobrazenie $f^{-1} \in X^X$.

Binárnu operáciu $*$ na konečnej množine X možno zadať pomocou tzv. *multiplikatívnej tabuľky*, ktorej stĺpce i riadky sú označené prvkami množiny X. Do poľa tabuľky ležiaceho v priesečníku x-tého riadku a y-tého stĺpca vpíšeme hodnotu $x * y$.

Napr. tabuľkami

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

sú zadané dve asociatívne a komutatívne operácie $+$ a $\cdot$ na množine $\{0, 1, 2, 3, 4\}$. Ďalej 0 je neutrálny prvok operácie $+$ a 1 je neutrálny prvok operácie $\cdot$. Navyše ku každému prvku

a tejto množiny existuje inverzný prvok vzhľadom na operáciu $+$: k prvkom 0, 1, 2, 3, 4 sú to postupne prvky 0, 4, 3, 2, 1. Pokiaľ ide o operáciu $\cdot$, vidíme, že k prvku 0 neexistuje inverzný prvok; k prvkom 1, 2, 3 však inverzné prvky existujú: sú to postupne 1, 3, 2.

Komutativitu binárnej operácie možno ľahko nahliadnuť z jej multiplikatívnej tabuľky – prejaví sa symetriou tabuľky podľa hlavnej diagonály spájajúcej ľavý horný a pravý dolný roh. Taktiež neutrálny prvok možno odhaliť na prvý pohľad, lebo v jeho riadku i stĺpci sa zreprodukuje riadok resp. stĺpec zo záhlavia tabuľky. Ak už poznáme neutrálny prvok, možno overiť aj existenciu inverzného k danému – treba nájsť neutrálny prvok v riadku i v stĺpci daného prvku. Ak sa nám to podarí pre dvojicu polí tabuľky, ktoré ležia v stĺpci resp. riadku toho istého prvku, tak ide o hľadaný inverzný prvok. Asociatívnosť, žiaľ, tak jednoducho nahliadnuť nemožno.

0.5. Permutácie

Kým znalosť predchádzajúcich paragrafov je nevyhnutným predpokladom, aby čitateľ mohol začať so štúdiom kapitoly 1, tento paragraf budeme potrebovať až neskôr, keď začneme preberať determinanty.

Nech X je ľubovoľná množina. *Permutáciou* množiny X rozumieme ľubovoľné bijektívne zobrazenie $\sigma : X \to X$. Množinu všetkých permutácií množiny X značíme $\mathcal{S}(X)$. Ak X je konečná množina, tak počet prvkov množiny $SS(X)$ je daný známym vzťahom

$$\#\,\mathcal{S}(X) = (\#\,X)!\,,$$

kde $n! = 1 \cdot 2 \cdot \ldots \cdot n$ je *faktoriál* prirodzeného čísla n (pritom $0! = 1! = 1$).

Uvedomme si, že transformácia $f : X \to X$ *konečnej* množiny X je injektívna práve vtedy, keď je surjektívna. Jedna i druhá podmienka totiž hovorí, že množina $f(X) \subseteq X$ má rovnaký počet prvkov ako X. Teda už jedna z uvedených podmienok je postačujúca na to, aby f bola permutáciou konečnej množiny X.

Keďže zloženie $\sigma \circ \tau$ dvoch permutácií $\sigma, \tau \in \mathcal{S}(X)$ dáva opäť permutáciu množiny X, kompozícia $\circ$ je asociatívna binárna operácia na množine $\mathcal{S}(X)$. Ľahko sa možno presvedčiť, že – okrem prípadu, keď $\# X \leq 2$, – táto operácia nie je komutatívna. Zrejme $\mathrm{id}_X \in \mathcal{S}(X)$ je neutrálny prvok tejto operácie a inverzným prvkom k permutácii $\sigma \in \mathcal{S}(X)$ je inverzná permutácia $\sigma^{-1} \in \mathcal{S}(X)$.

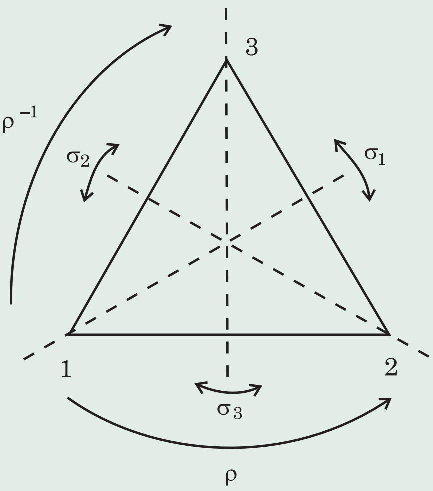
Pre $X = \{1, 2, \ldots, n\}$ namiesto $\mathcal{S}(X)$ píšeme $\mathcal{S}_n$. Permutáciu $\sigma \in \mathcal{S}_n$ zvyčajne zapisujeme v tvare

Prvky množiny $\mathcal{S}_3$, t. j. permutácie množiny $\{1, 2, 3\}$, si môžeme predstaviť ako symetrie rovnostranného trojuholníka s vrcholmi označenými číslami 1, 2, 3.

Ak si identickú permutáciu tejto množiny označíme ako ι, otočenia okolo ťažiska trojuholníka proti smeru resp. v smere hodinových ručičiek o uhol $\pi/3$ ako ϱ resp. ϱ^{-1}, a osovú súmernosť podľa osi prechádzajúcej i-tým vrcholom a stredom protiľahlej strany ako σ_i, pre $i = 1, 2, 3$, tak množina permutácií $\mathcal{S}_3$ bude pozostávať z permutácií

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \varrho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \varrho^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$



Obr. 0.1. Symetrie trojuholníka

Multiplikatívna tabuľka binárnej operácie $\circ$ na množine $\mathcal{S}_3$ vyzerá takto:

$\circ$	ι	ϱ	ϱ^{-1}	σ_1	σ_2	σ_3
ι	ι	ϱ	ϱ^{-1}	σ_1	σ_2	σ_3
ϱ	ϱ	ϱ^{-1}	ι	σ_3	σ_1	σ_2
ϱ^{-1}	ϱ^{-1}	ι	ϱ	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	ι	ϱ	ϱ^{-1}
σ_2	σ_2	σ_3	σ_1	ϱ^{-1}	ι	ϱ
σ_3	σ_3	σ_1	σ_2	ϱ	ϱ^{-1}	ι

Permutáciu $\sigma \in \mathcal{S}(X)$ nazývame *transpozíciou*, ak existujú $x, y \in X$ také, že $x \neq y$, $\sigma(x) = y$, $\sigma(y) = x$ a $\sigma(z) = z$ pre každé $z \in X \setminus \{x, y\}$. Inak povedané, transpozícia je výmena dvoch prvkov množiny X.

Zrejme $\sigma_1, \sigma_2, \sigma_3 \in \mathcal{S}_3$ sú transpozície.

Z názoru je zrejmé (dôkaz je v cvičení 0.14), že každú permutáciu σ konečnej množiny X možno získať postupnými výmenami dvojíc prvkov, teda každá taká permutácia je kompozíciou transpozícií. Tento rozklad na transpozície nie je jednoznačný: napr. $\iota \in \mathcal{S}_3$ možno zapísať ako ι, t. j. kompozíciu 0 transpozícií, a taktiež ako $\iota = \sigma_1 \circ \sigma_1 = \sigma_2 \circ \sigma_2 = \sigma_3 \circ \sigma_3$, t. j. aspoň troma ďalšími spôsobmi ako kompozíciu dvoch transpozícií.

Dĺžkou permutácie σ konečnej množiny X nazveme najmenší počet transpozícií, na kompozíciu ktorých možno σ rozložiť, a označíme ju $|\sigma|$. Samotná dĺžka $|\sigma|$ nie je dôležitá, význam má len parita tohto čísla, t. j. vlastne výraz $\operatorname{sgn} \sigma = (-1)^{|\sigma|}$, ktorý nazývame *znakom*, prípadne *znamienkom permutácie* σ.

Permutácia σ konečnej množiny X sa nazýva *párna* resp. *nepárna*, ak číslo $|\sigma|$ je párne resp. nepárne, t. j. ak jej znak je 1 resp. -1.

Z nasledujúcej vety vyplýva, že pri určovaní znamienka permutácie σ môžeme použiť jej *ľubovoľný* rozklad na transpozície $\sigma = \tau_1 \circ \ldots \circ \tau_k$ a nemusíme sa starať o to, či tento rozklad je naozaj najkratší – pre ľubovoľný taký rozklad totiž platí

$$(-1)^{|\sigma|} = (-1)^k.$$

0.5.1. Veta. *Nech X je konečná množina. Potom pre ľubovoľné $\sigma, \tau \in \mathcal{S}(X)$ platí*

$$(-1)^{|\sigma \circ \tau|} = (-1)^{|\sigma|} \cdot (-1)^{|\tau|}.$$

Dôkaz. Zrejme stačí dokázať uvedenú rovnosť pre prípad, keď τ je transpozícia a $X = \{1, 2, \dots, n\}$.

Pre každé $\sigma \in \mathcal{S}_n$ označme $p(\sigma)$ súčin všetkých rozdielov tvaru $\sigma(j)-\sigma(i)$, kde $1 \le i < j \le n$. Zrejme pre všetky $\sigma \in \mathcal{S}_n$ majú výrazy $p(\sigma)$ rovnakú absolútnu hodnotu a líšia sa nanajvýš znamienkom. Toto znamienko závisí od parity počtu záporných členov v súčine $p(\sigma)$. Člen $\sigma(j)-\sigma(i)$ je záporný práve vtedy, keď $i < j$ a $\sigma(i) > \sigma(j)$, – každdú takú dvojicu (i, j) nazývame *inverziou* permutácie σ. Identita id_X má 0 inverzií a $p(\mathrm{id}_X) = 1^{n-1} \cdot 2^{n-2} \cdot \ldots \cdot (n-1)^1 = 1! \cdot 2! \cdot \ldots \cdot (n-1)! > 0$.

Stačí teda dokázať, že počet inverzií permutácií σ a $\sigma \circ \tau$ sa líši o nepárnu hodnotu. Nech $1 \le k < l \le n$ sú tie dva prvky, ktoré vymieňa transpozícia τ. Potom

$$
\begin{aligned}
\sigma &= \begin{pmatrix} 1 & \dots & k & \dots & l & \dots & n \\ \sigma(1) & \dots & \sigma(k) & \dots & \sigma(l) & \dots & \sigma(n) \end{pmatrix}, \\
\sigma \circ \tau &= \begin{pmatrix} 1 & \dots & k & \dots & l & \dots & n \\ \sigma(1) & \dots & \sigma(l) & \dots & \sigma(k) & \dots & \sigma(n) \end{pmatrix}.
\end{aligned}
$$

Inverzie (i, j) permutácie σ, v ktorých nevystupuje k ani l, sú tiež inverziami permutácie $\sigma \circ \tau$. Inverzie, v ktorých vystupujú prvky i, k, a i, l, kde $i \ne k, l$, alebo obe súčasne vzniknú alebo súčasne zaniknú v $\sigma \circ \tau$ oproti σ. Konečne, pokiaľ (k, l) nebola inverziou v σ, stane sa ňou v $\sigma \circ \tau$; pokiaľ ňou bola, táto inverzia v $\sigma \circ \tau$ zanikne. Teda celkový rozdiel počtu inverzií permutácií σ a $\sigma \circ \tau$ je nepárny.

0.6. Ekvivalencie a rozklady

Podobne ako predošlý, i tento paragraf môže čitateľ zatiaľ preskočiť. Jeho znalosť bude potrebná až neskôr, v súvislosti s niektorými otázkami teórie grúp. S pojmom ekvivalencie sa síce stretneme už predtým, dovtedy ho však nebudeme systematicky využívať.

Nech $\sim$ je nejaký dvojmiestny vzťah, do ktorého vstupujú prvky nejakého oboru objektov $\mathcal{M}$ (tento obor môže, ale nemusí byť množinou). Zápisom $x \sim y$ značíme, že prvky $x, y \in \mathcal{M}$ sa nachádzajú vo vzťahu $\sim$; ak sa $x, y \in \mathcal{M}$ nenachádzajú v tomto vzťahu, píšeme $x \not\sim y$.

Hovoríme, že vzťah $\sim$ je na obore $\mathcal{M}$

(a) *reflexívny*, ak pre všetky $x \in \mathcal{M}$ platí $x \sim x$;

(b) *symetrický*, ak pre všetky $x, y \in \mathcal{M}$ platí $x \sim y \ \Rightarrow\ y \sim x$;

(c) *tranzitívny*, ak pre všetky $x, y, z \in \mathcal{M}$ platí $x \sim y \ \&\ y \sim z \ \Rightarrow\ x \sim z$.

Vzťah $\sim$, ktorý je reflexívny, symetrický a tranzitívny na obore $\mathcal{M}$, nazývame *vzťahom ekvivalencie* alebo len krátko *ekvivalenciou* na obore $\mathcal{M}$. Ekvivalencie budeme väčšinou značiť znakmi $\sim$, $\approx$, $\equiv$ a pod.

Každý vzťah ekvivalencie na nejakej množine či obore objektov $\mathcal{M}$ predstavuje isté hľadisko, z ktorého považujeme niektoré prvky z $\mathcal{M}$ za rovnocenné, t. j. ekvivalentné, a iné nie. Napr. na množine všetkých hracích guličiek v danej jamke možno zaviesť vzťah ekvivalencie, v ktorom sa nachádzajú ľubovoľné dve guličky práve vtedy, keď majú rovnakú farbu. Vzťah, v ktorom sa nachádzajú dve takéto guličky práve vtedy, keď majú rovnakú hmotnosť, je iným príkladom ekvivalencie na tejto množine.

Jedným dychom však poznamenajme, že uvedené príklady neslobodno brať príliš vážne, lebo rovnocennosť sa v nich mieša s podobnosťou, – „naozajstné“ ekvivalencie predstavujú len v značne idealizovanom prípade. S reflexívnosťou a symetriou nie je problém, v reálnom živote však zvykne zlyhať tranzitívnosť. Môžeme sa napríklad zhodnúť, že guličky a, b majú rovnakú farbu, a takisto majú rovnakú farbu guličky b, c. No farba guličiek a, c sa nám už rovnakou zdať nemusí. Podobne môžeme v rámci presnosti našich váh dospieť k záveru, že guličky p, q ako aj guličky q, r majú rovnakú hmotnosť. Avšak hmotnosť guličiek p, r sa nám už vážením môže podariť rozlíšiť. Lepším príkladom ekvivalencie je tak vzťah na množine všetkých bankoviek danej meny, v ktorom sa nachádzajú dve bankovky práve vtedy, keď majú rovnakú nominálnu hodnotu.

Na rozdiel od reálneho života sa v matematike nemusíme trápiť podobnými ťažkosťami. Všetky ekvivalencie, s ktorými sa tu stretneme, budú mať v plnej miere všetky tri uvedené vlastnosti. Ešte jeden príklad za všetky: vzťahom

$$x \sim y \iff |x| = |y|$$

je definovaná ekvivalencia „mať rovnakú absolútnu hodnotu“ na množine $\mathbb{C}$ všetkých komplexných čísel.

Nech $\sim$ je ekvivalencia na množine X. Pre $x \in X$ označme

$$\tilde{x} = \{u \in X;\ u \sim x\}$$

množinu všetkých prvkov $u \in X$ ekvivalentných s x, ktorú nazývame *triedou* alebo *blokom ekvivalencie* prvku x. Zrejme pre ľubovoľné $x \in X$ platí $x \in \tilde{x}$. Ľahko tiež možno dokázať (skúste sami), že

$$x \sim y \iff \tilde{x} = \tilde{y} \iff x \in \tilde{y} \iff y \in \tilde{x} \iff \tilde{x} \cap \tilde{y} \neq \emptyset$$

pre všetky $x, y \in X$. Množinu

$$X/\sim\ = \{\tilde{x};\, x \in X\}$$

všetkých tried ekvivalencie prvkov množiny X nazývame *faktorovou množinou* množiny X podľa ekvivalencie $\sim$. (Podotýkame, že v zhode s paragrafom 0.2 sa každá trieda $\tilde{x}$ nachádza v množine $X/\sim$ iba raz, i keď prvkov $y \in X$, pre ktoré platí $\tilde{x} = \tilde{y}$, môže byť mnoho.)

Priradením $x \mapsto \tilde{x}$ je definované surjektívne zobrazenie $X \to X/\sim$, ktoré nazývame *prirodzenou* alebo tiež *kanonickou projekciou* množiny X na faktorovú množinu $X/\sim$.

Na faktorovú množinu $X/\sim$ sa možno dívať dvojakým spôsobom. Jednak ako na výsledok stotožnenia či zlepenia navzájom ekvivalentných prvkov množiny X; v takom prípade sa na bloky $\tilde{x}$ dívame predovšetkým ako na *prvky*, ktoré vznikli „stiahnutím“ celej triedy $\tilde{x}$ do jediného bodu, a vedome si nevšímame fakt, že sú to zároveň množiny. Použitím názvu „faktorová množina“ naznačujeme, že v danej chvíli dávame tomuto pohľadu prednosť. Na druhej strane sa na množinu $X/\sim$ možno dívať ako na *rozklad* množiny X na navzájom disjunktné neprázdne množiny $\tilde{x}$.

Rozkladom množiny X nazývame ľubovoľný systém (t. j. množinu) jej neprázdnych podmnožín $\mathcal{R}$ taký, že každý prvok množiny X padne do práve jednej množiny zo systému $\mathcal{R}$. Inými slovami, systém $\mathcal{R}$ neprázdnych podmnožín množiny X je jej rozkladom práve vtedy, keď spĺňa nasledujúce dve podmienky:

(1) zjednotením všetkých množín $A \in \mathcal{R}$ je celá množina X, t. j.

$$(\forall\, x \in X)(\exists\, A \in \mathcal{R})(x \in A);$$

(2) množiny z $\mathcal{R}$ sú navzájom disjunktné, t. j.

$$(\forall\, A, B \in \mathcal{R})(A \neq B \;\Rightarrow\; A \cap B = \emptyset).$$

Ľahko možno nahliadnuť, že faktorová množina $X/\!\sim$ množiny X podľa ekvivalencie $\sim$ je zároveň rozkladom množiny X, ktorý je tvorený triedami navzájom ekvivalentných prvkov. Taktiež naopak, každý rozklad $\mathcal{R}$ množiny X určuje predpisom

$$x \sim_{\mathcal{R}} y \;\Leftrightarrow\; (\exists\, A \in \mathcal{R})(x, y \in A)$$

ekvivalenciu na množine X. Inak povedané, prvky $x, y \in X$ sú vo vzťahu ekvivalencie určenej rozkladom $\mathcal{R}$ práve vtedy, keď sa nachádzajú v tej istej (jednoznačne určenej) množine z tohto rozkladu. Čitateľovi prenechávame, aby si samostane overil, že takto definovaný vzťah $\sim_{\mathcal{R}}$ je reflexívny, symetrický a tranzitívny, t. j. má všetky tri požadované vlastnosti ekvivalencie, ako aj rovnosť $X/\!\sim_{\mathcal{R}} = \mathcal{R}$, t. j. že rozklad (faktorová množina) určený ekvivalenciou $\sim_{\mathcal{R}}$ splýva s pôvodným rozkladom $\mathcal{R}$.

0.6.1. Príklad. Rozklad prislúchajúci k spomínanej ekvivalencii $x \sim y \;\Leftrightarrow\; |x| = |y|$ na množine $\mathbb{C}$ je vlastne rozkladom komplexnej roviny na navzájom sústredné kružnice so stredom v počiatku 0 a ľubovoľným polomerom $r \geq 0$ (kružnicu s nulovým polomerom prirodzene stotožňujeme s jej stredom).

0.7. O matematických dôkazoch

Matematika je veda vybudovaná prevažne (hoci nie výlučne) *deduktívne*. To znamená, že v tej-ktorej matematickej teórii vychádzame z určitých základných pojmov, ktoré považujeme za intuitívne jasné vďaka istým s nimi spojeným názorným predstavám. Ďalšie pojmy potom definujeme pomocou pojmov základných alebo skôr definovaných. Základné pojmy označujú základné objekty, ktoré tvoria predmet nášho štúdia, alebo určité základné vzťahy medzi nimi. Tieto objekty a vzťahy sú charakterizované istými východzími tvrdeniami, ktorým hovoríme *axiómy*. V najjednoduchších prípadoch je platnosť axióm jasná z názoru, ktorý stojí v pozadí príslušnej teórie. V zložitejších prípadoch však môžu názorné predstavy zlyhať – vtedy sa na axiómy dívame ako na *implicitné definície* základných pojmov. To znamená, že rezignujeme na otázku, čo „naozaj" označujú základné pojmy. Môžu označovať čokoľvek, čo spĺňa dané axiómy – to je všetko, čo o nich predpokladáme. Zisk z takéhoto prístupu spočíva v *univerzálnosti matematiky* – aj výsledky matematických teórií sa potom vzťahujú na veľmi rôznorodé oblasti reality. Totiž na tie, v ktorých možno interpretovať základné pojmy danej teórie tak, že sú pritom splnené jej axiómy.

Pri deduktívnej výstavbe nejakej teórie vyvodzujeme ďalšie poznatky z jej axióm logickými prostriedkami, t. j. dokazujeme ich. Týmto dokázaným poznatkom hovoríme *vety*, *tvrdenia*, *lemy* a *dôsledky*, čím naznačujeme rôzny stupeň dôležitosti, ktorý im pripisujeme. Názvom *veta* označujeme tie najdôležitejšie z nich, menej dôležité nazývame *tvrdeniami* a tvrdenia pomocného charakteru označujeme ako *lemy*. *Dôsledky*, ako už samotný názov napovedá, pripájame ako bezprostredné dôsledky niektorých viet, tvrdení či liem, pokiaľ ich význam nedosahuje úroveň viet. Poznamenajme, že toto rozdelenie má značne subjektívny charakter a vývoj ho často zvykne prekonať. Mnohé vety časom upadajú do zabudnutia, kým naopak mnohé lemy postupne nadobúdajú na význame.

Základným prostriedkom odvodzovania nových poznatkov v deduktívnej teórii je *dôkaz*. V tomto paragrafe sa veľmi stručne zoznámime s hlavnými typmi matematických dôkazov: s *priamym dôkazom*, s *nepriamym dôkazom* a s *dôkazom sporom*. Uvidíme, že toto rozdelenie tak trochu súvisí so stratégiou vedenia príslušného dôkazu. V nasledujúcom paragrafe sa ešte zoznámime s *dôkazom matematickou indukciou.*

Väčšina matematických tvrdení má tvar implikácie $P \Rightarrow Q$, t. j. tvrdí sa v nich, že z predpokladu P vyplýva záver Q. Pritom predpoklad P je často konjunkciou nejakých dielčích predpokladov, čiže má tvar P_1 & ... & P_n. Na tomto mieste sa obmedzíme na niekoľko poznámok o dôkazoch tvrdení takéhoto tvaru.

0.7.1. Priamy dôkaz. Pri *priamom dôkaze* implikácie $P \Rightarrow Q$ dokazujeme (či sa aspoň pokúšame dokázať) záver Q z predpokladu P. Spočiatku sa snažíme dokázať priamo záver Q z daných axióm a už skôr dokázaných tvrdení. Postupujeme pri tom tak ďaleko, ako sa len dá, pričom jedným očkom stále pokukujeme po predpoklade P, či dielčích predpokladoch $P_1, \dots, P_n$. Vo chvíli, keď už nevieme ako ďalej, siahneme po tom z dielčích predpokladov P_i, ktorý nám umožní pohnúť sa dopredu. Opäť postupujeme ďalej a vo vhodnej chvíli zasa použijeme niektorý dielčí predpoklad P_j (nie nevyhnutne rôzny od P_i). Ak sme úspešní, nakoniec sa nám podarí dospieť k záveru Q, čím dôkaz končí. Ak sme neúspešní, musíme to skúsiť inak, prípadne sa zamyslieť nad otázkou, či spomínaná implikácia vôbec platí.

Môže sa stať, že pri našom úspešnom dôkaze sme nepoužili všetky dielčie predpoklady $P_1, \dots, P_n$, ale povedzme prvý a posledný z nich sme nepotrebovali. To znamená, že miesto pôvodného tvrdenia (P_1 & P_2 & ... & P_{n-1} & P_n) $\Rightarrow Q$ sme dokázali *silnejšie* tvrdenie (P_2 & ... & P_{n-1}) $\Rightarrow Q$.

0.7.2. Nepriamy dôkaz. Pri *nepriamom dôkaze* implikácie $P \Rightarrow Q$ dokazujeme miesto nej logicky ekvivalentnú tzv. *transponovanú implikáciu* $\neg Q \Rightarrow \neg P$ práve opísanou metódou priameho dôkazu. Za tým účelom býva často užitočné (pokiaľ to ide) rozčleniť predpoklad

$\neg Q$ na konjunkciu dielčích predpokladov $R_1 \ \& \ \ldots \ \& \ R_m$. Ak pôvodný predpoklad P bol konjunkciou dielčích predpokladov $P_1 \ \& \ \ldots \ \& \ P_n$, tak jeho negácia $\neg P$ je ekvivalentná s alternatívou $\neg P_1 \vee \ldots \vee \neg P_n$. Potom transponovaná implikácia $\neg Q \Rightarrow \neg P$ je logicky ekvivalentná s ľubovoľnou z implikácií

$$(\neg Q \ \& \ P_1 \ \& \ \ldots \ \& \ P_{i-1} \ \& \ P_{i+1} \ \& \ \ldots \ \& \ P_n) \Rightarrow \neg P_i,$$

kde $1 \leq i \leq n$. Nový záver $\neg P_i$ sa, samozrejme, usilujeme vybrať čo najvýhodnejšie, na čo neexistuje jednoznačný recept, no časom sa nám azda podarí nadobudnúť cit, ktorým sa budeme môcť riadiť.

0.7.3. Dôkaz sporom. *Dôkaz sporom* do istej miery pripomína nepriamy dôkaz a často sa s ním zvykne zamieňať. Najmä začiatočník by mal k nemu siahnuť až vtedy, keď sa mu priamy ani nepriamy dôkaz nedarí, prípadne keď v ňom skrsne podozrenie, že dokazované tvrdenie neplatí. Namiesto dokazovanej implikácie $P \Rightarrow Q$ prijmeme predpoklad $P \ \& \ \neg Q$, ktorý je logicky ekvivalentný s jej negáciou $\neg(P \Rightarrow Q)$. Tento predpoklad sa usilujeme *doviesť k sporu*, čím sa myslí nejaký logicky absurdný záver, ako napr. $x \neq x$, alebo spor s niektorým z pôvodných predpokladov P, $\neg Q$, prípadne spor s niektorou z axióm alebo s niektorým zo skôr dokázaných tvrdení.

Na rozdiel od priameho alebo nepriameho dôkazu, dôkaz sporom nemá vopred stanovený smer určený nejakým známym záverom – ten by sa mal objaviť až v jeho priebehu. Ak sa ani pokus doviesť k sporu predpoklad $P \ \& \ \neg Q$ neskončí úspešne, je namieste pokúsiť sa ho dokázať, to znamená vyvrátiť pôvodnú hypotézu $P \Rightarrow Q$.

0.7.4. Dôkaz ekvivalencie. Niekedy sa nám môže podariť dokázať ekvivalenciu $P \Leftrightarrow Q$ postupnosťou logicky ekvivalentných krokov, no to je skôr výnimka než pravidlo. Vo všeobecnosti si jej dôkaz vyžaduje dokázať zvlášť každú z implikácií $P \Rightarrow Q$, $Q \Rightarrow P$. Pritom na každú z nich možno použiť ľubovoľnú z troch skôr spomínaných metód. Často sa jedna z uvedených implikácií dokazuje priamo a druhá nepriamo, teda dôkaz uvedenej ekvivalencie pozostáva napr. z priamych dôkazov implikácií $P \Rightarrow Q$ a $\neg P \Rightarrow \neg Q$.

V našom kurze sa neraz stretneme s vetami, v ktorých sa tvrdí ekvivalencia viacerých podmienok $P_1, \dots, P_n$. V tom je zahrnutých $n(n-1)$ jednotlivých implikácií $P_i \Rightarrow P_j$ pre rôzne $i, j \leq n$. Dokazovať ich všetky by pre $n \geq 3$ bolo značne neefektívne a taktiež zbytočné. Stačí totiž dokázať n implikácií tvoriacich cyklus

$$P_{\sigma(1)} \Rightarrow P_{\sigma(2)} \Rightarrow \dots \Rightarrow P_{\sigma(n-1)} \Rightarrow P_{\sigma(n)} \Rightarrow P_{\sigma(1)},$$

kde σ je ľubovoľná permutácia množiny indexov $\{1, \dots, n\}$, ktorú si volíme tak, aby to bolo čo najvýhodnejšie. S príkladmi všetkých uvedených typov dôkazov sa budeme v našom kurze neustále stretávať.

0.8. Matematická indukcia a rekurzia

Množinu všetkých nezáporných celých čísel značíme $\mathbb{N} = \{0, 1, 2, \dots,\}$ a nazývame ju tiež množinou všetkých *prirodzených čísel*.

0.8.1. Dôkaz matematickou indukciou. Platnosť nejakého tvrdenia $P(n)$ pre všetky prirodzené čísla, t. j. tvrdenie $(\forall n \in \mathbb{N})P(n)$ sa obvykle dokazuje *matematickou induk-*

ciou. Dôkaz indukciou spočíva v dôkaze dvoch tvrdení: nato, aby sme dokázali, že každé prirodzené číslo n má vlastnosť P, stačí dokázať, že platí

1° $P(0)$, t. j. 0 má vlastnosť P;

2° $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$,

t. j. ak n je ľubovoľné prirodzené číslo, ktoré má vlastnosť P, tak aj číslo

$n+1$ má vlastnosť P.

Štruktúru *dôkazu matematickou indukciou* tak možno zhrnúť do schémy

$$\big(P(0) \ \&\ (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))\big) \Rightarrow (\forall n \in \mathbb{N})P(n).$$

V bode 2° sa vlastne tvrdí platnosť všetkých implikácií $P(0) \Rightarrow P(1)$, $P(1) \Rightarrow P(2)$, $P(2) \Rightarrow P(3)$, … . Z bodu 1° a prvej z nich vyplýva $P(1)$, z toho spolu s druhou implikáciou dostávame $P(2)$, z čoho pomocou tretej implikácie plynie $P(3)$, atď.

Princíp matematickej indukcie je logicky ekvivalentný so zdanlivo očividným *princípom dobrého usporiadania*, ktorý tvrdí, že každá neprázdna množina $A \subseteq \mathbb{N}$ má najmenší prvok. Keďže pre väčšinu študentov býva tento princíp ľahšie prijateľný než princíp indukcie, predvedieme ako možno princíp indukcie z neho dokázať. Dôkaz princípu dobrého usporiadania z princípu indukcie prenechávame na rozmyslenie čitateľovi.

Predpokladajme teda platnosť princípu dobrého usporiadania. Nech P je vlastnosť taká, že platí $P(0)$ a $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$. Označme $A = \{n \in \mathbb{N};\ \neg P(n)\}$. Ak neplatí $(\forall n \in \mathbb{N})P(n)$, tak $A \neq \emptyset$. Nech m je najmenší prvok množiny A. Potom zrejme $m \neq 0$ a

$m-1 \notin A$, teda platí $P(m-1)$. No keďže $P(m-1) \Rightarrow P(m)$, platí $P(m)$, čiže $m \notin A$, čo je spor.

Z pedagogických dôvodov sa budeme (najmä spočiatku) pri dôkazoch indukciou odvolávať radšej na princíp dobrého usporiadania než na princíp indukcie, a tomu tiež podriadime redakciu dôkazu.

Poznámka. (a) Niekedy je potrebné miesto počiatočného tvrdenia 1° osobitne dokázať niekoľko prvých tvrdení $P(0), P(1), \dots, P(k)$ a potom prejsť k dôkazu modifikovaného tvrdenia 2°, totiž $(\forall\, n \geq k)(P(n) \Rightarrow P(n+1))$.

(b) Indukciou možno dokazovať aj tvrdenia tvaru $(\forall\, n \geq m)P(n)$, kde m je nejaké pevné prirodzené číslo. Stačí dokázať mierne upravené verzie tvrdení 1° a 2°: $P(m)$ a $(\forall\, n \geq m)(P(n) \Rightarrow P(n+1))$.

(c) Pri dôkaze indukciou možno bod 2° nahradiť tvrdením

$$(\forall\, n \in \mathbb{N})\big((P(0)\ \&\ \dots\ \&\ P(n)) \Rightarrow P(n+1)\big).$$

Inak povedané, pri dôkaze záveru $P(n+1)$ v bode 2° sa nemusíme opierať len o predpoklad $P(n)$, ale v prípade potreby môžeme ako predpoklady použiť všetky predchádzajúce tvrdenia $P(0), \dots, P(n)$. Takýto dôkaz indukciou sa vlastne riadi schémou

$$(\forall\, n \in \mathbb{N})\big((\forall\, k < n)P(k) \Rightarrow P(n)\big) \Rightarrow (\forall\, n \in \mathbb{N})P(n).$$

Rozmyslite si, ako je predpoklad 1°, t. j. tvrdenie $P(0)$, už zahrnutý v predpoklade novej schémy pre $n = 0$, t. j. v tvrdení $(\forall\, k < 0)(P(k) \Rightarrow P(0))$. Ďalej si premyslite, ako možno transpozíciou uvedenej implikácie priamo dostať matematickú formuláciu princípu dobrého usporiadania.

0.8.2. Rekurzia. Princíp matematickej indukcie sa používa nielen na dôkazy tvrdení o prirodzených číslach. Možno ho použiť aj na konštrukciu rôznych, či už konečných alebo nekonečných postupností. V takom prípade miesto indukcie budeme radšej hovoriť o postupnosti definovanej či zostrojenej *rekurziou*.

Nech X je množina a F je zobrazenie, ktoré každej konečnej postupnosti, (usporiadanej n-tici) $(x_1, \dots, x_n)$ prvkov z X (akejkoľvek dĺžky $n \in \mathbb{N}$) priradí nejaký prvok $F(x_1, \dots, x_n) \in X$. Pomocou zobrazenia F možno zostrojiť nekonečnú postupnosť $(a_n)_{n=0}^{\infty}$ prvkov z X tak, že položíme

$$a_0 = F(\emptyset), \qquad a_{n+1} = F(a_0, a_1, \dots, a_n)$$

pre každé $n \in \mathbb{N}$. V takom prípade, hovoríme, že postupnosť (a_n) je definovaná *rekurziou* pomocou zobrazenia F.

Druhú rovnosť možno samozrejme zapísať v tvare $a_n = F(a_0, a_1, \dots, a_{n-1})$ pre $n > 0$. Taktiež možno definíciu rekurziou obmedziť len na nejaký počiatočný úsek $0, 1, \dots, n$ množiny prirodzených čísel a dostať tak rekurziou konečnú postupnosť $(a_0, a_1, \dots, a_n)$. Niekedy rekurziu začíname nie od nuly ale od jednotky, prípadne od ľubovoľného prirodzeného čísla k.

Prvým členom postupnosti (a_n) zostrojenej rekurziou pomocou zobrazenia F je prvok $a_0 = F(\emptyset) \in X$. Ďalšie členy potom vyzerajú takto: $a_1 = F(a_0)$, $a_2 = F(a_0, a_1)$, $a_3 = F(a_0, a_1, a_2)$, …, $a_n = F(a_0, \dots, a_{n-1})$, $a_{n+1} = F(a_0, \dots, a_n)$, atď.

Najčastejšie sa stretáme s prípadom, keď sa pri rekurzívnej konštrukcii člena a_{n+1} nepoužíva celá predchádzajúca časť postupnosti $(a_0, \dots, a_n)$ ale len jej posledný člen a_n. Napríklad v aritmetickej postupnosti reálnych čísel s počiatočným členom a_0 a diferenciou

d platí $a_{n+1} = a_n + d$; podobne rekurentný vzťah pre geometrickú postupnosť reálnych čísel s počiatočným členom a_0 a kvocientom q má tvar $a_{n+1} = qa_n$.

Iným známym číselným príkladom je tzv. *Fibonacciho postupnosť* $(\phi_n)_{n=0}^{\infty}$, ktorej rekurzívna definícia

$$\phi_0 = \phi_1 = 1, \qquad \phi_{n+2} = \phi_n + \phi_{n+1}$$

používa dva predchádzajúce členy. Rozmyslite si, ako táto definícia zapadá do našej všeobecnej schémy.

0.8.3. Príklad. *Bellove čísla* sú definované rekurziou

$$B_0 = 1, \qquad B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k,$$

pri ktorej sa využívajú všetky predchádzajúce členy. Pre istotu pripomíname, že

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}$$

označuje *binomický koeficient* alebo *kombinačné číslo* udávajúce počet všetkých k-prvkových podmnožín n-prvkovej množiny.

Vypočítame niekoľko počiatočných hodnôt Bellových čísel:

$$B_0 = 1, \qquad B_1 = \binom{0}{0} B_0 = 1, \qquad B_2 = \binom{1}{0} B_0 + \binom{1}{1} B_1 = 2,$$

$$B_3 = \binom{2}{0} B_0 + \binom{2}{1} B_1 + \binom{2}{2} B_2 = 5,$$

$$B_4 = \binom{3}{0} B_0 + \binom{3}{1} B_1 + \binom{3}{2} B_2 + \binom{3}{3} B_3 = 15,$$

$$B_5 = \binom{4}{0} B_0 + \binom{4}{1} B_1 + \binom{4}{2} B_2 + \binom{4}{3} B_3 + \binom{4}{4} B_4 = 52,$$

$$B_6 = \binom{5}{0} B_0 + \binom{5}{1} B_1 + \binom{5}{2} B_2 + \binom{5}{3} B_3 + \binom{5}{4} B_4 + \binom{5}{5} B_5 = 203, \ \ldots$$

Matematickou indukciou teraz dokážeme, že počet všetkých rozkladov n-prvkovej množiny (teda aj ekvivalencií na n-prvkovej množine) je rovný číslu B_n. Zrejme na prázdnej možine existuje jediný rozklad $\mathcal{R} = \emptyset$. Predpokladajme teraz, že pre každé $k \leq n$ existuje práve B_k rozkladov k-prvkovej množiny. Všetky rozklady $(n+1)$-prvkovej množiny $\{0, 1, \ldots, n\}$ možno získať nasledujúcim spôsobom:

(1) zvolíme si ľubovoľné $k \leq n$ a ľubovoľnú k-prvkovú podmnožinu A množiny $\{1, \ldots, n\}$ – to pre dané k možno urobiť práve $\binom{n}{k}$ spôsobmi;

(2) vezmeme ľubovoľný rozklad $\mathcal{R}$ množiny A – ten podľa indukčného predpokladu možno vybrať práve B_k spôsobmi – a množinu $A' = \{0, 1, \dots, n\} \setminus A$ pridáme k pôvodnému rozkladu $\mathcal{R}$.

Zrejme sme takto získali nejaký rozklad $\mathcal{R}_A = \mathcal{R} \cup \{A'\}$ $(n+1)$-prvkovej množiny $\{0, 1, \dots, n\}$, pričom každý rozklad $\mathcal{S}$ množiny $\{0, 1, \dots, n\}$ má tvar $\mathcal{S} = \mathcal{R}_A$ pre jednoznačne určenú dvojicu $(\mathcal{R}, A)$. Všetkých rozkladov $(n+1)$-prvkovej množiny teda je $\sum_{k=0}^{n} \binom{n}{k} B_k = B_{n+1}$.

Cvičenia

0.1. Pre ľubovoľné množiny X, Y sú nasledujúce štyri podmienky ekvivalentné:
(i) $X \subseteq Y$, (ii) $X \cap Y = X$, (iii) $X \cup Y = Y$, (iv) $X \setminus Y = \emptyset$.
Dokážte.

0.2. Vzťah inklúzie je reflexívny a tranzitívny, t. j. pre ľubovoľné množiny X, Y, Z platí:
(a) $X \subseteq X$; (b) $X \subseteq Y \;\&\; Y \subseteq Z \;\Rightarrow\; X \subseteq Z$
Dokážte. Nájdite príklad dosvedčujúci, že nie je symetrický.

0.3. Nech $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ označuje množinu všetkých celých čísel. Pre každé $0 \neq n \in \mathbb{Z}$ označme $n\mathbb{Z} = \{nx;\, x \in \mathbb{Z}\}$ množinu všetkých celých čísel deliteľných číslom n. Dokážte, že pre ľubovoľné nenulové celé čísla m, n platí
(a) $m\mathbb{Z} \subseteq n\mathbb{Z} \;\Leftrightarrow\; m$ je násobkom n;
(b) $m\mathbb{Z} = n\mathbb{Z} \;\Leftrightarrow\; |m| = |n|$;
(c) $m\mathbb{Z} \cap n\mathbb{Z} = k\mathbb{Z}$, kde k je najmenší spoločný násobok čísel m a n;
(d) Môže pre niektoré m, n nastať rovnosť $m\mathbb{Z} \cap n\mathbb{Z} = \emptyset$, prípadne $m\mathbb{Z} \cap n\mathbb{Z} = \{0\}$? Zdôvodnite.

0.4. Pre ľubovoľné množiny X, Y, Z platí

$$
\begin{aligned}
X \cap Y &= Y \cap X, & X \cup Y &= Y \cup X,\\
X \cap (Y \cap Z) &= (X \cap Y) \cap Z, & X \cup (Y \cup Z) &= (X \cup Y) \cup Z,\\
X \cap X &= X, & X \cup X &= X,\\
X \cap \emptyset &= \emptyset, & X \cup \emptyset &= X,\\
X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z), & X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z),\\
X \setminus X &= \emptyset, & X \setminus \emptyset &= X,\\
X \cap (Y \setminus X) &= \emptyset, & X \cup (Y \setminus X) &= X \cup Y,\\
(X \cap Y) \setminus Z &= (X \setminus Z) \cap (Y \setminus Z), & (X \cup Y) \setminus Z &= (X \setminus Z) \cup (Y \setminus Z),\\
X \setminus (Y \cap Z) &= (X \setminus Y) \cup (X \setminus Z), & X \setminus (Y \cup Z) &= (X \setminus Y) \cap (X \setminus Z),\\
(X \setminus Y) \setminus Z &= X \setminus (Y \cup Z), & X \setminus (Y \setminus Z) &= (X \setminus Y) \cup (X \cap Z),\\
(X \setminus Y) \cap Z &= (X \cap Z) \setminus Y, & (X \setminus Y) \cup Z &= (X \cup Z) \setminus (Y \setminus Z).
\end{aligned}
$$

Dokážte. Pomenujte niektoré z uvedených vlastností binárnych operácií $\cap$, $\cup$ a $\setminus$ (komutatívnosť, asociatívnosť, …).

0.5. Pre ľubovoľné množiny X, Y, Z platí

$$
\begin{aligned}
X \times (Y \cap Z) &= (X \times Y) \cap (X \times Z), & X \times (Y \cup Z) &= (X \times Y) \cup (X \times Z),\\
X \times (Y \setminus Z) &= (X \times Y) \setminus (X \times Z), & X \times \emptyset &= \emptyset.
\end{aligned}
$$

Dokážte. Napíšte analogické vzťahy distributívnosti karteziánskeho súčinu vzhľadom na operácie prieniku, zjednotenia a množinového rozdielu pri násobení sprava.

0.6. Nech X, Y, Z sú ľubovoľné množiny. Nájdite čo najprirodzenejšiu bijekciu a k nej inverzné zobrazenie medzi každou z nasledujúcich dvojíc množín (množina $\mathcal{P}(X)$ všetkých podmnožín množiny

X z časti (f) sa nazýva *potenčná množina* množiny X):

(a) $X \times Y$, $Y \times X$;

(b) $X \times (Y \times Z)$, $(X \times Y) \times Z$;

(c) $(X \times Y)^Z$, $X^Z \times Y^Z$;

(d) $X^{Y \times Z}$, $\left(X^Y\right)^Z$;

(e) X^n, $X^{\{1,\dots,n\}}$;

(f) $\{0,1\}^X$, $\mathcal{P}(X) = \{A;\ A \subseteq X\}$;

(g) $X^{Y \cup Z}$, $X^Y \times X^{Z \smallsetminus Y}$;

(h) $X^Y \times X^Z$, $X^{(Y \times \{0\}) \cup (Z \times \{1\})}$.

0.7. Nech $\mathbb{R}$ označuje množinu všetkých reálnych čísel. Funkcie $f, g, h : \mathbb{R} \to \mathbb{R}$ sú dané predpismi $f(x) = (x+1)^2$, $g(x) = 1 - \sin 2x$, $h(x) = \mathrm{e}^{-x}$. Napíšte a zjednodušte predpisy pre zložené funkcie $f \circ f$, $f \circ g$, $g \circ f$, $f \circ h$, $h \circ f$, $g \circ h$, $h \circ g$, $f \circ g \circ h$, $h \circ g \circ f$, $g \circ f \circ h$ a $g \circ h \circ f$.

0.8. Nech $f : X \to Y$, $g : Y \to Z$ sú ľubovoľné zobrazenia. Dokážte postupne nasledujúce tvrdenia:
(a) Ak f, g sú injektívne, tak aj $g \circ f$ je injektívne.
(b) Ak f, g sú surjektívne, tak aj $g \circ f$ je surjektívne.
(c) Ak f, g sú bijektívne, tak aj $g \circ f$ je bijektívne.
(d) Ak $g \circ f$ je injektívne, tak aj f je injektívne.
(e) Ak $g \circ f$ je surjektívne, tak aj g je surjektívne.
(f) Ak $g \circ f$ je bijektívne, tak f je injektívne a g je surjektívne.

Na príklade ukážte, že v prípade (f) g nemusí byť injektívne ani f surjektívne. Čo z toho vyplýva pre prípady (d) a (e)?

0.9. Pre ľubovoľné zobrazenia $f : X \to Y$, $g : Y \to Z$ a množiny $A \subseteq X$, $B \subseteq Z$ dokážte rovnosti:

(a) $(g \circ f)(A) = g(f(A))$;

(b) $(g \circ f)^{-1}(B) = f^{-1}(g^{-1}(B))$.

0.10. Nech $f : X \to Y$ je ľubovoľné zobrazenie. Potom pre všetky A, $B \subseteq X$, C, $D \subseteq Y$ platí

(a) $A \subseteq B \Rightarrow f(A) \subseteq f(B)$;

(b) $C \subseteq D \Rightarrow f^{-1}(C) \subseteq f^{-1}(D)$;

(c) $f(A \cap B) \subseteq f(A) \cap f(B)$;

(d) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$;

(e) $f(A \cup B) = f(A) \cup f(B)$;

(f) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$;

(g) $f(A \smallsetminus B) \supseteq f(A) \smallsetminus f(B)$;

(h) $f^{-1}(C \smallsetminus D) = f^{-1}(C) \smallsetminus f^{-1}(D)$;

(i) $f^{-1}(f(A)) \supseteq A$;

(j) $f\big(f^{-1}(C)\big) \subseteq C$.

Dokážte. Na príkladoch sa presvedčte, že inklúzie v prípadoch (c), (g), (i) a (j) nemožno zameniť rovnosťami. Ukážte, že rovnosť pre všetky A, $B \subseteq X$ je v ľubovoľnom z prípadov (c), (g) a (i) ekvivalentná s injektívnoťou zobrazenia f. Podobne je rovnosť pre každé $C \subseteq Y$ v prípade (j) ekvivalentná so surjektívnosťou f.

0.11. Nech $f : X \to Y$, $g : Y \to Z$ sú bijektívne zobrazenia. Potom $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Dokážte. Odvoďte z toho, že pre každú permutáciu $\sigma \in \mathcal{S}_n$ platí $|\sigma| = |\sigma^{-1}|$ a $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$.

0.12. (a) Sformulujte pojmy ľavého a pravého neutrálneho prvku binárnej operácie $*$ na množine X.
(b) Nech $x \triangleright y = y$ pre všetky $x, y \in X$. Je táto binárna operácia na množine X asociatívna resp. komutatívna? Nájdite všetky ľavé a všetky pravé neutrálne prvky operácie $\triangleright$.
(c) Predpokladajme, že e je jediným neutrálnym prvkom (či už ľavým, pravým alebo obojstranným) binárnej operácie $*$ na množine X. Sformulujte pojmy ľavého a pravého inverzného prvku k danému prvku $x \in X$.
(d) Pomocou multiplikatívnej tabuľky nájdite príklad (neasociatívnej) binárnej operácie $*$ na množine X, ktorá má jediný (obojstranný) neutrálny prvok e, pričom niektorý prvok $a \in X$ má jediný ľavý inverzný a dva rôzne pravé inverzné prvky, a iný prvok $b \in X$ má jediný ľavý inverzný no žiadny pravý inverzný prvok. Aké situácie môžu ešte nastať? (Pozri cvičenie 0.18.)

0.13. Nech $\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ sú permutácie množiny $\{1, 2, 3, 4\}$. Vypočítajte permutácie σ^{-1}, ϱ^{-1} $\sigma \circ \varrho$, $\varrho \circ \sigma$, $\sigma \circ \varrho^{-1}$, $\varrho \circ \sigma^{-1}$ a $\varrho^{-1} \circ \sigma \circ \varrho$.

0.14. Nech $1 \le i \le n \in \mathbb{N}$. Permutácia $\alpha \in \mathcal{S}_n$ sa nazýva *i-cyklus*, ak na nejakej i-prvkovej množine $\{a_1, a_2, \dots, a_i\} \subseteq \{1, 2, \dots, n\}$ operuje cyklicky podľa schémy $\alpha : a_1 \mapsto a_2 \mapsto \dots \mapsto a_i \mapsto a_1$ a na zvyšku množiny $\{1, \dots, n\}$ identicky, t. j. $\alpha(a) = a$ pre $a \in \{1, \dots, n\} \smallsetminus \{a_1, \dots, a_i\}$. Skrátene

píšeme $\alpha = (a_1, \ldots, a_i)$. Dva *cykly* $\alpha = (a_1, \ldots, a_i)$, $\beta = (b_1, \ldots, b_j)$ sa nazývajú *disjunktné*, ak $\{a_1, \ldots, a_i\} \cap \{b_1, \ldots, b_j\} = \emptyset$. Zrejme identickú permutáciu možno považovať za 1-cyklus a každá transpozícia je 2-cyklus. Dokážte postupne nasledujúce tvrdenia:
(a) Nech $\alpha, \beta \in \mathcal{S}_n$ sú dva cykly. Potom $\alpha \circ \beta = \beta \circ \alpha$ práve vtedy, keď cykly α, β sú disjunktné alebo aspoň jeden z nich je 1-cyklus.
(b) Každá permutácia $\sigma \in \mathcal{S}_n$, je kompozíciou disjunktných cyklov $\sigma = \alpha_1 \circ \ldots \circ \alpha_k$. Ak do tejto kompozície zahrnieme aj všetky 1-cykly, tak uvedený rozklad je určený jednoznačne až na poradie jednotlivých cyklov. (*Návod*: Vytvorte cyklus $(1, \sigma(1), \sigma^2(1), \ldots, \sigma^{i-1}(1))$. Na zvyšku množiny $\{1, \ldots, n\}$, ak nejaký zostal, postup opakujte.)
(c) Každý cyklus je kompozíciou transpozícií (napr. $(1, 2, \ldots, n) = (1, n) \circ \ldots \circ (1, 3) \circ (1, 2)$).
(d) Každá permutácia $\sigma \in \mathcal{S}_n$ je kompozíciou transpozícií.
(e) Dĺžka i-cyklu α je $|\alpha| = i - 1$ a jeho znak je $\operatorname{sgn} \alpha = (-1)^{i-1}$.
(f) Nech $\sigma = \alpha_1 \circ \ldots \circ \alpha_k$ je rozklad permutácie σ na disjunktné cykly, pričom α_j je i_j-cyklus. Potom dĺžka permutácie σ je $|\sigma| = i_1 + \ldots + i_k - k$ a jej znak je $\operatorname{sgn} \sigma = (-1)^{i_1 + \ldots + i_k - k}$. Ak uvedený rozklad zahŕňa aj všetky 1-cykly, tak $|\sigma| = n - k$ a $\operatorname{sgn} \sigma = (-1)^{n-k}$.

0.15. (a) Rozložte každú z permutácií zo zadania aj výsledkov v cvičení 0.11 na kompozíciu disjunktných cyklov (vrátane 1-cyklov) a pre každú z nich určte jej dĺžku a znamienko.
(b) Spočítajte pre každú z uvedených permutácií počet jej inverzií a porovnajte s jej dĺžkou. Presvedčte sa, že obe čísla sa nemusia rovnať, no vždy majú rovnakú paritu.
(c) Rozložte permutáciu $\tau = (1, 3, 5, 7) \circ (1, 2) \circ (2, 4, 6, 8) \circ (4, 5, 6) \in \mathcal{S}_{10}$ na *disjunktné* cykly (vrátane 1-cyklov) a určte jej dĺžku a znamienko.

0.16. (a) Nech $n \in \mathbb{Z}$ (pozri cvičenie 0.3). Dokážte, že vzťahom $x \equiv_n y \;\Leftrightarrow\; x - y \in n\mathbb{Z}$ je definovaná ekvivalencia na množine $\mathbb{Z}$. Túto ekvivalenciu značíme tiež $x \equiv y \mod n$ a nazývame ju *kongruenciou modulo* n.
(b) Predpokladajme, že $n > 0$, a označme $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \{x \in \mathbb{Z};\, 0 \le x < n\}$. Potom $(\forall\, x \in \mathbb{Z})(\exists! z \in \mathbb{Z}_n)(x \equiv_n z)$. Dokážte. Toto jednoznačne určené $z \in \mathbb{Z}_n$ nazývame *zvyškom po delení* čísla x číslom n.
(c) Pre ľubovoľné $n \in \mathbb{Z}$ platí $(\forall\, x, y, u, v \in \mathbb{Z})(x \equiv_n y \;\&\; u \equiv_n v \;\Rightarrow\; x + u \equiv_n y + v \;\&\; xu \equiv_n yv)$.

(d) Ako vyzerajú triedy rozkladu množiny $\mathbb{Z}$ podľa kongruencie $\equiv_n$?

0.17. Matematickou indukciou dokážte nasledujúce vzorce:
(a) $\sum_{i=1}^{n} i = 1 + 2 + \ldots + n = \frac{1}{2}n(n+1)$;
(b) $\sum_{j=1}^{n} j(j+1) = 1\cdot 2 + 2\cdot 3 + \ldots + n(n+1) = \frac{1}{3}n(n+1)(n+2)$;
(c) $\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1)$;
(d) $\sum_{k=0}^{n} q^k = 1 + q + q^2 + \ldots + q^n = \frac{q^{n+1}-1}{q-1}$, $(q \neq 1)$;
(e) $\sum_{p=1}^{n} \sin px = \sin x + \sin 2x + \ldots + \sin nx = \frac{\sin(nx/2)\sin((n+1)x/2)}{\sin(x/2)}$, $(x \neq 2k\pi,\ k \in \mathbb{Z})$;
(f) $\sum_{p=0}^{n} \cos px = \cos 0 + \cos x + \ldots + \cos nx = \frac{\cos(nx/2)\sin((n+1)x/2)}{\sin(x/2)}$, $(x \neq 2k\pi,\ k \in \mathbb{Z})$;
(g) $\phi_n = \frac{\left(1+\sqrt{5}\right)^{n+1} - \left(1-\sqrt{5}\right)^{n+1}}{2^{n+1}\sqrt{5}}$, ($\phi_n$ sú Fibonacciho čísla).

0.18. (a) Priamym výpočtom overte, že binomické koeficienty $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ vyhovujú rovnosti $\binom{n}{k} = \binom{n}{n-k}$ a pravidlám *Pascalovho trojuholníka*, t. j. $\binom{n}{0} = \binom{n}{n} = 1$ a $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ pre $1 \leq k \leq n$.
(b) Označme $C(n,k)$ počet všetkých k-prvkových podmnožín n-prvkovej množiny. Kombinatorickou úvahou dokážte, že aj tzv. *kombinačné čísla* $C(n,k)$ vyhovujú pravidlám Pascalovho trojuholníka, t. j. $C(n,0) = C(n,n) = 1$ a $C(n+1,k) = C(n,k-1) + C(n,k)$ pre $1 \leq k \leq n$.
(c) Na základe (a) a (b) odvoďte známy vzorec $C(n,k) = \binom{n}{k}$. Kde treba pritom použiť matematickú indukciu?
(d) Pre $k > n$ dodefinujme $\binom{n}{k} = C(n,k) = 0$. Predpisom $n * k = C(n,k)$ je tak definovaná binárna operácia na množine $\mathbb{N}$. Je táto operácia komutatívna resp. asociatívna? Má nejaký ľavý resp. pravý neutrálny prvok? (Pozri cvičenie 0.12.) Ako je to s prípadnými ľavými či pravými inverznými prvkami?
(e) Riešte úlohu (d) aj pre binárnu operáciu $n \bullet k = C(n+k,k) = \frac{(n+k)!}{n!\,k!}$ na množine $\mathbb{N}$.

0.19. Matematickou indukciou dokážte princíp dobrého usporiadania množiny $\mathbb{N}$ (t. j. každá neprázdna

podmnožina A množiny $\mathbb{N}$ má najmenší prvok).
(*Návod*: Transponujte implikáciu $(\forall\, n \in \mathbb{N})\big((\forall\, k < n)P(k) \Rightarrow P(n)\big) \Rightarrow (\forall\, n \in \mathbb{N})P(n)$, a nahraďte vlastnosť $P(n)$ vlastnosťou $n \notin A$.)

1. Polia a vektorové priestory

V tejto kapitole zavedieme dva druhy algebraických štruktúr, ktoré budú hrať v celom ďalšom výklade kľúčovú úlohu, a dokážeme o nich niekoľko jednoduchých základných tvrdení. Ide štruktúry, ktoré zahŕňame pod pojem *poľa* a pojem *vektorového priestoru*.

Prvky poľa budeme nazývať *skaláry*, a niekedy len čísla. Fyzikálne ich možno interpretovať ako hodnoty fyzikálnych veličín, ktoré sú určené iba svojou veľkosťou a znamienkom. Prvky vektorového priestoru, t. j. *vektory*, zasa zodpovedajú fyzikálnym veličinám, ktoré sú okrem veľkosti určené tiež smerom a orientáciou.

1.1. Základné číselné obory

Predpokladáme, že čitateľ pozná základné číselné obory, ako sú *prirodzené čísla*, *celé čísla*, *racionálne čísla*, *reálne čísla* a *komplexné čísla*. Každý z týchto číselných oborov tvorí množinu. Dohodneme sa, že ich budeme označovať tzv. tučnými tabuľovými písmenami:

$\mathbb{N}$ – množina všetkých prirodzených čísel,
$\mathbb{Z}$ – množina všetkých celých čísel,
$\mathbb{Q}$ – množina všetkých racionálnych čísel,
$\mathbb{R}$ – množina všetkých reálnych čísel,
$\mathbb{C}$ – množina všetkých komplexných čísel.

Ešte poznamenajme, že i nulu považujeme za prirodzené číslo, t. j. $0 \in \mathbb{N}$. *Imaginárnu jednotku* (ktorá je prvkom $\mathbb{C} \setminus \mathbb{R}$) budeme značiť $\imath$.

Konštatovaním, že uvedené číselné obory tvoria množiny, sme však ich štruktúru zďaleka nevyčerpali. Omnoho dôležitejšie je, že na každej z týchto množín sú definované dve binárne operácie, *sčítanie* $+$ a *násobenie* $\cdot$. Pritom na každej z uvedených množín sú obe tieto operácie asociatívne a komutatívne. Navyše, násobenie je (z oboch strán) *distributívne* vzhľadom na sčítanie, t. j. pre všetky prvky x, y, z príslušnej množiny platí

$$x(y+z) = xy + xz, \qquad (x+y)z = xz + yz.$$

Číselný obor $\mathbb{N}$ je v porovnaní s obormi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ akýsi „chudobnejší“ – kým rovnice tvaru $x+a=b$ majú v oboroch $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ riešenie $x=b-a$ pre ľubovoľné a, b, v $\mathbb{N}$ je takáto rovnica riešiteľná len ak $a \leq b$. Obory $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ sú však „bohatšie“ nielen v porovnaní s $\mathbb{N}$ no i so $\mathbb{Z}$ – rovnice tvaru $ax=b$ majú v oboroch $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ riešenie pre ľubovoľné $a \neq 0$ a b, kým v $\mathbb{N}$ či $\mathbb{Z}$ sú riešiteľné len ak a je deliteľom b.

Nás budú zaujímať práve vlastnosti číselných oborov $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ s operáciami sčítania a násobenia. Pritom využijeme, že uvedené operácie na týchto oboroch majú rad spoločných vlastností, čo nám umožňuje skúmať ich do veľkej miery jednotným spôsobom a súčasne. To dosiahneme tým, že sformulujeme abstraktný pojem *poľa*, pod ktorý zahrnieme všetky spomínané prípady, ako i mnohé ďalšie, ktoré sa nám objavia až akosi dodatočne. Ako sme spomínali už v úvode, práve takýto prístup je charakteristický pre algebru, presnejšie, v ňom spočíva jej podstata.

1.2. Polia

Poľom nazývame množinu K s dvoma význačnými prvkami – *nulou* 0 a *jednotkou* 1 – a dvomi binárnymi operáciami na K – *sčítaním* $+$ a *násobením* $\cdot$ – takými, že platí

$$\begin{array}{ll} (\forall\, a,b \in K)(a+b=b+a), & (\forall\, a,b \in K)(a\cdot b=b\cdot a),\\ (\forall\, a,b,c \in K)(a+(b+c)=(a+b)+c), & (\forall\, a,b,c \in K)(a\cdot(b\cdot c)=(a\cdot b)\cdot c),\\ (\forall\, a \in K)(a+0=a), & (\forall\, a \in K)(1\cdot a=a),\\ (\forall\, a \in K)(\exists\, b \in K)(a+b=0), & (\forall\, a \in K \smallsetminus \{0\})(\exists\, b \in K)(a\cdot b=1),\\ (\forall\, a,b,c \in K)(a\cdot(b+c)=(a\cdot b)+(a\cdot c)), & 0 \neq 1. \end{array}$$

Teda sčítanie a násobenie v poli sú komutatívne a asociatívne operácie a násobenie je distributívne vzhľadom na sčítanie. Ďalej 0 je neutrálny prvok sčítania a 1 je neutrálny prvok násobenia, pričom tieto dva prvky sú rôzne. Jednoducho možno nahliadnuť, že prvok $b \in K$ taký, že $a+b=0$, t. j. inverzný prvok vzhľadom na operáciu sčítania, je k danému prvku $a \in K$ určený jednoznačne (pozri paragraf 0.4). Tento jednoznačne určený prvok k danému a označujeme $-a$ a nazývame *opačný prvok* k a. Miesto $a+(-b)$ zvykneme písať len $a-b$. Takisto prvok $b \in K$ taký, že $a \cdot b = 1$, je k danému $0 \neq a \in K$ určený jednoznačne – označujeme ho a^{-1} alebo $\frac{1}{a}$, prípadne $1/a$ a nazývame *inverzný prvok* k a alebo *prevrátená hodnota* prvku a. Miesto $a \cdot b^{-1}$ píšeme tiež $\frac{a}{b}$ alebo a/b.

Znak násobenia budeme väčšinou vynechávať a násobenie bude mať prednosť pred sčítaním, teda napr. miesto $(a\cdot b)+c$ budeme písať len $ab+c$. Asociatívnosť nám umožňuje vynechávať zátvorky a súčty či súčiny ľubovoľných konečných postupností prvkov poľa jednoznačne zapisovať v tvare $a_1+a_2+\ldots+a_n$ resp. $a_1\cdot a_2\cdot\ldots\cdot a_n$ prípadne len $a_1a_2\ldots a_n$;

komutatívnosť nám navyše dovoľuje nestarať sa o poradie sčítancov resp. činiteľov. Kvôli úplnosti sa dohodneme, že pre $n = 1$ sa oba uvedené výrazy rovnajú a_1; pre $n = 0$ kladieme prázdny súčet rovný 0 a prázdný súčin rovný 1. Ak $a_1 = \ldots = a_n = a$, tak miesto $a_1 + \ldots + a_n$ píšeme na a miesto $a_1 \ldots a_n$ len a^n.

Teraz si ukážeme, ako možno niektoré najzákladnejšie pravidlá počítania, na ktoré sme zvyknutí v číselných oboroch $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$, odvodiť len z axióm poľa. Zhrnieme ich do nasledujúceho tvrdenia. Okrem iného z neho vyplýva, že k 0 nemôže v poli existovať inverzný prvok (podmienka (c)).

1.2.1. Tvrdenie. *Nech K je pole. Potom pre ľubovoľné $n \in \mathbb{N}$ a $a, b, c, b_1, \ldots, b_n \in K$ platí*

(a) $a + b = a + c \;\Rightarrow\; b = c$,

(b) $(ab = ac \;\&\; a \neq 0) \;\Rightarrow\; b = c$,

(c) $a0 = 0$,

(d) $ab = 0 \;\Rightarrow\; (a = 0 \,\vee\, b = 0)$,

(e) $-a = (-1)a$,

(f) $a(b - c) = ab - ac$,

(g) $a(b_1 + \ldots + b_n) = ab_1 + \ldots + ab_n$.

Dôkaz. (a), (b) Keďže obe podmienky možno dokázať v podstate rovnako, urobíme to len pre druhú z nich. Z $ab = ac$ vyplýva $a^{-1}ab = a^{-1}ac$. Ľavá strana sa rovná b a pravá c.

(c) $a0 + a0 = a(0 + 0) = a0 = a0 + 0$. Podľa (a) z toho vyplýva $a0 = 0$.

(d) Nech $ab = 0$. Potom podľa (c) $ab = 0 = a0$. Ak $a \neq 0$, tak podľa (b) z toho vyplýva $b = 0$.

(e) Vďaka jednoznačnosti opačného prvku k a stačí overiť, že $(-1)a+a = 0$. Jednoduchý výpočet dáva $(-1)a + a = (-1)a + 1a = (-1 + 1)a = 0a = 0$ podľa (c).

(f) Podľa (e) $a(b - c) = a(b + (-1)c) = ab + a(-1)c = ab + (-1)ac = ab - ac$.

(g) Rovnosť zrejme platí pre $n = 0, 1, 2$. Keby neplatila pre všetky prirodzené čísla, označme n najmenšie prirodzené číslo, pre ktoré existujú $a, b_1, \ldots, b_n \in K$ také, že uvedená rovnosť neplatí. Potom $n > 2$ a pre $n - 1$ rovnosť platí. Preto

$$a(b_1 + \ldots + b_{n-1} + b_n) = a(b_1 + \ldots + b_{n-1}) + ab_n = ab_1 + \ldots + ab_{n-1} + ab_n.$$

To je však spor.

Doplňme, že podmienky (a) a (b) sa nazývajú *zákony o krátení* pre sčítanie resp. násobenie v poli.

Podmienka (e) nám umožňuje zaviesť ľubovoľné celočíselné násobky prvkov z poľa. Pre $a \in K$, $n \in \mathbb{N}$ kladieme $(-n)a = -(na) = n(-a)$. Podobne možno pre nenulové prvky poľa zaviesť i ľubovoľné celočíselné mocniny. Pre $0 \neq a \in K$, $n \in \mathbb{N}$ kladieme $a^{-n} = (a^n)^{-1} = (a^{-1})^n$.

Čitateľovi prenechávame, aby si sám odvodil nasledujúce rovnosti známe z bežných číselných oborov:

$$
\begin{array}{ll}
0a = 0, \quad 1a = a, & a \in K, \\
n(a+b) = na + nb, & a, b \in K,\ n \in \mathbb{Z}, \\
(m+n)a = ma + na, & a \in K,\ m, n \in \mathbb{Z}, \\
(mn)a = m(na), & a \in K,\ m, n \in \mathbb{Z}, \\
(mn)(ab) = (ma)(nb), & a, b \in K,\ m, n \in \mathbb{Z}, \\
a^0 = 1, \quad a^1 = a, & a \in K, \\
(ab)^n = a^n b^n, & a, b \in K,\ n \in \mathbb{Z},\ n < 0 \ \Rightarrow\ a \neq 0 \neq b, \\
a^{m+n} = a^m a^n, & a \in K,\ m, n \in \mathbb{Z},\ (m < 0 \vee n < 0) \ \Rightarrow\ a \neq 0, \\
a^{mn} = (a^m)^n, & a \in K,\ m, n \in \mathbb{Z},\ (m < 0 \vee n < 0) \ \Rightarrow\ a \neq 0,
\end{array}
$$

Ešte podotýkame, že v rovnostiach v prvom a šiestom riadku označujú 0 a 1 na ľavých stranách prirodzené čísla, t. j. prvky množiny $\mathbb{N}$, kým 0 a 1 na pravých stranách v prvom riadku označujú prvky poľa K. Vzhľadom na to, že pre všetky tri príklady polí, s ktorými sme doteraz stretli, platí $\mathbb{N} \subseteq K$, môže sa nám toto rozlíšenie zdať nepodstatné. Vo všeobecnosti však uvedená inklúzia platiť nemusí.

Nech K je pole a $L \subseteq K$. Hovoríme, že L je *podpole* poľa K, ak $0, 1 \in L$ a pre všetky $a, b \in L$ platí $a + b \in L$, $ab \in L$, $-a \in L$ a, ak $a \neq 0$, tak aj $a^{-1} \in L$. Inak povedané, podpole poľa K je taká jeho podmnožina L, ktorá obsahuje nulu a jednotku a je uzavretá vzhľadom na sčítanie, násobenie, opačný a inverzný prvok. Zrejme každé podpole poľa K je s týmito operáciami zúženými z K na L i samo poľom. Hovoríme tiež, že pole K je *rozšírením* poľa L.

Zrejme pole $\mathbb{Q}$ je podpoľom poľa $\mathbb{R}$ i poľa $\mathbb{C}$; pole $\mathbb{C}$ je rozšírením poľa $\mathbb{Q}$ aj $\mathbb{R}$.

Charakteristikou poľa K, označenie $\operatorname{char} K$, nazývame najmenšie kladné celé číslo n také, že $n1 = 0$; ak také n neexistuje, t. j. $n1 \neq 0$ pre každé celé $n > 0$, hovoríme že K má charakteristiku ∞ (niektorí autori vtedy kladú $\operatorname{char} K = 0$).

Ak pole K je rozšírením poľa L, tak polia K a L majú tú istú jednotku, preto $\operatorname{char} K = \operatorname{char} L$.

Zrejme $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = \infty$.

1.2.2. Veta. *Nech K je pole. Potom* $\operatorname{char} K$ *je ∞ alebo prvočíslo.*

Dôkaz Keďže $0 \neq 1$, zrejme $\operatorname{char} K > 1$. Predpokladajme, že $\operatorname{char} K = n$ je zložené číslo. Potom existujú celé čísla $k, l > 1$ také, že $n = kl$. Keďže $k, l < n$, je $k1 \neq 0 \neq l1$. Na druhej strane $(k1)(l1) = (kl)(1 \cdot 1) = n1 = 0$. Podľa tvrdenia 1.2.1.(d) z toho vyplýva $k1 = 0$ alebo $l1 = 0$, čo je spor.

1.3. Polia $\mathbb{Z}_p$

V tomto krátkom paragrafe si ukážeme príklady polí, ktorých charakteristika nie je ∞. Z toho dôvodu sa tieto polia výrazne odlišujú od našich dôverne známych číselných polí. Presnejšie, pre každé prvočíslo p zostrojíme isté konečné pole $\mathbb{Z}_p$, ktoré má p prvkov a charakteristiku p. Na druhej strane, spomínané číselné polia (ako vôbec všetky polia nekonečnej charakteristiky) sú nekonečné. Poznamenajme, že pre každé prvočíslo p a kladné celé číslo k existuje p^k-prvkové pole s charakteristikou p ako aj nekonečné polia charakteristiky p. Ich konštrukcia však presahuje rámec nášho úvodného kurzu.

Pre potreby matematickej analýzy, teda aj z hľadiska fyzikálnych aplikácií, sú najdôležitejšími poľami $\mathbb{R}$ a $\mathbb{C}$. Konečné polia však v súčasnosti zohrávajú dôležitú úlohu napr. v kódovaní a kryptografii.

Pre každé kladné celé číslo n označme

$$\mathbb{Z}_n = \{k \in \mathbb{N};\, k < n\} = \{0, 1, \dots, n-1\}.$$

Množinu $\mathbb{Z}_n$ zo zrejmých dôvodov (pozri cvičenie 0.12) nazývame *množinou zvyškových tried modulo* n. Na tejto množine teraz zavedieme dve binárne operácie – sčítanie $\oplus$ a násobenie $\odot$ (toto trochu ťažkopádne označenie budeme používať len v tomto paragrafe, neskôr sa vrátime k obvyklým $+$ a $\cdot$; v definícii však treba odlíšiť sčítanie a násobenie v $\mathbb{Z}_n$ od príslušných operácií v $\mathbb{Z}$). Pre $a, b \in \mathbb{Z}_n$ kladieme

$$\begin{aligned} a \oplus b &= \text{zvyšok po delení } (a+b) : n, \\ a \odot b &= \text{zvyšok po delení } (ab) : n. \end{aligned}$$

Čitateľovi prenechávame na overenie (prípadne na uverenie), že $\oplus$ a $\odot$ sú asociatívne a komutatívne operácie na $\mathbb{Z}_n$ a násobenie je distributívne vzhľadom na sčítanie. Ďalej 0 je neutrálny prvok sčítania a, pre $n > 1$, je 1 neutrálny prvok násobenia. Navyše $\ominus a = n - a$ je opačný prvok k $a \in \mathbb{Z}_n \setminus \{0\}$; pre $a = 0$ je samozrejme $\ominus 0 = 0$.

1.3.1. Veta. *Množina $\mathbb{Z}_n$ s operáciami $\oplus$ a $\odot$ je pole práve vtedy, keď n je prvočíslo.*

Dôkaz. Zrejme n je najmenšie kladné celé číslo také, že

$$n1 = \underbrace{1 \oplus \ldots \oplus 1}_{n\text{-krát}} = 0.$$

Preto, ak $\mathbb{Z}_n$ je pole, tak $\operatorname{char}\mathbb{Z}_n = n$, a podľa vety 1.2.2. je n prvočíslo.

Dokážeme, že $\mathbb{Z}_p$ je pole pre každé prvočíslo p. Najprv overíme, že v $\mathbb{Z}_p$ platí zákon o krátení

$$(a \odot b = a \odot c \ \& \ a \neq 0) \Rightarrow b = c.$$

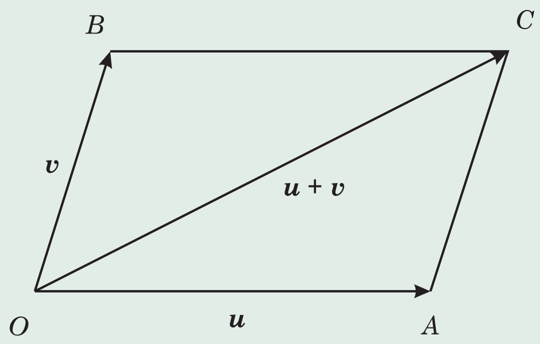
Rovnosť $a \odot b = a \odot c$ znamená, že číslo $ab - ac = a(b-c)$ je deliteľné číslom p. Keďže p je prvočíslo, musí byť aspoň jedno z čísel a, $b-c$ deliteľné číslom p. Nakoľko $0 < a < p$, može to byť len $b - c$. Pre $b, c \in \mathbb{Z}_p$ to však znamená $b = c$.

Zostáva overiť existenciu inverzného prvku ku každému $0 \neq a \in \mathbb{Z}_p$. Uvažujme postupnosť mocnín $a^1 = a$, $a^2 = a \odot a$, $a^3 = a \odot a \odot a$, $\dots$, atď. Keďže $a \neq 0$, z dokázaného krátenia vyplýva, že všetky jej členy sú nenulové. Pretože množina $\mathbb{Z}_p$ je konečná, nemôžu byť všetky členy uvedenej postupnosti rôzne. Musia preto existovať kladné celé čísla k, l také, že $a^k = a^{k+l} = a^k \odot a^l$. Potom platí $a^k \odot a^l = a^k \odot 1$, z čoho krátením dostávame $a^l = 1$. Keďže $a^l = a \odot a^{l-1}$, je $a^{-1} = a^{l-1}$ inverzný prvok k a.

Multiplikatívne tabuľky sčítania a násobenia v poli $\mathbb{Z}_5$ sme si ako príklady binárnych operácií uviedli v paragrafe 0.4).

1.4. Vektory v rovine a v trojrozmernom priestore

Vektory v rovine či v priestore si predstavujeme ako orientované úsečky, t. j. úsečky, ktorých jeden krajný bod považujeme za počiatočný a druhý za koncový – ten je označený šípkou. Pritom dve rovnako dlhé, rovnobežné a súhlasne orientované úsečky predstavujú ten istý vektor – hovoríme, že sú umiestneniami toho istého vektora. Ak si teda zvolíme nejaký



Obr. 1.1. Vektorový rovnobežník

pevný bod O, tak všetky vektory v rovine či priestore môžeme jednoznačne reprezentovať ako orientované úsečky $\overrightarrow{OA}$ s počiatkom v O, pričom ich koncom môže byť ľubovoľný bod A roviny či priestoru, bod O nevynímajúc – orientovaná úsečka $\overrightarrow{OO}$ totiž predstavuje tzv. nulový vektor.

Vektory v rovine i v priestore možno sčítať pomocou tzv. *vektorového rovnobežníka*. Súčet vektorov $\boldsymbol{u} = \overrightarrow{OA}$, $\boldsymbol{v} = \overrightarrow{OB}$ je potom znázornený orientovanou uhlopriečkou $\boldsymbol{u} + \boldsymbol{v} = \overrightarrow{OC}$ rovnobežníka, ktorého dve priľahlé strany tvoria úsečky OA, OB.

Vektory možno taktiež násobiť ľubovoľnými skalármi, t. j. reálnymi číslami: ak $c \in \mathbb{R}$ a $\boldsymbol{v}$ je vektor, tak $c\boldsymbol{v}$ je vektor, t. j. orientovaná úsečka s počiatkom v O, ktorej dĺžka je $|c|$-násobkom dĺžky úsečky $\boldsymbol{v}$, leží na tej istej priamke ako $\boldsymbol{v}$ a je orientovaná súhlasne s $\boldsymbol{v}$, ak $c > 0$, resp. nesúhlasne s $\boldsymbol{v}$, ak $c < 0$, (ak $c = 0$ alebo $\boldsymbol{v}$ je nulový vektor, tak, samozrejme, aj $c\boldsymbol{v}$ je nulový vektor, takže nezáleží na jeho smere ani orientácii).

Ak si okrem počiatku O zvolíme v rovine či priestore ešte dve resp. tri súradné osi, t. j. navzájom kolmé priamky prechádzajúce počiatkom, a na každej z nich jeden bod v rovnakej jednotkovej vzdialenosti od počiatku, dostaneme pravouhlý súradnicový systém v rovine či v priestore. Každý bod roviny či priestoru je potom jednoznačne určený usporiadanou dvojicou, resp. trojicou svojich súradníc a tiež naopak, každá dvojica resp. trojica súradníc jednoznačne určuje nejaký bod roviny či priestoru. Taktiež každý vektor v rovine či v priestore je potom jednoznačne určený súradnicami svojho koncového bodu a tiež naopak ľubovoľná usporiadaná dvojica resp. trojica súradníc jednoznačne určuje nejaký vektor v rovine či priestore. Pri pevnom súradnicovom systéme tak možno množinu všetkých vektorov v rovine stotožniť s množinou $\mathbb{R}^2$ a množinu všetkých vektorov v priestore s množinou $\mathbb{R}^3$.

Ak (pri takomto stotožnení) $\boldsymbol{u} = (u_1, u_2) \in \mathbb{R}^2$, $\boldsymbol{v} = (v_1, v_2) \in \mathbb{R}^2$ sú dva vektory v rovine, tak ľahko nahliadneme, že pre ich súčet $\boldsymbol{u} + \boldsymbol{v}$, daný vektorovým rovnobežníkom, platí

$$\boldsymbol{u} + \boldsymbol{v} = (u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2).$$

Ak $c \in \mathbb{R}$, tak pre skalárny násobok $c\boldsymbol{u}$ dostávame

$$c\boldsymbol{u} = c(u_1, u_2) = (cu_1, cu_2).$$

Podobne možno reprezentovať aj operácie súčtu a skalárneho násobku vektorov v priestore príslušnými operáciami na množine $\mathbb{R}^3$ všetkých usporiadaných trojíc reálnych čísel.

Ešte si všimnime, že predpoklady kolmosti súradných osí a rovnosti jednotkových dĺžok v jednotlivých smeroch nehrali v našich úvahách nijakú úlohu. Stačí, aby systém súradných osí tvorili dve rôznobežné priamky (v rovine) resp. tri nekomplanárne priamky (v priestore) pretínajúce sa v počiatku O. Za jednotkové dĺžky v smeroch jednotlivých súradných osí možno zvoliť dĺžky ľubovoľných (nie nevyhnutne rovnako dlhých) úsečiek.

Operácie súčtu vektorov a násobenia vektora skalárom majú rad vlastností, ktoré nie sú viazané len na ich špecifickú geometrickú reprezentáciu v rovine či priestore. Napríklad, prostredníctvom súradnicovej reprezentácie vektorov by sme ich mohli priamočiaro zovšeobecniť na usporiadané n-tice skalárov z ľubovoľného poľa K pre akékoľvek $n \in \mathbb{N}$. Tým by sme dostali akési „n-rozmerné vektorové priestory nad poľom K“. V duchu algebry teraz zadefinujeme abstraktný pojem vektorového priestoru nad daným poľom, pričom budeme abstrahovať od akýchkoľvek súradníc aj „dimenzie“. Podstatné budú pre nás len algebraické vlastnosti operácií súčtu vektorov a skalárneho násobku vektora. K spomínaným príkladom sa však budeme sústavne vracať.

1.5. Vektorové priestory

Nech K je pole. *Vektorovým* alebo tiež *lineárnym priestorom* nad poľom K nazývame množinu V s význačným prvkom $\mathbf{0}$ a dvomi binárnymi operáciami – *sčítaním* $+ : V \times V \to V$ a *násobením* $\cdot : K \times V \to V$ – takými, že platí

$$
\begin{aligned}
&(\forall\, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V)(\boldsymbol{x} + (\boldsymbol{y} + \boldsymbol{z}) = (\boldsymbol{x} + \boldsymbol{y}) + \boldsymbol{z})),\\
&(\forall\, \boldsymbol{x}, \boldsymbol{y} \in V)(\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{y} + \boldsymbol{x}),\\
&(\forall\, \boldsymbol{x} \in V)(\boldsymbol{x} + \mathbf{0} = \boldsymbol{x}),\\
&(\forall\, \boldsymbol{x} \in V)(\exists\, \boldsymbol{y} \in V)(\boldsymbol{x} + \boldsymbol{y} = \mathbf{0}),\\
&(\forall\, a, b \in K)(\forall\, \boldsymbol{x} \in V)(a \cdot (b \cdot \boldsymbol{x}) = (ab) \cdot \boldsymbol{x}),\\
&(\forall\, \boldsymbol{x} \in V)(1 \cdot \boldsymbol{x} = \boldsymbol{x}),\\
&(\forall\, a \in K)(\forall\, \boldsymbol{x}, \boldsymbol{y} \in V)(a \cdot (\boldsymbol{x} + \boldsymbol{y}) = (a \cdot \boldsymbol{x}) + (a \cdot \boldsymbol{y})),\\
&(\forall\, a, b \in K)(\forall\, \boldsymbol{x} \in V)((a + b) \cdot \boldsymbol{x} = (a \cdot \boldsymbol{x}) + (b \cdot \boldsymbol{x})).
\end{aligned}
$$

Ako si čitateľ asi všimol, skaláry značíme „obyčajnými“ malými latinskými písmenami a vektory tučnými malými latinskými písmenami. Tejto implicitnej dohody sa budeme väčšinou držať, nie však za každú cenu. Kedykoľvek by nás obmedzovala, nebudeme váhať ju porušiť.

I keď sčítanie skalárov v poli a sčítanie vektorov značíme rovnakým znakom $+$, ide o rôzne operácie. Podobne násobenie v poli a násobenie vektora skalárom sú rôzne operácie, hoci obe značíme $\cdot$. Neskôr tento prístup dovedieme ešte ďalej, keď budeme rovnako značiť príslušné operácie a nuly v rôznych vektorových priestoroch. Rozlišovanie znakov pre nulu $0 \in K$ a $\mathbf{0} \in V$, hoci tieto prvky plnia rovnakú funkciu v K resp. vo V, je tak trochu proti duchu tohto prístupu. Ide vlastne o zbytočný luxus, ktorý je však v zhode s prijatou dohodou o značení skalárov a vektorov.

Z formálneho hľadiska pripomínajú axiómy vektorového priestoru axiómy poľa: sčítanie vektorov je opäť asociatívna a komutatívna binárna operácia na V s neutrálnym prvkom $\mathbf{0} \in V$, operácia násobenia vektora skalárom tiež spĺňa akúsi podmienku „asociatívnosti“,

$1 \in K$ je jej „neutrálnym prvkom" a platia dva „distributívne zákony". Je tu však jeden podstatný rozdiel – kým násobenie v poli K je binárnou operáciou na množine K, t. j. zobrazením $\cdot : K \times K \to K$, násobenie vo vektorovom priestore V nad poľom K nie je binárnou operáciou na V, ale binárnou operáciou $\cdot : K \times V \to V$. To nám však nebráni zaviesť obdobné dohody ako pre operácie v poli: i teraz bude mať násobenie prednosť pre sčítaním a znak násobenia budeme väčšinou vynechávať, t. j. písať napr. $a\boldsymbol{x} + \boldsymbol{y}$ miesto $(a \cdot \boldsymbol{x}) + \boldsymbol{y}$. Takisto budeme vynechávať zátvorky, ktorých umiestnenie neovplyvní výslednú hodnotu výrazov ako napr. v $ab\boldsymbol{x}$ alebo $a_1\boldsymbol{x}_1 + \ldots + a_n\boldsymbol{x}_n$. Posledný výraz budeme tiež značiť

$$\sum_{i=1}^{n} a_i \boldsymbol{x}_i$$

a nazývať *lineárnou kombináciou* vektorov $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ s koeficientmi $a_1, \ldots, a_n$. Špeciálne pre $n = 1$ to znamená $\sum_{i=1}^{1} a_i\boldsymbol{x}_i = a_1\boldsymbol{x}_1$; kvôli úplnosti pre $n = 0$ ešte kladieme prázdnu lineárnu kombináciu $\sum_{i=1}^{0} a_i\boldsymbol{x}_i$ rovnú $\mathbf{0}$.

Podobne ako v prípade polí, možno z axióm vektorových priestorov odvodiť niektoré základne pravidlá pre počítanie so skalármi a vektormi. Predovšetkým prvok $\boldsymbol{y} \in V$ taký, že $\boldsymbol{x} + \boldsymbol{y} = \mathbf{0}$, je k danému $\boldsymbol{x} \in V$ určený jednoznačne – značíme ho $-\boldsymbol{x}$ a nazývame *opačný vektor* k $\boldsymbol{x}$. Namiesto $\boldsymbol{x} + (-\boldsymbol{y})$ opäť píšeme len $\boldsymbol{x} - \boldsymbol{y}$. Tieto pravidlá zhrnieme v nasledujúcej analógii tvrdenia 1.2.1.

1.5.1. Tvrdenie. *Nech V je vektorový priestor nad poľom K. Potom pre ľubovoľné $n \in \mathbb{N}$, $a, b, a_1, \ldots, a_n \in K$ a $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in V$ platí*

(a) $\boldsymbol{x} + \boldsymbol{y} = \boldsymbol{x} + \boldsymbol{z} \Rightarrow \boldsymbol{y} = \boldsymbol{z}$,

(b) $(a\boldsymbol{x} = a\boldsymbol{y} \;\&\; a \neq 0) \Rightarrow \boldsymbol{x} = \boldsymbol{y}$, $\quad (a\boldsymbol{x} = b\boldsymbol{x} \;\&\; \boldsymbol{x} \neq \mathbf{0}) \Rightarrow a = b$,

(c) $a\mathbf{0} = \mathbf{0} = 0\boldsymbol{x}$,

(d) $a\boldsymbol{x} = \mathbf{0} \Rightarrow (a = 0 \vee \boldsymbol{x} = \mathbf{0})$,

(e) $-\boldsymbol{x} = (-1)\boldsymbol{x}$,

(f) $a(\boldsymbol{x} - \boldsymbol{y}) = a\boldsymbol{x} - a\boldsymbol{y}$, $\quad (a - b)\boldsymbol{x} = a\boldsymbol{x} - b\boldsymbol{x}$,

(g) $a(\boldsymbol{x}_1 + \ldots + \boldsymbol{x}_n) = a\boldsymbol{x}_1 + \ldots + a\boldsymbol{x}_n$, $\quad (a_1 + \ldots + a_n)\boldsymbol{x} = a_1\boldsymbol{x} + \ldots + a_n\boldsymbol{x}$.

Dôkaz Všetky podmienky, s výnimkou druhej implikácie v (b), možno dokázať celkom analogicky ako príslušné časti tvrdenia 1.2.1. Dokážeme aj túto. Nech $a\boldsymbol{x} = b\boldsymbol{x}$ a $\boldsymbol{x} \neq \mathbf{0}$. Potom $(a - b)\boldsymbol{x} = a\boldsymbol{x} - b\boldsymbol{x} = \mathbf{0}$. Podľa (d) z toho vyplýva $a - b = 0$, teda $a = b$.

Práve definované vektorové priestory by sme presnejšie mohli nazvať „ľavými“ vektorovými priestormi, lebo v operácii skalárneho násobku píšeme skalár vľavo od vektora. Celkom obdobne by sme mohli definovať aj „pravé“ vektorové priestory, v ktorých by sme operáciu skalárneho násobku chápali ako zobrazenie $V \times K \to V$ a zapisovali ju v tvare $\boldsymbol{x} \cdot a$ alebo len $\boldsymbol{x}a$ pre $\boldsymbol{x} \in V$, $a \in K$. Vďaka komutatívnosti násobenia v poli K si však môžeme dovoliť chápať naše „ľavé“ vektorové priestory zároveň ako „pravé“. Pre všetky $a \in K$, $\boldsymbol{x} \in V$ jednoducho položíme $\boldsymbol{x}a = a\boldsymbol{x}$. Jediný problém – zabezpečiť pre všetky $a, b \in K$, $\boldsymbol{x} \in V$ rovnosť $(ab)\boldsymbol{x} = (ba)\boldsymbol{x}$, ktorá z takejto definície vyplýva výpočtom

$$(ab)\boldsymbol{x} = a(b\boldsymbol{x}) = a(\boldsymbol{x}b) = (\boldsymbol{x}b)a = \boldsymbol{x}(ba) = (ba)\boldsymbol{x},$$

– je vyriešený práve v dôsledku komutatívnosti násobenia v K. Teda, ak sa nám v operácii skalárneho násobku vyskytne skalár vpravo od vektora, nemusí nás to vyviesť z miery – kľudne ho môžeme prehodiť vľavo a ani o zátvorky sa nemusíme príliš starať.

1.6. Príklady vektorových priestorov

1.6.1. Rozšírenia polí. Zrejme každé pole K možno považovať za vektorový priestor nad sebou samým. Všeobecnejšie, ak pole L je rozšírením poľa K, tak L možno považovať za vektorový priestor nad poľom K (formálne stačí „zabudnúť“ násobenie niektorých dvojíc prvkov $a, b \in L$ a súčin ab pripustiť len pre $a \in K$, $b \in L$). Podobným spôsobom možno vektorový priestor V nad poľom L zúžením násobenia $L \times V \to V$ na násobenie $K \times V \to V$ prerobiť na vektorový priestor nad poľom K.

1.6.2. n-rozmerné riadkové a stĺpcové vektory nad daným poľom. Pre ľubovoľné pole K a $n \in \mathbb{N}$ množina

$$K^n = \{(x_1, \ldots, x_n);\, x_1, \ldots, x_n \in K\}$$

všetkých usporiadaných n-tíc prvkov z K spolu s operáciami

$$\boldsymbol{x} + \boldsymbol{y} = (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$
$$c\boldsymbol{x} = c(x_1, \ldots, x_n) = (cx_1, \ldots, cx_n),$$

kde $\boldsymbol{x} = (x_1, \ldots, x_n) \in K^n$, $\boldsymbol{y} = (y_1, \ldots, y_n) \in K^n$ a $c \in K$, tvorí vektorový priestor nad poľom K. Zrejme usporiadaná n-tica $\mathbf{0}_n = (0, \ldots, 0)$ hrá úlohu nuly v K^n. Ak bude potrebné rozlíšiť nulové vektory v priestoroch K^n pre rôzne prirodzené čísla n, budeme pre nulu v K^n používať označenie $\mathbf{0}_n$. Opačný prvok k $\boldsymbol{x} = (x_1, \dots, x_n) \in K^n$ je zrejme

$$-\boldsymbol{x} = -(x_1, \dots, x_n) = (-x_1, \dots, -x_n)$$

Hovoríme, že operácie na K^n sú definované *po zložkách*. Prvky tohto vektorového priestoru nazývame *n-rozmerné riadkové vektory* nad poľom K. Kvôli úplnosti ešte poznamenajme, že vektorový priestor K^0 pozostáva z jediného prvku $\emptyset$, predstavujúceho „usporiadanú nulaticu“, ktorá tak je nevyhnutne nulou v K^0.

Niekedy je (a väčšinou i bude) výhodnejšie pracovať s *n-rozmernými stĺpcovými vektormi* nad poľom K, t. j. s vektormi tvaru

$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

kde $x_1, \dots, x_n \in K$. Čitateľ si iste sám doplní definície príslušných operácií (opäť po zložkách) a dalšie podrobnosti. Pokiaľ nebude hroziť nedorozumenie, budeme i tento priestor označovať K^n, prípadne len slovne naznačíme, či tým máme na mysli priestor n-rozmerných riadkových alebo stĺpcových vektorov. V súlade s tým $\mathbf{0}_n$ alebo len $\mathbf{0}$ môže označovať aj nulový vektor-stĺpec.

1.6.3. Polynómy nad daným poľom. Pod *polynómom* alebo tiež *mnohočlenom* $f(x)$ *stupňa* n, kde $n \in \mathbb{N}$, v premennej x nad poľom K rozumieme formálny výraz tvaru

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n = \sum_{i=0}^{n} a_i x^i,$$

kde $a_0, a_1, \ldots, a_{n-1}, a_n \in$ sú skaláry, nazývané *koeficienty* polynómu f, a $a_n \neq 0$; nulu $0 \in K$ považujeme za polynóm stupňa -1 a nenulové skaláry $a \in K$ za polynómy stupňa 0. Zrejme každý polynóm $f(x)$ definuje (rovnako značenú) funkciu $f : K \to K$ danú predpisom $c \mapsto f(c)$, t. j. dosadením konkrétnych hodnôt $c \in K$ za premennú x do polynómu $f(x)$. Množinu všetkých polynómov v premennej x nad K *stupňa nanajvýš* n, kde $-1 \leq n \in \mathbb{Z}$, budeme značiť $K^{(n)}[x]$; množinu *všetkých polynómov* v premennej x nad K značíme $K[x]$. Ľubovoľný polynóm $g(x) = \sum_{i=0}^{m} b_i x^i \in K[x]$ stupňa $m < n$ môžeme tiež písať v tvare

$$g(x) = b_0 + b_1 x + \ldots + b_m x^m + 0x^{m+1} + \ldots + 0x^n,$$

t. j. v tvare $g(x) = \sum_{i=0}^{n} b_i x^i$, kde $b_i = 0$ pre $m < i \leq n$. S použitím tejto konvencie možno definovať súčet $f(x) + g(x)$ polynómov $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ z $K[x]$ predpisom

$$(f+g)(x) = f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i.$$

Ak navyše $c \in K$, kladieme

$$(cf)(x) = cf(x) \sum_{i=0}^{n} c a_i x^i.$$

Ľahko možno nahliadnuť, že s takto po zložkách definovanými operáciami súčtu a skalárneho násobku tvorí každá z množín polynómov $K^{(n)}[x]$, kde $-1 \leq n \in \mathbb{Z}$, ako i množina všetkých polynómov $K[x]$ vektorový priestor nad poľom K. Štruktúrou vektorového priestoru sa však algebra polynómov nevyčerpáva. Popri súčte a skalárnom násobku možno na

$K[x]$ definovať aj súčin $f(x)\,g(x)$ uvedených polynómov $f(x)$, $g(x)$ predpisom

$$(fg)(x) = f(x)\,g(x) = \sum_{k=0}^{m+n} c_k x^k,$$

kde $c_k = \sum_{i=0}^{k} a_i b_{k-i}$.

1.6.4. Priame súčiny vektorových priestorov. Nech V_1 a V_2 sú vektorové priestory nad tým istým poľom K. *Priamym súčinom* (niekedy tiež *vonkajším priamym súčtom*) priestorov V_1, V_2 nazývame množinu $V_1 \times V_2$, t. j. karteziánsky súčin množín V_1, V_2, s operáciami súčtu vektorov a skalárneho násobku definovanými po zložkách. Teda pre $(\boldsymbol{u}_1, \boldsymbol{u}_2)$, $(\boldsymbol{v}_1, \boldsymbol{v}_2) \in V_1 \times V_2$, $c \in K$ kladieme

$$(\boldsymbol{u}_1, \boldsymbol{u}_2) + (\boldsymbol{v}_1, \boldsymbol{v}_2) = (\boldsymbol{u}_1 + \boldsymbol{v}_1, \boldsymbol{u}_2 + \boldsymbol{v}_2),$$
$$c(\boldsymbol{u}_1, \boldsymbol{u}_2) = (c\boldsymbol{u}_1, c\boldsymbol{u}_2).$$

Zrejme $(\mathbf{0}, \mathbf{0})$ je nulou tohto vektorového priestoru a $-(\boldsymbol{u}_1, \boldsymbol{u}_2) = (-\boldsymbol{u}_1, -\boldsymbol{u}_2)$ je opačný prvok k $(\boldsymbol{u}_1, \boldsymbol{u}_2)$. Čitateľovi prenechávame, aby si overil, že priamy súčin $V_1 \times V_2$ s takto definovanými operáciami naozaj tvorí vektorový priestor nad poľom K, a taktiež, aby si premyslel, ako možno uvedenú konštrukciu zovšeobecniť na priamy súčin $V_1 \times \ldots \times V_n$ ľubovoľného konečného počtu vektorových priestorov $V_1, \ldots, V_n$ nad K. Ak $V = V_1 = \ldots = V_n$, tak píšeme $V_1 \times \ldots \times V_n = V^n$ a tento vektorový priestor nazývame n-tou *priamou mocninou* priestoru V. Pre $V = K$ uvedená konštrukcia dáva nám už známy vektorový priestor K^n z 1.6.2,

1.6.5. Vektorové priestory funkcií. Nech V je vektorový priestor nad poľom K a X je ľubovoľná množina. Pripomeňme, že V^X označuje množinu všetkých funkcií $f : X \to V$. Teraz ukážeme, ako možno z tejto množiny urobiť vektorový priestor nad poľom K. Operácie súčtu a skalárneho násobku budeme definovať opäť po zložkách. To znamená, že pre $f, g \in V^X$ a $c \in K$ budeme definovať funkcie $f + g \in V^X$ a $cf \in V^X$ tak, že pre každé $x \in X$ položíme

$$(f+g)(x) = f(x) + g(x),$$
$$(cf)(x) = cf(x).$$

Znovu možno ľahko nahliadnuť, že V^X s takto definovanými operáciami tvorí vektorový priestor nad poľom K – nazývame ho *vektorovým priestorom všetkých funkcií* z X do V. Nulou vo V^X je funkcia $\mathbf{0} : X \to V$ identicky rovná prvku $\mathbf{0} \in V$; opačným prvkom k funkcii $f \in V^X$ je funkcia $-f \in V^X$ daná predpisom $x \mapsto -f(x)$ pre $x \in X$.

V špeciálnom prípade pre $V = K$ takto dostaneme vektorový priestor K^X všetkých funkcií z množiny X do poľa K. Ak K je pole všetkých reálnych prípadne komplexných čísel a X je napr. nejaký uzavretý interval $\langle a, b\rangle$ reálnych čísel, tak dostávame vektorové priestory funkcií $\mathbb{R}^{\langle a,b\rangle}$ resp. $\mathbb{C}^{\langle a,b\rangle}$, ktoré sa hojne vyskytujú v matematickej analýze.

Cvičenia

Cvičenia 1–4 sú opakovaním základných poznatkov o komplexných číslach.

1.1. Vypočítajte:

(a) $(5 + 3\mathrm{i}) + (7 - \mathrm{i})$, (b) $(11 - 10\mathrm{i}) - (8 - 5\mathrm{i})$,
(c) $(-2 + 5\mathrm{i}) \cdot (3 + 2\mathrm{i})$, (d) $(4 - \mathrm{i}) \cdot (2 + 9\mathrm{i})$,
(e) $(12 + 5\mathrm{i})^{-1}$, (f) $(7 + \mathrm{i})/(3 - 4\mathrm{i})$.

1.2. (a) Pre komplexné číslo $x = a + bi$, kde $a, b \in \mathbb{R}$, nazývame $a = \operatorname{Re} x$, $b = \operatorname{Im} x$ jeho *reálnou* resp. *imaginárnou časťou*. Teda $\operatorname{Re} x$ aj $\operatorname{Im} x$ sú *reálne čísla*. Dokážte vzorce:

$$\operatorname{Re}(x+y) = \operatorname{Re} x + \operatorname{Re} y, \qquad \operatorname{Re}(xy) = \operatorname{Re} x \operatorname{Re} y - \operatorname{Im} x \operatorname{Im} y,$$
$$\operatorname{Im}(x+y) = \operatorname{Im} x + \operatorname{Im} y, \qquad \operatorname{Im}(xy) = \operatorname{Re} x \operatorname{Im} y + \operatorname{Im} x \operatorname{Re} y.$$

(b) Ak si v (reálnej) rovine zvolíme pravouhlý súradnicový systém, môžeme každé komplexné číslo $x = a + bi$ reprezentovať bodom či vektorom so súradnicami (a, b). Ak prostredníctvom bijekcie $x \mapsto (\operatorname{Re} x, \operatorname{Im} x)$ stotožníme každé komplexné číslo s jeho obrazom a množinu $\mathbb{C}$ s rovinou (množinou $\mathbb{R}^2$), hovoríme o tzv. *Gaussovej rovine*. Znázornite čísla zo zadaní aj výsledkov cvičenia 1 v Gaussovej rovine.

1.3. *Absolútna hodnota* komplexného čísla $x = a + bi$, kde $a, b \in \mathbb{R}$, je definovaná ako $|x| = \sqrt{a^2 + b^2}$, t. j. ako vzdialenosť bodu x od počiatku v Gaussovej rovine. *Komplexne združené číslo* k číslu x je $\overline{x} = a - bi$, t. j. číslo súmerne združené s x podľa reálnej osi.
(a) Nájdite absolútne hodnoty jednotlivých čísel zo zadaní aj výsledkov v cvičení 1.
(b) Dokážte nasledujúce vzťahy:

$$\begin{aligned}
\operatorname{Re} \overline{x} &= \operatorname{Re} x, & \operatorname{Im} \overline{x} &= -\operatorname{Im} x;\\
\overline{\overline{x}} &= x, & xy^{-1} &= (x\overline{y})/|y|^2, \quad (y \neq 0),\\
\overline{x+y} &= \overline{x} + \overline{y}, & \overline{xy} &= \overline{x}\,\overline{y},\\
|x| &= |\overline{x}|, & |x|^2 &= x\overline{x},\\
|xy| &= |x|\,|y|, & |x+y| &\leq |x| + |y|.
\end{aligned}$$

(c) V poslednom vzťahu nastane rovnosť práve vtedy, keď existuje nezáporné číslo $c \in \mathbb{R}$ také, že $x = cy$ alebo $y = cx$. Dokážte.

1.4. Každé komplexné číslo x možno vyjadriť v tzv. *goniometrickom tvare* $x = r(\cos\alpha + \mathrm{i}\sin\alpha)$, kde $r = |x|$ a α je uhol, ktorý (pre $x \neq 0$) zviera v Gaussovej rovine „vektor“ $\overrightarrow{01}$ s „vektorom“ $\overrightarrow{0x}$ (pre $x = 0$ vyhovuje ľubovoľné $\alpha \in \mathbb{R}$).

(a) Pre $x \neq 0$ vyjadrite $\cos\alpha$ a $\sin\alpha$ pomocou $\operatorname{Re} x$, $\operatorname{Im} x$ a $|x|$. Dokážte, že α je určené jednoznačne až na sčítanec $2k\pi$, kde $k \in \mathbb{Z}$.
(b) Pre $x = r(\cos\alpha + \mathrm{i}\sin\alpha)$, $y = s(\cos\beta + \mathrm{i}\sin\beta)$ platí $xy = rs(\cos(\alpha+\beta) + \mathrm{i}\sin(\alpha+\beta))$. Dokážte.
(c) Matematickou indukciou dokážte tzv. *Moivreovu vetu*: $(\cos\alpha + \mathrm{i}\sin\alpha)^n = \cos n\alpha + \mathrm{i}\sin n\alpha$, pre každé $n \in \mathbb{N}$. Rozšírte jej platnosť na všetky $n \in \mathbb{Z}$.
(d) Vyjadrite všetky čísla zo zadaní aj výsledkov v cvičení 1 v goniometrickom tvare.
(e) Pomocou Moivreovej vety vypočítajte $(\sqrt{3} + \mathrm{i})^{11}$, $(1 - \mathrm{i})^{-7}$.
(f) Na základe Moivreovej vety napíšte vzorec pre všetkých n riešení *binomickej rovnice* $x^n = c$, kde $c \in \mathbb{C}$. (*Návod*: Riešte najprv prípad $|c| = 1$.)
(g) Nájdite všetky riešenia binomických rovníc $x^3 = (\sqrt{3} - \mathrm{i})/2$, $y^4 = 1 + \mathrm{i}$ a $z^5 = -4 + 3\mathrm{i}$.

1.5. Podrobne dokážte vzťahy uvedené za dôkazom tvrdenia 1.2.1. Kde treba, použite matematickú indukciu.

1.6. V každom z nasledujúcich prípadov rozhodnite, či množina A je podpoľom poľa K. Svoje rozhodnutie zdôvodnite.
(a) $K = \mathbb{Q}$, $A = \mathbb{Z}$;
(b) $K = \mathbb{R}$, $A = \mathbb{Q}\big[\sqrt{2}\big] = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$;
(c) $K = \mathbb{R}$, $A = \langle -1, 1\rangle$;
(d) $K = \mathbb{C}$, $A = \mathbb{Z}[\,\mathrm{i}\,] = \{a + b\mathrm{i};\ a, b \in \mathbb{Z}\}$;
(e) $K = \mathbb{Z}_{11}$, $A = \mathbb{Z}_5$;
(f) $K = \mathbb{C}$, $A = \mathbb{Q}[\omega] = \{a + b\omega + c\omega^2;\ a, b, c \in \mathbb{Q}\}$, kde $\omega = (-1 + \mathrm{i}\sqrt{3})/2$.

1.7. Zostrojte multiplikatívne tabuľky sčítania a násobenia v $\mathbb{Z}_n$ pre $2 \leq n \leq 6$. Na ich základe zdôvodnite, prečo $\mathbb{Z}_4$ a $\mathbb{Z}_6$ nie sú polia.

1.8. Vynechajme z definície poľa podmienku $0 \neq 1$ a podmienku požadujúcu existenciu inverzného prvku vzhľadom na násobenie ku každému nenulovému prvku $a \in K$. Množina K s význačnými prvkami $0, 1 \in K$, vybavená binárnymi operáciami súčtu a súčinu, spĺňajúcimi zvyšné podmienky sa nazýva *komutatívny okruh s jednotkou.*[1] Komutatívny okruh s jednotkou sa nazýva *netriviálny*, ak v ňom predsa len platí $0 \neq 1$. Dokážte postupne nasledujúce tvrdenia:

[1] Občas sa v literatúre takáto štruktúra nazýva len komutatívny okruh.

(a) $\mathbb{Z}$ s obvyklými operáciami súčtu a súčinu je netriviálny komutatívny okruh s jednotkou.
(b) Pre každé $n \in \mathbb{N}$, $n \neq 0$, je $\mathbb{Z}_n$ so sčítaním a násobením modulo n komutatívny okruh s jednotkou. Tento okruh je netriviálny práve vtedy, keď $n \geq 2$.
(c) Komutatívny okruh s jednotkou je netriviálny práve vtedy, keď obsahuje aspoň dva rôzne prvky.

1.9. (a) V ľubovoľnom komutatívnom okruhu s jednotkou K zadefinujte výrazy tvaru na pre ľubovoľné $n \in \mathbb{Z}$, $a \in K$ rovnako ako v poli. Taktiež zadefinujte výrazy tvaru a^n pre $n \in \mathbb{N}$, $a \in K$. Dokážte pre ne analogické tvrdenia, ako platia v poli. Čo je prekážkou definície a^n pre všetky $n \in \mathbb{Z}$?
(b) Zadefinujte *charakteristiku* ľubovoľného *komutatívneho okruhu s jednotkou* rovnakým spôsobom ako v prípade poľa.
(c) Dokážte, že pre komutatívny okruh s jednotkou K platí $\operatorname{char} K = 1$ práve vtedy, keď K je triviálny.
(d) Pre každé $n \in \mathbb{N}$, $n \neq 0$, platí $\operatorname{char} \mathbb{Z}_n = n$.
(e) Pre každé prvočíslo p zostrojte príklad komutatívneho okruhu s jednotkou, ktorý má charakteristiku p, no nie je poľom. (*Návod*: Pozri cvičenie 1.12.)

1.10. (a) Matematickou indukciou dokážte platnosť binomickej vety *v ľubovoľnom komutatívnom okruhu s jednotkou* K (teda aj v ľubovoľnom poli). To znamená, že pre všetky $n \in \mathbb{N}$, $a, b \in K$ platí

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \ldots + \binom{n}{n-1} a b^{n-1} + b^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

(b) Predpokladajme, že charakteristikou komutatívneho okruhu s jednotkou K je prvočíslo p. Nech $m \in \mathbb{Z}$ je násobkom p. Dokážte, že pre každé $c \in K$ platí $mc = 0$.
(c) Na základe (a) a (b) dokážte, že v komutatívnom okruhu s jednotkou prvočíselnej charakteristiky p platí pre exponent $n = p$ nasledujúci „populárny“ variant binomickej vety:

$$(a+b)^p = a^p + b^p.$$

1.11. Doplňte vynechané časti dôkazu tvrdenia 1.5.1.

1.12. V každom z príkladov 1.6.1–5, podrobne overte, že uvedená množina s príslušnými operáciami tvorí vektorový priestor.

1.13. Rovnako ako v príklade 1.6.3, zadefinujte pre ľubovoľný komutatívny okruh s jednotkou K množinu $K[x]$ všetkých polynómov v premennej x s koeficientmi z K a na nej operácie súčtu a súčinu. Dokážte, že $K[x]$ s takto definovanými operáciami je opäť komutatívny okruh s jednotkou a platí $\operatorname{char} K[x] = \operatorname{char} K$.

1.14. Na množine $\mathbb{R}^+$ všetkých kladných reálnych čísel definujme nové „sčítanie“ $\oplus$ ako násobenie, t. j. $x \oplus y = xy$. Ďalej definujme novú operáciu „skalárneho násobku“ $\odot : \mathbb{R} \times \mathbb{R}^+ \to \mathbb{R}^+$ ako umocňovanie, t. j. predpisom $a \odot x = x^a$. Dokážte, že množina $\mathbb{R}^+$ s uvedenými operáciami tvorí vektorový priestor nad poľom $\mathbb{R}$. Čo je nulový vektor $\mathbf{0} \in \mathbb{R}^+$? Ako vyzerá opačný vektor $\ominus x$ k vektoru $x \in \mathbb{R}^+$? Vyjadrite pomocou pôvodných operácií násobenia a umocňovania lineárnu kombináciu $(a_1 \odot x_1) \oplus \ldots \oplus (a_n \odot x_n)$, kde $a_1, \ldots, a_n \in \mathbb{R}$, $x_1, \ldots, x_n \in \mathbb{R}^+$.

2. Základy maticového počtu

V tejto kapitole sa zoznámime s *maticami*, t. j. obdĺžnikovými tabuľkami, pomocou ktorých budeme kódovať najrôznejšie dôležité údaje o vektorových priestoroch, a naučíme sa s nimi zaobchádzať. Niektoré operácie s maticami budú zatiaľ nemotivované, ich význam vyjde najavo až neskôr. Od čitateľa tak žiadame istú dávku trpezlivosti, podobnú tej, akú musí prejaviť prváčik na základnej škole, ktorý tiež musí najprv zvládnuť jednotlivé písmenká, potom sa naučiť, ako sa z nich skladajú slová, a až potom môže začať čítať zmysluplné texty. Tento vklad sa nám zúročí neskôr, keď nám umožní hladko napredovať a nezdržiavať sa pri nepodstatných otázkach.

Pri prvom čítaní možno vynechať odstavce venované blokovým maticiam a maticiam nad vektorovými priestormi. Celkom postačí nalistovať si príslušnú časť až vo chvíli, keď sa s blokovými maticami stretneme v ďalších kapitolách.

2.1. Matice nad danou množinou

2.1.1. Typy matíc. Nech X je ľubovoľná množina a $m, n \in \mathbb{N}$. *Maticou typu* $m \times n$, alebo tiež $m \times n$-*rozmernou maticou* nad množinou X rozumieme obdĺžnikovu tabuľku

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

pozostávajúcu z prvkov množiny X. Skrátene tiež píšeme $\boldsymbol{A} = (a_{ij})_{m\times n}$, alebo len $\boldsymbol{A} = (a_{ij})$. Prvky $a_{ij} \in X$, kde $1 \le i \le m$, $1 \le j \le n$, sa nazývajú *prvkami matice* $\boldsymbol{A}$. Prvok a_{ij} nachádzajúci sa v i-tom riadku a j-tom stĺpci matice $\boldsymbol{A}$ nazývame tiež *prvok v mieste* (i, j), prípadne (i, j)-*ty prvok* matice $\boldsymbol{A}$. Množinu všetkých $m \times n$-rozmerných matíc nad množinou X značíme $X^{m\times n}$. Ak $m = n$, hovoríme o *štvorcových maticiach rádu* n nad množinou X.

Poznamenajme, že v prípade, keď niektoré z čísel m, n je 0, množina $X^{m\times n}$ pozostáva z jedinej a to *prázdnej* matice $\emptyset$. Neskôr sa ukáže rozumné stotožniť túto maticu s tzv. nulovou maticou. Aby sme sa vyhli trivialitám, budeme sa vždy baviť len o maticiach kladných rozmerov $m \times n$, čitateľ by si však mal aspoň občas uvedomiť, že väčšina našich úvah si zachováva platnosť aj v prípade, keď $m = 0$ alebo $n = 0$.

Dve matice nad množinou X považujeme za *navzájom rovné* alebo *totožné*, ak majú rovnaké rozmery a rovnaké prvky na príslušných miestach. To znamená, že pre matice $\boldsymbol{A} = (a_{ij})_{m\times n}$, $\boldsymbol{B} = (b_{ij})_{p\times q}$ nad X kladieme $\boldsymbol{A} = \boldsymbol{B}$ práve vtedy, keď $m = p$, $n = q$ a pre všetky $i = 1, \dots, m$, $j = 1, \dots, n$ platí $a_{ij} = b_{ij}$.

Množina matíc typu $1 \times n$ nad X splýva s množinou X^n, ak usporiadané n-tice prvkov z X zapisujeme do riadku. Podobne, ak usporiadné m-tice prvkov z X zapisujeme do stĺpca, tak množina matíc typu $m \times 1$ nad X splýva s množinou X^m. Pokiaľ bude z kontextu jasné, či ide o riadky alebo stĺpce, prípadne, ak na tom nebude záležať, budeme písať jednoducho X^n, X^m a pod. Podrobnejšie označenie $X^{1\times n}$, $X^{m\times 1}$ a pod. budeme používať, len ak bude treba rozlíšiť riadky a stĺpce.

2.1.2. Riadky a stĺpce matice. Nech $\boldsymbol{A} = (a_{ij}) \in X^{m\times n}$. Usporiadanú n-ticu

$$\boldsymbol{r}_i(\boldsymbol{A}) = (a_{i1}, a_{i2}, \dots, a_{in}) \in X^{1\times n},$$

kde $1 \le i \le m$, nazývame *i-tym riadkom* matice $\boldsymbol{A}$. Podobne, usporiadnú m-ticu

$$\boldsymbol{s}_j(\boldsymbol{A}) = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix},$$

kde $1 \le j \le n$, nazývame *j-tym stĺpcom* matice $\boldsymbol{A}$. Maticu $\boldsymbol{A}$ tak možno stotožniť so stĺpcom jej riadkov ako aj s riadkom jej stĺpcov, t. j.

$$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} \boldsymbol{r}_1(\boldsymbol{A}) \\ \boldsymbol{r}_2(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_m(\boldsymbol{A}) \end{pmatrix} = (\boldsymbol{s}_1(\boldsymbol{A}), \boldsymbol{s}_2(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})).$$

2.1.3. Transponovaná matica. Maticu, ktorú získame z matice $\boldsymbol{A} = (a_{ij})_{m\times n}$ zámenou jej riadkov a stĺpcov, nazývame *transponovanou maticou* k matici $\boldsymbol{A}$ a značíme ju $\boldsymbol{A}^T$. Teda trochu podrobnejšie

$$\boldsymbol{A}^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}.$$

To znamená, že $\boldsymbol{A}^T \in X^{n\times m}$ a prvok v mieste (i,j) matice $\boldsymbol{A}^T$ je a_{ji}.

Zrejme pre ľubovoľnú maticu $\boldsymbol{A} \in X^{m\times n}$ platí

$$(\boldsymbol{A}^T)^T = \boldsymbol{A}.$$

Transpozíciou matíc-riadkov z $X^{1\times n}$ dostaneme matice-stĺpce z $X^{n\times 1}$ a transpozíciou matíc-stĺpcov z $X^{m\times 1}$ matice-riadky z $X^{1\times m}$. Na základe tejto poznámky možno nahliadnuť, že pre ľubovoľnú maticu $\boldsymbol{A} \in X^{m\times n}$ a $1 \le i \le m$, $1 \le j \le n$ platí

$$\boldsymbol{s}_i\left(\boldsymbol{A}^T\right) = \boldsymbol{r}_i(\boldsymbol{A})^T, \qquad \boldsymbol{r}_j\left(\boldsymbol{A}^T\right) = \boldsymbol{s}_j(\boldsymbol{A})^T.$$

Štvorcová matica $\boldsymbol{A} \in X^{n\times n}$ sa nazýva *symetrická*, ak $\boldsymbol{A} = \boldsymbol{A}^T$, t. j. ak $a_{ij} = a_{ji}$ pre všetky $i, j = 1, \dots, n$. Postupnosť prvkov $(a_{11}, a_{22}, \dots, a_{nn})$ nazývame *diagonálou* štvorcovej matice $\boldsymbol{A}$. Transponovanú maticu k štvorcovej matici $\boldsymbol{A}$ zrejme získame „osovou súmernosťou“ jej prvkov podľa diagonály.

2.1.4. Blokové matice. Niekedy bude užitočné spojiť dve matice $\boldsymbol{A} \in X^{m\times n_1}$, $\boldsymbol{B} \in X^{m\times n_2}$ s rovnakým počtom riadkov do jednej matice tak, že príslušné tabuľky jednoducho napíšeme vedľa seba. Výsledná matica je typu $m \times (n_1 + n_2)$ a značíme ju $(\boldsymbol{A}, \boldsymbol{B})$, prípadne $(\boldsymbol{A} \mid \boldsymbol{B})$.

Podobne možno spojiť dve matice $\boldsymbol{A} \in X^{m_1\times n}$, $\boldsymbol{B} \in X^{m_2\times n}$ s rovnakým počtom stĺpcov do jednej matice tak, že príslušné tabuľky napíšeme pod seba. Výsledná matica je typu $(m_1 + m_2) \times n$ a značíme ju $\begin{pmatrix} \boldsymbol{A} \\ \boldsymbol{B} \end{pmatrix}$, prípadne $\begin{pmatrix} \boldsymbol{A} \\ \hline \boldsymbol{B} \end{pmatrix}$.

Práve popísané konštrukcie sú príkladmi tzv. *blokových matíc*. Pôvodné matice, z ktorých takto vytvárame blokovú maticu, potom nazývame jej *blokmi*. Takisto môžeme vedľa seba resp. pod seba zoradiť väčší počet blokov, nie len dva.

Naopak, niekedy sa môže ukázať účelné vyznačiť v danej matici nejaké menšie obdĺžnikove časti ako jej bloky. Vtedy hovoríme o tzv. *blokovom tvare* danej matice. Príkladom toho bol zápis matice $\boldsymbol{A} \in X^{m\times n}$ ako riadku jej stĺpcov, prípadne ako stĺpca jej riadkov.

Uvedené dve schémy vytvárania blokových matíc „vedľa seba“ a „pod seba“ možno tiež kombinovať. Napr. z matíc $\boldsymbol{A}_{11} \in X^{m_1\times n_1}$, $\boldsymbol{A}_{12} \in X^{m_1\times n_2}$, $\boldsymbol{A}_{21} \in X^{m_2\times n_1}$, $\boldsymbol{A}_{22} \in X^{m_2\times n_2}$ možno vytvoriť blokovú maticu

$$\begin{pmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{12} \\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} \end{pmatrix}$$

typu $(m_1 + m_2) \times (n_1 + n_2)$.

Túto konštrukciu možno zrejmým spôsobom zovšeobecniť i na väčšie systémy matíc. Voľne povedané, blokové matice sú vlastne matice, ktorých prvkami sú opäť matice, pričom všetky matice v tom istom riadku blokovej matice majú rovnaký počet riadkov a všetky matice v tom istom stĺpci blokovej matice majú rovnaký počet stĺpcov. Takto chápanú blokovú maticu možno zapísať v tvare

$$\boldsymbol{A} = (\boldsymbol{A}_{ij})_{k\times l} = \begin{pmatrix} \boldsymbol{A}_{11} & \dots & \boldsymbol{A}_{1l} \\ \vdots & \ddots & \vdots \\ \boldsymbol{A}_{k1} & \dots & \boldsymbol{A}_{kl} \end{pmatrix},$$

pričom jednotlivé bloky $\boldsymbol{A}_{ij}$ sú matice nad X rozmerov $m_i \times n_j$, kde $(m_1, \dots, m_k)$, $(n_1, \dots, n_l)$ sú nejaké konečné postupnosti prirodzených čísel. Maticu nad množinou X z tejto „matice matíc“ dostaneme tak, že si v $\boldsymbol{A}$ odmyslíme vnútorné zátvorky oddeľujúce jej jednotlivé bloky $\boldsymbol{A}_{ij}$.

2.2. Matice nad daným poľom

Na množine X, nad ktorou sme vytvárali príslušné matice, sme zatiaľ nepredpokladali nijakú ďalšiu štruktúru. Jednako na množinách matíc $X^{m\times n}$ sa nám pomerne bohatá štruktúra prirodzene vynorila. Všetky doposiaľ zavedené maticové operácie a vlastnosti však mali výlučne *pozičný charakter* – zakladali sa na reprezentácii každej matice ako príslušnej obdĺžnikovej tabuľky. Ďalšie maticové operácie a vlastnosti, ktoré hodláme zaviesť a neskôr využívať, už budú podmienené prítomnosťou istej štruktúry na množine X.

Najdôležitejší a, až na pár výnimiek, vlastne jediný druh matíc, ktorými sa budeme v tomto kurze zaoberať, tvoria matice nad nejakým poľom. Teda v celom paragrafe K označuje pevne zvolené, inak však ľubovoľné pole. V súlade s predošlým paragrafom $K^{m\times n}$, kde $m, n \in \mathbb{N}$, označuje množinu všetkých matíc typu $m \times n$ nad poľom K.

2.2.1. Vektorový priestor matíc. Pre pevné $m, n \in K$ budeme na množine matíc $K^{m\times n}$ definovať po zložkách operácie súčtu a skalárneho násobku. Teda pre matice $\boldsymbol{A} = (a_{ij})_{m\times n}$, $\boldsymbol{B} = (b_{ij})_{m\times n}$ nad K a $c \in K$ položíme

$$\begin{aligned} \boldsymbol{A} + \boldsymbol{B} &= (a_{ij} + b_{ij})_{m\times n}, \\ c\boldsymbol{A} &= (ca_{ij})_{m\times n}. \end{aligned}$$

Podotýkame, že súčet matíc $\boldsymbol{A} + \boldsymbol{B}$ je definovaný len pre matice $\boldsymbol{A}$, $\boldsymbol{B}$ rovnakého typu a samotná matica $\boldsymbol{A}+\boldsymbol{B}$ je toho istého typu ako $\boldsymbol{A}$ a $\boldsymbol{B}$. Neutrálnym prvkom operácie sčítania na $K^{m\times n}$ je matica typu $m \times n$, ktorej všetky prvky sú nulové; nazývame ju *nulová matica* typu $m\times n$ a označujeme ju $\mathbf{0}_{m,n}$, prípadne len $\mathbf{0}$, keď jej rozmer je jasný z kontextu alebo na ňom nezáleží. Opačným prvkom k matici $A = (a_{ij})_{m\times n}$ je zrejme matica $-\boldsymbol{A} = (-a_{ij})_{m\times n}$.

Čitateľ si iste sám ľahko overí, že matice ľubovoľného pevného typu $m\times n$ nad poľom K s takto definovanými operáciami súčtu a skalárneho násobku tvoria *vektorový priestor* nad poľom K. Odteraz teda $K^{m\times n}$ už označuje nielen množinu takýchto matíc, ale príslušný vektorový priestor. Nám už známe vektorové priestory $K^{1\times n}$ a $K^{m\times 1}$ riadkových resp. stĺpcových vektorov sú zrejme špeciálnymi prípadmi vektorových priestorov matíc.

2.2.2. Násobenie matíc. Okrem štruktúry vektorového priestoru na množine matíc pevného typu $m\times n$ budeme definovať aj operáciu násobenia matíc, ktorá spája matice rôznych, „vhodne do seba zapadajúcich“ rozmerov.

Pod vplyvom doterajšieho výkladu čitateľ po takomto nadpise asi očakáva, že i súčin matíc budeme definovať na množine $K^{m\times n}$ po zložkách. Hoci by to, samozrejme, bolo možné a na prvý pohľad sa to zdá prirodzené, násobenie matíc budeme definovať diametrálne odlišným spôsobom, ktorý sa nám zatiaľ môže zdať čudný a neprirodzený. Dôvody pre takúto definíciu budú postupne vychádzať najavo a jej prednosti budeme mať mnohokrát možnosť oceniť.

Najprv sa naučíme násobiť niektoré dvojice vektorov. Pod *súčinom* $\boldsymbol{x} \cdot \boldsymbol{y}$ *riadkového vektora* $\boldsymbol{x} = (x_1, \dots, x_n) \in K^{1\times n}$ *a stĺpcového vektora* $\boldsymbol{y} = (y_1, \dots, y_n)^T \in K^{n\times 1}$ rozumieme skalár

$$\boldsymbol{x} \cdot \boldsymbol{y} = (x_1, \dots, x_n) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + \ldots + x_n y_n = \sum_{i=1}^{n} x_i y_i \,.$$

Teda, až na „nepochopiteľné“ miešanie riadkových a stĺpcových vektorov, ide o bežný „skalárny súčin“ vektorov $\boldsymbol{x}, \boldsymbol{y} \in K^n$.

Pre takto definovaný súčin vektorov sú tiež splnené dobre známe vlastnosti „skalárneho súčinu“. Ľahko možno nahliadnuť, prípadne priamym výpočtom overiť, že pre všetky $n \in \mathbb{N}$, $c \in K$ a $\boldsymbol{x}, \boldsymbol{x}' \in K^{1\times n}$, $\boldsymbol{y}, \boldsymbol{y}' \in K^{n\times 1}$ platí

$$\begin{aligned} \boldsymbol{x} \cdot (\boldsymbol{y} + \boldsymbol{y}') &= \boldsymbol{x} \cdot \boldsymbol{y} + \boldsymbol{x} \cdot \boldsymbol{y}', \\ (\boldsymbol{x} + \boldsymbol{x}') \cdot \boldsymbol{y} &= \boldsymbol{x} \cdot \boldsymbol{y} + \boldsymbol{x}' \cdot \boldsymbol{y}, \\ \boldsymbol{x} \cdot c\boldsymbol{y} &= c(\boldsymbol{x} \cdot \boldsymbol{y}) = c\boldsymbol{x} \cdot \boldsymbol{y}, \\ \boldsymbol{x} \cdot \boldsymbol{y} &= \boldsymbol{y}^T \cdot \boldsymbol{x}^T. \end{aligned}$$

Hovoríme, že násobenie riadkových a stĺpcových vektorov je *distributívne* (z oboch strán) vzhľadom na sčítanie a *komutuje*, t. j. je zameniteľné s operáciou skalárneho násobku. Poslednú rovnosť možno chápať ako svojho druhu *„komutatívnosť“* tohto súčinu; vďačíme za ňu komutatívnosti násobenia v poli K.

Nech $m, n, p \in \mathbb{N}$ a $\boldsymbol{A} = (a_{ij})_{m \times n}$, $\boldsymbol{B} = (b_{jk})_{n \times p}$. Pod *súčinom matíc* $\boldsymbol{A}$, $\boldsymbol{B}$ rozumieme maticu

$$\boldsymbol{A} \cdot \boldsymbol{B} = (\boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{s}_k(\boldsymbol{B}))_{m \times p}.$$

Všimnime si, že súčin matíc $\boldsymbol{A}$, $\boldsymbol{B}$ je definovaný, len ak sa počet stĺpcov matice $\boldsymbol{A}$ rovná počtu riadkov matice $\boldsymbol{B}$, t. j. práve vtedy, keď riadky matice $\boldsymbol{A}$ a stĺpce matice $\boldsymbol{B}$ majú rovnaký rozmer. Ďalej, súčin matíc typov $m \times n$ a $n \times p$ je matica typu $m \times p$, čo si možno ľahko zapamätať v symbolickom tvare

$$[m \times n] \cdot [n \times p] = [m \times p],$$

pripomínajúcom rozmerové vzťahy vo fyzike. Špeciálne, súčin dvoch štvorcových matíc typu $n \times n$ je opäť matica typu $n \times n$. Konečne, prvok na mieste (i, k) matice $\boldsymbol{A} \cdot \boldsymbol{B}$ dostaneme ako súčin i-teho riadku matice $\boldsymbol{A}$ a k-teho stĺpca matice $\boldsymbol{B}$, teda ako výraz

$$\boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{s}_k(\boldsymbol{B}) = (a_{i1}, \ldots, a_{in}) \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix} = a_{i1}b_{1k} + \ldots + a_{in}b_{nk} = \sum_{j=1}^{n} a_{ij}b_{jk}\,.$$

Na základe toho možno ľahko nahliadnuť (prípadne priamym výpočtom overiť) nasledujúce rovnosti

$$\boldsymbol{r}_i(\boldsymbol{A} \cdot \boldsymbol{B}) = \boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{B}, \qquad \boldsymbol{s}_k(\boldsymbol{A} \cdot \boldsymbol{B}) = \boldsymbol{A} \cdot \boldsymbol{s}_k(\boldsymbol{B}).$$

Násobenie matíc je (z oboch strán) *distributívne* vzhľadom na sčítanie. To znamená že pre ľubovoľné $m, n \in \mathbb{N}$ a matice $\boldsymbol{A}$, $\boldsymbol{A}' \in K^{m \times n}$, $\boldsymbol{B}$, $\boldsymbol{B}' \in K^{n \times p}$ platí

$$\boldsymbol{A} \cdot (\boldsymbol{B} + \boldsymbol{B}') = \boldsymbol{A} \cdot \boldsymbol{B} + \boldsymbol{A} \cdot \boldsymbol{B}',$$
$$(\boldsymbol{A} + \boldsymbol{A}') \cdot \boldsymbol{B} = \boldsymbol{A} \cdot \boldsymbol{B} + \boldsymbol{A}' \cdot \boldsymbol{B}.$$

Vďaka distributívnosti súčinu vektorov voči ich súčtu je totiž jasné, že (i,k)-ty prvok matice $\boldsymbol{A}\cdot(\boldsymbol{B}+\boldsymbol{B}')$ je

$$\boldsymbol{r}_i(\boldsymbol{A})\cdot\boldsymbol{s}_k(\boldsymbol{B}+\boldsymbol{B}') = \boldsymbol{r}_i(\boldsymbol{A})\cdot(\boldsymbol{s}_k(\boldsymbol{B})+\boldsymbol{s}_k(\boldsymbol{B}')) = \boldsymbol{r}_i(\boldsymbol{A})\cdot\boldsymbol{s}_k(\boldsymbol{B})+\boldsymbol{r}_i(\boldsymbol{A})\cdot\boldsymbol{s}_k(\boldsymbol{B}'),$$

teda sa rovná (i,k)-temu prvku matice $\boldsymbol{A}\cdot\boldsymbol{B}+\boldsymbol{A}\cdot\boldsymbol{B}'$. Rovnako pre druhú rovnosť.

Podobne, s využitím zameniteľnosti súčinu vektorov a skalárneho násobku možno dokázať, že pre ľubovoľný skalár $c\in K$ a všetky matice $\boldsymbol{A}\in K^{m\times n}$, $\boldsymbol{B}\in K^{n\times p}$ platí

$$\boldsymbol{A}\cdot c\boldsymbol{B} = c(\boldsymbol{A}\cdot\boldsymbol{B}) = c\boldsymbol{A}\cdot\boldsymbol{B}.$$

Hovoríme, že násobenie matíc *komutuje*, t. j. je zameniteľné s operáciou skalárneho násobku.

Násobenie matíc je tiež *asociatívne* v nasledujúcom zmysle: súčin matíc $\boldsymbol{A}\cdot(\boldsymbol{B}\cdot\boldsymbol{C})$ je definovaný práve vtedy, keď je definovaný súčin $(\boldsymbol{A}\cdot\boldsymbol{B})\cdot\boldsymbol{C}$, a v takom prípade sa obe matice rovnajú. Teda podrobnejšie, pre $m,n,p,q\in\mathbb{N}$ a $\boldsymbol{A}\in K^{m\times n}$, $\boldsymbol{B}\in K^{n\times p}$, $\boldsymbol{C}\in K^{p\times q}$ platí

$$\boldsymbol{A}\cdot(\boldsymbol{B}\cdot\boldsymbol{C}) = (\boldsymbol{A}\cdot\boldsymbol{B})\cdot\boldsymbol{C}.$$

Na dôkaz toho si stačí uvedomiť, že pre ľubovoľné vektory $\boldsymbol{x}=(x_1,\dots,x_n)\in K^{1\times n}$, $\boldsymbol{y}=(y_1,\dots,y_p)^T\in K^{p\times 1}$ platí

$$\begin{aligned}\boldsymbol{x}\cdot(\boldsymbol{B}\cdot\boldsymbol{y}) &= (x_1,\dots,x_n)\cdot\begin{pmatrix}\sum_{k=1}^p b_{1k}y_k\\ \vdots\\ \sum_{k=1}^p b_{nk}y_k\end{pmatrix} = \sum_{j=1}^n x_j\Big(\sum_{k=1}^p b_{jk}y_k\Big)\\ &= \sum_{k=1}^p\Big(\sum_{j=1}^n x_jb_{jk}\Big)y_k = \Big(\sum_{j=1}^n x_jb_{j1},\dots,\sum_{j=1}^n x_jb_{jp}\Big)\cdot\begin{pmatrix}y_1\\ \vdots\\ y_p\end{pmatrix} = (\boldsymbol{x}\cdot\boldsymbol{B})\cdot\boldsymbol{y}.\end{aligned}$$

Potom pre $1 \leq i \leq m$, $1 \leq l \leq q$, prvok na mieste (i, l) matice $\boldsymbol{A} \cdot (\boldsymbol{B} \cdot \boldsymbol{C})$ je

$$\begin{aligned} \boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{s}_l(\boldsymbol{B} \cdot \boldsymbol{C}) &= \boldsymbol{r}_i(\boldsymbol{A}) \cdot (\boldsymbol{B} \cdot \boldsymbol{s}_l(\boldsymbol{C})) \\ &= (\boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{B}) \cdot \boldsymbol{s}_l(\boldsymbol{C}) = \boldsymbol{r}_i(\boldsymbol{A} \cdot \boldsymbol{B}) \cdot \boldsymbol{s}_l(\boldsymbol{C}), \end{aligned}$$

teda sa rovná (i, l)-tému prvku matice $(\boldsymbol{A} \cdot \boldsymbol{B}) \cdot \boldsymbol{C}$. Štvorcovú maticu rádu n, ktorá má všetky prvky na diagonále rovné 1 a mimo diagonály 0, označujeme $\boldsymbol{I}_n$ a nazývame *jednotkovou maticou* rádu n. S použitím tzv. *Kroneckerovho symbolu*

$$\delta_{ij} = \begin{cases} 1, & \text{ak } i = j, \\ 0, & \text{ak } i \neq j, \end{cases}$$

môžeme písať

$$\boldsymbol{I}_n = (\delta_{ij})_{n \times n} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Jednotkové matice hrajú úlohu neutrálnych prvkov pre násobenie matíc. Presnejšie, pre ľubovoľnú maticu $\boldsymbol{A} \in K^{m \times n}$ platí

$$\boldsymbol{I}_m \cdot \boldsymbol{A} = \boldsymbol{A} = \boldsymbol{A} \cdot \boldsymbol{I}_n.$$

Rozmyslite si prečo.

Špeciálne, množina $K^{n\times n}$ všetkých štvorcových matíc rádu n je tak popri štruktúre vektorového priestoru navyše vybavená asociatívnou operáciou násobenia, ktorá je (z oboch strán) distributívna vzhľadom na sčítanie matíc, komutuje s operáciou skalárneho násobku a jednotková matica $\boldsymbol{I}_n$ je jej neutrálny prvok. To nám, podobne ako pre prvky poľa K, umožňuje zaviesť i *mocniny štvorcových matíc*. Pre $\boldsymbol{A} \in K^{n\times n}$, kladieme

$$\boldsymbol{A}^0 = \boldsymbol{I}_n \quad \text{a} \quad \boldsymbol{A}^k = \underbrace{\boldsymbol{A} \cdot \ldots \cdot \boldsymbol{A}}_{k\text{-krát}}$$

ak $0 < k \in \mathbb{N}$; teda $\boldsymbol{A}^1 = \boldsymbol{A}$, $\boldsymbol{A}^2 = \boldsymbol{A} \cdot \boldsymbol{A}$, $\boldsymbol{A}^3 = \boldsymbol{A} \cdot \boldsymbol{A} \cdot \boldsymbol{A}$, atď.

Na druhej strane si treba uvedomiť, že pre $n > 1$ – napriek komutatívnosti násobenia v poli K – násobenie matíc z pozičných dôvodov *nie je komutatívne* na $K^{n\times n}$. Napríklad

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1+1 \\ 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1+1 \end{pmatrix}.$$

(Uvedomte si, že na to, aby oba súčiny $\boldsymbol{A} \cdot \boldsymbol{B}$, $\boldsymbol{B} \cdot \boldsymbol{A}$ boli definované a mali rovnaké rozmery, teda, aby vôbec malo zmysel uvažovať o komutatívnosti súčinu, $\boldsymbol{A}$, $\boldsymbol{B}$ musia byť štvorcové matice rovnakého typu.)

Napriek tomu komutatívnosť násobenia v poli K má za dôsledok, že pre všetky m, n, p a matice $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{B} \in K^{n\times p}$ platí rovnosť

$$(\boldsymbol{A} \cdot \boldsymbol{B})^T = \boldsymbol{B}^T \cdot \boldsymbol{A}^T.$$

Naozaj, $(\boldsymbol{A} \cdot \boldsymbol{B})^T$ aj $\boldsymbol{B}^T \cdot \boldsymbol{A}^T$ sú matice typu $p \times m$ a pre $1 \leq i \leq m$, $1 \leq k \leq p$, (k, i)-ty prvok matice $(\boldsymbol{A} \cdot \boldsymbol{B})^T$ je (i, k)-ty prvok matice $\boldsymbol{A} \cdot \boldsymbol{B}$, t. j.

$$\boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{s}_k(\boldsymbol{B}) = \boldsymbol{s}_k(\boldsymbol{B})^T \cdot \boldsymbol{r}_i(\boldsymbol{A})^T = \boldsymbol{r}_k(\boldsymbol{B}^T) \cdot \boldsymbol{s}_i(\boldsymbol{A}^T),$$

čo je (k,i)-ty prvok matice $\boldsymbol{B}^T \cdot \boldsymbol{A}^T$. Pritom sme využili už spomínanú „komutatívnosť“ $\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y}^T \cdot \boldsymbol{x}^T$ súčinu vektorov.

Na margo poslednej rovnosti ešte podotknime, že pre $\boldsymbol{x} \in K^{1\times n}$, $\boldsymbol{y} \in K^{m\times 1}$ je taktiež definovaný súčin $\boldsymbol{y} \cdot \boldsymbol{x}$. Nie je to však skalár, ale matica typu $m \times n$:

$$\boldsymbol{y} \cdot \boldsymbol{x} = (y_i x_j)_{m\times n} = \begin{pmatrix} y_1 x_1 & \dots & y_1 x_n \\ \vdots & \ddots & \vdots \\ y_m x_1 & \dots & y_m x_n \end{pmatrix}.$$

Teda, okrem prípadu $m = n = 1$, rovnosť $\boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{y} \cdot \boldsymbol{x}$ nemôže nastať už z rozmerových dôvodov.

2.2.3. Operácie s blokovými maticami. Operácie maticového súčtu a skalárneho násobku, vďaka tomu, že boli definované po zložkách, možno na blokových maticiach rozložiť na jednotlivé bloky. Ak $\boldsymbol{A} = (\boldsymbol{A}_{ij})_{k\times l}$, $\boldsymbol{B} = (\boldsymbol{B}_{ij})_{k\times l}$ sú blokové matice nad poľom K, pričom zodpovedajúce si bloky $\boldsymbol{A}_{ij}$, $\boldsymbol{B}_{ij}$ majú rovnaký typ $m_i \times n_j$, tak ich súčet je opäť bloková matica

$$\boldsymbol{A} + \boldsymbol{B} = (\boldsymbol{A}_{ij} + \boldsymbol{B}_{ij})_{k\times l}$$

s blokmi rovnakých typov. S operáciou skalárneho násobku je to ešte jednoduchšie, lebo sa nemusíme starať o zhodnosť rozmerov jednotlivých blokov. Pre $c \in K$ jednoducho dostávame

$$c\boldsymbol{A} = (c\boldsymbol{A}_{ij})_{k\times l}.$$

Bloková štruktúra sa prenáša aj na súčin matíc za podmienky, že stĺpce prvej matice sú v rovnakom poradí rozdelené na rovnaký počet rovnako veľkých skupín, povedzme

$n_1 + n_2 + \ldots + n_\nu$, ako riadky druhej matice. Teda ak $\boldsymbol{A} = (\boldsymbol{A}_{ij})_{\mu\times\nu}$, $\boldsymbol{B} = (\boldsymbol{B}_{jk})_{\nu\times\vartheta}$ sú blokové matice nad K, pričom blok $\boldsymbol{A}_{ij}$ je typu $m_i \times n_j$ a blok $\boldsymbol{B}_{jk}$ typu $n_j \times p_k$, tak aj ich súčin je bloková matica tvaru $\boldsymbol{A} \cdot \boldsymbol{B} = (\boldsymbol{C}_{ik})_{\mu\times\vartheta}$, kde blok

$$\boldsymbol{C}_{ik} = \boldsymbol{A}_{i1} \cdot \boldsymbol{B}_{1k} + \boldsymbol{A}_{i2} \cdot \boldsymbol{B}_{2k} + \ldots + \boldsymbol{A}_{i\nu} \cdot \boldsymbol{B}_{\nu k}$$

je typu $m_i \times p_k$. Inak povedané, blokové matice násobíme tak ako „obyčajné“ matice, len s tým rozdielom, že súčet resp. súčin v poli K nahradíme súčtom resp. súčinom matíc. Vo výsledku, ak chceme, si nakoniec môžeme odmyslieť zátvorky oddeľujúce jednotlivé bloky a matica, ktorú takto dostaneme, sa rovná matici, ktorú by sme dostali, keby sme „normálne“ vynásobili „odblokované“ matice $\boldsymbol{A}$ a $\boldsymbol{B}$.

Jednotkové matice $\boldsymbol{I}_n$ sú príkladom tzv. diagonálnych matíc. Štvorcovú maticu $\boldsymbol{A} = (a_{ij})_{n\times n}$ nazývame *diagonálnou*, ak $a_{ij} = 0$ pre všetky $i \neq j$, t. j. ak všetky jej prvky mimo diagonály sú nuly.

Diagonálnu maticu, ktorá má na diagonále postupne prvky $d_1, d_2, \ldots, d_n \in K$ značíme $\operatorname{diag}(d_1, d_2, \ldots, d_n)$. Teda napr.

$$\boldsymbol{I}_n = \operatorname{diag}(\underbrace{1, \ldots, 1}_{n\text{-krát}}).$$

Podobne možno definovať aj tzv. blokovo diagonálne matice. Ak $\boldsymbol{A}_1$, $\boldsymbol{A}_2, \ldots, \boldsymbol{A}_k$ sú štvorcové matice rádov $n_1, n_2, \ldots, n_k$, tak *blokovo diagonálnou maticou* s blokmi $\boldsymbol{A}_1$, $\boldsymbol{A}_2, \ldots, \boldsymbol{A}_k$

nazývame štvorcovú blokovú maticu

$$\operatorname{diag}(\boldsymbol{A}_1, \boldsymbol{A}_2, \dots, \boldsymbol{A}_k) = \begin{pmatrix} \boldsymbol{A}_1 & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & \boldsymbol{A}_2 & \dots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \dots & \boldsymbol{A}_k \end{pmatrix},$$

kde $\mathbf{0}$ nachádzajúca sa na mieste (i, j) označuje nulovú maticu $\mathbf{0}_{n_i n_j}$.

Pred chvíľou uvedené pravidlo o súčine blokových matíc sa redukuje na obzvlášť jednoduchý tvar pre blokovo diagonálne matíce – ich násobenie totiž funguje *diagonálne po zložkách*. Ak $\boldsymbol{A} = \operatorname{diag}(\boldsymbol{A}_1, \dots, \boldsymbol{A}_k)$, $\boldsymbol{B} = \operatorname{diag}(\boldsymbol{B}_1, \dots, \boldsymbol{B}_k)$ sú blokovo diagonálne matice, pričom zodpovedajúce si bloky $\boldsymbol{A}_i$, $\boldsymbol{B}_i$ sú štvorcové matice rovnakého rádu n_i, tak aj ich súčin je blokovo diagonálna matica tvaru

$$\boldsymbol{A} \cdot \boldsymbol{B} = \operatorname{diag}(\boldsymbol{A}_1 \cdot \boldsymbol{B}_1, \dots, \boldsymbol{A}_k \cdot \boldsymbol{B}_k)$$

so štvorcovými blokmi rádov $n_1, \dots, n_k$. Špeciálne, pre „obyčajné“ diagonálne matice platí

$$\operatorname{diag}(a_1, \dots, a_n) \cdot \operatorname{diag}(b_1, \dots, b_n) = \operatorname{diag}(a_1 b_1, \dots, a_n b_n).$$

Formuláciu analogických pravidiel pre súčet a skalárny násobok (blokovo) diagonálnych matíc prenechávame čitateľovi.

2.3. Matice nad vektorovým priestorom

Matice nad typu $m \times n$ nad poľom K sú špeciálnym druhom blokových matíc. Maticu $\boldsymbol{A} = (a_{ij}) \in K^{m\times n}$ môžeme považovať jednak za blokovú maticu s blokmi a_{ij} typu 1×1, jednak, ako sme už neraz naznačili, môžeme sa na ňu dívať ako na riadok jej stĺpcov resp. ako na stĺpec jej riadkov. V takom prípade $\boldsymbol{A}$ chápeme ako maticu typu $m \times 1$ nad vektorovým priestorom $K^{1\times n}$, resp. ako maticu typu $1\times n$ nad vektorovým priestorom $K^{m\times 1}$. Konkrétna podoba týchto vektorových priestorov je však teraz pre nás nepodstatná – pre ľubovoľné $m, n \in \mathbb{N}$ a ľubovoľný (abstraktný) vektorový priestor V máme totiž definovanú množinu $V^{m\times n}$ všetkých matíc nad množinou V.

Na množine $V^{m\times n}$ možno zaviesť operácie súčtu a skalárneho násobku po zložkách. $V^{m\times n}$ s týmito operáciami opäť tvorí vektorový priestor nad poľom K. Čitateľovi ponechávame, aby si sám doplnil a premyslel potrebné detaily.

My sa sústredíme na zovšeobecnenie operácie skalárneho násobku $K\times V \to V$ na operácie súčinu medzi maticami vhodných typov nad K a nad V. Pre matice $\boldsymbol{A} = (a_{ij}) \in K^{m\times n}$, $\boldsymbol{\alpha} = (\boldsymbol{u}_{jk}) \in V^{n\times p}$ kladieme $\boldsymbol{A} \cdot \boldsymbol{\alpha} = (\boldsymbol{v}_{ik}) \in V^{m\times p}$, kde

$$\boldsymbol{v}_{ik} = \sum_{j=1}^{n} a_{ij}\boldsymbol{u}_{jk} \,.$$

Teda súčin $\boldsymbol{A} \cdot \boldsymbol{\alpha}$ definujeme z formálneho hľadiska rovnako ako súčin matíc nad poľom K, len s tým rozdielom že operácia súčtu v K je nahradená operáciou súčtu vo V a operácia súčinu v K operáciou skalárneho násobku $K \times V \to V$.

Celkom obdobne ako v odstavci 2.2.2 aj pre násobenie matíc nad V maticami nad K možno overiť distributívnosť (z oboch strán) vzhľadom na sčítanie, zameniteľnosť s operáciou skalárneho násobku, asociatívnosť a postavenie jednotkových matíc ako neutrálnych prvkov. To znamená, že pre všetky $l, m, n, p \in \mathbb{N}$, $c \in K$, $\boldsymbol{A}$, $\boldsymbol{B} \in K^{m\times n}$, $\boldsymbol{C} \in K^{l\times m}$ $\boldsymbol{\alpha}$, $\boldsymbol{\beta} \in V^{n\times p}$ platí:

$$\boldsymbol{A}\cdot(\boldsymbol{\alpha}+\boldsymbol{\beta}) = \boldsymbol{A}\cdot\boldsymbol{\alpha}+\boldsymbol{A}\cdot\boldsymbol{\beta},$$
$$(\boldsymbol{A}+\boldsymbol{B})\cdot\boldsymbol{\alpha} = \boldsymbol{A}\cdot\boldsymbol{\alpha}+\boldsymbol{B}\cdot\boldsymbol{\alpha},$$
$$\boldsymbol{A}\cdot(c\boldsymbol{\alpha}) = c(\boldsymbol{A}\cdot\boldsymbol{\alpha}) = (c\boldsymbol{A})\cdot\boldsymbol{\alpha},$$
$$\boldsymbol{C}\cdot(\boldsymbol{A}\cdot\boldsymbol{\alpha}) = (\boldsymbol{C}\cdot\boldsymbol{A})\cdot\boldsymbol{\alpha},$$
$$\boldsymbol{I}_n\cdot\boldsymbol{\alpha} = \boldsymbol{\alpha}.$$

Vzhľadom na našu dohodu, podľa ktorej $\boldsymbol{x}c = c\boldsymbol{x}$ pre $c \in K$, $\boldsymbol{x} \in V$, môžeme definovať aj súčin matíc $\boldsymbol{\beta} = (\boldsymbol{v}_{ij}) \in V^{m\times n}$, $\boldsymbol{B} = (\boldsymbol{b}_{jk}) \in K^{n\times p}$ v obrátenom poradí ako maticu $\boldsymbol{\beta}\cdot\boldsymbol{B} = (\boldsymbol{w}_{ik}) \in V^{m\times p}$ takú, že

$$\boldsymbol{w}_{ik} = \sum_{j=1}^{n} \boldsymbol{v}_{ij} b_{jk} = \sum_{j=1}^{n} b_{jk}\boldsymbol{v}_{ij}\,.$$

S využitím poslednej definície možno pre $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{\alpha} \in V^{n\times p}$, $\boldsymbol{\beta} \in V^{m\times n}$, $\boldsymbol{B} \in K^{n\times p}$ dokázať tiež rovnosti

$$(\boldsymbol{A}\cdot\boldsymbol{\alpha})^T = \boldsymbol{\alpha}^T\cdot\boldsymbol{A}^T, \qquad (\boldsymbol{\beta}\cdot\boldsymbol{B})^T = \boldsymbol{B}^T\cdot\boldsymbol{\beta}^T.$$

Aplikáciou týchto vzťahov na predchádzjúci zoznam rovností (no taktiež priamo) možno aj pre súčin matíc tvaru $\boldsymbol{\beta}\cdot\boldsymbol{B}$, kde $\boldsymbol{\beta} \in V^{m\times n}$, $\boldsymbol{B} \in K^{n\times p}$, overiť jeho distributívnosť (z oboch strán) vzhľadom na sčítanie, zameniteľnosť s operáciou skalárneho násobku, asociatívnosť a postavenie jednotkových matíc ako neutrálnych prvkov. To znamená, že pre všetky $m, n, p, q \in \mathbb{N}$, $c \in K$, $\boldsymbol{\alpha}$, $\boldsymbol{\beta} \in K^{m\times n}$, $\boldsymbol{A}$, $\boldsymbol{B} \in V^{n\times p}$, $\boldsymbol{C} \in K^{p\times q}$ platí:

$$(\boldsymbol{\alpha}+\boldsymbol{\beta})\cdot\boldsymbol{A} = \boldsymbol{\alpha}\cdot\boldsymbol{A}+\boldsymbol{\beta}\cdot\boldsymbol{A},$$
$$\boldsymbol{\alpha}\cdot(\boldsymbol{A}+\boldsymbol{B}) = \boldsymbol{\alpha}\cdot\boldsymbol{A}+\boldsymbol{\alpha}\cdot\boldsymbol{B},$$
$$\boldsymbol{\alpha}\cdot(c\boldsymbol{A}) = c(\boldsymbol{\alpha}\cdot\boldsymbol{A}) = (c\boldsymbol{\alpha})\cdot\boldsymbol{A},$$
$$\boldsymbol{\alpha}\cdot(\boldsymbol{A}\cdot\boldsymbol{C}) = (\boldsymbol{\alpha}\cdot A)\cdot\boldsymbol{C},$$
$$\boldsymbol{\alpha}\cdot\boldsymbol{I}_n = \boldsymbol{\alpha}.$$

Taktiež vzťahy pre riadky a stĺpce súčinu z odseku 2.2.2 zostávajú zachované pre oba typu súčinov matíc nad K a V, t. j.

$$\begin{aligned} \boldsymbol{r}_i(\boldsymbol{A}\cdot\boldsymbol{\alpha}) &= \boldsymbol{r}_i(\boldsymbol{A})\cdot\boldsymbol{\alpha}, &\qquad \boldsymbol{s}_k(\boldsymbol{A}\cdot\boldsymbol{\alpha}) &= \boldsymbol{A}\cdot\boldsymbol{s}_k(\boldsymbol{\alpha}) \\ \boldsymbol{r}_i(\boldsymbol{\beta}\cdot\boldsymbol{B}) &= \boldsymbol{r}_i(\boldsymbol{\beta})\cdot\boldsymbol{B}, &\qquad \boldsymbol{s}_k(\boldsymbol{\beta}\cdot\boldsymbol{B}) &= \boldsymbol{\beta}\cdot\boldsymbol{s}_k(\boldsymbol{B}) \end{aligned}$$

pre všetky $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{\alpha} \in V^{n\times p}$ $\boldsymbol{\beta} \in V^{m\times n}$, $\boldsymbol{B} \in K^{n\times p}$.

Napokon si ešte uvedomme, že definície súčinov $\boldsymbol{A}\cdot\boldsymbol{\alpha}$, $\boldsymbol{\beta}\cdot\boldsymbol{B}$ sú v zhode s pôvodným násobením matíc. Ak totiž maticu $\boldsymbol{A} \in K^{m\times n}$ chápame ako riadok, t. j. ako maticu typu $1\times n$ nad priestorom stĺpcových vektorov K^m, tak pre $\boldsymbol{B} \in K^{n\times p}$ splýva matica $(\boldsymbol{s}_1(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A}))\cdot\boldsymbol{B}$ vypočítaná podľa „novej" definície s blokovým tvarom $(\boldsymbol{A}\cdot\boldsymbol{s}_1(\boldsymbol{B}), \dots, \boldsymbol{A}\cdot\boldsymbol{s}_p(\boldsymbol{B}))$ matice $\boldsymbol{A}\cdot\boldsymbol{B}$. Podobne, ak $\boldsymbol{B}$ chápeme ako stĺpec, t. j. ako maticu typu $n\times 1$ nad priestorom riadkových vektorov K^p, tak

$$\boldsymbol{A}\cdot\begin{pmatrix}\boldsymbol{r}_1(\boldsymbol{B})\\ \vdots\\ \boldsymbol{r}_n(\boldsymbol{B})\end{pmatrix} = \begin{pmatrix}\boldsymbol{r}_1(\boldsymbol{A})\cdot\boldsymbol{B}\\ \vdots\\ \boldsymbol{r}_m(\boldsymbol{A})\cdot\boldsymbol{B}\end{pmatrix} = \boldsymbol{A}\cdot\boldsymbol{B}.$$

(Doplňte si vynechané podrobnosti – pozri cvičenie 2.6.)

Špeciálne, lineárnu kombináciu $a_1\boldsymbol{x}_1 + \dots a_n\boldsymbol{x}_n$ vektorov $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n \in V$ s koeficientmi $a_1, \dots, a_n \in K$ môžeme s využitím vektorových matíc zapísať v tvare súčinov

$$a_1\boldsymbol{x}_1 + \dots + a_n\boldsymbol{x}_n = (a_1, \dots, a_n) \cdot \begin{pmatrix} \boldsymbol{x}_1 \\ \vdots \\ \boldsymbol{x}_n \end{pmatrix} = (\boldsymbol{x}_1, \dots, \boldsymbol{x}_n) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Cvičenia

2.1. Nech $\boldsymbol{A} = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 5 & 2 \\ 1 & -4 & 0 \end{pmatrix}$, $\boldsymbol{B} = \begin{pmatrix} 0 & 1 & 2 \\ -2 & 9 & 3 \\ 10 & 6 & 0 \end{pmatrix}$, $\boldsymbol{C} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \\ 1 & 2 & 4 \end{pmatrix}$ sú matice nad $\mathbb{R}$. Vypočítatjte matice
$\boldsymbol{A} + 2\boldsymbol{B}$, $\boldsymbol{A} - \boldsymbol{B}^T - 3\boldsymbol{C}$, $\boldsymbol{A} \cdot \boldsymbol{B}$, $\boldsymbol{B} \cdot \boldsymbol{A}$, $\boldsymbol{A} \cdot (\boldsymbol{B} + \boldsymbol{C})$,
$(3\boldsymbol{A}^T + \boldsymbol{B}) \cdot \boldsymbol{C}$, $\boldsymbol{B} \cdot \boldsymbol{C}^2$, $\boldsymbol{C}^2 \cdot \boldsymbol{B}$, $\boldsymbol{C} \cdot \boldsymbol{B} \cdot \boldsymbol{C}$, $\boldsymbol{A} \cdot \boldsymbol{C} - \boldsymbol{C} \cdot \boldsymbol{A}$, $\boldsymbol{A} \cdot \boldsymbol{B} \cdot \boldsymbol{C}$ a $\boldsymbol{C}^T \cdot \boldsymbol{A} \cdot \boldsymbol{C}$.

2.2. Vypočítajte súčin $\boldsymbol{A} \cdot \boldsymbol{B}$ komplexných matíc $\boldsymbol{A} = \begin{pmatrix} 1+\mathrm{i} & -2 & -\mathrm{i} \\ 1-\mathrm{i} & \mathrm{i} & 2+3\mathrm{i} \end{pmatrix}$, $\boldsymbol{B} = \begin{pmatrix} 3\mathrm{i} & 2+\mathrm{i} \\ -4 & 1-2\mathrm{i} \\ 0 & 4\mathrm{i} \end{pmatrix}$.

2.3. Nájdite matice $\boldsymbol{A}, \boldsymbol{B} \in \mathbb{Q}^{2\times 2}$ také, že $\boldsymbol{A} \cdot \boldsymbol{B} = \boldsymbol{0} \neq \boldsymbol{B} \cdot \boldsymbol{A}$.

2.4. Uvažujte matice $\boldsymbol{A} = \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}$, $\boldsymbol{B} = \begin{pmatrix} 0 & 1 \\ 4 & 1 \end{pmatrix}$, $\boldsymbol{C} = \begin{pmatrix} 4 & 3 \\ 4 & 0 \end{pmatrix}$ nad poľom
(a) $\mathbb{Z}_5$, (b) $\mathbb{Z}_7$, (c) $\mathbb{Z}_{11}$, (d) $\mathbb{Q}$.
V každom z uvedených prípadov vypočítajte maticu $\boldsymbol{A} \cdot (\boldsymbol{B} + \boldsymbol{C})$. Skúste riešiť úlohy (a)–(d) v optimálnom poradí.

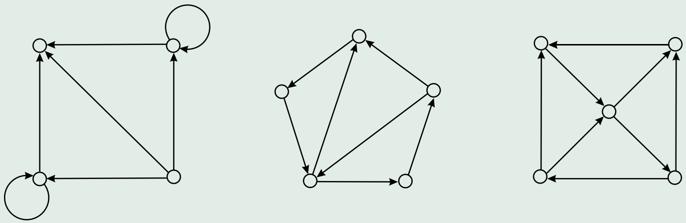
2.5. Sú dané reálne blokové matice $\boldsymbol{A} = \begin{pmatrix} \boldsymbol{A}_{11} & \boldsymbol{A}_{12} \\ \boldsymbol{A}_{21} & \boldsymbol{A}_{22} \end{pmatrix}$, $\boldsymbol{B} = \begin{pmatrix} \boldsymbol{B}_{11} & \boldsymbol{B}_{12} & \boldsymbol{B}_{13} \\ \boldsymbol{B}_{21} & \boldsymbol{B}_{22} & \boldsymbol{B}_{23} \end{pmatrix}$, kde

$\boldsymbol{A}_{11} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\boldsymbol{A}_{12} = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$, $\boldsymbol{A}_{21} = \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\boldsymbol{A}_{22} = \left(\begin{smallmatrix} 2 & 2 \\ 0 & 1 \end{smallmatrix}\right)$,
$\boldsymbol{B}_{11} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $\boldsymbol{B}_{12} = \boldsymbol{B}_{13} = \left(\begin{smallmatrix} 1 & 2 \\ 1 & -1 \end{smallmatrix}\right)$, $\boldsymbol{B}_{21} = \left(\begin{smallmatrix} 2 & 1 \\ -1 & 1 \end{smallmatrix}\right)$, $\boldsymbol{B}_{22} = \boldsymbol{B}_{23} = \left(\begin{smallmatrix} 2 & 2 \\ -1 & -1 \end{smallmatrix}\right)$.

Vynásobte $\boldsymbol{A}$ a $\boldsymbol{B}$ ako blokové matice aj ako matice, v ktorých ste zabudli na rozdelenie do blokov, a oba výsledky porovnajte.

2.6. Maticu $\boldsymbol{A} = (a_{ij})_{m\times n}$ nad ľubovoľným poľom K uvažujte ako riadok jej stĺpcov, t. j. ako blokovú maticu $\boldsymbol{A} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, kde $\boldsymbol{u}_j = \boldsymbol{s}_j(\boldsymbol{A})$ pre $j \le n$. Nech $\boldsymbol{c} = (c_1, \dots, c_n)^T \in K^n$ je stĺpcový vektor. Ukážte, že lineárna kombinácia $c_1\boldsymbol{u}_1 + \dots + c_n\boldsymbol{u}_n$ splýva s „obyčajným“ maticovým súčinom $\boldsymbol{A} \cdot \boldsymbol{c}$. Vysvetlite tento fakt pomocou násobenia blokových matíc.

2.7. Nech X je konečná množina. Ľubovoľná množina $H \subseteq X^2$ určuje *orientovaný graf* (X, H) s množinou *vrcholov* X a s množinou *orientovaných hrán* H: vrcholy (t. j. prvky množiny X) si znázorníme krúžkami v rovine a z vrcholu x vedieme orientovanú hranu (t. j. šípku) do vrcholu y práve vtedy, keď $(x, y) \in H$ (pozri obr. 2.1). Konečnú postupnosť $(z_0, z_1, \dots, z_k)$ prvkov množiny X takú, že pre každé $1 \le i \le k$ platí $(z_{i-1}, z_i) \in H$, nazývame *cestou* dĺžky k *v orientovanom grafe* (X, H). Predpokladajme, že $X = \{x_1, \dots, x_n\}$ má práve n prvkov. Maticu $\boldsymbol{H} = (h_{ij}) \in \mathbb{R}^{n\times n}$ takú, že $h_{ij} = 1$, ak $(x_i, x_j) \in H$, a $h_{ij} = 0$, ak $(x_i, x_j) \notin H$, nazývame *incidenčnou maticou orientovaného grafu* (X, H). Prvky k-tej mocniny incidenčnej matice $\boldsymbol{H}$ označme $h_{ij}^{(k)}$, t. j. $\boldsymbol{H}^k = \left(h_{ij}^{(k)}\right)$. Potom číslo $h_{ij}^{(k)}$ udáva počet ciest dĺžky k z vrcholu x_i do vrcholu x_j v orientovanom grafe (X, H). Dokážte (napr. matematickou indukciou).



Obr. 2.1. Príklady orientovaných grafov

2.8. Očíslujte vrcholy orientovaných grafov z obrázku 2.1). Pre každý graf napíšte jeho incidenčnú maticu a pre každú dvojicu (x_i, x_j) jeho vrcholov určte počet ciest dĺžky 2, 3, 4 a 5 z x_i do x_j.

2.9. Nech K je komutatívny okruh s jednotkou (pozri cvičenie 1.7). Presvedčte sa, že pre ľubovoľné $m, n \in \mathbb{N}$ možno na množine matíc $K^{m\times n}$ definovať operácie súčtu $\boldsymbol{A} + \boldsymbol{B}$ a skalárneho násobku $c\boldsymbol{A}$ rovnako ako v odstavci 2.2.1. Taktiež možno pre $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{B} \in K^{n\times p}$ definovať súčin $\boldsymbol{A} \cdot \boldsymbol{B} \in K^{m\times p}$ rovnako ako v odstavci 2.2.2. Ukážte, že všetky vlastnosti maticových operácií uvedené v kapitole 2 zostávajú v platnosti aj v tomto všeobecnejšom prípade.

2.10. Vynechajme z definície poľa, popri nerovnosti $0 \neq 1$ a požiadavke existencie inverzného prvku ku každému nenulovému $a \in K$, aj podmienku komutatívnosti násobenia, namiesto ktorej pridajme ešte jeden distributívny zákon $(\forall\, a, b, c \in K)((a + b)c = ac + bc)$. Množina K s význačnými prvkami 0 a 1, vybavená operáciami sčítania a násobenia, ktoré vyhovujú uvedeným podmienkam, sa nazýva *okruh s jednotkou.*[1]

(a) Okruh s jednotkou K sa nazýva *netriviálny*, ak v ňom platí $0 \neq 1$. Dokážte, že okruh s jednotkou K je netriviálny práve vtedy, keď obsahuje aspoň dva rôzne prvky.

(b) Nech K je okruh s jednotkou. Presvedčte sa, že pre matice nad K možno zaviesť operácie súčtu,

[1] Občas sa v literatúre takáto štruktúra nazýva len okruh.

skalárneho násobku a súčinu rovnako ako pre matice nad poľom. Ukážte, že všetky vlastnosti týchto operácií uvedené v kapitole 2, s výnimkou rovností $(\boldsymbol{x} \cdot \boldsymbol{y})^T = \boldsymbol{y}^T \cdot \boldsymbol{x}^T$, $(\boldsymbol{A} \cdot \boldsymbol{B})^T = \boldsymbol{B}^T \cdot \boldsymbol{A}^T$ a možnosti zapisovať „lineárne kombinácie“ v tvare $c_1 \boldsymbol{u}_1 + \ldots c_n \boldsymbol{u}_n = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) \cdot (c_1, \ldots, c_n)^T$, zostávajú v platnosti.

2.11. Nech K je okruh s jednotkou a $n \in \mathbb{N}$. Dokážte postupne nasledujúce tvrdenia:

(a) Množina $K^{n \times n}$ so sčítaním a násobením matíc tvorí okruh s jednotkou.

(b) Okruh s jednotkou $K^{n \times n}$ je triviálny práve vtedy, keď K je triviálny alebo $n = 0$.

(c) Okruh s jednotkou $K^{n \times n}$ je komutatívny práve vtedy, keď $n = 0$, alebo $n = 1$ a K je komutatívny.

2.12. (a) Rovnako ako v prípade poľa zadefinujte *charakteristiku* ľubovoľného *okruhu s jednotkou.*

(b) Dokážte, že okruh s jednotkou K je triviálny práve vtedy, keď $\operatorname{char} K = 1$.

(c) Nech K je ľubovoľný okruh a $1 \leq n \in \mathbb{N}$. Potom $\operatorname{char} K^{n \times n} = \operatorname{char} K$. Dokážte.

(d) Pre každé $2 \leq m \in \mathbb{N} \cup \{\infty\}$ uveďte príklad *nekomutatívneho* okruhu s jednotkou charakteristiky m.

2.13. Nech K je okruh s jednotkou.

(a) Pre všetky $n \in \mathbb{N}$ zadefinujte mocniny a^n prvku $a \in K$ rovnako ako v poli a dokážte, že pre $m, n \in \mathbb{N}$ platí $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$. Čo bráni definícii mocnín a^n pre záporné exponenty $n \in \mathbb{Z}$?

(b) Prvok $a \in K$ sa nazýva *invertovateľný*, ak k nemu existuje (obostranný, teda nutne jediný) inverzný prvok a^{-1} vzhľadom na násobenie. Pre invertovateľné prvky $a \in K$ rozšírte definíciu mocnín a^n na všetky $n \in \mathbb{Z}$ a dokážte rovnosti z (a) pre ľubovoľné $m, n \in \mathbb{Z}$.

(c) Nech $a, b \in K$. Čo je prekážkou všeobecnej platnosti rovnosti $(ab)^n = a^n b^n$ pre $n \geq 2$? Dokážte, že ak a, b *komutujú*, t. j. $ab = ba$, tak uvedená rovnosť platí pre všetky $n \in \mathbb{N}$.

(d) Pre $K = \mathbb{R}^{2 \times 2}$ nájdite príklad matíc $\boldsymbol{A}$, $\boldsymbol{B} \in K$ takých, že $(\boldsymbol{A} \cdot \boldsymbol{B})^2 \neq \boldsymbol{A}^2 \cdot \boldsymbol{B}^2$.

(e) Nech $a, b \in K$ sú invertovateľné. Dokážte, že potom aj prvok ab je invertovateľný a platí $(ab)^{-1} = b^{-1}a^{-1}$. Čo je prekážkou všeobecnej platnosti rovnosti $(ab)^{-n} = b^{-n}a^{-n}$ pre $n \geq 2$?

2.14. (a) Rovnako ako v príklade 1.6.3 a v cvičení 1.12 zadefinujte množinu $K[x]$ všetkých polynómov v premennej x nad ľubovoľným okruhom s jednotkou K a na nej operácie súčtu a súčinu. Dokážte, že $K[x]$ s takto definovanými operáciami je opäť okruh s jednotkou a platí $\operatorname{char} K[x] = \operatorname{char} K$.

(b) Dokážte, že $K[x]$ je komutatívny práve vtedy, keď K je komutatívny.

(c) Dokážte, že polynóm $f(x)$ je invertovateľný prvok okruhu $K[x]$ práve vtedy, keď $f(x) = a$ je konštantný polynóm, pričom a je invertovateľný prvok okruhu K.

3. Sústavy lineárnych rovníc

V tejto kapitole sa predbežne zoznámime so sústavami lineárnych rovníc nad všeobecným poľom K a naučíme sa ich riešiť. Využijeme pri tom zápis sústavy pomocou istej matice. Štruktúrne vlastnosti množiny všetkých riešení danej sústavy a ich dôsledky preštudujeme a využijeme až neskôr, keď sa bližšie oboznámime so štruktúrou vektorových priestorov.

3.1. Maticový zápis sústavy lineárnych rovníc

Pod *lineárnou rovnicou* o n neznámych $x_1, \ldots, x_n$ nad poľom K rozumieme formulu tvaru

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b,$$

kde $a_1, a_2, \ldots, a_n, b \in K$, v premenných $x_1, x_2, \ldots, x_n$. *Sústavou m lineárnych rovníc* o n neznámych $x_1, x_2, \ldots, x_n$ nad poľom K rozumieme konjunkciu formúl tvaru

$$\begin{array}{llll} a_{11}x_1 & + a_{21}x_2 & + \ldots + a_{1n}x_n & = b_1 \\ a_{21}x_1 & + a_{22}x_2 & + \ldots + a_{2n}x_n & = b_2 \\ \multicolumn{4}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \\ a_{m1}x_1 & + a_{m2}x_2 & + \ldots + a_{mn}x_n & = b_m, \end{array}$$

kde a_{ij}, b_i, pre $1 \leq i \leq m$, $1 \leq j \leq n$, sú skaláry z poľa K. Maticu $\boldsymbol{A} = (a_{ij}) \in K^{m\times n}$ nazývame *maticou sústavy*, stĺpcový vektor $\boldsymbol{b} = (b_1, \ldots, b_m)^T \in K^m$ nazývame jej *pravou* *stranou.* Konečne *rozšírenou maticou sústavy* nazývame blokovú maticu $(\boldsymbol{A} \mid \boldsymbol{b}) \in K^{m\times(n+1)}$. Sústava sa nazýva *homogénna*, ak $\boldsymbol{b} = \boldsymbol{0}$; v opačnom prípade sa nazýva *nehomogénna.*

Uvedenú sústavu možno stručne a úsporne zapísať v *maticovom tvare*

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b},$$

prípadne, ak ide o homogénnu sústavu, v tvare

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{0}.$$

Riešením sústavy $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ nazývame ľubovoľný vektor-stĺpec $\boldsymbol{x} = (x_1, x_2, \dots, x_n)^T \in K^n$, ktorého zložky vyhovujú každej z rovníc tejto sústavy, t. j. platí preň $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$. *Vyriešiť sústavu* znamená nájsť *všetky* jej riešenia, t. j. popísať *množinu* všetkých jej riešení.

Dve *sústavy* $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ a $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$, kde $\boldsymbol{A}, \boldsymbol{B} \in K^{m\times n}$, $\boldsymbol{b}, \boldsymbol{c} \in K^{m\times 1}$, sa nazývajú *ekvivalentné*, ak majú rovnakú množinu riešení, t. j. ak pre všetky $\boldsymbol{x} \in K^n$ platí $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ práve vtedy, keď $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$.

Skôr než prikročíme k otázke riešenia sústav lineárnych rovníc, považujeme za potrebné upozorniť čitateľa na dve veci.

(a) Podčiarkujeme, že riešením sústavy rozumieme vždy *vektor* $\boldsymbol{x}$ a nie jeho zložky. Tak napríklad sústava

$$\begin{aligned} 2x + 3y &= 12 \\ 3x - 2y &= 5 \end{aligned}$$

nad poľom $\mathbb{R}$ má, ako ľahko nahliadneme, jediné riešenie $\binom{x}{y} = \binom{3}{2}$ a nie dve riešenia $x = 3$, $y = 2$. Keď si toto poriadne uvedomíme, môžeme (a samozrejme aj budeme) sa naďalej vyjadrovať obvyklým spôsobom. Budeme teda hovoriť, že sústava má *jediné* riešenie $x = 3$, $y = 2$.

(b) Všimnite si, že počet rovníc sústavy a počet neznámych sa nemusia rovnať. V obvyklom prípade, keď rovníc je rovnaký počet ako neznámych, očakávame, že sústava bude mať jediné riešenie. Keď je rovníc menej než neznámych, môžeme očakávať, že sústava bude mať viacero (prípadne i nekonečne mnoho) riešení. Naopak, keď je rovníc viac ako neznámych, môže sa stať, že sústava nebude mať nijaké riešenie. Napriek tomu, že tieto očakávania vyjadrujú niečo ako „prevládajúci trend“, ľahko možno nájsť príklady, keď sa nemusia splniť. Zatiaľ len poznamenajme, že homogénna sústava $\boldsymbol{A} \cdot \boldsymbol{x} = \mathbf{0}$ má (bez ohľadu na počet neznámych a počet rovníc) vždy aspoň jedno riešenie – je ním nulový vektor $\boldsymbol{x} = \mathbf{0}$.

Nie je dôležité, akými znakmi sú označené neznáme v sústave $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$. Na jej riešenie nemá nijaký vplyv, či si vektor neznámych označíme $\boldsymbol{x} = (x_1, \ldots, x_n)^T$ alebo $\boldsymbol{y} = (y_1, \ldots, y_n)^T$ alebo nejako inak. To znamená, že celá informácia o tejto sústave, potrebná na nájdenie všetkých jej riešení, je obsiahnutá v rozšírenej matici sústavy $(\boldsymbol{A} \,|\, \boldsymbol{b})$, prípadne, ak ide o homogénnu sústavu, len v matici sústavy $\boldsymbol{A}$. Preto i metóda riešenia sústav lineárnych rovníc, s ktorou sa teraz zoznámime, bude založená len na úprave tejto matice.

Stručne povedané, rozšírenú maticu $(\boldsymbol{A} \,|\, \boldsymbol{b})$ sústavy $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ budeme upravovať tak, aby sme dostali vhodnú maticu $(\boldsymbol{B} \,|\, \boldsymbol{c})$, zodpovedajúcu novej sústave $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$, ktorá spĺňa nasledujúce dve podmienky:

(a) Je ekvivalentná s pôvodnou sústavou $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$, t. j. má rovnakú množinu riešení.

(b) Všetky jej riešenia možno priamo vyčítať z jej rozšírenej matice $(\boldsymbol{B} \,|\, \boldsymbol{c})$.

V takom prípade hovoríme, že sústava $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$ je *vyriešená.*

3.2. Redukovaný stupňovitý tvar matice

Našou prvou úlohou teda bude vyjasniť si, ako by mala vyzerať matica $(\boldsymbol{B}\,|\,\boldsymbol{c})$, aby sme príslušnú sústavu $\boldsymbol{B}\cdot\boldsymbol{x}=\boldsymbol{c}$ mohli považovať za vyriešenú. Za tým účelom teraz zavedieme niekoľko pojmov.

Hovoríme, že prvok a_{ij} matice $\boldsymbol{A}\in K^{m\times n}$ je *vedúci prvok* i-teho riadku matice $\boldsymbol{A}$, ak $a_{ij}\neq 0$, a $j=1$ alebo $a_{il}=0$ pre všetky $1\leq l<j$. Inak povedané, vedúci prvok nenulového riadku je prvý nenulový prvok tohto riadku. Nulový riadok nemá vedúci prvok.

Hovoríme, že matica $\boldsymbol{A}=(a_{ij})\in K^{m\times n}$ je v *redukovanom stupňovitom tvare*, ak spĺňa nasledujúce štyri podmienky:

(a) Ak $\boldsymbol{r}_i(\boldsymbol{A})\neq\boldsymbol{0}$ a $\boldsymbol{r}_k(\boldsymbol{A})=\boldsymbol{0}$, tak $i<k$;
t. j. každý nenulový riadok matice $\boldsymbol{A}$ leží nad každým jej nulovým riadkom.

(b) Ak a_{ij}, a_{kl} sú vedúce prvky i-teho resp. k-teho riadku a $i<k$, tak aj $j<l$;
t. j. vedúci prvok vyššieho riadku leží viac vľavo než vedúci prvok nižšieho riadku.

(c) Ak a_{ij} je vedúci prvok i-teho riadku, tak $a_{ij}=1$;
t. j. vedúci prvok každého nenulového riadku je 1.

(d) Ak a_{ij} je vedúci prvok i-teho riadku, tak $a_{kj}=0$ pre každé $k\neq i$;
t. j. v stĺpci, v ktorom sa nachádza vedúci prvok nejakého riadku, sú všetky ostatné prvky rovné 0.

Pokiaľ matica $\boldsymbol{A}$ spĺňa len podmienky (a), (b), hovoríme, že je v *stupňovitom tvare*. Používa sa tiež názov (redukovaný) *schodovitý tvar*.

Napríklad z uvedených matíc nad poľom $\mathbb{R}$

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

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

ani jedna z matíc vľavo nie je v stupňovitom tvar; obe matice v strednom stĺpci sú v stupňovitom tvare, nie však v redukovanom stupňovitom tvare; konečne, obe matice vpravo sú v redukovanom stupňovitom tvare. (V každom jednotlivom prípade si podrobne premyslite prečo.)

Taktiež každá jednotková matica $\boldsymbol{I}_n$, ako aj všetky nulové matice $\mathbf{0}_{mn}$ sú v redukovanom stupňovitom tvare.

Uvedomme si teraz, akej sústave lineárnych rovníc zodpovedá rozšírená matica v redukovanom stupňovitom tvare. Napríklad

$$(\boldsymbol{B} \,|\, \boldsymbol{c}) = \left(\begin{array}{ccccc|c} 1 & 0 & -2 & 0 & 0 & 3 \\ 0 & 1 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right)$$

je matica v redukovanom stupňovitom tvare nad $\mathbb{R}$. Táto matica zodpovedá sústave

$$\begin{aligned} x_1 \quad\quad - 2x_3 \quad\quad &= 3 \\ x_2 + 6x_3 \quad\quad &= 0 \\ x_4 &= 1 \end{aligned}$$

v neznámych x_1, x_2, x_3, x_4, x_5. Hneď vidíme, že táto sústava má nekonečne mnoho riešení. Každej voľbe *parametrov* $s, t \in \mathbb{R}$ totiž zodpovedá jedno riešenie

$$\begin{aligned} x_1 &= 3 + 2s \\ x_2 &= \quad - 6s \\ x_3 &= \quad\quad s \\ x_4 &= 1 \\ x_5 &= \quad\quad\quad\quad t. \end{aligned}$$

Asi sa zhodneme na tom, že preznačenie neznámych za parametre $x_3 = s$, $x_5 = t$ a ich presun na pravú stranu, je úprava natoľko bezprostredná, že sústavu prislúchajúcu k matici $(\boldsymbol{B} \mid \boldsymbol{c})$ už možno považovať za vyriešenú. Na napísanie jej riešenia nemusíme písať príslušnú sústavu, môžeme ho napísať priamo na základe matice $(\boldsymbol{B} \mid \boldsymbol{c})$.

Dohodneme sa teda, že sústavu lineárnych rovníc $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$ nad poľom K budeme nazývať *vyriešenou sústavou*, ak jej rozšírená matica $(\boldsymbol{B} \mid \boldsymbol{c})$ je v redukovanom stupňovitom tvare. V prípade homogénnej sústavy sa, samozrejme, stačí obmedziť na maticu $\boldsymbol{B}$.

Teraz si predvedieme, ako možno k danej blokovej matici $(\boldsymbol{B} \mid \boldsymbol{c})$ v redukovanom stupňovitom tvare, nájsť všetky riešenia sústavy $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$.

Najprv si ujasníme, kedy je taká sústava *riešiteľná*, t. j. má aspoň jedno riešenie. Odpoveď na túto otázku je jednoduchá: Sústava $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$ má riešenie práve vtedy, keď sa v matici $(\boldsymbol{B} \mid \boldsymbol{c})$ nenachádza riadok tvaru

$$(\underbrace{0, \dots, 0}_{n\text{-krát}} \mid 1).$$

Taký riadok totiž zodpovedá rovnici $0 = 1$, ktorá očividne nemá riešenie. To, že neprítomnosť takého riadku je i postačujúcou podmienkou riešiteľnosti sústavy, vyplýva z nasledujúceho postupu, ako toto riešenie nájsť.

Ak sa v j-tom stĺpci matice $\boldsymbol{B}$ nenachádza vedúci prvok žiadneho riadku, tak si neznámu x_j zvolíme za parameter; ak sa v j-tom stĺpci nachádza vedúci prvok nejakého riadku, tak neznámu x_j si vyjadríme pomocou parametrov tak, že stĺpce matice $\boldsymbol{B}$ prislúchajúce týmto parametrom „prehodíme s opačným znamienkom na druhú stranu“.

Presnejšiu formuláciu celého postupu vo všeobecnej podobe si odpustíme. Názornejšie bude osvetliť ho na ešte jednom príklade.

$$(\boldsymbol{B} \mid \boldsymbol{c}) = \left(\begin{array}{ccccc|c} 1 & 0 & 0 & 2/3 & -1/2 & 5 \\ 0 & 1 & 0 & 3/4 & 0 & 2 \\ 0 & 0 & 1 & -4 & -2/5 & -2 \end{array}\right)$$

je reálna matica v redukovanom stupňovitom tvare. Vidíme, že sa v nej nenachádza riadok tvaru $(0, 0, 0, 0 \mid 1)$, teda sústava $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$ by mala mať riešenie. Vedúce prvky riadkov matice $\boldsymbol{B}$ sa nachádzajú v stĺpcoch 1, 2 a 3. Za parametre si teda zvolíme neznáme x_4 a x_5.

Riešením sústavy je každý vektor $(x_1, x_2, x_3, x_4, x_5)^T \in \mathbb{R}$ tvaru

$$\begin{aligned} x_1 &= 5 - \frac{2}{3}s + \frac{1}{2}t \\ x_2 &= 2 - \frac{3}{4}s \\ x_3 &= -2 + 4s + \frac{2}{5}t \\ x_4 &= s \\ x_5 &= \phantom{-2 + 4s + \frac{2}{5}}t, \end{aligned}$$

kde parametre $s, t \in \mathbb{R}$ môžu nadobúdať ľubovoľné hodnoty. Pre estétov ešte poznamenajme, že zlomkov pri parametroch sa možno jednoducho zbaviť. Je totiž jedno, či si parametrické premenné zvolíme v tvare $x_4 = s$, $x_5 = t$ alebo v tvare $x_4 = 12s$, $x_5 = 10t$, kde $s, t \in \mathbb{R}$. Pri takejto voľbe parametrov dostaneme všetky riešenia sústavy v tvare bez zlomkov

$$\begin{aligned} x_1 &= 5 - 8s + 5t \\ x_2 &= 2 - 9s \\ x_3 &= -2 + 36s + 4t \\ x_4 &= 12s \\ x_5 &= 10t. \end{aligned}$$

3.3. Elementárne riadkové a stĺpcové operácie (ERO a ESO)

Zatiaľ sme si ujasnili, na *aký tvar* treba upraviť rozšírenú maticu $(\boldsymbol{A} \,|\, \boldsymbol{b})$ sústavy $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$, aby sme získali s ňou ekvivalentnú *vyriešenú* sústavu $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$: rozšírená matica $(\boldsymbol{B} \,|\, \boldsymbol{c})$ novej sústavy musí byť v *redukovanom stupňovitom tvare*. Teraz si ukážeme, *ako* to možno urobiť. Maticu $(\boldsymbol{A} \,|\, \boldsymbol{b})$ budeme na redukovaný stupňovitý tvar upravovať pomocou tzv. elementárnych riadkových operácií.

Elementárnou riadkovou operáciou, skrátene tiež ERO, na matici $\boldsymbol{A} \in K^{m \times n}$ rozumieme

I. výmenu dvoch riadkov matice $\boldsymbol{A}$;

II. vynásobenie niektorého riadku matice $\boldsymbol{A}$ *nenulovým* skalárom z poľa K;

III. pripočítanie skalárneho násobku niektorého riadku matice $\boldsymbol{A}$ k jej inému riadku.

Matice $\boldsymbol{A}, \boldsymbol{B} \in K^{m \times n}$ sa nazývajú *riadkovo ekvivalentné*, označenie $\boldsymbol{A} \sim \boldsymbol{B}$, ak jednu z nich možno upraviť na druhú konečným počtom elementárnych riadkových operácií. Riešenie sústavy lineárnych rovníc úpravou jej rozšírenej matice pomocou ERO na riadkovo ekvivalentnú maticu v redukovanom stupňovitom tvare sa nazýva *Gaussova-Jordanova eliminácia*.

Prenechávame čitateľovi, aby si sám sformuloval analogické pojmy *elementárnych stĺpcových operácií* (ESO) a *stĺpcovej ekvivalencie* matíc, označenie $\boldsymbol{A} \wr \boldsymbol{B}$. Ich význam vyjde najavo až v neskorších kapitolách.

Výmenou i-teho a k-teho riadku v matici

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{r}_1(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_i(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_k(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_m(\boldsymbol{A}) \end{pmatrix} \qquad \text{dostaneme maticu} \qquad \begin{pmatrix} \boldsymbol{r}_1(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_k(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_i(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_m(\boldsymbol{A}) \end{pmatrix}.$$

Opätovnou výmenou i-teho a k-teho riadku v tejto matici získame zasa maticu $\boldsymbol{A}$.

Vynásobením i-teho riadku matice $\boldsymbol{A}$ skalárom $c \neq 0$ dostaneme maticu

$$\begin{pmatrix} \boldsymbol{r}_1(\boldsymbol{A}) \\ \vdots \\ c\boldsymbol{r}_i(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_k(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_m(\boldsymbol{A}) \end{pmatrix}.$$

Vynásobením i-teho riadku tejto matice skalárom $c^{-1} \neq 0$ získame opäť maticu $\boldsymbol{A}$.

Konečne, pripočítaním c-násobku i-teho riadku matice $\boldsymbol{A}$ k jej k-temu riadku z nej dostaneme maticu

$$\begin{pmatrix} \boldsymbol{r}_1(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_i(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_k(\boldsymbol{A}) + c\boldsymbol{r}_i(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_m(\boldsymbol{A}) \end{pmatrix}.$$

Všimnite si, že i-ty riadok pri tom zostáva nezmenený. Maticu $\boldsymbol{A}$ z tejto matice získame pripočítaním $(-c)$-násobku jej i-teho riadku ku k-temu riadku.

Ak $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ je sústava s rozšírenou maticou $(\boldsymbol{A} \mid \boldsymbol{b})$ a bloková matica $(\boldsymbol{A}' \mid \boldsymbol{b}')$ vznikne z $(\boldsymbol{A} \mid \boldsymbol{b})$ vykonaním jednej (nezáleží ktorej) ERO, tak sústava $\boldsymbol{A}' \cdot \boldsymbol{x} = \boldsymbol{b}'$ je ekvivalentná s pôvodnou sústavou $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$. Elementárne riadkové operácie na matici $(\boldsymbol{A} \mid \boldsymbol{b})$ totiž zodpovedajú postupne zámene poradia dvoch rovníc sústavy, vynásobením niektorej rovnice nenulovým skalárom a pripočítaním nejakého násobku jednej rovnice k inej rovnici (presnejšie nahradením dojice rovníc $\boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{x} = b_i$, $\boldsymbol{r}_k(\boldsymbol{A}) \cdot \boldsymbol{x} = b_k$ dvojicou rovníc $\boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{x} = b_i$, $(\boldsymbol{r}_k(\boldsymbol{A}) + c\boldsymbol{r}_i(\boldsymbol{A})) \cdot \boldsymbol{x} = b_k + cb_i$). Z pred chvíľou vykonaných úvah vyplýva, že ide o ekvivalentné úpravy, ktorými sa množina riešení sústavy nezmení – od novej sústavy $\boldsymbol{A}' \cdot \boldsymbol{x} = \boldsymbol{b}'$ sa možno vhodnou ERO vykonanou na jej rozšírenej matici opäť vrátiť k pôvodnej sústave $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$.

3.3.1. Tvrdenie. *Nech K je pole, $\boldsymbol{A}, \boldsymbol{B} \in K^{m\times n}$, $\boldsymbol{b}, \boldsymbol{c} \in K^m$. Ak sú blokové matice $(\boldsymbol{A} \mid \boldsymbol{b})$, $(\boldsymbol{B} \mid \boldsymbol{c})$ riadkovo ekvivalentné, tak i sústavy lineárnych rovníc $\boldsymbol{A}\cdot\boldsymbol{x} = \boldsymbol{b}$, $\boldsymbol{B}\cdot\boldsymbol{x} = \boldsymbol{c}$ sú ekvivalentné.*

Dôkaz. Podľa predpokladu existuje postupnosť blokových matíc $(\boldsymbol{A} \mid \boldsymbol{b}) = (\boldsymbol{C}_0 \mid \boldsymbol{d}_0)$, $(\boldsymbol{C}_1 \mid \boldsymbol{d}_1)$, $\dots, (\boldsymbol{C}_p \mid \boldsymbol{d}_p) = (\boldsymbol{B} \mid \boldsymbol{c})$ typu $m \times (n+1)$ takých, že pre každé $l < p$ matica $(\boldsymbol{C}_{l+1} \mid \boldsymbol{d}_{l+1})$ vznikne vykonaním jedinej ERO z matice $(\boldsymbol{C}_l \mid \boldsymbol{d}_l)$. Potom všetky sústavy $\boldsymbol{C}_l \cdot \boldsymbol{x} = \boldsymbol{d}_l$ majú tú istú množinu riešení, t. j. sú ekvivalentné.

3.3.2. Veta. *Každá matica nad poľom K je riadkovo ekvivalentná s jednoznačne určenou maticou v redukovanom stupňovitom tvare.*

Dôkaz existencie a jednoznačnosti spomínanej matice odložíme do cvičení 3.12 a 3.13 (pozri tiež cvičenie 5.13). Zatiaľ sa radšej len na konkrétnych príkladoch naučíme, ako možno k danej matici $\boldsymbol{A}$ nájsť s ňou riadkovo ekvivalentnú maticu v redukovanom stupňovitom tvare. Takýto prístup má navyše tú výhodu, že z radu možných postupov, medzi ktorými si možno pružne voliť podľa okolností, nám nesugeruje jedinú stratégiu, na jednu z ktorých by sme sa nevyhnutne museli obmedziť pri všeobecnom dôkaze. Ambicióznejší čitateľ v uvedených príkladoch ľahko i sám zahliadne myšlienku všeobecného dôkazu, ktorú potom bude môcť uplatniť v cvičení 3.12. Napokon, aby sme sa nebavili iba o maticiach, začneme zakaždým s nejakou sústavou lineárnych rovníc. Tým sa zároveň naučíme *riešiť* ľubovoľnú sústavu lineárnych rovníc nad daným poľom Gaussovou-Jordanovou elimináciou, prípadne rozpoznať, že daná sústava nemá riešenie.

3.3.3. Príklad. Je daná sústava

$$\begin{aligned} 2x_1 + 3x_2 \phantom{{}+4x_3} - x_4 &= 1 \\ 3x_1 + 2x_2 + 4x_3 - 2x_4 &= 0 \\ x_1 - x_2 + 4x_3 - x_4 &= 2 \end{aligned}$$

troch rovníc o štyroch neznámych nad poľom $\mathbb{R}$. Jej rozšírená matica je

$$\left(\begin{array}{cccc|c} 2 & 3 & 0 & -1 & 1 \\ 3 & 2 & 4 & -2 & 0 \\ 1 & -1 & 4 & -1 & 2 \end{array}\right).$$

Pri jej úprave na redukovaný stupňovitý tvar (podobne ako i v ďalších príkladoch) budeme vynechávať niektoré medzikroky a zaznamenáme len niektoré výsledky viacerých vykonaných ERO. Posledný riadok matice dáme na prvé miesto, potom jeho (-2)-násobok pripočítame k pôvodnému prvému riadku, ktorý posunieme na druhé miesto, a (-3)-násobok toho istého riadku pripočítame k pôvodnému druhému riadku, ktorý posunieme na tretie miesto. Dostaneme tak maticu

$$\left(\begin{array}{cccc|c} 1 & -1 & 4 & -1 & 2 \\ 0 & 5 & -8 & 1 & -3 \\ 0 & 5 & -8 & 1 & -6 \end{array}\right).$$

Pripočítaním (-1)-násobku druhého riadku k tretiemu dostaneme maticu

$$\left(\begin{array}{cccc|c} 1 & -1 & 4 & -1 & 2 \\ 0 & 5 & -8 & 1 & -3 \\ 0 & 0 & 0 & 0 & -3 \end{array}\right).$$

Už z tohto tvaru vidíme, že sústava zodpovedajúca poslednej matici nemá riešenie – obsahuje totiž rovnicu $0 = -3$. Teda ani pôvodná sústava (hoci neznámych je v nej viac než rovníc) nemá riešenie. Z cvičných dôvodov však dokončíme úpravu na redukovaný stupňovitý tvar, ktorý dostaneme vynásobením tretieho riadku skalárom $-1/3$, pripočítaním (-2)-násobku resp. 3-násobku tohto nového riadku k prvému resp. druhému riadku a, konečne, vynásobením druhého riadku skalárom $1/5$:

$$\left(\begin{array}{cccc|c} 1 & 0 & 12/5 & -4/5 & 0 \\ 0 & 1 & -8/5 & 1/5 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right).$$

Čitateľ by si mal všimnúť, že po nastavení vedúceho prvku niektorého riadku na hodnotu 1 okamžite pristupujeme k nulovaniu zvyšných prvkov stĺpca, v ktorom leží tento vedúci prvok.

3.3.4. Príklad. Riešme sústavu

$$\begin{aligned} x + \quad 2\mathrm{i}y \qquad\qquad &= 5 + 4\mathrm{i} \\ (3 - \mathrm{i})y + (6 - 2\mathrm{i})z &= 10 \\ 2x \qquad\qquad - \qquad z &= 5 + 3\mathrm{i} \\ x + \qquad y + \qquad z &= 5 + 2\mathrm{i} \end{aligned}$$

štyroch rovníc o troch neznámych nad poľom $\mathbb{C}$. Jej rozšírená matica je

$$\left(\begin{array}{ccc|c} 1 & 2\mathrm{i} & 0 & 5+4\mathrm{i} \\ 0 & 3-\mathrm{i} & 6-2\mathrm{i} & 10 \\ 2 & 0 & -1 & 5+3\mathrm{i} \\ 1 & 1 & 1 & 5+2\mathrm{i} \end{array}\right).$$

Prehoďme jej posledný riadok na prvé miesto a zvyšné riadky posuňme o jedno miesto nadol. V takto získanej matici pripočítajme (-1)-násobok prvého riadku k druhému riadku a (-2)-násobok prvého riadku k štvrtému riadku. Konečne vynásobme tretí riadok skalárom $(3+\mathrm{i})/10$. Dostaneme maticu

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 5+2\mathrm{i} \\ 0 & -1+2\mathrm{i} & -1 & 2\mathrm{i} \\ 0 & 1 & 2 & 3+\mathrm{i} \\ 0 & -2 & -3 & -5-\mathrm{i} \end{array}\right).$$

(-1)-násobok tretieho riadku pripočítame k prvému riadku, jeho $(1-2\mathrm{i})$-násobok k druhému a 2-násobok k štvrtému. Nakoniec výmenou druhého a tretieho riadku dostaneme maticu

$$\left(\begin{array}{ccc|c} 1 & 0 & -1 & 2+\mathrm{i} \\ 0 & 1 & 2 & 3+\mathrm{i} \\ 0 & 0 & 1-4\mathrm{i} & 5-3\mathrm{i} \\ 0 & 0 & 1 & 1+\mathrm{i} \end{array}\right).$$

Pripočítajme posledný riadok k prvému, (-2)-násobok posledného riadku k druhému a jeho $(-1+4\mathrm{i})$-násobok k tretiemu. Zostáva vymeniť tretí a štvrtý riadok – výsledná matica je už v redukovanom stupňovitom tvare

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 3+2\mathrm{i} \\ 0 & 1 & 0 & 1-\mathrm{i} \\ 0 & 0 & 1 & 1+\mathrm{i} \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Vidíme, že pôvodná sústava (hoci obsahuje viac rovníc než neznámych) má jediné riešenie $x = 3+2\mathrm{i}$, $y = 1-\mathrm{i}$, $z = 1+\mathrm{i}$, teda presnejšie vektor $(3+2\mathrm{i}, 1-\mathrm{i}, 1+\mathrm{i})^T \in \mathbb{C}^3$.

3.3.5. Príklad. Uvažujme sústavu

$$\begin{aligned} x_1 + x_2 + 2x_3 + 3x_4 &= 0 \\ 2x_1 \phantom{{}+2x_2} + 4x_3 \phantom{{}+3x_4} &= 0 \\ x_1 + 2x_2 + x_3 + 3x_4 &= 0 \\ 3x_3 + 4x_4 &= 0 \end{aligned}$$

štyroch rovníc o štyroch neznámych nad poľom $\mathbb{Z}_5$. Keďže ide o homogénnu sústavu (ktorej ľavá strana je nulový stĺpcový vektor, teda sa nemení pri žiadnej ERO), stačí upravovať jej (nerozšírenú) maticu

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

(-2)-násobok, t. j. 3-násobok prvého riadku pripočítame k druhému riadku a jeho (-1)-násobok, t. j. 4-násobok pripočítame k tretiemu riadku. Dostaneme tak maticu

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

(-1)-násobok, t. j. 4-násobok tretieho riadku pripočítame k prvému riadku a jeho (-3)-násobok, t. j. 2-násobok pripočítame k druhému riadku. Konečne výmenou druhého a tretieho riadku dostaneme maticu

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

Tretí riadok odpočítame od prvého aj od štvrtého riadku. Ďalej ho vynásobíme skalárom $3^{-1} = 2$. Napokon jeho (-4)-násobok, t. j. priamo tento nový tretí riadok pripočítame k druhému riadku. Výsledná matica je už v redukovanom stupňovitom tvare

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

Premennú x_4 si zvolíme za parameter. Všetky riešenia sústavy majú potom tvar $x_1 = t$, $x_2 = 2t$, $x_3 = 2t$, $x_4 = t$, kde $t \in \mathbb{Z}_5$. Vidíme teda, že pôvodná sústava (hoci počet jej rovníc je rovnaký ako počet neznámych) má viac než jedno riešenie; nie je ich však nekonečne veľa ale len 5. Práve toľko je totiž možných volieb parametra t, t. j. prvkov poľa $\mathbb{Z}_5$.

Zaznamenajme ešte jeden očakávaný dôsledok tvrdenia 3.3.1., vety 3.3.2. a spôsobu, ako napísať riešenie sústavy s (rozšírenou) maticou v redukovanom stupňovitom tvare, uvedeného v paragrafe 3.2.

3.3.6. Tvrdenie. *Nech $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{b} \in K^m$ a $m < n$, t. j. sústavy $\boldsymbol{A}\cdot\boldsymbol{x} = \mathbf{0}$, $\boldsymbol{A}\cdot\boldsymbol{x} = \boldsymbol{b}$ obsahujú menej rovníc než neznámych. Potom*

(a) *homogénna sústava $\boldsymbol{A}\cdot\boldsymbol{x} = \mathbf{0}$ má popri riešení $\boldsymbol{x}_0 = \mathbf{0}$ aspoň jedno riešenie $\boldsymbol{x} \neq \mathbf{0}$;*

(b) *ak existuje aspoň jedno riešenie sústavy $\boldsymbol{A}\cdot\boldsymbol{x} = \boldsymbol{b}$, tak táto sústava má viac než jedno riešenie.*

Dôkaz. (a) Upravme maticu sústavy $\boldsymbol{A}$ na redukovaný stupňovitý tvar $\boldsymbol{B}$. Uvedomme si, že matice $\boldsymbol{A}$ aj $\boldsymbol{B}$ majú m riadkov a n stĺpcov. Riadky matice $\boldsymbol{B}$ majú nanajvýš m vedúcich prvkov. Keďže $m < n$, aspoň v jednom stĺpci matice $\boldsymbol{B}$ neleží vedúci prvok žiadneho riadku. Nech je to napr. j-ty stĺpec. Potom voľbe parametra $x_j = t \in K$, $t \neq 0$ zodpovedá aspoň jedno nenulové riešenie sústavy $\boldsymbol{A}\cdot\boldsymbol{x} = \mathbf{0}$.

(b) prenechávame ako cvičenie čitateľovi.

3.4. Gaussova eliminačná metóda

Hlavne z historických dôvodov ešte stručne spomenieme metódu riešenia sústav lineárnych rovníc tzv. *Gaussovou elimináciou*. Pri riešení touto metódou upravíme rozšírenú maticu sústavy len na stupňovitý (teda nie nevyhnutne redukovaný stupňovitý) tvar. Už z tohto tvaru možno ľahko spoznať, či sústava má nejaké riešenie (príslušná matica nesmie obsahovať riadok tvaru $(0,\dots,0\,|\,d)$, kde $0 \neq d \in K$). V tom prípade možno všetky riešenia sústavy získať voľbou parametrov (opäť si za ne volíme neznáme x_j také, že j-tom stĺpci sa nevyskytuje vedúci prvok žiadneho riadku) a spätným dosadzovaním, t. j. *elimináciou* neznámych pomocou parametrov.

3.4.1. Príklad. Predpokladajme, že rozšírenú maticu nejakej sústavy nad $\mathbb{R}$ sme už pomocou ERO upravili na stupňovitý tvar

$$\left(\begin{array}{cccccc|c} 0 & 2 & 3 & 0 & -1 & 4 & 1 \\ 0 & 0 & 0 & -2 & 5 & 4 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 4 \end{array}\right).$$

Táto matica zodpovedá sústave

$$\begin{aligned} 2x_2 + 3x_3 \qquad\quad - x_5 + 4x_6 &= 1 \\ - 2x_4 + 5x_5 + 4x_6 &= 0 \\ 3x_5 + x_6 &= 4. \end{aligned}$$

Za parametre si zvolíme premenné x_1, x_3 a x_6. Spätným dosadzovaním postupne dostaneme všetky riešenia v parametrickom tvare

$$\begin{aligned}
x_6 &= t\\
x_5 &= \frac{1}{3}(4 - x_6) = \frac{4}{3} - \frac{1}{3}t\\
x_4 &= \frac{1}{2}(5x_5 + 4x_6) = \frac{10}{3} - \frac{7}{6}t\\
x_3 &= s\\
x_2 &= \frac{1}{2}(1 - 3x_3 + x_5 - 4x_6) = \frac{7}{6} - \frac{3}{2}s - \frac{13}{6}t\\
x_1 &= r,
\end{aligned}$$

kde $r, s, t \in \mathbb{R}$. Prípadne, po trochu „šikovnejšej" voľbe parametrov, v tvare $x_6 = 6t$, $x_5 = \frac{4}{3} - 2t$, $x_4 = \frac{10}{3} - 7t$, $x_3 = 2s$, $x_2 = \frac{7}{6} - 3s + 13t$, $x_1 = r$.

Pozorný čitateľ si iste všimol, že spätné dosadzovanie možno nahradiť ďalšou úpravou rozšírenej matice sústavy pomocou ERO na *redukovaný* stupňovitý tvar. Stačí totiž vynásobiť nenulové riadky prevrátenými hodnotami ich vedúcich prvkov a pripočítaním vhodných násobkov týchto riadkov vynulovať zvyšné nenulové prvky v stĺpcoch obsahujúcich vedúce prvky jednotlivých riadkov.

I tak však môže byť Gaussova eliminačná metóda v niektorých prípadoch užitočná – najmä keď nám nejde ani tak o explicitný tvar riešení, ako skôr o samotnú otázku riešiteľnosti sústavy, prípadne o počet parametrov, ktoré sa v nich vyskytujú. Všetko to možno totiž spoznať už na základe nejakej matice v stupňovitom tvare, riadkovo ekvivalentnej s pôvodnou rozšírenou maticou sústavy. V takom prípade si teda môžeme odpustiť nielen ďalšiu úpravu na redukovaný stupňovitý tvar, ale aj spätné dosadzovanie.

Cvičenia

3.1. Podrobne prepočítajte sústavy lineárnych rovníc z príkladov 3.3.3.– 3.3.5.

3.2. Gaussovou-Jordanovou elimináciou riešte sústavu lineárnych rovníc $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}$ nad poľom $\mathbb{R}$ pre matice:

(a) $\boldsymbol{A}=\begin{pmatrix}2&1&2&0&-6\\1&0&0&2&-5\\1&1&2&0&-3\\0&1&2&0&1\end{pmatrix}$, $\boldsymbol{b}=\begin{pmatrix}4\\1\\1\\2\end{pmatrix}$; (b) $\boldsymbol{A}=\begin{pmatrix}3&-6&1&10\\1&-2&1&4\\2&-4&3&9\\1&-2&0&3\end{pmatrix}$, $\boldsymbol{b}=\begin{pmatrix}6\\3\\2\\2\end{pmatrix}$.

3.3. Gaussovou-Jordanovou elimináciou riešte sústavu lineárnych rovníc $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}$ nad poľom $\mathbb{C}$ pre matice:
(a) $\boldsymbol{A}=\begin{pmatrix}1+\mathrm{i}&0&\mathrm{i}-1\\2-\mathrm{i}&1&1+\mathrm{i}\end{pmatrix}$, $\boldsymbol{b}=\begin{pmatrix}1-2\mathrm{i}\\0\end{pmatrix}$; (b) $\boldsymbol{A}=\begin{pmatrix}1+2\mathrm{i}&2-\mathrm{i}&1-\mathrm{i}\\5\mathrm{i}&5&3-\mathrm{i}\end{pmatrix}$, $\boldsymbol{b}=\begin{pmatrix}1\\2+\mathrm{i}\end{pmatrix}$.

3.4. Gaussovou-Jordanovou elimináciou riešte sústavu $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}$ lineárnych rovníc nad poľom $\mathbb{Z}_{11}$ pre matice:
(a) $\boldsymbol{A}=\begin{pmatrix}1&2&3&4\\2&3&1&1\\7&3&5&3\end{pmatrix}$, $\boldsymbol{b}=\begin{pmatrix}1\\5\\1\end{pmatrix}$; (b) $\boldsymbol{A}=\begin{pmatrix}1&1&4&5\\3&2&0&1\\1&9&1&7\end{pmatrix}$, $\boldsymbol{b}=\boldsymbol{0}$.
Pre každú sústavu určte počet jej riešení.

3.5. Riešte sústavy z cvičenia 4 nad poľom $\mathbb{Z}_{13}$ a opäť určte počet riešení každej z nich.

3.6. V paragrafe 3.2 definovaný (redukovaný) stupňovitý tvar matice by sme mohli presnejšie nazvať *riadkovým* (redukovaným) stupňovitým tvarom. Sformulujte definíciu *stĺpcového* (redukovaného) stupňovitého tvaru matice. Podrobne definujte elementárne stĺpcové operácie (ESO) typov I, II a III.

3.7. Nech $\boldsymbol{A}=(a_{ij})_{m\times n}$, $\boldsymbol{B}=(\boldsymbol{b}_{ik})_{m\times p}$ sú matice nad poľom K. Označme $\boldsymbol{b}_k=\boldsymbol{s}_k(\boldsymbol{B})$ k-ty stĺpec matice $\boldsymbol{B}$. Uvažujme maticovú rovnicu $\boldsymbol{A}\cdot\boldsymbol{X}=\boldsymbol{B}$ s neznámou maticou $\boldsymbol{X}=(x_{jk})_{n\times p}$. Dokážte postupne nasledujúce tvrdenia:
(a) Matica $\boldsymbol{X}\in K^{n\times p}$ je riešením maticovej rovnice $\boldsymbol{A}\cdot\boldsymbol{X}=\boldsymbol{B}$ práve vtedy, keď pre každé $k\le p$ je jej k-ty stĺpec $\boldsymbol{x}_k=\boldsymbol{s}_k(\boldsymbol{X})$ riešením sústavy $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}_k$.
(b) Maticová rovnica $\boldsymbol{A}\cdot\boldsymbol{X}=\boldsymbol{B}$ má riešenie práve vtedy, keď každá zo sústav $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}_k$ $(k=1,\dots,p)$ má riešenie.
Na základe (a) a (b) navrhnite metódu, ako možno úpravou vhodnej blokovej matice pomocou ERO riešiť naraz viacero sústav $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}_k$ s rovnakou ľavou stranou a rôznymi pravými stranami $\boldsymbol{b}_1,\dots,\boldsymbol{b}_p$.

3.8. Nech $\boldsymbol{A} = (a_{ij})_{m\times n}$, $\boldsymbol{C} = (c_{kj})_{q\times n}$ sú matice nad poľom K. S hromadným riešením akých sústav lineárnych rovníc súvisí riešenie maticovej rovnice $\boldsymbol{Y}\cdot\boldsymbol{A} = \boldsymbol{C}$ s neznámou maticou $\boldsymbol{Y} = (y_{ki})_{q\times m}$? Navrhnite metódu založenú na úprave vhodnej blokovej matice pomocou ESO. Ako sa možno vyhnúť ESO a nahradiť ich ERO?

3.9. Riešte maticové rovnice $\boldsymbol{A}\cdot\boldsymbol{X} = \boldsymbol{B}$ a $\boldsymbol{Y}\cdot\boldsymbol{A} = \boldsymbol{C}$ pre matice $\boldsymbol{A} = \left(\begin{smallmatrix} 3 & 2 & 4 \\ 2 & 1 & 3 \end{smallmatrix}\right)$, $\boldsymbol{B} = \left(\begin{smallmatrix} 1 & 3 & -1 \\ 1 & 2 & 4 \end{smallmatrix}\right)$, $\boldsymbol{C} = \left(\begin{smallmatrix} 12 & 7 & 17 \\ 3 & 3 & 7 \end{smallmatrix}\right)$ nad poľom $\mathbb{Q}$. Určte najprv rozmery matíc $\boldsymbol{X}$ a $\boldsymbol{Y}$. Aké sústavy lineárnych rovníc ste takto vyriešili? Napíšte riešenie každej z nich (ak existuje).

3.10. Nad poľom $\mathbb{R}$ riešte sústavy lineárnych rovníc v neznámych x, y, z a urobte diskusiu počtu riešení vzhľadom na parametre $a \in \mathbb{R}$ resp. $c, d \in \mathbb{R}$:

(a)
$$\begin{aligned} x + y + (2a^2-1)z &= a^2+a+1, \\ x + y + (a^2+a-1)z &= 1, \\ x + a^2 z &= a^2 + a; \end{aligned}$$

(b)
$$\begin{aligned} cx + y + (c+1)dz &= c+2d+1, \\ cx + cdz &= d+1, \\ cy + 2cdz &= 2c^2+cd-1. \end{aligned}$$

3.11. Nech K je pole a $m, n \in \mathbb{N}$. Dokážte, že vzťah $\boldsymbol{A} \sim \boldsymbol{B}$ riadkovej ekvivalencie na množine $K^{m\times n}$ spĺňa podmienky $\boldsymbol{A} \sim \boldsymbol{A}$, $\boldsymbol{A} \sim \boldsymbol{B} \Rightarrow \boldsymbol{B} \sim \boldsymbol{A}$ a $\boldsymbol{A} \sim \boldsymbol{B}$ & $\boldsymbol{B} \sim \boldsymbol{C} \Rightarrow \boldsymbol{A} \sim \boldsymbol{C}$ pre ľubovoľné $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in K^{m\times n}$. Inak povedané, tento vzťah je reflexívny, symetrický a tranzitívny, teda je naozaj reláciou ekvivalencie na množine $\boldsymbol{K}^{m\times n}$ (pozri paragraf 0.6). Sformulujte analogický výsledok pre vzťah stĺpcovej ekvivalencie $\boldsymbol{A} \wr \boldsymbol{B}$.

3.12. Dokážte vetu 3.3.2. matematickou indukciou podľa počtu riadkov matice. (*Návod*: Ukážte, že matica s jediným riadkom je riadkovo ekvivalentná s maticou v redukovanom stupňovitom tvare. Predpokladajte, že matica $\boldsymbol{A}$ vznikla z matice v redukovanom stupňovitom tvare pridaním jedného riadku. Ukážte, že aj $\boldsymbol{A}$ je riadkovo ekvivalentná s maticou v redukovanom stupňovitom tvare.)

3.13. Dokážte jednoznačnosť redukovaného stupňovitého tvaru matice. Presnejšie, dokážte, že pre matice $\boldsymbol{A}, \boldsymbol{B} \in K^{m\times n}$ v redukovanom stupňovitom tvare platí $\boldsymbol{A} \sim \boldsymbol{B} \Rightarrow \boldsymbol{A} = \boldsymbol{B}$. (*Návod*: Ak $\boldsymbol{A}$, $\boldsymbol{B}$ sú v redukovanom stupňovitom tvare a $\boldsymbol{A} \neq \boldsymbol{B}$, ukážte, že homogénne sústavy lineárnych rovníc nemajú rovnaké riešenia; to je však spor s $\boldsymbol{A} \sim \boldsymbol{B}$.)

3.14. Dokážte zosilnenie tvrdenia 3.3.1. do podoby ekvivalencie, t. j. pre ľubovoľné $\boldsymbol{A}$, $\boldsymbol{B} \in K^{m\times n}$, $\boldsymbol{b}, \boldsymbol{c} \in K^m$ platí: sústavy $\boldsymbol{A}\cdot\boldsymbol{x} = \boldsymbol{b}$ a $\boldsymbol{B}\cdot\boldsymbol{x} = \boldsymbol{c}$ sú ekvivalentné práve vtedy, keď $(\boldsymbol{A}\,|\,\boldsymbol{b}) \sim (\boldsymbol{B}\,|\,\boldsymbol{c})$. (*Návod*: Modifikujte myšlienku z predchádzajúceho cvičenia na nehomogénne sústavy.)

3.15. Dokážte tvrdenie 3.3.6.(b).

4. Lineárne podpriestory a lineárna nezávislosť

V tejto kapitole sa opäť vrátime k štúdiu abstraktných vektorových priestorov nad všeobecným poľom. K bude v celej kapitole označovať nejaké pevné, inak ľubovoľné pole a V bude nejaký pevne zvolený vektorový priestor nad K. Čitateľ sa však nedopustí nijakej chyby, ak si pod všeobecným poľom K bude predstavovať pole $\mathbb{R}$ všetkých reálnych čísel. Zakaždým, keď sa budeme odvolávať na geometrický názor, bude to dokonca užitočné. Na druhej strane by však nemal spúšťať zo zreteľa, že naše úvahy majú podstatne širšiu platnosť – okrem vektorových priestorov nad $\mathbb{R}$ sa z nám známych príkladov vzťahujú tak na vektorové priestory nad poľom $\mathbb{C}$ všetkých komplexných čísel, poľom $\mathbb{Q}$ všetkých racionálnych čísel ako i na vektorové priestory nad konečnými poľami $\mathbb{Z}_p$.

4.1. Lineárne podpriestory vektorového priestoru

Množina $S \subseteq V$ sa nazýva *lineárny podpriestor* vektorového priestoru V, ak $S \neq \emptyset$ a pre všetky skaláry $a \in K$ a vektory $\boldsymbol{x}, \boldsymbol{y} \in S$ platí $a\boldsymbol{x} \in S$ a $\boldsymbol{x} + \boldsymbol{y} \in S$. Inak povedané, neprázdna podmnožina $S \subseteq V$ je lineárny podpriestor práve vtedy, keď je uzavretá na operácie skalárneho násobku a súčtu vektorov.

Nasledujúce tvrdenie je bezprostredným dôsledkom práve vyslovenej definície.

4.1.1. Tvrdenie. *Nech S je lineárny podpriestor vektorového priestoru V. Potom $\mathbf{0} \in S$*

a S s operáciami súčtu vektorov a skalárneho násobku zúženými z V na S tvorí vektorový priestor nad poľom K.

V každom vektorovom priestore V sú $\{\mathbf{0}\}$ a V lineárne podpriestory (v prípade, keď $V = \{\mathbf{0}\}$, dokonca splývajú, inak ide o dva rôzne podpriestory) – $\{\mathbf{0}\}$ nazývame *triválny* alebo tiež *nulovýa* V *nevlastný* alebo tiež *plnýlineárny* podpriestor. Teda pre *vlastný netriviálny* lineárny podpriestor $S \subseteq V$ platí $\{\mathbf{0}\} \neq S \neq V$.

Napr. vo vektorovom priestore $\mathbb{R}^3$ netriviálne vlastné podpriestory sú práve všetky priamky a roviny prechádzajúce počiatkom $\mathbf{0}$.

Nasledujúce tvrdenie charakterizuje lineárne podpriestory ako množiny uzavreté na lineárne kombinácie.

4.1.2. Tvrdenie. *Pre ľubovoľnú podmnožinu S vektorového priestoru V nasledujúce podmienky sú ekvivalentné:*

(i) S je lineárny podpriestor vo V;

(ii) $S \neq \emptyset$ a pre všetky skaláry $a, b \in K$ a vektory $\boldsymbol{x}, \boldsymbol{y} \in S$ platí $a\boldsymbol{x} + b\boldsymbol{y} \in S$;

(iii) pre každé $n \in \mathbb{N}$ a pre všetky skaláry $a_1, \ldots, a_n \in K$ a vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in S$ platí $a_1\boldsymbol{x}_1 + \ldots + a_n\boldsymbol{x}_n \in S$.

Dôkaz. Postupne dokážeme implikácie (i) ⇒ (ii), (ii) ⇒ (iii) a (iii) ⇒ (i).

(i) ⇒ (ii): Ak S je lineárny podpriestor, tak $S \neq \emptyset$. Nech $a, b \in K$, $\boldsymbol{x}, \boldsymbol{y} \in S$. Keďže S je uzavreté na skalárne násobky, platí $a\boldsymbol{x}, b\boldsymbol{y} \in S$. Z uzavretosti S na súčet vyplýva $a\boldsymbol{x} + b\boldsymbol{y} \in S$.

(ii) ⇒ (iii): Nech platí (ii). Keďže $S \neq \emptyset$, existuje $\boldsymbol{s} \in S$. Potom $\mathbf{0} = 0\boldsymbol{s} + 0\boldsymbol{s} \in S$ a tiež $a\boldsymbol{x} = a\boldsymbol{x} + 0\boldsymbol{s} \in S$ pre každé $a \in K$, $\boldsymbol{x} \in S$. Teda podmienka z (iii) je splnená pre

$n = 0$ (lebo prázdna lineárna kombinácia je $\mathbf{0}$) a $n = 1$; podľa (ii) je splnená tiež pre $n = 2$. Keby nebola splnená pre všetky $n \in \mathbb{N}$, označíme n najmenšie prirodzené číslo s touto vlastnosťou. Potom $n > 2$ a pre všetky $k < n$ podmienka z (iii) platí. Nech $a_1, \dots, a_n \in K$, $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n \in S$ sú také, že $a_1\boldsymbol{x}_1 + \dots + a_n\boldsymbol{x}_n \notin S$. Avšak

$$a_1\boldsymbol{x}_1 + \dots + a_n\boldsymbol{x}_n = (a_1\boldsymbol{x}_1 + \dots + a_{n-1}\boldsymbol{x}_{n-1}) + a_n\boldsymbol{x}_n \in S,$$

keďže pre prirodzené čísla $n - 1$ a 2 podmienka z (iii) platí. To je spor.

(iii) $\Rightarrow$ (i): Z platnosti (iii) pre $n = 0$ vyplýva, že $\mathbf{0} \in S$ (prázdna lineárna kombinácia je totiž $\mathbf{0}$). Teda $S \neq \emptyset$. Voľbou $n = 1$ dostávame uzavretosť S na skalárne násobky. Uzavretosť S na súčet vyplýva z voľby $n = 2$, $a_1 = a_2 = 1$.

4.1.3. Príklad. Keďže s príkladmi lineárnych podpriestorov vektorových priestorov K^n sa ešte stretneme pri mnohých príležitostiach, uvedieme tu niekoľko „exotickejších“ príkladov. Napospol pôjde o podpriestory priestorov K^X všetkých funkcií z nejakej množiny X do poľa K (pozri príklad 1.6.5).

(a) Označme $K^{(X)}$ množinu všetkých funkcií $f : X \to K$ takých, že množina $\{x \in X;\ f(x) \neq 0\}$ je konečná. Pre ľubovoľnú lineárnu kombináciu funkcií $f, g \in K^{(X)}$ platí

$$\{x \in X;\ af(x) + bg(x) \neq 0\} \subseteq \{x \in X;\ f(x) \neq 0\} \cup \{x \in X;\ g(x) \neq 0\}.$$

Z toho vyplýva, že $K^{(X)}$ je lineárny podpriestor vektorového priestoru K^X. Ak X je konečná, tak $K^{(X)} = K^X$; ak X je nekonečná, tak $K^{(X)}$ je netriválny vlastný podpriestor v K^X.

(b) Nech $X \subseteq \mathbb{R}$ je ľubovoľná množina reálnych čísel. Potom $\mathcal{C}(X, \mathbb{R})$, alebo len stručne $\mathcal{C}(X)$ označuje množinu všetkých spojitých funkcií $f : X \to \mathbb{R}$. Keďže lineárne kombinácie spojitých funkcií sú zrejme opäť spojité fumkcie, $\mathcal{C}(X)$ je lineárny podpriestor v $\mathbb{R}^X$.
(c) Ak X je nejaký (ohraničený alebo neohraničený) interval reálnych čísel, tak $\mathcal{D}(X)$ označuje množinu všetkých funkcií $f : X \to \mathbb{R}$, ktoré majú v každom bode $x \in X$ konečnú deriváciu (v prípadných krajných bodoch intervalu X sa žiada existencia konečnej derivácie zľava alebo sprava). Keďže každá diferencovateľná funkcia je spojitá na svojom definičnom obore a lineárna kombinácia diferencovateľných funkcií je opäť diferencovateľná, $\mathcal{D}(X)$ je lineárny podpriestor vektorového priestoru $\mathcal{C}(X)$.

4.2. Lineárny obal množiny vektorov

Množinu všetkých lineárnych kombinácií vektorov z podmnožiny X vektorového priestoru V nazývame *lineárnym obalom* množiny X a označujeme ju $[X]$. Teda

$$[X] = \{a_1\boldsymbol{x}_1 + \ldots + a_n\boldsymbol{x}_n;\ n \in \mathbb{N}\ \&\ a_1, \ldots, a_n \in K\ \&\ \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in X\}.$$

Ak $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}$ je konečná množina, tak miesto $[\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\}]$ píšeme len $[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$. Zrejme tento zápis má zmysel aj pre ľubovoľnú usporiadanú n-ticu (nie nutne rôznych) vektorov $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$, a platí

$$[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n] = \{a_1\boldsymbol{x}_1 + \ldots + a_n\boldsymbol{x}_n;\ a_1, \ldots, a_n \in K\}.$$

4.2.1. Tvrdenie. *Nech X je podmnožina vektorového priestoru V. Potom lineárny obal $[X]$ množiny X je najmenší lineárny podpriestor vektorového priestoru V taký, že $X \subseteq [X]$.*

Dôkaz. Musíme dokázať dve veci:
(a) $[X]$ je lineárny podpriestor vo V;
(b) pre každý lineárny podpriestor $S \subseteq V$ platí $X \subseteq S \Rightarrow [X] \subseteq S$.

(a) Zrejme $[X]$ obsahuje $\mathbf{0}$ ako prázdnu lineárnu kombináciu, teda $[X] \neq \emptyset$. Nech $c, d \in K$ a $\boldsymbol{u} = a_1\boldsymbol{x}_1 + \ldots + a_n\boldsymbol{x}_n$, $\boldsymbol{v} = b_1\boldsymbol{y}_1 + \ldots + b_m\boldsymbol{y}_m$ sú prvky z $[X]$, pričom $a_i, b_j \in K$, $\boldsymbol{x}_i, \boldsymbol{y}_j \in X$. Potom

$$c\boldsymbol{u} + d\boldsymbol{v} = ca_1\boldsymbol{x}_1 + \ldots + ca_n\boldsymbol{x}_n + db_1\boldsymbol{y}_1 + \ldots + db_m\boldsymbol{y}_m \in [X],$$

keďže je to opäť lineárna kombinácia vektorov z X. Podľa podmienky (ii) tvrdenia 4.1.2. je $[X]$ lineárny podpriestor vo V.

(b) Nech $S \subseteq V$ je lineárny podpriestor taký, že $X \subseteq S$. Potom podľa podmienky (iii) tvrdenia 4.1.2. všetky lineárne kombinácie vektorov z S, a tým skôr vektorov z X, patria do S. Teda $[X] \subseteq S$.

Dokázané tvrdenie nás oprávňuje nazývať lineárny obal $[X]$ množiny $X \subseteq V$ tiež lineárnym podpriestorom *generovaným* množinou X. Ak $[X] = S$, hovoríme, že X *generuje* lineárny podpriestor S, prípadne že X je *generujúca množina* alebo tiež *množina generátorov* lineárneho podpriestoru $S \subseteq V$. Ak $S = V$, t. j. ak $[X] = V$, hovoríme krátko o *generujúcej množine*. Používa sa tiež názov *vytvárajúca množina*.

Kvôli prehľadnosti ešte zhrnieme základné vlastnosti operácie lineárneho obalu $X \mapsto [X]$.

4.2.2. Tvrdenie. *Pre ľubovoľné podmnožiny X, Y vektorového priestoru V a $\boldsymbol{v} \in V$ platí:*
(a) $[\emptyset] = [\mathbf{0}] = \{\mathbf{0}\}$;
(b) $X \subseteq [X]$;
(c) $X \subseteq Y \Rightarrow [X] \subseteq [Y]$;
(d) *X je lineárny podpriestor vo V práve vtedy, keď $X = [X]$;*
(e) $[[X]] = [X]$;
(f) $\boldsymbol{v} \in [X] \Leftrightarrow [X \cup \{\boldsymbol{v}\}] = [X]$.

Dôkaz. (a), (b) a (c) sú triviálne, (d) priamo vyplýva z tvrdenia 4.2.1. a (e) je bezprostredným dôsledkom (d).

(f) Nech $\boldsymbol{v} \in [X]$. S použitím (b), (c) a (e) dostávame

$$[X \cup \{\boldsymbol{v}\}] \subseteq [[X] \cup \{\boldsymbol{v}\}] = [[X]] = [X].$$

Teda $[X \cup \{\boldsymbol{v}\}] = [X]$. Keďže $\boldsymbol{v} \in [X \cup \{\boldsymbol{v}\}]$, obrátená implikácia je triviálna.

4.3. Prienik a súčet lineárnych podpriestorov

Nech X, Y sú ľubovoľné podmnožiny vektorového priestoru V. Potom množinu

$$X + Y = \{\boldsymbol{x} + \boldsymbol{y};\ \boldsymbol{x} \in X \ \&\ \boldsymbol{y} \in Y\}$$

nazývame *súčtom* množín X, Y.

4.3.1. Tvrdenie. *Nech S, T sú lineárne podpriestory vektorového priestoru V. Potom aj $S \cap T$ a $S+T$ sú lineárne podpriestory vo V. Navyše platí*

$$S + T = [S \cup T],$$

t. j. $S+T$ je najmenší lineárny podpriestor vo V, ktorý obsahuje S aj T.

Dôkaz. Zrejme $\mathbf{0} \in S \cap T$. Z toho, že S aj T sú uzavreté na lineárne kombinácie, vyplýva, že aj $S \cap T$ má túto vlastnosť.

Dokážeme, že aj $S+T$ je uzavreté na lineárne kombinácie. Nech $a_1, a_2 \in K$ a $\boldsymbol{u}_1 = \boldsymbol{x}_1 + \boldsymbol{y}_1$, $\boldsymbol{u}_2 = \boldsymbol{x}_2 + \boldsymbol{y}_2$ sú vektory z $S+T$, pričom $\boldsymbol{x}_1, \boldsymbol{x}_2 \in S$, $\boldsymbol{y}_1, \boldsymbol{y}_2 \in T$. Potom

$$\begin{aligned} a_1\boldsymbol{u}_1 + a_2\boldsymbol{u}_2 &= a_1(\boldsymbol{x}_1 + \boldsymbol{y}_1) + a_2(\boldsymbol{x}_2 + \boldsymbol{y}_2) \\ &= (a_1\boldsymbol{x}_1 + a_2\boldsymbol{x}_2) + (a_1\boldsymbol{y}_1 + a_2\boldsymbol{y}_2) \in S + T, \end{aligned}$$

lebo S, T sú lineárne podpriestory, teda $a_1\boldsymbol{x}_1 + a_2\boldsymbol{x}_2 \in S$ a $a_1\boldsymbol{y}_1 + a_2\boldsymbol{y}_2 \in T$.

Dokážeme poslednú rovnosť. Inklúzie $S \cup T \subseteq S+T \subseteq [S \cup T]$ sú zrejmé. Keďže $S+T$ je lineárny podpriestor vo V a $[S \cup T]$ je najmenší lineárny podpriestor vo V, ktorý obsahuje množinu $S \cup T$, platí tiež $[S \cup T] \subseteq S + T$.

Na druhej strane čitateľ iste ľahko nájde príklady na to, že zjednotenie dvoch lineárnych podpriestorov S, T vektorového priestoru V nemusí byť lineárnym podpriestorom. Presnejšie, $S \cup T$ je lineárny podpriestor vo V práve vtedy, keď $S \subseteq T$ alebo $T \subseteq S$. Porozmýšľajte prečo.

Každý prvok $\boldsymbol{z} \in S+T$ súčtu lineárnych podpriestorov $S, T \subseteq V$ možno vyjadriť v tvare $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$ pre nejaké $\boldsymbol{x} \in S$, $\boldsymbol{y} \in T$. Vo všeobecnosti to však možno urobiť viacerými spôsobmi. Súčet lineárnych podpriestorov S, T vektorového priestoru V nazývame *priamym* alebo tiež *direktným súčtom*, ak každé $\boldsymbol{z} \in S+T$ možno *jednoznačne* vyjadriť v tvare $\boldsymbol{z}=\boldsymbol{x}+\boldsymbol{y}$, kde $\boldsymbol{x} \in S$, $\boldsymbol{y} \in T$; takýto súčet zvykneme tiež označovať $S \oplus T$.

4.3.2. Tvrdenie. *Nech S, T sú lineárne podpriestory vektorového priestoru V. Potom nasledujúce podmienky sú ekvivalentné:*

(i) $S+T=S \oplus T$, *t. j. súčet $S+T$ je direktný;*

(ii) $S \cap T=\{\mathbf{0}\}$.

Dôkaz. (i) $\Rightarrow$ (ii): Nech $\boldsymbol{z} \in S \cap T$. Potom $\boldsymbol{z}$ možno vyjadriť v tvare $\boldsymbol{z}=\boldsymbol{z}+\mathbf{0}$, kde $\boldsymbol{z} \in S$, $\mathbf{0} \in T$, ako aj v tvare $\boldsymbol{z}=\mathbf{0}+\boldsymbol{z}$, kde $\mathbf{0} \in S$, $\boldsymbol{z} \in T$. Z predpokladanej jednoznačnosti vyplýva $\boldsymbol{z}=\mathbf{0}$. Teda $S \cap T=\{\mathbf{0}\}$.

(ii) $\Rightarrow$ (i): Nech $S \cap T=\{\mathbf{0}\}$. Predpokladajme, že vektor $\boldsymbol{z} \in S+T$ možno vyjadriť v tvaroch $\boldsymbol{z}=\boldsymbol{x}_1+\boldsymbol{y}_1=\boldsymbol{x}_2+\boldsymbol{y}_2$, kde $\boldsymbol{x}_1, \boldsymbol{x}_2 \in S$, $\boldsymbol{y}_1, \boldsymbol{y}_2 \in T$. Potom $\boldsymbol{x}_1-\boldsymbol{x}_2=\boldsymbol{y}_2-\boldsymbol{y}_1$. Keďže $\boldsymbol{x}_1-\boldsymbol{x}_2 \in S$, $\boldsymbol{y}_2-\boldsymbol{y}_1 \in T$, uvedená spoločná hodnota patrí do $S \cap T$. Preto $\boldsymbol{x}_1-\boldsymbol{x}_2=\boldsymbol{y}_2-\boldsymbol{y}_1=\mathbf{0}$, t. j. $\boldsymbol{x}_1=\boldsymbol{x}_2$, $\boldsymbol{y}_1=\boldsymbol{y}_2$. To dokazuje požadovanú jednoznačnosť.

Uvedenú definíciu možno zrejmým spôsobom zovšeobecniť na priamy súčet ľubovoľného konečného počtu lineárnych podpriestorov. Zodpovedajúce zovšeobecnenie podmienky (ii) z práve dokázaného tvrdenia však už celkom priamočiare nie je. Podrobnosti nájde čitateľ v cvičení 4.8.

4.4. Lineárna nezávislosť

Nech $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n \in V$. Hovoríme, že usporiadaná n-tica vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je *lineárne závislá*, ak existujú skaláry $c_1, \dots, c_n \in K$ také, že $(c_1, \dots, c_n) \neq \mathbf{0}$ a $c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = \mathbf{0}$. V opačnom prípade hovoríme, že usporiadaná n-tica vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je *lineárne nezávislá*. Pre $n = 0$ kvôli úplnosti dodávame, že usporiadanú 0-ticu (t. j. prázdnu postupnosť) vektorov považujeme za lineárne nezávislú.

Miesto „lineárne (ne)závislá usporiadaná n-tica vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$“ budeme často hovoriť len o lineárne (ne)závislých vektoroch $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$.

Rozmeňme si teraz „na drobné“, čo znamená ono „v opačnom prípade“ v definícii lineárnej nezávislosti. Podľa tejto definície vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ sú lineárne nezávislé práve vtedy, keď

$$(\forall\, c_1, \dots, c_n \in K)(c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = \mathbf{0} \Rightarrow c_1 = \ldots = c_n = 0).$$

Vidíme, že logická štruktúra pojmu lineárnej nezávislosti je trochu zložitejšia, než sme boli doteraz zvyknutí. Keďže ide o kľúčový pojem, je potrebné sa pri ňom na chvíľu pristaviť.

Uvedomme si, že pre n-ticu skalárov $(c_1, \dots, c_n) = \mathbf{0}$ platí $c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = \mathbf{0}$ *pre ľubovoľnú* n-ticu vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, bez ohľadu na to, či je lineárne závislá alebo nezávislá. Avšak pre niektoré n-tice vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ môžeme ako výsledok lineárnej kombinácie $c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n$ dostať $\mathbf{0}$ aj pomocou *inej* n-tice skalárov $(c_1, \dots, c_n)$ než len $\mathbf{0} = (0, \dots, 0)$ – takéto usporiadané n-tice $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ nazývame *lineárne závislé*. Pre niektoré usporiadané n-tice vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je voľba $(c_1, \dots, c_n) = \mathbf{0}$ *jediná možnosť* ako lineárnou kombináciou $c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n$ získať výsledok $\mathbf{0}$ – takéto usporiadané n-tice nazývame *lineárne nezávislé*.

Na precvičenie práve definovaných pojmov čitateľovi odporúčame, aby si dokázal štyri jednoduché no užitočné pozorovania:

(a) jediný vektor $\boldsymbol{u}$ je lineárne nezávislý práve vtedy, keď $\boldsymbol{u} \neq \mathbf{0}$;

(b) vektory $\boldsymbol{u}$, $\boldsymbol{v}$ sú lineárne závislé práve vtedy, keď jeden z nich je násobkom druhého;

(c) ak niektorý z vektorov $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je $\mathbf{0}$, tak tieto vektory sú lineárne závislé;

(d) ak sa niektoré dva z vektorov $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ rovnajú alebo niektorý z nich je násobkom iného, tak tieto vektory sú lineárne závislé.

Inak povedané, len usporiadaná n-tica nenulových a navzájom rôznych vektorov, z ktorých žiaden nie je násobkom druhého, môže (no stále ešte nemusí) byť lineárne nezávislá.

Nasledujúce tvrdenie asi vysvetľuje názov „lineárna závislosť“ lepšie než samotná definícia.

4.4.1. Tvrdenie. *Pre ľubovoľné $n \in \mathbb{N}$ a $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in V$ nasledujúce podmienky sú ekvivalentné:*

(i) vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sú lineárne závislé;

(ii) niektorý z vektorov $\boldsymbol{u}_k$, $k \leq n$, je lineárnou kombináciou predchádzajúcich;

(ii') niektorý z vektorov $\boldsymbol{u}_k$, $k \leq n$, je lineárnou kombináciou nasledujúcich;

(iii) niektorý z vektorov $\boldsymbol{u}_k$, $k \leq n$, je lineárnou kombináciou ostatných.

Dôkaz. Dokážeme implikácie (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) a (iii) $\Rightarrow$ (i). Rovnako by bolo možné dokázať aj implikácie (i) $\Rightarrow$ (ii') $\Rightarrow$ (iii).

(i) $\Rightarrow$ (ii): Nech $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sú lineárne závislé vektory a $c_1, \ldots, c_n$ sú skaláry, nie všetky rovné 0, také, že $c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = \mathbf{0}$. Nech k je najväčší z indexov $1, \ldots, n$ taký, že $c_k \neq 0$.

Potom $c_i = 0$ pre $k < i \leq n$, teda $c_1\boldsymbol{u}_1 + \ldots + c_k\boldsymbol{u}_k = \sum_{i=1}^n c_i\boldsymbol{u}_i = \mathbf{0}$. Z toho dostávame

$$\boldsymbol{u}_k = c_k^{-1}(c_1\boldsymbol{u}_1 + \ldots + c_{k-1}\boldsymbol{u}_{k-1}),$$

t. j. $\boldsymbol{u}_k$ je lineárnou kombináciou predchádzajúcich vektorov.

(ii) $\Rightarrow$ (iii) platí triválne.

(iii) $\Rightarrow$ (i): Ak $\boldsymbol{u}_k = \sum_{\substack{i=1\\ i\neq k}}^n c_i\boldsymbol{u}_i$ je lineárnou kombináciou ostatných vektorov, položme $c_k = -1$. Potom pre n-ticu skalárov $(c_1, \ldots, c_n) \neq \mathbf{0}$ platí $c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = \mathbf{0}$, teda vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sú lineárne závislé.

Poznámka. Všimnite si, že dôkaz implikácie (i) $\Rightarrow$ (ii) pokrýva aj prípad $k = 1$. Vtedy $c_1 \neq 0$ a $c_1\boldsymbol{u}_1 = \mathbf{0}$, preto tiež $\boldsymbol{u}_1 = \mathbf{0}$. Teda $\boldsymbol{u}_1$ je naozaj lineárnou kombináciou predchádzajúcich (t. j. prázdnej postupnosti) vektorov.

Každý vektor $\boldsymbol{x}$ z lineárneho obalu $[\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n]$ možno vyjadriť v tvare

$$\boldsymbol{x} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n$$

pre nejakú n-ticu skalárov $(c_1, \ldots, c_n)$. Nasledujúce tvrdenie ukazuje, že lineárna nezávislosť vektorov $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ je ekvivalentná s jednoznačnosťou tohto vyjadrenia.

4.4.2. Veta. *Vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sú lineárne nezávislé práve vtedy, keď každý vektor $\boldsymbol{x} \in [\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n]$ možno vyjadriť v tvare $\boldsymbol{x} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n$ pre jedinú usporiadanú n-ticu $(c_1, \ldots, c_n) \in K^n$.*

Dôkaz. Nech $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sú lineárne nezávislé vektory. Predpokladajme, že vektor $\boldsymbol{x} \in [\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n]$ možno vyjadriť v tvaroch

$$\boldsymbol{x} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = d_1\boldsymbol{u}_1 + \ldots + d_n\boldsymbol{u}_n,$$

kde $(c_1,\dots,c_n),(d_1,\dots,d_n)\in K^n$. Potom

$$(c_1-d_1)\boldsymbol{u}_1+\dots+(c_n-d_n)\boldsymbol{u}_n=\mathbf{0}.$$

Z lineárnej nezávislosti vektorov $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n$ vyplýva $c_1-d_1=\dots=c_n-d_n=0$, čiže $(c_1,\dots,c_n)=(d_1,\dots,d_n)$. Teda vyjadrenie vektora $\boldsymbol{x}$ v tvare lineárnej kombinácie vektorov $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n$ je jednoznačné.

Predpokladajme teraz, že každý vektor $\boldsymbol{x}\in[\boldsymbol{u}_1,\dots,\boldsymbol{u}_n]$ má jednoznačné vyjadrenie v tvare lineárnej kombinácie vektorov $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n$. Špeciálne to platí aj pre vektor $\boldsymbol{x}=\mathbf{0}$, ktorý má vyjadrenie $\mathbf{0}=0\boldsymbol{u}_1+\dots+0\boldsymbol{u}_n$. Z jednoznačnosti tohto vyjadrenia vyplýva

$$c_1\boldsymbol{u}_1+\dots+c_n\boldsymbol{u}_n=\mathbf{0}\ \Rightarrow\ c_1=\dots=c_n=0$$

pre ľubovoľnú n-ticu skalárov $(c_1,\dots,c_n)$. Teda vektory $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n$ sú lineárne nezávislé.

Nasledujúce tvrdenie dáva do súvislosti lineárnu (ne)závislosť s lineárnym obalom.

4.4.3. Tvrdenie. *Nech $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}\in V$ pričom vektory $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n$ sú lineárne nezávislé. Potom nasledujúce podmienky sú ekvivalentné:*

(i) $\boldsymbol{v}\in[\boldsymbol{u}_1,\dots,\boldsymbol{u}_n]$;

(ii) *vektory* $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}$ *sú lineárne závislé;*

(iii) $[\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}]=[\boldsymbol{u}_1,\dots,\boldsymbol{u}_n]$.

Dôkaz. (i) $\Rightarrow$ (ii): Ak $\boldsymbol{v}\in[\boldsymbol{u}_1,\dots,\boldsymbol{u}_n]$ tak vektory $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}$ sú lineárne závislé podľa tvrdenia 4.4.1.

(ii) $\Rightarrow$ (iii): Nech vektory $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n,\boldsymbol{v}$ sú lineárne závislé. Potom niektorý z nich je lineárnou kombináciou predchádzajúcich. Keďže vektory $\boldsymbol{u}_1,\dots,\boldsymbol{u}_n$ sú lineárne nezávislé, môže to byť len vektor $\boldsymbol{v}$. Teda $\boldsymbol{v}\in[\boldsymbol{u}_1,\dots,\boldsymbol{u}_n]$.

(iii) $\Rightarrow$ (i) je obsiahnuté v bode (f) tvrdenia 4.2.2.

4.4.4. Veta. *Nech $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in V$, pričom vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ sú lineárne nezávislé. Potom z množiny $\{1, \dots, m\}$ možno vybrať indexy $i_1 < \dots < i_k$ tak, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_k}$ sú lineárne nezávislé a generujú rovnaký podpriestor ako vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_m$.*

Dôkaz. Označme $X = \{\boldsymbol{v}_1, \dots, \boldsymbol{v}_m\}$. Vektory $\boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_k}$ vyberieme z množiny X nasledujúcim spôsobom. Ak $X \subseteq [\boldsymbol{u}_1, \dots, \boldsymbol{u}_n]$, položme $k = 0$, t. j. nevyberieme žiaden z nich. V opačnom prípade nech $\boldsymbol{v}_{i_1}$ je prvý z vektorov množiny X, ktorý neleží v podpriestore $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_n]$. Ak $X \subseteq [\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}]$, tak $k = 1$ a $\boldsymbol{v}_{i_1}$ je jediný vybraný vektor. Podľa predchádzajúceho tvrdenia sú vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}$ lineárne nezávislé. Ak $X \not\subseteq [\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}]$, označíme $\boldsymbol{v}_{i_2}$ prvý vektor množiny X, ktorý neleží v $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}]$ (zrejme $i_1 < i_2$ a $\boldsymbol{v}_{i_1} \neq \boldsymbol{v}_{i_2}$). Vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}, \boldsymbol{v}_{i_2}$ sú podľa tvrdenia 4.4.3. opäť lineárne nezávislé. Podľa potreby pokračujeme rovnakým spôsobom, až kým pre takto získané lineárne nezávislé vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_k}$ neplatí inklúzia $X \subseteq [\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_k}]$, kedy sa zastavíme. (V krajnom prípade dostaneme $k = m$, t. j. vyberieme všetky vektory z množiny X.) Z uvedenej inklúzie okamžite vyplýva rovnosť

$$[\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_1, \dots, \boldsymbol{v}_m] = [\boldsymbol{u}_1, \dots, \boldsymbol{u}_n, \boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_k}],$$

keďže každý z generátorov podpriestoru na ľavej strane je prvkom podpriestoru na pravej strane.

4.5. Lineárny obal a lineárna nezávislosť v priestoroch K^m

V tomto paragrafe si ukážeme, ako možno na základe našich doterajších znalostí o sústavách lineárnych rovníc tou istou metódou úpravy matíc pomocou ERO na (redukovaný) stupňovitý tvar riešiť pre vektory z priestoru K^m nasledujúce tri otázky:

(1) rozhodnúť pre dané vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y} \in K^m$ či $\boldsymbol{y}$ patrí alebo nepatrí do lineárneho obalu $[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$;

(2) rozhodnúť pre dané vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in K^m$ či sú lineárne závislé alebo nezávislé;

(3) vybrať z vektorov $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in K^m$ lineárne nezávislé vektory $\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_k}$ $(j_1 < \ldots < j_k)$ tak, aby vektory $\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_k}$ generovali vo V ten istý lineárny podpriestor ako vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$.

Hoci všetky tri otázky možno riešiť naraz jednotným spôsobom, z metodických dôvodov začneme jednoduchšími otázkami (1) a (2), a až potom pristúpime k trochu zložitejšej otázke (3). Navyše pri tom zavedieme označenie, ktorého sa budeme držať v celom paragrafe.

Nech $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{y} \in K^m$ sú stĺpcové vektory, pričom

$$\boldsymbol{x}_j = \begin{pmatrix} x_{1j} \\ \vdots \\ x_{mj} \end{pmatrix}, \qquad \boldsymbol{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Označme $\boldsymbol{X} = (x_{ij}) \in K^{m\times n}$ maticu so stĺpcami $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$, a $(\boldsymbol{X} \,|\, \boldsymbol{y}) \in K^{m\times(n+1)}$ blokovú maticu zloženú z matice $\boldsymbol{X}$ a vektora $\boldsymbol{y}$. Potom pre $\boldsymbol{c} = (c_1, \ldots, c_n)^T \in K^n$ platí:

(1) $c_1\boldsymbol{x}_1 + \ldots + c_n\boldsymbol{x}_n = \boldsymbol{y} \;\Leftrightarrow\; \boldsymbol{X}\cdot\boldsymbol{c} = \boldsymbol{y}$;
(2) $c_1\boldsymbol{x}_1 + \ldots + c_n\boldsymbol{x}_n = \mathbf{0} \;\Leftrightarrow\; \boldsymbol{X}\cdot\boldsymbol{c} = \mathbf{0}$.
Inak povedané: (1) $\boldsymbol{y} \in [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$ práve vtedy, keď sústava $\boldsymbol{X}\cdot\boldsymbol{c} = \boldsymbol{y}$ s rozšírenou maticou $(\boldsymbol{X}\,|\,\boldsymbol{y})$ má aspoň jedno riešenie; (2) vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ sú lineárne nezávislé práve vtedy, keď homogénna sústava $\boldsymbol{X}\cdot\boldsymbol{c} = \mathbf{0}$ má jediné riešenie $\boldsymbol{c} = \mathbf{0}$; ak táto sústava má aj nejaké nenulové riešenie, tak vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ sú lineárne závislé. (Nedajte sa spliesť atypickým označením: x_{ij} sú teraz koeficienty sústavy, y_i sú zložky pravej strany a c_j sú neznáme.)

Otázku (1) už vieme riešiť. Stačí pomocou ERO upraviť maticu $(\boldsymbol{X}\,|\,\boldsymbol{y})$ na stupňovitý tvar. Ak výsledná matica obsahuje riadok tvaru $(0, \ldots, 0\,|\,z)$, kde $z \neq 0$, tak sústava $\boldsymbol{X}\cdot\boldsymbol{c} = \boldsymbol{y}$ nemá riešenie a $\boldsymbol{y} \notin [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$. Ak sa taký riadok vo výslednej matici nenachádza, tak sústava má aspoň jedno riešenie a $\boldsymbol{y} \in [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$.

Podobne je to s otázkou (2). Opäť stačí pomocou ERO upraviť maticu $\boldsymbol{X}$ na stupňovitý tvar a pozrieť sa, či v každom stĺpci leží vedúci prvok nejakého riadku. Ak je to tak, niet čo voliť za parametre, $\boldsymbol{c} = \mathbf{0}$ je jediným riešením sústavy $\boldsymbol{X}\cdot\boldsymbol{c} = \mathbf{0}$ a vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ sú lineárne nezávislé. V opačnom prípade máme možnosť voľby aspoň jedného parametra, sústava má aj nejaké nenulové riešenie a vektory $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ sú lineárne závislé.

Ešte si všimnime úzku súvislosť oboch otázok. Vedúcim prvkom riadku $(0, \ldots, 0\,|\,z)$, kde $z \neq 0$, je práve v $(n+1)$-om stĺpci ležiaci prvok z. Teda matica v stupňovitom tvare riadkovo ekvivalentná s $(\boldsymbol{X}\,|\,\boldsymbol{y})$ neobsahuje taký riadok práve vtedy, keď v jej poslednom stĺpci neleží vedúci prvok žiadneho riadku.

4.5.1. Príklad. Uvažujme stĺpcové vektory $\boldsymbol{x}_1 = (1, 1, -1, -1)^T$, $\boldsymbol{x}_2 = (0, 1, 0, 1)^T$, $\boldsymbol{x}_3 = (3, 1, -3, -5)^T$, $\boldsymbol{x}_4 = (0, 0, 1, 2)^T$, $\boldsymbol{y} = (3, 5, -2, 1)^T$, $\boldsymbol{z} = (1, 1, 1, 1)^T$ v priestore $\mathbb{R}^4$. Máme rozhodnúť, či vektory $\boldsymbol{y}$, $\boldsymbol{z}$ patria do lineárneho obalu $[\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4]$. Označme si nasledujúce matice

$$(\boldsymbol{X}\,|\,\boldsymbol{y}) = \left(\begin{array}{rrrr|r} 1 & 0 & 3 & 0 & 3 \\ 1 & 1 & 1 & 0 & 5 \\ -1 & 0 & -3 & 1 & -2 \\ -1 & 1 & -5 & 2 & 1 \end{array}\right), \qquad (\boldsymbol{X}\,|\,\boldsymbol{z}) = \left(\begin{array}{rrrr|r} 1 & 0 & 3 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ -1 & 0 & -3 & 1 & 1 \\ -1 & 1 & -5 & 2 & 1 \end{array}\right).$$

Matice $(\boldsymbol{X}\,|\,\boldsymbol{y})$, $(\boldsymbol{X}\,|\,\boldsymbol{z})$ sú riadkovo ekvivalentné s maticami

$$\left(\begin{array}{rrrr|r} 1 & 0 & 3 & 0 & 3 \\ 0 & 1 & -2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \quad \text{resp.} \quad \left(\begin{array}{rrrr|r} 1 & 0 & 3 & 0 & 1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & -2 \end{array}\right).$$

Okamžite vidíme, že platí $\boldsymbol{y} \in [\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4]$ a $\boldsymbol{z} \notin [\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{x}_4]$.

4.5.2. Príklad. Zistíme, či stĺpce reálnej matice

$$\boldsymbol{X} = \begin{pmatrix} 2 & 0 & 1 & 3 \\ 2 & 1 & 2 & 3 \\ 0 & 2 & 3 & 2 \\ 1 & 2 & 4 & 2 \end{pmatrix}$$

sú lineárne závislé alebo nezávislé. Táto matica je riadkovo ekvivalentná s maticou

$$\begin{pmatrix} 1 & 2 & 4 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 5 \end{pmatrix}.$$

Vidíme, že stĺpce matice $\boldsymbol{X}$ sú lineárne nezávislé. Na druhej strane, ako matica nad poľom $\mathbb{Z}_5$ je $\boldsymbol{X}$ riadkovo ekvivalentná s maticou

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

Teda stĺpce matice $\boldsymbol{X}$, chápané ako vektory z vektorového priestoru $\mathbb{Z}_5^4$, sú lineárne závislé.

Kľúčom k odpovedi na otázku (3) je nasledujúce tvrdenie.

4.5.3. Tvrdenie. *Nech $\boldsymbol{X}$, $\boldsymbol{Y} \in K^{m\times n}$ sú riadkovo ekvivalentné matice, pričom matica $\boldsymbol{Y}$ je v stupňovitom tvare. Pre $1 \le j \le n$ označme $\boldsymbol{x}_j = \boldsymbol{s}_j(\boldsymbol{X})$ j-ty stĺpec matice $\boldsymbol{X}$. Nech $j_1 < \ldots < j_k$ sú indexy všetkých stĺpcov matice $\boldsymbol{Y}$, v ktorých ležia vedúce prvky jej riadkov. Potom platí:*

(a) *vektory $\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_k}$ sú lineárne nezávislé;*

(b) *ak v j-tom stĺpci matice $\boldsymbol{Y}$ neleží vedúci prvok žiadneho jej riadku (t. j. $1 \le j \le n$ a $j \ne j_1, \ldots, j_k$), tak vektor $\boldsymbol{x}_j$ je lineárnou kombináciou vektorov $\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_l}$, kde $l \le k$ je najväčší index, pre ktorý platí $j_l < j$;*

(c) $[\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_k}] = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$.

Dôkaz. (a) Označme $\boldsymbol{X}'$, $\boldsymbol{Y}'$ matice, ktoré pozostávajú len zo stĺpcov s indexmi $j_1, \ldots, j_k$ matíc $\boldsymbol{X}$ resp. $\boldsymbol{Y}$ (ostatné stĺpce vynecháme). Potom postupnosťou tých istých ERO, ktorými sme $\boldsymbol{X}$ upravili na $\boldsymbol{Y}$, dostaneme z $\boldsymbol{X}'$ maticu $\boldsymbol{Y}'$, teda $\boldsymbol{X}' \sim \boldsymbol{Y}'$. Matica $\boldsymbol{Y}'$ je však v stupňovitom tvare a má v každom stĺpci vedúci prvok nejakého svojho riadku. Preto homogénna sústava $\boldsymbol{X}' \cdot \boldsymbol{d} = \boldsymbol{0}$ má jediné riešenie $\boldsymbol{d} = \boldsymbol{0} \in K^k$, čo znamená, že stĺpce matice $\boldsymbol{X}'$, t. j. vektory $\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_k}$, sú lineárne nezávislé.

(b) Bez ujmy na všeobecnosti môžeme predpokladať, že matica $\boldsymbol{Y}$ je dokonca v redukovanom stupňovitom tvare. Poloha vedúcich prvkov riadkov v jednotlivých stĺpcoch bude stále rovnaká. Nech $j \neq j_1, \ldots, j_k$. Pri voľbe parametra $c_j = 1$ a voľbou 0 za hodnotu všetkých ostatných parametrov (ak nejaké zostali) dostaneme jedno riešenie $\boldsymbol{c} = (c_1, \ldots, c_n)^T \neq \boldsymbol{0}$ sústavy $\boldsymbol{X} \cdot \boldsymbol{c} = \boldsymbol{0}$. Nech $l \leq k$ je najväčší index taký, že $j_l < j$. Pre naše riešenie $\boldsymbol{c}$ navyše platí $c_p = 0$, ak $j \leq p \leq n$. Ak je totiž c_p parameter, tak je to dôsledok našej voľby, a vo vyjadrení neznámych c_{j_h} pre $l < h \leq k$ sa (jediný nenulový) parameter c_j nevyskytuje. Označme $\boldsymbol{X}''$ maticu, ktorá pozostáva len zo stĺpcov matice $\boldsymbol{X}$ s indexmi $j_1, \ldots, j_l$ a j. Z uvedených dôvodov je vektor $\boldsymbol{c}'' = (c_{j_1}, \ldots, c_{j_l}, 1)^T$ riešením sústavy $\boldsymbol{X}'' \cdot \boldsymbol{c}'' = \boldsymbol{0}$. To znamená, že

$$\boldsymbol{x}_j = -(c_{j_1}\boldsymbol{x}_{j_1} + \ldots + c_{j_l}\boldsymbol{x}_{j_l}) \in [\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_l}].$$

(c) je bezprostredným dôsledkom (b) a tvrdenia 4.4.3.

Práve dokázané tvrdenie nám dáva priamy návod na riešenie otázky (3). Stačí pomocou ERO upraviť maticu $\boldsymbol{X} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n)$ na maticu $\boldsymbol{Y}$ v stupňovitom tvare a zistiť v nej indexy $j_1 < \ldots < j_k$ všetkých stĺpcov, v ktorých ležia vedúce prvky jej riadkov. Potom $\boldsymbol{x}_{j_1}, \ldots, \boldsymbol{x}_{j_k}$ sú hľadané lineárne nezávislé vektory, ktoré generujú lineárny podpriestor $[\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n]$.

4.5.4. Príklad. Zo stĺpcov reálnej matice

$$\boldsymbol{X} = \begin{pmatrix} 1 & 1 & 3 & -1 & 1 \\ 2 & 0 & 2 & 1 & 3 \\ 1 & 1 & 3 & 2 & 4 \\ 2 & 0 & 2 & 0 & 2 \end{pmatrix}$$

treba vybrať lineárne nezávislé stĺpce, ktoré generujú lineárny obal všetkých stĺpcov matice $\boldsymbol{X}$. Matica $\boldsymbol{X}$ je riadkovo ekvivalentná s maticou

$$\boldsymbol{Y} = \begin{pmatrix} 1 & 1 & 3 & -1 & 1 \\ 0 & 1 & 2 & 2 & -3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

v stupňovitom tvare. Vedúce prvky riadkov matice $\boldsymbol{Y}$ sa nachádzajú v stĺpcoch 1, 2 a 4. Hľadané vektory sú teda stĺpce 1, 2 a 4 matice $\boldsymbol{X}$. Zapísané vedľa seba tvoria maticu

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

I keď sme celý postup riešenia otázok (1), (2) a (3) vyložili len pre priestory stĺpcových vektorov K^m a týchto priestorov sa týkali aj všetky príklady, čitateľovi by už nemalo robiť ťažkosti modifikovať popísanú metódu aj na priestory riadkových vektorov K^m – či už transponovaním, príslušných matíc riadkových vektorov alebo nahradením elementárnych riadkových operácií stĺpcovými.

4.6. Lineárne nezávislé postupnosti a množiny

V tomto paragrafe stručne doplníme pojmy lineárnej závislosti a nezávislosti spôsobom, ktorý umožňuje ich použitie i v prípade nekonečných postupností a ľubovoľných (t. j. konečných aj nekonečných) množín vektorov. Nakoľko však tieto otázky zostávajú na okraji nášho záujmu, popri príslušných definíciách sa obmedzíme len na niekoľko jednoduchých zovšeobecnení výsledkov o lineárnej (ne)závislosti usporiadaných n-tíc. *Nekonečnú postupnosť* $(\boldsymbol{u}_k)_{k=0}^{\infty} = (\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k, \ldots)$ vektorov z priestoru V nazývame *lineárne nezávislou*, ak každá jej konečná podpostupnosť $(\boldsymbol{u}_{k_1}, \ldots, \boldsymbol{u}_{k_n})$, kde $0 \le k_1 < \ldots < k_n$, je lineárne nezávislá.

Dôkaz nasledujúceho jednoduchého tvrdenia prenechávame čitateľovi.

4.6.1. Tvrdenie. *Nekonečná postupnosť $(\boldsymbol{u}_k)_{k=0}^{\infty}$ vektorov z V je lineárne nezávislá práve vtedy, keď pre každé $n \in \mathbb{N}$ jej počiatočný úsek $(\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ je lineárne nezávislý.*

Napríklad postupnosť $(1, x, x^2, \ldots, x^k, \ldots)$ všetkých mocnín x je lineárne nezávislá postupnosť vo vektorovom priestore $K[x]$ všetkých polynómov v premennej x nad poľom K. Polynóm $f(x) = a_0 + a_1x + \ldots + a_nx^n$ je totiž (definitoricky) nulový práve vtedy, keď $a_0 = a_1 = \ldots = a_n = 0$. *Množina* $X \subseteq V$ sa nazýva *lineárne nezávislá*, ak pre ľubovoľné

$n \in \mathbb{N}$ každá usporiadaná n-tica *navzájom rôznych* vektorov $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ z množiny X je lineárne nezávislá.

Ešte raz podčiarkujeme ono „navzájom rôznych“ – keby totiž $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ neboli navzájom rôzne vektory, nemohli by byť lineárne nezávislé.

Lineárna závislosť či nezávislosť usporiadanej n-tice vektorov nezávisí od ich poradia – zrejme usporiadaná n-tica $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je lineárne nezávislá práve vtedy, keď je lineárne nezávislá usporiadaná n-tica $(\boldsymbol{u}_{\sigma(1)}, \dots, \boldsymbol{u}_{\sigma(n)})$, kde σ je ľubovoľná permutácia množiny $\{1, \dots, n\}$. Inak povedané, lineárna (ne)závislosť usporiadanej n-tice $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ navzájom rôznych vektorov je vlastnosťou množiny $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_n\}$. Čitateľ už iste ľahko nahliadne platnosť nasledujúceho očividného tvrdenia.

4.6.2. Tvrdenie. *Usporiadaná n-tica $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ navzájom rôznych vektorov z V je lineárne nezávislá práve vtedy, keď množina $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_n\} \subseteq V$ je lineárne nezávislá.*

Naše záverečné tvrdenie, ktoré dáva do súvisu lineárnu (ne)závislosť množiny s jej lineárnym obalom, je obdobou tvrdenia 4.4.3. Taktiež jeho dôkaz možno získať malou obmenou dôkazu spomínaného tvrdenia.

4.6.3. Tvrdenie. *Nech $X \subseteq V$ je lineárne nezávislá množina a $\boldsymbol{v} \in V$. Potom nasledujúce podmienky sú ekvivalentné:*

(i) $\boldsymbol{v} \in [X]$;

(ii) *množina $X \cup \{\boldsymbol{v}\}$ je lineárne závislá;*

(iii) $[X \cup \{\boldsymbol{v}\}] = [X]$.

Cvičenia

4.1. Nech S, T sú lineárne podpriestory vektorového priestoru V. Potom $S \cup T$ je lineárny podpriestor V práve vtedy, keď $S \subseteq T$ alebo $T \subseteq S$. Dokážte.

4.2. V každom z nasledujúcich prípadov rozhodnite, či daná podmnožina S vektorového priestoru V nad poľom K je jeho lineárnym podpriestorom. Svoje rozhodnutie zdôvodnite. Ak S nie je lineárny podpriestor, popíšte jeho lineárny obal $[S]$.

(a) $K = \mathbb{R}$, $V = \mathbb{R}$, $S = \langle -1, 1 \rangle$;

(b) $K = \mathbb{C}$, $V = \mathbb{C}$, $S = \{z \in \mathbb{C};\ |z| = 1\}$;

(c) $K = \mathbb{R}$, $V = \mathbb{R}^2$, $S = \{(x, y) \in \mathbb{R}^2;\ x - 2y = 0\}$;

(d) $K = \mathbb{C}$, $V = \mathbb{C}^2$, $S = \{(x, y) \in \mathbb{C}^2;\ x + \mathrm{i}y = 1\}$;

(e) $K = \mathbb{R}$, $V = \mathbb{C}$, $S = \{x \in \mathbb{C};\ \operatorname{Re} x = \operatorname{Im} x\}$;

(f) $K = \mathbb{Q}$, $V = \mathbb{R}$, $S = \mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3};\ a, b \in \mathbb{Q}\}$;

(g) $K = \mathbb{Z}_2$, $V = \mathbb{Z}_2^3$, $S = \{(0,0,0), (1,0,0), (0,1,0), (0,0,1)\}$;

(h) $K = \mathbb{Z}_3$, $V = \mathbb{Z}_3^2$, $S = \{(0,0), (1,2), (2,1)\}$;

(i) K ľubovoľné, $V = K[x]$, $S = \{f(x) \in K[x];\ f(1) = 0\}$;

(j) K ľubovoľné, $V = K[x]$, $S = \{f(x) \in K[x];\ f(0) = 1\}$;

(k) K ľubovoľné, $V = K[x]$, $S = \{f(x) \in K[x]; f(0) = f(1)\}$;

(l) K ľubovoľné, $V = K[x]$, $S = \{a + bx + (a + b)x^2;\ a, b \in K\}$;

(m) K ľubovoľné, $V = K[x]$, $S = \{a + bx + (a + b + 1)x^2;\ a, b \in K\}$.

4.3. V každom z nasledujúcich prípadov rozhodnite, či uvedené vektory z vektorového priestoru V nad poľom K sú lineárne nezávislé. Svoje rozhodnutie odôvodnite.

(a) $K = \mathbb{Q}$, $V = \mathbb{Q}^2$, $\boldsymbol{u} = (0, 0)$, $\boldsymbol{v} = (1, 1)$;

(b) $K = \mathbb{Q}$, $V = \mathbb{Q}^3$, $\boldsymbol{w} = (1, 2, 3)^T$;

(c) $K = \mathbb{R}$, $V = \mathbb{R}^4$, $\boldsymbol{x} = (0, 1, 0, 1)^T$, $\boldsymbol{y} = (1, 0, 1, 0)^T$, $\boldsymbol{z} = (1, 0, 0, 1)^T$;

(d) $K = \mathbb{C}$, $V = \mathbb{C}^3$, $\boldsymbol{u} = (1, \mathrm{i}, -\mathrm{i})$, $\boldsymbol{v} = (2 + \mathrm{i}, 3 - \mathrm{i}, 1 + 2\mathrm{i})$, $\boldsymbol{w} = (2 + 2\mathrm{i}, 2 - \mathrm{i}, 2 + 2\mathrm{i})$;

(e) $K = \mathbb{Z}_5$, $V = \mathbb{Z}_5^4$, $\boldsymbol{x} = (1, 3, 2, 4)$, $\boldsymbol{y} = (2, 2, 1, 1)$, $\boldsymbol{z} = (4, 2, 4, 2)$;

(f) $K = \mathbb{Z}_7$, $V = \mathbb{Z}_7^4$, $\boldsymbol{x} = (1, 3, 2, 4)$, $\boldsymbol{y} = (2, 2, 1, 1)$, $\boldsymbol{z} = (4, 2, 4, 2)$;

(g) $K = \mathbb{R}$, $V = \mathbb{R}^{(3)}[x]$, $f_0(x) = 1$, $f_1(x) = x$, $f_2(x) = x(x - 1)$, $f_3(x) = x(x - 1)(x - 2)$;

(h) $K = \mathbb{Z}_3$, $V = \mathbb{Z}_{13}[x]$, $f(x) = 5 + 12x$, $g(x) = 12 + 8x$;

(i) $K = \mathbb{R}$, $V = \mathbb{R}[x]$, $f(x) = 5 + 12x$, $g(x) = 12 + 8x$.

4.4. Nech V je vektorový priestor nad poľom K, $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in V$ sú lineárne nezávislé vektory a $\boldsymbol{A} \in K^{m\times n}$. Pre $i = 1, \ldots, m$ označme $\boldsymbol{v}_i = a_{i1}\boldsymbol{u}_1 + \ldots + a_{in}\boldsymbol{u}_n = \boldsymbol{r}_i(\boldsymbol{A}) \cdot (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)^T$. Potom vektory $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in V$ sú lineárne nezávislé práve vtedy, keď riadky matice $\boldsymbol{A}$ sú lineárne nezávislé vektory v K^n. Dokážte. Čo sa zmení, ak $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ sú lineárne závislé?

4.5. Nech V je vektorový priestor nad poľom K. V každom z nasledujúcich prípadov rozhodnite, či vektor $\boldsymbol{u} \in V$ patrí do lineárneho obalu vektorov $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in V$.

(a) $K = \mathbb{R}$, $V = \mathbb{R}^3$, $\boldsymbol{x} = (1, 1, 2)^T$, $\boldsymbol{y} = (-2, 1, -1)^T$, $\boldsymbol{z} = (0, 1, 1)^T$, $\boldsymbol{u} = (1, 2, -1)^T$;

(b) $K = \mathbb{C}$, $V = \mathbb{C}^2$, $\boldsymbol{x} = (\mathrm{i}, 1 + \mathrm{i})$, $\boldsymbol{y} = (1, 1 - \mathrm{i})$, $\boldsymbol{z} = (\mathrm{i}, -\mathrm{i})$, $\boldsymbol{u} = (1 + \mathrm{i}, 1 - \mathrm{i})$;

(c) $K = \mathbb{Z}_3$, $V = \mathbb{Z}_3^3$, $\boldsymbol{x} = (0, 1, 2)$, $\boldsymbol{y} = (1, 2, 0)$, $\boldsymbol{z} = (2, 0, 1)$, $\boldsymbol{u} = (1, 0, 1)$;

(d) $K = \mathbb{Z}_5$, $V = \mathbb{Z}_5^3$, $\boldsymbol{x} = (0, 1, 2)$, $\boldsymbol{y} = (1, 2, 0)$, $\boldsymbol{z} = (2, 0, 1)$, $\boldsymbol{u} = (1, 0, 1)$.

4.6. V každej z úloh (a)–(i) cvičenia 4.3 vyberte z daných vektorov lineárne nezávislé vektory, ktoré generujú ten istý lineárny podpriestor ako pôvodné vektory. Riešte rovnaký problém pre vektory $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$, $\boldsymbol{u}$ v každej z úloh (a)–(d) cvičenia 4.5. Využite pri tom výsledky cvičení 4.3 a 4.5.

4.7. Doplňte chýbajúce dôkazy častí (a)–(e) tvrdenia 4.2.2.

4.8. (a) Zovšeobecnite definíciu *priameho súčtu* na ľubovoľný konečný počet lineárnych podpriestorov daného vektorového priestoru.

(b) Nech $S_1, \dots, S_n$ $(n \geq 2)$ sú lineárne podpriestory vektorového priestoru V. Pre $i = 1, \dots, n$ označme $T_i = S_1 + \ldots + S_{i-1} + S_{i+1} + \ldots + S_n$, t. j. $T_1 = S_2 + \ldots + S_n$, $T_2 = S_1 + S_3 + \ldots + S_n$, $\dots$, $T_n = S_1 + \ldots + S_{n-1}$. Potom $S_1 + \ldots + S_n = S_1 \oplus \ldots \oplus S_n$, t. j. súčet podpriestorov $S_1, \dots, S_n$ je priamy, práve vtedy, keď pre každé $i \leq n$ platí $S_i \cap T_i = \{\mathbf{0}\}$. Dokážte.

4.9. Nech V je vektorový priestor nad poľom K a $X \subseteq V$ je ľubovoľná podmnožina. Dokážte tzv. *podmienku zámeny*: $(\forall\, \boldsymbol{u}, \boldsymbol{v} \in V)(\boldsymbol{u} \in [X \cup \{\boldsymbol{v}\}] \smallsetminus [X] \;\Rightarrow\; \boldsymbol{v} \in [X \cup \{\boldsymbol{u}\}])$. Rozhodnite, či platí dokonca ekvivalencia $(\forall\, \boldsymbol{u}, \boldsymbol{v} \in V)(\boldsymbol{u} \in [X \cup \{\boldsymbol{v}\}] \smallsetminus [X] \;\Leftrightarrow\; \boldsymbol{v} \in [X \cup \{\boldsymbol{u}\}] \smallsetminus [X])$?

4.10. Dokážte tvrdenia 4.6.1., 4.6.2. a 4.6.3.

4.11. Nech K je pole a $(p_k(x))_{k=0}^{\infty}$ je postupnosť polynómov z $K[x]$ taká, že pre $k \neq l$ majú polynómy $p_k(x)$, $p_l(x)$ rôzny stupeň. Dokážte, že potom ide o lineárne nezávislú postupnosť.

5. Báza a dimenzia

V tejto kapitole sa oboznámime s pojmom *bázy* vektorového priestoru, čo nám v niektorých vektorových priestoroch umožní zaviesť *súradnice*. Ďalej budeme definovať *dimenziu* vektorového priestoru a odvodíme jej základné vlastnosti. V nasledujúcej kapitole si potom okrem iného dokážeme, že dimenzia je základný štruktúrny invariant tzv. *konečnorozmerných* vektorových priestorov.

I v tejto kapitole V označuje nejaký vektorový priestor nad pevným poľom K.

5.1. Steinitzova veta a konečnorozmerné priestory

Začneme jedným technickým výsledkom kľúčového významu.

5.1.1. Tvrdenie. (Steinitzova veta) *Nech* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in V$. *Ak vektory* $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ *sú lineárne nezávislé a všetky patria do lineárneho obalu* $[\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m]$, *tak* $n \leq m$.

Dôkaz. Keďže $\boldsymbol{u}_j \in [\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m]$ pre každé $j \leq n$, existujú $\boldsymbol{c}_j = (c_{1j}, \ldots, c_{mj})^T \in K^m$ také, že

$$\boldsymbol{u}_j = c_{1j}\boldsymbol{v}_1 + \ldots + c_{mj}\boldsymbol{v}_m = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) \cdot \boldsymbol{c}_j.$$

Inak povedané

$$(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) \cdot \boldsymbol{C},$$

kde $\boldsymbol{C} = (c_{ij})_{m\times n}$ je matica so stĺpcami $\boldsymbol{c}_1, \dots, \boldsymbol{c}_n$.

Predpokladajme, že $m < n$. Potom podľa tvrdenia 3.3.6. má homogénna sústava $\boldsymbol{C}\cdot\boldsymbol{x} = \boldsymbol{0}$ aspoň jedno riešenie $\boldsymbol{x} = (x_1, \dots, x_n)^T \neq \boldsymbol{0}$. Jednoduchým výpočtom dostávame

$$\begin{aligned} x_1\boldsymbol{u}_1 + \ldots + x_n\boldsymbol{u}_n &= (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)\cdot\boldsymbol{x} \\ &= (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)\cdot\boldsymbol{C}\cdot\boldsymbol{x} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)\cdot\boldsymbol{0} = \boldsymbol{0}, \end{aligned}$$

čo je v spore s lineárnou nezávislosťou vektorov $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$.

5.1.2. Tvrdenie. *Pre ľubovoľný vektorový priestor V nasledujúce podmienky sú ekvivalentné:*

(i) existuje konečná množina $X \subseteq V$ taká, že $[X] = V$;

(ii) každá lineárne nezávislá množina $Y \subseteq V$ je konečná.

Dôkaz. (i) $\Rightarrow$ (ii): Nech $X \subseteq V$ je konečná množina, ktorá generuje V. Podľa Steinitzovej vety pre ľubovoľné lineárne nezávislé vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ platí $n \leq \# X$, teda každá lineárne nezávislá množina $Y \subseteq V$ je konečná.

(ii) $\Rightarrow$ (i): Budeme dokazovať logicky ekvivalentnú implikáciu $\neg$ (i) $\Rightarrow$ $\neg$ (ii).

Predpokladajme, že žiadna konečná podmnožina priestoru V negeneruje V. Potom vo V môžeme zostrojiť postupnosť vektorov $(\boldsymbol{y}_n)_{n=0}^{\infty}$ takú, že $\boldsymbol{y}_0 \neq \boldsymbol{0}$ a pre každé $n > 0$ platí $\boldsymbol{y}_n \notin [\boldsymbol{y}_0, \dots, \boldsymbol{y}_{n-1}]$. Podľa tvrdenia 4.4.1. je každý počiatočný úsek $(\boldsymbol{y}_0, \dots, \boldsymbol{y}_n)$ tejto postupnosti lineárne nezávislý, takže celá postupnosť je lineárne nezávislá podľa tvrdenia 4.6.1. Teda vo V existuje nekonečná lineárne nezávislá množina, napr. $Y = \{\boldsymbol{y}_n;\ n \in \mathbb{N}\}$.

Hovoríme, že vektorový priestor V je *konečnorozmerný* , ak spĺňa niektorú (teda nevyhnutne obe) z ekvivalentných podmienok (i), (ii) práve dokázaného tvrdenia. V opačnom prípade hovoríme, že V je *nekonečnorozmerný* vektorový priestor.

5.2. Báza a dimenzia konečnorozmerného priestoru

Nech V je konečnorozmerný vektorový priestor. *Bázou* priestoru V nazývame každú lineárne nezávislú usporiadnú n-ticu $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ vektorov z V, ktorá generuje celý priestor V. Stručne tiež hovoríme, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ tvoria bázu priestoru V.

Nasledujúce tvrdenie je priamym dôsledkom vety 4.4.4.

5.2.1. Tvrdenie. *Nech V je konečnorozmerný vektorový priestor. Potom*

(a) ľubovoľnú lineárne nezávislú usporiadanú k-ticu $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ vektorov z V možno doplniť do nejakej bázy $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \dots, \boldsymbol{u}_n)$ priestoru V;

(b) z ľubovoľnej generujúcej usporiadanej m-tice $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ vektorov z V možno vybrať nejakú bázu $(\boldsymbol{v}_{i_1}, \dots, \boldsymbol{v}_{i_n})$ priestoru V.

5.2.2. Veta. *Nech V je konečnorozmerný vektorový priestor. Potom*

(a) V má aspoň jednu bázu;

(b) ľubovoľné dve bázy priestoru V majú rovnaký počet prvkov.

Dôkaz. (a) je bezprostredným dôsledkom predchádzajúceho tvrdenia, ktoré nám dokonca dáva dva varianty dôkazu: jeden doplnením prázdnej množiny (ktorá je lineárne nezávislá) na bázu vo V, druhý výberom bázy z nejakej konečnej generujúcej množiny vo V.

(b) je bezprostredným dôsledkom Steinitzovej vety. Ak sú totiž $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ dve bázy vo V, tak, keďže $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je lineárne nezávislá a $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ generuje celý priestor V, musí platiť $n \leq m$. Nakoľko však i $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_m)$ je lineárne nezávislá a $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ generuje celé V, platí tiež $m \leq n$. Teda $m = n$.

Práve dokázaná veta nám umožňuje korektne definovať *dimenziu* alebo tiež *rozmer* konečnorozmerného vektorového priestoru V ako počet prvkov jeho ľubovoľnej bázy. Dimenziu vektorového priestoru V značíme $\dim V$. Ak $\dim V = n$, hovoríme, že V je *n-rozmerný* vektorový priestor. Ak V je nekonečnorozmerný priestor, kladieme $\dim V = \infty$. V prípade, že bude potrebné zdôrazniť úlohu poľa K, budeme používať podrobnejšie označenie $\dim_K V$.

Teda V je konečnorozmerný práve vtedy, keď $\dim V < \infty$.

Dôkaz nasledujúceho tvrdenia prenechávame ako cvičenie čitateľovi.

5.2.3. Tvrdenie. *Nech* $\dim V = n$, $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m \in V$. *Potom ľubovoľné dve z nasledujúcich podmienok implikujú tretiu:*

(i) *vektory* $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m$ *sú lineárne nezávislé;*

(ii) $[\boldsymbol{v}_1, \dots, \boldsymbol{v}_m] = V$*;*

(iii) $m = n$.

To okrem iného znamená, že na overenie, či n vektorov $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ tvorí bázu n-rozmerného vektorového priestoru V, stačí overiť len jednu (a to ľubovoľnú) z podmienok (i), (ii).

5.3. Súradnice vektora vzhľadom na danú bázu

Nasledujúca veta je špeciálnym prípadom vety 4.4.2.

5.3.1. Veta. *Vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ tvoria bázu vektorového priestoru V práve vtedy, keď každý vektor $\boldsymbol{x} \in V$ možno jednoznačne vyjadriť v tvare lineárnej kombinácie*

$$\boldsymbol{x} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n.$$

Uvedomme si, že existencia aspoň jedného vyjadrenia $\boldsymbol{x} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n$ je ekvivalentná s podmienkou, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ generujú V. Jednoznačnosť tohto vyjadrenia je zasa ekvivalentná s lineárnou nezávislosťou vektorov $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$.

Teda $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je bázou V vtedy a len vtedy, keď pre každé $\boldsymbol{x} \in V$ existuje práve jedno $\boldsymbol{c} = (c_1, \dots, c_n)^T \in K^n$ také, že

$$\boldsymbol{x} = c_1\boldsymbol{u}_1 + \ldots + c_n\boldsymbol{u}_n = \boldsymbol{\alpha} \cdot \boldsymbol{c}.$$

Tento jednoznačne určený stĺpcový vektor $\boldsymbol{c} \in K^n$ budeme nazývať *súradnice vektora* $\boldsymbol{x}$ *vzhľadom na bázu* $\boldsymbol{\alpha}$ a označovať

$$\boldsymbol{c} = (\boldsymbol{x})_{\boldsymbol{\alpha}}.$$

Teda každá báza $\boldsymbol{\alpha}$ v n-rozmernom vektorovom priestore V definuje *súradnicové zobrazenie* $\boldsymbol{x} \mapsto (\boldsymbol{x})_{\boldsymbol{\alpha}}$ z V do stĺpcového vektorového priestoru K^n.

Jednoduchý dôkaz nasledujúceho tvrdenia prenechávame ako cvičenie čitateľovi.

5.3.2. Tvrdenie. *Nech $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je báza konečnorozmerného vektorového priestoru V. Potom príslušné súradnicové zobrazenie $V \to K^n$ je bijektívne a zachováva lineárne kombinácie, t. j. pre ľubovoľné $a, b \in K$, $\boldsymbol{x}, \boldsymbol{y} \in V$ platí*

$$(a\boldsymbol{x} + b\boldsymbol{y})_{\boldsymbol{\alpha}} = a(\boldsymbol{x})_{\boldsymbol{\alpha}} + b(\boldsymbol{y})_{\boldsymbol{\alpha}}.$$

K nemu inverzné zobrazenie $K^n \to V$ je dané predpisom $\boldsymbol{c} \mapsto \boldsymbol{\alpha} \cdot \boldsymbol{c}$.

V označení posledného tvrdenia teda pre ľubovoľné $\boldsymbol{x} \in V$, $\boldsymbol{c} \in K^n$ platí

$$\boldsymbol{x} = \boldsymbol{\alpha} \cdot (\boldsymbol{x})_{\boldsymbol{\alpha}}, \qquad (\boldsymbol{\alpha} \cdot \boldsymbol{c})_{\boldsymbol{\alpha}} = \boldsymbol{c}.$$

Prvá rovnosť ukazuje, ako možno vektor $\boldsymbol{x}$ zrekonštruovať z danej bázy $\boldsymbol{\alpha}$ a jeho súradníc $(\boldsymbol{x})_{\boldsymbol{\alpha}}$ v tejto báze; druhá zachytáva zrejmý fakt, že súradnice lineárnej kombinácie $\sum_{i=1}^{n} c_i \boldsymbol{u}_i$ v báze $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ tvorí vektor $(c_1, \dots, c_n)^T$.

Práve zavedené súradnice by sme mohli podrobnejšie nazvať *stĺpcovými súradnicami* vzhľadom na danú bázu. Podobným spôsobom možno zaviesť i *riadkové súradnice* a dokázať pre ne analogické tvrdenia ako pre stĺpcové. V takom prípade je samozrejme vhodnejšie zapisovať príslušnú bázu ako stĺpcový vektor $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)^T$ a v prípade riadkového priestoru $V = K^n$ ju stotožniť s maticou s riadkami $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$. Podrobnosti prenechávame na doplnenie čitateľovi.

5.3.3. Príklad. Označme $\boldsymbol{e}_i^{(n)} = \boldsymbol{s}_i(\boldsymbol{I}_n) \in K^n$ stĺpcový vektor pozostávajúci zo samých núl, okrem i-tej zložky, ktorá je 1. Potom $\boldsymbol{\varepsilon}^{(n)} = \left(\boldsymbol{e}_1^{(n)}, \dots, \boldsymbol{e}_n^{(n)}\right)$ je báza stĺpcového vektorového priestoru K^n. Nazývame ju *kanonickou bázou* tohto priestoru. Túto bázu možno zrejmým spôsobom stotožniť s jednotkovou maticou $\boldsymbol{I}_n$. Pokiaľ nebude hroziť nedorozumenie, budeme horný index (n) vynechávať a príslušnú bázu označovať stručne $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$. Pre ľubovoľný vektor $\boldsymbol{x} = (x_1, \dots, x_n)^T \in K^n$ platí

$$\boldsymbol{x} = x_1\boldsymbol{e}_1 + \ldots + x_n\boldsymbol{e}_n,$$

preto $(\boldsymbol{x})_{\boldsymbol{\varepsilon}} = \boldsymbol{x}$, t. j. každý vektor $\boldsymbol{x} \in K^n$ splýva so svojimi vlastnými súradnicami v kanonickej báze.

Kanonická báza riadkového vektorového priestoru K^n je tvorená riadkami jednotkovej matice $\boldsymbol{I}_n$ a značíme ju rovnako ako v predchádzajúcom prípade $\boldsymbol{\varepsilon}^{(n)} = \left(\boldsymbol{e}_1^{(n)}, \dots, \boldsymbol{e}_n^{(n)}\right)^T$ alebo stručne $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)^T$, len s tým rozdielom, že $\boldsymbol{\varepsilon}^{(n)} = \boldsymbol{\varepsilon}$ je teraz stĺpec vektorov a každé $\boldsymbol{e}_i$ je riadok pozostávajúci zo samých núl, okrem i-teho miesta, ktoré je 1.

V predošlom príklade je, okrem iného, zahrnutý aj dôkaz nasledujúceho očakávaného výsledku.

5.3.4. Veta. *Pre ľubovoľné $n \in \mathbb{N}$ platí* $\dim K^n = n$.

5.3.5. Príklad. Stĺpce matice

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

tvoria bázu $\boldsymbol{\alpha}$ (stĺpcového) vektorového priestoru K^4 (presvedčte sa o tom s využitím tvrdenia 5.2.3. a vety 5.3.4. Súradnice vektora $\boldsymbol{x} = (x_1, x_2, x_3, x_4)^T \in K^n$ v báze $\boldsymbol{\alpha}$ sú dané vzťahom

$$(\boldsymbol{x})_{\boldsymbol{\alpha}} = (x_4, x_3 - x_4, x_2 - x_3, x_1 - x_2)^T.$$

Platí totiž

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = x_4 \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + (x_3 - x_4) \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} + (x_2 - x_3) \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + (x_1 - x_2) \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Overte.

5.3.6. Príklad. Označme $\boldsymbol{\xi}^{(n)} = (1, x, \dots, x^n)$ usporiadanú $(n+1)$-ticu prvých $n + 1$ mocnín premennej x. Ľahko nahliadneme, že $\boldsymbol{\xi}^{(n)}$ je báza vektorového priestoru $K^{(n)}[x]$ všetkých polynómov stupňa $\leq n$ v premennej x nad poľom K. Súradnice polynómu $f(x) = \sum_{i=0}^{n} a_i x^i$ v tejto báze tvorí vektor

$$(f)_{\boldsymbol{\xi}^{(n)}} = (a_0, a_1, \dots, a_n)^T \in K^{n+1}.$$

Teda $\dim K^{(n)}[x] = n + 1$. Na druhej strane vektorový priestor $K[x]$ všetkých polynómov v premennej x nad poľom K zrejme nie je konečnorozmerný, teda $\dim K[x] = \infty$.

5.3.7. Príklad. Nech $m, n \in \mathbb{N}$. Pre ľubovoľné $1 \leq k \leq m$, $1 \leq l \leq n$ označme $\boldsymbol{E}_{kl}^{(m,n)} = \boldsymbol{E}_{kl} = (\delta_{ik}\delta_{jl})_{m \times n}$ maticu typu $m \times n$ nad poľom K, pozostávajúcu zo samých núl, okrem miesta (k,l), na ktorom je 1. Zrejme každú maticu $\boldsymbol{A} = (a_{kl}) \in K^{m\times n}$ možno jednoznačne vyjadriť v tvare

$$\boldsymbol{A} = \sum_{k=1}^{m}\sum_{l=1}^{n} a_{kl}\boldsymbol{E}_{kl},$$

z čoho vyplýva, že matice $\boldsymbol{E}_{kl}^{(m,n)}$, $1 \le k \le m$, $1 \le l \le n$, tvoria bázu vektorového priestoru $K^{m\times n}$ všetkých matíc typu $m \times n$ nad poľom K. Jej špeciálnym prípadom je kanonická báza $\boldsymbol{\varepsilon}^{(n)}$ v priestore K^n. Dostávame tak ďalší očakávaný vzťah: $\dim K^{m\times n} = mn$.

5.3.8. Príklad. Pole $\mathbb{C}$ všetkých komplexných čísel je rozšírením poľa $\mathbb{R}$ všetkých reálnych čísel. Teda $\mathbb{C}$ možno považovať za vektorový priestor nad poľom $\mathbb{R}$ (príklad 1.6.1). Každé komplexné číslo z možno jednoznačne vyjadriť v tvare

$$z = a + b\mathrm{i} = a1 + b\mathrm{i},$$

kde $a = \operatorname{Re} z$, $b = \operatorname{Im} z$ sú reálne čísla, nazývané *reálna* resp. *imaginárna časť* komplexného čísla z, a i je *imaginárna jednotka.* To znamená, že komplexné čísla (t. j. vektory) $1, \mathrm{i}$ tvoria bázu vektorového priestoru $\mathbb{C}$ nad poľom $\mathbb{R}$. Súradnicové zobrazenie vzhľadom na túto bázu je dané vzťahom

$$(z)_{(1,\mathrm{i})} = \begin{pmatrix} \operatorname{Re} z \\ \operatorname{Im} z \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(z+\bar z) \\ \frac{1}{2\mathrm{i}}(z-\bar z) \end{pmatrix},$$

kde $\bar z = a - b\mathrm{i}$ je číslo *komplexne združené* k číslu $z = a + b\mathrm{i}$. Teda $\dim_{\mathbb{R}} \mathbb{C} = 2$. Na druhej strane každé pole K, uvažované ako vektorový priestor nad sebou samým má dimenziu 1, t. j. $\dim_K K = 1$. Špeciálne $\dim_{\mathbb{R}} \mathbb{R} = 1$ aj $\dim_{\mathbb{C}} \mathbb{C} = 1$.

5.4. Dimenzia prieniku, súčtu a súčinu vektorových priestorov

V tomto paragrafe preskúmame niektoré základné vlastnosti dimenzie, uvažovanej ako zobrazenie definované na všetkých vektorových priestoroch nad pevným poľom K.

Na začiatok si uvedomme, že ľubovoľný lineárny podpriestor S vektorového priestoru V je i sám vektorovým priestorom nad tým istým poľom, teda pojmy ako báza podpriestoru S a dimenzia podpriestoru S majú dobre definovaný význam. Zrejme každý podpriestor konečnorozmerného vektorového priestoru je i sám konečnorozmerný.

5.4.1. Veta. *Nech S, $T \subseteq V$ sú konečnorozmerné lineárne podpriestory vektorového priestoru V. Potom*

$$\dim(S+T) = \dim S + \dim T - \dim(S \cap T).$$

Dôkaz. Označme $\dim S = m$, $\dim T = n$, $\dim(S \cap T) = k$. Nech $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ je báza podpriestoru $S \cap T$. Doplňme túto bázu do bázy $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$, $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{m-k}$ podpriestoru S, a taktiež do bázy $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-k}$ podpriestoru T. Dokážeme, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$, $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{m-k}$, $\boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-k}$ tvoria bázu podpriestoru $S+T$. Tým budeme hotoví, lebo potom naozaj platí

$$\begin{aligned}\dim(S+T) &= k + (m-k) + (n-k) = m + n - k \\ &= \dim S + \dim T - \dim(S \cap T).\end{aligned}$$

Keďže vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$, $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{m-k}$, $\boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-k}$ zrejme generujú podpriestor $S+T$ (premyslite si detaily), zostáva dokázať, že sú tiež lineárne nezávislé. Nech $a_1, \dots, a_k$, $b_1, \dots, b_{m-k}$, $c_1, \dots, c_{n-k}$ sú skaláry také, že

$$a_1\boldsymbol{u}_1 + \ldots + a_k\boldsymbol{u}_k + b_1\boldsymbol{v}_1 + \ldots + b_{m-k}\boldsymbol{v}_{m-k} + c_1\boldsymbol{w}_1 + \ldots + c_{n-k}\boldsymbol{w}_{m-k} = \mathbf{0}.$$

Potom

$$a_1\boldsymbol{u}_1 + \ldots + a_k\boldsymbol{u}_k + b_1\boldsymbol{v}_1 + \ldots + b_{m-k}\boldsymbol{v}_{m-k} = -(c_1\boldsymbol{w}_1 + \ldots + c_{n-k}\boldsymbol{w}_{m-k}),$$

pričom vektor na ľavej strane patrí do S a vektor na pravej do T. Túto spoločnú hodnotu $\boldsymbol{z} \in S \cap T$ možno vyjadriť ako lineárnu kombináciu len vektorov $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$. Z jednoznačnosti vyjadrenia $\boldsymbol{z}$ v báze $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m-k}$ podpriestoru S tak dostávame $b_1 = \ldots = b_{m-k} = 0$. Preto

$$a_1\boldsymbol{u}_1 + \ldots + a_k\boldsymbol{u}_k + c_1\boldsymbol{w}_1 + \ldots + c_{m-k}\boldsymbol{w}_{n-k} = \mathbf{0}.$$

Z lineárnej nezávislosti bázy $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$, $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-k}$ podpriestoru T potom vyplýva $a_1 = \ldots = a_k = 0$, $c_1 = \ldots = c_{n-k} = 0$. Teda $\boldsymbol{u}_1, \ldots,$ $\boldsymbol{u}_k$, $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{m-k}$, $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{n-k}$ sú lineárne nezávislé vektory.

5.4.2. Dôsledok. *Nech S, T sú lineárne podpriestory vektorového priestoru V. Potom $S \cap T = \{\mathbf{0}\}$, t. j. súčet $S + T$ je direktný, práve vtedy, keď*

$$\dim(S + T) = \dim S + \dim T.$$

Práve dokázané vzťahy pre dimenzie konečnorozmerných podpriestorov nejakého vektorového priestoru nápadne pripomínajú vzťah

$$\#\,(X \cup Y) = \#\,X + \#\,Y - \#\,(X \cap Y)$$

pre počty prvkov konečných množín z paragrafu 0.2, ktorý sa v prípade disjunktných množín redukuje na rovnosť

$$\#\,(X \cup Y) = \#\,X + \#\,Y.$$

To znamená, že konečnorozmerné vektorové priestory (hoci v typickom prípade priestorov nenulovej dimenzie nad nekonečným poľom ide o nekonečné množiny) sa správajú do značnej miery podobne ako konečné množiny. Dimenzia $\dim V$ konečnorozmerného priestoru V je tak akousi mierou jeho „veľkosti", podobne ako počet prvkov $\# X$ je mierou veľkosti konečnej množiny X. Direktný (priamy) súčet lineárnych podpriestorov je tak analógiou zjednotenia disjunktných množín.

Na rozdiel od multiplikatívneho charakteru počtu prvkov karteziánskeho súčinu konečných množín, ktorý je daný formulou

$$\#(X \times Y) = \# X \cdot \# Y,$$

sa však dimenzia priameho súčinu konečnorozmerných vektorových priestorov (pozri príklad 1.6.4) správa aditívne, t. j. do značnej miery podobne ako logaritmus.

5.4.3. Tvrdenie. *Nech V, W sú konečnorozmerné vektorové priestory nad poľom K. Potom pre dimenziu ich priameho súčinu platí*

$$\dim(V \times W) = \dim V + \dim W.$$

Dôkaz. Nech $\boldsymbol{v}_1, \dots, \boldsymbol{v}_m$ je báza priestoru V a $\boldsymbol{w}_1, \dots, \boldsymbol{w}_n$ je báza priestoru W. Stačí overiť, že vektory $(\boldsymbol{v}_1, \mathbf{0}), \dots, (\boldsymbol{v}_m, \mathbf{0}), (\mathbf{0}, \boldsymbol{w}_1), \dots, (\mathbf{0}, \boldsymbol{w}_n)$ tvoria bázu priameho súčinu $V \times W$. Podrobnosti prenechávame čitateľovi.

V dôsledku toho pre konečnorozmerné priestory $V_1, \dots, V_k$ nad poľom K platí

$$\dim(V_1 \times \ldots \times V_k) = \dim V_1 + \ldots + \dim V_k,$$

a pre k-tu priamu mocninu V^k priestoru V máme

$$\dim V^k = k \dim V.$$

Poznámka. Ak obvyklým spôsobom rozšírime aritmetiku prirodzených čísel aj na symbol ∞, t. j. položíme $n + \infty = \infty + n = \infty + \infty = \infty$ pre $n \in \mathbb{N}$, $0 \cdot \infty = \infty \cdot 0 = 0$ a $n \cdot \infty = \infty \cdot n = \infty \cdot \infty = \infty$ pre $n > 0$, ľahko nahliadneme, že vzťahy dokázané v tomto paragrafe zostávajú v platnosti aj pre nekonečnorozmerné priestory.

5.5. Usporiadané a neusporiadané bázy

Ak $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je báza vektorového priestoru V, tak $(\boldsymbol{u}_{\sigma(1)}, \dots, \boldsymbol{u}_{\sigma(n)})$ je tiež báza V pre ľubovoľnú premutáciou σ množiny $\{1, \dots, n\}$. Inak povedané, vlastnosť „byť bázou vektorového priestoru" nezávisí od poradia vektorov v báze – nie je to ani tak vlastnosť príslušnej usporiadanej n-tice $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ ako skôr množiny $\{\boldsymbol{u}_1, \dots, \boldsymbol{u}_n\}$. Na druhej strane je rozumné považovať bázy $(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ a $(\boldsymbol{u}_{\sigma(1)}, \dots, \boldsymbol{u}_{\sigma(n)})$, kde σ je neidentická permutácia, za rôzne. Prislúchajú im totiž rôzne súradnicové zobrazenia. Napr. $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$, $\boldsymbol{\eta} = (\boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_1)$ sú bázy stĺpcového priestoru K^3, líšiace sa len poradím svojich vektorov. Pre súradnice ľubovoľného vektora $\boldsymbol{x} = (x_1, x_2, x_3)^T \in K^3$ v týchto bázach však platí:

$$(\boldsymbol{x})_{\boldsymbol{\varepsilon}} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \qquad (\boldsymbol{x})_{\boldsymbol{\eta}} = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}.$$

Teda $(\boldsymbol{x})_{\boldsymbol{\varepsilon}} \neq (\boldsymbol{x})_{\boldsymbol{\eta}}$, okrem prípadu, keď $x_1 = x_2 = x_3$.

Doteraz študované bázy by sme vlastne mali presnejšie nazývať *konečnými usporiadanými bázami*. To naznačuje možnosti uvažovať jednak o nekonečných, jednak o „neusporiadaných" bázach. Keďže v centre nášho záujmu naďalej zostávajú iba konečnorozmerné priestory, oboch týchto otázok sa len letmo dotkneme.

Hovoríme, že nekonečná postupnosť $(\boldsymbol{u}_k)_{k=0}^{\infty} = (\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2, \dots, \boldsymbol{u}_k, \dots)$ je *báza*, presnejšie *usporiadaná báza* vektorového priestoru V, ak je lineárne nezávislá a generuje celý priestor V.

Treba zdôrazniť, že podmienka generovania priestoru V hovorí, že každý vektor $\boldsymbol{x} \in V$ možno vyjadriť ako *konečnú* lineárnu kombináciu $\boldsymbol{x} = \sum_{k=0}^{n} c_k \boldsymbol{u}_k$, kde $n \in \mathbb{N}$ a $c_0, \dots, c_n \in K$, prvkov príslušnej bázy. „Nekonečné lineárne kombinácie" tvaru $\sum_{k=0}^{\infty} c_k \boldsymbol{u}_k$ sme zatiaľ nedefinovali a len samotná algebraická štruktúra vektorého priestoru nám to vo všeobecnosti ani neumožňuje.

Nasledujúce tvrdenie, ktorého dôkaz neuvádzame, je obdobou vety 5.3.1.

5.5.1. Tvrdenie. *Postupnosť vektorov $(\boldsymbol{u}_k)_{k=0}^{\infty}$ je bázou vektorového priestoru V práve vtedy, keď každý vektor $\boldsymbol{x} \in V$ možno jednoznačne až na nulové členy vyjadriť v tvare lineárnej kombinácie*

$$\boldsymbol{x} = c_0 \boldsymbol{u}_0 + c_1 \boldsymbol{u}_1 + \ldots + c_n \boldsymbol{u}_n,$$

kde $n \in \mathbb{N}$ a $c_0, c_1, \dots, c_n \in K$.

Uvedomme si podstatnosť vsuvky „až na nulové členy". Vzhľadom na premennú hodnotu n dĺžky príslušnej lineárnej kombinácie možno napr. vektor $\boldsymbol{u}_0 - \boldsymbol{u}_1 \in V$ písať aj v tvare $\boldsymbol{u}_0 - \boldsymbol{u}_1 + 0\boldsymbol{u}_2 + 0\boldsymbol{u}_3$ a pod.

Na druhej strane, pri danej báze $\boldsymbol{\alpha} = (\boldsymbol{u}_k)_{k=0}^{\infty}$ priestoru V každý vektor $\boldsymbol{x} \in V$ jednoznačne určuje postupnosť skalárov $(c_k)_{k=0}^{\infty} \in K^{\mathbb{N}}$ takú, že $c_k = 0$ pre všetky k až na konečný počet, t. j. $(c_k)_{k=0}^{\infty} \in K^{(\mathbb{N})}$ (pozri príklad 4.1.3. (a)), a platí

$$\boldsymbol{x} = \sum_{k=0}^{\infty} c_k \boldsymbol{u}_k.$$

Všimnite si, že takéto lineárne kombinácie obsahujú len konečne mnoho nenulových sčítancov, takže s ich definíciou nie je žiaden problém. Uvedenú postupnosť $(c_k)_{k=0}^{\infty}$ potom nazývame *súradnicami vektora* $\boldsymbol{x}$ *vzhľadom na bázu* $\boldsymbol{\alpha}$ a označujeme ju $(\boldsymbol{x})_{\boldsymbol{\alpha}}$. (Vzhľadom na to, že nemienime ďalej rozvíjať príslušnú teóriu pre nekonečnorozmerné priestory, nemá zmysel bližšie špecifikovať, či tým mienime „riadkovú“ alebo „stĺpcovú“ postupnosť $(c_k)_{k=0}^{\infty}$.)

5.5.2. Príklad. Postupnosť $\boldsymbol{\xi} = (x^n)_{n=0}^{\infty} = (1, x, x^2, \dots, x^n, \dots)$ všetkých mocnín premennej x je bázou priestoru $K[x]$ všetkých polynómov v premennej x nad poľom K. (Presvedčte sa o tom.) Súradnicami polynómu

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n = \sum_{i=0}^{n} a_i x^i \in K[x]$$

v tejto báze je postupnosť

$$(f)_{\boldsymbol{\xi}} = (a_0, a_1, \dots, a_n, 0, 0, \dots) \in K^{(\mathbb{N})}.$$

Podmnožinu X vektorového priestoru V nazývame *bázou*, presnejšie *neusporiadanou bázou* priestoru V, ak X je lineárne nezávislá a $[X] = V$. Používa sa tiež názov *Hamelova báza*.

Aj v prípade Hamelových báz platí obdoba tvrdení 5.3.1. a 5.5.1., čo umožňuje zaviesť na priestore V s takouto bázou súradnicové zobrazenie $V \to K^{(X)}$ (pripomíname, že $K^{(X)}$ označuje vektorový priestor všetkých zobrazení $f : X \to K$ takých, že $f(\boldsymbol{x}) = 0$ pre všetky $\boldsymbol{x} \in X$ až na konečný počet – pozri príklad 4.1.3.). *Súradnicami vektora $\boldsymbol{v} \in V$ vzhľadom na bázu X* nazývame jednoznačne určené zobrazenie $f \in K^{(X)}$, pre ktoré platí

$$\boldsymbol{v} = \sum_{\boldsymbol{x} \in X} f(\boldsymbol{x})\boldsymbol{x}.$$

(Vzhľadom na konečný počet nenulových sčítancov je uvedená lineárna kombinácia dobre definovaná.) I tieto súradnice označujeme obvyklým spôsobom $(\boldsymbol{v})_X = f$.

Zostáva otázka, či aj každý nekonečnorozmerný vektorový priestor má bázu, podobne ako konečnorozmerné priestory resp. nekonečnorozmerné priestory polynómov $K[x]$. Inak povedané, radi by sme vedieť, či vôbec každý vektorový priestor má bázu. Na základe základných axióm teórie množín nemožno na túto otázku odpovedať. Až prijatie tzv. *axiómy výberu*, postulujúcej platnosť istého princípu platného pre konečné množiny aj pre nekonečné množiny, nám umožňuje dať na uvedenú otázku kladnú odpoveď. Teda za predpokladu axiómy výberu má každý vektorový priestor nad ľubovoľným poľom Hamelovu bázu. Na druhej strane pre väčšinu nekonečnorozmerných priestorov nám toto tvrdenie zaručuje skutočne len existenciu takejto bázy a nič viac. Nedáva nám nijakú konkrétnu bázu ani návod ako ju zostrojiť.

K príkladom vektorových priestorov, v ktorých nevieme nijako rozumne popísať Hamelovu bázu, hoci jej existenciu máme zaručenú, patria priestory K^X, kde X je nekonečná množina, priestor $\mathcal{C}\langle a, b\rangle$ všetkých spojitých funkcií z netriviálneho uzavretého intervalu $\langle a, b\rangle$ do množiny $\mathbb{R}$, no taktiež polia $\mathbb{R}$ či $\mathbb{C}$ uvažované ako vektorové priestory nad poľom

$\mathbb{Q}$. Nie je to však až taká chyba, lebo v mnohých nekonečnorozmerných priestoroch študovaných vo funkcionálnej analýze sú užitočnejšie iné typy „báz“, umožňujúce vyjadrovať vektory z priestoru napr. v tvare istých „nekonečných lineárnych kombinácií“ $\sum_{n=0}^{\infty} c_n \boldsymbol{x}_n$ prvkov „bázy“.

5.6. Fyzika v n-rozmernom priestore*

Na záver kapitoly si dovolíme jedno odbočenie od hlavnej témy. Keď sa už toľko bavíme o dimenzii, môžeme spolu trochu porozmýšľať, ako sa trojrozmernosť „nášho“ priestoru prejavuje v matematickej podobe niektorých fyzikálnych zákonov. Na základe toho sa pokúsime o extrapoláciu týchto zákonov za hranice trojrozmerného priestoru. Inak povedané, podnikneme spolu metafyzikálny (nie metafyzický) myšlienkový experiment, v ktorom sa pokúsime trochu pošpekulovať nad otázkou, ako by asi mohla vyzerať „fyzika v n-rozmernom priestore“. Samozrejme, nie je jasné, či by pre $n \neq 3$ v n-rozmernom priestore mohli existovať vôbec nejakí „fyzici“, t. j. či by tú „fyziku“ mal kto pestovať. Touto otázkou sa však zaoberať nebudeme, hoci naše úvahy nám aj na ňu naznačia istú odpoveď. Ale nebudeme predbiehať.

Ak sa len trochu hlbšie zamyslíme nad charakterom priestoru, do ktorého sme nevdojak vrhnutí, uvedomíme si, že je plný záhad. Je konečný (ohraničený) alebo nekonečný (neohraničený)? Je diskrétny (pozostávajúci z akýchsi najmenších, ďalej už nedeliteľných častí) alebo spojitý (súvislý a donekonečna deliteľný)? Keďže skúsenosť nám na tieto otázky nedáva jednoznačnú odpoveď, filozofi sa oddávna pokúšali zodpovedať ich na základe špekulatívnych úvah. Aktuálne nekonečno, či už smerom do diaľky (t. j. smerom k čoraz väčším rozmerom) alebo smerom do hĺbky (t. j. smerom k čoraz menším rozmerom) sa však vymyká našim predstavám. Rovnako problematická je však predstava ohraničeného priestoru ako i predstava akejsi najmenšej, ďalej už nedeliteľnej priestorovej oblasti. Priestor si totiž nepredstavujeme ako súcno, t. j. ako „niečo“, ale ako prázdnu formu, naplnenú súcnami. Za hranicou, ohraničujúcou „celý priestor“, by už nemohlo byť absolútne nič, čo si však nedokážeme predstaviť inak, ako prázdny priestor. Podobne, akákoľvek malá priestorová oblasť, je aspoň myšlienkovo (hoc nie nutne fyzikálne) ďalej deliteľná na menšie časti.

Moderná fyzika sa s podobnými otázkami nevysporadúva nijakou definitívnou odpoveďou. Namiesto toho konštruuje rôzne matematické modely a na ich základe získava predpovede, ktoré možno porovnať s výsledkami experimentov. Tým sa tieto modely čiastočne potvrdzujú alebo falzifikujú. Navyše hypotéza zakriveného priestoru oddeľuje otázky (ne)konečnosti a (ne)ohraničenosti. Zakrivený priestor môže byť (sám v sebe) neohraničený a pritom mať konečný objem. Ale tak, ako zakrivená guľová plocha poukazuje na existenciu trojrozmerného (nezakriveného) priestoru, zakrivený konečne veľký trojrozmerný priestor vyvoláva otázku existencie nejakého viacrozmerného, neohraničeného a nezakriveného priestoru.

My sa však na tomto mieste nemienime zaoberať otázkou konečnosti či nekonečnosti priestoru, či už smerom k čoraz väčším alebo čoraz menším vzdialenostiam. Svoju pozornosť upriamime na omnoho tvrdšiu hranicu priestoru, ktorú predstavuje jeho trojrozmernosť. Na túto hranicu narazíme, keď sa pokúsime uskutočniť štyri rôzne, navzájom kolmé úsečky, vychádzajúce z jedného bodu. Priestor nám také niečo nedovolí. Pritom existencia takýchto úsečiek nevedie nevyhnutne k sporu, ich uskutočneniu nebránia nijaké logické zákony, ale len a len priestor. Aby sme si uvedomili rozdiel medzi priestorovou nepredstaviteľnosťou a logickou nemožnosťou, pokúsime sa vmyslieť do postavenia akýchsi plochých bytostí, obývajúcich dvojrozmerný priestor, t. j. rovinu. V rovine možno uskutočniť len dve rôzne navzájom kolmé úsečky vychádzajúce z daného bodu. Naši „dvojrozmerní ľudkovia“ by si zrejme nevedeli predstaviť tri takéto úsečky, čo pre nás nepredstavuje nijaký problém. Podobne nejaké bytosti, obývajúce n-rozmerný priestor, kde $n \geq 3$, by si asi vedeli predstaviť n navzájom kolmých úsečiek. Teda ich existencia je *logicky možná*.

Vráťme sa však k pôvodnej otázke: ako sa prejavuje trojrozmernosť nášho priestoru v matematickej podobe niektorých fyzikálnych zákonov a akú „fyziku“ by asi objavili „fyzici“ v n-rozmernom priestore.

Samozrejme, nebudeme sa zaoberať uvedenými otázkami v celej ich šírke, len sa pokúsime ilustrovať naznačenú problematiku na príklade Newtonovho gravitačného zákona. Úplne analogicky by sme mohli postupovať i v prípade Coulombovho zákona pre elektrostatickú silu.

Podľa Newtonovho gravitačného zákona centrálne symetrické teleso o hmotnosti M vytvára okolo seba centrálne symetrické gravitačné pole, ktoré na hmotný bod o hmotnosti m vo vzdialenosti r od stredu telesa pôsobí silou

$$F = \varkappa \frac{mM}{r^2},$$

kde $\varkappa$ je gravitačná konštanta, ktorej hodnotu možno stanoviť experimentálne. Gravitačná hmotnosť je priamo definovaná ako miera gravitačného účinku telesa, čo vyjadruje priama úmernosť uvedenej sily hmotnostiam oboch telies. Z centrálnej symetrie gravitačného poľa, ktorá je dôsledkom izotropie (homogenity) priestoru, vyplýva, že uvedená sila závisí len od vzájomnej vzdialenosti oboch telies a nie od ďalších parametrov ich vzájomnej polohy, napr. od smeru. Navyše je rozumné predpokladať, že gravitačná sila bude slabnúť so vzdialenosťou r. Na prvý pohľad však nie je jasné, prečo by mala slabnúť akurát nepriamo úmerne jej druhej mocnine. Ukážeme si, že práve to je dôsledkom trojrozmernosti priestoru. Rovnako oprávnene však možno tvrdiť, že trojrozmernosť priestoru je dôsledkom príslušnej podoby v ňom platného gravitačného zákona.

Gravitačné pole si znázorňujeme geometricky pomocou kriviek nazývaných *siločiary*. Tie majú v prípade centrálne symetrického poľa v izotropnom priestore tvar polpriamok vychádzajúcich zo stredu zdroja. Veľkosť príťažlivej sily pôsobiacej na hmotný bod je (okrem jeho hmotnosti) priamo úmerná hustote týchto siločiar v danom mieste. Keďže na povrchu guľovej plochy s polomerom r, opísanej okolo stredu príťažlivosti je hustota siločiar všade rovnaká, táto hustota klesá so vzdialenosťou r nepriamo úmerne plošnému obsahu povrchu danej guľovej plochy. Tento obsah má hodnotu $4\pi r^2$. To znamená, že veľkosť príťažlivej sily F je nepriamo úmerná druhej mocnine vzdialenosti r.

Pod $(n-1)$-rozmernou sférou rozumieme povrch n-rozmernej gule v n-rozmernom priestore. Ak si jej stred zvolíme za počiatok súradnej sústavy, tak $(n-1)$-rozmernú sféru s polomerom r možno stotožniť s množinou

$$S^{(n-1)}(r) = \{(x_1, \dots, x_n) \in \mathbb{R}^n;\ x_1^2 + \dots + x_n^2 = r^2\}.$$

Veľkosť $(n-1)$-rozmerného povrchu sféry $S^{(n-1)}(r)$ je priamo úmerná mocnine r^{n-1}. Rovnakou úvahou ako v predchádzajúcom odstavci tak možno odvodiť nasledujúci tvar Newtonovho gravitačného zákona v n-rozmernom priestore:

$$F = \varkappa_n \frac{mM}{r^{n-1}},$$

kde $\varkappa_n$ je gravitačná konštanta, M je hmotnosť centrálne symetrického telesa vytvárajúceho príslušné gravitačné pole, m je hmotnosť hmotného bodu a r jeho vzdialenosť od stredu príťažlivosti. Špeciálne si uvedomme, že v jednorozmernom priestore, t. j. na priamke, gravitačná sila nezávisí na vzdialenosti (siločiary sa nemajú kam rozptýliť, ich hustota sa so vzdialenosťou nemení).

Práca, ktorú je potrebné vynaložiť na premiestnenie hmotného bodu s hmotnosťou m zo vzdialenosti $r_1 > 0$ do vzdialenosti $r_2 > r_1$ od stredu príťažlivosti, je daná integrálom

$$A = \int_{r_1}^{r_2} F \,\mathrm{d}\, r = \varkappa_n m M \int_{r_1}^{r_2} r^{1-n} \,\mathrm{d}\, r.$$

Pre jednotlivé hodnoty n dostávame

$$\begin{aligned} A &= \varkappa_1 m M (r_2 - r_1), && \text{ak } n = 1, \\ A &= \varkappa_2 m M \ln \frac{r_2}{r_1}, && \text{ak } n = 2, \\ A &= \varkappa_n \frac{mM}{n-2} \left(\frac{1}{r_1^{n-2}} - \frac{1}{r_2^{n-2}} \right), && \text{ak } n \geq 3. \end{aligned}$$

Ďalšou analýzou uvedených vzťahov (čo už nebudeme robiť) možno zistiť, že pohyb v jedno- a dvojrozmernom priestore, t. j. na priamke a v rovine, by bol nesmierne energeticky náročný. Vymaniť sa z gravitačného poľa daného telesa ($r_2 \to \infty$) by si vyžiadalo nekonečne veľkú energiu. Navyše v rovine je v takomto poli možný len pohyb po kruhových uzavretých orbitách, alebo po neuzavretých orbitách (tvaru ružice), pričom oba typy sú stabilné. Uzavretá dráha prechádzajúca v rôznych vzdialenostiach od stredu príťažlivosti nie je možná. (Prípadom $n = 1$ sa ani nemusíme zaoberať, lebo na priamke jednoducho „nie je dosť miesta“ na pohyb bodu po uzavretej orbite „okolo“ iného bodu – zrážka by bola nevyhnutná.) Gravitačné pôsobenie v n-rozmernom priestore je pre $n \geq 4$ zasa ďaleko od zdroja také slabé a blízko zdroja také silné, že iné uzavreté orbity ako kruhové nie sú možné, a i tie sú nestabilné. Aj tá najmenšia odchýlka od kruhovej dráhy (zapríčinená napr. pôsobením ďalších planét) by spôsobila zmenu kruhovej dráhy na špirálovú (napr. únik Zeme od Slnka alebo pád naň). Nestabilita pre $n = 4$ má špeciálny charakter: za veľmi idealizovaných predpokladov si možno predstaviť prechod z jednej kruhovej orbity na inú v dôsledku dvoch po sebe nasledujúcich presne zladených „drgnutí" v opačných smeroch (pri ktorých sa zachová energia a moment hybnosti). Každopádne však stabilné kruhové orbity sú možné len v dimenziách 2 a 3 a stabilné eliptické orbity len v dimenzii 3.

K podobným efektom by dochádzalo aj pôsobením elektrostatickej sily, pod vplyvom ktorej sa elektróny pohybujú okolo jadra atómu. Dvojrozmerný atóm by bol natoľko stabilný, že by sa vôbec nemohol ionizovať, teda v dvojrozmernom priestore by vôbec nemohlo dochádzať ku vzniku chemických zlúčenín. Vo viac než trojrozmernom priestore by zas nemohli existovať stabilné atómy – pri najmenšej odchýlke by elektrón po špirálovej dráhe z atómu unikol alebo spadol na jadro. Jemnejšia analýza kvantovomechanických javov ukazuje, že pre $n \geq 5$ – aj bez pôsobenia vyvolávajúceho malú odchýlku – by elektróny v obale atómu samovoľne prechádzali na čoraz vzdialenejšie orbity, teda atóm vo viac než štvorrozmernom priestore by sa spontánne ionizoval. Prípad $n = 4$ je opäť singulárny: moment hybnosti obiehajúceho elektrónu by mohol nadobúdať len jedinú pevne stanovenú hodnotu.

Pokiaľ teda uznáme oprávnenosť vykonanej extrapolácie fyzikálnych zákonov trojrozmerného sveta aj na svety iných rozmerov (čo je zrejme najproblematickejšie miesto našich úvah), dochádzame k záveru, že tak stabilné systémy planét obiehajúcich okolo centrálnych hviezd ako aj stabilné a jednako zlučovania schopné atómy pozostávajúce z jadra a elektrónového obalu sú možné len v trojrozmernom priestore.

Cvičenia

5.1. Dokážte tvrdenie 5.2.3. (*Návod*: Použite Stenitzovu vetu 5.1.1. a tvrdenie 5.2.1.)

5.2. Vyberte z daných vektorov bázu vektorového priestoru V nad poľom K (ak je to možné; ak to nie je možné, zdôvodnite prečo):

(a) $K = \mathbb{R}$, $V = \mathbb{R}^3$, $\boldsymbol{x} = (2,2,3)^T$, $\boldsymbol{y} = (-1,0,2)^T$, $\boldsymbol{z} = (0,2,7)^T$, $\boldsymbol{u} = (1,2,7)^T$, $\boldsymbol{v} = (3,2,1)^T$;

(b) $K = \mathbb{C}$, $V = \mathbb{C}^4$, $\boldsymbol{x} = (1,\mathrm{i},1,\mathrm{i})$, $\boldsymbol{y} = (\mathrm{i},1,\mathrm{i},1)$, $\boldsymbol{z} = (1,1,1,1)$, $\boldsymbol{u} = (1,0,0,1)$, $\boldsymbol{v} = (0,\mathrm{i},\mathrm{i},0)$;

(c) $K = \mathbb{Z}_5$, $V = \mathbb{Z}_5^3$, $\boldsymbol{x} = (0,1,2,3)^T$, $\boldsymbol{y} = (1,2,3,4)^T$, $\boldsymbol{z} = (2,1,0,4)^T$, $\boldsymbol{u} = (1,3,0,2)^T$, $\boldsymbol{v} = (3,4,0,1)^T$;

(d) $K = \mathbb{Q}$, $V = \mathbb{Q}^{(3)}[x]$, $f_0(x) = 1$, $f_1(x) = 1 + x$, $f_2(x) = (1+x)^2$, $f_3(x) = (1+x)^3$.

5.3. Doplňte uvedené vektory do bázy vektorového priestoru V nad poľom K (ak je to možné; ak to nie je možné, zdôvodnite prečo):

(a) $K = \mathbb{R}$, $V = \mathbb{R}^{(2)}[x]$, $g(x) = 1 + 2x + 7x^2$, $h(x) = 1 + x$;

(b) $K = \mathbb{C}$, $V = \mathbb{C}^4$, $\boldsymbol{u} = (1+\mathrm{i}, 1-\mathrm{i}, 2, 2\mathrm{i})^T$, $\boldsymbol{v} = (1+3\mathrm{i}, 3-\mathrm{i}, 4+2\mathrm{i}, -2+4\mathrm{i})^T$;

(c) $K = \mathbb{Z}_7$, $V = \mathbb{Z}_7^{(3)}[x]$, $f_0(x) = 5 + 6x + 5x^2 + 6x^3$, $f_1(x) = 6 + 5x + 6x^2 + 5x^3$;

(d) $K = \mathbb{Z}_{11}$, $V = \mathbb{Z}_{11}^{(3)}[x]$, $f_0(x) = 5 + 6x + 5x^2 + 6x^3$, $f_1(x) = 6 + 5x + 6x^2 + 5x^3$.

5.4. V každej z úloh cvičení 5.2 a 5.3 určte dimenziu lineárneho podpriestoru generovaného všetkými danými vektormi.

5.5. Dokážte tvrdenie 5.3.2.

5.6. Podrobne dokážte, že $\boldsymbol{\varepsilon}^{(n)} = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ je báza vektorového priestoru K^n.

5.7. Doplňte vynechané podrobnosti v príklade 5.3.5.

5.8. Dokážte, že uvedená konečná postupnosť vektorov $\boldsymbol{\beta}$ tvorí bázu vektorového priestoru V nad poľom K a nájdite súradnice vektorov $\boldsymbol{x}$, $\boldsymbol{y}$ v tejto báze.

(a) $K = \mathbb{R}$, $V = \mathbb{R}^3$, $\boldsymbol{\beta} = \big((1,2,3)^T, (1,-1,1)^T, (2,1,0)^T\big)$, $\boldsymbol{x} = (1,1,1)^T$, $\boldsymbol{y} = (0,1,-2)^T$;

(b) $K = \mathbb{C}$, $V = \mathbb{C}^{(2)}[z]$, $\boldsymbol{\beta} = (1+\mathrm{i}, 1+\mathrm{i}z, \mathrm{i}-z^2)$, $\boldsymbol{x} = f(z) = z$, $\boldsymbol{y} = g(z) = 1+z^2$;

(c) $K = \mathbb{Z}_2$, $V = \mathbb{Z}_2^4$, $\boldsymbol{\beta} = \big((1,1,0,0)^T, (0,0,1,1)^T, (1,0,0,1)^T, (0,1,1,1)^T\big)$, $\boldsymbol{x} = (1,0,0,0)^T$, $\boldsymbol{y} = (1,1,1,0)^T$;

(d) $K = \mathbb{R}$, $V = \mathbb{C}$, $\boldsymbol{\beta} = (1+\mathrm{i}, 1-\mathrm{i})$, $\boldsymbol{x} = 1$, $\boldsymbol{y} = \mathrm{i}$.

5.9. Dokážte, že vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k, \boldsymbol{v}_1, \dots, \boldsymbol{v}_{m-k}, \boldsymbol{w}_1, \dots, \boldsymbol{w}_{n-k}$ z dôkazu vety 5.4.1. naozaj generujú lineárny podpriestor $S + T$.

5.10. Zovšeobecnite dôsledok 5.4.2. na súčet ľubovoľného konečného počtu lineárnych podpriestorov a dokážte toto zovšeobecnenie.

5.11. Doplňte vynechané podrobnosti v dôkaze tvrdenia 5.4.3.

5.12. Nech $\boldsymbol{A} \in K^{m\times n}$ je matica v stupňovitom tvare. Dokážte, že

(a) jej nenulové riadky tvoria bázu lineárneho podpriestoru $[\boldsymbol{r}_1(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] \subseteq K^{1\times n}$;

(b) jej stĺpce, v ktorých ležia vedúce prvky jej riadkov, tvoria bázu lineárneho podpriestoru

$$[\boldsymbol{s}_1(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})] \subseteq K^{m\times 1}.$$

(c) Odvoďte z (a) a (b), že pre matice v stupňovitom tvare platí

$$\dim[\boldsymbol{r}_1(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] = \dim[\boldsymbol{s}_1(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})].$$

5.13. Nech $\boldsymbol{A}, \boldsymbol{B} \in K^{m\times n}$. Dokážte postupne nasledujúce tvrdenia:

(a) $\boldsymbol{A} \sim \boldsymbol{B} \;\Rightarrow\; [\boldsymbol{r}_1(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] = [\boldsymbol{r}_1(\boldsymbol{B}), \dots, \boldsymbol{r}_m(\boldsymbol{B})]$.

(b) Ak $\boldsymbol{A} \sim \boldsymbol{B}$ a $\boldsymbol{B}$ je navyše v stupňovitom tvare, tak jej nenulové riadky tvoria bázu lineárneho podpriestoru $[\boldsymbol{r}_1(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] \subseteq K^{1\times n}$.

(c) Na základe (b) sformulujte postup, ako možno úpravou vhodnej matice pomocou ERO nájsť k daným (riadkovým) vektorom $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m \in K^n$ nejakú bázu ich lineárneho obalu $[\boldsymbol{x}_1, \dots, \boldsymbol{x}_m]$. Táto báza nie je spravidla (až na veľmi špeciálne prípady) vybraná z vektorov $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$, na druhej strane však možno úpravou príslušnej matice na redukovaný stupňovitý tvar dosiahnuť veľmi jednoduchý a prehľadný tvar tejto bázy.

(d) Riešte analogickú úlohu ako v (c) pre stĺpcové vektory.

5.14. S využitím cvičenia 5.13(b) nanovo dokážte jednoznačnosť redukovaného stupňovitého tvaru danej matice, t. j. pre ľubovoľné matice $\boldsymbol{A}, \boldsymbol{B} \in \boldsymbol{K}^{m\times n}$ v redukovanom stupňovitom tvare platí $\boldsymbol{A} \sim \boldsymbol{B} \Rightarrow \boldsymbol{A} = \boldsymbol{B}$ (porovnaj s cvičením 3.13) (*Návod*: Uvedomte si, že sa stačí obmedziť na matice s nenulovými riadkami, a ďalej postupujte indukciou podľa počtu riadkov m.)

5.15. S použitím cvičenia 5.14 dokážte zosilnenie tvrdenia z cvičenia 5.13 (a) do podoby ekvivalencie, t. j. pre ľubovoľné $\boldsymbol{A}, \boldsymbol{B} \in K^{m\times n}$ platí $\boldsymbol{A} \sim \boldsymbol{B} \;\Leftrightarrow\; [\boldsymbol{r}_1(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] = [\boldsymbol{r}_1(\boldsymbol{B}), \dots, \boldsymbol{r}_m(\boldsymbol{B})]$.

5.16. S využitím výsledkov cvičenia 5.13 nájdite pre uvedené vektory z vektorového priestoru V nad poľom K „čo najjednoduchšiu“ bázu ich lineárneho obalu a doplňte ju (ak treba) do „čo najjednoduchšej“ bázy celého priestoru V:

(a) $K = \mathbb{R}$, $V = \mathbb{R}^4$, $\boldsymbol{x} = (2,0,0,3)$, $\boldsymbol{y} = (4,-1,4,0)$, $\boldsymbol{z} = (2,-1,4,3)$, $\boldsymbol{u} = (-2,2,-8,-9)$;

(b) $K = \mathbb{R}$, $V = \mathbb{R}^4$, $\boldsymbol{x} = (0,0,2,-1)^T$, $\boldsymbol{y} = (3,-1,2,0)^T$, $\boldsymbol{z} = (-3,1,2,-2)^T$, $\boldsymbol{u} = (2,-1,1,-2)^T$;

(c) $K = \mathbb{C}$, $V = \mathbb{C}^3$, $\boldsymbol{x} = (\mathrm{i},1,1+\mathrm{i})$, $\boldsymbol{y} = (1+\mathrm{i},1-\mathrm{i},2)$, $\boldsymbol{z} = (2,-\mathrm{i},3-2\mathrm{i})^T$;

(d) $K = \mathbb{R}$, $V = \mathbb{R}^{(3)}[x]$, $f(x) = 2+x+x^2-x^3$, $g(x) = 2x^2-x^3$, $h(x) = 1-x+2x^2$;

(e) $K = \mathbb{Z}_5$, $V = \mathbb{Z}_5^3$, $\boldsymbol{x} = (2,4,3)$, $\boldsymbol{y} = (0,1,2)$, $\boldsymbol{z} = (4,0,0)$;

(f) $K = \mathbb{Z}_7$, $V = \mathbb{Z}_7^{(2)}[x]$, $f(x) = 2 + 4x + 3x^2$, $g(x) = x + 2x^2$, $h(x) = 4$.

5.17. Nech $q \neq \pm 1$ je ľubovoľné reálne číslo. Pre $k, n \in \mathbb{N}$, $k \leq n$, definujme *q-binomický koeficient* ako výraz

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^{n-1} - 1)\dots(q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\dots(q - 1)}.$$

Špeciálne pre $k = 0$ sa tým myslí $\binom{n}{0}_q = 1$. Pre $k > n$ navyše kladieme $\binom{n}{k}_q = 0$. Potom pre ľubovoľné $k \leq n$ platí:

(a) $\binom{n}{k}_q = \binom{n}{n-k}_q$, (b) $\binom{n}{k} = \lim_{q \to 1} \binom{n}{k}_q$, (c) $\binom{n}{0}_q = \binom{n}{n}_q = 1$,

(d) $\binom{n+1}{k}_q = \binom{n}{k-1}_q + q^k \binom{n}{k}_q = q^{n-k+1} \binom{n}{k-1}_q + \binom{n}{k}_q$, ak $1 \leq k \leq n$.

Dokážte. Rovnosti (c) a (d) sa nazývajú pravidlami *q-Pascalovho trojuholníka* pre q-binomické koeficienty (porovnaj s cvičením 0.18).

5.18. Nech pole K je konečné a má práve q prvkov. Pre $k, n \in \mathbb{N}$ označme $C_q(n, k)$ počet všetkých k-rozmerných lineárnych podpriestorov vektorového priestoru K^n. Dokážte postupne nasledujúce tvrdenia:

(a) Pre ľubovoľné n platí $C_q(n, 0) = C_q(n, n) = 1$ a $C_q(n, k) = 0$ pre $k > n$.

(b) $C_q(n, k)$ sa rovná počtu všetkých matíc $\boldsymbol{A} \in K^{k \times n}$ v redukovanom stupňovitom tvare, ktoré majú všetky riadky nenulové. (*Návod*: Uvažujte K^n ako priestor riadkových vektorov a na základe cvičení 5.13 a 5.14 reprezentujte každý jeho k-rozmerný lineárny podpriestor jednoznačne určenou bázou, ktorej vektory, zapísané ako riadky pod sebou, tvoria maticu v redukovanom stupňovitom tvare.)

(c) Pre $1 \leq k \leq n$ platí $C_q(n+1, k) = C_q(n, k-1) + q^k C_q(n, k)$. To spolu s (a) zabezpečuje, že čísla $C_q(n, k)$ vyhovujú rovnakým podmienkam q-Pascalovho trojuholníka ako q-binomické koeficienty $\binom{n}{k}_q$. (*Návod*: Využite (b); matice $\boldsymbol{A} \in K^{k \times (n+1)}$ v redukovanom stupňovitom tvare s nenulovými riadkami rozdeľte do dvoch skupín podľa toho, či vedúci prvok posledného riadku leží alebo neleží v poslednom stĺpci – ukážte, že prvých je $C_q(n, k-1)$ a druhých $q^k C_q(n, k)$.)

(d) Odvoďte z (a) a (c) rovnosť $C_q(n, k) = \binom{n}{k}_q$ pre všetky $k, n \in \mathbb{N}$.

(e) Koľko k-rozmerných lineárnych podpriestorov majú vektorové priestory $\mathbb{Z}_p^n$ nad poľom $\mathbb{Z}_p$ pre $p = 2, 3, 5, 7$, $n = 0, 1, 2, 3, 4, 5$, $0 \le k \le n$? Zostrojte počiatočné úseky príslušných p-Pascalových trojuholníkov.

5.19. Nech K je pole a $(p_k(x))_{k=0}^{\infty}$ je postupnosť polynómov z $K[x]$ taká, že stupeň polynómu $p_k(x)$ je práve k. Dokážte, že postupnosť $(p_k(x))$ je bázou vektorového priestoru $K[x]$ (využite cvičenie 4.11).

6. Lineárne zobrazenia

Zatiaľ sme sa pri štúdiu lineárnej algebry sústredili zakaždým na štruktúru jedného, izolovaného vektorového priestoru. Doteraz sme si nevybudovali pojmy, ktoré by nám umožnili štúdium vzťahov medzi viacerými vektorovými priestormi. V tejto kapitole hodláme zaplniť túto medzeru. Zavedieme a bližšie preskúmame pojem *lineárneho zobrazenia*, ktorý nám umožní porovnávať štruktúry rôznych vektorových priestorov nad tým istým pevne zvoleným poľom. Voľne povedané, pôjde o zobrazenia medzi vektorovými priestormi, ktoré zachovávajú ich lineárnu štruktúru.

6.1. Lineárne zobrazenia

Nech U, V sú vektorové priestory nad tým istým poľom K. Hovoríme, že $\varphi : V \to U$ je *lineárne zobrazenie*, ak φ zachováva operácie vektorového súčtu a skalárneho násobku, t. j. ak pre ľubovoľné $\boldsymbol{x}, \boldsymbol{y} \in V$, $c \in K$ platí

$$\varphi(\boldsymbol{x} + \boldsymbol{y}) = \varphi(\boldsymbol{x}) + \varphi(\boldsymbol{y}),$$
$$\varphi(c\boldsymbol{x}) = c\varphi(\boldsymbol{x}).$$

Ako cvičenie si dokážte, že lineárne zobrazenia zachovávajú nulu a opačné vektory, t. j. pre lineárne zobrazenie $\varphi : V \to U$ a $\boldsymbol{x} \in V$ platí

$$\varphi(\boldsymbol{0}) = \boldsymbol{0}, \qquad \varphi(-\boldsymbol{x}) = -\varphi(\boldsymbol{x}).$$

Zrejme pre každý vektorový priestor V identita $\mathrm{id}_V : V \to V$ je lineárne zobrazenie. Taktiež pre ľubovoľné vektorové priestory U, V nad poľom K zobrazenie $\mathbf{0} : V \to U$, ktoré každému vektoru $\boldsymbol{x} \in V$ priradí nulový vektor $\mathbf{0} \in U$, je lineárne. Komutatívnosť operácie súčinu v poli a jeho distributívnosť vzhľadom na sčítanie znamená, že pre ľubovoľný pevný skalár $a \in K$ je priradením $x \mapsto ax$ definované lineárne zobrazenie $K \to K$. Čoskoro sa zoznámime aj s menej triviálnymi príkladmi lineárnych zobrazení.

No zatiaľ si ešte všimnime jednu odlišnosť v použití názvu „lineárne zobrazenie" v lineárnej algebre oproti matematickej analýze, kde sa pod lineárnou funkciou $\mathbb{R} \to \mathbb{R}$ rozumie ľubovoľná funkcia tvaru $f(x) = ax + b$, kde $a, b \in \mathbb{R}$. Ľahko sa možno presvedčiť, že takéto $f : \mathbb{R} \to \mathbb{R}$ je lineárne zobrazenie v zmysle našej definície práve vtedy, keď $b = 0$. Neskôr zavedieme širšiu triedu zobrazení medzi vektorovými priestormi, ktorá zahŕňa aj takéto „v zmysle matematickej analýzy lineárne" zobrazenia.

Lineárne zobrazenia možno charakterizovať ako zobrazenia medzi vektorovými priestormi (nad tým istým poľom), ktoré zachovávajú lineárne kombinácie. Jednoduchý dôkaz tohto pozorovania prenechávame čitateľovi. (*Návod*: Pozrite sa na dôkaz tvrdenia 4.1.2.)

6.1.1. Tvrdenie. *Nech U, V sú vektorové priestory nad poľom K a $\varphi : V \to U$ je ľubovoľné zobrazenie. Nasledujúce podmienky sú ekvivalentné:*

(i) *φ je lineárne zobrazenie;*

(ii) *pre všetky $\boldsymbol{x}, \boldsymbol{y} \in V$, $a, b \in K$ platí $\varphi(a\boldsymbol{x} + b\boldsymbol{y}) = a\varphi(\boldsymbol{x}) + b\varphi(\boldsymbol{y})$;*

(iii) *pre ľubovoľné $n \in \mathbb{N}$ a všetky $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n \in V$, $c_1, \dots, c_n \in K$ platí $\varphi(c_1\boldsymbol{x}_1 + \ldots + c_n\boldsymbol{x}_n) = c_1\varphi(\boldsymbol{x}_1) + \ldots + c_n\varphi(\boldsymbol{x}_n)$.*

Nasledujúce dve tvrdenia zachytávajú významné vlastnosti lineárnych zobrazení: kompozícia lineárnych zobrazení je opäť lineárne zobrazenie a obrazy i vzory lineárnych podpriestorov v lineárnych zobrazeniach sú tiež lineárnymi podpriestormi.

6.1.2. Tvrdenie. *Nech U, V, W sú vektorové priestory nad poľom K a $\psi: W \to V$, $\varphi: V \to U$ sú lineárne zobrazenia. Potom aj ich kompozícia $\varphi \circ \psi: W \to U$ je lineárne zobrazenie.*

Dôkaz Overíme, že i zložené zobrazenie $\varphi \circ \psi$ zachováva lineárne kombinácie. Nech $\boldsymbol{x}, \boldsymbol{y} \in W$, $a, b \in K$. S využitím linearity zobrazení ψ a φ postupne dostávame

$$\begin{aligned}(\varphi \circ \psi)(a\boldsymbol{x} + b\boldsymbol{y}) = \varphi(\psi(a\boldsymbol{x} + b\boldsymbol{y})) &= \varphi(a\psi\boldsymbol{x} + b\psi\boldsymbol{y}) \\ &= a\varphi(\psi\boldsymbol{x}) + b\varphi(\psi\boldsymbol{y}) = a(\varphi \circ \psi)(\boldsymbol{x}) + b(\varphi \circ \psi)(\boldsymbol{y}).\end{aligned}$$

Podľa tvrdenia 6.1.1. to znamená, že zobrazenie $\varphi \circ \psi$ je lineárne.

6.1.3. Tvrdenie. *Nech U, V sú vektorové priestory nad poľom K a $\varphi: V \to U$ je lineárne zobrazenie.*

(a) *Ak S je lineárny podpriestor priestoru V, tak $\varphi(S)$ je lineárny podpriestor priestoru U.*

(b) *Ak T je lineárny podpriestor priestoru U, tak $\varphi^{-1}(T)$ je lineárny podpriestor priestoru V.*

Dôkaz (a) Keďže $\mathbf{0} \in S$, $\mathbf{0} = \varphi(\mathbf{0}) \in \varphi(S)$. Overíme, že obraz $\varphi(S)$ je uzavretý vzhľadom na lineárne kombinácie. Nech $a, b \in K$, $\boldsymbol{u}, \boldsymbol{v} \in \varphi(S)$. Potom existujú $\boldsymbol{x}, \boldsymbol{y} \in S$ také, že

$\boldsymbol{u} = \varphi(\boldsymbol{x})$, $\boldsymbol{v} = \varphi(\boldsymbol{y})$. S využitím linearity φ dostávame:

$$a\boldsymbol{u} + b\boldsymbol{v} = a\varphi(\boldsymbol{x}) + b\varphi(\boldsymbol{y}) = \varphi(a\boldsymbol{x} + b\boldsymbol{y}) \in \varphi(S),$$

lebo $a\boldsymbol{x} + b\boldsymbol{y} \in S$, nakoľko $S \subseteq V$ je lineárny podpriestor.

(b) Keďže $\varphi(\mathbf{0}) = \mathbf{0} \in T$, $\mathbf{0} \in \varphi^{-1}(T)$. Ukážeme, že aj vzor $\varphi^{-1}(T)$ je uzavretý vzhľadom na lineárne kombinácie. Zvoľme $a, b \in K$, $\boldsymbol{x}, \boldsymbol{y} \in \varphi^{-1}(T)$. To znamená, že $\varphi(\boldsymbol{x}), \varphi(\boldsymbol{y}) \in T$. Z linearity φ vyplýva

$$\varphi(a\boldsymbol{x} + b\boldsymbol{y}) = a\varphi(\boldsymbol{x}) + b\varphi(\boldsymbol{y}) \in T,$$

lebo $T \subseteq U$ je lineárny podpriestor. Preto $a\boldsymbol{x} + b\boldsymbol{y} \in \varphi^{-1}(T)$.

6.1.4. Príklad. Nech K je pole. Distributívnosť súčinu matíc vzhľadom na ich súčet a jeho zameniteľnosť s operáciou skalárneho násobku (pozri odstavec 2.2.2) vlastne hovorí, že pre pevné $m, n, p \in \mathbb{N}$ a ľubovoľnú maticu $\boldsymbol{A} \in K^{m\times n}$ je priradením $\boldsymbol{X} \mapsto \boldsymbol{A} \cdot \boldsymbol{X}$ definované lineárne zobrazenie medzi vektorovými priestormi matíc $K^{n\times p} \to K^{m\times p}$. Podobne je priradením $\boldsymbol{Y} \mapsto \boldsymbol{Y} \cdot \boldsymbol{A}$ definované lineárne zobrazenie $K^{p\times m} \to K^{p\times n}$. Špeciálne pre $p = 1$ je takto definované lineárne zobrazenie $\boldsymbol{x} \mapsto \boldsymbol{A} \cdot \boldsymbol{x}$ medzi stĺpcovými vektorovými priestormi $K^n \to K^m$, resp. lineárne zobrazenie $\boldsymbol{y} \mapsto \boldsymbol{y} \cdot \boldsymbol{A}$ medzi riadkovými vektorovými priestormi $K^m \to K^n$. Neskôr uvidíme, že každé lineárne zobrazenie medzi *konečnorozmernými* vektorovými priestormi nad K má „v podstate“ takúto podobu.

6.1.5. Príklad. Nech K je pole. Pre $m, n \in \mathbb{N}$ a pevné $1 \leq i \leq m$, $1 \leq j \leq n$ sú predpismi $\boldsymbol{A} \mapsto \boldsymbol{r}_i(\boldsymbol{A})$, $\boldsymbol{A} \mapsto \boldsymbol{s}_j(\boldsymbol{A})$ definované lineárne zobrazenia $K^{m\times n} \to K^{1\times n}$ resp. $K^{m\times n} \to K^{m\times 1}$. Takisto $\boldsymbol{A} \mapsto \boldsymbol{A}^T$ je lineárne zobrazenie $K^{m\times n} \to K^{n\times m}$.

6.1.6. Príklad. Nech V je vektorový priestor nad poľom K, X je množina a $x \in X$ je pevne zvolený prvok. Pripomeňme, že V^X je vektorový priestor všetkých funkcií $f : X \to V$ (pozri 1.6.5) Dosadenie prvku x do funkcie f, t. j. priradenie $f \mapsto f(x)$, je lineárne zobrazenie $V^X \to V$. Podobne, pre ľubovoľnú podmnožinu $Y \subseteq X$ je zúženie $f \mapsto f \restriction Y$ lineárne zobrazenie $V^X \to V^Y$.

6.1.7. Príklad. Označme V množinu všetkých konvergentných postupností reálnych čísel. Zrejme V je lineárny podpriestor vektorového priestoru $\mathbb{R}^{\mathbb{N}}$ všetkých postupností reálnych čísel. Potom zobrazenie $V \to \mathbb{R}$, ktoré postupnosti $\boldsymbol{a} = (a_n)_{n=0}^{\infty} \in V$ priradí jej limitu $\lim_{n\to\infty} a_n$, je lineárne.

6.1.8. Príklad. (a) Nech $X \subseteq \mathbb{R}$ a V označuje množinu všetkých zobrazení $X \to \mathbb{R}$, ktoré majú v pevne zvolenom *vnútornom* bode a množiny X konečnú deriváciu. Zrejme V je lineárny podpriestor vektorového priestoru $\mathbb{R}^X$. Potom zobrazenie $V \to \mathbb{R}$, ktoré funkcii $f \in V$ priradí jej deriváciu $f'(a)$ v bode a, je lineárne.

(b) Nech $X \subseteq \mathbb{R}$ je ľubovoľný netriviálny interval. Pripomeňme, že $\mathcal{D}(X)$ označuje lineárny podpriestor vektorového priestoru $\mathbb{R}^X$, tvorený všetkými funkciami $f : X \to \mathbb{R}$, ktoré majú v každom bode $x \in X$ konečnú deriváciu (pozri príklad 4.1.3. (c)). Potom derivácia, t. j. priradenie $f \mapsto f'$, je lineárne zobrazenie $\mathcal{D}(X) \to \mathbb{R}^X$.

6.1.9. Príklad. Pre reálne čísla $a < b$ označuje $\mathcal{C}\langle a, b\rangle$ lineárny podpriestor vektorového priestoru $\mathbb{R}^{\langle a,b\rangle}$, tvorený všetkými spojitými funkciami $f : \langle a, b\rangle \to \mathbb{R}$ (pozri príklad 4.1.3. (b)).

(a) Určitý integrál $f \mapsto \int_a^b f(x)\,\mathrm{d}\,x$ je lineárne zobrazenie $\mathcal{C}\langle a, b\rangle \to \mathbb{R}$.

(b) Podobne, na určitý integrál ako funkciu hornej medze, ktorý funkcii $f \in \mathcal{C}\langle a,b\rangle$ priradí jej primitívnu funkciu $F \in \mathcal{C}\langle a,b\rangle$ danú predpisom

$$F(x) = \int_a^x f(t)\,\mathrm{d}\,t, \qquad (a \le x \le b),$$

sa možno dívať ako na lineárne zobrazenie $\mathcal{C}\langle a,b\rangle \to \mathcal{C}\langle a,b\rangle$.

6.2. Jadro a obraz lineárneho zobrazenia

Nech $\varphi : V \to U$ je lineárne zobrazenie medzi vektorovými priestormi nad poľom K. Jeho *jadrom* nazývame množinu

$$\operatorname{Ker}\varphi = \varphi^{-1}(\mathbf{0}) = \{\boldsymbol{x} \in V;\ \varphi(\boldsymbol{x}) = \mathbf{0}\}.$$

Obrazom lineárneho zobrazenia φ nazývame, v zhode s paragrafom 0.3, množinu

$$\operatorname{Im}\varphi = \varphi(V) = \{\varphi(\boldsymbol{x});\ \boldsymbol{x} \in V\}.$$

(Označenie pochádza z anglických slov *kernel* a *image*.)

Keďže $\{\mathbf{0}\}$ je lineárny podpriestor priestoru U a V je lineárny podpriestor priestoru V, ako špeciálny prípad tvrdenia 6.1.3. dostávame nasledujúci výsledok.

6.2.1. Tvrdenie. *Nech $\varphi : V \to U$ je lineárne zobrazenie medzi vektorovými priestormi nad poľom K. Potom $\operatorname{Ker}\varphi$ je lineárny podpriestor priestoru V a $\operatorname{Im}\varphi$ je lineárny podpriestor priestoru U.*

Pomocou pojmov jadra a obrazu možno charakterizovať injektívne resp. surjektívne lineárne zobrazenia.

6.2.2. Veta. *Nech $\varphi : V \to U$ je lineárne zobrazenie. Potom*

(a) φ je injektívne práve vtedy, keď $\operatorname{Ker}\varphi = \{\mathbf{0}\}$;

(b) φ je surjektívne práve vtedy, keď $\operatorname{Im}\varphi = U$.

Dôkaz. (a) Ak φ je injektívne, tak $\mathbf{0} \in V$ je jediný prvok priestoru V, ktorý sa zobrazí na $\mathbf{0} \in U$. Teda $\operatorname{Ker}\varphi = \{\mathbf{0}\}$. Naopak, ak φ nie je injektívne, tak existujú $\boldsymbol{x}, \boldsymbol{y} \in V$ také, že $\boldsymbol{x} \neq \boldsymbol{y}$ a $\varphi(\boldsymbol{x}) = \varphi(\boldsymbol{y})$. Potom $\boldsymbol{x}-\boldsymbol{y} \neq \mathbf{0}$ a $\varphi(\boldsymbol{x}-\boldsymbol{y}) = \varphi(\boldsymbol{x})-\varphi(\boldsymbol{y}) = \mathbf{0}$, teda $\boldsymbol{x}-\boldsymbol{y} \in \operatorname{Ker}\varphi$. Inak povedané, $\operatorname{Ker}\varphi \neq \{\mathbf{0}\}$.

(b) je priamo definícia surjektívnosti.

Treba poznamenať, že zakiaľ časť (b) uvedeného tvrdenia je triviálna a platí aj bez predpokladu linearity zobrazenia φ, o časti (a) to už povedať nemožno. Pre všeobecné zobrazenie $\varphi : V \to U$ by sa totiž mohlo stať, že $\mathbf{0} \in V$ je jediný prvok, ktorý sa zobrazí na $\mathbf{0} \in U$, no φ aj tak nie je injektívne. Stále by totiž mohol existovať nejaký vektor $\mathbf{0} \neq \boldsymbol{u} \in U$ a dva rôzne vektory $\boldsymbol{x}, \boldsymbol{y} \in V$ také, že $\varphi(\boldsymbol{x}) = \boldsymbol{u} = \varphi(\boldsymbol{y})$. Spomínané tvrdenie teda hovorí, že lineárne zobrazenia majú značne homogénnu štruktúru, takže ich injektivitu nemusíme zisťovať „všade" – dá sa rozpoznať už podľa množiny vzorov jediného prvku $\mathbf{0} \in U$.

6.2.3. Veta. *Nech $\varphi : V \to U$ je lineárne zobrazenie, pričom vektorový priestor V je konečnorozmerný. Potom aj $\operatorname{Ker}\varphi$ a $\operatorname{Im}\varphi$ sú konečnorozmerné priestory a platí*

$$\dim V = \dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi.$$

Dôkaz. Stačí dokázať uvedenú rovnosť pre dimenzie, konečný rozmer podpriestorov $\operatorname{Ker}\varphi$ a $\operatorname{Im}\varphi$ je už jej dôsledkom.

Označme $k = \dim \operatorname{Ker}\varphi$, $l = \dim V - k$. Zrejme $l \geq 0$. Nech $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ je nejaká báza priestoru $\operatorname{Ker}\varphi$. Doplňme ju do bázy $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ priestoru V. Potom $\varphi(\boldsymbol{u}_1) = \ldots = \varphi(\boldsymbol{u}_k) = \mathbf{0}$. Dokážeme, že vektory $\varphi(\boldsymbol{v}_1), \ldots, \varphi(\boldsymbol{v}_l)$ tvoria bázu priestoru $\operatorname{Im}\varphi$, z čoho už vyplýva požadovaná rovnosť.

Najprv dokážeme, že vektory $\varphi(\boldsymbol{v}_1), \ldots, \varphi(\boldsymbol{v}_l)$ generujú podpriestor $\operatorname{Im}\varphi \subseteq U$. Každý vektor $\boldsymbol{w} \in \operatorname{Im}\varphi$ možno vyjadriť v tvare $\boldsymbol{w} = \varphi(\boldsymbol{x})$ pre nejaké $\boldsymbol{x} \in V$, ktoré je vhodnou lineárnou kombináciou $\boldsymbol{x} = a_1\boldsymbol{u}_1 + \ldots + a_k\boldsymbol{u}_k + b_1\boldsymbol{v}_1 + \ldots + b_l\boldsymbol{v}_l$ vektorov $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ bázy priestoru V. Potom

$$\begin{aligned}
\boldsymbol{w} = \varphi(\boldsymbol{x}) &= \varphi(a_1\boldsymbol{u}_1 + \ldots + a_k\boldsymbol{u}_k + b_1\boldsymbol{v}_1 + \ldots + b_l\boldsymbol{v}_l) \\
&= a_1\varphi(\boldsymbol{u}_1) + \ldots + a_k\varphi(\boldsymbol{u}_k) + b_1\varphi(\boldsymbol{v}_1) + \ldots + b_l\varphi(\boldsymbol{v}_l) \\
&= b_1\varphi(\boldsymbol{v}_1) + \ldots + b_l\varphi(\boldsymbol{v}_l),
\end{aligned}$$

teda $\boldsymbol{w} \in [\varphi(\boldsymbol{v}_1), \ldots, \varphi(\boldsymbol{v}_l)]$.

Zostáva dokázať lineárnu nezávislosť vektorov $\varphi(\boldsymbol{v}_1), \ldots, \varphi(\boldsymbol{v}_l)$. Nech $c_1, \ldots, c_l$ sú skaláry také, že $c_1\varphi(\boldsymbol{v}_1) + \ldots + c_l\varphi(\boldsymbol{v}_l) = \mathbf{0}$. Potom $\varphi(c_1\boldsymbol{v}_1 + \ldots + c_le\boldsymbol{v}_l) = \mathbf{0}$, teda $c_1e\boldsymbol{v}_1 + \ldots + c_l\boldsymbol{v}_l \in \operatorname{Ker}\varphi$. Preto sa tento vektor musí dať vyjadriť ako lineárna kombinácia $c_1\boldsymbol{v}_1 + \ldots + c_l\boldsymbol{v}_l = d_1\boldsymbol{u}_1 + \ldots + d_k\boldsymbol{u}_k$ vektorov bázy $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k$ podpriestoru $\operatorname{Ker}\varphi$. Z lineárnej nezávislosti bázy $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_l$ priestoru V vyplýva $c_1 = \ldots = c_l = 0 = d_1 = \ldots = d_k$, teda aj nezávislosť vektorov $\varphi(\boldsymbol{v}_1), \ldots, \varphi(\boldsymbol{v}_l)$.

Dimenziu obrazu $\operatorname{Im}\varphi$ nazývame *hodnosťou* lineárneho zobrazenia φ a značíme ju

$$h(\varphi) = \dim \operatorname{Im}\varphi.$$

Lineárne zobrazenie $\varphi: V \to V$ vektorového priestoru V do seba nazývame *lineárnym operátorom* alebo *lineárnou transformáciou*.

Ako sme spomínali v paragrafe 0.5, transformácia $f : X \to X$ konečnej množiny X je injektívna práve vtedy, keď je surjektívna. Ako dôsledok práve dokázanej vety dostávame analogický výsledok aj pre lineárne transformácie konečnorozmerných vektorových priestorov.

6.2.4. Dôsledok. *Nech $\varphi : V \to V$ je lineárna transformácia konečnorozmerného vektorového priestoru V. Potom φ je injektívna práve vtedy, keď je surjektívna.*

Dôkaz. Nech $\dim V = n$. Potom φ je injektívne práve vtedy, keď $\dim \operatorname{Ker} \varphi = 0$, a surjektívne práve vtedy, keď $\dim \operatorname{Im} \varphi = n$. Keďže $\dim \operatorname{Ker} \varphi + \dim \operatorname{Im} \varphi = n$, obe tieto podmienky sú ekvivalenté.

6.3. Lineárne izomorfizmy

Bijektívne lineárne zobrazenie $\varphi : V \to U$ medzi vektorovými priestormi V, U nad tým istým poľom K nazývame *lineárny izomorfizmus*. Hovoríme, že vektorové priestory V, U sú *lineárne izomorfné* alebo len krátko *izomorfné*, označenie $V \cong U$, ak existuje nejaký lineárny izomorfizmus $\varphi : V \to U$.

6.3.1. Tvrdenie. *Nech U, V, W sú vektorové priestory nad poľom K.*

(a) $\mathrm{id}_V : V \to V$ *je lineárny izomorfizmus.*

(b) *Ak $\varphi : V \to U$ je lineárny izomorfizmus, tak aj $\varphi^{-1} : U \to V$ je lineárny izomorfizmus.*

(c) *Ak $\psi : W \to V$, $\varphi : V \to U$ sú lineárne izomorfizmy, tak aj $\varphi \circ \psi : W \to U$ je lineárny izomorfizmus.*

Dôkaz. (a) je triviálne, (c) vyplýva z toho, že kompozícia bijekcií je bijekcia a kompozícia lineárnych zobrazení je lineárne zobrazenie. Zostáva dokázať (b). Treba overiť, že inverzné zobrazenie $\varphi^{-1} : U \to V$ k lineárnej bijekcii $\varphi : V \to U$ je tiež lineárne (jeho bijektívnosť je totiž zrejmá).

Zvoľme $\boldsymbol{u}, \boldsymbol{v} \in U$, $a, b \in K$. Máme dokázať rovnosť

$$\varphi^{-1}(a\boldsymbol{u} + b\boldsymbol{v}) = a\varphi^{-1}(\boldsymbol{u}) + b\varphi^{-1}(\boldsymbol{v}),$$

ktorá je ekvivalentná s podmienkou

$$a\boldsymbol{u} + b\boldsymbol{v} = \varphi\big(a\varphi^{-1}(\boldsymbol{u}) + b\varphi^{-1}(\boldsymbol{v})\big).$$

Vďaka linearite φ a vzťahu $\varphi \circ \varphi^{-1} = \mathrm{id}_U$ naozaj dostávame

$$\varphi\big(a\varphi^{-1}(\boldsymbol{u}) + b\varphi^{-1}(\boldsymbol{v})\big) = a\varphi\varphi^{-1}(\boldsymbol{u}) + b\varphi\varphi^{-1}(\boldsymbol{v}) = a\boldsymbol{u} + b\boldsymbol{v}.$$

Z práve dokázaného tvrdenia okamžite vyplýva nasledujúci dôsledok.

6.3.2. Dôsledok. *Pre vektorové priestory U, V, W nad tým istým poľom platí:*

(a) $V \cong V$;

(b) $V \cong U \;\Rightarrow\; U \cong V$;

(c) $W \cong V \;\&\; V \cong U \;\Rightarrow\; W \cong U$.

Hovoríme, že vzťah izomorfnosti $\cong$ je *reflexívny*, *symetrický* a *tranzitívny*, t. j. je vzťahom *ekvivalencie*. Z formálneho hľadiska s ním teda môžeme narábať podobne ako so vzťahom rovnosti $=$.

Izomorfné vektorové priestory majú rovnakú štruktúru, líšia sa nanajvýš označením svojich prvkov, nie však vzťahmi medzi nimi. Preto ich možno v prípade potreby stotožniť, či nahradiť jeden vektorový priestor jeho izomorfnou kópiou. Z toho dôvodu je dôležité mať k dispozícii vhodnú triedu vektorových priestorov nad daným poľom, ktorá by pre každý vektorový priestor obsahovala nejaký priestor s ním izomorfný.

6.3.3. Príklad. (a) Nech V je konečnorozmerný vektorový priestor nad poľom K, $\dim V = n$ a $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ je nejaká jeho báza. Potom tvrdenie 5.3.2. vlastne hovorí, že súradnicové zobrazenie $\boldsymbol{x} \mapsto (\boldsymbol{x})_{\boldsymbol{\beta}}$ je lineárny izomorfizmus $V \to K^n$.

(b) Podobne možno nahliadnuť, že (i v nekonečnorozmernom prípade) určuje Hamelova báza X vektorového priestoru V súradnicové zobrazenie $\boldsymbol{v} \mapsto (\boldsymbol{v})_X$, ktoré je lineárnym izomorfizmom $V \to K^{(X)}$ (pozri záver paragrafu 5.5).

Na záver tohto paragrafu ešte ukážeme, že typ izomorfizmu daného konečnorozmerného priestoru je jednoznačne určený jeho dimenziou.

6.3.4. Veta. *Nech U, V sú konečnorozmerné vektorové priestory nad poľom K. Potom*

$$V \cong U \iff \dim V = \dim U.$$

Dôkaz. Nech $V \cong U$ a $\varphi : V \to U$ je lineárny izomorfizmus. Potom $\operatorname{Ker}\varphi = \{\mathbf{0}\}$ a $\operatorname{Im}\varphi = U$ Podľa vety 6.2.3. o dimenzii jadra a obrazu

$$\dim V = \dim \operatorname{Ker}\varphi + \dim \operatorname{Im}\varphi = 0 + \dim U = \dim U.$$

Naopak, nech $\dim V = \dim U = n$. Podľa príkladu 6.3.3. (a) platí $V \cong K^n \cong U$.

Teda konečnorozmerný vektorový priestor V nad poľom K je izomorfný so stĺpcovým (no rovnako aj s riadkovým) vektorovým priestorom K^n práve vtedy, keď $n = \dim V$. Pritom každá báza $\boldsymbol{\beta}$ priestoru V určuje jeden takýto izomorfizmus $V \to K^n$ – je ním súradnicové zobrazenie $\boldsymbol{x} \mapsto (\boldsymbol{x})_{\boldsymbol{\beta}}$.

6.4. Matica lineárneho zobrazenia

Uvažujme nejaké lineárne zobrazenie $\varphi : K^n \to K^m$. V priestore K^n máme kanonickú bázu $\boldsymbol{\varepsilon}^{(n)} = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$. Keďže obrazy $\varphi(\boldsymbol{e}_j)$ vektorov tejto bázy sú stĺpcové vektory z priestoru K^m, môžeme vytvoriť maticu

$$\boldsymbol{A} = (\varphi(\boldsymbol{e}_1), \ldots, \varphi(\boldsymbol{e}_n)) \in K^{m \times n},$$

ktorej stĺpcami sú práve tieto vektory, t. j. platí $\boldsymbol{s}_j(\boldsymbol{A}) = \varphi(\boldsymbol{e}_j)$ pre $1 \leq j \leq n$. Ukážeme, ako možno obraz $\varphi(\boldsymbol{x})$ ľubovoľného vektora $\boldsymbol{x} = (x_1, \ldots, x_n)^T \in K^n$ vypočítať len zo znalosti tejto matice. Uvedomme si, že $\boldsymbol{x} = x_1\boldsymbol{e}_1 + \cdots + x_n\boldsymbol{e}_n$, a počítajme

$$\begin{aligned} \varphi(\boldsymbol{x}) &= \varphi(x_1\boldsymbol{e}_1 + \ldots + x_n\boldsymbol{e}_n) = x_1\varphi(\boldsymbol{e}_1) + \ldots + x_n\varphi(\boldsymbol{e}_n) \\ &= (\boldsymbol{s}_1(\boldsymbol{A}), \ldots, \boldsymbol{s}_n(\boldsymbol{A})) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \boldsymbol{A} \cdot \boldsymbol{x} \end{aligned}$$

Teda *každé* lineárne zobrazenie $\varphi : K^n \to K^m$ má tvar $\varphi(\boldsymbol{x}) = \boldsymbol{A} \cdot \boldsymbol{x}$ pre vhodnú maticu $\boldsymbol{A} \in K^{m \times n}$. Keďže každý konečnorozmerný vektorový priestor nad poľom K je izomorfný s priestorom K^n pre $n = \dim V$, pri voľbe pevných báz v konečnorozmerných priestoroch U, V bude možné ľubovoľné lineárne zobrazenie $\varphi : V \to U$ zakódovať pomocou vhodnej matice $\boldsymbol{A}$.

Nech U, V sú konečnorozmerné vektorové priestory nad poľom K, $\dim U = m$, $\dim V = n$ a $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_m)$, $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ sú bázy v U, resp. vo V. *Maticou lineárneho zobrazenia* $\varphi : V \to U$ *vzhľadom na bázy* $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ nazývame maticu

$$\boldsymbol{A} = \big((\varphi \boldsymbol{v}_1)_{\boldsymbol{\alpha}}, \dots, (\varphi \boldsymbol{v}_n)_{\boldsymbol{\alpha}}\big) \in K^{m\times n},$$

ktorej stĺpce sú tvorené súradnicami obrazov $\varphi(\boldsymbol{v}_j)$ vektorov bázy $\boldsymbol{\beta}$ vzhľadom na bázu $\boldsymbol{\alpha}$, t. j. platí $\boldsymbol{s}_j(\boldsymbol{A}) = (\varphi \boldsymbol{v}_j)_{\boldsymbol{\alpha}}$ pre $1 \le j \le n$. Túto maticu značíme tiež

$$\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}.$$

(Všimnite si obrátené poradie znakov báz voči poradiu vektorových priestorov v označení zobrazenia $\varphi : V \to U$.)

Maticu $\boldsymbol{A}$ zo začiatku tohto paragrafu by sme teda mohli nazvať *maticou lineárneho zobrazenia* $\varphi : K^n \to K^m$ *vzhľadom na kanonické bázy* $\boldsymbol{\varepsilon}^{(n)}$, $\boldsymbol{\varepsilon}^{(m)}$. Pokiaľ nepovieme inak, budeme pod maticou lineárneho zobrazenia $\varphi : K^n \to K^m$ medzi stĺpcovými vektorovými priestormi vždy rozumieť maticu $(\varphi)_{\boldsymbol{\varepsilon}^{(m)},\boldsymbol{\varepsilon}^{(n)}}$ zobrazenia φ vzhľadom na kanonické bázy.

Pri štúdiu lineárnych transformácií $\varphi : V \to V$ konečnorozmerného vektorového priestoru V budeme spravidla vzory i obrazy vektorov z V vyjadrovať v tej istej báze. *Maticou lineárnej transformácie* $\varphi : V \to V$ vzhľadom na bázu $\boldsymbol{\alpha}$ priestoru V teda rozumieme maticu

$$(\varphi)_{\boldsymbol{\alpha}} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\alpha}}.$$

Pri dôkaze nasledujúcej vety bude potrebné si uvedomiť, že $(\boldsymbol{v}_j)_{\boldsymbol{\beta}} = \boldsymbol{e}_j^{(n)}$ pre ľubovoľný vektor $\boldsymbol{v}_j$ bázy $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ priestoru V. Z toho je zrejmé, že pre každú bázu $\boldsymbol{\beta}$ n-rozmerného vektorového priestoru V platí

$$(\mathrm{id}_V)_{\boldsymbol{\beta},\boldsymbol{\beta}} = \boldsymbol{I}_n.$$

6.4.1. Veta. *Nech $\varphi : V \to U$ je lineárne zobrazenie medzi konečnorozmernými vektorovými priestormi nad poľom K, $\dim V = n$, $\dim U = m$ a $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ sú bázy priestorov U resp. V. Potom pre všetky $\boldsymbol{x} \in V$ platí*

$$(\varphi \boldsymbol{x})_{\boldsymbol{\alpha}} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}}$$

a $\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je jediná matica s touto vlastnosťou.

Dôkaz. Nech $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$. Zvoľme ľubovoľný vektor $\boldsymbol{x} \in V$ a označme $(\boldsymbol{x})_{\boldsymbol{\beta}} = (x_1, \dots, x_n)^T$, teda $\boldsymbol{x} = x_1 e \boldsymbol{v}_1 + \cdots + x_n \boldsymbol{v}_n$. Podobne ako v špeciálnom prípade zo začiatku tohto paragrafu, i teraz dostávame

$$\begin{aligned}
\varphi(\boldsymbol{x}) &= \varphi(x_1 \boldsymbol{v}_1 + \ldots + x_n \boldsymbol{v}_n) = x_1 \varphi(\boldsymbol{v}_1) + \ldots + x_n \varphi(\boldsymbol{v}_n), \\
(\varphi \boldsymbol{x})_{\boldsymbol{\alpha}} &= \big(x_1 \varphi(\boldsymbol{v}_1) + \ldots + x_n \varphi(\boldsymbol{v}_n)\big)_{\boldsymbol{\alpha}} = x_1 (\varphi \boldsymbol{v}_1)_{\boldsymbol{\alpha}} + \ldots + x_n (\varphi \boldsymbol{v}_n)_{\boldsymbol{\alpha}} \\
&= \big((\varphi \boldsymbol{v}_1)_{\boldsymbol{\alpha}}, \dots, (\varphi \boldsymbol{v}_n)_{\boldsymbol{\alpha}}\big) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}}.
\end{aligned}$$

Zostáva ukázať, že pre ľubovoľnú maticu $\boldsymbol{A} \in K^{m \times n}$ platí

$$\big(\forall\, \boldsymbol{x} \in V\big)\big((\varphi \boldsymbol{x})_{\boldsymbol{\alpha}} = \boldsymbol{A} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}}\big) \;\Rightarrow\; \boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}.$$

Za uvedeného predpokladu voľbou $\boldsymbol{x} = \boldsymbol{v}_j$ dostávame

$$(\varphi \boldsymbol{v}_j)_{\boldsymbol{\alpha}} = \boldsymbol{A} \cdot (\boldsymbol{e} v_j)_{\boldsymbol{\beta}} = \boldsymbol{A} \cdot \boldsymbol{e}_j = \boldsymbol{s}_j(\boldsymbol{A})$$

pre každé $1 \leq j \leq n$. Teda matice $\boldsymbol{A}$ a $(\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ majú rovnaké stĺpce, preto sa rovnajú.

Matica $(\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ lineárneho zobrazenia $\varphi : V \to U$ z n-rozmerného vektorového priestoru V do m-rozmerného vektorového priestoru U nad poľom K vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ je teda medzi všetkými maticami $\boldsymbol{A} \in K^{m \times n}$ jednoznačne určená podmienkou

$$(\varphi \boldsymbol{x})_{\boldsymbol{\alpha}} = \boldsymbol{A} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}}$$

pre každé $\boldsymbol{x} \in V$.

Ďalej si ukážeme, že skladanie lineárnych zobrazení zodpovedá násobeniu matíc, čo umožňuje vypočítať maticu kompozície lineárnych zobrazení $\varphi \circ \psi$ len zo znalosti matíc jednotlivých zobrazení φ a ψ. Tento výsledok definitívne „ospravedlňuje“ spôsob, akým sme súčin matíc definovali v odstavci 2.2.2

6.4.2. Veta. *Nech U, V, W sú konečnorozmerné vektorové priestory nad poľom K, $\boldsymbol{\alpha}$ je báza U, $\boldsymbol{\beta}$ je báza V a $\boldsymbol{\gamma}$ je báza W. Potom pre ľubovoľné lineárne zobrazenia $\psi : W \to V$, $\varphi : V \to U$ platí*

$$(\varphi \circ \psi)_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot (\psi)_{\boldsymbol{\beta},\boldsymbol{\gamma}}.$$

Dôkaz. Označme $\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ maticu lineárneho zobrazenia φ vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ a $\boldsymbol{B} = (\psi)_{\boldsymbol{\beta},\boldsymbol{\gamma}}$ maticu lineárneho zobrazenia ψ vzhľadom na bázy $\boldsymbol{\gamma}$, $\boldsymbol{\beta}$. Dokážeme rovnosť

$$(\varphi \circ \psi)_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = \boldsymbol{A} \cdot \boldsymbol{B}.$$

Na základe definície matíc $\boldsymbol{A}$, $\boldsymbol{B}$ pre ľubovoľné $\boldsymbol{x} \in U$ platí

$$\begin{aligned}\big((\varphi \circ \psi)\boldsymbol{x}\big)_{\boldsymbol{\alpha}} = \big(\varphi(\psi \boldsymbol{x})\big)_{\boldsymbol{\alpha}} &= \boldsymbol{A} \cdot (\psi \boldsymbol{x})_{\boldsymbol{\beta}} \\ &= \boldsymbol{A} \cdot \big(\boldsymbol{B} \cdot (\boldsymbol{x})_{\boldsymbol{\gamma}}\big) = (\boldsymbol{A} \cdot \boldsymbol{B}) \cdot (\boldsymbol{x})_{\boldsymbol{\gamma}}.\end{aligned}$$

Keďže matica kompozície $\varphi \circ \psi$ vzhľadom na bázy $\boldsymbol{\gamma}$, $\boldsymbol{\alpha}$ je podľa vety 6.4.1. touto podmienkou určená jednoznačne, dôkaz je hotový.

V nasledujúcich príkladoch sa zoznámime s niekoľkými dôležitými lineárnymi transformáciami roviny $\mathbb{R}^2$ a ich maticami vzhľadom na kanonickú bázu $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \boldsymbol{e}_2)$.

6.4.3. Príklad. *Otočenie* roviny okolo počiatku o uhol $\alpha \in \mathbb{R}$ je lineárne zobrazenie $\boldsymbol{R}_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$. Homogenita je zrejmá na prvý pohľad. O aditivite sa presvedčíme nasledujúcou úvahou. Ak otočíme rovnobežník vektorov $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^2$ o uhol α, dostaneme tak rovnobežník prislúchajúci vektorom $\boldsymbol{R}_\alpha(\boldsymbol{x}), \boldsymbol{R}_\alpha(\boldsymbol{y})$. Pritom uhlopriečka prvého rovnobežníka prejde na uhlopriečku druhého. Teda $\boldsymbol{R}_\alpha(\boldsymbol{x} + \boldsymbol{y}) = \boldsymbol{R}_\alpha(\boldsymbol{x}) + \boldsymbol{R}_\alpha(\boldsymbol{y})$ (nakreslite si obrázok). Maticu tohto lineárneho zobrazenia vzhľadom na kanonickú bázu $\boldsymbol{\varepsilon}$ budeme značiť rovnako $\boldsymbol{R}_\alpha$, teda pre $\boldsymbol{x} \in \mathbb{R}^2$ budeme písať $\boldsymbol{R}_\alpha(\boldsymbol{x}) = \boldsymbol{R}_\alpha \cdot \boldsymbol{x}$. Jej stĺpce získame otočením vektorov $\boldsymbol{e}_1 = (1, 0)^T$, $\boldsymbol{e}_2 = (0, 1)^T$ o uhol α. Z definície goniometrických funkcií sínus a kosínus pomocou jednotkovej kružnice priamo dostávame

$$\boldsymbol{R}_\alpha \cdot \boldsymbol{e}_1 = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}, \qquad \boldsymbol{R}_\alpha \cdot \boldsymbol{e}_2 = \begin{pmatrix} \cos\left(\frac{\pi}{2} + \alpha\right) \\ \sin\left(\frac{\pi}{2} + \alpha\right) \end{pmatrix} = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}.$$

To znamená, že

$$\boldsymbol{R}_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

a obrazom ľubovoľného vektora $(x, y)^T \in \mathbb{R}^2$ v otočení $\boldsymbol{R}_\alpha$ je vektor

$$\boldsymbol{R}_\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\alpha - y\sin\alpha \\ x\sin\alpha + y\cos\alpha \end{pmatrix}.$$

Na základe znalostí matíc $\boldsymbol{R}_\alpha$ je už jednoduché napísať matice otočení v $\mathbb{R}^3$ okolo súradných osí vzhľadom na kanonickú bázu $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$. Otočenia okolo osí $x = [\boldsymbol{e}_1]$, $y = [\boldsymbol{e}_2]$ resp $z = [\boldsymbol{e}_3]$ o uhol α majú postupne matice

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}, \qquad \begin{pmatrix} \cos\alpha & 0 & \sin\alpha \\ 0 & 1 & 0 \\ -\sin\alpha & 0 & \cos\alpha \end{pmatrix}, \qquad \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Na orientáciu otočení používame *pravidlo pravej ruky*, t. j. prsty pravej ruky ukazujú smer otáčania a palec určuje orientáciu osi: v prvom prípade prsty od vektora $\boldsymbol{e}_2$ k $\boldsymbol{e}_3$ a palec v smere vektora $\boldsymbol{e}_1$, v druhom prsty od $\boldsymbol{e}_3$ k $\boldsymbol{e}_1$ a palec v smere $\boldsymbol{e}_2$, v treťom prsty od $\boldsymbol{e}_1$ k $\boldsymbol{e}_2$ a palec v smere $\boldsymbol{e}_3$.

6.4.4. Príklad. *Osová súmernosť* roviny podľa ľubovoľnej priamky prechádzajúcej počiatkom definuje zobrazenie $\boldsymbol{S}_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$, kde $\alpha \in \mathbb{R}$ je uhol, ktorý zviera os súmernosti s osou x. Obdobnou úvahou ako v prípade otočení možno nahliadnuť, že i $\boldsymbol{S}_\alpha$ je lineárne zobrazenie. Jeho maticu vzhľadom na kanonickú bázu $\boldsymbol{\varepsilon}$ budeme značiť rovnako $\boldsymbol{S}_\alpha$. Zrejme matica súmernosti podľa osi x je

$$\boldsymbol{S}_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

a osovú súmernosť $\boldsymbol{S}_\alpha$ možno dostať ako kompozíciu otočenia $\boldsymbol{R}_{-\alpha}$, osovej súmernosti $\boldsymbol{S}_0$ a otočenia $\boldsymbol{R}_\alpha$, t. j.

$$\boldsymbol{S}_\alpha = \boldsymbol{R}_\alpha \cdot \boldsymbol{S}_0 \cdot \boldsymbol{R}_{-\alpha}.$$

Po vynásobení príslušných matíc z toho s využitím pár trigonometrických vzorcov dostávame

$$\boldsymbol{S}_\alpha = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}.$$

Teda osová súmernosť $\boldsymbol{S}_\alpha$ zobrazí vektor $(x, y)^T \in \mathbb{R}^2$ do vektora

$$\boldsymbol{S}_\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos 2\alpha + y \sin 2\alpha \\ x \sin 2\alpha - y\cos 2\alpha \end{pmatrix}.$$

6.4.5. Príklad. *Rovnoľahlosť* alebo tiež *homotetia* so stredom v počiatku a s koeficientom podobnosti $0 \neq c \in \mathbb{R}$ je opäť lineárne zobrazenie $\mathbb{R}^2 \to \mathbb{R}^2$ s maticou $c\boldsymbol{I}_2 = \operatorname{diag}(c, c)$. Tento príklad možno zrejmým spôsobom zovšeobecniť na ľubovoľnú dimenziu n.

6.4.6. Príklad. *Skosenie v smere osi x s parametrom a.* Pre ľubovoľné $a \in \mathbb{R}$ je priradením

$$\varphi \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + ay \\ y \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

definovaná lineárna transformácia roviny, ktorá posúva každú jej „vodorovnú vrstvu“ $\{(x, y);\ y = s\}$, $s \in \mathbb{R}$, o vektor $as\boldsymbol{e}_1$ (nakreslite si obrázok). Analogické lineárne transformácie fungujú aj vo viacrozmerných priestoroch $\mathbb{R}^n$ ako aj v konečnorozmerných vektorových priestoroch nad ľubovoľným poľom.

6.4.7. Príklad. *Galileova transformácia* „roviny“, alebo skôr „časopriamky“ $\mathbb{R}^2$ je z formálneho hľadiska totožná so skosením v smere priestorovej osi x s parametrom $a = -v$:

$$\begin{aligned} t' &= t \\ x' &= -vt + x, \end{aligned} \qquad \text{t. j.} \qquad \begin{pmatrix} t' \\ x' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -v & 1 \end{pmatrix} \cdot \begin{pmatrix} t \\ x \end{pmatrix}.$$

Ak k týmto rovniciam ešte doplníme $y' = y$, $z' = z$, dostaneme Galileovu transformáciu „časopriestoru“ $\mathbb{R}^4$. Vektor $(t, x, y, z)^T$ interpretujeme ako súradnice času (t) a polohy (x, y, z), ktoré nejakej okamžitej bodovej udalosti v trojrozmernom fyzikálnom priestore priradí pozorovateľ P, a vektor $(t', x', y', z')^T$ ako súradnice, ktoré jej priradí pozorovateľ P', ktorý sa vzhľadom na P pohybuje rovnomerne priamočiaro rýchlosťou v v smere osi x (pričom počiatky ich súradných sústav sú zhodne stanovené okamihom a miestom ich stretnutia, kedy tiež splývajú ich príslušné súradné osi). Galileova transformácia potom udáva vzťah medzi týmito súradnicami, ku ktorému dospejeme na základe princípov klasickej mechaniky. Je v nej zachytený newtonovský princíp absolútneho času a priestoru, rovnakého pre všetkých pozorovateľov nezávisle od ich pohybu, a galileovský princíp relatívnosti pohybu, ktorý sa prejavuje v rovnocennosti súradných sústav ľubovoľných navzájom rovnomerne priamočiaro sa pohybujúcich pozorovateľov. Je známe, že Galileova transformácia sa veľmi dobre zhoduje so skutočnosťou pre rýchlosti v z „bežného života“, ktoré sú malé v porovnaní s rýchlosťou svetla. Pre rýchlosti blízke rýchlosti svetla však stráca svoju platnosť a treba ju nahradiť tzv. Lorentzovou transformáciou, s ktorou sa zoznámime neskôr.

6.5. Priestory lineárnych zobrazení

Nech U, V sú vektorové priestory nad poľom K. Ak zabudneme na štruktúru vektorového priestoru vo V, t. j. V budeme považovať len za množinu, môžeme vytvoriť vektorový priestor U^V *všetkých* zobrazení $f : V \to U$ s operáciami súčtu a skalárneho násobku definovanými po zložkách (pozri odstavec 1.6.5). Potom pre množinu $\mathcal{L}(V,U)$ všetkých *lineárnych* zobrazení $\varphi : V \to U$, samozrejme, platí $\mathcal{L}(V,U) \subseteq U^V$.

6.5.1. Tvrdenie. *Nech U, V sú vektorové priestory nad poľom K. Potom $\mathcal{L}(V,U)$ je lineárny podpriestor vektorového priestoru U^V. Teda $\mathcal{L}(V,U)$ je vektorový priestor nad poľom K.*

Dôkaz. Treba overiť, že pre ľubovoľné $a, b \in K$ lineárna kombinácia $\vartheta = a\varphi + b\psi$ lineárnych zobrazení $\varphi, \psi : V \to U$, definovaná pre $\boldsymbol{x} \in V$ predpisom

$$\vartheta(\boldsymbol{x}) = a\varphi(\boldsymbol{x}) + b\psi(\boldsymbol{x}),$$

je tiež lineárne zobrazenie $\vartheta : V \to U$. Zvoľme $\boldsymbol{x}, \boldsymbol{y} \in V$, $c, d \in K$. Priamym výpočtom dostávame

$$\begin{aligned}\vartheta(c\boldsymbol{x} + d\boldsymbol{y}) &= a\varphi(c\boldsymbol{x} + d\boldsymbol{y}) + b\psi(c\boldsymbol{x} + d\boldsymbol{y}) = a(c\varphi(\boldsymbol{x}) + d\varphi(\boldsymbol{y})) + b(c\psi(\boldsymbol{x}) + d\psi(\boldsymbol{y})) \\ &= c(a\varphi(\boldsymbol{x}) + b\psi(\boldsymbol{x})) + d(a\varphi(\boldsymbol{y}) + b\psi(\boldsymbol{y})) = c\vartheta(\boldsymbol{x}) + d\vartheta(\boldsymbol{y}).\end{aligned}$$

Teda $\vartheta \in \mathcal{L}(V,U)$.

6.5.2. Tvrdenie. *Nech U, V sú konečnorozmerné vektorové priestory nad poľom K a $\dim U = m$, $\dim V = n$. Potom*

$$\mathcal{L}(V, U) \cong K^{m\times n},$$

teda $\dim \mathcal{L}(V, U) = mn$.

Dôkaz. Zvoľme bázy $\boldsymbol{\alpha}$ v priestore U a $\boldsymbol{\beta}$ v priestore V. Z výsledkov predchádzajúceho paragrafu vyplýva, že priradenie $\varphi \mapsto (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je bijekcia $\mathcal{L}(V, U) \to K^{m\times n}$. Stačí teda dokázať, že je to aj lineárne zobrazenie, to znamená, že pre $a, b \in K$, $\varphi, \psi \in \mathcal{L}(V, U)$ platí

$$(a\varphi + b\psi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = a(\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} + b(\psi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}.$$

To je však zrejmé. Čitateľovi, ktorý má nejaké pochybnosti, odporúčame, aby si jednoduchým výpočtom porovnal stĺpce matíc na ľavej a pravej strane.

Na maticu $(\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ sa teda možno dívať ako na súradnice vektora $\varphi \in \mathcal{L}(V, U)$ v priestore $K^{m\times n}$, vzhľadom na dvojicu báz $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$.

Lineárne zobrazenie $\varphi : V \to K$ z vektorového priestoru V do poľa K sa nazýva *lineárny funkcionál* alebo *lineárna forma* na V. Vektorový priestor $\mathcal{L}(V, K)$ všetkých lineárnych foriem na V sa nazýva *duálny priestor* alebo len krátko *duál* vektorového priestoru V. Budeme používať označenie $\mathcal{L}(V, K) = V^*$

Keďže v poli K budeme vždy uvažovať len kanonickú bázu pozostávajúcu z jediného vektora $1 \in K$, ľubovoľná báza $\boldsymbol{\beta}$ v konečnorozmernom priestore V určuje lineárny izomorfizmus $V^* \to V$ daný predpisom $\varphi \mapsto (\varphi)_{1,\boldsymbol{\beta}}$. Tým sme dokázali nasledujúce tvrdenie.

6.5.3. Tvrdenie. *Pre ľubovoľný konečnorozmerný vektorový priestor V nad poľom K platí* $V^* \cong V$.

Uvedomme si, že matica $(\varphi)_{1,\boldsymbol{\beta}}$ lineárneho funkcionálu $\varphi : V \to K$ je riadkový vektor z priestoru $K^{1\times n}$. To nám odkrýva nový pohľad na vektorový priestor riadkov $K^{1\times n}$. Pri voľbe kanonickej bázy $\boldsymbol{\varepsilon}$ v stĺpcovom priestore $K^{n\times 1}$ možno riadkový priestor $K^{1\times n}$ stotožniť s duálom $\left(K^{n\times 1}\right)^*$ stĺpcového priestoru $K^{n\times 1}$.

Ešte raz podčiarknime, že izomorfizmus konečnorozmerného priestoru V a jeho duálu V^* závisí od výberu bázy vo V. Na druhej strane, pre ľubovoľný vektorový priestor V možno definovať kanonické, t. j. od výberu bázy nezávislé zobrazenie z priestoru V do jeho *druhého duálu* V^{**} dané predpisom $\boldsymbol{x} \mapsto \widehat{\boldsymbol{x}}$, kde

$$\widehat{\boldsymbol{x}}(\varphi) = \varphi(\boldsymbol{x})$$

pre $\boldsymbol{x} \in V$, $\varphi \in V^*$.

6.5.4. Veta. *Nech V je vektorový priestor nad poľom K. Potom*

(a) *$\boldsymbol{x} \mapsto \widehat{\boldsymbol{x}}$ je injektívne lineárne zobrazenie $V \to V^{**}$;*

(b) *ak V je konečnorozmerný, tak $\boldsymbol{x} \mapsto \widehat{\boldsymbol{x}}$ je lineárny izomorfizmus $V \to V^{**}$.*

Dôkaz. Najprv ukážeme, že pre každé $\boldsymbol{x} \in V$ vôbec platí $\widehat{\boldsymbol{x}} \in V^{**}$, t. j. $\widehat{\boldsymbol{x}}$ je lineárny funkcionál na priestore V^*. Pre $\varphi, \psi \in V^*$, $a, b \in K$ jednoduchý výpočet dáva

$$\widehat{\boldsymbol{x}}(a\varphi + b\psi) = (a\varphi + b\psi)(\boldsymbol{x}) = a\varphi(\boldsymbol{x}) + b\psi(\boldsymbol{x}) = a\widehat{\boldsymbol{x}}(\varphi) + b\widehat{\boldsymbol{x}}(\psi).$$

(a) Pre $\boldsymbol{x} \in V$ označme $\widehat{\boldsymbol{x}} = \eta(\boldsymbol{x})$. Dokážeme, že $\eta : V \to V^{**}$ je lineárne zobrazenie. Zvoľme $\boldsymbol{x}, \boldsymbol{y} \in V$ $c, d \in K$. Treba overiť, že zobrazenia $\eta(c\boldsymbol{x} + d\boldsymbol{y})$ a $c\eta(\boldsymbol{x}) + d\eta(\boldsymbol{y})$ sa rovnajú, t. j. že každému $\varphi \in V^*$ priradia tú istú hodnotu. Počítajme

$$\begin{aligned}\eta(c\boldsymbol{x}+d\boldsymbol{y})(\varphi) &= \varphi(c\boldsymbol{x}+d\boldsymbol{y}) = c\varphi(\boldsymbol{x}) + d\varphi(\boldsymbol{y})\\ &= c\widehat{\boldsymbol{x}}(\varphi) + d\widehat{\boldsymbol{y}}(\varphi) = (c\eta(\boldsymbol{x}) + d\eta(\boldsymbol{y}))(\varphi).\end{aligned}$$

Injektívnosť zobrazenia η spoznáme podľa jeho jadra. Stačí si uvedomiť, že pre ľubovoľné $\mathbf{0} \neq \boldsymbol{x} \in V$ existuje $\varphi \in V^*$ také, že $\varphi(\boldsymbol{x}) \neq 0$. [1]

Potom

$$\eta(\boldsymbol{x})(\varphi) = \widehat{\boldsymbol{x}}(\varphi) = \varphi(\boldsymbol{x}) \neq 0,$$

teda $\eta(\boldsymbol{x})$ sa nerovná identicky nulovému zobrazeniu $\mathbf{0} : V^* \to K$, ktoré je nulou vo V^{**}. Preto $\boldsymbol{x} \notin \operatorname{Ker}\eta$ pre $\boldsymbol{x} \neq \mathbf{0}$, čiže $\operatorname{Ker}\eta = \{\mathbf{0}\}$.

(b) Ak V je konečnorozmerný, tak s vyžitím vety 6.2.3., už dokázanej časti (a) a tvrdenia 6.5.3. dostávame

$$\dim \operatorname{Im}\eta = \dim V - \dim \operatorname{Ker}\eta = \dim V = \dim V^* = \dim V^{**}.$$

Preto $\operatorname{Im}\eta = V^{**}$, čiže η je i surjektívne.

Každý vektor $\boldsymbol{x} \in V$ tak definuje lineárny funkcionál $\widehat{\boldsymbol{x}}$ na duálnom priestore V^*. Pritom konečnorozmerný vektorový priestor V možno prostredníctvom priradenia $\boldsymbol{x} \mapsto \widehat{\boldsymbol{x}}$ *prirodzene* stotožniť s duálom priestoru V^*. Napr. stĺpcový priestor $K^{n\times 1}$ možno stotožniť s duálom

[1] V konečnorozmernom prípade ide o očividné tvrdenie. V nekonečnorozmernom prípade však jeho dôkaz využíva existenciu Hamelovej bázy vo V, prípadne si vyžaduje nejaký iný vhodný dôsledok axiómy výberu (pozri záverečnú časť paragrafu 5.5 a cvičenie 6.15).

riadkového priestoru $K^{1\times n}$. Vo všeobecnom prípade možno V stotožniť s lineárnym podpriestorom $\operatorname{Im}\eta = \{\widehat{\boldsymbol{x}};\ \boldsymbol{x}\in V\}$ jeho druhého duálu V^{**}.

Poznámka. Prostriedkami, ktoré presahujú rámec tohto kurzu, možno dokázať, že $V \not\cong V^*$ a $V \not\cong V^{**}$ pre každý nekonečnorozmerný vektorový priestor V. Zjednodušene povedané, duál V^* je vždy „podstatne väčší“ než pôvodný priestor V a druhý duál V^{**} je „ešte väčší“. Teda ani $\boldsymbol{x}\mapsto\widehat{\boldsymbol{x}}$ nemôže byť surjektívne zobrazenie $V\to V^{**}$.

Cvičenia

6.1. Nech U, V sú vektorové priestory nad poľom K a $\varphi: V\to U$ je lineárne zobrazenie. Potom $\varphi(\mathbf{0})=\mathbf{0}$ a pre každé $\boldsymbol{x}\in V$ platí $\varphi(-\boldsymbol{x})=-\varphi(\boldsymbol{x})$. Dokážte.

6.2. Dokážte tvrdenie 6.1.1.

6.3. Nech $\boldsymbol{A}\in K^{m\times n}$. Uvažujme lineárne zobrazenie $\varphi: K^m\to K^n$ dané predpisom $\varphi(\boldsymbol{x})=\boldsymbol{A}\cdot\boldsymbol{x}$. Ako súvisí jadro $\operatorname{Ker}\varphi$ s homogénnou sústavou lineárnych rovníc $\boldsymbol{A}\cdot\boldsymbol{x}=\mathbf{0}$?

6.4. (a) V príkladoch 6.1.5.–9 podrobne overte, že v nich definované zobrazenia sú naozaj lineárne.

(b) Pre každé z uvedených lineárnych zobrazení určte jeho jadro a obraz.

6.5. Zdôvodnite, prečo žiadne z nasledujúcich zobrazení $\mathbb{R}\to\mathbb{R}$ nie je lineárne:

(a) $\varphi(x)=1-3x$,
(b) $\psi(x)=|x|$,
(c) $f(x)=x^2$,
(d) $g(x)=x^3$,
(e) $h(x)=\sqrt{|x|}$,
(f) $k(x)=\sqrt[3]{x}$,
(g) $l(x)=\ln(1+x^2)$
(h) $s(x)=\sin x$,
(i) $\eta(x)=\mathrm{e}^x$,
(j) $\sigma(x)=\sinh x=\frac{1}{2}(\mathrm{e}^x-\mathrm{e}^{-x})$.

6.6. (a) Uvažujte $\mathbb{C}$ ako vektorový priestor nad poľom $\mathbb{R}$. Ukážte, že komplexná konjugácia $z \mapsto \overline{z}$ je lineárne zobrazenie $\mathbb{C} \to \mathbb{C}$.

(b) Uvažujte $\mathbb{C}$ ako vektorový priestor nad poľom $\mathbb{C}$. Ukážte, že komplexná konjugácia $z \mapsto \overline{z}$ *nie je* lineárne zobrazenie $\mathbb{C} \to \mathbb{C}$.

6.7. Lineárne zobrazenie $\varphi : \mathbb{R}^3 \to \mathbb{R}^2$ je pre $\boldsymbol{x} = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ dané predpisom $\varphi(\boldsymbol{x}) = (x_1 + 2x_2, 3x_1 + 7x_2 - x_3)^T$.

(a) Napíšte maticu lineárneho zobrazenia φ vzhľadom na kanonické bázy $\boldsymbol{\varepsilon}^{(3)}$ v $\mathbb{R}^3$, $\boldsymbol{\varepsilon}^{(2)}$ v $\mathbb{R}^2$.

(b) Napíšte maticu φ vzhľadom na bázy $\boldsymbol{\beta} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{v})$ v $\mathbb{R}^3$, $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \boldsymbol{u}_2)$ v $\mathbb{R}^2$, kde $\boldsymbol{v} = (-2, 1, 1)^T$, $\boldsymbol{u}_1 = (1, 3)^T$, $\boldsymbol{u}_2 = (2, 7)^T$.

(c) Napíšte priamo nejaké bázy lineárnych podpriestorov $\operatorname{Ker}\varphi \subseteq \mathbb{R}^3$ a $\operatorname{Im}\varphi \subseteq \mathbb{R}^2$.

6.8. Báza $\boldsymbol{\beta}$ vektorového priestoru $\mathbb{R}^3$ je tvorená stĺpcami matice $\begin{pmatrix} 1 & 1 & 2 \\ 2 & 0 & 2 \\ 3 & -1 & 1 \end{pmatrix}$ a báza $\boldsymbol{\alpha}$ vektorového priestoru $\mathbb{R}^4$ je tvorená stĺpcami matice $\begin{pmatrix} 1 & 2 & 3 & 1 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & 1 & -1 \\ 0 & 1 & 2 & 1 \end{pmatrix}$. Lineárne zobrazenie $\psi : \mathbb{R}^3 \to \mathbb{R}^4$ má vzhľadom na tieto bázy maticu $\boldsymbol{A} = (\psi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

(a) Napíšte priamo nejaké bázy lineárnych podpriestorov $\operatorname{Ker}\psi \subseteq \mathbb{R}^3$ a $\operatorname{Im}\psi \subseteq \mathbb{R}^4$.

(b) Napíšte maticu ψ vzhľadom na kanonické bázy $\boldsymbol{\varepsilon}^{(3)}$ v $\mathbb{R}^3$, $\boldsymbol{\varepsilon}^{(4)}$ v $\mathbb{R}^{(3)}$.

6.9. Nech $n \in \mathbb{N}$. Uvažujme deriváciu $f \mapsto f'$ ako lineárnu transformáciu $D : \mathbb{R}^{(n)}[x] \to \mathbb{R}^{(n)}[x]$.

(a) Určte lineárne podpriestory $\operatorname{Ker} D$ a $\operatorname{Im} D$ v $\mathbb{R}^{(n)}[x]$ a nájdite nejaké ich bázy. Zistite dimenzie oboch podpriestorov a overte vzťah $\dim \operatorname{Ker} D + \dim \operatorname{Im} D = n$.

(b) Napíšte maticu lineárnej transformácie D vzhľadom na bázu $\boldsymbol{\xi}^{(n)} = (1, x, x^2, \ldots, x^n)$.

(c) Napíšte maticu D vzhľadom na bázu $\boldsymbol{\zeta}^{(n)} = \left(1, \frac{1}{1!}x, \frac{1}{2!}x^2, \ldots, \frac{1}{n!}x^n\right)$.

6.10. *Operátor diferencie* $\Delta : \mathbb{R}^{(n)}[x] \to \mathbb{R}^{(n)}[x]$ je daný predpisom $\Delta(f)(x) = f(x+1) - f(x)$.

(a) Dokážte, že Δ je lineárny operátor.

(b) Určte lineárne podpriestory $\operatorname{Ker}\Delta$ a $\operatorname{Im}\Delta$ v $\mathbb{R}^{(n)}[x]$ a nájdite nejaké ich bázy. Zistite dimenzie oboch podpriestorov.

(c) Napíšte maticu lineárnej transformácie Δ vzhľadom na bázu $\boldsymbol{\xi}^{(n)} = (1, x, x^2, \dots, x^n)$.

(d) Dokážte, že polynómy $1, x, [x]_2, \dots, [x]_n$, kde $[x]_k = x(x-1)\dots(x-k+1)$, tvoria bázu vektorového priestoru $\mathbb{R}^{(n)}[x]$.

(e) Napíšte maticu Δ vzhľadom na bázu $\boldsymbol{\eta}^{(n)} = (1, x, [x]_2, \dots, [x]_n)$.

(f) Nájdite nejakú bázu vektorového priestoru $\mathbb{R}^{(n)}[x]$, vzhľadom na ktorú má Δ maticu tvaru $\begin{pmatrix} \mathbf{0}_{n,1} & \boldsymbol{I}_n \\ 0 & \mathbf{0}_{1,n} \end{pmatrix}$.

6.11. Pre ľubovoľné $\alpha, \beta \in \mathbb{R}$ vynásobením príslušných matíc dokážte uvedené rovnosti a interpretujte ich v reči lineárnych transformácií roviny $\mathbb{R}^2$:

$$\boldsymbol{R}_\alpha \cdot \boldsymbol{R}_\beta = \boldsymbol{R}_{\alpha+\beta}, \qquad \boldsymbol{R}_\alpha \cdot \boldsymbol{S}_\beta = \boldsymbol{S}_{\beta+\alpha/2},$$

$$\boldsymbol{S}_\alpha \cdot \boldsymbol{S}_\beta = \boldsymbol{R}_{2(\beta-\alpha)}, \qquad \boldsymbol{S}_\beta \cdot \boldsymbol{R}_\alpha = \boldsymbol{S}_{\beta-\alpha/2}.$$

6.12. Predpismi $\varphi(x_1, x_2, x_3)^T = (x_1 - 2x_3, 2x_1 + x_2 + 3x_4, -x_1 - x_4, x_3 + 2x_4)^T$, $\psi(x_1, x_2, x_3, x_4)^T = (2x_1 - x_3, 3x_3 + x_4, x_2 + x_4)^T$ sú dané lineárne zobrazenia $\varphi : \mathbb{R}^3 \to \mathbb{R}^4$, $\psi : \mathbb{R}^4 \to \mathbb{R}^3$. Napíšte matice lineárnych zobrazení $\psi \circ \varphi : \mathbb{R}^3 \to \mathbb{R}^3$, $\varphi \circ \psi : \mathbb{R}^4 \to \mathbb{R}^4$ vzhľadom na kanonické bázy vektorových priestorov $\mathbb{R}^3$ resp. $\mathbb{R}^4$.

6.13. Nech S, T sú lineárne podpriestory vektorového priestoru V.

(a) Priradením $(\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{x} + \boldsymbol{y}$ je definované surjektívne lineárne zobrazenie $\mu : S \times T \to S + T$. Dokážte.

(b) Nájdite jadro $\operatorname{Ker}\mu$ a dokážte, že μ je injektívne práve vtedy, keď $S \cap T = \{\mathbf{0}\}$.

(c) Odvoďte z toho, že vektorové priestory $S \times T$ a $S + T$ sú izomorfné práve vtedy, keď $S + T = S \oplus T$.

(d) Zovšeobecnite na ľubovoľný konečný počet lineárnych podpriestorov (pozri cvičenie 4.8).

6.14. *Galileova transformácia* „časopriestoru“ $\mathbb{R}^4$ je daná priradením $(t,x,y,z)^T \mapsto (t',x',y',z')^T$, kde $t'=t$, $x' = x - v_x t$, $y' = y - v_y t$, $z' = z - v_z t$, pričom vektor $\boldsymbol{v} = (v_x, v_y, v_z)^T \in \mathbb{R}^3$ interpretujeme ako rýchlosť (pozri príklad 6.4.7.).

(a) Napíšte maticu $\boldsymbol{G_v}$ Galileovej transformácie.

(b) Uvažujme dvoch pozorovateľov P a P'. Vysvetlite, za akých podmienok je uvedenou transformáciou sprostredkovaný vzťah medzi časmi a priestorovými súradnicami udalostí z hľadiska pozorovateľov P a P'. (Riešte otázku v rámci klasickej fyziky, bez ohľadu na relativistické efekty.)

(c) Vynásobením matíc dokážte vzťah $\boldsymbol{G_u} \cdot \boldsymbol{G_v} = \boldsymbol{G_{u+v}}$. Vysvetlite, prečo sa tento vzťah nazýva *klasickým pravidlom skladania rýchlostí.*

6.15. (a) Dokážte nasledujúcu konečnorozmernú verziu *Hahnovej-Banachovej vety*: Nech V je konečnorozmerný vektorový priestor nad poľom K, $S \subset V$ je vlastný lineárny podpriestor a $\psi : S \to K$ je lineárny funkcionál. Potom pre každé $\boldsymbol{x} \in V \setminus S$ existuje lineárny funkcionál $\varphi \in V^*$ taký, že $\varphi(\boldsymbol{x}) \neq 0$ a $\varphi \restriction S = \psi$.

(b) Zovšeobecnite tvrdenie (a) aj na nekonečnorozmerné vektorové priestory. (*Návod*: Predpokladajte, že V má Hamelovu bázu X takú, že $\boldsymbol{x} \in X$ a $X \cap S$ je Hamelova báza podpriestoru S – pozri záverečnú časť paragrafu 5.5).

(c) Pre každý vektor $\mathbf{0} \neq \boldsymbol{x} \in V$ existuje lineárny funkcionál $\varphi \in V^*$ taký, že $\varphi(\boldsymbol{x}) \neq 0$. Dokážte jednak priamo podľa vzoru (a) resp. (b), jednak z nich odvoďte ako špeciálny prípad.

6.16. Nech K je konečné pole, ktoré má práve q prvkov. Potom q je mocninou nejakého prvočísla. Dokážte. (*Návod*: Ukážte, že K nesie prirodzenú štruktúru vektorového priestoru nad poľom $\mathbb{Z}_p$, kde $p = \operatorname{char} K$.)

6.17. Nech K je konečné pole, $q = \#K$ a U, V sú vektorové priestory nad K s konečnými rozmermi $\dim U =$

m, $\dim V = n$. Akú dimenziu a koľko prvkov má vektorový priestor $\mathcal{L}(V, U)$ všetkých lineárnych zobrazení $V \to U$? Porovnajte s dimenziou a počtom prvkov vektorového priestoru U^V všetkých zobrazení $V \to U$. Aká je pravdepodobnosť, že náhodne vybrané zobrazenie $f \in U^V$ bude lineárne?

7. Inverzné matice a zmena bázy

V tejto kapitole zavedieme pojem *inverznej matice* k danej štvorcovej matici a dáme ho do súvisu s pojmom inverzného lineárneho zobrazenia. Ďalej sa naučíme počítať inverzné matice a matice prechodu z jednej súradnej bázy do druhej. Nakoniec preskúmame vplyv zmeny bázy na maticu lineárneho zobrazenia. Začneme však s pojmom *hodnosti matice*, ktorý nám umožní rozhodnúť o existencii inverznej matice a – ako uvidíme neskôr – bude nám ešte veľakrát užitočný.

V celej kapitole K označuje pevné pole, m, n, p sú kladné celé čísla.

7.1. Hodnosť matice

V tomto paragrafe je potrebné rozlišovať medzi vektorovými priestormi riadkových resp. stĺpcových vektorov. Nebudeme teda používať nešpecifikované označenie K^n, ale priestor riadkových vektorov budeme značiť $K^{1\times n}$ a priestor stĺpcových vektorov $K^{n\times 1}$.

Pripomeňme, že $\boldsymbol{r}_i(\boldsymbol{A}) \in K^{1\times n}$ označuje i-tý riadok a $\boldsymbol{s}_j(\boldsymbol{A}) \in K^{m\times 1}$ zase j-tý stĺpec matice $\boldsymbol{A} = (a_{ij})_{m\times n}$. Túto maticu teda môžeme zapísať v blokových tvaroch

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{r}_1(\boldsymbol{A}) \\ \boldsymbol{r}_2(\boldsymbol{A}) \\ \vdots \\ \boldsymbol{r}_m(\boldsymbol{A}) \end{pmatrix} = (\boldsymbol{s}_1(\boldsymbol{A}), \boldsymbol{s}_2(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})).$$

Riadkovou hodnosťou $h_r(\boldsymbol{A})$ matice $\boldsymbol{A}$ nazývame dimenziu lineárneho podpriestoru vektorového priestoru $K^{1\times n}$ generovaného riadkami matice $\boldsymbol{A}$. Podobne, *stĺpcovou hodnosťou* $h_s(\boldsymbol{A})$ matice $\boldsymbol{A}$ nazývame dimenziu lineárneho podpriestoru vektorového priestoru $K^{m\times 1}$ generovaného stĺpcami matice $\boldsymbol{A}$. Teda

$$h_r(\boldsymbol{A}) = \dim[\boldsymbol{r}_1(\boldsymbol{A}), \boldsymbol{r}_2(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})],$$
$$h_s(\boldsymbol{A}) = \dim[\boldsymbol{s}_1(\boldsymbol{A}), \boldsymbol{s}_2(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})]$$

Označme $\varphi : K^{n\times 1} \to K^{m\times 1}$ lineárne zobrazenie dané predpisom $\varphi(\boldsymbol{x}) = \boldsymbol{A}\cdot\boldsymbol{x}$ pre $\boldsymbol{x} \in K^{n\times 1}$. Pripomeňme, že hodnosťou lineárneho zobrazenia φ nazývame dimenziu jeho obrazu, t. j. $h(\varphi) = \dim \operatorname{Im}\varphi$. V našom prípade zrejme platí $h(\varphi) = h_s(\boldsymbol{A})$, keďže lineárny podpriestor $\operatorname{Im}\varphi \subseteq K^{m\times 1}$ je generovaný stĺpcami matice $\boldsymbol{A}$.

7.1.1. Lema. *Nech* $\boldsymbol{A} \in K^{m\times n}$.

(a) *Nech matica* $\boldsymbol{B}$ *vznikne z matice* $\boldsymbol{A}$ *vykonaním jednej (inak ľubovoľnej) ERO. Potom* $[\boldsymbol{r}_1(\boldsymbol{A}), \boldsymbol{r}_2(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] = [\boldsymbol{r}_1(\boldsymbol{B}), \boldsymbol{r}_2(\boldsymbol{B}), \dots, \boldsymbol{r}_m(\boldsymbol{B})]$.

(b) *Nech matica* $\boldsymbol{C}$ *vznikne z matice* $\boldsymbol{A}$ *vykonaním jednej (inak ľubovoľnej) ESO. Potom* $[\boldsymbol{s}_1(\boldsymbol{A}), \boldsymbol{s}_2(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})] = [\boldsymbol{s}_1(\boldsymbol{C}), \boldsymbol{s}_2(\boldsymbol{C}), \dots, \boldsymbol{s}_n(\boldsymbol{C})]$.

Dôkaz. Zrejme pre ľubovoľné vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ v každom vektorovom priestore V a ľubovoľný skalár $c \in K$ platí:

$$\begin{aligned}
[\boldsymbol{u}_1, \dots, \boldsymbol{u}_i, \dots, \boldsymbol{u}_j, \dots, \boldsymbol{u}_k] &= [\boldsymbol{u}_1, \dots, \boldsymbol{u}_j, \dots, \boldsymbol{u}_i, \dots, \boldsymbol{u}_k],\\
[\boldsymbol{u}_1, \dots, \boldsymbol{u}_i, \dots, \boldsymbol{u}_k] &= [\boldsymbol{u}_1, \dots, c\boldsymbol{u}_i, \dots, \boldsymbol{u}_k] \qquad (\text{ak } c \neq 0),\\
[\boldsymbol{u}_1, \dots, \boldsymbol{u}_i, \dots, \boldsymbol{u}_j, \dots, \boldsymbol{u}_k] &= [\boldsymbol{u}_1, \dots, \boldsymbol{u}_i, \dots, c\boldsymbol{u}_i + \boldsymbol{u}_j, \dots, \boldsymbol{u}_k].
\end{aligned}$$

7.1.2. Tvrdenie. *Pre každú maticu $\boldsymbol{A} \in K^{m\times n}$ platí $h_r(\boldsymbol{A}) = h_s(\boldsymbol{A})$.*

Dôkaz. Upravme $\boldsymbol{A}$ pomocou ERO na redukovaný stupňovitý tvar $\boldsymbol{B} \in K^{m\times n}$ a označme k počet nenulových riadkov v matici $\boldsymbol{B}$. Podľa práve dokázanej lemy platí $[\boldsymbol{r}_1(\boldsymbol{A}), \dots, \boldsymbol{r}_m(\boldsymbol{A})] = [\boldsymbol{r}_1(\boldsymbol{B}), \dots, \boldsymbol{r}_m(\boldsymbol{B})]$. Preto tiež $h_r(\boldsymbol{A}) = h_r(\boldsymbol{B})$. Keďže nenulové riadky matice $\boldsymbol{B}$ sú zrejme lineárne nezávislé (rozmyslite si prečo), $h_r(\boldsymbol{B}) = k$, čo je vlastne počet stĺpcov matice $\boldsymbol{B}$, v ktorých sa nachádza vedúci prvok nejakého jej riadku. Označme $1 \le j_1 < \ldots < j_k \le n$ indexy týchto stĺpcov. Podľa tvrdenia 4.5.3. vektory $\boldsymbol{s}_{j_1}(\boldsymbol{A}), \dots, \boldsymbol{s}_{j_k}(\boldsymbol{A})$ sú lineárne nezávislé a platí $[\boldsymbol{s}_1(\boldsymbol{A}), \dots, \boldsymbol{s}_n(\boldsymbol{A})] = [\boldsymbol{s}_{j_1}(\boldsymbol{A}), \dots, \boldsymbol{s}_{j_k}(\boldsymbol{A})]$. Preto tiež $h_s(\boldsymbol{A}) = k = h_r(\boldsymbol{A})$.

Keďže riadková a stĺpcová hodnosť ľubovoľnej matice $\boldsymbol{A}$ splývajú, túto ich spoločnú hodnotu budeme odteraz značiť jednoducho $h(\boldsymbol{A})$ a nazývať *hodnosťou matice* $\boldsymbol{A}$. Zrejme pre $\boldsymbol{A} \in K^{m\times n}$ je $h(\boldsymbol{A}) \le \min(m, n)$.

Práve vykonané úvahy majú dva bezprostredné dôsledky.

7.1.3. Tvrdenie. *Nech $\boldsymbol{A} \in K^{m\times n}$. Potom $h(\boldsymbol{A}) = h(\boldsymbol{A}^T)$.*

7.1.4. Tvrdenie. *Nech* $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n \in K^{m\times 1}$ *sú ľubovoľné vektory a* $\boldsymbol{A} \in K^{m\times n}$ *je matica taká, že* $\boldsymbol{s}_j(\boldsymbol{A}) = \boldsymbol{u}_j$ *pre* $1 \le j \le n$. *Potom*

(a) $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$ *sú lineárne nezávislé práve vtedy, keď* $h(\boldsymbol{A}) = n$;

(b) $[\boldsymbol{u}_1, \dots, \boldsymbol{u}_n] = K^{m\times 1}$ *práve vtedy, keď* $h(\boldsymbol{A}) = m$.

Všimnite si, že prípad (a) môže nastať iba vtedy, keď $n \le m$; naopak, (b) môže nastať jedine za predpokladu $m \le n$.

Sami si sformulujte a premyslite analogické tvrdenia pre riadkové vektory.

Ešte si dokážeme jeden odhad hodnosti súčinu matíc pomocou hodností jednotlivých činiteľov.

7.1.5. Tvrdenie. *Nech* $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{B} \in K^{n\times p}$. *Potom*

$$h(\boldsymbol{A}\cdot\boldsymbol{B}) \le \min\big(h(\boldsymbol{A}), h(\boldsymbol{B})\big).$$

Dôkaz. Označme $\varphi : K^n \to K^m$, $\psi : K^p \to K^n$ lineárne zobrazenia dané predpismi $\varphi(\boldsymbol{x}) = \boldsymbol{A}\cdot\boldsymbol{x}$ pre $\boldsymbol{x} \in K^n$ resp. $\psi(\boldsymbol{y}) = \boldsymbol{B}\cdot\boldsymbol{y}$ pre $\boldsymbol{y} \in K^p$. Zrejme $\operatorname{Im}(\varphi\circ\psi) \subseteq \operatorname{Im}\varphi$, preto

$$h(\boldsymbol{A}\cdot\boldsymbol{B}) = h(\varphi\circ\psi) \le h(\varphi) = h(\boldsymbol{A}).$$

S využitím toho druhý potrebný odhad už dostaneme priamym výpočtom

$$h(\boldsymbol{A}\cdot\boldsymbol{B}) = h\big((\boldsymbol{A}\cdot\boldsymbol{B})^T\big) = h\big(\boldsymbol{B}^T\cdot\boldsymbol{A}^T\big) \le h\big(\boldsymbol{B}^T\big) = h(\boldsymbol{B}).$$

7.2. Inverzné matice a inverzné lineárne zobrazenia

Nech $\boldsymbol{A} \in K^{n\times n}$, t. j. $\boldsymbol{A}$ je *štvorcová* matica typu $n \times n$. *Inverznou maticou* k matici $\boldsymbol{A}$ rozumieme maticu $\boldsymbol{B} \in K^{n\times n}$ takú, že

$$\boldsymbol{A} \cdot \boldsymbol{B} = \boldsymbol{I}_n = \boldsymbol{B} \cdot \boldsymbol{A}.$$

Zrejme k danej štvorcovej matici $\boldsymbol{A}$ existuje najviac jedna inverzná matica (rozmyslite si prečo). Túto jednoznačne určenú maticu (ak existuje) budeme značiť $\boldsymbol{A}^{-1}$.

Nasledujúca veta je bezprostredným dôsledkom súvisu medzi lineárnymi zobrazeniami a ich maticami.

7.2.1. Veta. *Nech U, V sú vektorové priestory nad poľom K a* $\dim U = \dim V = n$. *Nech ďalej $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ sú nejaké bázy v U, resp. vo V a $\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je matica lineárneho zobrazenia $\varphi : V \to U$ vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$. Potom k matici $\boldsymbol{A}$ existuje inverzná matica $\boldsymbol{A}^{-1}$ práve vtedy, keď k zobrazeniu φ existuje inverzné zobrazenie φ^{-1}. V tom prípade $\boldsymbol{A}^{-1}$ je maticou lineárneho zobrazenia $\varphi^{-1} : U \to V$ vzhľadom na bázy $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, t. j.*

$$\boldsymbol{A}^{-1} = \left((\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}\right)^{-1} = \left(\varphi^{-1}\right)_{\boldsymbol{\beta},\boldsymbol{\alpha}}.$$

Hovoríme, že štvorcová matica $\boldsymbol{A} \in K^{n\times n}$ je *regulárna*, ak k nej existuje inverzná matica $\boldsymbol{A}^{-1}$; v opačnom prípade hovoríme, že $\boldsymbol{A}$ je *singulárna*.

7.2.2. Veta. *Matica $\boldsymbol{A} \in K^{n\times n}$ je regulárna práve vtedy, keď $h(\boldsymbol{A}) = n$.*

Dôkaz. Označme $\varphi : K^n \to K^n$ lineárnu transformáciu danú predpisom $\varphi(\boldsymbol{x}) = \boldsymbol{A} \cdot \boldsymbol{x}$ pre $\boldsymbol{x} \in K^n$. K matici $\boldsymbol{A}$ existuje inverzná matica $\boldsymbol{A}^{-1}$ práve vtedy, keď k zobrazeniu φ

existuje inverzné zobrazenie φ^{-1}, t. j. práve vtedy, keď φ je bijekcia. Podľa dôsledku 6.2.4. to nastane práve vtedy, keď φ je surjekcia, čiže $\operatorname{Im}\varphi = K^n$, čo je ekvivalentné s rovnosťou $\dim \operatorname{Im}\varphi = n$. Na dokončenie dôkazu si stačí spomenúť, že $h(\boldsymbol{A}) = h(\varphi) = \dim \operatorname{Im}\varphi$.

Z praktických dôvodov bude užitočný si uvedomiť, že na to, aby sme sa presvedčili, že matica $\boldsymbol{B} \in K^{n\times n}$ je inverzná k matici $\boldsymbol{A} \in K^{n\times n}$, stačí overiť len jednu (a to hocktorú) z rovností $\boldsymbol{A}\cdot\boldsymbol{B} = \boldsymbol{I}_n$, $\boldsymbol{B}\cdot\boldsymbol{A} = \boldsymbol{I}_n$.

7.2.3. Tvrdenie. *Pre ľubovoľné $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ platí $\boldsymbol{A}\cdot\boldsymbol{B} = \boldsymbol{I}_n$ práve vtedy, keď $\boldsymbol{B}\cdot\boldsymbol{A} = \boldsymbol{I}_n$.*

Dôkaz. Označme $\varphi, \psi : K^n \to K^n$ lineárne transformácie dané pre $\boldsymbol{x} \in K^n$ predpismi $\varphi(\boldsymbol{x}) = \boldsymbol{A}\cdot\boldsymbol{x}$, resp. $\psi(\boldsymbol{x}) = \boldsymbol{B}\cdot\boldsymbol{x}$. Nech $\boldsymbol{A}\cdot\boldsymbol{B} = \boldsymbol{I}_n$. To nastane práve vtedy, keď $\varphi\circ\psi = \mathrm{id}_{K^n}$. Z toho vyplýva, že φ je surjekcia a ψ je injekcia (pozri paragraf 0.3). Keďže φ, ψ sú lineárne transformácie konečnorozmerného vektorového priestoru, podľa dôsledku 6.2.4. to znamená, že φ aj ψ sú bijekcie, teda lineárne izomorfizmy, a $\psi = \varphi^{-1}$. Potom však $\boldsymbol{B} = \boldsymbol{A}^{-1}$, preto tiež $\boldsymbol{B}\cdot\boldsymbol{A} = \boldsymbol{I}_n$. Obrátená implikácia vyplýva zo symetrie tvrdenia.

S využitím posledného tvrdenia si ako cvičenie overte nasledujúce vzorce, z ktorých už vyplýva zvyšok tvrdenia.

7.2.4. Tvrdenie. *Nech $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ sú regulárne matice. Potom aj matice $\boldsymbol{A}^{-1}$, $\boldsymbol{A}\cdot\boldsymbol{B}$ a $\boldsymbol{A}^T$ sú regulárne a platí:*

$$\left(\boldsymbol{A}^{-1}\right)^{-1} = \boldsymbol{A}, \qquad (\boldsymbol{A}\cdot\boldsymbol{B})^{-1} = \boldsymbol{B}^{-1}\cdot\boldsymbol{A}^{-1}, \qquad \left(\boldsymbol{A}^{T}\right)^{-1} = \left(\boldsymbol{A}^{-1}\right)^{T}.$$

7.3. Výpočet inverznej matice

Prakticky všetky úlohy lineárnej algebry, s ktorými sme sa doteraz stretli, sme riešili tak, že sme danú situáciu reprezentovali nejakou vhodnou maticou, tú sme ďalej pomocou ERO upravili na redukovaný stupňovitý tvar a tento výsledný tvar sme potom interpretovali v závislosti na charaktere pôvodnej úlohy. Prezraďme už vopred, že zatiaľ sme všetky úlohy, ktoré sa riešia úpravou matíc pomocou ERO prípadne ESO, zďaleka nevyčerpali. Naopak, táto metóda nás bude v lineárnej algebre neustále sprevádzať.

Skôr než pristúpime k ďalšiemu využitiu tejto metódy, tentoraz pri výpočte inverznej matice, však bude potrebné si uvedomiť, že ERO aj ESO možno realizovať pomocou násobenia matíc.

7.3.1. Tvrdenie. *Nech* $\boldsymbol{A} \in K^{m\times n}$.

(a) *Nech* $\boldsymbol{B} \in K^{m\times n}$ *vznikne z* $\boldsymbol{A}$ *vykonaním jednej (inak ľubovoľnej) ERO. Označme* $\boldsymbol{E}$ *maticu, ktorá vznikne z matice* $\boldsymbol{I}_m$ *vykonaním tej istej ERO. Potom* $\boldsymbol{B} = \boldsymbol{E} \cdot \boldsymbol{A}$.

(b) *Nech* $\boldsymbol{C} \in K^{m\times n}$ *vznikne z* $\boldsymbol{A}$ *vykonaním jednej (inak ľubovoľnej) ESO. Označme* $\boldsymbol{F}$ *maticu, ktorá vznikne z matice* $\boldsymbol{I}_n$ *vykonaním tej istej ESO. Potom* $\boldsymbol{C} = \boldsymbol{A} \cdot \boldsymbol{F}$.

Dôkaz. Možno overiť priamym výpočtom pre každý jednotlivý druh ERO resp. ESO. Ako cvičenie si to skúste napr. pre maticu $\boldsymbol{A}$ typu 3×2, resp. 3×3.

Štvorcové matice $\boldsymbol{E} \in K^{n\times n}$, ktoré vzniknú z jednotkovej matice $\boldsymbol{I}_n$ vykonaním jedinej ERO alebo ESO, nazývame *elementárne matice*. Posledná veta teda hovorí, že ľubovoľnú ERO (ESO) na matici $\boldsymbol{A}$ možno realizovať vynásobením matice $\boldsymbol{A}$ vhodnou elementárnou maticou $\boldsymbol{E}$ zľava (sprava).

Návod na výpočet inverznej matice k danej štvorcovej matici $\boldsymbol{A} \in K^{n\times n}$ si možno najľahšie zapamätať v tvare nasledujúcej schémy:

$$(\boldsymbol{A} \mid \boldsymbol{I}_n) \xrightarrow{\text{ERO}} (\boldsymbol{I}_n \mid \boldsymbol{A}^{-1}).$$

Tento postup má navyše tú výhodu, že sa nemusíme vopred starať, či inverzná matica k matici $\boldsymbol{A}$ existuje alebo nie. Ak $\boldsymbol{A}^{-1}$ existuje, tak ju nakoniec vypočítame, ak neexistuje, tak to odhalíme počas nášho výpočtu a ďalej v ňom nebudeme pokračovať. Celý postup si teraz vysvetlíme trochu podrobnejšie.

Bloková matica $(\boldsymbol{A} \mid \boldsymbol{I}_n)$ vznikne tak, že matice $\boldsymbol{A}$ a $\boldsymbol{I}_n$ jednoducho napíšeme vedľa seba. Túto maticu teraz budeme upravovať pomocou ERO tak, aby sme v ľavej časti z matice $\boldsymbol{A}$ dostali jednotkovú maticu $\boldsymbol{I}_n$. Akonáhle sa nám to podarí, matica v pravej časti výslednej blokovej matice je už hľadaná matica $\boldsymbol{A}^{-1}$. Ak sa nám to nepodarí, t. j. matica $\boldsymbol{A}$ nie je riadkovo ekvivalentná s jednotkovou maticou (čo nastane práve vtedy, keď $h(\boldsymbol{A}) < n$, a spoznáme to podľa toho, že sa nám v ľavej časti objaví nejaký nulový riadok), tak inverzná matica k matici $\boldsymbol{A}$ neexistuje.

Korektnosť uvedeného postupu vyplýva z nasledujúceho očividného tvrdenia a skutočnosti, že ERO možno reprezentovať násobením elementárnymi maticami zľava. Taktiež tu hrá úlohu fakt, že pre $\boldsymbol{B} \in K^{n\times n}$ platí $\boldsymbol{B} = \boldsymbol{A}^{-1}$ práve vtedy, keď $\boldsymbol{B} \cdot \boldsymbol{A} = \boldsymbol{I}_n$, uvedený v tvrdení 7.2.3.

7.3.2. Tvrdenie. *Nech $\boldsymbol{A} \in K^{n\times n}$ a $\boldsymbol{E}_1, \boldsymbol{E}_2, \dots, \boldsymbol{E}_k \in K^{n\times n}$ sú elementárne matice také, že $\boldsymbol{E}_k \cdot \ldots \cdot \boldsymbol{E}_2 \cdot \boldsymbol{E}_1 \cdot \boldsymbol{A} = \boldsymbol{I}_n$. Potom $\boldsymbol{A}^{-1} = \boldsymbol{E}_k \cdot \ldots \cdot \boldsymbol{E}_2 \cdot \boldsymbol{E}_1$.*

Poznamenajme, že k rovnakému cieľu vedie tiež postup reprezentovaný schémou:

$$\left(\frac{\boldsymbol{A}}{\boldsymbol{I}_n}\right) \xrightarrow{\text{ESO}} \left(\frac{\boldsymbol{I}_n}{\boldsymbol{A}^{-1}}\right).$$

Rozmyslite si prečo a sformulujte príslušné tvrdenie.

Z práve vykonaných úvah vyplývajú nasledujúce tri dôsledky. Posledný z nich je čiastočným obrátením odhadu hodnosti súčinu matíc za predpokladu regularity aspoň jedného z činiteľov.

7.3.3. Tvrdenie. *Matica $\boldsymbol{A} \in K^{n\times n}$je regulárna práve vtedy, keď ju možno rozložiť na súčin $\boldsymbol{A} = \boldsymbol{E}_1 \cdot \ldots \cdot \boldsymbol{E}_k$ konečného počtu elementárnych matíc $\boldsymbol{E}_1, \ldots, \boldsymbol{E}_k \in K^{n\times n}$.*

7.3.4. Tvrdenie. *Pre ľubovoľné $\boldsymbol{A}$, $\boldsymbol{B} \in K^{m\times n}$ platí:*

(a) *$\boldsymbol{A}$ je riadkovo ekvivalentná s $\boldsymbol{B}$ práve vtedy, keď existuje regulárna matica $\boldsymbol{P} \in K^{m\times m}$ taká, že $\boldsymbol{A} = \boldsymbol{P} \cdot \boldsymbol{B}$;*

(b) *$\boldsymbol{A}$ je stĺpcovo ekvivalentná s $\boldsymbol{B}$ práve vtedy, keď existuje regulárna matica $\boldsymbol{Q} \in K^{n\times n}$ taká, že $\boldsymbol{A} = \boldsymbol{B} \cdot \boldsymbol{Q}$.*

7.3.5. Tvrdenie. *Nech $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{P} \in K^{m\times m}$, $\boldsymbol{Q} \in K^{n\times n}$, pričom $\boldsymbol{P}$, $\boldsymbol{Q}$ sú regulárne matice. Potom*

$$h(\boldsymbol{A}) = h(\boldsymbol{P} \cdot \boldsymbol{A}) = h(\boldsymbol{A} \cdot \boldsymbol{Q}) = h(\boldsymbol{P} \cdot \boldsymbol{A} \cdot \boldsymbol{Q}).$$

Trochu všeobecnejšie možno uvedené úvahy použiť na násobenie ľubovoľnej matice vhodného rozmeru maticou $\boldsymbol{A}^{-1}$ (ak existuje) zľava resp. sprava. Tieto operácie možno uskutočniť pre regulárnu $\boldsymbol{A} \in K^{n\times n}$ a ľubovoľné $\boldsymbol{B} \in K^{n\times m}$, $\boldsymbol{C} \in K^{m\times n}$ podľa nasledujúcich schém:

$$(\boldsymbol{A} \mid \boldsymbol{B}) \xrightarrow{\text{ERO}} (\boldsymbol{I}_n \mid \boldsymbol{A}^{-1} \cdot \boldsymbol{B}),$$

$$\left(\frac{\boldsymbol{A}}{\boldsymbol{C}}\right) \xrightarrow{\text{ESO}} \left(\frac{\boldsymbol{I}_n}{\boldsymbol{C}\cdot\boldsymbol{A}^{-1}}\right).$$

Ešte si všimnime, že v špeciálnom prípade sme niečo podobné vlastne robili už dávno, pri riešení sústav lineárnych rovníc úpravou na redukovaný stupňovitý tvar pomocou ERO. Aj tento postup totiž možno vyjadriť pomocou schémy

$$(\boldsymbol{A} \mid \boldsymbol{b}) \xrightarrow{\text{ERO}} (\boldsymbol{B} \mid \boldsymbol{c}),$$

ktorá má pre regulárnu $\boldsymbol{A} \in K^{n\times n}$ tvar

$$(\boldsymbol{A} \mid \boldsymbol{b}) \xrightarrow{\text{ERO}} (\boldsymbol{I}_n \mid \boldsymbol{A}^{-1} \cdot \boldsymbol{b}).$$

Ako vedľajší produkt našich úvah tak dostávame nasledujúci výsledok o riešení sústav n lineárnych rovníc o n neznámych.

7.3.6. Veta. *Nech $\boldsymbol{A} \in K^{n\times n}$, $\boldsymbol{b} \in K^n$. Ak $\boldsymbol{A}$ je regulárna, tak sústava $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ má jediné riešenie $\boldsymbol{x} = \boldsymbol{A}^{-1} \cdot \boldsymbol{b}$.*

7.4. Matica prechodu

Nech V je vektorový priestor nad poľom K a $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ sú jeho dve bázy. *Maticou prechodu* z bázy $\boldsymbol{\beta}$ do bázy $\boldsymbol{\alpha}$ nazývame maticu identického zobrazenia

$\mathrm{id}_V : V \to V$ vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$, ktorú značíme $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$. Teda

$$\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = (\mathrm{id}_V)_{\boldsymbol{\alpha},\boldsymbol{\beta}}.$$

Podľa definície matice lineárneho zobrazenia vzhľadom na dané bázy (pozri paragraf 6.4), stĺpce matice prechodu $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ sú tvorené súradnicami vektorov bázy $\boldsymbol{\beta}$ vzhľadom na bázu $\boldsymbol{\alpha}$, t. j. $\boldsymbol{s}_j(\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}) = (\boldsymbol{v}_j)_{\boldsymbol{\alpha}}$ pre $1 \leq j \leq n$. Teda

$$\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \big((\boldsymbol{v}_1)_{\boldsymbol{\alpha}}, (\boldsymbol{v}_2)_{\boldsymbol{\alpha}}, \dots, (\boldsymbol{v}_n)_{\boldsymbol{\alpha}}\big),$$

a podľa vety 6.4.1. je táto matica jednoznačne určená podmienkou transformácie súradníc

$$(\boldsymbol{x})_{\boldsymbol{\alpha}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}}$$

pre ľubovoľné $\boldsymbol{x} \in V$.

Ak do zrejmej rovnosti $\boldsymbol{x} = \boldsymbol{\alpha} \cdot (\boldsymbol{x})_{\boldsymbol{\alpha}}$ (pozri paragraf 5.3) budeme za $\boldsymbol{x}$ postupne dosadzovať vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ bázy $\boldsymbol{\beta}$, s využitím vzťahu pre stĺpce súčinu matíc z paragrafu 2.3 dostaneme

$$\boldsymbol{v}_j = \boldsymbol{\alpha} \cdot (\boldsymbol{v}_j)_{\boldsymbol{\alpha}} = \boldsymbol{\alpha} \cdot \boldsymbol{s}_j(\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}) = \boldsymbol{s}_j(\boldsymbol{\alpha} \cdot \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}})$$

pre každé $1 \leq j \leq n$. Tým sme dostali ďalší dôležitý vzťah, ktorý jednoznačne charakterizuje maticu prechodu $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$:

$$\boldsymbol{\alpha} \cdot \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \boldsymbol{\beta}.$$

(Podotýkame, že súčin $\boldsymbol{\alpha} \cdot \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ treba chápať v zmysle paragrafu 2.3)

Priradenie $\boldsymbol{u}_i \mapsto \boldsymbol{v}_i$ pre $i \le n$ možno jednoznačne rozšíriť do bijektívnej lineárnej transformácie $\vartheta : V \to V$. Skrátene píšeme $\vartheta(\boldsymbol{\alpha}) = \boldsymbol{\beta}$. Matica transformácie ϑ vzhľadom na bázu $\boldsymbol{\alpha}$ je opäť

$$(\vartheta)_{\boldsymbol{\alpha}} = (\vartheta)_{\boldsymbol{\alpha},\boldsymbol{\alpha}} = \big((\vartheta \boldsymbol{u}_1)_{\boldsymbol{\alpha}}, \dots, (\vartheta \boldsymbol{u}_n)_{\boldsymbol{\alpha}}\big) = \big((\boldsymbol{v}_1)_{\boldsymbol{\alpha}}, \dots, (\boldsymbol{v}_n)_{\boldsymbol{\alpha}}\big) = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}.$$

Zhrnutím vykonaných úvah dostávame štyri ekvivalentné charakterizácie matice prechodu.

7.4.1. Tvrdenie. *Nech $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ sú dve bázy n-rozmerného vektorového priestoru V nad poľom K. Potom pre ľubovoľnú maticu $\boldsymbol{P} \in K^{n\times n}$ nasledujúce podmienky sú ekvivalentné:*

(i) $\boldsymbol{P} = (\mathrm{id}_V)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$, *t. j. $\boldsymbol{P}$ je matica prechodu z bázy $\boldsymbol{\beta}$ do bázy $\boldsymbol{\alpha}$;*

(ii) $(\boldsymbol{x})_{\boldsymbol{\alpha}} = \boldsymbol{P} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}}$ pre každé $\boldsymbol{x} \in V$;

(iii) $\boldsymbol{\alpha} \cdot \boldsymbol{P} = \boldsymbol{\beta}$;

(iv) $\boldsymbol{P} = (\vartheta)_{\boldsymbol{\alpha}}$, *kde $\vartheta : V \to V$ je lineárna transformácia taká, že $\vartheta(\boldsymbol{\alpha}) = \boldsymbol{\beta}$.*

Z definície matice prechodu a vety 6.4.2. okamžite vyplývajú nasledujúce rovnosti.

7.4.2. Tvrdenie. *Nech $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$ sú bázy konečnorozmerného vektorového priestoru V nad poľom K. Potom*

$$\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\alpha}} = \boldsymbol{I}_n, \qquad \boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\alpha}} = {\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}}^{-1}, \qquad \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot \boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\gamma}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\gamma}}.$$

Z druhej z uvedených podmienok vidno, že matica prechodu $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je vždy *regulárna*. Taktiež naopak, každá regulárna matica $\boldsymbol{P} \in K^{n\times n}$ je maticou prechodu medzi vhodnou dvojicou báz.

7.4.3. Tvrdenie. *Nech V je n-rozmerný vektorový priestor nad poľom K, $\boldsymbol{P} = (p_{ij}) \in K^{n\times n}$ je ľubovoľná regulárna matica a $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$ je nejaká báza vo V. Položme*

$$\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = \boldsymbol{\alpha} \cdot \boldsymbol{P}, \qquad \boldsymbol{\gamma} = (\boldsymbol{w}_1, \dots, \boldsymbol{w}_n) = \boldsymbol{\alpha} \cdot \boldsymbol{P}^{-1},$$

t. j. pre $1 \le j \le n$ platí $\boldsymbol{v}_j = p_{1j}\boldsymbol{u}_1 + \dots + p_{nj}\boldsymbol{u}_n$ a $\boldsymbol{w}_j = q_{1j}\boldsymbol{u}_1 + \dots + q_{nj}\boldsymbol{u}_n$, kde $\boldsymbol{P}^{-1} = (q_{ij})_{n\times n}$. Potom $\boldsymbol{P}$ je maticou prechodu z bázy $\boldsymbol{\beta}$ do bázy $\boldsymbol{\alpha}$ a taktiež z bázy $\boldsymbol{\alpha}$ do bázy $\boldsymbol{\gamma}$, čiže

$$\boldsymbol{P} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \boldsymbol{P}_{\boldsymbol{\gamma},\boldsymbol{\alpha}}.$$

Špeciálne, $\boldsymbol{P}$ je maticou prechodu z bázy $(\boldsymbol{s}_1(\boldsymbol{P}), \dots, \boldsymbol{s}_n(\boldsymbol{P}))$ do bázy $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \dots, \boldsymbol{e}_n)$ v K^n a taktiež z bázy $\boldsymbol{\varepsilon}$ do bázy $(\boldsymbol{s}_1(\boldsymbol{P}^{-1}), \dots, \boldsymbol{s}_n(\boldsymbol{P}^{-1}))$.

V prípade, keď $V = K^n$ je priestor stĺpcových vektorov, možno každú jeho bázu $\boldsymbol{\alpha}$ stotožniť s príslušnou regulárnou maticou, ktorej stĺpcami sú vektory danej bázy. Pri takomto stotožnení je návod na výpočet matice prechodu obsiahnutý v nasledujúcom tvrdení.

7.4.4. Tvrdenie. *Nech $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n)$, $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ sú dve bázy stĺpcového vektorového priestoru K^n. Potom $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \boldsymbol{\alpha}^{-1} \cdot \boldsymbol{\beta}$.*

Dôkaz. Z podmienky $\boldsymbol{\alpha} \cdot \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \boldsymbol{\beta}$ okamžite vyplýva požadovaná rovnosť.

To nám dáva návod na výpočet matice prechodu pre bázy $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ vektorového priestoru

K^n podľa už známej schémy

$$(\boldsymbol{\alpha} \mid \boldsymbol{\beta}) \xrightarrow{\text{ERO}} (\boldsymbol{I}_n \mid \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}) = (\boldsymbol{\varepsilon} \mid \boldsymbol{\alpha}^{-1} \cdot \boldsymbol{\beta}).$$

7.5. Matice lineárneho zobrazenia vzhľadom na rôzne bázy

V tomto článku sa budeme zaoberať vplyvom zmeny báz na maticu lineárneho zobrazenia, presnejšie, vzťahom medzi maticami daného lineárneho zobrazenia vzhľadom na rôzne dvojice báz.

7.5.1. Veta. *Nech V_1, V_2 sú konečnorozmerné vektorové priestory nad poľom K, $\varphi : V_1 \to V_2$ je lineárne zobrazenie, $\boldsymbol{\alpha}_1$, $\boldsymbol{\beta}_1$ sú dve bázy priestoru V_1 a $\boldsymbol{\alpha}_2$, $\boldsymbol{\beta}_2$ sú dve bázy priestoru V_2. Potom*

$$(\varphi)_{\boldsymbol{\beta}_2,\boldsymbol{\beta}_1} = \boldsymbol{P}_{\boldsymbol{\beta}_2,\boldsymbol{\alpha}_2} \cdot (\varphi)_{\boldsymbol{\alpha}_2,\boldsymbol{\alpha}_1} \cdot \boldsymbol{P}_{\boldsymbol{\alpha}_1,\boldsymbol{\beta}_1}.$$

Dôkaz. Označme $\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha}_2,\boldsymbol{\alpha}_1}$, $\boldsymbol{B} = (\varphi)_{\boldsymbol{\beta}_2,\boldsymbol{\beta}_1}$ matice lineárneho zobrazenia φ vzhľadom na bázy $\boldsymbol{\alpha}_1$, $\boldsymbol{\alpha}_2$, resp. bázy $\boldsymbol{\beta}_1$, $\boldsymbol{\beta}_2$. Pre ľubovoľné $\boldsymbol{x} \in V_1$ platí:

$$\begin{aligned} \boldsymbol{B} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}_1} &= (\varphi\boldsymbol{x})_{\boldsymbol{\beta}_2} = \boldsymbol{P}_{\boldsymbol{\beta}_2,\boldsymbol{\alpha}_2} \cdot (\varphi\boldsymbol{x})_{\boldsymbol{\alpha}_2} \\ &= \boldsymbol{P}_{\boldsymbol{\beta}_2,\boldsymbol{\alpha}_2} \cdot \boldsymbol{A} \cdot (\boldsymbol{x})_{\boldsymbol{\alpha}_1} = \boldsymbol{P}_{\boldsymbol{\beta}_2,\boldsymbol{\alpha}_2} \cdot \boldsymbol{A} \cdot \boldsymbol{P}_{\boldsymbol{\alpha}_1,\boldsymbol{\beta}_1} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}_1}. \end{aligned}$$

Na základe vety 6.4.1. z toho okamžite vyplýva dokazovaná rovnosť

$$\boldsymbol{B} = \boldsymbol{P}_{\boldsymbol{\beta}_2,\boldsymbol{\alpha}_2} \cdot \boldsymbol{A} \cdot \boldsymbol{P}_{\boldsymbol{\alpha}_1,\boldsymbol{\beta}_1}.$$

Poslednú transformačnú formulku si možno najľahšie zapamätať pomocou nasledujúceho diagramu:

$$\begin{array}{ccc}
(V_1,\boldsymbol{\alpha}_1) & \xrightarrow{\ \boldsymbol{A}\ } & (V_2,\boldsymbol{\alpha}_2)\\
{\scriptstyle \boldsymbol{P}_{\boldsymbol{\alpha}_1,\boldsymbol{\beta}_1}}\Big\uparrow & & \Big\downarrow{\scriptstyle \boldsymbol{P}_{\boldsymbol{\beta}_2,\boldsymbol{\alpha}_2}}\\
(V_1,\boldsymbol{\beta}_1) & \xrightarrow[\ \boldsymbol{B}\ ]{} & (V_2,\boldsymbol{\beta}_2)
\end{array}$$

Nezabudnite, že zobrazenia skladáme „v obrátenom poradí“, a tomu musí zodpovedať aj „obrátené poradie“ násobenia matíc!

7.5.2. Príklad. Nech $\varphi : K^n \to K^m$ je lineárne zobrazenie a $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ sú nejaké bázy priestorov K^m resp. K^n. Označme $\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$, $\boldsymbol{M} = (\varphi)_{\boldsymbol{\varepsilon}^{(m)},\boldsymbol{\varepsilon}^{(n)}}$ matice zobrazenia φ vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ resp. vzhľadom na kanonické bázy $\boldsymbol{\varepsilon}^{(n)}$, $\boldsymbol{\varepsilon}^{(m)}$. Podľa poslednej vety platí:

$$\boldsymbol{A} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\varepsilon}^{(m)}} \cdot \boldsymbol{M} \cdot \boldsymbol{P}_{\boldsymbol{\varepsilon}^{(n)},\boldsymbol{\beta}},$$
$$\boldsymbol{M} = \boldsymbol{P}_{\boldsymbol{\varepsilon}^{(m)},\boldsymbol{\alpha}} \cdot \boldsymbol{A} \cdot \boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\varepsilon}^{(n)}}.$$

Ak stotožníme každú bázu s regulárnou maticou, ktorej stĺpce sú vektory tejto bázy, tak uvedené rovnosti nadobudnú tvar

$$\boldsymbol{A} = \boldsymbol{\alpha}^{-1} \cdot \boldsymbol{I}_m \cdot \boldsymbol{M} \cdot \boldsymbol{I}_n^{-1} \cdot \boldsymbol{\beta} = \boldsymbol{\alpha}^{-1} \cdot \boldsymbol{M} \cdot \boldsymbol{\beta},$$
$$\boldsymbol{M} = \boldsymbol{I}_m^{-1} \cdot \boldsymbol{\alpha} \cdot \boldsymbol{A} \cdot \boldsymbol{\beta}^{-1} \cdot \boldsymbol{I}_n = \boldsymbol{\alpha} \cdot \boldsymbol{A} \cdot \boldsymbol{\beta}^{-1},$$

umožňujúci priamy výpočet jednej z matíc $\boldsymbol{A}$, $\boldsymbol{M}$ na základe znalosti báz $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ a druhej z nich.

Položme si teraz obrátenú otázku. Za akých podmienok sú matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{m\times n}$ maticami toho istého lineárneho zobrazenia $\varphi : V \to U$ vzhľadom na nejaké dve (možno no nie nutne rôzne) dvojice báz konečnorozmerných vektorových priestorov U, V? Odpoveď na ňu dáva nasledujúca veta.

7.5.3. Veta. *Nech U je m-rozmerný a V je n-rozmerný vektorový priestor nad poľom K. Potom pre ľubovoľné matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{m\times n}$ nasledujúce podmienky sú ekvivalentné:*

(i) *$\boldsymbol{A}$, $\boldsymbol{B}$ sú maticami toho istého lineárneho zobrazenia $\varphi : V \to U$ vzhľadom na nejaké dve (možno no nie nutne rôzne) dvojice báz priestorov U, V;*

(ii) *existujú regulárne matice $\boldsymbol{P} \in K^{m\times m}$, $\boldsymbol{Q} \in K^{n\times n}$ také, že $\boldsymbol{B} = \boldsymbol{P} \cdot \boldsymbol{A} \cdot \boldsymbol{Q}$;*

(iii) $h(\boldsymbol{A}) = h(\boldsymbol{B})$.

Dôkaz. Ekvivalencia (i) $\Leftrightarrow$ (ii) je priamym dôsledkom vety 7.5.1. a tvrdenia 7.4.3. Implikácia (ii) $\Rightarrow$ (iii) vyplýva z tvrdenia 7.3.5.

Zostáva dokázať (iii) $\Rightarrow$ (ii). Označme $h = h(\boldsymbol{A}) = h(\boldsymbol{B})$. Pomocou ERO upravíme $\boldsymbol{A}$ aj $\boldsymbol{B}$ na redukovaný trojuholníkový tvar $\boldsymbol{A}' = \boldsymbol{P}_1 \cdot \boldsymbol{A}$, resp. $\boldsymbol{B}' = \boldsymbol{P}_2 \cdot \boldsymbol{B}$, kde $\boldsymbol{P}_1$, $\boldsymbol{P}_2$ sú regulárne matice. Zrejme $\boldsymbol{A}'$, $\boldsymbol{B}'$ majú rovnaký počet nenulových riadkov rovný h. $\boldsymbol{A}'$ aj $\boldsymbol{B}'$ možno ďalej pomocou ESO upraviť na blokový tvar

$$\boldsymbol{A}'' = \boldsymbol{A}' \cdot \boldsymbol{Q}_1 = \begin{pmatrix} \boldsymbol{I}_h & \boldsymbol{0}_{h,n-h} \\ \boldsymbol{0}_{m-h,h} & \boldsymbol{0}_{m-h,n-h} \end{pmatrix} = \boldsymbol{B}' \cdot \boldsymbol{Q}_2 = \boldsymbol{B}'',$$

kde $\boldsymbol{Q}_1$, $\boldsymbol{Q}_2$ sú regulárne matice. Stačí pomocou vedúcich prvkov jednotlivých riadkov vynulovať prípadné ďalšie nenulové prvky týchto riadkov a, ak treba, vymeniť poradie niektorých stĺpcov. Potom $\boldsymbol{P}_1 \cdot \boldsymbol{A} \cdot \boldsymbol{Q}_1 = \boldsymbol{P}_2 \cdot \boldsymbol{B} \cdot \boldsymbol{Q}_2$, teda $\boldsymbol{B} = \boldsymbol{P}_2^{-1} \cdot \boldsymbol{P}_1 \cdot \boldsymbol{A} \cdot \boldsymbol{Q}_1 \cdot \boldsymbol{Q}_2^{-1}$ a matice $\boldsymbol{P} = \boldsymbol{P}_2^{-1} \cdot \boldsymbol{P}_1$, $\boldsymbol{Q} = \boldsymbol{Q}_1 \cdot \boldsymbol{Q}_2^{-1}$ sú zrejme regulárne.

Na základe dôkazu tejto vety okamžite dostávame záverečný výsledok.

7.5.4. Veta. *Pre každé lineárne zobrazenie $\varphi : V \to U$ medzi konečnorozmernými vektorovými priestormi nad poľom K možno zvoliť bázu $\boldsymbol{\beta}$ priestoru V a bázu $\boldsymbol{\alpha}$ priestoru U tak, že φ má vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ maticu v blokovom tvare*

$$(\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \begin{pmatrix} \boldsymbol{I}_h & \mathbf{0}_{h,n-h} \\ \mathbf{0}_{m-h,h} & \mathbf{0}_{m-h,n-h} \end{pmatrix},$$

kde $n = \dim V$, $m = \dim U$ a $h = h(\varphi)$.

Skúste si túto vetu dokázať priamo a bližšie špecifikovať bázy $\boldsymbol{\beta}$ a $\boldsymbol{\alpha}$. (*Návod*: Spomeňte si na dôkaz vety 6.2.3. o dimenzii jadra a obrazu.)

7.6. Pohyblivé bázy

Lineárnu transformáciu konečnorozmerného vektorového priestoru V je často výhodné popisovať zadaním obrazov vektorov nejakej bázy. Pritom pre rôzne transformácie môžu byť výhodné rôzne bázy. Napr. pri sledovaní nejakého pohybujúceho sa objektu je prirodzené udávať jeho polohu vzhľadom na bázu spojenú s „nehybným“ pozorovateľom. Zmenu orientácie takého objektu spôsobenú jeho rotáciou je však výhodnejšie udávať vzhľadom na bázu spojenú s týmto objektom.

Uvažujme bázy $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ vektorového priestoru V. Nech $\vartheta : V \to V$ je lineárna transformácia taká, že $\vartheta(\boldsymbol{\alpha}) = \boldsymbol{\beta}$. Ak prechod od vektora $\boldsymbol{x} \in V$ k jeho obrazu $\vartheta(\boldsymbol{x}) \in V$ chápeme ako výsledok nejakého pohybu (napr. otočenia) v priestore V, tak bázu $\boldsymbol{\beta}$ možno považovať za novú polohu premiestnenej bázy $\boldsymbol{\alpha}$. Ak $\boldsymbol{\gamma}$ je ďalšia báza vo V a $\eta : V \to V$ je lineárna transformácia taká, že $\eta(\boldsymbol{\beta}) = \boldsymbol{\gamma}$, tak bázu $\boldsymbol{\gamma}$ môžeme chápať jednak ako bázu $\boldsymbol{\beta}$ premiestnenú transformáciou η, jednak ako pôvodnú bázu $\boldsymbol{\alpha}$ premiestnenú transformáciou $\eta \circ \vartheta$.

Pre maticu zloženej transformácie $\eta \circ \vartheta$ vzhľadom na bázu $\boldsymbol{\alpha}$ dostávame popri obvyklom vyjadrení pomocou „pevnej“ bázy $\boldsymbol{\alpha}$

$$(\eta \circ \vartheta)_{\boldsymbol{\alpha}} = (\eta)_{\boldsymbol{\alpha}} \cdot (\vartheta)_{\boldsymbol{\alpha}}$$

taktiež vyjadrenie pomocou „pohyblivej“ bázy $\boldsymbol{\alpha}$, t. j. pomocou báz $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$,

$$(\eta \circ \vartheta)_{\boldsymbol{\alpha}} = (\vartheta)_{\boldsymbol{\alpha}} \cdot (\eta)_{\boldsymbol{\beta}}.$$

ktoré je zaujímavé obráteným poradím činiteľov. Stačí si uvedomiť, že zo vzťahov $\vartheta(\boldsymbol{\alpha}) = \boldsymbol{\beta}$, $\eta(\boldsymbol{\beta}) = \boldsymbol{\gamma}$ vyplýva $(\eta \circ \vartheta)(\boldsymbol{\alpha}) = \boldsymbol{\gamma}$, a ďalej podľa časti (iv) tvrdenia 7.4.1. a tvrdenia 7.4.2. tiež

$$(\eta \circ \vartheta)_{\boldsymbol{\alpha}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot \boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\gamma}} = (\vartheta)_{\boldsymbol{\alpha}} \cdot (\eta)_{\boldsymbol{\beta}}.$$

Toto pozorovanie možno matematickou indukciou rozšíriť na ľubovoľný konečný počet báz a lineárnych transformácií.

7.6.1. Veta. *Nech $\boldsymbol{\alpha}_0, \boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_k$ sú bázy konečnorozmerného vektorového priestoru V a $\vartheta_1, \dots, \vartheta_k : V \to V$ sú lineárne transformácie také, že $\vartheta_i(\boldsymbol{\alpha}_{i-1}) = \boldsymbol{\alpha}_i$ pre $1 \le i \le k$. Potom* *maticu zloženej transformácie $\vartheta = \vartheta_k \circ \ldots \circ \vartheta_1$ vzhľadom na pôvodnú bázu $\boldsymbol{\alpha}_0$ možno vyjadriť ako súčin*

$$(\vartheta)_{\boldsymbol{\alpha}_0} = (\vartheta_1)_{\boldsymbol{\alpha}_0} \cdot \ldots \cdot (\vartheta_k)_{\boldsymbol{\alpha}_{k-1}}$$

matíc $(\vartheta_i)_{\boldsymbol{\alpha}_{i-1}}$ dielčích transformácií ϑ_i vzhľadom na jednotlivé polohy $\boldsymbol{\alpha}_{i-1}$ pohyblivej bázy $\boldsymbol{\alpha}_0$.

7.6.2. Príklad. Nájdeme maticu lineárnej transformácie $\Omega : \mathbb{R}^3 \to \mathbb{R}^3$ ktorá vznikne zložením otočenia Ω_1 okolo osi $z = [\boldsymbol{e}_3]$ o uhol $\pi/4$ s otočením Ω_2 okolo osi so smerovým vektorom $\Omega_1(\boldsymbol{e}_1)$ o uhol $\pi/3$.

Lineárna transformácia Ω_1 má v báze $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$ maticu

$$(\Omega_1)_{\boldsymbol{\varepsilon}} = \begin{pmatrix} \cos(\pi/4) & -\sin(\pi/4) & 0 \\ \sin(\pi/4) & \cos(\pi/4) & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 & 0 \\ \sqrt{2}/2 & \sqrt{2}/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Lineárna transformácia Ω_2 má v báze $\boldsymbol{\beta} = \Omega_1(\boldsymbol{\varepsilon}) = (\Omega_1(\boldsymbol{e}_1), \Omega_1(\boldsymbol{e}_2), \boldsymbol{e}_3)$ (t. j. v „novej“ báze $\boldsymbol{\varepsilon}$) maticu

$$(\Omega_2)_{\boldsymbol{\beta}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\pi/3) & -\sin(\pi/3) \\ 0 & \sin(\pi/6) & \cos(\pi/6) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & -\sqrt{3}/2 \\ 0 & \sqrt{3}/2 & 1/2 \end{pmatrix}.$$

Preto

$$
\begin{aligned}
(\Omega)_{\boldsymbol{\varepsilon}} = (\Omega_2 \circ \Omega_1)_{\boldsymbol{\varepsilon}} &= (\Omega_1)_{\boldsymbol{\varepsilon}} \cdot (\Omega_2)_{\boldsymbol{\beta}} \\
&= \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/2 & 0 \\ \sqrt{2}/2 & \sqrt{2}/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & -\sqrt{3}/2 \\ 0 & \sqrt{3}/2 & 1/2 \end{pmatrix} \\
&= \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/4 & \sqrt{6}/4 \\ \sqrt{2}/2 & \sqrt{2}/4 & -\sqrt{6}/4 \\ 0 & \sqrt{3}/2 & 1/2 \end{pmatrix}.
\end{aligned}
$$

Na základe rovnosti $(\Omega)_{\boldsymbol{\varepsilon}} = (\Omega_2)_{\boldsymbol{\varepsilon}} \cdot (\Omega_1)_{\boldsymbol{\varepsilon}}$ je už teraz hračkou vypočítať aj samotnú maticu otočenia Ω_2 vzhľadom na kanonickú bázu $\boldsymbol{\varepsilon}$:

$$
\begin{aligned}
(\Omega_2)_{\boldsymbol{\varepsilon}} = (\Omega)_{\boldsymbol{\varepsilon}} \cdot (\Omega_1)_{\boldsymbol{\varepsilon}}^{-1} &= \begin{pmatrix} \sqrt{2}/2 & -\sqrt{2}/4 & \sqrt{6}/4 \\ \sqrt{2}/2 & \sqrt{2}/4 & -\sqrt{6}/4 \\ 0 & \sqrt{3}/2 & 1/2 \end{pmatrix} \cdot \begin{pmatrix} \sqrt{2}/2 & \sqrt{2}/2 & 0 \\ -\sqrt{2}/2 & \sqrt{2}/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 3/4 & 1/4 & \sqrt{6}/4 \\ 1/4 & 3/4 & -\sqrt{6}/4 \\ -\sqrt{6}/4 & \sqrt{6}/4 & 1/2 \end{pmatrix}.
\end{aligned}
$$

Cvičenia

7.1. Nech U, V sú vektorové priestory nad poľom K a $\varphi : V \to U$ je lineárne zobrazenie. Potom pre ľubovoľné vektory $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n \in V$ platí $\varphi[\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n] = [\varphi(\boldsymbol{v}_1), \ldots, \varphi(\boldsymbol{v}_n)]$. Dokážte. Odvoďte z toho, že ak $e\boldsymbol{v}_1, \dots, e\boldsymbol{v}_n$ generujú V, tak $\varphi(\boldsymbol{v}_1), \dots, \varphi(\boldsymbol{v}_n)$ generujú $\operatorname{Im}\varphi$. Špeciálne, stĺpce matice $\boldsymbol{A} \in K^{m\times n}$ generujú lineárny podpriestor $\operatorname{Im}\varphi \subseteq K^m$, kde $\varphi : K^n \to K^m$ je dané predpisom $\varphi(\boldsymbol{x}) = \boldsymbol{A}\cdot\boldsymbol{x}$.

7.2. Určte hodnosť matice $\boldsymbol{A}$ nad poľom K:

(a) $K = \mathbb{R}$, $\boldsymbol{A} = \begin{pmatrix} 2 & 2 & -1 \\ 3 & 0 & 1 \end{pmatrix}$;

(b) $K = \mathbb{C}$, $\boldsymbol{A} = \begin{pmatrix} 1+\mathrm{i} & 1+3\mathrm{i} & 2 \\ 3+\mathrm{i} & 5+5\mathrm{i} & 4-2\mathrm{i} \end{pmatrix}$;

(c) $K = \mathbb{Z}_7$, $\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 2 \\ 3 & 5 & 4 \\ 1 & 3 & 0 \end{pmatrix}$;

(d) $K = \mathbb{Z}_{17}$, $\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 2 \\ 3 & 5 & 4 \\ 1 & 3 & 0 \end{pmatrix}$.

7.3. (a) Dokážte vzorce z tvrdenia 7.2.4.

(b) Dokážte, že pre ľubovoľnú maticu $\boldsymbol{A} \in K^{n\times n}$ a $k, l \in \mathbb{N}$ platí $\boldsymbol{A}^k \cdot \boldsymbol{A}^l = \boldsymbol{A}^{k+l}$ a $(\boldsymbol{A}^k)^l = \boldsymbol{A}^{kl}$.

(c) Pre regulárnu maticu $\boldsymbol{A} \in K^{n\times n}$ rozšírte definíciu jej mocniny $\boldsymbol{A}^k$ na ľubovovoľný celočíselný exponent k a dokážte rovnosti $\boldsymbol{A}^k \cdot \boldsymbol{A}^l = \boldsymbol{A}^{k+l}$, $(\boldsymbol{A}^k)^l = \boldsymbol{A}^{kl}$ pre všetky $k, l \in \mathbb{Z}$ (porovnaj s cvičením 2.13).

(d) Za akých okolností platí pre matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ rovnosť $(\boldsymbol{A}\cdot\boldsymbol{B})^k = \boldsymbol{A}^k \cdot \boldsymbol{B}^k$ pre ľubovoľné $k \in \mathbb{N}$?

(e) Za akých okolností platí pre regulárne matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ rovnosť $(\boldsymbol{A}\cdot\boldsymbol{B})^k = \boldsymbol{B}^k \cdot \boldsymbol{A}^k$ pre ľubovoľné $k \in \mathbb{Z}$?

(f) Nájdite príklad regulárnych matíc $\boldsymbol{A}$, $\boldsymbol{B} \in \mathbb{R}^{2\times 2}$ takých, že všetky štyri matice $(\boldsymbol{A}\cdot\boldsymbol{B})^{-2}$, $(\boldsymbol{B}\cdot\boldsymbol{A})^{-2}$, $\boldsymbol{A}^{-2}\cdot\boldsymbol{B}^{-2}$, $\boldsymbol{B}^{-2}\cdot\boldsymbol{A}^{-2}$ sú rôzne. Dá sa táto úloha riešiť aj bez počítania inverzných matíc?

7.4. Nech $\boldsymbol{P} \in K^{n\times n}$ je regulárna matica. Potom pre ľubovoľné matice $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{B} \in K^{n\times q}$ platí $h(\boldsymbol{A}\cdot\boldsymbol{P}) = h(\boldsymbol{A})$, $h(\boldsymbol{P}\cdot\boldsymbol{B}) = h(\boldsymbol{B})$. Dokážte.

7.5. Zistite, či uvedená matica $\boldsymbol{A}$ nad poľom K je regulárna; v tom prípade vypočítajte k nej inverznú maticu $\boldsymbol{A}^{-1}$:

(a) $K = \mathbb{Q}$, $\boldsymbol{A} = \begin{pmatrix} 3 & 2 & 1 \\ 4 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}$;

(b) $K = \mathbb{R}$, $\boldsymbol{A} = \begin{pmatrix} 1 & \sqrt{2} & \sqrt{6} \\ 0 & 1 & \sqrt{3} \\ 0 & 0 & 1 \end{pmatrix}$;

(c) $K = \mathbb{C}$, $\boldsymbol{A} = \begin{pmatrix} 1+2\mathrm{i} & 1-\mathrm{i} \\ \mathrm{i}-2 & 1 \end{pmatrix}$;

(d) $K = \mathbb{C}$, $\boldsymbol{A} = \begin{pmatrix} 1+2\mathrm{i} & 1-\mathrm{i} \\ \mathrm{i}-2 & 1+\mathrm{i} \end{pmatrix}$;

(e) $K=\mathbb{Z}_2$, $\boldsymbol{A}=\left(\begin{smallmatrix}1&1&0\\1&0&1\\0&1&1\end{smallmatrix}\right)$; (f) $K=\mathbb{Z}_3$, $\boldsymbol{A}=\left(\begin{smallmatrix}1&1&0\\1&0&1\\0&1&1\end{smallmatrix}\right)$.

7.6. Pre matice $\boldsymbol{A}$, $\boldsymbol{B}$ nad poľom $\mathbb{R}$ vypočítajte maticu $\boldsymbol{C}=\boldsymbol{A}^{-1}\cdot\boldsymbol{B}$ (ak $\boldsymbol{A}$ je regulárna):

(a) $\boldsymbol{A}=\left(\begin{smallmatrix}-2&1\\3&-2\end{smallmatrix}\right)$, $\boldsymbol{B}=\left(\begin{smallmatrix}2&1&-1\\3&2&-5\end{smallmatrix}\right)$; (b) $\boldsymbol{A}=\begin{pmatrix}2&1&3\\1&-2&0\\3&0&3\end{pmatrix}$, $\boldsymbol{B}=\begin{pmatrix}2&1\\2&2\\-2&0\end{pmatrix}$

Ako skúšku správnosti vypočítajte maticu $\boldsymbol{A}\cdot\boldsymbol{C}$ – mali by ste dostať $\boldsymbol{B}$.

7.7. Pre matice $\boldsymbol{A}$, $\boldsymbol{B}$ nad poľom $\mathbb{R}$ vypočítajte maticu $\boldsymbol{C}=\boldsymbol{A}\cdot\boldsymbol{B}^{-1}$ (ak $\boldsymbol{B}$ je regulárna)

(a) $\boldsymbol{A}\begin{pmatrix}-2&1&1\\-3&0&5\\0&2&3\end{pmatrix}$, $\boldsymbol{B}=\begin{pmatrix}0&1&1\\0&2&5\\1&0&0\end{pmatrix}$; (b) $\boldsymbol{A}=\left(\begin{smallmatrix}2&5\\1&0\\7&4\end{smallmatrix}\right)$, $\boldsymbol{B}=\left(\begin{smallmatrix}2&1\\2&2\end{smallmatrix}\right)$.

Ako skúšku správnosti vypočítajte maticu $\boldsymbol{C}\cdot\boldsymbol{B}$ – mali by ste dostať $\boldsymbol{A}$.

7.8. Ná základe skúseností nadobudnutých v cvičeniach 7.5, 7.6 a 7.7 dokážte tvrdenie 7.3.1.

7.9. Nájdite inverzné matice k maticiam $\boldsymbol{R}_\alpha$, $\boldsymbol{S}_\alpha$ z príkladov 6.4.3., 6.4.4. Vysvetlite geometrický význam získaných výsledkov.

7.10. Bázy $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ vektorového priestoru $\mathbb{R}^3$ sú tvorené stĺpcami matíc $\left(\begin{smallmatrix}1&1&1\\0&1&1\\0&0&1\end{smallmatrix}\right)$ resp. $\left(\begin{smallmatrix}1&0&0\\-1&1&0\\0&-1&1\end{smallmatrix}\right)$

(a) Nájdite matice prechodu $\boldsymbol{P}_{\boldsymbol{\varepsilon},\boldsymbol{\alpha}}$, $\boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\varepsilon}}$, $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ a $\boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\alpha}}$.

(b) Vektor $\boldsymbol{x}\in\mathbb{R}^3$ má vzhľadom na bázu $\boldsymbol{\beta}$ súradnice $(2,7,1)^T$. Nájdite vektor $\boldsymbol{x}$ ako aj jeho súradnice vzhľadom na bázu $\boldsymbol{\alpha}$.

7.11. Báza $\boldsymbol{\alpha}$ vektorového priestoru $\mathbb{R}^3$ je tvorená stĺpcami matice $\left(\begin{smallmatrix}1&0&1\\2&1&3\\0&2&1\end{smallmatrix}\right)$. Nájdite bázy $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$ priestoru $\mathbb{R}^3$, ak poznáte matice prechodu $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}=\left(\begin{smallmatrix}1&2&1\\2&1&2\\1&0&1\end{smallmatrix}\right)$ a $\boldsymbol{P}_{\boldsymbol{\gamma},\boldsymbol{\alpha}}=\left(\begin{smallmatrix}0&1&0\\2&0&1\\1&1&1\end{smallmatrix}\right)$. Vypočítajte matice prechodu $\boldsymbol{P}_{\boldsymbol{\beta},\boldsymbol{\gamma}}$ a $\boldsymbol{P}_{\boldsymbol{\gamma},\boldsymbol{\beta}}$.

7.12. Lineárne zobrazenie $\varphi:\mathbb{R}^3\to\mathbb{R}^4$ je dané predpisom $\varphi(x,y,z)^T=(x+y,x-y,3x+y+z,z)^T$.

(a) Nájdite maticu zobrazenia φ vzhľadom na bázy $\boldsymbol{\beta}$ priestoru $\mathbb{R}^3$ a $\boldsymbol{\alpha}$ priestoru $\mathbb{R}^4$ tvorené stĺpcami matíc $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix}$ resp. $\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & -1 & 1 & -1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

(b) Nech $\boldsymbol{x} = (1, -4, 3)^T \in \mathbb{R}^3$. Nájdite súradnice vektora $\varphi(\boldsymbol{x}) \in \mathbb{R}^4$ vzhľadom na bázu $\boldsymbol{\alpha}$.

(c) Vektor $\boldsymbol{y} \in \mathbb{R}^3$ má vzhľadom na bázu $\boldsymbol{\beta}$ súradnice $(1, 1, 1)^T$. Nájdite vektor $\varphi(\boldsymbol{y}) \in \mathbb{R}^4$.

(d) Každú z úloh (b), (c) možno riešiť dvoma spôsobmi – vysvetlite ako.

(e) Určte hodnosť h zobrazenia ψ a nájdite nejaké bázy priestorov $\mathbb{R}^3$, $\mathbb{R}^4$, vzhľadom na ktoré má matica φ blokový tvar $\begin{pmatrix} \boldsymbol{I}_h & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}$. Napíšte explicitne túto maticu.

7.13. Lineárne zobrazenie $\psi : \mathbb{R}^4 \to \mathbb{R}^3$ má vzhľadom na bázy $\boldsymbol{\beta}$ priestoru $\mathbb{R}^4$ a $\boldsymbol{\alpha}$ priestoru $\mathbb{R}^3$ tvorené stĺpcami matíc $\boldsymbol{A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ $\boldsymbol{A} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ maticu $\boldsymbol{A} = \begin{pmatrix} 0 & 5 & 0 & 7 \\ 1 & 1 & 2 & 2 \\ 5 & 2 & 9 & 0 \end{pmatrix}$.

(a) Nájdite maticu zobrazenia ψ vzhľadom na kanonické bázy $\boldsymbol{\varepsilon}^{(4)}$, $\boldsymbol{\varepsilon}^{(3)}$.

(b) Nech $\boldsymbol{u} = (2, 1, 0, -1)^T \in \mathbb{R}^4$. Nájdite súradnice vektora $\psi(\boldsymbol{u}) \in \mathbb{R}^3$ vzhľadom na bázu $\boldsymbol{\alpha}$.

(c) Vektor $\boldsymbol{v} \in \mathbb{R}^4$ má vzhľadom na bázu $\boldsymbol{\beta}$ súradnice $(1, -1, 1, -1)^T$. Nájdite vektor $\psi(\boldsymbol{v}) \in \mathbb{R}^3$.

(d) Každú z úloh (b), (c) možno riešiť dvoma spôsobmi – vysvetlite ako.

(e) Určte hodnosť h zobrazenia ψ a nájdite nejaké bázy priestorov $\mathbb{R}^4$, $\mathbb{R}^3$, vzhľadom na ktoré má matica ψ blokový tvar $\begin{pmatrix} \boldsymbol{I}_h & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}$. Napíšte explicitne túto maticu.

7.14. Dokážte, že $\boldsymbol{\zeta} = \boldsymbol{\zeta}^{(n)} = (1, 1+x, (1+x)^2, \ldots, (1+x)^n)$ je bázou vektorového priestoru $\mathbb{R}^{(n)}[x]$ a nájdite matice prechodu $\boldsymbol{P}_{\boldsymbol{\xi},\boldsymbol{\zeta}}$, $\boldsymbol{P}_{\boldsymbol{\zeta},\boldsymbol{\xi}}$, kde $\boldsymbol{\xi} = \boldsymbol{\xi}^{(n)} = (1, x, x^2, \ldots, x^n)$ je kanonická báza priestoru $\mathbb{R}^{(n)}[x]$.

7.15. Podľa cvičenia 6.10 je $\boldsymbol{\eta}^{(n)} = \boldsymbol{\eta} = \big(1, x, [x]_2, \ldots, [x]_n\big)$ bázou vektorového priestoru $\mathbb{R}^{(n)}[x]$. Pre $0 \le k, m \le n$ označme $s(m,k)$ prvok na mieste (k,m) matice prechodu $\boldsymbol{P}_{\boldsymbol{\xi},\boldsymbol{\eta}}$ a $S(m,k)$ prvok na mieste (k,m) matice prechodu $\boldsymbol{P}_{\boldsymbol{\eta},\boldsymbol{\xi}}$. To znamená, že pre $0 \le m \le n$ platí $[x]_m = \sum_{k=0}^n s(m,k)x^k$ a

$x^m = \sum_{k=0}^{n} S(m,k)[x]_k$. Koeficienty $s(m,k)$, $S(m,k)$ sa nazývajú *Stirlingove čísla prvého* resp. *druhého druhu*.

(a) Dokážte, že Stirlingove čísla prvého druhu vyhovujú podmienkam $s(0,0) = 1$, $s(n,0) = 0$ pre $n \geq 1$, $s(n,n) = 1$ a $s(n,k) = 0$ pre $k > n$.

(b) Dokážte, že pre $1 \leq k \leq n$ platí $s(n+1,k) = s(n,k-1) - ns(n,k)$. (*Návod*: Vyjadrite polynóm $[x]_{n+1} = [x]_n(x-n)$ dvojakým spôsobom a porovnajte koeficienty pri x^k.)

(c) Označme $c(n,k)$ počet všetkých permutácií n-prvkovej množiny, pozostávajúcich z práve k disjunktných cyklov (vrátane 1-cyklov) – pozri cvičenie 0.14. Dokážte, že čísla $c(n,k)$ vyhovujú podmienkam $c(0,0) = 1$, $c(n,0) = 0$ pre $n \geq 1$, $c(n,n) = 1$ a $c(n,k) = 0$ pre $k > n$.

(d) Kombinatorickou úvahou dokážte rovnosť $c(n+1,k) = c(n,k-1) + nc(n,k)$ pre $1 \leq k \leq n$. (*Návod*: Všetky permutácie $(n+1)$-prvkovej množiny $\{0,1,\ldots,n\}$ pozostávajúce z k disjunktných cyklov rozdeľte do dvoch skupín podľa toho, či obsahujú alebo neobsahujú 1-cyklus (0). Ukážte, že prvých je $c(n,k-1)$ a druhých $nc(n,k)$.)

(e) Na základe (a), (b), (c) a (d) dokážte, že pre všetky $k,n \in \mathbb{N}$ platí $c(n,k) = (-1)^{n-k}s(n,k) = |s(n,k)|$. Čísla $c(n,k)$ sa nazývajú *znamienkovo prosté Stirlingove čísla prvého druhu*.

(f) Uvedomte si, že (c), (d) sú vlastne akýmisi pravidlami modifikovaného Pascalovho trojuholníka pre čísla $c(n,k)$. Vypočítajte hodnoty týchto čísel pre $n \leq 5$, $0 \leq k \leq n$.

(g) Dokážte, že Stirlingove čísla druhého druhu vyhovujú podmienkam $S(0,0) = 1$, $S(n,0) = 0$ pre $n \geq 1$, $S(n,n) = 1$ a $S(n,k) = 0$ pre $k > n$.

(h) Dokážte, že pre $1 \leq k \leq n$ platí $S(n+1,k) = S(n,k-1) + kS(n,k)$. (*Návod*: S využitím rovnosti $[x]_{k+1} = [x]_k(x-k)$ vyjadrite polynóm $x^{n+1} = x^n x$ dvojakým spôsobom a porovnajte koeficienty pri $[x]_k$.)

(i) Označme $\overline{S}(n,k)$ počet všetkých rozkladov n-prvkovej množiny, pozostávajúcich z práve k disjunktných množín – pozri paragraf 0.6 Dokážte, že čísla $\overline{S}(n,k)$ vyhovujú podmienkam $\overline{S}(0,0) = 1$, $\overline{S}(n,0) = 0$ pre $n \geq 1$, $\overline{S}(n,n) = 1$ a $\overline{S}(n,k) = 0$ pre $k > n$.

(j) Kombinatorickou úvahou dokážte rovnosť $\overline{S}(n+1,k) = \overline{S}(n,k-1) + k\overline{S}(n,k)$ pre $1 \leq k \leq n$. (*Návod*: Všetky rozklady $(n+1)$-prvkovej množiny $\{0,1,\ldots,n\}$ na k disjunktných podmnožín rozdeľte do dvoch skupín podľa toho, či obsahujú alebo neobsahujú jednoprvkovú množinu $\{0\}$. Ukážte, že prvých je $\overline{S}(n,k-1)$ a druhých $k\overline{S}(n,k)$.)

(k) Na základe (g), (h), (i) a (j) dokážte, že pre všetky $k,n \in \mathbb{N}$ platí $\overline{S}(n,k) = S(n,k)$.

(l) Uvedomte si, že (g), (h) sú vlastne akýmisi pravidlami modifikovaného Pascalovho trojuholníka pre čísla $S(n,k)$. Vypočítajte hodnoty týchto čísel pre $n \leq 5$, $0 \leq k \leq n$.

7.16. (a) Nech $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ sú dve bázy konečnorozmerného vektorového priestoru V a $\vartheta : V \to V$ je lineárna transformácia taká, že $\vartheta(\boldsymbol{\alpha}) = \boldsymbol{\beta}$. Potom $(\vartheta)_{\boldsymbol{\beta}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$. Dokážte.

(b) Nech $\boldsymbol{\gamma}$ je tretia báza vo V a $\eta : V \to V$ je lineárna transformácia taká, že $\eta(\boldsymbol{\beta}) = \boldsymbol{\gamma}$. Odvoďte nasledujúce vyjadrenie pre maticu zloženej transformácie $\eta \circ \vartheta$ vo výslednej báze $\boldsymbol{\gamma}$ pomocou jej *predchádzajúcich* polôh $\boldsymbol{\alpha}$ a $\boldsymbol{\beta}$: $(\eta \circ \vartheta)_{\boldsymbol{\gamma}} = (\vartheta)_{\boldsymbol{\beta}} \circ (\eta)_{\boldsymbol{\gamma}}$.

(c) Zovšeobecnite (b) na ľubovoľný počet k lineárnych transformácií a $k+1$ báz podľa vzoru vety 7.6.1.

7.17. (a) Pre ľubovoľnú dvojicu vektorov $\boldsymbol{e}_i \neq \boldsymbol{e}_j$ kanonickej bázy $\boldsymbol{\varepsilon}$ v $\mathbb{R}^3$ nájdite maticu $(\Omega)_{\boldsymbol{\varepsilon}}$ transformácie Ω, ktorá vznikne zložením otočenia Ω_1 okolo osi $[\boldsymbol{e}_i]$ o uhol φ s otočením Ω_2 okolo osi $[\boldsymbol{e}_j]$ o uhol ψ.

(b) Na základe (a) nájdite maticu otočenia o uhol ψ okolo priamky, ktorá leží v rovine $[\boldsymbol{e}_i, \boldsymbol{e}_j]$ a zviera s osou $[\boldsymbol{e}_i]$ uhol φ, vzhľadom na bázu $\boldsymbol{\varepsilon}$. (Všetky otočenia orientujte podľa pravidla pravej ruky.)

(c) Riešte úlohy (a) a (b) pre niekoľko konkrétnych volieb bázických vektorov $\boldsymbol{e}_i$, $\boldsymbol{e}_j$ a uhlov φ, ψ.

7.18. Nech $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n)$ je nejaká báza vektorového priestoru V nad poľom K a $\boldsymbol{\beta} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ je ľubovoľná usporiadaná m-tica vektorov z V. Uvedomte si, že maticu $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \big((\boldsymbol{v}_1)_{\boldsymbol{\alpha}}, \ldots, (\boldsymbol{v}_m)_{\boldsymbol{\alpha}}\big) \in K^{n\times m}$ možno definovať aj za takýchto všeobecnejších pomienok a dokážte nasledujúce tvrdenia:

(a) Pre hodnosť matice $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ platí $h(\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}) = \dim[\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m]$.

(b) Ak $m = n$, tak matica $\boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je regulárna práve vtedy, keď aj $\boldsymbol{\beta}$ je báza priestoru V.

(c) Ak $m = n$, tak pre jednoznačne určené (nie nutne bijektívne) lineárne zobrazenie $\vartheta : V \to V$ také, že $\vartheta(\boldsymbol{u}_i) = \boldsymbol{v}_i$ pre $i \leq n$ stále platí $(\vartheta)_{\boldsymbol{\alpha}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}}$.

8. Afinné podpriestory a afinné zobrazenia

Keď sme v paragrafe 4.1, odvolávajúc sa na geometrický názor, ilustrovali pojem lineárneho podpriestoru, ako príklad sme uviedli, že netriválne vlastné lineárne podpriestory „nášho“ trojrozmerného vektorového priestoru $\mathbb{R}^3$ sú práve priamky a roviny *prechádzajúce počiatkom* $\mathbf{0}$. Kritickejší čitateľ mohol vtedy oprávnene zapochybovať o adekvátnosti a prirodzenosti tohto pojmu, či aspoň pocítiť potrebu zaviesť taký pojem podpriestoru, ktorý by napr. v $\mathbb{R}^3$ zahŕňal *všetky* priamky a roviny, nielen tie prechádzajúce počiatkom. Podobne sme v paragrafe 6.1 hneď po definícii pojmu lineárneho zobrazenia boli nútení učiniť poznámku o jeho odlišnosti od pojmu lineárnej funkcie používaného v matematickej analýze. Vzápätí sme prijali záväzok, že sa s týmto nedostatkom v príhodný čas vyrovnáme.

Ten čas práve nastal. Spomínané medzery zaplníme definíciami pojmu *afinného podpriestoru* alebo tiež *lineárnej variety* a pojmu *afinného zobrazenia*. *Afinita* znamená *príbuznosť, spriaznenosť*. Čitateľ sám uvidí, že objekty označené prívlastkom „afinný“ sú úzko spriaznené so zodpovedajúcimi objektmi nesúcimi prívlastok „lineárny“. Ťažiskom kapitoly bude klasifikácia vzájomnej polohy afinných podpriestorov vo vektorovom priestore.

8.1. Body a vektory

Na vektory, čiže na prvky vektorových priestorov – aspoň pokiaľ ide o konečnorozmerné vektorové priestory nad $\mathbb{R}$, – sa dívame ako na orientované úsečky s počiatkom v bode $\mathbf{0}$.

Už táto veta prezrádza, že *pôvodne* sa na prvky takéhoto priestoru dívame ako na *body* a celý priestor chápeme ako *homogénny*, t. j. všetky body považujeme za rovnocenné a nevyčleňujeme v ňom nijaký privilegovaný bod za počiatok. Až na základe tohto pôvodného porozumenia dokážeme po vyčlenení nejakého počiatku O (ktorým sa môže stať ľubovoľný bod homogénneho priestoru) nahradiť bod A príslušného priestoru orientovanou úsečkou $\overrightarrow{OA}$ a následne abstrahovať od jej polohy, to znamená uvidieť za ňou *vektor* $\boldsymbol{u} = \overrightarrow{OA}$, daný len jej veľkosťou, smerom a orientáciou, ktorý možno umiestniť do ľubovoľného bodu priestoru – nielen do počiatku.

Afinným priestorom nad poľom K rozumieme vektorový priestor V nad týmto poľom, pri pohľade na ktorý sme sa vrátili k onomu pôvodnému porozumeniu jeho štruktúre a prvkom. Tie sa z vektorov stali opäť bodmi a počiatok (t. j. nulový vektor) stratil svoje výsadné postavenie – stal sa z neho bod ako každý iný.

Formálnu definíciu afinného priestoru nad poľom K tu uvádzať nebudeme. Sme totiž toho názoru, že matematická formalizácia rozdielu medzi oboma spomínanými pohľadmi na prvky vektorového priestoru by v tejto chvíli vniesla do veci viac zmätku než svetla. Celkom postačí, keď úlohu prepínača medzi oboma pohľadmi zveríme dvojiciam slov „bod“ – „vektor“ a „afinný“,– „lineárny“, prípadne „afinný“ – „vektorový“. Na druhej strane však pred nami vyvstáva potreba formálnej definície podmnožín vektorového priestoru, ktoré sú „vernými kópiami“ lineárnych podpriestorov – nemusia však prechádzať počiatkom, ale možu byť umiestnené „kdekoľvek“.

8.2. Afinné podpriestory

V celom tomto a nasledujúcich dvoch paragrafoch V označuje nejaký pevný, no inak ľubovoľný, vektorový priestor nad poľom K a m, n sú prirodzené čísla.

Kvôli pohodliu čitateľa budeme písmenami $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$ (možno s indexmi) značiť výlučne body, $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ označujú zasa výlučne vektory, kým $\boldsymbol{x}$, $\boldsymbol{y}$, $\boldsymbol{z}$ môžu podľa potreby označovať body i vektory. Taktiež sa dohodneme, že rozdiel dvoch bodov budeme chápať ako vektor, kým súčet bodu a vektora ako bod.

Nech $\boldsymbol{p}, \boldsymbol{q} \in V$, $\boldsymbol{p} \neq \boldsymbol{q}$. *Priamkou* prechádzajúcou alebo tiež určenou bodmi $\boldsymbol{p}, \boldsymbol{q}$ rozumieme množinu $\ell(\boldsymbol{p}, \boldsymbol{q})$, ktorú dostaneme tak, že do bodu $\boldsymbol{p}$ umiestnime všetky možné skalárne násobky vektora $\boldsymbol{q} - \boldsymbol{p}$. Typický bod priamky $\ell(\boldsymbol{p}, \boldsymbol{q})$ má teda

$$\boldsymbol{x} = \boldsymbol{p} + t(\boldsymbol{q} - \boldsymbol{p}) = (1 - t)\boldsymbol{p} + t\boldsymbol{q},$$

kde $t \in K$, čiže

$$\ell(\boldsymbol{p}, \boldsymbol{q}) = \{s\boldsymbol{p} + t\boldsymbol{q};\ s, t \in K \ \&\ s + t = 1\} \subseteq V.$$

tvar Tento výraz má, samozrejme, zmysel aj pre $\boldsymbol{p} = \boldsymbol{q}$, vtedy však nejde o priamku ale o jednobodovú množinu $\ell(\boldsymbol{p}, \boldsymbol{p}) = \{\boldsymbol{p}\}$. Z uvedeného tvaru ihneď vidíme, že

$$\ell(\boldsymbol{p}, \boldsymbol{q}) = \ell(\boldsymbol{q}, \boldsymbol{p})$$

pre ľubovoľné $\boldsymbol{p}, \boldsymbol{q} \in V$.

Lineárnu kombináciu, t. j. výraz tvaru

$$t_0\boldsymbol{p}_0 + t_1\boldsymbol{p}_1 + \ldots + t_n\boldsymbol{p}_n = \sum_{i=0}^{n} t_i\boldsymbol{p}_i,$$

kde $n \in \mathbb{N}$, $\boldsymbol{p}_0, \dots, \boldsymbol{p}_n \in V$, $t_0, t_1, \dots, t_n \in K$, nazývame *afinnou* alebo tiež *barycentrickou*[1] *kombináciou* bodov $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n$, ak platí $t_0 + t_1 + \ldots + t_n = 1$. Výsledok afinnej kombinácie bodov budeme chápať ako bod; iné lineárne kombinácie bodov ako afinné sa v našich úvahách nevyskytnú. (Ešte si všimnite, že každá afinná kombinácia je neprázdna, t. j. obsahuje aspoň jeden člen.)

Neprázdnu podmnožinu M vektorového priestoru V nazývame jeho *afinným podpriestorom*, prípadne *lineárnou varietou* vo V, ak pre všetky body $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r} \in M$ a každý skalár $s \in K$ platí

$$s\boldsymbol{p} + (1-s)\boldsymbol{q} \in M \qquad \text{a} \qquad \boldsymbol{p} - \boldsymbol{q} + \boldsymbol{r} \in M.$$

Inak povedané, $\emptyset \neq M \subseteq V$ je afinný podpriestor, ak M je uzavretá vzhľadom na afinné kombinácie uvedených dvoch typov. Prvá podmienka znamená, že pre všetky $\boldsymbol{p}, \boldsymbol{q} \in M$ platí $\ell(\boldsymbol{p}, \boldsymbol{q}) \subseteq M$, t. j. M s každou dvojicou bodov obsahuje celú priamku nimi určenú. Druhú podmienku dodávame len kvôli poliam charakteristiky 2; ak $\operatorname{char} K \neq 2$, tak už vyplýva z prvej, takže je vlastne zbytočná. Na druhej strane, napr. vo vektorovom priestore V nad poľom $\mathbb{Z}_2$ pre všetky body $\boldsymbol{p}, \boldsymbol{q} \in V$ platí $\ell(\boldsymbol{p}, \boldsymbol{q}) = \{\boldsymbol{p}, \boldsymbol{q}\}$, teda len prvej podmienke by vyhovovala *každá podmnožina* $M \subseteq V$. Podrobnejšie o tom pojednáva nasledujúce tvrdenie, ktoré je očividne analógiou tvrdenia 4.1.2.

8.2.1. Tvrdenie. *Pre ľubovoľnú neprázdnu množinu $M \subseteq V$ nasledujúce podmienky sú ekvivalentné:*

(i) *M je afinný podpriestor vo V, t. j. pre ľubovoľné $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r} \in M$, $s \in K$ platí $s\boldsymbol{p} + (1-s)\boldsymbol{q} \in M$ a $\boldsymbol{p} - \boldsymbol{q} + \boldsymbol{r} \in M$;*

[1] *Barycentrum* znamená *ťažisko*.

(ii) *M je uzavretá vzhľadom na ľubovoľné afinné kombinácie trojíc bodov, t. j. pre všetky $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r} \in M$, $s, t \in K$ platí $s\boldsymbol{p} + t\boldsymbol{q} + (1 - s - t)\boldsymbol{r} \in M$;*

(iii) *M je uzavretá vzhľadom na akékoľvek afinné kombinácie, t. j. pre všetky $n \in \mathbb{N}$, body $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n \in M$ a skaláry $t_0, t_1, \dots, t_n \in K$ také, že $t_0 + t_1 + \ldots + t_n = 1$, platí $t_0\boldsymbol{p}_0 + t_1\boldsymbol{p}_1 + \ldots + t_n\boldsymbol{p}_n \in M$;*

Ak $\operatorname{char} K \neq 2$, *tak uvedené podmienky sú navyše ekvivalentné s podmienkou*

(i^-) *pre ľubovoľné $\boldsymbol{p}, \boldsymbol{q} \in M$, $s \in K$ platí $s\boldsymbol{p} + (1 - s)\boldsymbol{q} \in M$.*

Dôkaz. Implikácie (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) sú zrejmé aj bez predpokladu $\operatorname{char} K \neq 2$. Dokážeme implikáciu (i) $\Rightarrow$ (iii); pri dôkaze vyjde navyše najavo, že pre $\operatorname{char} K \neq 2$ stačí na odvodenie záveru (iii) slabšia podmienka (i^-) miesto (i).

Predpokladajme (i) (teda tým skôr (i^-)) a pripusťme, že podmienka (iii) neplatí. Označme n najmenšie prirodzené číslo, pre ktoré to nastane. Potom $n \geq 2$ a pre všetky $k < n$ podmienka (iii) platí, čiže M je uzavretá na afinné kombinácie $\leq n$ bodov. Nech $\boldsymbol{p}_0, \dots, \boldsymbol{p}_n \in M$, $t_0, \dots, t_n \in K$ sú také, že $t_0 + \ldots + t_n = 1$ a $t_0\boldsymbol{p}_0 + \ldots + t_n\boldsymbol{p}_n \notin M$. Treba zvážiť dve možnosti.

(a) Ak $t_i \neq 1$ pre aspoň jedno $i \leq n$, tak bez ujmy na všeobecnosti môžeme predpokladať, že $t_0 \neq 1$. Označme

$$\boldsymbol{q} = \frac{t_1}{1 - t_0}\boldsymbol{p}_1 + \ldots + \frac{t_n}{1 - t_0}\boldsymbol{p}_n.$$

Keďže

$$\frac{t_1}{1 - t_0} + \ldots + \frac{t_n}{1 - t_0} = \frac{t_1 + \ldots + t_n}{1 - t_0} = 1,$$

$\boldsymbol{q} \in M$, lebo $\boldsymbol{q}$ je afinnou kombináciou n bodov z M. Potom

$$t_0\boldsymbol{p}_0 + t_1\boldsymbol{p}_1 + \ldots + t_n\boldsymbol{p}_n = t_0\boldsymbol{p}_0 + (1 - t_0)\boldsymbol{q} \in M$$

vyplýva už z podmienky (i$^-$). To je však spor.

(b) Ak $t_i = 1$ pre všetky $i \le n$, tak ide o afinnú kombináciu $\boldsymbol{p}_0 + \boldsymbol{p}_1 + \ldots + \boldsymbol{p}_{n-1} + \boldsymbol{p}_n$ a $t_1 + \ldots + t_{n-1} = -1$. Potom $\boldsymbol{q} = -\boldsymbol{p}_1 - \ldots - \boldsymbol{p}_{n-1}$ je afinnou kombináciou $n-1$ bodov z M, teda $\boldsymbol{q} \in M$. Podľa druhej z podmienok v (i) máme

$$\boldsymbol{p}_0 + \boldsymbol{p}_1 + \ldots + \boldsymbol{p}_{n-1} + \boldsymbol{p}_n = \boldsymbol{p}_0 - \boldsymbol{q} + \boldsymbol{p}_n \in M,$$

čo je opäť spor.

Ak $\operatorname{char} K \neq 2$, možno sa zaobísť bez tejto podmienky. Keďže $\frac{1}{2} + \frac{1}{2} = 1$, už z (i$^-$) vyplýva $\frac{1}{2}\boldsymbol{p}_0 + \frac{1}{2}\boldsymbol{p}_n \in M$. Nakoľko $2 + (-1) = 1$, opäť len z (i$^-$) dostávame

$$\boldsymbol{p}_0 + \boldsymbol{p}_1 + \ldots + \boldsymbol{p}_{n-1} + \boldsymbol{p}_n = 2\left(\frac{1}{2}\boldsymbol{p}_0 + \frac{1}{2}\boldsymbol{p}_n\right) - \boldsymbol{q} \in M.$$

Poznámka. Ak $\operatorname{char} K = \infty$, tak možnosť (b) zrejme nemôže nastať, teda v uvedenom dôkaze stačí uvažovať len možnosť (a). Zároveň vidno, že v druhej časti bodu (b) je podstatný predpoklad $\operatorname{char} K \neq 2$. Bez neho by sme totiž nevedeli zaručiť existenciu prvku $1/2 = 2^{-1} \in K$ inverzného k prvku $2 = 1 + 1 \in K$.

Nasledujúca veta ukazuje, že afinné podpriestory skutočne nie sú ničím iným, než lineárnymi podpriestormi posunutými do ľubovoľného bodu príslušného vektorového priestoru.

8.2.2. Veta. *Nech $M \subseteq V$. Potom M je afinný podpriestor vo V práve vtedy, keď existuje bod $\boldsymbol{p} \in V$ a lineárny podpriestor $S \subseteq V$ taký, že*

$$M = \boldsymbol{p} + S = \{\boldsymbol{p} + \boldsymbol{u};\ \boldsymbol{u} \in S\}.$$

V tom prípade pre všetky $\boldsymbol{q}, \boldsymbol{r} \in M$, $\boldsymbol{u} \in S$ platí

$$\boldsymbol{q} - \boldsymbol{r} \in S, \qquad \boldsymbol{q} + \boldsymbol{u} \in M, \qquad M = \boldsymbol{q} + S,$$
$$S = \{\boldsymbol{x} - \boldsymbol{q};\ \boldsymbol{x} \in M\} = \{\boldsymbol{x} - \boldsymbol{y};\ \boldsymbol{x}, \boldsymbol{y} \in M\}.$$

Dôkaz. Nech $M \subseteq V$ je afinný podpriestor a $\boldsymbol{p} \in M$ je jeho ľubovoľný bod. Položme

$$S = \{\boldsymbol{x} - \boldsymbol{p};\ \boldsymbol{x} \in M\}.$$

Potom zrejme $M = \boldsymbol{p} + S$. Stačí teda dokázať, že $S \subseteq V$ je lineárny podpriestor. Keďže $\boldsymbol{p} \in M$, platí $\boldsymbol{0} = \boldsymbol{p} - \boldsymbol{p} \in S$. Ukážeme uzavretosť S na lineárne kombinácie. Nech $\boldsymbol{u}, \boldsymbol{v} \in S$, $a, b \in K$. Potom $\boldsymbol{u} = \boldsymbol{x} - \boldsymbol{p}$, $\boldsymbol{v} = \boldsymbol{y} - \boldsymbol{p}$ pre nejaké $\boldsymbol{x}, \boldsymbol{y} \in M$. Jednoduchý výpočet dáva

$$a\boldsymbol{u} + b\boldsymbol{v} = a(\boldsymbol{x} - \boldsymbol{p}) + b(\boldsymbol{y} - \boldsymbol{p}) = a\boldsymbol{x} + b\boldsymbol{y} + (1 - a - b)\boldsymbol{p} - \boldsymbol{p}.$$

Prvé tri sčítance tvoria afinnú kombináciu bodov z M, teda $a\boldsymbol{x} + b\boldsymbol{y} + (1 - a - b)\boldsymbol{p} \in M$; preto tiež $a\boldsymbol{u} + b\boldsymbol{v} \in S$

Nech naopak $M = \boldsymbol{p} + S$ pre nejaký bod $\boldsymbol{p} \in V$ a lineárny podpriestor $S \subseteq V$. Podľa tvrdenia 8.2.1. stačí ukázať uzavretosť M na afinné kombinácie trojíc. Nech $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in M$, $s, t \in K$. Potom $\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{u}$, $\boldsymbol{y} = \boldsymbol{p} + \boldsymbol{v}$, $\boldsymbol{z} = \boldsymbol{p} + \boldsymbol{w}$ pre nejaké $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in S$. Počítajme

$$\begin{aligned} s\boldsymbol{x} + t\boldsymbol{y} + (1 - s - t)\boldsymbol{z} &= s(\boldsymbol{p} + \boldsymbol{u}) + t(\boldsymbol{p} + \boldsymbol{v}) + (1 - s - t)(\boldsymbol{p} + \boldsymbol{w}) \\ &= \boldsymbol{p} + s\boldsymbol{u} + t\boldsymbol{v} + (1 - s - t)\boldsymbol{w}. \end{aligned}$$

Keďže $t\boldsymbol{u} + s\boldsymbol{v} + (1-s-t)\boldsymbol{w} \in S$, dostávame $s\boldsymbol{x} + t\boldsymbol{y} + (1-s-t)\boldsymbol{z} \in M$.

Ďalšie tri podmienky možno teraz overiť priamymi výpočtami, ktoré prenechávame čitateľovi; štvrtá z nich okamžite vyplýva.

8.2.3. Dôsledok. *Každý lineárny podpriestor S vektorového priestoru V je jeho afinným podpriestorom. Afinný podpriestor M vektorového priestoru V je jeho lineárnym podpriestorom práve vtedy, keď $\mathbf{0} \in M$.*

Zameraním alebo tiež *smerovým podpriestorom* afinného podpriestoru $M \subseteq V$ nazývame lineárny podpriestor

$$\operatorname{Dir} M = \{\boldsymbol{x} - \boldsymbol{y};\ \boldsymbol{x}, \boldsymbol{y} \in M\} \subseteq V.$$

(Označenie pochádza z anglického slova *direction*). Podľa vety 8.2.2. je $\operatorname{Dir} M$ jediný lineárny podpriestor vo V taký, že $M = \boldsymbol{p} + \operatorname{Dir} M$ pre nejaké (pre každé) $\boldsymbol{p} \in M$. Taktiež pre každé $\boldsymbol{p} \in M$ platí

$$\operatorname{Dir} M = \{\boldsymbol{x} - \boldsymbol{p};\ \boldsymbol{x} \in M\}.$$

Pre každú usporiadanú $(n+1)$-ticu bodov $(\boldsymbol{p}_0, \dots, \boldsymbol{p}_n)$, vektorového priestoru V, prípadne pre jeho konečnú neprázdnu podmnožinu $\{\boldsymbol{p}_0, \dots, \boldsymbol{p}_n\}$, označme

$$\ell(\boldsymbol{p}_0, \dots, \boldsymbol{p}_n) = \{t_0\boldsymbol{p}_0 + \ldots + t_n\boldsymbol{p}_n;\ t_0, \dots, t_n \in K \ \&\ t_0 + \ldots + t_n = 1\}$$

množinu všetkých afinných kombinácií bodov $\boldsymbol{p}_0, \dots, \boldsymbol{p}_n$. Z práve dokázaného tvrdenia vyplýva, že $\ell(\boldsymbol{p}_0, \dots, \boldsymbol{p}_n)$ je najmenší afinný podpriestor vo V, ktorý obsahuje všetky body $\boldsymbol{p}_0, \dots, \boldsymbol{p}_n$; nazývame ho *afinný obal* bodov $\boldsymbol{p}_0, \dots, \boldsymbol{p}_n$ alebo tiež *afinný podpriestor generovaný* bodmi $\boldsymbol{p}_0, \dots, \boldsymbol{p}_n$.

Vo všeobecnosti možno pre ľubovoľnú (i nekonečnú) neprázdnu množinu $X \subseteq V$ definovať jej *afinný obal* $\ell(X)$, nazývaný tiež *afinný podpriestor generovaný* množinou X, ako množinu všetkých (konečných) afinných kombinácií bodov z X. Opäť platí, že $\ell(X)$ je najmenší afinný podpriestor vo V, pre ktorý $X \subseteq \ell(X)$.

8.2.4. Tvrdenie. *Nech* $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n \in V$. *Potom*

$$\begin{aligned} \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n) &= \boldsymbol{p}_0 + [\boldsymbol{p}_1 - \boldsymbol{p}_0, \dots, \boldsymbol{p}_n - \boldsymbol{p}_0], \\ \operatorname{Dir} \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n) &= [\boldsymbol{p}_1 - \boldsymbol{p}_0, \dots, \boldsymbol{p}_n - \boldsymbol{p}_0]. \end{aligned}$$

Dôkaz. prenechávame ako cvičenie čitateľovi.

Dimenziou alebo tiež *rozmerom* afinného podpriestoru $M \subseteq V$, označenie $\dim M$, nazývame dimenziu jeho zamerania, teda

$$\dim M = \dim \operatorname{Dir} M.$$

Body $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ vektorového priestoru V nazývame *afinne nezávislé*, ak vektory $\boldsymbol{p}_1 - \boldsymbol{p}_0, \dots, \boldsymbol{p}_n - \boldsymbol{p}_0$ sú lineárne nezávislé. Z nasledujúceho očividného tvrdenia okrem iného vyplýva, že body $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n \in V$ sú afinne nezávislé práve vtedy, keď pre nejaké (pre každé) $0 \le k \le n$ vektory $\boldsymbol{p}_j - \boldsymbol{p}_k$, kde $0 \le j \le n$ a $j \ne k$, sú lineárne nezávislé. Inak povedané, platí

8.2.5. Tvrdenie. *Body* $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n \in V$ *sú afinne nezávislé práve vtedy, keď*

$$\dim \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n) = n$$

Zrejme 0-rozmerné afinné podpriestrory vo V sú práve všetky body $\boldsymbol{p} \in V$ (presnejšie, všetky jednobodové podmnožiny vo V). Tieto afinné podpriestory nazývame tiež *triviálne*. Jednorozmené afinné podpriestory vo V nazývame *priamkami*. Každá priamka má naozaj tvar $\ell(\boldsymbol{p}, \boldsymbol{q})$ pre nejaké afinne nezávislé (t. j. rôzne) body $\boldsymbol{p}, \boldsymbol{q} \in V$. Dvojrozmerné afinné podpriestory vo V nazývame *rovinami*. Taktiež samotný priestor V je svojim *nevlastným* afinným podpriestorom. Ak $\dim V = n$, tak $(n-1)$-rozmerné afinné podpriestory vo V nazývame *nadrovinami*.

Kým pojmy „bod“, „priamka“ a „rovina“ sú absolútne v tom zmysle, že závisia len na dimenzii príslušného afinného podpriestoru, pojem nadroviny je relatívny, lebo závisí na vzťahu dimenzií afinného podpriestoru a celého priestoru. Napríklad ak $\dim V = 1$ (t. j. ak samotné V je priamka), tak každý bod vo V je zároveň nadrovinou. Nadrovinami v dvojrozmernom priestore (t. j. v rovine) sú zasa všetky priamky. V trojrozmernom priestore V pojmy roviny a nadroviny splývajú. V štvorrozmernom priestore sú zasa nadrovinami trojrozmerné podpriestory; atď. Ešte poznamenajme, že v 0-rozmernom (t. j. jednobodovom) priestore V niet priamok, rovín ani nadrovín.

8.3. Prienik a spojenie afinných podpriestorov

V tomto paragrafe mierne zovšeobecníme niektoré výsledky paragrafov 4.3 a 5.4 o prieniku a súčte lineárnych podpriestorov do podoby použiteľnej pre afinné podpriestory.

8.3.1. Tvrdenie. *Nech M, $N \subseteq V$ sú afinné podpriestory. Potom $M \cap N$ je afinný pod-*

priestor vo V práve vtedy, keď $M \cap N \neq \emptyset$. V tom prípade

$$\operatorname{Dir}(M \cap N) = \operatorname{Dir} M \cap \operatorname{Dir} N.$$

Dôkaz. Ak $M \cap N = \emptyset$, tak to samozrejme nie je afinný podpriestor. Nech $M \cap N \neq \emptyset$. Označme $S = \operatorname{Dir} M$, $T = \operatorname{Dir} N$ príslušné smerové podpriestory. Zvoľme ľubovoľný bod $\boldsymbol{p} \in M \cap N$. Stačí dokázať rovnosť

$$M \cap N = \boldsymbol{p} + (S \cap T).$$

Zvoľme $\boldsymbol{q} \in M \cap N$. K nemu existujú $\boldsymbol{u} \in S$, $\boldsymbol{v} \in T$ také, že $\boldsymbol{q} = \boldsymbol{p} + \boldsymbol{u} = \boldsymbol{p} + \boldsymbol{v}$. Potom $\boldsymbol{u} = \boldsymbol{v} \in S \cap T$ a $\boldsymbol{q} \in \boldsymbol{p} + (S \cap T)$. Teda $M \cap N \subseteq \boldsymbol{p} + (S \cap T)$. Obrátená inklúzia je triviálna.

Neprázdnosť prieniku $M \cap N$ možno zaručiť za predpokladu, že lineárny priestor $\operatorname{Dir} M + \operatorname{Dir} N$ je „dosť veľký“.

8.3.2. Tvrdenie. *Nech M, $N \subseteq V$ sú afinné podpriestory. Potom*

$$\operatorname{Dir} M + \operatorname{Dir} N = V \;\Rightarrow\; M \cap N \neq \emptyset.$$

Dôkaz. Označme $S = \operatorname{Dir} M$, $T = \operatorname{Dir} N$. Zvoľme ľubovoľné $\boldsymbol{p} \in M$, $\boldsymbol{q} \in N$. Keďže $S + T = V$, existujú vektory $\boldsymbol{u} \in S$, $\boldsymbol{v} \in T$ také, že $\boldsymbol{q} - \boldsymbol{p} = \boldsymbol{u} + \boldsymbol{v}$. Potom

$$\boldsymbol{q} = \boldsymbol{p} + (\boldsymbol{q} - \boldsymbol{p}) = \boldsymbol{p} + \boldsymbol{u} + \boldsymbol{v}$$

V dôsledku toho $\boldsymbol{p} + \boldsymbol{u} = \boldsymbol{q} - \boldsymbol{v} \in M \cap N$, lebo $\boldsymbol{p} + \boldsymbol{u} \in M$ a $\boldsymbol{q} - \boldsymbol{v} \in N$.

Spojením afinných podpriestorov M, $N \subseteq V$, označenie $M \sqcup N$, nazývame afinný obal ich zjednotenia. Teda
$$M \sqcup N = \ell(M \cup N).$$
Zrejme $M \sqcup N$ je najmenší afinný podpriestor vo V, ktorý obsahuje M aj N, a pre lineárne podpriestory S, $T \subseteq V$ platí $S \sqcup T = S + T$.

8.3.3. Tvrdenie. *Nech M, $N \subseteq V$ sú afinné podpriestory.*

(a) *Ak $M \cap N \neq \emptyset$, tak*
$$\mathrm{Dir}(M \sqcup N) = \mathrm{Dir}\, M + \mathrm{Dir}\, N,$$
$$M \sqcup N = M + \mathrm{Dir}\, N = N + \mathrm{Dir}\, M.$$

(b) *Ak $M \cap N = \emptyset$, tak pre ľubovoľné $\boldsymbol{p} \in M$, $\boldsymbol{q} \in N$ platí*
$$\mathrm{Dir}(M \sqcup N) = [\boldsymbol{q} - \boldsymbol{p}] + \mathrm{Dir}\, M + \mathrm{Dir}\, N,$$
$$M \sqcup N = M + ([\boldsymbol{q} - \boldsymbol{p}] + \mathrm{Dir}\, N) = N + ([\boldsymbol{q} - \boldsymbol{p}] + \mathrm{Dir}\, M).$$

Poznámka. Stojí za zmienku, že obe rovnosti z (b) sú splnené aj za predpokladu $M \cap N \neq \emptyset$. V tom prípade však pre ľubovoľné $\boldsymbol{r} \in M \cap N$ platí
$$\boldsymbol{q} - \boldsymbol{p} = (\boldsymbol{r} - \boldsymbol{p}) + (\boldsymbol{q} - \boldsymbol{r}) \in \mathrm{Dir}\, M + \mathrm{Dir}\, N,$$
takže vektor $\boldsymbol{q} - \boldsymbol{p}$ možno v príslušných vzťahoch vynechať. Rovnako tomu bude i v príklade 8.3.5.

Dôkaz. Stačí dokázať len (b), lebo (a) z neho vyplýva vo svetle našej poznámky. Označme $S = \operatorname{Dir} M$, $T = \operatorname{Dir} N$ a zvoľme $\boldsymbol{p} \in M$, $\boldsymbol{q} \in N$. Budeme dokazovať iba rovnosť

$$M \sqcup N = \boldsymbol{p} + [\boldsymbol{q} - \boldsymbol{p}] + S + T;$$

zvyšok je už jej bezprostredným dôsledkom.

Každý bod $\boldsymbol{r} \in M \sqcup N$ je afinnou kombináciou

$$\boldsymbol{r} = \sum_{i=0}^{m} s_i \boldsymbol{p}_i + \sum_{j=0}^{n} t_j \boldsymbol{q}_j$$

kde $\boldsymbol{p}_0, \ldots, \boldsymbol{p}_m \in M$, $\boldsymbol{q}_0, \ldots, \boldsymbol{q}_n \in M$, $s_0, \ldots, s_m, t_0, \ldots, t_n \in K$ a $\sum_i s_i + \sum_j t_j = 1$. Potom $\boldsymbol{p}_i - \boldsymbol{p} \in S$, $\boldsymbol{q}_j - \boldsymbol{q} \in T$ pre $i \le m$, $j \le n$. Označme $s = s_0 + \ldots + s_m$, $t = t_0 + \ldots + t_n$ a počítajme

$$\begin{aligned}
\boldsymbol{r} &= (s\boldsymbol{p} + t\boldsymbol{q}) + \sum_{i=0}^{m} s_i(\boldsymbol{p}_i - \boldsymbol{p}) + \sum_{j=0}^{n} t_j(\boldsymbol{q}_j - \boldsymbol{q}) \\
&= \boldsymbol{p} + t(\boldsymbol{q} - \boldsymbol{p}) + \sum_{i=0}^{m} s_i(\boldsymbol{p}_i - \boldsymbol{p}) + \sum_{j=0}^{n} t_j(\boldsymbol{q}_j - \boldsymbol{q}) \in \boldsymbol{p} + [\boldsymbol{q} - \boldsymbol{p}] + S + T,
\end{aligned}$$

keďže $s = 1 - t$. Teda $M \sqcup N \subseteq \boldsymbol{p} + [\boldsymbol{q} - \boldsymbol{p}] + S + T$. Obrátená inklúzia je triviálna.

8.3.4. Dôsledok. *Nech M, $N \subseteq V$ sú konečnorozmerné afinné podpriestory. Potom*

$$\dim(M \sqcup N) = \begin{cases} \dim M + \dim N - \dim(M \cap N), & \text{ak } M \cap N \neq \emptyset, \\ \dim M + \dim N - \dim(\operatorname{Dir} M \cap \operatorname{Dir} N) + 1, & \text{ak } M \cap N = \emptyset. \end{cases}$$

8.3.5. Príklad. Vo vektorovom priestore V uvažujme konečnorozmerné afinné podpriestory

$$M = \boldsymbol{p} + [\boldsymbol{u}_1, \dots, \boldsymbol{u}_m], \qquad N = \boldsymbol{q} + [\boldsymbol{v}_1, \dots, \boldsymbol{v}_n].$$

Potom

$$M \sqcup N = \begin{cases} \boldsymbol{p} + [\boldsymbol{u}_1, \dots, \boldsymbol{u}_m, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n], & \text{ak } M \cap N \neq \emptyset, \\ \boldsymbol{p} + [\boldsymbol{q} - \boldsymbol{p}, \boldsymbol{u}_1, \dots, \boldsymbol{u}_m, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n], & \text{ak } M \cap N = \emptyset, \end{cases}$$

$$\dim(M \sqcup N) = \begin{cases} \dim[\boldsymbol{u}_1, \dots, \boldsymbol{u}_m, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n], & \text{ak } M \cap N \neq \emptyset, \\ \dim[\boldsymbol{q} - \boldsymbol{p}, \boldsymbol{u}_1, \dots, \boldsymbol{u}_m, \boldsymbol{v}_1, \dots, \boldsymbol{v}_n]), & \text{ak } M \cap N = \emptyset. \end{cases}$$

Ak navyše predpokladáme, že tak vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_m$ ako aj vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ sú lineárne nezávislé, tak

$$\dim(M \sqcup N) = \begin{cases} m + n - k, & \text{ak } M \cap N \neq \emptyset, \\ m + n - k + 1, & \text{ak } M \cap N = \emptyset, \end{cases}$$

kde $k = \dim([\boldsymbol{u}_1, \dots, \boldsymbol{u}_m] \cap [\boldsymbol{v}_1, \dots, \boldsymbol{v}_n])$.

8.3.6. Príklad. V stĺpcovom priestore $\mathbb{R}^4$ sú dané vektory $\boldsymbol{x} = (1, 2, 3, 4)^T$, $\boldsymbol{y} = (0, -3, 1, -1)^T$, $\boldsymbol{z} = (1, 1, 0, 0)^T$, $\boldsymbol{u} = (0, -2, 4, 3)^T$, $\boldsymbol{v} = (2, 6, 2, 5)^T$, $\boldsymbol{w} = (0, 0, 1, 1)^T$ a bližšie neurčené body $\boldsymbol{p}$, $\boldsymbol{q}$. Potom $S = [\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}]$, $T = [\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}]$ sú lineárne podpriestory a $M = \boldsymbol{p} + S$, $N = \boldsymbol{q} + N$ sú afinné podpriestory v $\mathbb{R}^4$. Nájdeme dimenzie lineárnych podpriestorov $S + T$, $S \cap T$ a afinných podpriestorov $M \cap N$, $M \sqcup N$ v závislosti na $\boldsymbol{p}$, $\boldsymbol{q}$.

Lineárny podpriestor $S+T$ je generovaný stĺpcami blokovej matice

$$\left(\begin{array}{rrr|rrr} 1 & 0 & 1 & 0 & 2 & 0 \\ 2 & -3 & 1 & -2 & 6 & 0 \\ 3 & 1 & 0 & 4 & 2 & 1 \\ 4 & -1 & 0 & 3 & 5 & 1 \end{array}\right),$$

pričom stĺpce ľavého bloku generujú lineárny podpriestor S a stĺpce pravého bloku lineárny podpriestor T. Táto matica je riadkovo ekvivalentná s blokovou maticou

$$\left(\begin{array}{rrr|rrr} 1 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & -3 & 4 & -4 & 0 \\ 0 & 0 & 3 & -3 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

v stupňovitom tvare, ktorej riadky majú vedúce prvky v stĺpcoch 1, 2, 3 a 6. Hneď vidíme, že vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ tvoria bázu S a vektory $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ bázu $S+T$. Doupravovaním pravého bloku na riadkovo ekvivalentný stupňovitý tvar

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

sa možno presvedčiť, že i vektory $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$ sú lineárne nezávislé, teda tvoria bázu T. Zhrnutím dostávame $\dim S = \dim T = 3$, $\dim(S+T) = 4$. Odtiaľ podľa vety 5.4.1. vyplýva

$\dim(S \cap T) = 3 + 3 - 4 = 2$. Takže $S + T = \mathbb{R}^4$, a bez toho, že by sme čokoľvek ďalej počítali, z tvrdenia 8.3.2. vieme, že nezávisle na bodoch $\boldsymbol{p}$, $\boldsymbol{q}$ platí $M \cap N \neq \emptyset$. Preto $\dim(M \cap N) = \dim(S \cap T) = 2$ podľa tvrdenia 8.3.1. S použitím tvrdenia 8.3.3. a dôsledku 8.3.4. dostávame $\dim(M \sqcup N) = \dim(S + T) = 4$.

8.4. Vzájomná poloha afinných podpriestorov

V tomto paragrafe podáme sľúbenú klasifikáciu vzájomnej polohy dvojíc netriviálnych vlastných afinných podpriestorov vo vektorovom priestore V. (Hoci to nie je z logického hľadiska nevyhnutné, aby sme sa vyhli triedeniu trivialít, body a celý priestor V z našich úvah vylučujeme.) Táto téma prirodzeným spôsobom rozširuje látku stredoškolskej geometrie, zahŕňajúcu klasifikáciu vzájomnej polohy priamok v rovine resp. priamok a rovín v (trojrozmernom) priestore.

Polohu netriviálnych vlastných lineárnych variet $M, N \subseteq V$ budeme klasifikovať na základe dvoch kritérií:

(A) Ak platí $\operatorname{Dir} M \subseteq \operatorname{Dir} N \wedge \operatorname{Dir} N \subseteq \operatorname{Dir} M$, hovoríme, že M, N sú *rovnobežné* a píšeme $M \parallel N$.
V opačnom prípade, t. j. ak platí $\operatorname{Dir} M \not\subseteq \operatorname{Dir} N$ & $\operatorname{Dir} N \not\subseteq \operatorname{Dir} M$, hovoríme, že M, N *nie sú rovnobežné*, a píšeme $M \nparallel N$.

(B) Ak platí $M \cap N \neq \emptyset$, hovoríme, že M, N *sa pretínajú.*
V opačnom prípade, t. j. ak $M \cap N = \emptyset$, hovoríme, že M, N *sa nepretínajú*, alebo, že sú *disjunktné*.

Celkovo teda dostávame štyri možnosti:

(1) $M \parallel N \ \& \ M \cap N \neq \emptyset$, čiže M, N sú rovnobežné a pretínajú sa.

Ľahko možno nahliadnuť, že v takom prípade platí $\operatorname{Dir} M \subseteq \operatorname{Dir} N \ \Leftrightarrow \ M \subseteq N$ a $\operatorname{Dir} N \subseteq \operatorname{Dir} M \ \Leftrightarrow \ N \subseteq M$. Teda $M \subseteq N$ alebo $M \subseteq N$. Hovoríme, že jedna z lineárnych variet M, N je *podvarietou* druhej, alebo, že M, N sú vo vzťahu *inklúzie*.

(2) $M \parallel N \ \& \ M \cap N = \emptyset$, čiže M, N sú rovnobežné a nepretínajú sa.
Tento prípad nazývame vzťahom *pravej rovnobežnosti*.

(3) $M \nparallel N \ \& \ M \cap N \neq \emptyset$, čiže M, N nie sú rovnobežné a pretínajú sa.
Hovoríme, že M, N sú *rôznobežné*.

(4) $M \nparallel N \ \& \ M \cap N = \emptyset$, čiže M, N nie sú rovnobežné a nepretínajú sa.
V tomto prípade ešte rozlišujeme dve ďalšie možnosti:
(4a) Ak $\operatorname{Dir} M \cap \operatorname{Dir} N = \{\mathbf{0}\}$, hovoríme, že M, N sú *mimobežné*.
(4b) Ak $\operatorname{Dir} M \cap \operatorname{Dir} N \neq \{\mathbf{0}\}$, hovoríme, že M, N sú *čiastočne rovnobežné*.

Prípady (1), (2), (3) sú nám dobre známe zo stredoškolskej planimetrie, s prípadom (4) sa však v rovine stretnúť nemožno – dve priamky v rovine buď splývajú alebo sú to pravé rovnobežky alebo rôznobežky. Zo stredoškolskej stereometrie, okrem prípadov (1), (2), (3), ktoré sa realizujú vo vzájomných polohách dvojíc priamok, dvojíc rovín ako i priamky a roviny v trojrozmernom priestore, poznáme aj prípad (4a) – ide o prípad mimobežných priamok. S prípadom (4b), t. j. s prípadom čiastočnej rovnobežnosti sme sa však dosiaľ nestretli a nedokážeme ho spojiť so žiadnou názornou geometrickou predstavou. Nie je to náhoda. Platí totiž nasledujúce tvrdenie.

8.4.1. Tvrdenie. *Nech M, $N \subseteq V$ sú čiastočne rovnobežné lineárne variety. Potom* $\dim M \geq 2$, $\dim N \geq 2$ *a* $\dim V \geq 4$.

Dôkaz. Označme $S = \operatorname{Dir} M$, $T = \operatorname{Dir} N$. Potom $S \cap T$ je netriválny vlastný lineárny podpriestor každého zo zameraní S, T. Teda $\dim(S \cap T) \geq 1$, $\dim M = \dim S \geq 2$, $\dim N = \dim T \geq 2$ a taktiež

$$\dim(S \cap T) \leq \min(\dim S, \dim T) - 1.$$

S použitím vety 5.4.1. z toho vyplýva

$$\begin{aligned} \dim(S + T) &= \dim S + \dim T - \dim(S \cap T) \\ &\geq \dim S + \dim T - \min(\dim S, \dim T) + 1 \\ &= \max(\dim S, \dim T) + 1 \geq 3. \end{aligned}$$

Keďže $M \cap N = \emptyset$, podľa tvrdenia 8.3.2. je $S + T$ vlastný lineárny podpriestor vo V. Preto

$$\dim V \geq \dim(S + T) + 1 \geq 4.$$

Na druhej strane v ľubovoľnom vektorovom priestore V dimenzie ≥ 4 nie je ťažké nájsť príklady čiastočne rovnobežných lineárnych variet. Presvedčte sa, že napr.

$$M = [\boldsymbol{e}_1, \boldsymbol{e}_2], \qquad N = \boldsymbol{e}_4 + [\boldsymbol{e}_2, \boldsymbol{e}_3]$$

sú čiastočne rovnobežné roviny v K^4. Skúste nájsť iné príklady.

8.5. Afinné zobrazenia

Nech U, V sú vektorové priestory nad tým istým poľom K. Hovoríme, že $f : V \to U$ je *afinné zobrazenie*, ak pre ľubovoľné body $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r} \in V$ a skalár $s \in K$ platí

$$f(s\boldsymbol{p} + (1-s)\boldsymbol{q} = sf(\boldsymbol{p}) + (1-s)f(\boldsymbol{q}),$$
$$f(\boldsymbol{p} - \boldsymbol{q} + \boldsymbol{r}) = f(\boldsymbol{p}) - f(\boldsymbol{q}) + f(\boldsymbol{r}).$$

Podobným spôsobom ako tvrdenie 8.2.1. možno dokázať, že afinné sú práve tie zobrazenia $f : V \to U$, ktoré zachovávajú všetky afinné kombinácie trojíc bodov, či, takisto, vôbec všetky afinné kombinácie; v prípade poľa charakteristiky $\neq 2$ stačí žiadať zachovávanie afinných kombinácií dvojíc.

8.5.1. Tvrdenie. *Nech U, V sú vektorové priestory nad poľom K. Potom pre ľubovoľné zobrazenie $f : V \to U$ nasledujúce podmienky sú ekvivalentné:*

(i) *f je afinné zobrazenie;*

(ii) *pre všetky $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r} \in V$, $s, t \in K$ platí*

$$f(s\boldsymbol{p} + t\boldsymbol{q} + (1-s-t)\boldsymbol{r}) = sf(\boldsymbol{p}) + tf(\boldsymbol{q}) + (1-s-t)f(\boldsymbol{r});$$

(iii) *pre každé $n \in \mathbb{N}$ a všetky body $\boldsymbol{p}_0, \boldsymbol{p}_1 \dots, \boldsymbol{p}_n \in V$ a skaláry $t_0, t_1, \dots, t_n \in K$ také, že $t_0 + t_1 + \dots + t_n = 1$, platí*

$$f(t_0\boldsymbol{p}_0 + t_1\boldsymbol{p}_1 + \dots + t_n\boldsymbol{p}_n) = t_0 f(\boldsymbol{p}_0) + t_1 f(\boldsymbol{p}_1) + \dots + t_n f(\boldsymbol{p}_n).$$

Ak char $K \neq 2$, *tak uvedené podmienky sú navyše ekvivalentné s podmienkou*

(ii$^-$) pre všetky $\boldsymbol{p}, \boldsymbol{q} \in V$, $s \in K$ *platí*

$$f(s\boldsymbol{p} + (1-s)\boldsymbol{q}) = sf(\boldsymbol{p}) + (1-s)f(\boldsymbol{q}).$$

Posunutím alebo *transláciou* vektorového priestoru V o vektor $\boldsymbol{u} \in V$ nazývame zobrazenie $V \to V$ dané predpisom $\boldsymbol{x} \mapsto \boldsymbol{x} + \boldsymbol{u}$.

Zrejme kompozíciou posunutia o vektor $\boldsymbol{u} \in V$ a posunutia o vektor $\boldsymbol{v} \in V$ je posunutie o vektor $\boldsymbol{u} + \boldsymbol{v}$. Každé posunutie je bijektívne zobrazenie; inverzné zobrazenie k posunutiu o vektor $\boldsymbol{u}$ je posunutie o opačný vektor $-\boldsymbol{u}$.

Z nasledujúcej vety okrem iného vyplýva, že každé afinné zobrazenie možno dostať kompozíciou lineárneho zobrazenia a posunutia.

8.5.2. Veta. *Nech* U, V *sú vektorové priestory nad poľom* K. *Potom zobrazenie* $f : V \to U$ *je afinné práve vtedy, keď existuje vektor* $\boldsymbol{u} \in U$ *a lineárne zobrazenie* $\varphi : V \to U$ *také, že pre každé* $\boldsymbol{x} \in V$ *platí*

$$f(\boldsymbol{x}) = \varphi(\boldsymbol{x}) + \boldsymbol{u}.$$

Dôkaz. Treba dokázať dve veci:

(1) Pre ľubovoľný vektor $\boldsymbol{u} \in U$ a lineárne zobrazenie $\varphi : V \to U$ je predpisom $f(\boldsymbol{x}) = \varphi(\boldsymbol{x}) + \boldsymbol{u}$ dané afinné zobrazenie $f : V \to U$.

(2) Ak $f : V \to U$ je afinné zobrazenie, tak priradenie $\varphi(\boldsymbol{x}) = f(\boldsymbol{x}) - f(\boldsymbol{0})$ definuje lineárne zobrazenie $\varphi : V \to U$.

V jednom i druhom prípade možno zachovávanie príslušných afinných resp. lineárnych kombinácií overiť priamymi výpočtami, ktoré prenechávame čitateľovi.

Zrejme vektor $\boldsymbol{u} \in U$ ako aj lineárne zobrazenie φ sú podmienkou vety určené jednoznačne. Zobrazenie $\varphi = f - f(\mathbf{0})$ nazývame *lineárnou časťou* a vektor $\boldsymbol{u} = f(\mathbf{0})$ *absolútnym členom* afinného zobrazenia f. Píšeme tiež $f = \varphi + \boldsymbol{u}$.

Afinné zobrazenia sú tak zovšeobecnením funkcií $f : K \to K$ tvaru $f(x) = ax + b$, kde $a, b \in K$, ktoré (najmä v prípade $K = \mathbb{R}$) v matematickej analýze nazývame lineárnymi, na viacrozmerné vektorové priestory.

8.5.3. Dôsledok. *Nech U, V sú vektorové priestory nad poľom K. Potom*

(a) *ľubovoľná translácia priestoru V je afinné zobrazenie;*

(b) *ľubovoľné lineárne zobrazenie $\varphi : V \to U$ je afinné;*

(c) *afinné zobrazenie $f : V \to U$ je lineárne práve vtedy, keď $f(\mathbf{0}) = \mathbf{0}$.*

8.5.4. Tvrdenie. *Nech U, V, W sú vektorové priestory nad poľom K a $g : W \to V$, $f : V \to U$ sú afinné zobrazenia. Potom aj ich kompozícia $f \circ g : W \to U$ je afinné zobrazenie.*

Dôkaz. Hoci priamym výpočtom možno overiť, že $f \circ g$ zachováva afinné kombinácie, podáme radšej dôkaz založený na vete 8.5.2., ktorý nám poskytne informáciu navyše.

Nech $f = \varphi + \boldsymbol{u}$, $g = \psi + \boldsymbol{v}$, kde $\varphi : V \to U$, $\psi : W \to V$ sú lineárne zobrazenia a $\boldsymbol{u} = f(\mathbf{0})$, $\boldsymbol{v} = g(\mathbf{0})$. Potom pre $\boldsymbol{z} \in W$ s využitím linearity φ dostávame

$$(f \circ g)(\boldsymbol{z}) = \varphi(\psi(\boldsymbol{z}) + \boldsymbol{v}) + \boldsymbol{u} = (\varphi \circ \psi)(\boldsymbol{z}) + \varphi(\boldsymbol{v}) + \boldsymbol{u}.$$

Teda $f \circ g$ je afinné zobrazenie zložené z lineárneho zobrazenia $\varphi \circ \psi$ a posunutia o vektor $\varphi(\boldsymbol{v}) + \boldsymbol{u}$.

Vzorec odvodený v našom dôkaze stojí za zaznamenanie. Pre lineárne zobrazenia $\psi : W \to V$, $\varphi : V \to U$ a vektory $\boldsymbol{v} \in V$, $\boldsymbol{u} \in U$ platí

$$(\varphi + \boldsymbol{u}) \circ (\psi + \boldsymbol{v}) = (\varphi \circ \psi) + (\varphi \boldsymbol{v} + \boldsymbol{u}).$$

8.5.5. Tvrdenie. *Nech U, V sú vektorové priestory nad poľom K, $f : V \to U$ je afinné zobrazenie a $M \subseteq V$, $N \subseteq U$ sú afinné podpriestory. Potom $f(M)$ je afinný podpriestor v U a $f^{-1}(N)$ je afinný podpriestor vo V alebo prázdna množina.*

Dôkaz. Nech $f = \varphi + \boldsymbol{u}$, kde φ je lineárna časť f a $\boldsymbol{u} = f(\boldsymbol{0})$. Nech ďalej $M = \boldsymbol{p} + S$, $N = \boldsymbol{q} + T$, kde $\boldsymbol{p} \in M$, $\boldsymbol{q} \in N$ a $S \subseteq V$, $T \subseteq U$ sú lineárne podpriestory. Potrebný záver vyplýva z tvrdení 6.1.3., a vety 8.2.2. a nasledujúcich rovností

$$\begin{aligned} f(M) &= f(\boldsymbol{p}) + \varphi(S), \\ f^{-1}(N) &= \begin{cases} \boldsymbol{z} + \varphi^{-1}(T), & \text{kde } \boldsymbol{z} \in V \text{ je ľubovoľné také, že } \varphi(\boldsymbol{z}) = \boldsymbol{q} - \boldsymbol{u}, \\ \emptyset, & \text{ak neexistuje } \boldsymbol{z} \in V \text{ také, že } \varphi(\boldsymbol{z}) = \boldsymbol{q} - \boldsymbol{u}, \end{cases} \end{aligned}$$

ktorých dôkaz prenechávame čitateľovi.

Keďže každé posunutie je bijekcia, afinné zobrazenie $f = \varphi + \boldsymbol{u} : V \to U$ s lineárnou časťou φ je injektívne práve vtedy, keď φ je injektívne. Podobne, f je surjektívne práve vtedy, keď φ je surjektívne. Z toho už priamo vyplývajú ďalšie tri výsledky.

Prvý z nich zovšeobecňuje vetu 6.2.3. o dimenzii jadra a obrazu.

8.5.6. Veta. *Nech $f : V \to U$ je afinné zobrazenie, pričom V je konečnorozmerný vektorový priestor. Potom pre ľubovoľné $\boldsymbol{y} \in \operatorname{Im} f$ platí*

$$\dim V = \dim f^{-1}(\boldsymbol{y}) + \dim \operatorname{Im} f.$$

Afinnou transformáciou vektorového priestoru V nazývame ľubovoľné afinné zobrazenie $f : V \to V$. Aj pre afinné transformácie platí obdoba dôsledku 6.2.4.

8.5.7. Dôsledok. *Nech $f : V \to V$ je afinná transformácia konečnorozmerného vektorového priestoru V. Potom f je injektívna práve vtedy, keď je surjektívna.*

8.5.8. Tvrdenie. *Nech $f : V \to U$ je afinné zobrazenie s lineárnou časťou φ a absolútnym členom $\boldsymbol{u} = f(\mathbf{0})$. Potom f je bijektívne práve vtedy, keď φ je bijektívne. V tom prípade aj inverzné zobrazenie $f^{-1} : U \to V$ je afinné a platí*

$$f^{-1} = \varphi^{-1} - \varphi^{-1}(\boldsymbol{u}).$$

Teda f^{-1} je kompozíciou lineárneho zobrazenia φ^{-1} a posunutia o vektor $-\varphi^{-1}(\boldsymbol{u})$.

Nech U, V sú konečnorozmerné vektorové priestory a $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ sú bázy v U resp. vo V. *Rozšírenou maticou* afinného zobrazenia $f : V \to U$ s lineárnou časťou φ a absolútnym členom $\boldsymbol{u}$ vzhľadom na bázy $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ nazývame blokovú maticu

$$(f)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \big((\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}} \,|\, (\boldsymbol{u})_{\boldsymbol{\alpha}}\big).$$

Ak teda $\dim U = m$, $\dim V = n$, $\boldsymbol{A} = (\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je matica lineárneho zobrazenia φ v bázach $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$, $\boldsymbol{\alpha}$ a $\boldsymbol{a} = (\boldsymbol{u})_{\boldsymbol{\alpha}}$ sú súradnice vektora $\boldsymbol{u}$ v báze $\boldsymbol{\alpha}$, tak rozšírenou maticou afinného zobrazenia f v bázach $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$ je bloková matica

$$(f)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = \big((\varphi\boldsymbol{v}_1)_{\boldsymbol{\alpha}}, \dots, (\varphi\boldsymbol{v}_n)_{\boldsymbol{\alpha}} \,|\, (\boldsymbol{u})_{\boldsymbol{\alpha}}\big) = (\boldsymbol{A} \,|\, \boldsymbol{a}) \in K^{m\times(n+1)}.$$

Súradnice bodu $\boldsymbol{x} \in V$ v báze $\boldsymbol{\beta}$ a súradnice jeho obrazu $f(\boldsymbol{x}) \in U$ v báze $\boldsymbol{\alpha}$ sú tak spojené rovnosťou

$$(f\boldsymbol{x})_{\boldsymbol{\alpha}} = (\varphi)_{\alpha,\boldsymbol{\beta}} \cdot (\boldsymbol{x})_{\boldsymbol{\beta}} + (\boldsymbol{u})_{\boldsymbol{\alpha}} = \boldsymbol{A} \cdot (\boldsymbol{x})_{\boldsymbol{\alpha}} + \boldsymbol{a}.$$

Samozrejme, ak f je lineárne zobrazenie, t. j. ak $f = \varphi$ a $\boldsymbol{u} = \boldsymbol{0}$, nemá význam rozširovať maticu $(\varphi)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ o nulový stĺpec.

Z tvrdenia 8.5.4., presnejšie z formuly odvodenej počas jeho dôkazu, a z tvrdenia 8.5.8. s použitím výsledkov paragrafov 6.4 a 7.2 vyplýva náš záverečný výsledok.

8.5.9. Tvrdenie. *Nech U, V, W sú konečnorozmerné vektorové priestory nad poľom K a $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}$ sú nejaké bázy priestorov U, V, resp. W.*

(a) *Ak $g : W \to V$, $f : V \to U$ sú afinné zobrazenia, ktoré majú v príslušných bázach rozšírené matice $(g)_{\boldsymbol{\beta},\boldsymbol{\gamma}} = (\boldsymbol{B} \,|\, \boldsymbol{b})$, $(f)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = (\boldsymbol{A} \,|\, \boldsymbol{a})$, tak ich kompozícia $f \circ g : W \to U$ má v bázach $\boldsymbol{\gamma}$, $\boldsymbol{\alpha}$ rozšírenú maticu*

$$(f \circ g)_{\boldsymbol{\alpha},\boldsymbol{\gamma}} = (\boldsymbol{A} \cdot \boldsymbol{B} \,|\, \boldsymbol{A} \cdot \boldsymbol{b} + \boldsymbol{a}).$$

(b) *Ak $f : V \to U$ je afinná bijekcia s rozšírenou maticou $(f)_{\boldsymbol{\alpha},\boldsymbol{\beta}} = (\boldsymbol{A} \,|\, \boldsymbol{a})$ v bázach $\boldsymbol{\beta}$, $\boldsymbol{\alpha}$, tak k nej inverzné zobrazenie je afinná bijekcia $f^{-1} : U \to V$, ktorá má v bázach $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ rozšírenú maticu*

$$\big(f^{-1}\big)_{\boldsymbol{\beta},\boldsymbol{\alpha}} = \big(\boldsymbol{A}^{-1} \,|\, -\boldsymbol{A}^{-1} \cdot \boldsymbol{a}\big).$$

Cvičenia

8.1. Dokážte postupne záverečné štyri podmienky z vety 8.2.2.

8.2. Nech V je vektorový priestor nad poľom K.

(a) Tri afinne nezávislé body $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2 \in V$ sa nazývajú *nekolineárne*. Dokážte, že $\boldsymbol{p}_0$, $\boldsymbol{p}_1$, $\boldsymbol{p}_2$ sú *kolineárne* práve vtedy, keď ležia na jednej priamke.

(b) Podobne, štyri afinne nezávislé body $\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3 \in V$ sa nazývajú *nekomplanárne*. Dokážte, že $\boldsymbol{p}_0$, $\boldsymbol{p}_1$, $\boldsymbol{p}_2$ $\boldsymbol{p}_3$ sú *komplanárne* práve vtedy, keď ležia v jednej rovine.

8.3. Nech V je vektorový priestor nad poľom K a $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n, \boldsymbol{q} \in V$. Dokážte postupne nasledujúce tvrdenia:

(a) Body $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ sú afinne nezávislé práve vtedy, keď pre nejaké (ľubovoľné) $i \leq n$ sú lineárne nezávislé vektory $\boldsymbol{p}_j - \boldsymbol{p}_i$, kde $j \in \{0, 1, \dots, n\} \smallsetminus \{i\}$.

(b) $\boldsymbol{q} \in \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n)$ práve vtedy, keď $\boldsymbol{q} - \boldsymbol{p}_0 \in [\boldsymbol{p}_1 - \boldsymbol{p}_0, \dots, \boldsymbol{p}_n - \boldsymbol{p}_0]$. Odvoďte z toho obe rovnosti z tvrdenia 8.2.4.

(c) Ak body $\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n$ sú afinne nezávislé, tak $\boldsymbol{q} \in \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \dots, \boldsymbol{p}_n)$ práve vtedy, keď vektory $\boldsymbol{p}_1 - \boldsymbol{p}_0, \dots, \boldsymbol{p}_n - \boldsymbol{p}_0, \boldsymbol{q} - \boldsymbol{p}_0$ sú lineárne závislé.

8.4. Vo vektorovom priestore $\mathbb{R}^4$ sú dané body $\boldsymbol{p}_0 = (1,1,2,2)^T$, $\boldsymbol{p}_1 = (0,1,0,1)^T$, $\boldsymbol{p}_2 = (1,2,0,3)^T$ a $\boldsymbol{q} = (0,2,-4,2)^T$, $\boldsymbol{r} = (-1,2,-4,1)^T$.

(a) Zistite, či platí $\boldsymbol{q} \in \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2)$, $\boldsymbol{r} \in \ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2)$.

(b) Vypočítajte dimenzie afinných podpriestorov $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2)$, $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{q})$, $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{r})$.

(c) Vypočítajte dimenzie afinných podpriestorov $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2) \cap \ell(\boldsymbol{q}, \boldsymbol{r})$, $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2) \sqcup \ell(\boldsymbol{q}, \boldsymbol{r})$ a určte vzájomnú polohu afinných podpriestorov $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2)$, $\ell(\boldsymbol{q}, \boldsymbol{r})$.

(d) Vypočítajte dimenzie afinných podpriestorov $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1) \cap \ell(\boldsymbol{q}, \boldsymbol{r})$, $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1) \sqcup \ell(\boldsymbol{q}, \boldsymbol{r})$ a určte vzájomnú polohu afinných podpriestorov $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1)$, $\ell(\boldsymbol{q}, \boldsymbol{r})$.

8.5. (a) Nájdite príklad troch priamok v $\mathbb{R}^3$ tak, aby ľubovoľné dve z nich boli mimobežné.

(b) Dokážte, že priamka a rovina v trojrozmernom vektorovom priestore nemôžu byť mimobežné.

(c) Vo vektorovom priestore $\mathbb{R}^4$ nájdite príklad mimobežnej priamky a roviny.

(d) Dokážte, že dve roviny vo štvorrozmernom vektorovom priestore nemôžu byť mimobežné.

(e) Nájdite príklad dvoch mimobežných rovín v $\mathbb{R}^5$.

8.6. Nech $\boldsymbol{p}_0$, $\boldsymbol{p}_1$, $\boldsymbol{p}_2$, $\boldsymbol{p}_3$, $\boldsymbol{p}_4$ sú ľubovoľné afinne nezávislé body vo vektorovom priestore V nad poľom K. Potom roviny $\ell(\boldsymbol{p}_0, \boldsymbol{p}_1, \boldsymbol{p}_2)$, $\boldsymbol{p}_4 + [\boldsymbol{p}_2 - \boldsymbol{p}_0, \boldsymbol{p}_3 - \boldsymbol{p}_0]$ sú čiastočne rovnobežné. Dokážte.

8.7. *Repér* vo vektorovom priestore sa zvykne definovať ako usporiadaná $(n+1)$-tica afinne nezávislých bodov $\boldsymbol{\rho} = (\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_n) \in V^{n+1}$, taká, že $\ell(\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_n) = V$, prípadne ako usporiadaná $(n+1)$-tica $(\boldsymbol{r}, \boldsymbol{\beta}) = (\boldsymbol{r}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n) \in V^{n+1}$, pozostávajúca z ľubovoľného bodu $\boldsymbol{r} \in V$ a bázy $\boldsymbol{\beta} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ vektorového priestoru V. Dokážte nasledujúce dve tvrdenia:

(a) Nech $\boldsymbol{\rho} = (\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_n)$ je usporiadaná $(n+1)$-tica bodov z V. Potom $\boldsymbol{\rho}$ je repér vo V v zmysle prvej definície, práve vtedy, keď $\boldsymbol{\beta} = (\boldsymbol{r}_1 - \boldsymbol{r}_0, \ldots, \boldsymbol{r}_n - \boldsymbol{r}_0)$ je báza vektorového priestoru V, t. j. práve vtedy, keď $(\boldsymbol{r}_0, \boldsymbol{\beta})$ je repér v zmysle druhej definície.

(b) Nech $\boldsymbol{r}$ je bod z V a $\boldsymbol{\beta} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ je usporiadaná n-tica vektorov z V. Potom $(\boldsymbol{r}, \boldsymbol{\beta})$ je repér v zmysle druhej definície práve vtedy, keď $\boldsymbol{\rho} = (\boldsymbol{r}, \boldsymbol{r} + \boldsymbol{v}_1, \ldots, \boldsymbol{r} + \boldsymbol{v}_n)$ je repér v zmysle prvej definície.

Z toho dôvodu nie je potrebné rozlišovať medzi repérmi v zmysle jednej či druhej definície.

8.8. Nech $\boldsymbol{\rho} = (\boldsymbol{r}, \boldsymbol{\beta})$ je repér vo vektorovom priestore V nad poľom K. *Afinnými* alebo tiež *barycentrickými súradnicami bodu* $\boldsymbol{x} \in V$ vzhľadom na repér $\boldsymbol{\rho}$ nazývame súradnice vektora $\boldsymbol{x} - \boldsymbol{r}$ vzhľadom na bázu $\boldsymbol{\beta}$, čiže $(\boldsymbol{x})_{\boldsymbol{\rho}} = (\boldsymbol{x} - \boldsymbol{r})_{\boldsymbol{\beta}}$. Ak je repér $\boldsymbol{\rho}$ známy z kontextu, hovoríme len o *afinných (barycentrických) súradniciach bodu* $\boldsymbol{x}$. Dokážte postupne nasledujúce tvrdenia:

(a) $(\mathbf{0}, \boldsymbol{\varepsilon})$, kde $\boldsymbol{\varepsilon} = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ je kanonická báza, je repér v K^n a pre každé $\boldsymbol{x} \in K^n$ platí $(\boldsymbol{x})_{(\mathbf{0}, \boldsymbol{\varepsilon})} = \boldsymbol{x}$.

(b) Body repéru $\boldsymbol{\rho} = (\boldsymbol{r}_0, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_n)$ majú vzhľadom na tento repér afinné súradnice $(\boldsymbol{r}_0)_{\boldsymbol{\rho}} = \mathbf{0}$, $(\boldsymbol{r}_1)_{\boldsymbol{\rho}} = \boldsymbol{e}_1$, ..., $(\boldsymbol{r}_n)_{\boldsymbol{\rho}} = \boldsymbol{e}_n$.

(c) Ak $\dim V = n$ a $\boldsymbol{\rho} = (\boldsymbol{r}, \boldsymbol{\beta})$ je repér vo V, tak predpisom $\boldsymbol{x} \mapsto (\boldsymbol{x})_{\boldsymbol{\rho}}$ je definované bijektívne afinné zobrazenie $V \to K^n$ a pre každé $\boldsymbol{x} \in V$, $=(c_1, \dots, c_n)^T \in K^n$ platí

$$\boldsymbol{x} = \boldsymbol{r} + \boldsymbol{\beta} \cdot (\boldsymbol{x})_{\boldsymbol{\rho}}, \qquad\qquad (\boldsymbol{r} + \boldsymbol{\beta} \cdot \boldsymbol{c})_{\boldsymbol{\rho}} = \boldsymbol{c}.$$

8.9. V $\mathbb{R}^3$ sú dané body $\boldsymbol{r}_0 = (5,2,1)^T$, $\boldsymbol{r}_1 = (0,2,1)^5$, $\boldsymbol{r}_2 = (5,0,2)^T$, $\boldsymbol{r}_3 = (5,2,0)^T$.

(a) Dokážte, že $\boldsymbol{\rho} = (\boldsymbol{r}_0, \boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3)$ je repér v $\mathbb{R}^3$.

(b) Nájdite afinné súradnice bodov $\boldsymbol{x} = (4,4,-3)^T$, $\boldsymbol{y} = (-5,-2,-1)^T$, $\boldsymbol{z} = (0,0,0)^T$ vzhľadom na repér $\boldsymbol{\rho}$.

(c) Nájdite body $\boldsymbol{p}$, $\boldsymbol{q}$, $\boldsymbol{r}$, ak poznáte ich afinné súradnice $(\boldsymbol{p})_{\boldsymbol{\rho}} = (0,2,1)^T$, $(\boldsymbol{q})_{\boldsymbol{\rho}} = (-1,1,-1)^T$, $(\boldsymbol{r})_{\boldsymbol{\rho}} = (0,0,0)^T$.

8.10. Nech $\boldsymbol{\pi} = (\boldsymbol{p}, \boldsymbol{\alpha})$, $\boldsymbol{\rho} = (\boldsymbol{r}, \boldsymbol{\beta})$ sú dva repéry vo vektorovom priestore V nad poľom K. Potom afinné súradnice ľubovoľného bodu $\boldsymbol{x} \in V$ vzhľadom na tieto repéry sú zviazané vzťahom

$$(\boldsymbol{x})_{\boldsymbol{\pi}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot (\boldsymbol{x} - \boldsymbol{p})_{\boldsymbol{\beta}} = \boldsymbol{P}_{\boldsymbol{\alpha},\boldsymbol{\beta}} \cdot \big((\boldsymbol{x})_{\boldsymbol{\rho}} - (\boldsymbol{p})_{\boldsymbol{\rho}}\big),$$

kde $\boldsymbol{P}_{\alpha,\boldsymbol{\beta}}$ je matica prechodu z bázy $\boldsymbol{\beta}$ do bázy $\boldsymbol{\alpha}$. Dokážte.

8.11. Dokážte tvrdenie 8.5.1. (*Návod*: Modifikujte dôkaz tvrdenia 8.2.1.)

8.12. Dokážte podmienky (1), (2) z dôkazu vety 8.5.2.

8.13. Doplňte vynechané dôkazy oboch rovností z dôkazu tvrdenia 8.5.5.

8.14. Na základe tvrdenia 8.5.5. doplňte dôkazy vety 8.5.6., dôsledku 8.5.7. a tvrdenia 8.5.8.

8.15. Predpokladajme, že dvaja pozorovatelia P a P' popisujú udalosti v čase a v trojrozmernom priestore vzhľadom na po dvoch rovnobežné a rovnako orientované súradné osi x, y, z, resp. x', y', z', pričom počiatok súradnej sústavy pozorovateľa P' má z hľadiska pozorovateľa P v čase $t = t_0$, zodpovedajúcom času $t' = 0$ pozorovateľa P', súradnice $(x_0, y_0, z_0)^T$. Nech navyše pozorovateľ P' sa vzhľadom na pozorovateľa P pohybuje rovnomerne priamočiaro rýchlosťou $\boldsymbol{v} = (v_x, v_y, v_z)^T$ (pozri príklad 6.4.7. a cvičenie 6.14.

(a) Odvoďte tvar *Galileovej transformácie*, ktorou sú za týchto okolností v klasickej (t. j. v nerelativistickej) fyzike zviazané časopriestorové súradnice bodových udalostí z hľadiska pozorovateľov P resp. P':

$$t' = t - t_0, \qquad x' = x - x_0 - v_x t, \qquad y' = y - y_0 - v_y t, \qquad z' = z - z_0 - v_z t.$$

Nahliadnite, že ide o afinnú transformáciu s rozšírenou maticou $(\boldsymbol{G_v} \,|\, -\boldsymbol{s}_0)$, kde $\boldsymbol{G_v}$ je matica Galileovej transformácie z cvičenia 6.14 a $\boldsymbol{s}_0 = (t_0, x_0, y_0, z_0)^T$.

(b) Nech $f, g : \mathbb{R}^4 \to \mathbb{R}^4$ sú Galileove transformácie s rozšírenými maticami $(\boldsymbol{G_v} \,|\, -\boldsymbol{s}_0)$ resp. $(\boldsymbol{G_w} \,|\, -\boldsymbol{s}_1)$, kde $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{R}^3$, $\boldsymbol{s}_0, \boldsymbol{s}_1 \in \mathbb{R}^4$. Nájdite rozšírenú maticu kompozície afinných zobrazení $f \circ g$ a rozšírenú maticu inverzného zobrazenia f^{-1}. Dokážte, že ide opäť o Galileove transformácie uvedeného typu a vysvetlite fyzikálny význam získaných výsledkov.

8.16. Nech U, V sú vektorové priestory nad poľom K. Označme $\mathcal{A}(V, U)$ množinu všetkých *afinných* zobrazení $f : V \to U$. Dokážte postupne nasledujúce tvrdenia:

(a) $\mathcal{A}(V, U)$ s operáciami súčtu a skalárneho násobku definovanými po zložkách tvorí *lineárny* podpriestor vektorového priestoru U^V. $\mathcal{A}(V, U)$ navyše obsahuje vektorový priestor $\mathcal{L}(V, U)$ všetkých lineárnych zobrazení $fi : V \to U$ ako svoj lineárny podpriestor. (Pozri príklad 1.6.5 a tvrdenie 6.5.1.)

(b) Priradením $f \mapsto (f - f(\mathbf{0}), f(\mathbf{0}))$ je definovaný lineárny izomorfizmus vektorových priestorov $\mathcal{A}(V, U) \to \mathcal{L}(V, U) \times U$ (pozri príklad 1.6.4).

(c) Nech $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ sú nejaké bázy priestorov U resp. V. Potom priradením $f \mapsto (f)_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ je daný lineárny izomorfizmus vektorových priestorov $\mathcal{A}(V, U) \to K^{m \times (n+1)}$.

(d) Predpokladajme, že U, V sú konečnorozmerné a $\dim U = m$, $\dim V = n$. Odvoďte, či už z (b) alebo z (c), že potom aj $\mathcal{A}(V,U)$ je konečnorozmerný a $\dim \mathcal{A}(V,U) = m(n+1)$.

(e) Ak V je konečnorozmerný, tak jeho duál $V^* = \mathcal{L}(V,K)$ tvorí nadrovinu v $\mathcal{A}(V,K)$ (pozri text tesne pred tvrdením 6.5.3.).

9. Afinné podpriestory a sústavy lineárnych rovníc

V tejto kapitole sa opäť pozrieme cez prizmu toho, čo sme sa dosiaľ naučili, na sústavy lineárnych rovníc. Uvidíme, že množina riešení každej takej sústavy tvorí afinný (v homogénnom prípade dokonca lineárny) podpriestor niektorého stĺpcového vektorového priestoru K^n. Taktiež naopak, ukážeme, že každý afinný podpriestor v K^n možno popísať ako podpriestor riešení vhodnej sústavy lineárnych rovníc. Na vyjadrenie množiny riešení tejto sústavy pomocou parametrov sa potom možno dívať ako na *parametrické rovnice* príslušného afinného podpriestoru. Získané znalosti nám umožnia v konkrétnych prípadoch určiť vzájomnú polohu afinných podpriestorov.

V celej kapitole K označuje pevné, inak ľubovoľné, pole; m, n sú ľubovoľné, pevne zvolené prirodzené čísla.

9.1. Podpriestor riešení homogénnej sústavy a jeho báza

Nech $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{b} \in K^m$. Uvažujme homogénnu sústavu lineárnych rovníc s maticou $\boldsymbol{A}$

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{0},$$

a nehomogénnu sústavu s maticou $\boldsymbol{A}$ a pravou stranou $\boldsymbol{b}$

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}.$$

Množiny ich riešení označíme

$$\mathcal{R}(\boldsymbol{A}) = \{\boldsymbol{x} \in K^n;\ \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{0}\},$$

resp.

$$\mathcal{R}(\boldsymbol{A} \,|\, \boldsymbol{b}) = \{\boldsymbol{x} \in K^n;\ \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}\}.$$

Predpisom $\varphi(\boldsymbol{x}) = \boldsymbol{A} \cdot \boldsymbol{x}$ je definované lineárne zobrazenie $\varphi : K^n \to K^m$, pričom $\mathcal{R}(\boldsymbol{A}) = \operatorname{Ker} \varphi$. Z toho okamžite vyplýva

9.1.1. Tvrdenie. *Pre ľubovoľnú maticu $\boldsymbol{A} \in K^{m \times n}$ množina $\mathcal{R}(\boldsymbol{A})$ riešení homogénnej sústavy $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{0}$ tvorí lineárny podpriestor vektorového priestoru K^n.*

Doteraz sme homogénnu sústavu riešili úpravou jej matice $\boldsymbol{A}$ na redukovaný stupňovitý tvar $\boldsymbol{B}$. Z tohto tvaru sme potom vyčítali, ktoré neznáme si zvolíme za parametre a ktoré neznáme si vyjadríme pomocou nich. Presnejšie, neznámu x_j sme si zvolili za parameter práve vtedy, keď sa v j-tom stĺpci matice $\boldsymbol{B}$ nenachádzal vedúci prvok žiadneho riadku matice $\boldsymbol{B}$; ak sa v j-tom stĺpci nachádzal vedúci prvok nejakého riadku, tak neznámu x_j sme si vyjadrili pomocou týchto parametrov.

Uvedená veta nám umožňuje alternatívny popis množiny riešení $\mathcal{R}(\boldsymbol{A})$ – kedže ide o lineárny podpriestor v K^n, môžeme ho najúspornejšie popísať zadaním (niektorej) jeho bázy. Každú bázu priestoru $\mathcal{R}(\boldsymbol{A})$ nazývame tiež *fundamentálnym systémom riešení* sústavy $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{0}$. Potom každé riešenie príslušnej homogénnej sústavy možno jednoznačne vyjadriť ako lineárnu kombináciu vektorov z fundamentálneho systému riešení, a tiež naopak, každá lineárna kombinácia vektorov fundamentálneho systému je riešením príslušnej sústavy. Fundamentálny systém riešení nájdeme nasledujúcim postupom.

Maticu $\boldsymbol{A}$ upravíme pomocou ERO na redukovaný stupňovitý tvar $\boldsymbol{B} \in K^{m\times n}$. Množinu $\{1,\dots,n\}$ rozdelíme na dve podmnožiny J, J', podľa toho, či sa v j-tom stĺpci matice $\boldsymbol{B}$ nachádza alebo nenachádza vedúci prvok nejakého jej riadku. Označme k počet prvkov množiny J' a zapíšme ju v tvare $J' = \{j_1 < j_2 < \dots < j_k\}$. Pre každý index $j_l \in J'$ zostrojíme vektor $\boldsymbol{v}_l = (v_{1l},\dots,v_{nl})^T \in K^n$ takto: Zvolíme $v_{j_l l} = 1$ a $v_{j_i l} = 0$ pre $i \neq l$. Pre $j \in J$ vypočítame hodnoty v_{jl} k uvedeným hodnotám parametrov $v_{j_1 l},\dots,v_{j_k l}$ tak, aby celý vektor $\boldsymbol{v}_l$ vyhovoval podmienke $\boldsymbol{B}\cdot\boldsymbol{v}_l = \boldsymbol{0}$. Potom vektory $\boldsymbol{v}_1$, $\boldsymbol{v}_2,\dots,\boldsymbol{v}_k$ tvoria bázu podpriestoru riešení $\mathcal{R}(\boldsymbol{A})$. Pritom zrejme platí $k = n - h(\boldsymbol{A})$.

Namiesto dôkazu posledného tvrdenia si celý postup ozrejmíme na príklade.

9.1.2. Príklad. Predpokladajme, že sme maticu $\boldsymbol{A}$ pomocou ERO už upravili na redukovaný stupňovitý tvar

$$\boldsymbol{B} = \begin{pmatrix} 1 & 2 & 0 & 0 & -1/3 \\ 0 & 0 & 1 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Vedúce prvky riadkov sa nachádzajú v stĺpcoch 1, 3 a 4. Teda neznáme x_2 a x_5 si zvolíme za parametre a neznáme x_1, x_3 a x_4 si vyjadríme pomocou nich. Naša prvá voľba je $x_2 = 1$, $x_5 = 0$. Tomu zodpovedá vektor $\boldsymbol{v}_1 = (-2,1,0,0,0)^T$. Druhá voľba parametrov je $x_2 = 0$, $x_5 = 1$. Tomu zodpovedá vektor $\boldsymbol{v}_2 = (1/3,0,-1/2,2,1)^T$. Potom vektory $\boldsymbol{v}_1$, $\boldsymbol{v}_2$ tvoria bázu podpriestoru (fundamentálny systém) riešení $\mathcal{R}(\boldsymbol{A}) = \mathcal{R}(\boldsymbol{B}) \subseteq \mathbb{R}^5$.

Ak sa „z estetických dôvodov“ chceme vyhnúť zlomkom vo výsledku, stačí miesto vektorov obsahujúcich ako súradnice zlomky vziať ich vhodné nenulové skalárne násobky. V našom prípade stačí nahradiť bázový vektor $\boldsymbol{v}_2$ „krajším“ bázovým vektorom $6\boldsymbol{v}_2 = (2,0,-3,12,6)^T$.

Pre „veľkosť“ podpriestoru riešení homogénnej sústavy z našich úvah vyplýva

9.1.3. Tvrdenie. *Pre ľubovoľnú maticu $\boldsymbol{A} \in K^{m\times n}$ platí*

$$\dim \mathcal{R}(\boldsymbol{A}) = n - h(\boldsymbol{A}).$$

9.2. Podpriestor riešení nehomogénnej sústavy

Prejdime teraz k otázke štruktúry množiny riešení $\mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b})$ nehomogénnej sústavy $\boldsymbol{A}\cdot\boldsymbol{x} = \boldsymbol{b}$.

9.2.1. Tvrdenie. *Nech $\boldsymbol{A} \in K^{m\times n}$, $\boldsymbol{b} \in K^m$.*

(a) *Ak $\boldsymbol{y}, \boldsymbol{z} \in \mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b})$, tak $\boldsymbol{y} - \boldsymbol{z} \in \mathcal{R}(\boldsymbol{A})$.*

(b) *Ak $\boldsymbol{z} \in \mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b})$, $\boldsymbol{x} \in \mathcal{R}(\boldsymbol{A})$, tak $\boldsymbol{z} + \boldsymbol{x} \in \mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b})$.*

Dôkaz. Možno overiť priamym výpočtom.

Z uvedeného tvrdenia vyplýva, že na popis množiny $\mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b})$ všetkých riešení nehomogénnej sústavy stačí poznať podpriestor $\mathcal{R}(\boldsymbol{A})$ všetkých riešení príslušnej homogénnej sústavy, t. j. nejaký fundamentálny systém $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$ jej riešení, a ľubovoľné jedno riešenie $\boldsymbol{z} \in \mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b})$ nehomogénnej sústavy. Tvrdenie možno potom schématicky zapísať v niektorom z tvarov

$$\begin{aligned}\mathcal{R}(\boldsymbol{A}\,|\,\boldsymbol{b}) &= \boldsymbol{z} + \mathcal{R}(\boldsymbol{A}) = \{\boldsymbol{z} + \boldsymbol{x};\ \boldsymbol{x} \in \mathcal{R}(\boldsymbol{A})\}\\ &= \boldsymbol{z} + [\boldsymbol{v}_1, \dots, \boldsymbol{v}_n] = \{\boldsymbol{z} + c_1\boldsymbol{v}_1 + \dots + c_k\boldsymbol{v}_k;\ c_1, \dots, c_k \in K\}.\end{aligned}$$

Každý si môže vybrať ten, ktorý sa mu najväčšmi pozdáva.

S využitím pojmov predchádzajúcej kapitoly možno naše úvahy zhrnúť do nasledujúcej podoby.

9.2.2. Tvrdenie. *Nech* $\boldsymbol{A} \in K^{m \times n}$, $\boldsymbol{b} \in K^m$. *Ak sústava* $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ *má aspoň jedno riešenie, tak* $\mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b})$ *je afinný podpriestor v* K^n *so zameraním* $\mathcal{R}(\boldsymbol{A})$. *To znamená,*

$$\operatorname{Dir} \mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) = \mathcal{R}(\boldsymbol{A}) \quad \text{a} \quad \dim \mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) = \dim \mathcal{R}(\boldsymbol{A}) = n - h(\boldsymbol{A}).$$

9.3. Frobeniova veta a riešenie nehomogénnej sústavy

Odpoveď na otázku riešiteľnosti nehomogénnej sústavy možno dať porovnaním hodnosti jej základnej a rozšírenej matice.

Začneme pozorovaním, že sústava $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ má aspoň jedno riešenie $\boldsymbol{z} \in K^n$ práve vtedy, keď $\boldsymbol{b} \in \operatorname{Im} \varphi$ (kde $\varphi(\boldsymbol{x}) = \boldsymbol{A} \cdot \boldsymbol{x}$). Ak tento prípad nastane, tak, ako sme už ukázali, $\mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) = \boldsymbol{z} + \mathcal{R}(\boldsymbol{A})$.

9.3.1. Veta. (Frobenius) *Nech* $\boldsymbol{A} \in K^{m \times n}$, $\boldsymbol{b} \in K^m$. *Potom nehomogénna sústava* $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ *má riešenie práve vtedy, keď* $h(\boldsymbol{A} \mid \boldsymbol{b}) = h(\boldsymbol{A})$.

Dôkaz. Z poznámky vyslovenej tesne pred vetou vyplýva, že sústava $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ má riešenie práve vtedy, keď $\boldsymbol{b} \in [\boldsymbol{s}_1(\boldsymbol{A}), \ldots, \boldsymbol{s}_n(\boldsymbol{A})]$, t. j. práve vtedy keď

$$[\boldsymbol{s}_1(\boldsymbol{A}), \ldots, \boldsymbol{s}_n(\boldsymbol{A}), \boldsymbol{b}] = [\boldsymbol{s}_1(\boldsymbol{A}), \ldots, \boldsymbol{s}_n(\boldsymbol{A})].$$

Keďže

$$h(\boldsymbol{A} \mid \boldsymbol{b}) = \dim[\boldsymbol{s}_1(\boldsymbol{A}), \ldots, \boldsymbol{s}_n(\boldsymbol{A}), \boldsymbol{b}],$$
$$h(\boldsymbol{A}) = \dim[\boldsymbol{s}_1(\boldsymbol{A}), \ldots, \boldsymbol{s}_n(\boldsymbol{A})]$$

a druhý z týchto podpriestorov je podpriestorom prvého, uvedená podmienka je zrejme ekvivalentná s rovnosťou $h(\boldsymbol{A} \,|\, \boldsymbol{b}) = h(\boldsymbol{A})$.

Frobeniova veta vlastne hovorí už známu vec: nehomogénna sústava $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ nemá riešenie práve vtedy, keď sa pri úprave jej rozšírenej matice $(\boldsymbol{A} \,|\, \boldsymbol{b})$ na redukovaný stupňovitý tvar objaví nejaký riadok tvaru $(0, \dots, 0 \,|\, d) \in K^{n+1}$, kde $0 \neq d \in K$. Takýto riadok totiž zodpovedá rovnici $0 = d$.

Ak upravíme pomocou ERO rozšírenú maticu $(\boldsymbol{A} \,|\, \boldsymbol{b})$ na redukovaný stupňovitý tvar $(\boldsymbol{B} \,|\, \boldsymbol{c})$, kde $\boldsymbol{B} \in K^{m \times n}$ a $\boldsymbol{c} \in K^m$, tak $\boldsymbol{B}$ je tiež v redukovanom stupňovitom tvare. Potom $\mathcal{R}(\boldsymbol{A} \,|\, \boldsymbol{b}) = \mathcal{R}(\boldsymbol{B} \,|\, \boldsymbol{c}) \neq \emptyset$ práve vtedy, keď sa žiaden vedúci prvok nejakého riadku matice $(\boldsymbol{B} \,|\, \boldsymbol{c})$ nenachádza v poslednom, t. j. $(n+1)$-om stĺpci. Bázu priestoru riešení $\mathcal{R}(\boldsymbol{A}) = \mathcal{R}(\boldsymbol{B})$ nájdeme postupom popísaným v paragrafe 9.1 Nech J, J' a k majú tam uvedený význam. Jedno riešenie $\boldsymbol{z} = (z_1, \dots, z_n)^T$ nehomogénnej sústavy dostaneme voľbou parametrov $z_{j_1} = \dots = z_{j_k} = 0$ pre $j_l \in J'$. Zvyšné hodnoty z_j potom vypočítame tak, aby $\boldsymbol{z}$ vyhovovalo podmienke $\boldsymbol{B} \cdot \boldsymbol{z} = \boldsymbol{c}$, t. j. $z_j = c_j$ pre $j \in J$.

9.3.2. Príklad. Predpokladajme, že sme maticu $(\boldsymbol{A} \,|\, \boldsymbol{b})$ pomocou ERO už upravili na redukovaný stupňovitý tvar

$$(\boldsymbol{B} \,|\, \boldsymbol{c}) = \left(\begin{array}{cccccc|c} 1 & 0 & 0 & 3 & 1/4 & 0 & 2 \\ 0 & 1 & 0 & 4 & 2 & -1 & -1 \\ 0 & 0 & 1 & 1 & -5 & 6 & -2/7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Vidíme, že $h(\boldsymbol{B} \,|\, \boldsymbol{c}) = h(\boldsymbol{B}) = 3$, teda $\mathcal{R}(\boldsymbol{A} \,|\, \boldsymbol{b}) = \mathcal{R}(\boldsymbol{B} \,|\, \boldsymbol{c}) \neq \emptyset$. Vedúce prvky riadkov sa nachádzajú v stĺpcoch 1, 2 a 3. Teda neznáme x_4, x_5 a x_6 si zvolíme za parametre a neznáme x_1, x_2 a x_3 si vyjadríme pomocou nich. Prvej voľbe $x_4 = 1$, $x_5 = x_6 = 0$ zodpovedá vektor $\boldsymbol{v}_1 = (-3, -4, -1, 1, 0, 0)^T$. Druhá voľba $x_4 = 0$, $x_5 = 1$, $x_6 = 0$ nám dá vektor $\boldsymbol{v}_2 = (-1/4, -2, 5, 0, 1, 0)^T$. Treťou voľbou $x_4 = x_5 = 0$, $x_6 = 1$ získame vektor $\boldsymbol{v}_3 = (0, 1, -6, 0, 0, 1)^T$. Potom vektory $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, $\boldsymbol{v}_3$ tvoria bázu podpriestoru riešení $\mathcal{R}(\boldsymbol{A}) = \mathcal{R}(\boldsymbol{B}) \subseteq \mathbb{R}^6$ príslušnej homogénnej sústavy. Konečne voľbou parametrov $x_4 = x_5 = x_6 = 0$ získame jedno riešenie $\boldsymbol{z} = (2, -1, -2/7, 0, 0, 0)^T$ nehomogénnej sústavy.

Výsledok možno prehľadne zapísať do tabuľky (treba si však uvedomiť, že sme ju vypĺňali uvedeným postupom):

	$\boldsymbol{v}_1$	$\boldsymbol{v}_2$	$\boldsymbol{v}_3$	$\boldsymbol{z}$
x_1	-3	$-1/4$	0	2
x_2	-4	-2	1	-1
x_3	-1	5	-6	$-2/7$
x_4	1	0	0	0
x_5	0	1	0	0
x_6	0	0	1	0

Porovnajte túto tabuľku s maticou $(\boldsymbol{B} \,|\, \boldsymbol{c})$!

9.4. Parametrické a všeobecné rovnice afinných podpriestorov

Hoci sa v tomto i v nasledujúcom paragrafe obmedzíme len na afinné podpriestory stĺpcového vektorového priestoru K^n, naše úvahy majú širšiu platnosť. Zvolením pevnej bázy ich možno pomocou súradnicového zobrazenia zrejmým spôsobom preniesť aj na afinné podpriestory ľubovoľného konečnorozmerného vektorového priestoru V.

Každý afinný podpriestor $M \subseteq K^n$ má tvar

$$M = \boldsymbol{p} + [\boldsymbol{u}_1, \dots, \boldsymbol{u}_k] = \boldsymbol{p} + [\boldsymbol{\alpha}]$$

pre nejaký bod $\boldsymbol{p} = (p_1, \dots, p_n)^T \in M$ a vhodnú usporiadanú k-ticu $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ vektorov z K^n, kde $\boldsymbol{u}_j = (u_{1j}, \dots, u_{nj})^T$. To znamená, že pre ľubovoľné $\boldsymbol{x} \in K^n$ platí $\boldsymbol{x} \in M$ práve vtedy, keď existuje $\boldsymbol{t} = (t_1, \dots, t_k)^T \in K^k$ také, že

$$\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{\alpha} \cdot \boldsymbol{t},$$

kde usporiadanú k-ticu $\boldsymbol{\alpha}$ sme ako obyčajne stotožnili s maticou $(u_{ij}) \in K^{n \times k}$ so stĺpcami $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$. Rovnosť $\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{\alpha} \cdot \boldsymbol{t}$ je maticovým zápisom *parametrických rovníc* afinného podpriestoru $M \subseteq K^n$. Vektor $\boldsymbol{t} \in K^n$ nazývame *vektorom parametrov* a jeho zložky $t_1, \dots, t_k \in K$ *parametrami*. Po rozpísaní do zložiek

$$\begin{array}{c} x_1 = p_1 + u_{11}t_1 + u_{12}t_2 + \ldots + u_{1k}t_k \\ x_2 = p_2 + u_{21}t_1 + u_{22}t_2 + \ldots + u_{2k}t_k \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = p_n + u_{n1}t_1 + u_{n2}t_n + \ldots + u_{nk}t_k \end{array}$$

dostaneme obvyklejší tvar, s akým sme sa v dimenzii $n = 2$ resp. $n = 3$ už stretli v stredoškolskej analytickej geometrii.

Ak navyše vektory $\boldsymbol{u}_1, \dots, \boldsymbol{u}_k$ sú lineárne nezávislé, čo možno vždy dosiahnuť vynechaním „nadbytočných“ vektorov, tak parametrické rovnice podpriestoru M nám priamo ukážu jeho dimenziu: $\dim M = k$.

Zápis afinného podpriestoru $M \subseteq K^n$ v tvare $M = \boldsymbol{p} + [\boldsymbol{\alpha}]$, kde $\boldsymbol{p} \in M$ a $\boldsymbol{\alpha}$ je nejaká usporiadaná k-tica, ktorá generuje jeho zameranie $\operatorname{Dir} M$ (môžeme si dovoliť predpokladať, že $\boldsymbol{\alpha}$ je dokonca báza v $\operatorname{Dir} M$), budeme nazývať jeho *parametrickým vyjadrením*. Parametrické vyjadrenie $M = \boldsymbol{p} + [\boldsymbol{\alpha}]$ afinného podpriestoru možno priamo prepísať do jeho parametrických rovníc $\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{\alpha} \cdot \boldsymbol{t}$, ($\boldsymbol{t} \in K^k$). Taktiež naopak, z jeho parametrických rovníc možno okamžite získať jeho parametrické vyjadrenie. Súvis medzi týmito dvoma druhmi popisu je natoľko bezprostredný, že ich ani nemusíme príliš úzkostlivo rozlišovať. Na druhej strane, v predchádzajúcich paragrafoch sme videli, že každá sústava lineárnych rovníc $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ s rozšírenou maticou $(\boldsymbol{A} \mid \boldsymbol{b}) \in K^{m \times (n+1)}$ (pokiaľ má riešenie), popisuje afinný podpriestor $\mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) \subseteq K^n$. Nájsť parametrické rovnice tohto podpriestoru už vieme, treba si to len uvedomiť. Ak totiž $\boldsymbol{\beta} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_k)$ je báza podpriestoru $\mathcal{R}(\boldsymbol{A})$ riešení príslušenej homogénnej sústavy a $\boldsymbol{z} \in \mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b})$ je ľubovoľné jedno riešenie nehomogénnej sústavy – a jedno i druhé (pokiaľ existuje) naozaj vieme nájsť –, tak

$$\boldsymbol{x} = \boldsymbol{z} + \boldsymbol{\beta} \cdot \boldsymbol{t},$$

kde $\boldsymbol{t} \in K^k$ je vektor parametrov, sú parametrické rovnice afinného podpriestoru $\mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) \subseteq K^n$.

Inak povedané, vyriešiť sústavu lineárnych rovníc $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ znamená vlastne nájsť nejaké (prípadne nie celkom hocaké ale v istom zmysle „pekné“) parametrické rovnice (alebo parametrické vyjadrenie) afinného podpriestoru $\mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) \subseteq K^n$.

Často je však potrebné riešiť obrátenú úlohu: k parametricky zadanému afinnému podpriestoru $M \subseteq K^n$ nájsť jeho *všeobecné rovnice*, t. j. sústavu lineárnych rovníc $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ o n neznámych $x_1, \dots, x_n$ takú, že $M = \mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b})$.

Nech teda $M = \boldsymbol{p} + [\boldsymbol{\alpha}]$ je afinný podpriestor v K^n, daný bodom $\boldsymbol{p} \in K^n$ a usporiadanou k-ticou $\boldsymbol{\alpha} = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)$ vektorov z K^n, ktorú stotožníme s maticou $\boldsymbol{\alpha} = (u_{ij}) \in K^{n \times k}$ so stĺpcami $\boldsymbol{u}_j$. Parametrické rovnice $\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{\alpha} \cdot \boldsymbol{t}$ podpriestoru M, kde $\boldsymbol{x} = (x_1, \ldots, \boldsymbol{x}_n)^T \in K^n$ je vektor neznámych a $\boldsymbol{t} = (t_1, \ldots, t_k)^T \in K^k$ je vektor parametrov, možno prepísať do tvaru

$$\boldsymbol{I}_n \cdot \boldsymbol{x} = \boldsymbol{\alpha} \cdot \boldsymbol{t} + \boldsymbol{p},$$

ktorý možno reprezentovať blokovou maticou

$$(\boldsymbol{I}_n \,|\, \boldsymbol{\alpha} \,|\, \boldsymbol{p}).$$

Naša metóda bude založená na *eliminácii parametrov* $t_1, \ldots, t_k$ úpravou tejto matice pomocou ERO. Maticu $(\boldsymbol{I}_n \,|\, \boldsymbol{\alpha} \,|\, \boldsymbol{p})$ budeme upravovať na riadkovo ekvivalentnú maticu tak, aby stredný blok vo výslednej matici bol v stupňovitom tvare. Môžu nastať dve možnosti

(1) $h(\boldsymbol{\alpha}) = n$, čo spoznáme podľa toho, že všetky riadky stredného bloku výslednej matice sú nenulové. V tom prípade $M = V$ a všeobecné rovnice tohto podpriestoru tvorí prázdna sústava (t. j. sústava ktorá neobsahuje žiadnu rovnicu). My sa jednoducho uspokojíme s konštatovaním $M = V$ a nijakými všeobecnými rovnicami sa ďalej nebudeme zaoberať.

(2) $h(\boldsymbol{\alpha}) < n$. Vtedy možno stredný blok výslednej matice rozdeliť do dvoch pod sebou umiestnených blokov $\left(\frac{\boldsymbol{D}}{\boldsymbol{0}}\right)$, kde horný blok $\boldsymbol{D}$ je stupňovitá matica typu $h(\boldsymbol{\alpha}) \times k$, ktorá má všetky riadky nenulové, teda dolný nulový blok má rozmer $(n - h(\boldsymbol{\alpha})) \times k$. Toto rozdelenie stredného bloku indukuje rozdelenie celej výslednej matice do blokov

$$\left(\begin{array}{c|c|c} \boldsymbol{A}' & \boldsymbol{D} & \boldsymbol{b}' \\ \hline \boldsymbol{A} & \boldsymbol{0} & \boldsymbol{b} \end{array}\right).$$

Potom $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ sú všeobecné rovnice afinného podpriestoru M, t. j. platí $M = \boldsymbol{p} + [\boldsymbol{\alpha}] = \mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b})$.

Popísaný algoritmus možno stručne zhrnúť do schémy

$$(\boldsymbol{I}_n \mid \boldsymbol{\alpha} \mid \boldsymbol{p}) \xrightarrow{\text{ERO}} \left(\begin{array}{c|c|c} \boldsymbol{A}' & \boldsymbol{D} & \boldsymbol{b}' \\ \hline \boldsymbol{A} & 0 & \boldsymbol{b} \end{array}\right),$$

kde $\boldsymbol{D}$ je matica v stupňovitom tvare s nenulovými riadkami (ktorých počet teda nutne je $h(\boldsymbol{D}) = h(\boldsymbol{\alpha})$). Ako vedľajší produkt takéhoto výpočtu, možno z k-tice $\boldsymbol{\alpha}$ vybrať bázu zamerania $\operatorname{Dir} M = [\boldsymbol{\alpha}]$: je tvorená vektormi $\boldsymbol{u}_{j_1}, \ldots, \boldsymbol{u}_{j_l}$, kde $1 \leq j_1 < \ldots < j_l \leq k$ sú indexy tých stĺpcov matice $\boldsymbol{D}$, v ktorých sa nachádzajú vedúce prvky jej riadkov (pozri tvrdenie 4.5.3.). Správnosť celého algoritmu vyplýva z nasledujúceho tvrdenia.

9.4.1. Tvrdenie. *Nech* $\boldsymbol{B} \in K^{n\times m}$, $\boldsymbol{C} \in K^{n\times k}$ a $\boldsymbol{p} \in K^n$. *Ak bloková matica* $(\boldsymbol{B} \mid \boldsymbol{C} \mid \boldsymbol{p})$ *je riadkovo ekvivalentná s blokovou maticou*

$$\left(\begin{array}{c|c|c} \boldsymbol{A}' & \boldsymbol{D} & \boldsymbol{b}' \\ \hline \boldsymbol{A} & 0 & \boldsymbol{b} \end{array}\right),$$

kde $\boldsymbol{D}$ *je matica v stupňovitom tvare s nenulovými riadkami, tak*

$$\mathcal{R}(\boldsymbol{A} \mid \boldsymbol{b}) = \left\{\boldsymbol{x} \in K^m;\ (\exists\, \boldsymbol{t} \in K^k)(\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{C} \cdot \boldsymbol{t} + \boldsymbol{p})\right\}.$$

Dôkaz. Matica $(\boldsymbol{B} \mid \boldsymbol{C} \mid \boldsymbol{p})$ zodpovedá sústave $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{C} \cdot \boldsymbol{t} + \boldsymbol{p}$ v neznámych $x_1, \ldots, x_m$, $t_1, \ldots, t_k$. Podobne matica

$$\left(\begin{array}{c|c|c} \boldsymbol{A}' & \boldsymbol{D} & \boldsymbol{b}' \\ \hline \boldsymbol{A} & 0 & \boldsymbol{b} \end{array}\right)$$

zodpovedá sústave

$$\begin{aligned} \boldsymbol{A}' \cdot \boldsymbol{x} &= \boldsymbol{D} \cdot \boldsymbol{t} + \boldsymbol{b}' \\ \boldsymbol{A} \cdot \boldsymbol{x} &= \boldsymbol{b} \end{aligned}$$

v rovnakých neznámych. Vzhľadom na riadkovú ekvivalenciu príslušných matíc sú obe sústavy ekvivalentné.

Dokážeme, že pre ľubovoľné $\boldsymbol{x} \in K^m$ nasledujúce podmienky sú ekvivalentné:

(i) $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$;

(ii) $(\exists\, \boldsymbol{t} \in K^k)(\boldsymbol{A}' \cdot \boldsymbol{x} = \boldsymbol{D} \cdot \boldsymbol{t} + \boldsymbol{b}' \ \&\ \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b})$;

(iii) $(\exists\, \boldsymbol{t} \in K^k)(\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{C} \cdot \boldsymbol{t} + \boldsymbol{p})$.

Keďže implikácie (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i) platia triviálne, vysvetlenie potrebuje iba implikácia (i) $\Rightarrow$ (ii). Zrejme hodnosť matice $\boldsymbol{D}$ sa rovná počtu jej riadkov a ten je $\leq n$. Preto tiež $h(\boldsymbol{D} \,|\, \boldsymbol{A}' \cdot \boldsymbol{x} - \boldsymbol{b}') = h(\boldsymbol{D})$ nezávisle na $\boldsymbol{x}$. Ale to podľa Frobeniovej vety 9.3.1. znamená, že sústava $\boldsymbol{D} \cdot \boldsymbol{t} = \boldsymbol{A}' \cdot \boldsymbol{x} - \boldsymbol{b}'$ (v neznámych $t_1, \dots, t_k$) má nejaké riešenie $\boldsymbol{t} \in K^k$ pre ľubovoľné $\boldsymbol{x} \in K^m$.

Poznámka. Z uvedeného dôkazu vyplýva, že tvrdenie 9.4.1. zostáva v platnosti, aj keď matica $\boldsymbol{D}$ nie je v stupňovitom tvare; stačí žiadať len lineárnu nezávislosť jej riadkov. Tú však možno najistejšie nahliadnuť práve úpravou príslušnej matice na stupňovitý tvar.

9.4.2. Príklad. Nájdeme všeobecné rovnice afinného podpriestorru $M = \boldsymbol{p} + [\boldsymbol{\alpha}]$ stĺpcového vektorového priestoru $\mathbb{Z}_{11}^5$ nad poľom $\mathbb{Z}_{11}$, kde $\boldsymbol{p} = (1,2,3,4,5)^T$ a $\boldsymbol{\alpha}$ je tvorená stĺpcami matice

$$\begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 5 & 2 & 6 \\ 0 & 2 & 7 & 0 \\ 1 & 6 & 0 & 9 \\ 0 & 3 & 5 & 8 \end{pmatrix}.$$

Budeme upravovať maticu

$$\left(\begin{array}{ccccc|cccc|c} 1 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 5 & 2 & 6 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 7 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 1 & 6 & 0 & 9 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 5 & 8 & 5 \end{array}\right)$$

pomocou ERO tak, aby stredný blok nadobudol stupňovitý tvar. Po niekoľkých krokoch dostaneme

$$\left(\begin{array}{ccccc|cccc|c} 1 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 1 \\ 5 & 1 & 0 & 0 & 0 & 0 & 10 & 2 & 0 & 7 \\ 4 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 8 & 4 \\ 10 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 6 \\ 9 & 3 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 2 \end{array}\right).$$

Predovšetkým vidíme, že tretí vektor štvorice $\boldsymbol{\alpha}$ je lineárnou kombináciou predchádzajúcich dvoch, preto ho možno v príslušnom parametrickom vyjadrení podpriestoru M vynechať. Zvyšné tri vektory v $\boldsymbol{\alpha}$ sú lineárne nezávislé, čiže $\dim M = 3$. Konečne, všeobecné rovnice podpriestoru M vyzerajú takto

$$\begin{aligned} 10x_1 + 2x_2 + x_3 \phantom{{}+ x_4 + x_5} &= 6 \\ 9x_1 + 3x_2 \phantom{{}+ x_3} + x_4 + x_5 &= 2\,. \end{aligned}$$

Dosadením sa možno presvedčiť, že bod $\boldsymbol{p}$ skutočne vyhovuje tejto sústave a vektory štvorice $\boldsymbol{\alpha}$ príslušnej homogénnej sústave.

9.5. Rovnice prieniku a spojenia afinných podpriestorov

V tomto paragrafe sa pokúsime zostaviť všeobecné recepty, pomocou ktorých budeme vedieť napísať či už všeobecné alebo parametrické rovnice prieniku a spojenia dvoch afinných podpriestorov stĺpcového vektorového priestoru K^n. Pri tom vezmeme do úvahy tri možnosti zadania pôvodných podpriestorov:

(1) Oba podpriestory sú zadané všeobecnými rovnicami.

(2) Oba podpriestory sú zadané parametricky.

(3) Jeden podpriestor je zadaný pomocou všeobecných rovníc a druhý parametricky.

Každú situáciu budeme ilustrovať na jednom až dvoch konkrétnych príkladoch, v ktorých navyše vyšetríme i vzájomnú polohu oboch afinných podpriestorov.

(1) Nech afinné podpriestory $M, N \subseteq K^n$ majú všeobecné rovnice $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ resp. $\boldsymbol{B} \cdot \boldsymbol{x} = \boldsymbol{c}$, kde $\boldsymbol{A} \in K^{m \times n}$, $\boldsymbol{b} \in K^m$, $\boldsymbol{B} \in K^{l \times n}$, $\boldsymbol{c} \in K^l$. Potom všeobecnými rovnicami

prieniku $M \cap N$ je sústava

$$\begin{aligned} \boldsymbol{A} \cdot \boldsymbol{x} &= \boldsymbol{b} \\ \boldsymbol{B} \cdot \boldsymbol{x} &= \boldsymbol{c} \end{aligned}$$

s rozšírenou maticou

$$\left(\begin{array}{c|c} \boldsymbol{A} & \boldsymbol{b} \\ \boldsymbol{B} & \boldsymbol{c} \end{array} \right).$$

Parametrické vyjadrenie prieniku $M \cap N$ možno získať vyriešením tejto sústavy.

Ak hľadáme parametrické vyjadrenie spojenia $M \sqcup N$, najprv vyriešením sústav s rozšírenými maticami $(\boldsymbol{A} \mid \boldsymbol{b})$ resp. $(\boldsymbol{B} \mid \boldsymbol{c})$ získame parametrické vyjadrenia jednotlivých podpriestorov M a N. Z nich na základe tvrdenia 8.3.3. (b) zostavíme parametrické vyjadrenie podpriestoru $M \sqcup N$ (pozri tiež príklad 8.3.5.). Konečne, ak nás zaujímajú všeobecné rovnice podpriestoru $M \sqcup N$, môžeme ich odvodiť z jeho parametrických rovníc metódou opísanou v druhej časti predchádzajúceho paragrafu 9.4 (pozri tvrdenie 9.4.1. a príklad 9.4.2.).

9.5.1. Príklad. Afinné podpriestory M, N vektorového priestoru $\mathbb{Q}^4$ sú dané sústavami

$$\begin{aligned} x_1 + x_2 - x_3 + x_4 &= 9 \\ x_1 - x_2 + x_3 - x_4 &= -3 \end{aligned}$$

resp.

$$\begin{aligned} x_1 + 3x_2 + 2x_3 - x_4 &= 0 \\ x_1 - 3x_2 - 2x_3 + x_4 &= 6\,. \end{aligned}$$

Ak dáme tieto sústavy dohromady, získame všeobecné rovnice prieniku. Ich riešenie však bude výhodné trochu odložiť a najprv upraviť rozšírené matice pôvodných sústav:

$$\left(\begin{array}{rrrr|r} 1 & 1 & -1 & 1 & 9 \\ 1 & -1 & 1 & -1 & -3 \end{array}\right) \sim \left(\begin{array}{rrrr|r} 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & -1 & 1 & 6 \end{array}\right),$$

$$\left(\begin{array}{rrrr|r} 1 & 3 & 2 & -1 & 0 \\ 1 & -3 & -2 & 1 & 6 \end{array}\right) \sim \left(\begin{array}{rrrr|r} 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & 2/3 & -1/3 & -1 \end{array}\right).$$

Z upravených matíc okamžite dostávame parametrické vyjadrenie pôvodných podpriestorov (matica v hranatých zátvorkách označuje lineárny podpriestor generovaný jej stĺpcami)

$$M = \begin{pmatrix} 3 \\ 6 \\ 0 \\ 0 \end{pmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & -1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad N = \begin{pmatrix} 3 \\ -1 \\ 0 \\ 0 \end{pmatrix} + \begin{bmatrix} 0 & 0 \\ -2 & 1 \\ 3 & 0 \\ 0 & 3 \end{bmatrix}.$$

Ak napíšeme obe upravené rozšírené matice všeobecných rovníc podpriestorov M a N do blokov pod seba, dostaneme rozšírenú maticu všeobecných rovníc podpriestoru $M \cap N$. Jej úpravou na redukovaný stupňovitý tvar vyjde

$$\left(\begin{array}{rrrr|r} 1 & 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & 1/5 & 9/5 \\ 0 & 0 & 1 & -4/5 & -21/5 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Odtiaľ už priamo vyplýva parametrické vyjadrenie

$$M \cap N = \begin{pmatrix} 3 \\ 9/5 \\ -21/5 \\ 0 \end{pmatrix} + \begin{bmatrix} 0 \\ -1 \\ 4 \\ 5 \end{bmatrix}.$$

Zistili sme, že dvojrozmerné afinné podpriestory M, N majú jednorozmerný prienik, teda sú *rôznobežné*. Preto tiež $\dim(M \sqcup N) = 2 + 2 - 1 = 3$.

Ak postavíme vedľa seba generátory smerových podpriestorov $\operatorname{Dir} M$ a $\operatorname{Dir} N$, úpravou príslušnej matice zistíme, že prvé tri sú lineárne nezávislé a posledný z nich je lineárnou kombináciou predchádzajúcich. Teda stĺpce matice

$$\boldsymbol{\beta} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & -1 & -2 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}$$

tvoria bázu zamerania afinného podpriestoru $M \sqcup N$. Jeho parametrické vyjadrenie je

$$M \sqcup N = \boldsymbol{p} + [\boldsymbol{\beta}],$$

kde $\boldsymbol{p} = (3, 9/5, -21/5, 0)^T$. Úpravou blokovej matice $(\boldsymbol{I}_4 \,|\, \boldsymbol{\beta} \,|\, \boldsymbol{p})$ podľa algoritmu z druhej časti paragrafu 9.4 (pozri poznámku za tvrdením 9.4.1.) výmenou prvého a posledného riadku dostaneme všeobecné rovnice podpriestoru $M \sqcup N$:

$$x_1 = 3\,.$$

(2) Nech $M = \boldsymbol{p} + [\boldsymbol{\alpha}]$, $N = \boldsymbol{q} + [\boldsymbol{\beta}]$ sú parametrické vyjadrenia dvoch afinných podpriestorov v K^n. Potom, ako už vieme, $M \sqcup N = \boldsymbol{p} + [\boldsymbol{q} - \boldsymbol{p}, \boldsymbol{\alpha}, \boldsymbol{\beta}]$ a podľa tvrdenia 4.5.3. vynechaním vhodných stĺpcov z blokovej matice $(\boldsymbol{q} - \boldsymbol{p}, \boldsymbol{\alpha}, \boldsymbol{\beta})$ možno dostať bázu zamerania $\mathrm{Dir}(M \sqcup N)$. Všeobecné rovnice podpriestoru $M \sqcup N$ dostaneme úpravou blokovej matice $(\boldsymbol{I}_n \mid \boldsymbol{q} - \boldsymbol{p}, \boldsymbol{\alpha}, \boldsymbol{\beta} \mid \boldsymbol{p})$, prípadne matice, v ktorej je prostredný blok nahradený bázou zamerania $\mathrm{Dir}(M \sqcup N)$, podľa algoritmu z paragrafu 9.4

Pokiaľ nás zaujímajú všeobecné rovnice prieniku $M \cap N$, najjednoduchšie ich získame tak, že parametrické rovnice každého z podpriestorov M, N prevedieme na všeobecné rovnice a tieto spojíme dohromady. Parametrické vyjadrenie prieniku $M \cap N$ dostaneme vyriešením jeho všeobecných rovníc.

Jestvuje aj iná cesta k parametrickým rovniciam prieniku $M \cap N$. Ako vedľajší produkt pri nej možno získať bázy zameraní $\mathrm{Dir}\, M$, $\mathrm{Dir}\, N$, $\mathrm{Dir}(M \sqcup N)$, teda aj parametrické rovnice spojenia $M \sqcup N$. Pri tejto metóde upravujeme blokovú maticu $(\boldsymbol{\alpha} \mid \boldsymbol{\beta} \mid \boldsymbol{q} - \boldsymbol{p})$ pomocou ERO na stupňovitý tvar

$$\left(\begin{array}{c|c|c} \boldsymbol{A}' & \boldsymbol{B}' & \boldsymbol{c}' \\ \hline \boldsymbol{0} & \boldsymbol{B} & \boldsymbol{c} \end{array}\right),$$

kde matica $\boldsymbol{A}'$ má všetky riadky nenulové (teda lineárne nezávislé a ich počet je $h(\boldsymbol{A}') = h(\boldsymbol{\alpha}) = \dim M$). Prienik $M \cap N$ je tvorený všetkými $\boldsymbol{x} = \boldsymbol{q} + \boldsymbol{\beta} \cdot \boldsymbol{t} \in N$, ktoré patria zároveň do M, t. j. existuje vektor parametrov $\boldsymbol{s}$ taký, že $\boldsymbol{x} = \boldsymbol{p} + \boldsymbol{\alpha} \cdot \boldsymbol{s}$. Hľadáme teda všetky vektory parametrov $\boldsymbol{t}$, ku ktorým existuje nejaký vektor parametrov $\boldsymbol{s}$ taký, že platí

$$\boldsymbol{\alpha} \cdot \boldsymbol{s} = \boldsymbol{\beta} \cdot \boldsymbol{t} + (\boldsymbol{q} - \boldsymbol{p}).$$

Podľa tvrdenia 9.4.1. (stačí v ňom zameniť poradie prvého a druhého zvislého bloku) k danému $\boldsymbol{t}$ existuje takéto $\boldsymbol{s}$ práve vtedy, keď $\boldsymbol{B} \cdot \boldsymbol{t} + \boldsymbol{c} = \boldsymbol{0}$. Vyriešením tejto sústavy získame parametrické vyjadrenie

$$\boldsymbol{t} = \boldsymbol{r} + \boldsymbol{\gamma} \cdot \boldsymbol{z},$$

kde $\boldsymbol{r} \in \mathcal{R}(\boldsymbol{B} | -\boldsymbol{c})$ a $\boldsymbol{\gamma}$ je báza lineárneho podpriestoru $\mathcal{R}(\boldsymbol{B})$, s vektorom parametrov $\boldsymbol{z}$, ktoré dosadíme do parametrických rovníc podpriestoru N. Dostaneme tak parametrické rovnice

$$\boldsymbol{x} = \boldsymbol{q} + \boldsymbol{\beta} \cdot (\boldsymbol{r} + \boldsymbol{\gamma} \cdot \boldsymbol{z}) = (\boldsymbol{q} + \boldsymbol{\beta} \cdot \boldsymbol{r}) + (\boldsymbol{\beta} \cdot \boldsymbol{\gamma}) \cdot \boldsymbol{z}$$

podpriestoru $M \cap N$.

Metóda zostavenia všeobecných rovníc prieniku $M \cap N$ ako i oboch typov rovníc spojenia $M \sqcup N$, popísaná v prvej časti bodu (2), je (aspoň dúfame) dostatočne jasná. V nasledujúcom príklade sa preto sústredíme len na nájdenie parametrických rovníc prieniku $M \cap N$ metódou z druhej časti a určenie vzájomnej polohy M a N.

9.5.2. Príklad. Nech

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 4 \\ 1 & 1 \\ 2 & 5 \end{bmatrix}, \qquad N_1 = \begin{pmatrix} 0 \\ 2 \\ 2 \\ 3 \end{pmatrix} + \begin{bmatrix} 1 & 2 & 3 \\ 2 & 2 & 8 \\ 5 & 0 & 9 \\ 3 & 4 & 11 \end{bmatrix}, \qquad N_2 = \begin{pmatrix} 1 \\ 1 \\ 2 \\ 2 \end{pmatrix} + \begin{bmatrix} 1 & 2 & 3 \\ 2 & 2 & 8 \\ 5 & 0 & 9 \\ 3 & 4 & 11 \end{bmatrix}$$

sú afinné podpriestory v $\mathbb{R}^4$. Zrejme $\operatorname{Dir} N_1 = \operatorname{Dir} N_2$; označme tento lineárny podpriestor D. Obe úlohy o dvojiciach podpriestorov M, N_1 aj M, N_2 budeme riešiť súčasne. Platí

$$\left(\begin{array}{cc|ccc|cc} 1 & 1 & 1 & 2 & 3 & 0 & 1 \\ 1 & 4 & 2 & 2 & 8 & 2 & 1 \\ 1 & 1 & 5 & 0 & 9 & 2 & 2 \\ 2 & 5 & 3 & 4 & 11 & 3 & 2 \end{array}\right) \sim \left(\begin{array}{cc|ccc|cc} 1 & 1 & 1 & 2 & 3 & 0 & 1 \\ 0 & 3 & 1 & 0 & 5 & 2 & 0 \\ 0 & 0 & 4 & -2 & 6 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right).$$

Ak si z matice na pravej strane odmyslíme krajný pravý blok, po vynechaní rovnice $0 = 0$ z nej dostaneme sústavu

$$4t_1 - 2t_2 + 6t_3 = 0.$$

Lineárny podpriestor $\operatorname{Dir} M \cap D$ je tvorený práve všetkými lineárnyni kombináciami $\boldsymbol{\beta} \cdot \boldsymbol{t}$, kde $\boldsymbol{\beta}$ je matica generátorov D (a jeho báza, čo možno zistiť doupravením stredného bloku na stupňovitý tvar) a $\boldsymbol{t}$ vyhovuje uvedenej homogénnej rovnici. Teda $\dim(\operatorname{Dir} M \cap D) = \dim \operatorname{Dir} M = 2$. Preto $\operatorname{Dir} M \subseteq D$ a platí $M \parallel N_1$ aj $M \parallel N_2$.

Sústava

$$\begin{aligned} 4t_1 - 2t_2 + 6t_3 &= -2 \\ 0 &= -1, \end{aligned}$$

ktorej musí vyhovovať vektor parametrov $\boldsymbol{t} = (t_1, t_2, t_3)^T$, aby ním určený bod z N_1 patril aj do M, nemá riešenie. Preto $M \cap N_1 = \emptyset$ a M, N_1 sú *pravé rovnobežky*.

Naopak, analogická sústava pre dvojicu M, N_2 vedie na jedinú, očividne riešiteľnú rovnicu

$$4t_1 - 2t_2 + 6t_3 = -1.$$

V dôsledku toho $M \subseteq N_2$.

(3) Nech afinný podpriestor $M \subseteq K^n$ je daný všeobecnými rovnicami $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$ a afinný podpriestor $N = \boldsymbol{q} + [\boldsymbol{\beta}] \subseteq K^n$ je daný parametricky. Ak hľadáme všeobecné rovnice prieniku $M \cap N$, stačí nájsť všeobecné rovnice podpriestoru N a pridať ich k sústave $\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{b}$. Ich vyriešením potom možno dostať aj parametrické vyjadrenie $M \cap N$. Ak hľadáme popis spojenia $M \sqcup N$, najvýhodnejšie je vyriešiť všeobecné rovnice podpriestoru M a z parametrických vyjadrení oboch podpriestorov M, N zostaviť parametrické vyjadrenie

$M \sqcup N$ podľa tvrdenia 8.3.3. a príkladu 8.3.5. Elimináciou parametrov odtiaľ dostaneme všeobecné rovnice podpriestoru $M \sqcup N$.

Iná metóda, ako nájsť parametrické vyjadrenie prieniku $M \cap N$ spočíva v dosadení parametrického vyjadrenia podpriestoru N do všeobecných rovníc podpriestoru M. Tým dostaneme sústavu

$$\boldsymbol{A} \cdot (\boldsymbol{q} + \boldsymbol{\beta} \cdot \boldsymbol{t}) = \boldsymbol{b},$$

alebo po úprave s ňou ekvivalentnú sústavu

$$(\boldsymbol{A} \cdot \boldsymbol{\beta}) \cdot \boldsymbol{t} = \boldsymbol{b} - \boldsymbol{A} \cdot \boldsymbol{q},$$

ktorej musí vyhovovať vektor parametrov $\boldsymbol{t}$, aby ním určený bod $\boldsymbol{x} = \boldsymbol{q} + \boldsymbol{\beta} \cdot \boldsymbol{t} \in N$ patril aj do podpriestoru M, teda do prieniku $M \cap N$. Uvedenú sústavu vyriešime úpravou jej rozšírenej matice $(\boldsymbol{A} \cdot \boldsymbol{\beta} \,|\, \boldsymbol{b} - \boldsymbol{A} \cdot \boldsymbol{q})$. Podobne ako v prípade (2) riešenie dostaneme v parametrickom tvare

$$\boldsymbol{t} = \boldsymbol{r} + \boldsymbol{\gamma} \cdot \boldsymbol{z},$$

kde $\boldsymbol{r} \in \mathcal{R}(\boldsymbol{A} \cdot \boldsymbol{\beta} \,|\, \boldsymbol{b} - \boldsymbol{A} \cdot \boldsymbol{q})$ a $\boldsymbol{\gamma}$ je báza lineárneho podpriestoru $\mathcal{R}(\boldsymbol{A} \cdot \boldsymbol{\beta})$, s vektorom parametrov $\boldsymbol{z}$, ktoré dosadíme do parametrických rovníc podpriestoru N. Tak získame parametrické rovnice

$$\boldsymbol{x} = \boldsymbol{q} + \boldsymbol{\beta} \cdot (\boldsymbol{r} + \boldsymbol{\gamma} \cdot \boldsymbol{z}) = (\boldsymbol{q} + \boldsymbol{\beta} \cdot \boldsymbol{r}) + (\boldsymbol{\beta} \cdot \boldsymbol{\gamma}) \cdot \boldsymbol{z}$$

podpriestoru $M \cap N$.

I tentokrát sa v nasledujúcom príklade zameriame len na nájdenie parametrických rovníc prieniku $M \cap N$ druhou z opísaných metód a na určenie vzájomnej polohy M a N.

9.5.3. Príklad. Afinný podpriestor $M \subseteq \mathbb{R}^4$ má všeobecné rovnice

$$\begin{aligned} x_1 - x_2 + x_3 - x_4 &= 1 \\ x_1 + x_2 - x_3 + x_4 &= 3. \end{aligned}$$

Rozšírenú maticu tejto sústavy označíme $(\boldsymbol{A} \mid \boldsymbol{b})$. Afinný podpriestor $N \subseteq \mathbb{R}^4$ je určený ako afinný obal $N = \ell(\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r}, \boldsymbol{s})$ bodov $\boldsymbol{p} = (3, 0, 1, 1)^T$, $\boldsymbol{q} = (4, -1, 2, 2)^T$, $\boldsymbol{r} = (4, 1, 2, 0)^T$ a $\boldsymbol{s} = (7, 3, 4, 5)^T$. Jeho parametrické vyjadrenie potom je

$$N = \boldsymbol{p} + [\boldsymbol{q} - \boldsymbol{p}, \boldsymbol{r} - \boldsymbol{p}, \boldsymbol{s} - \boldsymbol{p}] = \begin{pmatrix} 3 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{bmatrix} 1 & 1 & 4 \\ -1 & 1 & 3 \\ 1 & 1 & 3 \\ 1 & -1 & 4 \end{bmatrix}.$$

Keďže

$$\boldsymbol{A} \cdot (\boldsymbol{q} - \boldsymbol{p}, \boldsymbol{r} - \boldsymbol{p}, \boldsymbol{s} - \boldsymbol{p}) = \begin{pmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 4 \\ -1 & 1 & 3 \\ 1 & 1 & 3 \\ 1 & -1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 3 \\ 0 & 0 & 8 \end{pmatrix},$$

$$\boldsymbol{b} - \boldsymbol{A} \cdot \boldsymbol{p} = \begin{pmatrix} 1 \\ 3 \end{pmatrix} - \begin{pmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \end{pmatrix},$$

bod tvaru $\boldsymbol{p}+t_1(\boldsymbol{q}-\boldsymbol{p})+t_2(\boldsymbol{r}-\boldsymbol{p})+t_3(\boldsymbol{s}-\boldsymbol{p})\in N$ patrí do prieniku $M\cap N$ práve vtedy, keď príslušný vektor parametrov $\boldsymbol{t}=(t_1,t_2,t_3)^T$ vyhovuje sústave s rozšírenou maticou

$$\left(\begin{matrix}2&2&3\\0&0&8\end{matrix}\,\middle|\,\begin{matrix}-2\\0\end{matrix}\right)\sim\left(\begin{matrix}1&1&0\\0&0&1\end{matrix}\,\middle|\,\begin{matrix}-1\\0\end{matrix}\right).$$

Podpriestor riešení tejto sústavy má parametrické vyjadrenie

$$\begin{pmatrix}-1\\0\\0\end{pmatrix}+\begin{bmatrix}-1\\1\\0\end{bmatrix}.$$

Dosadením do parametrického vyjadrenia N dostaneme

$$\begin{aligned}M\cap N&=\begin{pmatrix}3\\0\\1\\1\end{pmatrix}+\begin{pmatrix}1&1&4\\-1&1&3\\1&1&3\\1&-1&4\end{pmatrix}\cdot\begin{pmatrix}-1\\0\\0\end{pmatrix}+\left[\begin{pmatrix}1&1&4\\-1&1&3\\1&1&3\\1&-1&4\end{pmatrix}\cdot\begin{pmatrix}-1\\1\\0\end{pmatrix}\right]\\&=\begin{pmatrix}2\\1\\0\\2\end{pmatrix}+\begin{bmatrix}0\\2\\0\\-2\end{bmatrix}\end{aligned}$$

a $\dim(M\cap N)=1$. Ľahko nahliadneme, že hodnosť matice sústavy podpriestoru M je 2, preto tiež $\dim M=4-2=2$, a $\dim N=3$. Z toho dôvodu $M\cap N$ je vlastný podpriestor tak v M ako aj v N, čiže M, N sú *rôznobežné*.

Cvičenia

9.1. Nájdite nejaký fundamentálny systém riešení sústavy homogénnych lineárnych rovníc $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{0}$ pre matice

(a) $\boldsymbol{A} = \begin{pmatrix} 1 & 0 & -1 & -1 & 0 \\ 2 & 0 & -1 & 1 & -1 \\ 1 & 0 & 1 & 5 & -2 \end{pmatrix} \in \mathbb{Q}^{3\times 5}$;

(b) $\boldsymbol{A} = \begin{pmatrix} \sqrt{2} & 1 & \sqrt{3} \\ 1 & \sqrt{2} & 1 \\ 3 & 2 & 1+\sqrt{6} \end{pmatrix} \in \mathbb{R}^{3\times 3}$;

(c) $\boldsymbol{A} = \begin{pmatrix} 1+\mathrm{i} & 1-\mathrm{i} & 2+3\mathrm{i} \\ 5-\mathrm{i} & -1-5\mathrm{i} & 13 \end{pmatrix} \in \mathbb{C}^{2\times 3}$;

(d) $\boldsymbol{A} = \begin{pmatrix} 0 & 4 & 0 & 9 \\ 0 & 3 & 2 & 5 \\ 0 & 1 & 1 & 0 \end{pmatrix} \in \mathbb{Z}_{11}^{3\times 4}$.

Vyjadrite všeobecné riešenie každej sústavy ako lineárnu kombináciu fundamentálneho systému riešení.

9.2. Nájdite nejaké riešenie nehomogénnej sústavy $\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{b}$ a fundamentálny systém riešení príslušnej homogénnej sústavy danej rozšírenou maticou

(a) $(\boldsymbol{A}\,|\,\boldsymbol{b}) = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 2 \\ 2 & 3 & 7 & 2 \\ 1 & 2 & 2 & 5 \end{array}\right) \in \mathbb{Q}^{3\times 4}$;

(b) $(\boldsymbol{A}\,|\,\boldsymbol{b}) = \left(\begin{array}{cc|c} 1 & \pi & \mathrm{e}-1 \\ \mathrm{e}^{-1} & -1 & \pi^2 \end{array}\right) \in \mathbb{R}^{2\times 3}$;

(c) $(\boldsymbol{A}\,|\,\boldsymbol{b}) = \left(\begin{array}{cccc|c} 1 & 2 & 1 & 0 & -1 \\ -1 & 1 & 2 & 1 & 2 \\ 2 & 7 & 5 & 1 & -1 \end{array}\right) \in \mathbb{R}^{3\times 5}$;

(d) $(\boldsymbol{A}\,|\,\boldsymbol{b}) = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 1 & 1 & 1 & 4 \\ 3 & 4 & 0 & 2 \end{array}\right) \in \mathbb{Z}_5^{3\times 4}$.

Vyjadrite všeobecné riešenie každej sústavy v tvare súčtu jedného jej riešenia a lineárnej kombinácie fundamentálneho systému riešení príslušnej homogénnej sústavy.

9.3. V každom z nasledujúcich prípadov napíšte parametrické rovnice afinného podpriestoru M vektorového priestoru $\mathbb{R}^3$ alebo $\mathbb{R}^4$ nad poľom $\mathbb{R}$ a nájdite jeho všeobecné rovnice:

(a) $M = \{(0,2,-1)\} \subseteq \mathbb{R}^3$;

(b) $M = (1,-1,2) + [(1,-5,4)] \subseteq \mathbb{R}^3$;

(c) $M = [(1,3,-1),(2,0,5)] \subseteq \mathbb{R}^3$;

(d) $M = \ell(\boldsymbol{e}_1 + \boldsymbol{e}_4, 2\boldsymbol{e}_2 - \boldsymbol{e}_3) \subseteq \mathbb{R}^4$

(e) $M = (0, 2, -1, 1) + [(3, 1, 10, -8), (3, 5, 8, -6)] \subseteq \mathbb{R}^4$;

(f) $M = \ell((1, 1, 1, 0), (1, 1, 0, 1), (1, 0, 1, 1), (0, 1, 1, 1)) \subseteq \mathbb{R}^4$;

(g) $M = \mathbb{R}^4$.

9.4. Pre dané lineárne podpriestory S, T vektorového priestoru $\mathbb{R}^4$ nájdite v každom z nasledujúcich prípadov nejaké bázy lineárnych podpriestorov $S \cap T$, $S + T \subseteq \mathbb{R}^4$ a určte ich dimenzie:

(a) $S = \big[(1, 1, 1, 1)^T, (2, 0, 0, 3)^T\big]$, $T = \big[(3, 2, 1, 0)^T, (6, 3, 2, 4)^T\big]$;

(b) $S = [\boldsymbol{e}_1 - \boldsymbol{e}_2 + 2\boldsymbol{e}_3 + \boldsymbol{e}_4]$, $T = \big[(1, 0, 2, 0)^T, (2, -1, 4, 1)^T, (4, -1, 8, 1)^T\big]$;

(c) $S = [\boldsymbol{e}_1 + \boldsymbol{e}_2, \boldsymbol{e}_2 + \boldsymbol{e}_3, \boldsymbol{e}_3 + \boldsymbol{e}_4]$, $T = \big[(1, 0, 1, 0)^T, (0, 1, 0, 1)^T, (1, 0, 0, 1)^T\big]$.

9.5. Pre dané afinné podpriestory M, N vektorového priestoru $\mathbb{R}^4$ nájdite v každom z nasledujúcich prípadov všeobecné aj parametrické rovnice ich prieniku $M \cap N$ a určte ich vzájomnú polohu ako aj dimenziu spojenia $M \sqcup N$:

(a) $M = \ell\big((1, 0, 2, 0)^T, (0, 2, 0, 1)^T\big)$, $N = (4, 1, 7, 2)^T + \big[(1, 2, 3, 4)^T, (0, 1, 2, 3)^T, (0, 0, 1, 2)^T\big]$;

(b) $M = (0, 0, 1, -1)^T + \big[(1, 2, 2, 1)^T, (2, 1, 1, 2)^T\big]$, $N = \big[(0, 1, 1, 0)^T, (1, 0, 0, 1)^T, (1, -1, 0, 0)^T\big]$;

(c) $M = [\boldsymbol{e}_1, \boldsymbol{e}_2]$, $N = (1, 1, 1, 1)^T + [\boldsymbol{e}_3, \boldsymbol{e}_4]$.

9.6. Afinné podpriestory M, N vektorového priestoru $\mathbb{R}^5$ sú dané všeobecnými rovnicami. V každom z nasledujúcich prípadov zistite ich vzájomnú polohu, napíšte parametrické rovnice ich prieniku aj spojenia a určte dimenzie afinných oboch podpriestorov $M \cap N$, $M \sqcup N$:

(a) $M:\ x_1 + 2x_2 = 0,\ x_2 - 3x_3 = 1,\ 4x_3 - x_4 + x_5 = 2,$

$N:\ 2x_1 + 3x_3 - x_5 = 5,\ x_2 + x_4 = 0,\ x_1 - 2x_3 = 7;$

(b) $M:\ x_1 + x_2 + x_3 + x_4 + x_5 = 5,\ x_1 - x_2 + x_3 = 1,\ x_2 + 2x_4 - x_5 = 2,\ x_3 = 1,$

$N:\ 3x_1 + x_2 + 2x_3 + 5x_4 - x_5 = 10,\ x_1 + x_3 + 2x_4 - x_5 = 1;$

(c) $M: x_1 = 1,\ x_2 = 2,\ x_3 = 3,$

$N: x_1 + x_2 + x_3 = 6,\ x_1 - x_2 + x_3 = 2.$

9.7. Jeden z afinných podpriestorov M, N vektorového priestoru $\mathbb{R}^4$ je daný všeobecnými rovnicami a druhý parametricky. V každom z nasledujúcich prípadov zistite ich vzájomnú polohu, napíšte parametrické rovnice ich prieniku $M \cap N$ a všeobecné rovnice ich spojenia $M \sqcup N$ a určte dimenzie afinných podpriestorov $M \cap N$, $M \sqcup N$:

(a) $M: x + y + z = 0,\ x - 2y + z = 4,\ x - u = 0,$ $\quad N = \left[(1, 0, -1, 0)^T\right];$

(b) $M: 2x - y + 2z = 3,\ x + z - 2u = 0,$ $\quad N = \left[(1, 4, 1, 1)^T, (1, 0, 1, 0)^T\right];$

(c) $M: x + y = 0,\ x + z = 1,\ x + u = 2,$ $\quad N = \ell\left((1, 1, 2, 2)^T, (2, 2, 3, 2)^T\right).$

9.8. Nech V je vektorový priestor nad poľom K a S je jeho lineárny podpriestor. Označme V/S množinu všetkých afinných podpriestorov M priestoru V takých, že $\operatorname{Dir} M = S$. Dokážte postupne nasledujúce tvrdenia:

(a) Pre každý prvok $\boldsymbol{x} \in V$ existuje práve jeden podpriestor $X \in V/S$ taký, že $\boldsymbol{x} \in X$. Inými slovami, množina V/S tvorí *rozklad* množiny V a triedou rozkladu, do ktorej patrí prvok $\boldsymbol{x} \in V$, je afinný podpriestor $\boldsymbol{x} + S \in V/S$ (pozri paragraf 0.6).

(b) Prvky $\boldsymbol{x}, \boldsymbol{y} \in V$ patria do tej istej triedy rozkladu V/S práve vtedy, keď $\boldsymbol{x} - \boldsymbol{y} \in S$. Inak povedané, vzťahom $\boldsymbol{x} \equiv_S \boldsymbol{y} \Leftrightarrow \boldsymbol{x} - \boldsymbol{y} \in S$ je definovaná ekvivalencia na množine V prislúchajúca k rozkladu V/S, teda $V/S = V/{\equiv_S}$.

(c) Nech $\boldsymbol{x}_1 \equiv_S \boldsymbol{x}_2$, $\boldsymbol{y}_1 \equiv_S \boldsymbol{y}_2$ a $c \in K$. Potom tiež $\boldsymbol{x}_1 + \boldsymbol{y}_1 \equiv_S \boldsymbol{x}_2 + \boldsymbol{y}_2$ a $c\boldsymbol{x}_1 \equiv_S c\boldsymbol{x}_2$.

(d) Nech $X = \boldsymbol{x} + S$, $Y = \boldsymbol{y} + S$ patria do V/S. Vďaka (c) sú predpismi $X + Y = (\boldsymbol{x} + \boldsymbol{y}) + S$, $cX = c\boldsymbol{x} + S$ korektne definované operácie na množine V/S (to znamená, že výsledky týchto operácií nezávisia na reprezentantoch $\boldsymbol{x}$, $\boldsymbol{y}$ tried X resp. Y ale výlučne na podpriestoroch X, Y).

(e) Množina V/S s uvedenými operáciami súčtu a skalárneho násobku tvorí vektorový priestor nad poľom K; nazývame ho *faktorový priestor* vektorového priestoru V podľa podpriestoru S. Čo je nulou v tomto vektorovom priestore?

(f) Priradením $\boldsymbol{x} \mapsto \zeta_S(\boldsymbol{x}) = \boldsymbol{x}+S$ je definované surjektívne lineárne zobrazenie $\zeta_S : V \to V/S$ s jadrom $\operatorname{Ker}\zeta_S = S$.

(g) Nech U, V sú vektorové priestory nad poľom K a $\varphi : V \to U$ je lineárne zobrazenie. Priradením $\boldsymbol{x} + \operatorname{Ker}\varphi \mapsto \varphi(\boldsymbol{x})$ je *korektne* definované injektívne lineárne zobrazenie $V/\operatorname{Ker}\varphi \to U$. V dôsledku toho platí $V/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

(h) Ak V je konečnorozmerný, tak $\dim V/S = \dim V - \dim S$, čo je ďalšia analógia medzi vlastnosťami dimenzie a logaritmu (porovnaj s tvrdením 5.4.3.).

9.9. Nech V je vektorový priestor nad poľom K a S, T sú jeho lineárne podpriestory. Dokážte tzv. *kosoštvorcovú vetu o izomorfizme*:

$$(S+T)/T \cong S/(S\cap T).$$

(*Návod*: Dokážte, že priradením $(\boldsymbol{x}+\boldsymbol{y})+T \mapsto \boldsymbol{x}+(S\cap T)$, kde $\boldsymbol{x}\in S$, $\boldsymbol{y}\in T$, je korektne definovaný lineárny izomorfizmus $(S+T)/T \to S/(S\cap T)$.)

9.10. Nech pole K má konečný počet prvkov q, V je vektorový priestor nad K konečnej dimenzie n a S je jeho lineárny podpriestor dimenzie k $(0 \le k \le n)$. Dokážte postupne nasledujúce tvrdenia:

(a) Faktorový priestor V/S má práve q^{n-k} prvkov.

(b) Počet všetkých k-rozmerných *afinných* podpriestorov priestoru V je práve $q^{n-k}\binom{n}{k}_q$, kde $\binom{n}{k}_q$ je q-binomický koeficient (pozri cvičenia 5.16, 5.17).

10. Determinanty

V tejto kapitole zavedieme *determinanty* štvorcových matíc ľubovoľného rozmeru $n \times n$ nad pevným poľom K, preskúmame ich základné vlastnosti a naučíme sa ich počítať. Taktiež si ukážeme niekoľko príkladov ich využitia.

Čitateľ sa pravdepodobne už na strednej škole stretol s determinantmi reálnych matíc rozmerov 2×2 a 3×3. Možno tiež vie previesť výpočet determinantov vyšších rádov na výpočet determinantov nižších rádov pomocou ich rozvoja podľa nejakého riadku alebo stĺpca. So všeobecnou definíciou determinantu sa však asi dosiaľ nestretol. Ako čoskoro uvidíme, nie je to nijako priezračná definícia a na prvý pohľad určite nepôsobí „prirodzeným“ dojmom. Keďže nechceme, aby táto definícia „spadla z neba“, náš výklad začneme pomerne dlhým úvodom, ktorý má poslúžiť ako jej motivácia.

10.1. Orientovaný objem a multilineárne alternujúce funkcie

Na začiatok si položme prirodzenú otázku: Ako vyzerajú vzorce pre plošný obsah rovnobežníka v rovine $\mathbb{R}^2$, ktorého dve susedné strany tvoria vektory $\boldsymbol{u} = (u_1, u_2)^T$, $\boldsymbol{v} = (v_1, v_2)^T$, resp. pre objem rovnobežnostena v priestore $\mathbb{R}^3$, ktorého tri susedné hrany tvoria vektory $\boldsymbol{u} = (u_1, u_2, u_3)^T$, $\boldsymbol{v} = (v_1, v_2, v_3)^T$, $\boldsymbol{w} = (w_1, w_2, w_3)^T$?

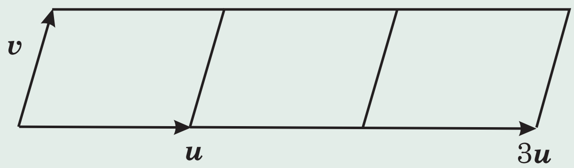
Vzorce, ktoré by vyjadrovali príslušný obsah alebo objem len pomocou súradníc vektorov $\boldsymbol{u}$, $\boldsymbol{v}$ resp. $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$, asi len tak z rukáva nevysypeme, môžeme sa však pokúsiť ich odvodiť. Najschodnejšia cesta vedie cez ujasnenie si vlastností, ktorým by mali takéto vzorce vyhovovať. Uvidíme, že tieto vlastnosti už jednoznačne (až na voľbu jednotkového obsahu či objemu) určujú hľadané vzorce nielen v rovine či v trojrozmernom priestore, ale možno ich bezprostredne zovšeobecniť na n-rozmerné vektorové priestory K^n nad ľubovoľným poľom K, hoci tu pojem „n-rozmerného objemu" stráca svoj názorný geometrický význam.

Označme teda $P(X)$ obsah rovinného útvaru X. Zrejme $P(X)$ je vždy nezáporné reálne číslo a pre zhodné útvary X, Y platí $P(X) = P(Y)$. Obsah je navyše *aditívny*, t. j. pre útvary X, Y také, že $P(X \cap Y) = 0$, platí $P(X \cup Y) = P(X) + P(Y)$. Konečne, $P(X) = 0$ pre ľubovoľnú úsečku X.

Obsah rovnobežníka $\{a\boldsymbol{u}+b\boldsymbol{v};\ a, b \in \langle 0, 1\rangle\}$ určeného vektormi $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^2$ budeme značiť $P(\boldsymbol{u}, \boldsymbol{v})$. Z práve sformulovaných vlastností obsahu vyplývajú rovnosti

$$P(\boldsymbol{u}, \boldsymbol{v}) = P(\boldsymbol{v}, \boldsymbol{u}), \qquad\qquad P(c\boldsymbol{u}, \boldsymbol{v}) = |c|P(\boldsymbol{u}, \boldsymbol{v})$$

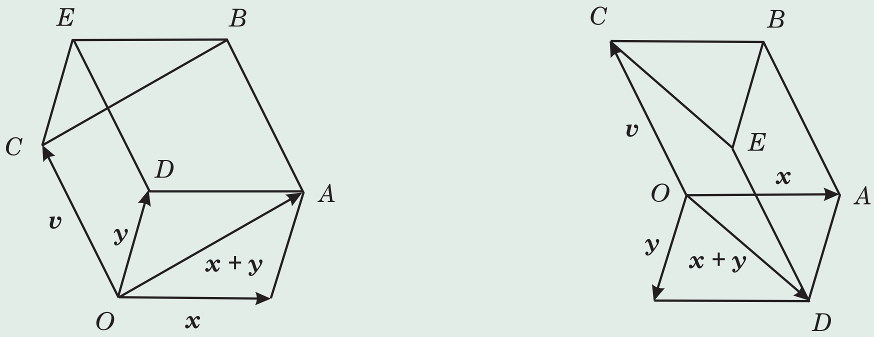
pre ľubovoľné $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^2$, $c \in \mathbb{Z}$. Druhá vlastnosť sa nazýva *pozitívna homogenita* a pre $c = 3$ je znázornená na nasledujúcom obrázku.



Obr. 10.1. K pozitívnej homogenite obsahu vektorového rovnobežníka

Platnosť druhej rovnosti pre všetky $c \in \mathbb{Q}$ možno už z toho jednoducho dokázať (pozri cvičenie 10.1). S jej platnosťou pre všetky $c \in \mathbb{R}$ je to už trochu zložitejšie – zakladá sa na istých úvah o „spojitosti" obsahu –, a tak jej radšej uveríme bez dôkazu.

Pozrime sa teraz na ďalšie dva obrázky. (Podotýkame, že oba znázorňujú situáciu *v rovine*, teda pri pohľade na ne treba potlačiť priestorové videnie, ktoré sa nám mimovoľne otvára.)



Obr. 10.2. K aditivite obsahu vektorového rovnobežníka

V prvom prípade určujú vektory $\boldsymbol{x}+\boldsymbol{y}$, $\boldsymbol{v}$ rovnobežník $OABC$, vektory $\boldsymbol{y}$, $\boldsymbol{v}$ rovnobežník $ODEC$ a rovnobežník vektorov $\boldsymbol{x}$, $\boldsymbol{v}$ je zhodný s rovnobežníkom $DABE$. Zo zhodnosti trojuholníkov OAD, CBE potom na základe uvedených vlastností obsahu vyplýva rovnosť

$$P(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{v}) = P(\boldsymbol{x}, \boldsymbol{v}) + P(\boldsymbol{y}, \boldsymbol{v}).$$

V druhom prípade určujú vektory $\boldsymbol{x}$, $\boldsymbol{v}$ rovnobežník $OABC$, vektory $\boldsymbol{x}+\boldsymbol{y}$, $\boldsymbol{v}$ rovnobežník $ODEC$ a rovnobežník vektorov $\boldsymbol{y}$, $\boldsymbol{v}$ je zhodný s rovnobežníkom $DABE$. Zo zhodnosti trojuholníkov ODA, CEB vyplýva $P(\boldsymbol{x}, \boldsymbol{v}) = P(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{v}) + P(\boldsymbol{y}, \boldsymbol{v})$, teda

$$P(\boldsymbol{x}+\boldsymbol{y}, \boldsymbol{v}) = P(\boldsymbol{x}, \boldsymbol{v}) - P(\boldsymbol{y}, \boldsymbol{v}).$$

To je v porovnaní s prvým prípadom nepríjemné prekvapenie, určite by sme dali prednosť rovnakej formule. Všimnime si však , že „kratšie otočenie“ vektora $\boldsymbol{y}$ do vektora $\boldsymbol{v}$ je orientované proti „kratším otočeniam“ vektorov $\boldsymbol{x}$ aj $\boldsymbol{x}+\boldsymbol{y}$ do vektora $\boldsymbol{v}$. V druhom prípade by sa nám preto hodilo, aby obsah rovnobežníka určeného vektormi $\boldsymbol{y}$, $\boldsymbol{v}$ mal z toho dôvodu opačné znamienko ako obsahy rovnobežníkov prislúchajúcich vektorom $\boldsymbol{x}$, $\boldsymbol{v}$ resp. $\boldsymbol{x}+\boldsymbol{y}$, $\boldsymbol{v}$. Tento cieľ možno dosiahnuť, ak namiesto plošného obsahu vektorových rovnobežníkov budeme uvažovať ich *orientovaný plošný obsah*, ktorý mení znamienko zámenou poradia dvoch vektorov, teda môže nadobúdať aj záporné hodnoty. Pôvodný nezáporný plošný obsah potom dostaneme ako absolútnu hodnotu orientovaného obsahu. Tento prístup nám navyše umožní zbaviť sa absolútnej hodnoty v rovnosti $P(c\boldsymbol{u}, \boldsymbol{v}) = |c|P(\boldsymbol{u}, \boldsymbol{v})$.

Podobnými úvahami, ktoré by si však vyžiadali trochu zložitejšie obrázky, tentokrát znázorňujúce naozaj priestorové situácie, by sme mohli dospieť i k potrebe skúmať *orientovaný objem* rovnobežnostena $\{a\boldsymbol{u} + b\boldsymbol{v} + c\boldsymbol{w};\ a, b, c \in \langle 0, 1\rangle\}$ určeného vektormi $\boldsymbol{u}$, $\boldsymbol{v}$, $\boldsymbol{w}$ v trojrozmernom priestore $\mathbb{R}^3$, prípadne *n-rozmerný n-rozmerný objem* rovnobežnostena $\{a_1\boldsymbol{u}_1 + \ldots + a_n\boldsymbol{u}_n;\ a_1, \ldots, a_n \in \langle 0, 1\rangle\}$ určeného vektormi $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ v n-rozmernom priestore $\mathbb{R}^n$ (pre $n > 3$ však bez možnosti sprostredkovať si geometrický vhľad obrázkami).

Pre čitateľa, ktorý sa už stretol s *vektorovým súčinom* v $\mathbb{R}^3$, poznamenajme, že orientovaný n-rozmerný objem sa správa do značnej miery podobne. Vektorový súčin $\boldsymbol{u} \times \boldsymbol{v}$ dvoch vektorov $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^3$, je vektor kolmý na rovinu $[\boldsymbol{u}, \boldsymbol{v}]$, ktorého dĺžka sa rovná plošnému obsahu rovnobežníka vektorov $\boldsymbol{u}$, $\boldsymbol{v}$ a orientácia je daná pravidlom pravej ruky (ak položíme dlaň pravej ruky malíčkom na vektor $\boldsymbol{u}$ tak, že zakrivené prsty smerujú k vektoru $\boldsymbol{v}$ po oblúku zodpovedajúcom uhlu $\leq 180°$, vztýčený palec ukazuje smer aj orientáciu vektora $\boldsymbol{u} \times \boldsymbol{v}$). Z toho dôvodu $\boldsymbol{u} \times \boldsymbol{v} = -(\boldsymbol{v} \times \boldsymbol{u})$.

Ak nahradíme reálne čísla ľubovoľným poľom K, vykonané úvahy nás privádzajú k nasledujúcim definíciám. Nech V je vektorový priestor nad poľom K a $1 \leq n \in \mathbb{N}$. Hovoríme, že zobrazenie $F : V^n \to K$ je

(a) *n-lineárne* alebo tiež *multilineárne*, ak pre každé $1 \leq j \leq n$ a ľubovoľné vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n \in V$ priradenie

$$\boldsymbol{x} \mapsto F(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{x}, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n)$$

definuje lineárne zobrazenie $V \to K$, t. j. pre všetky $\boldsymbol{x}, \boldsymbol{y} \in V$, $a, b \in K$ platí

$$\begin{aligned} &F(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, a\boldsymbol{x} + b\boldsymbol{y}, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n) \\ &\qquad = aF(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{x}, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n) + bF(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{j-1}, \boldsymbol{y}, \boldsymbol{u}_{j+1}, \ldots, \boldsymbol{u}_n); \end{aligned}$$

(b) *antisymetrické*, ak pre všetky $1 \leq i < j \leq n$ a ľubovoľné vektory $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in V$ platí

$$F(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_j, \ldots, \boldsymbol{u}_n) = -F(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_j, \ldots, \boldsymbol{u}_i, \ldots, \boldsymbol{u}_n).$$

Inak povedané, $F : V^n \to K$ je n-lineárne, ak dosadením ľubovoľných $n-1$ pevných vektorov na akékoľvek miesta do F dostaneme lineárne zobrazenie vo zvyšnej voľnej premennej;

F je antisymetrické, ak zámenou poradia ľubovoľných dvoch argumentov v F sa hodnota výsledku zmení na opačnú.

Cieľom našich úvah teda bolo čitateľa presvedčiť, že n-rozmerný orientovaný objem v $\mathbb{R}^n$ je multilineárna antisymetrická funkcia

$$\underbrace{\mathbb{R}^n \times \ldots \times \mathbb{R}^n}_{n\text{-krát}} \to \mathbb{R}.$$

Ukazuje sa však, že antisymetriu možno nahradiť zdanlivo slabšou, geometricky názornou podmienkou, motivovanou očividným vzťahom $P(\boldsymbol{u}, \boldsymbol{u}) = 0$ pre obsah degenerovaného vektorového rovnobežníka. Hovoríme, že zobrazenie $F : V^n \to K$ je

(c) *alternujúce*, ak pre ľubovoľné $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n \in V$ z podmienky $\boldsymbol{u}_i = \boldsymbol{u}_j$ pre nejaké $1 \leq i < j \leq n$ vyplýva
$$F(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n) = 0.$$

Ukážeme si, že uvedené tri vlastnosti spolu tesne súvisia. Najprv ale pripomeňme, že pole K má charakteristiku 2, ak v ňom platí $1 + 1 = 0$, čo je ekvivalentné s podmienkou $(\forall\, a \in K)(a = -a)$. Príkladom je pole $\mathbb{Z}_2$ (pozri paragraf 1.2). Ak $\operatorname{char} K \neq 2$, tak $(\forall\, a \in K)(a = -a \Rightarrow a = 0)$.

10.1.1. Lema. *Nech V je vektorový priestor nad poľom K a $F : V^n \to K$ je ľubovoľné zobrazenie.*

(a) *Ak* $\operatorname{char} K \neq 2$ *a F je antisymetrické, tak F je alternujúce.*

(b) *Ak F je multilineárne a alternujúce, tak F je antisymetrické.*

Dôkaz. (a) sme už vlastne dokázali v úvahe predchádzajúcej túto lemu.

(b) Nech F je multilineárne a alternujúce. Položme $\boldsymbol{x} = \boldsymbol{u}_i$, $\boldsymbol{y} = \boldsymbol{u}_j$ a zafixujme zvyšné z vektorov $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n$. Potom $G(\boldsymbol{x}, \boldsymbol{y}) = F(\boldsymbol{u}_1, \dots, \boldsymbol{x}, \dots, \boldsymbol{y}, \dots, \boldsymbol{u}_n)$ je bilineárne (t. j. 2-lineárne) alternujúce zobrazenie $V^2 \to K$. Stačí dokázať, že G je antisymentrické. Vďaka uvedeným vlastnostiam platí

$$\begin{aligned} G(\boldsymbol{x}, \boldsymbol{y}) + G(\boldsymbol{y}, \boldsymbol{x}) &= G(\boldsymbol{x}, \boldsymbol{x}) + G(\boldsymbol{x}, \boldsymbol{y}) + G(\boldsymbol{y}, \boldsymbol{x}) + G(\boldsymbol{y}, \boldsymbol{y}) \\ &= G(\boldsymbol{x} + \boldsymbol{y}, \boldsymbol{x} + \boldsymbol{y}) = 0, \end{aligned}$$

teda $G(\boldsymbol{x}, \boldsymbol{y}) = -G(\boldsymbol{y}, \boldsymbol{x})$.

Pre multilineárne zobrazenie tak alternácia implikuje antisymetriu, kým opačná implikácia platí len za dodatočného predpokladu $\operatorname{char} K \neq 2$ (no, na druhej strane, aj bez multilinearity).

10.1.2. Lema. *Nech $F : V^n \to K$, $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ sú ľubovoľné zobrazenia a $\boldsymbol{u}_1, \dots, \boldsymbol{u}_n \in V$.*

(a) *Ak F je antisymetrické a σ je permutácia, tak*

$$F(\boldsymbol{u}_{\sigma(1)}, \dots, \boldsymbol{u}_{\sigma(n)}) = (-1)^{|\sigma|} F(\boldsymbol{u}_1, \dots, \boldsymbol{u}_n).$$

(b) *Ak F je alternujúce a σ nie je permutácia, tak*

$$F(\boldsymbol{u}_{\sigma(1)}, \dots, \boldsymbol{u}_{\sigma(n)}) = 0.$$

Dôkaz. (a) Stačí si uvedomiť, že $|\sigma|$ označuje najmenší počet traspozícií (t. j. výmien poradia dvojíc), z ktorých možno zložiť permutáciu σ (pozri paragraf 0.5).

(b) Ak σ nie je permutácia, tak $\sigma(i) = \sigma(j)$, preto tiež $\boldsymbol{u}_{\sigma(i)} = \boldsymbol{u}_{\sigma(j)}$, pre nejaké $1 \leq i < j \leq n$. Označme $\boldsymbol{v}_k = \boldsymbol{u}_{\sigma(k)}$ pre $1 \leq k \leq n$. Potom $\boldsymbol{v}_i = \boldsymbol{v}_j$, a v dôsledku alternácie $F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j, \dots, \boldsymbol{v}_n) = 0$.

Zaznamenajme teraz niektoré základné vlastnosti multilineárnych alternujúcich (teda automaticky aj antisymetrických) zobrazení, ktoré budeme sústavne využívať.

10.1.3. Lema. *Nech $F : V^n \to K$ je multilineárne alternujúce zobraznie. Potom pre ľubovoľné $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in V$ platí:*

(a) *Pripočítaním skalárneho násobku nejakého z vektorov k inému vektoru sa hodnota $F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$ nezmení, t. j. pre ľubovoľné $c \in K$ a $i, j \leq n$ platí*

$$F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j + c\boldsymbol{v}_i, \dots, \boldsymbol{v}_n) = F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j, \dots, \boldsymbol{v}_n).$$

(b) *Ak sú vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ lineárne závislé, tak $F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_n) = 0$.*

Dôkaz. (a) Priamym výpočtom s použitím multilinearity a alternácie dostávame

$$\begin{aligned} &F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j + c\boldsymbol{v}_i, \dots, \boldsymbol{v}_n) \\ &\qquad = F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j, \dots, \boldsymbol{v}_n) + cF(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_n) \\ &\qquad = F(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j, \dots, \boldsymbol{v}_n) \end{aligned}$$

(b) Ak sú vektory $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$ lineárne závislé, tak niektorý z nich, povedzme $\boldsymbol{v}_k$, je lineárnou kombináciou ostatných, teda $\boldsymbol{v}_k = \sum_{i \neq k} c_i \boldsymbol{v}_i$ pre vhodné skaláry c_i. Z multilinearity a alternácie F potom vyplýva

$$F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k, \ldots, \boldsymbol{v}_n) = \sum_{i \neq k} c_i F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_n) = 0,$$

lebo v každom z uvedených výrazov $F(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_i, \ldots, \boldsymbol{v}_n)$ sa vektor $\boldsymbol{v}_i$ vyskytuje ako argument na i-tom aj na k-tom mieste.

Pozrime sa teraz bližšie, ako vyzerajú všetky bilineárne alternujúce zobrazenia $F : K^2 \times K^2 \to K$ nad poľom K. Zvoľme ľubovoľné vektory $\boldsymbol{u} = u_1\boldsymbol{e}_1 + u_2\boldsymbol{e}_2$ a $\boldsymbol{v} = v_1\boldsymbol{e}_1 + v_2\boldsymbol{e}_2$ z K^2. Ak dvakrát po sebe využijeme bilinearitu a na záver alternáciu a antisymetriu F, postupne dostaneme

$$\begin{aligned}
F(\boldsymbol{u}, \boldsymbol{v}) &= F(u_1\boldsymbol{e}_1 + u_2\boldsymbol{e}_2,\ \boldsymbol{v}) = u_1F(\boldsymbol{e}_1, \boldsymbol{v}) + u_2F(\boldsymbol{e}_2, \boldsymbol{v}) \\
&= u_1F(\boldsymbol{e}_1,\ v_1\boldsymbol{e}_1 + v_2\boldsymbol{e}_2) + u_2F(\boldsymbol{e}_2,\ v_1\boldsymbol{e}_1 + v_2\boldsymbol{e}_2) \\
&= u_1v_1F(\boldsymbol{e}_1, \boldsymbol{e}_1) + u_1v_2F(\boldsymbol{e}_1, \boldsymbol{e}_2) + u_2v_1F(\boldsymbol{e}_2, \boldsymbol{e}_1) + u_2v_2F(\boldsymbol{e}_2, \boldsymbol{e}_2) \\
&= F(\boldsymbol{e}_1, \boldsymbol{e}_2)(u_1v_2 - u_2v_1) = F(\boldsymbol{e}_1, \boldsymbol{e}_2)\begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix},
\end{aligned}$$

kde výraz

$$\begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix} = u_1v_2 - u_2v_1$$

čitateľ už iste pozná ako determinant matice $(\boldsymbol{u}, \boldsymbol{v}) = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \in K^{2\times 2}$.

Podobným spôsobom možno odvodiť aj tvar ľubovoľnej n-lineárnej alternujúcej funkcie $F : K^{n\times n} \to K$ (i teraz, ako obyčajne, prirodzene stotožňujeme n-tú karteziánsku mocninu $(K^n)^n$ stĺpcového vektorového priestoru $V = K^n$ s priestorom matíc $K^{n\times n}$). Nech $\boldsymbol{A} = (a_{ij}) \in K^{n\times n}$ je matica so stĺpcami

$$\boldsymbol{s}_j(\boldsymbol{A}) = a_{1j}\,\boldsymbol{e}_1 + \ldots + a_{nj}\,\boldsymbol{e}_n = \sum_{i=1}^{n} a_{ij}\,\boldsymbol{e}_i.$$

S využitím n-linearity F pre každý z n stĺpcov matice $\boldsymbol{A}$ možno výraz $F(\boldsymbol{A})$ postupne roznásobiť, čím dostaneme súčet n^n členov tvaru

$$a_{\sigma(1)\,1} \ldots a_{\sigma(n)\,n} F(\boldsymbol{e}_{\sigma(1)}, \ldots, \boldsymbol{e}_{\sigma(n)}),$$

z ktorých každý zodpovedá jednému zobrazeniu σ množiny $\{1, \ldots, n\}$ do seba. Podľa lemy 10.1.2. sčítance prislúchajúce zobrazeniam $\sigma \notin \mathcal{S}_n$ sú všetky rovné 0 a pre $\sigma \in \mathcal{S}_n$ platí

$$F(\boldsymbol{e}_{\sigma(1)}, \ldots, \boldsymbol{e}_{\sigma(n)}) = (-1)^{|\sigma|} F(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n).$$

Záverom tak dostávame

$$\begin{aligned} F(\boldsymbol{A}) &= F(\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) \sum_{\sigma\in\mathcal{S}_n} (-1)^{|\sigma|} a_{\sigma(1)\,1} \ldots a_{\sigma(n)\,n} \\ &= F(\boldsymbol{I}_n) \sum_{\sigma\in\mathcal{S}_n} (-1)^{|\sigma|} a_{\sigma(1)\,1} \ldots a_{\sigma(n)\,n}, \end{aligned}$$

kde príslušná suma obsahuje $n!$ sčítancov, jeden pre každú permutáciu $\sigma \in \mathcal{S}_n$.

10.2. Definícia a základné vlastnosti determinantu

Determinantom štvorcovej matice $\boldsymbol{A} = (a_{ij}) \in K^{n\times n}$ nazývame výraz

$$\det \boldsymbol{A} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum_{\sigma\in\mathcal{S}_n} (-1)^{|\sigma|} a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n}.$$

Ak nehrozí zámena s absolútnou hodnotou, používame tiež označenie $|\boldsymbol{A}|$. Determinant štvorcovej matice rádu n budeme nazývať *determinant rádu* n.

Špeciálne pre maticu $(a_{ij}) \in K^{3\times 3}$ dostávame vzorec

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33} - a_{11}a_{32}a_{23},$$

známy ako *Sarrusovo pravidlo.*

Skôr ako kuriozitu poznamenajme, že uvedená definícia zahŕňa aj prípad $n = 0$: pre (jedinú) prázdnu maticu $\boldsymbol{I}_0 = (\ ) \in K^{0\times 0}$ dáva $\det \boldsymbol{I}_0 = \det(\ ) = 1$.

Nasledujúce dve vlastnosti determinantov dokážeme ako dôsledky našej definície.

10.2.1. Tvrdenie. *Determinant transponovanej matice sa rovná determinantu pôvodnej matice, t. j.*

$$\det \boldsymbol{A}^T = \det \boldsymbol{A}$$

pre ľubovoľnú $\boldsymbol{A} \in K^{n\times n}$.

Dôkaz. Podľa definícií transponovanej matice a determinantu

$$\det \boldsymbol{A}^T = \sum_{\sigma \in \mathcal{S}_n} (-1)^{|\sigma|} a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

Keďže pre $\sigma \in \mathcal{S}_n$ platí $i = \sigma(j) \Leftrightarrow j = \sigma^{-1}(i)$, zoradením činiteľov v súčine $a_{1\sigma(1)} \dots a_{n\sigma(n)}$ podľa druhého indexu tento nadobudne tvar $a_{\sigma^{-1}(1)\,1} \dots a_{\sigma^{-1}(n)\,n}$. Pritom priradenie $\sigma \mapsto \sigma^{-1}$ je bijekcia $\mathcal{S}_n \to \mathcal{S}_n$. Navyše, ak $\sigma = \tau_1 \circ \dots \circ \tau_k$ je rozklad permutácie σ na transpozície, tak σ^{-1} je kompozícia tých istých transpozícií v opačnom poradí, preto $|\sigma| = \left|\sigma^{-1}\right|$. V dôsledku toho zámenou sumácie cez $\sigma \in \mathcal{S}_n$ za sumáciu cez $\sigma^{-1} = \varrho \in \mathcal{S}_n$ dostávame

$$\det \boldsymbol{A}^T = \sum_{\varrho \in \mathcal{S}_n} (-1)^{|\varrho|} a_{\varrho(1)\,1} \dots a_{\varrho(n)\,n} = \det \boldsymbol{A}.$$

Vďaka práve dokázanému tvrdeniu si všetky výsledky o determinantoch matíc zachovajú svoju platnosť, ak v nich každý výskyt slova „stĺpec“ nahradíme slovom „riadok“ a naopak. Tento princíp zámeny riadkov a stĺpcov budeme často využívať.

10.2.2. Tvrdenie. *Nech $1 \leq m < n$ a $\boldsymbol{A} \in K^{n\times n}$ je bloková matica tvaru*

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{D} \end{pmatrix},$$

kde $\boldsymbol{B} \in K^{m\times m}$, $\boldsymbol{C} \in K^{m\times(n-m)}$ a $\boldsymbol{D} \in K^{(n-m)\times(n-m)}$. Potom

$$\det \boldsymbol{A} = \det \boldsymbol{B} \cdot \det \boldsymbol{D}.$$

Dôkaz. Z uvedeného blokového tvaru matice $\boldsymbol{A}$ vyplýva

$$a_{ij} = \begin{cases} b_{ij}, & \text{ak } 1 \leq i, j \leq m, \\ c_{i\,j-m}, & \text{ak } 1 \leq i \leq m < j \leq n, \\ 0, & \text{ak } 1 \leq j \leq m < i \leq n, \\ d_{i-m\,j-m}, & \text{ak } m < i, j \leq n. \end{cases}$$

Označme $G = \{\sigma \in \mathcal{S}_n;\ (\forall\, j \leq m)(\sigma(j) \leq m)\}$. Potom pre $\sigma \in \mathcal{S}_n \smallsetminus G$ platí $a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n} = 0$, teda do hodnoty determinantu matice $\boldsymbol{A}$ prispievajú len sčítance zodpovedajúce permutáciám $\sigma \in G$. Navyše, $(\forall\, \sigma \in G)(m < j \ \Rightarrow\ m < \sigma(j))$, takže pre $\sigma \in G$ možno definovať permutácie $\sigma' \in \mathcal{S}_m$ a $\sigma'' \in \mathcal{S}_{n-m}$ predpismi $\sigma'(j) = \sigma(j)$, ak $1 \leq j \leq m$, resp. $\sigma''(k) = \sigma(k+m) - m$, ak $1 \leq k \leq n-m$. Zrejme priradením $\sigma \mapsto (\sigma', \sigma'')$ je daná bijekcia $G \to \mathcal{S}_m \times \mathcal{S}_{n-m}$ a platí $|\sigma| = |\sigma'| + |\sigma''|$. Takže môžeme písať

$$\begin{aligned} \det \boldsymbol{A} &= \sum_{\sigma \in G} (-1)^{|\sigma|} a_{\sigma(1)\,1} \dots a_{\sigma(m)\,m} a_{\sigma(m+1)\,m+1} \dots a_{\sigma(n)\,n} \\ &= \sum_{\sigma \in G} (-1)^{|\sigma'|+|\sigma''|} b_{\sigma'(1)\,1} \dots b_{\sigma'(m)\,m} d_{\sigma''(1)\,1} \dots d_{\sigma''(n-m)\,n-m} \\ &= \sum_{\sigma' \in \mathcal{S}_m} (-1)^{|\sigma'|} b_{\sigma'(1)\,1} \dots b_{\sigma'(m)\,m} \sum_{\sigma'' \in \mathcal{S}_{n-m}} (-1)^{|\sigma''|} d_{\sigma''(1)\,1} \dots d_{\sigma''(n-m)\,n-m} \\ &= \det \boldsymbol{B} \cdot \det \boldsymbol{D}. \end{aligned}$$

Na základe tvrdenia 10.2.1. teraz vieme, že $\det \boldsymbol{A} = \det \boldsymbol{B} \cdot \det \boldsymbol{D}$, aj keď sa nulový blok $\mathbf{0}$ nachádza nad a blok $\boldsymbol{C} \in K^{(n-m)\times m}$ pod diagonálou matice $\boldsymbol{A}$. Tvrdenie 10.2.2. možno taktiež zrejmým spôsobom zovšeobecniť na matice pozostávajúce z viacerých diagonálne zoradených štvorcových blokov, pod (nad) ktorými sú samé nuly. Spomeňme explicitne nasledujúce dva prípady:

(1) Ak $\boldsymbol{A}_1, \dots, \boldsymbol{A}_k$ sú štvorcové matice, tak

$$\det \operatorname{diag}(\boldsymbol{A}_1, \dots, \boldsymbol{A}_k) = \det \boldsymbol{A}_1 \cdot \ldots \cdot \det \boldsymbol{A}_k.$$

(2) Matica $\boldsymbol{A} \in K^{n \times n}$ sa nazýva *horná (dolná) trojuholníková matica*, ak $a_{ij} = 0$ pre $i < j$ (resp. pre $i > j$). Pre horné aj dolné trojuholníkové matice platí

$$\det \boldsymbol{A} = a_{11} \dots a_{nn},$$

t. j. determinant takej matice je súčinom jej diagonálnych prvkov. Špeciálne to platí pre diagonálne matice.

10.3. Charakterizácia determinantu a regulárnych matíc

Úvahy z paragrafu 10.1 možno zhrnúť do nasledujúcej vety.

10.3.1. Veta. *Determinant rádu n je n-lineárna alternujúca funkcia $K^{n \times n} \to K$ stĺpcov matice. Navyše, pre každý skalár $c \in K$ existuje jediné multilineárne alternujúce zobrazenie $F : K^{n \times n} \to K$ stĺpcov matice také, že $F(\boldsymbol{I}_n) = c$. Toto F je dané predpisom*

$$F(\boldsymbol{A}) = c \det \boldsymbol{A}.$$

Determinant $\det : K^{n\times n} \to K$ je teda jednoznačne určený ako n-lineárna alternujúca funkcia stĺpcov matice taká, že

$$\det \boldsymbol{I}_n = \det(\boldsymbol{e}_1, \dots, \boldsymbol{e}_n) = 1.$$

Táto rovnosť zodpovedá prirodzenej voľbe jednotky orientovaného n-rozmerného objemu v K^n – je ňou orientovaný objem rovnobežnostena určeného vektormi $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ (v tomto poradí).

V paragrafe 10.1 sme vlastne dokázali, že každá n-lineárna alternujúca funkcia $F : K^{n\times n} \to K$ musí mať uvedený tvar, t. j. je skalárnym násobkom determinantu. Zostáva však overiť, že determinant, tak, ako sme ho definovali v paragrafe 10.2, je naozaj multilineárne alternujúce zobrazenie. Hoci tieto vlastnosti sú intutívne jasné z našej konštrukcie, pre ambicióznejšieho čitateľa podáme ich dôkaz vychádzajúci len z definície determinantu. Navyše sa tým náš výklad stane formálne nezávislým na motivačných úvahách o orientovanom objeme z prvej časti úvodného paragrafu 10.1.

Dôkaz vety 10.3.1. odložíme až do nasledujúceho paragrafu, kde nám poslúži ako vhodný úvod do ďalšieho okruhu otázok. Na tomto mieste však zaznamenáme dva bezprostredné dôsledky tejto charakterizačnej vety. Samozrejme, v jej dôkaze sa na ne nebudeme odvolávať.

10.3.2. Veta. (Cauchy) *Pre ľubovoľné matice $\boldsymbol{A}$, $\boldsymbol{B} \in K^{n\times n}$ platí*

$$\det(\boldsymbol{A} \cdot \boldsymbol{B}) = \det \boldsymbol{A} \cdot \det \boldsymbol{B};$$

t. j. determinant súčinu matíc sa rovná súčinu ich determinantov.

Dôkaz. Zvoľme pevne maticu $\boldsymbol{A} \in K^{n\times n}$ a definujme zobrazenie $F : K^{n\times n} \to K$ predpisom $F(\boldsymbol{B}) = \det(\boldsymbol{A}\cdot\boldsymbol{B})$ pre $\boldsymbol{B} \in K^{n\times n}$. Overíme, že F je n-lineárne alternujúce zobrazenie stĺpcov matice $\boldsymbol{B}$; označme ich $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$.

Najprv overíme, že F je alternujúce. Nech $1 \le i < j \le n$ a $\boldsymbol{B}$ je matica taká, že $\boldsymbol{v}_i = \boldsymbol{v}_j$ pre nejaké $i < j$. Potom aj $\boldsymbol{A}\cdot\boldsymbol{v}_i = \boldsymbol{A}\cdot\boldsymbol{v}_j$, a s využitím alternácie determinantu dostávame

$$\begin{aligned} F(\boldsymbol{B}) &= \det(\boldsymbol{A}\cdot(\boldsymbol{v}_1, \dots, \boldsymbol{v}_i, \dots, \boldsymbol{v}_j, \dots, \boldsymbol{v}_n)) \\ &= \det(\boldsymbol{A}\cdot\boldsymbol{v}_1, \dots, \boldsymbol{A}\cdot\boldsymbol{v}_i, \dots, \boldsymbol{A}\cdot\boldsymbol{v}_j, \dots, \boldsymbol{A}\cdot\boldsymbol{v}_n) = 0. \end{aligned}$$

Teraz dokážeme multilinearitu F. Zafixujme stĺpce $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{j-1}, \boldsymbol{v}_{j+1}, \dots, \boldsymbol{v}_n$ a na miesto j-teho stĺpca dosaďme vektor $a\boldsymbol{x} + b\boldsymbol{y}$. S využitím n-linearity determinantu nám vyjde

$$\begin{aligned} F(\boldsymbol{v}_1, \dots, a\boldsymbol{x} + b\boldsymbol{y}, \dots, \boldsymbol{v}_n) &= \det(\boldsymbol{A}\cdot(\boldsymbol{v}_1, \dots, a\boldsymbol{x} + b\boldsymbol{y}, \dots, \boldsymbol{v}_n)) \\ &= \det(\boldsymbol{A}\cdot\boldsymbol{v}_1, \dots, \boldsymbol{A}\cdot(a\boldsymbol{x} + b\boldsymbol{y}), \dots, \boldsymbol{A}\cdot\boldsymbol{v}_n)) \\ &= \det(\boldsymbol{A}\cdot\boldsymbol{v}_1, \dots, a(\boldsymbol{A}\cdot\boldsymbol{x}) + b(\boldsymbol{A}\cdot\boldsymbol{y}), \dots, \boldsymbol{A}\cdot\boldsymbol{v}_n)) \\ &= a\det(\boldsymbol{A}\cdot\boldsymbol{v}_1, \dots, \boldsymbol{A}\cdot\boldsymbol{x}, \dots, \boldsymbol{A}\cdot\boldsymbol{v}_n) \\ &\qquad + b\det(\boldsymbol{A}\cdot\boldsymbol{v}_1, \dots, \boldsymbol{A}\cdot\boldsymbol{y}, \dots, \boldsymbol{A}\cdot\boldsymbol{v}_n) \\ &= a\det(\boldsymbol{A}\cdot(\boldsymbol{v}_1, \dots, \boldsymbol{x}, \dots, \boldsymbol{v}_n)) \\ &\qquad + b\det(\boldsymbol{A}\cdot(\boldsymbol{v}_1, \dots, \boldsymbol{y}, \dots, \boldsymbol{v}_n)) \\ &= aF(\boldsymbol{v}_1, \dots, \boldsymbol{x}, \dots, \boldsymbol{v}_n) + bF(\boldsymbol{v}_1, \dots, \boldsymbol{y}, \dots, \boldsymbol{v}_n). \end{aligned}$$

Podľa vety 10.3.1. má F tvar $F(\boldsymbol{B}) = c\det\boldsymbol{B}$ pre jednoznačne určený skalár $c = F(\boldsymbol{I}_n) = \det(\boldsymbol{A}\cdot\boldsymbol{I}_n) = \det\boldsymbol{A}$.

10.3.3. Veta. *Štvorcová matica* $\boldsymbol{A} \in K^{n\times n}$ *je regulárna práve vtedy, keď* $\det \boldsymbol{A} \neq 0$. *V tom prípade*

$$\det\bigl(\boldsymbol{A}^{-1}\bigr) = (\det \boldsymbol{A})^{-1}.$$

Dôkaz. Ak $\boldsymbol{A}$ je singulárna, tak jej stĺpce sú lineárne závislé. Podľa lemy 10.1.3. (b) je $F(\boldsymbol{A}) = 0$ pre ľubovoľnú n-lineárnu alternujúcu funkciu $F : K^{n\times n} \to K$. Teda špeciálne $\det \boldsymbol{A} = 0$. Naopak, nech $\boldsymbol{A}$ je regulárna. Potom podľa vety 10.3.2.,

$$\det \boldsymbol{A} \cdot \det\bigl(\boldsymbol{A}^{-1}\bigr) = \det\bigl(\boldsymbol{A} \cdot \boldsymbol{A}^{-1}\bigr) = \det \boldsymbol{I}_n = 1.$$

Preto $\det \boldsymbol{A} \neq 0$ a $\det\bigl(\boldsymbol{A}^{-1}\bigr) = (\det \boldsymbol{A})^{-1}$.

10.4. Laplaceov rozvoj determinantu

Náš výklad začneme sľúbeným dôkazom. Keďže pre $n = 0, 1$ niet čo dokazovať, aby sme sa vyhli rozpitvávaniu trivialít, budeme v celom paragrafe predopkladať, že $n \geq 2$.

Dôkaz vety 10.3.1. Najprv dokážeme, že determinant je alternujúca funkcia. Nech $\boldsymbol{A} \in K^{n\times n}$ je taká, že $\boldsymbol{s}_i(\boldsymbol{A}) = \boldsymbol{s}_j(\boldsymbol{A})$ pre nejaké $i < j$. Označme $\tau \in \mathcal{S}_n$ transpozíciu, ktorá vymieňa i a j (a ostatné prvky necháva namieste). Potom pre všetky $k, l \leq n$ platí $a_{kl} = a_{\tau(k)\,l}$. Množina všetkých párnych permutácií množiny $\{1, \ldots, n\}$ sa zvykne značiť $\mathcal{A}_n$. Zrejme priradením $\sigma \mapsto \tau \circ \sigma$ je daná bijekcia $\mathcal{A}_n \to \mathcal{S}_n \smallsetminus \mathcal{A}_n$. S využitím toho môžeme počítať

$$\begin{aligned}
\det \boldsymbol{A} &= \sum_{\sigma \in \mathcal{S}_n} (-1)^{|\sigma|} a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n} \\
&= \sum_{\sigma \in \mathcal{A}_n} a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n} - \sum_{\sigma \in \mathcal{S}_n \smallsetminus \mathcal{A}_n} a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n} \\
&= \sum_{\sigma \in \mathcal{A}_n} a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n} - \sum_{\sigma \in \mathcal{A}_n} a_{(\tau\circ\sigma)(1)\,1} \dots a_{(\tau\circ\sigma)(n)\,n} \\
&= \sum_{\sigma \in \mathcal{A}_n} \left(a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n} - a_{\tau(\sigma(1))\,1} \dots a_{\tau(\sigma(n))\,n}\right) = 0.
\end{aligned}$$

Teraz dokážeme, že $\det \boldsymbol{A}$ je lineárnou funkciou j-teho stĺpca $(a_{1j}, \dots, a_{nj})^T$. Pre $i \le n$ označme $\mathcal{S}_n(i,j) = \{\sigma \in \mathcal{S}_n;\ i = \sigma(j)\}$ a položme

$$\tilde{a}_{ij} = \sum_{\sigma \in \mathcal{S}_n(i,j)} (-1)^{|\sigma|} a_{\sigma(1)\,1} \dots a_{\sigma(j-1)\,j-1} a_{\sigma(j+1)\,j+1} \dots a_{\sigma(n)\,n}.$$

Potom zrejme

$$\det \boldsymbol{A} = \sum_{i=1}^{n} \tilde{a}_{ij} a_{ij} = (\tilde{a}_{1j}, \dots, \tilde{a}_{nj}) \cdot (a_{1j}, \dots, a_{nj})^T,$$

čo dokazuje spomínanú linearitu.

Na základe tvrdenia 10.2.1. platí aj „riadková verzia“ práve dokázanej vety 10.3.1. Špeciálne, determinant je takisto multilineárna alternujúca funkcia riadkov matice a (keďže

$\sigma \in \mathcal{S}_n(i,j) \Leftrightarrow \sigma^{-1} \in \mathcal{S}_n(j,i)$) pre i-ty riadok $(a_{i1}, \ldots, a_{in})$ matice $\boldsymbol{A}$ jej determinant má rozvoj

$$\det \boldsymbol{A} = \sum_{j=1}^{n} a_{ij}\tilde{a}_{ij} = (a_{i1}, \ldots, a_{in}) \cdot (\tilde{a}_{i1}, \ldots, \tilde{a}_{in})^T.$$

s rovnako definovanými koeficientmi $\tilde{a}_{ij}$.

Uvedený prvok $\tilde{a}_{ij}$ nazývame *algebraickým doplnkom* prvku a_{ij} v matici $\boldsymbol{A}$. Maticu $\widetilde{\boldsymbol{A}} = (\tilde{a}_{ij})_{n\times n}$ nazývame *maticou algebraických doplnkov* k matici $\boldsymbol{A}$.

10.4.1. Tvrdenie. *Nech $\boldsymbol{A}_{ij}$ označuje maticu rádu $n-1$, ktorá vznikne z matice $\boldsymbol{A} \in K^{n\times n}$ vynechaním i-teho riadku a j-teho stĺpca. Potom*

$$\tilde{a}_{ij} = (-1)^{i+j}|\boldsymbol{A}_{ij}|.$$

Dôkaz. Označme $\boldsymbol{B}$ maticu, ktorá vznikne nahradením j-teho stĺpca matice $\boldsymbol{A}$ stĺpcovým vektorom $\boldsymbol{e}_i \in K^n$. Zrejme $\tilde{a}_{ij} = |\boldsymbol{B}|$. Ak budeme v matici $\boldsymbol{B}$ postupne vymieňať stĺpce s indexmi j a $j+1$, ďalej $j+1$ a $j+2$, atď., až nakoniec $n-1$ a n, a potom riadky s indexmi i a $i+1$, ďalej $i+1$ a $i+2$, atď., až napokon $n-1$ a n, dostaneme maticu tvaru

$$\boldsymbol{C} = \begin{pmatrix} \boldsymbol{A}_{ij} & \mathbf{0} \\ \boldsymbol{b} & 1 \end{pmatrix},$$

kde $\boldsymbol{b}$ vznikne z i-teho riadku matice $\boldsymbol{A}$ vynechaním j-teho prvku a $\mathbf{0}$ je nulový stĺpec dĺžky $n-1$. Podľa tvrdenia 10.2.2. (a poznámky za jeho dôkazom), determinant tejto matice je $|\boldsymbol{A}_{ij}|$. Keďže determinant je alternujúca funkcia tak stĺpcov ako aj riadkov matice a všetkých výmien bolo dohromady $(n-j)+(n-i)=2n-(i+j)$, platí

$$\tilde{a}_{ij}=|\boldsymbol{B}|=(-1)^{2n-(i+j)}|\boldsymbol{C}|=(-1)^{i+j}|\boldsymbol{A}_{ij}|.$$

Determinanty matíc, ktoré vzniknú vynechaním niektorých riadkov a rovnakého počtu sĺtpcov z matice $\boldsymbol{A}\in K^{n\times n}$, nazývame jej *minormi*, prípadne *subdeterminantmi* determinantu $|\boldsymbol{A}|$. Dosadením získaných hodnôt algebraických doplnkov do rozvoja determinantu rádu n podľa niektorého riadku resp. stĺpca tak dostávame jeho vyjadrenie pomocou subdeterminantov rádu $n-1$.

10.4.2. Veta. *Nech $\boldsymbol{A}\in K^{n\times n}$, $1\leq k,l\leq n$. Potom*

$$|\boldsymbol{A}|=\sum_{j=1}^{n}(-1)^{k+j}a_{kj}\,|\boldsymbol{A}_{kj}|=\sum_{i=1}^{n}(-1)^{i+l}a_{il}\,|\boldsymbol{A}_{il}|.$$

Uvedené súčty nazývame *Laplaceovými rozvojmi* determinantu $|\boldsymbol{A}|$ – prvý podľa k-teho riadku, druhý podľa l-teho stĺpca.

10.5. Výpočet determinantu

Skôr než sa pustíme do výpočtov konkrétnych determinantov, skúsme si urobiť inventúru prostriedkov, ktoré máme nato k dispozícii, a posúdiť ich vhodnosť.

Asi sa zhodneme na tom, že výpočet determinantu rádu n podľa jeho definície, ako súčtu $n!$ súčinov po n činiteľoch, by bol značne ťažkopádny. Pokiaľ sme sa stretli len s prípadmi

$n = 2$ alebo $n = 3$, nemusíme si to jasne uvedomiť. Avšak už $4! = 24$, $5! = 120$ a funkcia $n!$ veľmi rýchlo rastie. Preto je potrebné pouvažovať o nejakej inej metóde.

Keďže determinant je multilineárnou alternujúcou funkciou tak riadkov ako aj stĺpcov matice, ako najprirodzenejšia sa nám ponúka metóda úpravy matice na hornú prípadne dolnú trojuholníkovú maticu pomocou elementárnych riadkových i stĺpcových operácií. Ako sme už spomínali v poznámke (2) za dôkazom tvrdenia 10.2.2.:

(0) Determinant trojuholníkovej matice sa rovná súčinu jej diagonálnych prvkov.

Pripomeňme si aj nasledujúce pravidlá z paragrafu 10.1 o vplyve ERO a ESO na determinant:

(1) Výmenou poradia dvoch riadkov alebo stĺpcov matice sa hodnota jej determinantu zmení na opačnú.

(2) Vynásobením nejakého riadku alebo stĺpca matice nenulovým skalárom $c \in K$ sa jej determinant zmení na c-násobok pôvodnej hodnoty.

(3) Pripočítaním skalárneho násobku nejakého riadku matice k jej inému riadku, resp. násobku nejakého jej stĺpca k inému stĺpcu sa hodnota jej determinantu nezmení.

Všimnite si, že len tretí typ menovaných úprav necháva determinant bezo zmeny! Poznamenajme, že úpravy typu (3) spolu s pravidlom (0) plne postačujú na výpočet akéhokoľvek determinantu. Bez pravidiel (1) a (2) sa možno kľudne zaobísť, občas nám však môžu pomôcť sprehľadniť situáciu, preto sa im nebudeme vyhýbať.

Často býva užitočné výslovne si uvedomiť nasledujúci dôsledok pravidiel (1) – (3):

(4) Ak matica obsahuje nulový riadok alebo stĺpec, prípadne dva rovnaké riadky alebo stĺpce, tak jej determinant je 0.

Mohlo by sa zdať, že sme akosi pozabudli na Laplaceov rozvoj. Táto metóda umožňuje previesť výpočet determinantu rádu n na výpočet n determinantov rádu $n-1$, presnejšie na istú ich lineárnu kombináciu. Ak by sme dôsledne pokračovali ďalej, mohli by sme túto úlohu previesť na výpočet $n(n-1)$ determinantov rádu $n-2$, atď., až by sme napokon dostali $n!$ determinantov rádu 1. Ak si to dobre premyslíme, zistíme, že takýto výpočet by bol rovnako efektívny (či, lepšie povedané, neefektívny) ako výpočet determinantu priamo na základe jeho definície.

Jednako sa Laplaceovho rozvoja celkom nezriekame. Odporúčame ho však používať len vtedy, keď sú všetky prvky príslušného riadku či stĺpca, podľa ktorého determinant rozvíjame, až na jednu výnimku rovné nule. Vtedy vlastne nejde ani tak o rozvoj ako o zníženie rádu daného determinantu o 1 (bez nárastu počtu determinantov). Toto odporúčanie sformulujeme do nášho predposledného pravidla:

(5) Nech všetky prvky i-teho riadku prípadne j-teho stĺpca matice $\boldsymbol{A}$ s výnimkou prvku a_{ij} sú rovné 0. Potom
$$|\boldsymbol{A}| = (-1)^{i+j} a_{ij}\, |\boldsymbol{A}_{ij}|.$$

Všimnite si, že pravidlo (0) možno dostať ako dôsledok $(n-1)$-násobného použitia pravidla (5) a zrejmého faktu, že determinant matice (a) typu 1×1 je samotná hodnota a.

Ak si ešte uvedomíme, že determinanty rádu 2 možno najvýhodnejšie počítať priamo z definície:

(6)
$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12},$$

je to už naozaj všetko, čo potrebujeme vedieť na *efektívny* výpočet determinantu.

10.5.1. Príklad. Vypočítame determinant reálnej matice

$$\boldsymbol{A} = \begin{pmatrix} 2 & 2 & 1 & 1 & 1 \\ 5 & 6 & 3 & 4 & 5 \\ 7 & 5 & 3 & 5 & 7 \\ 13 & 10 & 3 & 8 & 13 \\ 7 & 2 & 1 & 1 & 6 \end{pmatrix}.$$

Najprv odpočítame prvý riadok od piateho a druhý od štvrtého. V matici, ktorú takto získame, odpočítame piaty stĺpec od prvého a štvrtý od druhého. Postupne tak dostaneme

$$|\boldsymbol{A}| = \begin{vmatrix} 2 & 2 & 1 & 1 & 1 \\ 5 & 6 & 3 & 4 & 5 \\ 7 & 5 & 3 & 5 & 7 \\ 8 & 4 & 0 & 4 & 8 \\ 5 & 0 & 0 & 0 & 5 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 3 & 4 & 5 \\ 0 & 0 & 3 & 5 & 7 \\ 0 & 0 & 0 & 4 & 8 \\ 0 & 0 & 0 & 0 & 5 \end{vmatrix} = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$$

Priznávame, že výpočet, ktorý sme práve predviedli je tak trochu podraz voči čitateľovi. Úpravy, ktoré sme pri ňom použili, boli totiž len opačným postupom, ktorým sme pri formulácii úlohy z vopred narafičenej výslednej hornej trojuholníkovej matice „uvarili“ zadanie. Napokon, tak je tomu s väčšinou úloh v učebniciach. No čitateľ, ktorého autor „nevpustil do kuchyne“, má len malú nádej toto optimálne riešenie nájsť. Teda aspoň pokiaľ je úloha dobre postavená. Predvedieme preto aj iné, „normálne“ riešenie, na aké má šancu prísť aj nezasvätený riešiteľ.

Najprv odpočítame tretí stĺpec od štvrtého aj piateho a jeho dvojnásobok od prvého aj druhého stĺpca. V ďalšom kroku determinant rozvinieme podľa prvého riadku:

$$|\boldsymbol{A}| = \begin{vmatrix} 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 3 & 1 & 2 \\ 1 & -1 & 3 & 2 & 4 \\ 7 & 4 & 3 & 5 & 10 \\ 5 & 0 & 1 & 0 & 5 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 1 & 2 \\ 1 & -1 & 2 & 4 \\ 7 & 4 & 5 & 10 \\ 5 & 0 & 0 & 5 \end{vmatrix}.$$

Teraz odpočítame prvý stĺpec od posledného a získaný determinant rozvinieme podľa posledného riadku:

$$|\boldsymbol{A}| = \begin{vmatrix} -1 & 0 & 1 & 3 \\ 1 & -1 & 2 & 3 \\ 7 & 4 & 5 & 3 \\ 5 & 0 & 0 & 0 \end{vmatrix} = -5 \begin{vmatrix} 0 & 1 & 3 \\ -1 & 2 & 3 \\ 4 & 5 & 3 \end{vmatrix}.$$

Po odpočítaní trojnásobku druhého stĺpca od tretieho a rozvinutí podľa prvého riadku sme konečne v cieli:

$$|\boldsymbol{A}| = -5 \begin{vmatrix} 0 & 1 & 0 \\ -1 & 2 & -3 \\ 4 & 5 & -12 \end{vmatrix} = 5 \begin{vmatrix} -1 & -3 \\ 4 & -12 \end{vmatrix} = 5\,(12 + 3 \cdot 4) = 5 \cdot 24 = 120.$$

10.5.2. Príklad. Vypočítame tzv. *Vandermondov determinant* rádu n

$$\mathrm{VD}_n(x_1, x_2, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}.$$

Odpočítaním prvého riadku od všetkých ostatných riadkov a následným rozvojom podľa prvého stĺpca dostaneme

$$\mathrm{VD}_n(x_1, x_2, \dots, x_n) = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 0 & x_2 - x_1 & x_2^2 - x_1^2 & \dots & x_2^{n-1} - x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & x_n - x_1 & x_n^2 - x_1^2 & \dots & x_n^{n-1} - x_1^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} x_2 - x_1 & x_2^2 - x_1^2 & \dots & x_2^{n-1} - x_1^{n-1} \\ \vdots & \vdots & & \vdots \\ x_n - x_1 & x_n^2 - x_1^2 & \dots & x_n^{n-1} - x_1^{n-1} \end{vmatrix}.$$

Odpočítajme teraz od každého stĺpca počnúc druhým x_1-násobok predchádzajúceho stĺpca. V determinante, ktorý získame, je na mieste (i, k), kde $1 \leq i, k \leq n-1$, prvok

$$\left(x_{i+1}^k - x_1^k\right) - x_1\left(x_{i+1}^{k-1} - x_1^{k-1}\right) = x_{i+1}^{k-1}(x_{i+1} - x_1).$$

Ak teda vyjmeme z i-teho riadku činiteľ $x_{i+1} - x_1$, postupne nám vyjde

$$\mathrm{VD}_n(x_1, x_2, \ldots, x_n) = \begin{vmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \ldots & x_2^{n-2}(x_2 - x_1) \\ \vdots & \vdots & & \vdots \\ x_n - x_1 & x_n(x_n - x_1) & \ldots & x_n^{n-2}(x_n - x_1) \end{vmatrix}$$

$$= (x_2 - x_1) \ldots (x_n - x_1) \begin{vmatrix} 1 & x_2 & \ldots & x_2^{n-2} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \ldots & x_n^{n-2} \end{vmatrix}$$

$$= (x_2 - x_1) \ldots (x_n - x_1)\ \mathrm{VD}_{n-1}(x_2, \ldots, x_n).$$

Teraz už aj bez počítania determinantov vidíme, že

$$\mathrm{VD}_{n-1}(x_2, \ldots, x_n) = (x_3 - x_2) \ldots (x_n - x_2)\ \mathrm{VD}_{n-2}(x_3, \ldots, x_n),$$

atď. Keďže zrejme $\mathrm{VD}_1(x_n) = 1$, dostávame výsledok

$$\mathrm{VD}_n(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i),$$

kde symbolom $\prod$ označujeme súčin príslušných činiteľov.

10.6. Inverzná matica a Cramerovo pravidlo

V tomto záverečnom paragrafe si predvedieme dva príklady využitia determinantov. Vyjadríme pomocou nich inverznú maticu k regulárnej štvorcovej matici a riešenie sústavy lineárnych rovníc s regulárnou štvorcovou maticou. Vopred poznamenajme, že tieto vyjadrenia sa na priame výpočty príliš nehodia. Na druhej strane tým, že vyjadrujú inverznú maticu a riešenie spomínanej sústavy v tvare prehľadných ucelených formúl, sú významné hlavne z teoretického hľadiska.

Nech $\boldsymbol{A} \in K^{n\times n}$ a $1 \leq i, k \leq n$ sú rôzne indexy. Označme $\boldsymbol{B}$ maticu, ktorá vznikne z matice $\boldsymbol{A}$ nahradením jej k-teho riadku i-tym riadkom. Potom matica $\boldsymbol{B}$ má (aspoň) dva riadky rovnaké, menovite i-tý a k-tý, preto $|\boldsymbol{B}| = 0$. Na druhej strane matice $\boldsymbol{A}$ a $\boldsymbol{B}$ sa líšia nanajvýš v k-tom riadku, preto $\boldsymbol{A}_{kj} = \boldsymbol{B}_{kj}$ pre každé $1 \leq j \leq n$. Z toho dôvodu sú algebraické doplnky zodpovedajúcich si prvkov k-tych riadkov oboch matíc rovnaké:

$$\tilde{b}_{kj} = (-1)^{k+j}|\boldsymbol{B}_{kj}| = (-1)^{k+j}|\boldsymbol{A}_{kj}| = \tilde{a}_{kj}.$$

Ak rozvinieme determinant matice $\boldsymbol{B}$ podľa jej k-teho riadku, dostaneme

$$\det \boldsymbol{B} = \sum_{j=1}^{n} b_{kj}\tilde{b}_{kj} = \sum_{j=1}^{n} a_{ij}\tilde{a}_{kj} = 0.$$

Spojenie tejto rovnosti s Laplaceovým rozvojom determinantu matice $\boldsymbol{A}$ podľa k-teho riadku dáva

$$\sum_{j=1}^{n} a_{ij}\tilde{a}_{kj} = \boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{r}_k\big(\widetilde{\boldsymbol{A}}\big)^T = \boldsymbol{r}_i(\boldsymbol{A}) \cdot \boldsymbol{s}_k\big(\widetilde{\boldsymbol{A}}^T\big) = \begin{cases} |\boldsymbol{A}|, & \text{ak } i = k,\\ 0, & \text{ak } i \neq k.\end{cases}$$

Inak povedané

$$\boldsymbol{A} \cdot \widetilde{\boldsymbol{A}}^T = |\boldsymbol{A}|\, \boldsymbol{I}_n.$$

Inverznú maticu k regulárnej štvorcovej matici $\boldsymbol{A}$ potom dostaneme tak, že transponovanú maticu jej algebraických doplnkov vydelíme determinantom $|\boldsymbol{A}|$. Tým sme dokázali nasledujúcu vetu.

10.6.1. Veta. *Nech $\boldsymbol{A} \in K^{n\times n}$ je regulárna matica. Potom*

$$\boldsymbol{A}^{-1} = \frac{1}{|\boldsymbol{A}|}\widetilde{\boldsymbol{A}}^T.$$

10.6.2. Príklad. Nájdeme inverznú maticu k reálnej matici

$$\boldsymbol{A} = \begin{pmatrix} 1 & -2 \\ 5 & -3 \end{pmatrix}.$$

Jej determinant a maticu algebraických doplnkov vypočítame ľahko:

$$|\boldsymbol{A}| = 1 \cdot (-3) - 5 \cdot (-2) = 7, \qquad \widetilde{\boldsymbol{A}} = \begin{pmatrix} -3 & -5 \\ 2 & 1 \end{pmatrix}.$$

Preto

$$\boldsymbol{A}^{-1} = \frac{1}{7}\begin{pmatrix} -3 & 2 \\ -5 & 1 \end{pmatrix}.$$

Poznamenajme však, že okrem štvorcových matíc rádu 2, kedy je to v podstate jedno, je výpočet inverznej matice pomocou ERO alebo ESO, ako sme ho popísali v paragrafe ??, podstatne výhodnejší než výpočet na základe vety 10.6.1. Už pre matice rádu 3 by sme na to potrebovali vypočítať jeden determinant rádu 3 a deväť determinantov rádu 2. Vo všeobecnom prípade by sme museli vypočítať jeden determinant rádu n a n^2 determinantov rádu $n-1$. Čitateľ sa pravdepodobne po prvýkrát stretol s determinantmi v súvislosti s riešením sústav lineárnych rovníc, v ktorých je počet rovníc a neznámych ten istý. Možno by si v prípadoch 2×2 a 3×3 ešte vedel spomenúť aj na príslušné vzorce. Takéto vzorce, známe ako *Cramerovo pravidlo*, však platia v ľubovoľnom rozmere $n \times n$.

10.6.3. Veta. *Nech $\boldsymbol{A} \in K^{n\times n}$ je regulárna matica, $\boldsymbol{b} \in K^n$ a pre $1 \le j \le n$ nech $\boldsymbol{A}_j^{\boldsymbol{b}}$ označuje maticu, ktorá vznikne z matice $\boldsymbol{A}$ nahradením jej j-teho stĺpca stĺpcovým vektorom $\boldsymbol{b}$. Potom sústava $\boldsymbol{A}\cdot\boldsymbol{x} = \boldsymbol{b}$ má jediné riešenie*

$$\boldsymbol{x} = \left(\frac{|\boldsymbol{A}_1^{\boldsymbol{b}}|}{|\boldsymbol{A}|}, \frac{|\boldsymbol{A}_2^{\boldsymbol{b}}|}{|\boldsymbol{A}|}, \dots, \frac{|\boldsymbol{A}_n^{\boldsymbol{b}}|}{|\boldsymbol{A}|}\right)^T.$$

Dôkaz. Podľa vety ?? má uvedená sústava jediné riešenie $\boldsymbol{x} = \boldsymbol{A}^{-1}\cdot\boldsymbol{b}$. Ak do tohto vyjadrenia dosadíme za $\boldsymbol{A}^{-1}$ z vety 10.6.1., pre j-tu zložku vektora $\boldsymbol{x}$ nám vyjde

$$x_j = \frac{1}{|\boldsymbol{A}|}\sum_{i=1}^{n} \tilde{a}_{ij} b_i = \frac{|\boldsymbol{A}_j^{\boldsymbol{b}}|}{|\boldsymbol{A}|},$$

lebo zodpovedajúce si prvky j-tych stĺpcov matíc $\boldsymbol{A}$ a $\boldsymbol{A}_j^{\boldsymbol{b}}$ majú rovnaké algebraické doplnky, takže uvedený súčet je Laplaceov rozvoj determinantu $|\boldsymbol{A}_j^{\boldsymbol{b}}|$ podľa j-teho stĺpca.

Varujeme však čitateľa pred používaním Cramerovho pravidla na riešenie konkrétnych sústav n lineárnych rovníc o n neznámych. Metóda úpravy rozšírenej matice sústavy na redukovaný stupňovitý tvar pomocou ERO je oveľa rýchlejšia a pohodlnejšia. Kým vyriešenie takej sústavy pomocou ERO vyžaduje úpravu jedinej matice typu $n \times (n+1)$, pri riešení Cramerovým pravidlom by sme museli pri výpočte determinantov upraviť $n+1$ matíc typu $n \times n$.

Na obranu determinantov však poznamenajme, že stretnutie s najdôležitejšími príkladmi ich využitia nás ešte len čaká. Popri tzv. Gramových determinantoch to bude najmä v súvislosti s charakteristickým polynómom a vlastnými hodnotami lineárnych transformácií a štvorcových matíc.

Cvičenia

10.1. Nech U, V sú vektorové priestory nad poľom $\mathbb{Q}$. Dokážte nasledujúce tvrdenia:

(a) Ak $F : V \to U$ je zobrazenie také, že pre všetky $c \in \mathbb{Z}$, $\boldsymbol{v} \in V$ platí $F(c\boldsymbol{v}) = cF(\boldsymbol{v})$, tak uvedená rovnosť platí aj pre všetky $c \in \mathbb{Q}$.

(b) Ak $F : V \to U$ je zobrazenie také, že pre všetky $c \in \mathbb{Z}$, $\boldsymbol{v} \in V$ platí $F(c\boldsymbol{v}) = |c|F(\boldsymbol{v})$, tak uvedená rovnosť platí aj pre všetky $c \in \mathbb{Q}$.

10.2. Nech $U, V_1, \ldots, V_n$ sú vektorové priestory nad poľom K. Podobne ako v paragrafe 10.1 definujte pojem n-lineárneho zobrazenia $F : V_1 \times \ldots \times V_n \to U$. Označme $\mathcal{L}_n(V_1, \ldots, V_n, U)$ množinu všetkých n-lineárnych zobrazení $F : V_1 \times \ldots \times V_n \to U$; ak $V_1 = \ldots = V_n = V$, tak miesto $\mathcal{L}_n(V_1, \ldots, V_n, U)$ píšeme len $\mathcal{L}_n(V, U)$. Dokážte, že množina $\mathcal{L}_n(V_1, \ldots, V_n, U)$ tvorí lineárny podpriestor vektorového priestoru $U^{V_1\times\ldots\times V_n}$ všetkých zobrazení $V_1\times\ldots\times V_n\to U$.

10.3. Nech U, V sú vektorové priestory nad poľom K a $n\ge 2$. Definujte pojmy symetrického, antisymetrického a alternujúceho zobrazenia $F: V^n\to U$. Dokážte postupne nasledujúce tvrdenia:

(a) Množiny $\mathrm{Sym}_n(V,U)$ všetkých symetrických zobrazení $V^n\to U$, $\mathrm{Asym}_n(V,U)$ všetkých antisymetrických zobrazení $V^n\to U$ a $\mathrm{Alt}_n(V,U)$ všetkých alternujúcich zobrazení $V^n\to K$ sú lineárne podpriestory vektorového priestoru U^{V^n} všetkých zobrazení $V^n\to U$.

(b) Ak $\mathrm{char}\,K=2$, tak $\mathrm{Sym}_n(V,U)=\mathrm{Asym}_n(V,U)$.

(c) Ak $\mathrm{char}\,K\ne 2$, tak $\mathrm{Asym}_n(V,U)\subseteq\mathrm{Alt}_n(V,U)$ a $\mathrm{Sym}_n(V,U)\cap\mathrm{Asym}_n(V,U)=\{\mathbf{0}\}$, kde $\mathbf{0}$ tentokrát označuje identicky nulové zobrazenie $V^n\to U$.

(d) $\mathcal{L}_n(V,U)\cap\mathrm{Alt}_n(V,U)\subseteq\mathcal{L}_n(V,U)\cap\mathrm{Asym}_n(V,U)$.

(e) Ak $\mathrm{char}\,K\ne 2$, tak $\mathcal{L}_n(V,U)\cap\mathrm{Alt}_n(V,U)=\mathcal{L}_n(V,U)\cap\mathrm{Asym}_n(V,U)$.

(f) Nájdite príklad bilineárneho (t. j. 2-lineárneho) zobrazenia $\mathbb{Z}_2\times\mathbb{Z}_2\to\mathbb{Z}_2$, ktoré je symetrické (teda aj antisymetrické), no nie je alternujúce.

(g) Ak $\dim V=n$, tak $\dim\big(\mathcal{L}_n(V,K)\cap\mathrm{Alt}_n(V,K)\big)=1$. (*Návod*: Dobre si uvedomte, čo vlastne hovorí druhá časť vety 10.3.1.)

10.4. Dokážte Lemy 10.1.2. a 10.1.3. za všeobecnejších podmienok cvičenia 10.3, t. j. pre zobrazenia $F: V^n\to U$.

10.5. (a) Vypočítajte orientovaný aj neorientovaný plošný obsah rovnobežníka určeného vektormi $\boldsymbol{u}=(1,5)^T$, $\boldsymbol{v}=(3,-4)^T$ v rovine $\mathbb{R}^2$.

(b) Vypočítajte orientovaný aj neorientovaný objem rovnobežnostena určeného vektormi $\boldsymbol{u}=(3,2,-1)$, $\boldsymbol{v}=(5,0,4)$, $\boldsymbol{w}=(1,1,1)$ v priestore $\mathbb{R}^3$.

(c) Vypočítajte orientovaný aj neorientovaný štvorrozmerný objem štvorrozmerného „rovnobežnonadstena“ určeného vektormi $\boldsymbol{e}_1+\boldsymbol{e}_2$, $\boldsymbol{e}_2-2\boldsymbol{e}_3$, $4\boldsymbol{e}_3-2\boldsymbol{e}_4$, $3\boldsymbol{e}_1+\boldsymbol{e}_4$ v priestore $\mathbb{R}^4$.

10.6. Vypočítajte nasledujúce determinanty nad poľom $\mathbb{R}$:

(a) $\begin{vmatrix} 0 & 5 & 3 & -2 \\ 1 & 1 & 6 & -4 \\ 2 & 1 & -3 & 0 \\ 3 & 3 & 9 & -6 \end{vmatrix}$; (b) $\begin{vmatrix} 3 & 5 & 7 & 4 \\ 0 & 1 & 0 & -1 \\ 1 & 4 & 4 & 0 \\ 4 & 7 & 11 & 6 \end{vmatrix}$; (c) $\begin{vmatrix} 3 & 7 & 131 & -17 \\ 2 & 6 & -21 & 401 \\ 0 & 0 & 100 & 29 \\ 0 & 0 & 3 & 1 \end{vmatrix}$; (d) $\begin{vmatrix} 2 & -2 & 0 & 4 & 0 \\ 2 & 3 & 5 & 7 & 11 \\ 1 & -2 & 4 & 0 & 2 \\ 0 & 6 & 0 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 \end{vmatrix}$; (e) $\begin{vmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 & 5 \\ 1 & 2 & 3 & 0 & 4 \\ 1 & -1 & 0 & 7 & 0 \\ 1 & 0 & 1 & 2 & 3 \end{vmatrix}$.

10.7. Rozhodnite, pre ktoré hodnoty parametra λ je uvedená matica regulárna resp. singulárna. Riešte nad každým z polí $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$ a $\mathbb{Z}_7$ pre nasledujúce matice (ak vám prekáža, že niektorý prvok matice nepatrí do príslušného poľa $\mathbb{Z}_p$, nahraďte ho jeho zvyškom po delení číslom p):

(a) $\begin{pmatrix} 1 & \lambda & 0 \\ 0 & 1 & \lambda \\ \lambda & 0 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 1-\lambda & \lambda & 0 \\ \lambda & 2-\lambda & 0 \\ \lambda^3 & 3-\lambda^2 & \lambda \end{pmatrix}$; (c) $\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & \lambda & 1 & \lambda \\ 0 & 1 & \lambda & 1 \\ \lambda & 1 & 0 & 1 \end{pmatrix}$; (d) $\begin{pmatrix} \lambda-1 & 1 & 0 & 4 \\ -2 & \lambda+1 & 5 & 3 \\ 0 & 0 & \lambda-1 & 0 \\ 0 & 0 & 5 & \lambda \end{pmatrix}$.

10.8. Pre ľubovoľnú maticu $\boldsymbol{A}$ rozmeru $n \times n$ nad poľom K a skalár $c \in K$ platí $\det(c\boldsymbol{A}) = c^n \det \boldsymbol{A}$, špeciálne $\det(-\boldsymbol{A}) = (-1)^n \det \boldsymbol{A}$. Dokážte.

10.9. Nech $n \geq 2$ a $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$ sú štvorcové matice rádu n nad poľom K. Na príklade ukážte, že (okrem prípadu $\boldsymbol{B} = \mathbf{0}$ alebo $\boldsymbol{C} = \mathbf{0}$) pre z nich zloženú blokovú maticu neplatí nasledujúce „zovšeobecnenie“ pravidla na výpočet determinantu matíc rozmeru 2×2:

$$\begin{vmatrix} \boldsymbol{A} & \boldsymbol{B} \\ \boldsymbol{C} & \boldsymbol{D} \end{vmatrix} = |\boldsymbol{A}|\,|\boldsymbol{D}| - |\boldsymbol{B}|\,|\boldsymbol{C}|.$$

10.10. Pomocou algebraických doplnkov nájdite explicitné vyjadrenie pre inverzné matice k nasledujúcim maticiam a sformulujte nutné a postačujúce podmienky ich existencie:

(a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; (b) $\begin{pmatrix} 1 & x & x^2 \\ 1 & y & y^2 \\ 1 & z & z^2 \end{pmatrix}$; (c) $\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$; (d) $\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$; (e) $\begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix}$.

Zovšeobecnite výsledky úloh (d), (e) na matice ľubovoľného rádu n.

10.11. Nájdite riešenia nasledujúcich sústav lineárnych rovníc nad poľom $\mathbb{R}$ pomocou Cramerovho pravidla:

(a) $x + y = 1$, $3x - 5y = 4$;

(b) $x - 4y = -2$, $7x + 2y = 1$;

(c) $x + y - z = 0$, $2x + 3z = 3$, $3x + y - 2z = -5$;

(d) $2x + y + 2z = 10$, $4x - y = -3$, $y + 2z = 0$;

(e) $x + 2y + 3z + 4u = 10$, $y + 2z + 3u = 6$, $z + 2u = 3$, $y - z + u = 1$.

10.12. Nech $\boldsymbol{A} \in K^{m\times n}$ je matica nad poľom K a $I \subseteq \{1,\dots,m\}$, $J \subseteq \{1,\dots,n\}$ sú dve množiny indexov s rovnakým počtom prvkov $k \le \min(m,n)$. Označme $\boldsymbol{A}_{IJ} \in K^{k\times k}$ štvorcovú maticu rádu k tvorenú tými prvkami a_{ij} matice $\boldsymbol{A}$, pre ktoré $i \in I$ a $j \in J$. Determinanty takto vzniknutých matíc $\boldsymbol{A}_{IJ}$ nazývame *minormi matice* $\boldsymbol{A} \in K^{m\times n}$ rádu k. Jednoducho povedané, minory matice $\boldsymbol{A}$ sú determinanty štvorcových matíc, ktoré vzniknú vynechaním niektorých riadkov a stĺpcov matice $\boldsymbol{A}$. Minory prislúchajúce množinám indexov tvaru $I = J = \{1,\dots,k\}$ sa nazývajú *hlavné minory* matice $\boldsymbol{A}$.

Dokážte, že hodnosť matice $\boldsymbol{A}$ je najväčšie prirodzené číslo k, pre ktoré existuje nenulový minor rádu k matice $\boldsymbol{A}$. (*Návod*: Ukážte, že ak $\boldsymbol{r}_{i_1}(\boldsymbol{A})$, …, $\boldsymbol{r}_{i_k}(\boldsymbol{A})$ sú lineárne nezávislé riadky matice $\boldsymbol{A}$, tak existujú indexy stĺpcov j_1, …, j_k také, že matica $\left(a_{i_p j_q}\right)_{k\times k}$ má hodnosť k.)

10.13. (a) Vypočítajte všetky minory reálnej matice $\begin{pmatrix} 1 & 1 & -1 \\ 3 & 0 & -2 \end{pmatrix}$.

(b) Vypočítajte všetky hlavné minory komplexnej matice $\begin{pmatrix} 2+\mathrm{i} & 0 & 3\mathrm{i} & 4 \\ 4\mathrm{i} & 3-2\mathrm{i} & 2 & 6-\mathrm{i} \\ 2-\mathrm{i} & 1+5\mathrm{i} & 0 & 2\mathrm{i} \end{pmatrix}$.

10.14. Nech $\boldsymbol{A} \in K^{n\times n}$ je štvorcová matica rádu n a I, J sú dve podmnožiny množiny $\{1,\dots,n\}$ s rovnakým počtom prvkov $k \le n$. *Algebraickým doplnkom minora* $|\boldsymbol{A}_{IJ}|$ matice $\boldsymbol{A}$ (pozri cvičenie 12) nazývame výraz $(-1)^{I+J}|\boldsymbol{A}_{I'J'}|$, kde I', J' označujú doplnky množín I resp. J v množine $\{1,\dots,n\}$ a $I + J = \sum_{i\in I} i + \sum_{j\in J} j$. Nech ďalej $\mathcal{P}_k(n)$ označuje množinu všetkých k-prvkových podmnožín množiny $\{1,\dots,n\}$ (zrejme $\#\,\mathcal{P}_k(n) = \binom{n}{k}$).

Dokážte nasledujúce zovšeobecnenia Laplaceovho rozvoja determinantu z vety 10.4.2.:

(a) *Laplaceov rozvoj determinantu podľa vybraných riadkov.* Pre ľubovoľnú množinu $I \in \mathcal{P}_k(n)$ vybraných (indexov) riadkov matice $\boldsymbol{A}$ platí

$$|\boldsymbol{A}| = \sum_{J \in \mathcal{P}_k(n)} (-1)^{I+J} \, |\boldsymbol{A}_{IJ}| \, |\boldsymbol{A}_{I'J'}| \, .$$

(b) *Laplaceov rozvoj determinantu podľa vybraných stĺpcov.* Pre ľubovoľnú množinu $J \in \mathcal{P}_k(n)$ vybraných (indexov) stĺpcov matice $\boldsymbol{A}$ platí

$$|\boldsymbol{A}| = \sum_{I \in \mathcal{P}_k(n)} (-1)^{I+J} \, |\boldsymbol{A}_{IJ}| \, |\boldsymbol{A}_{I'J'}| \, .$$

10.15. (a) Vypočítajte algebraické doplnky minorov rádu 2 reálnej matice $\begin{pmatrix} 1 & 1 & 3 & 0 \\ -1 & 0 & -2 & 1 \\ 4 & 6 & 4 & -2 \\ 3 & 7 & 2 & 0 \end{pmatrix}$.

(b) Rozviňte determinant matice z úlohy (a) podľa prvého a druhého riadku. Výsledok prorovnajte s hodnotou determinatu získanou priamym výpočtom.

10.16. Nech K je pole, $x_0, x_1, \ldots, x_n$ sú navzájom rôzne a $y_0, y_1, \ldots, y_n$ sú ľubovoľné prvky z K.

(a) Dokážte, že potom existuje práve jeden polynóm $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in K^{(n)}[x]$ taký, že $f(x_0) = y_0$, $f(x_1) = y_1$, $\ldots$, $f(x_n) = y_n$; $f(x)$ sa nazýva *interpolačný polynóm* konečnej funkcie $x_i \mapsto y_i$, kde $0 \le i \le n$. (*Návod*: Rozpíšte uvedené rovnosti do sústavy lineárnych rovníc v neznámych $a_0, a_1, \ldots, a_n$ a využite Vandermondov determinant.)

(b) Odvoďte tzv. *Lagrangeov tvar interpolačného polynómu*

$$f(x) = \sum_{i=0}^{n} y_i \prod_{j \ne i} \frac{x - x_j}{x_i - x_j} \, .$$

(c) Vyjadrite koeficienty interpolačného polynómu $f(x)$ pomocou Cramerovho pravidla.

(d) Nech K je pole reálnych čísel $\mathbb{R}$. V prípade *ekvidistančného delenia* x_0, $x_1 = x_0 + d$, $x_2 = x_0 + 2d$, $\dots$, $x_n = x_0 + nd$ s krokom $d > 0$, nájdite explicitné vzorce pre koeficienty interpolačného polynómu, ak $0 \le n \le 3$.

10.17. S využitím výsledkov predchádzajúceho cvičenia riešte nasledujúce úlohy:

(a) Nájdite kvadratické polynómy $f_0(x), f_1(x), f_2(x) \in \mathbb{R}^{(2)}[x]$, ktorých grafy prechádzajú bodmi $(-1,0)$, $(1,0)$, $(3,-2)$, resp. $(-1,0)$, $(0,-1)$, $(2,5)$, resp. $(0,-1)$, $(2,5)$, $(3,-2)$.

(b) Nájdite kubické polynómy $g_1(x), g_2(x) \in \mathbb{R}^{(3)}[x]$, ktorých grafy prechádzajú bodmi $(0,-1)$, $(1,0)$, $(2,5)$, $(3,-2)$, resp. $(-1,0)$, $(0,-1)$, $(1,0)$, $(2,5)$.

(c) Nájdite bikvadratický polynóm $h(x) \in \mathbb{R}^{(4)}[x]$, ktorého graf prechádza bodmi $(-1,0)$, $(0,-1)$, $(1,0)$, $(2,5)$, $(3,-2)$.

(d) Načrtnite grafy funkcií f_0, f_1, f_2, g_1, g_2 a h na intervale $\langle -2, 4\rangle$ a porovnajte ich.

10.18. *Permanentom* štvorcovej matice $\boldsymbol{A} = (a_{ij})_{n\times n}$ nad poľom K nazývame výraz

$$\operatorname{per} \boldsymbol{A} = \sum_{\sigma\in\mathcal{S}_n} a_{\sigma(1)\,1} \dots a_{\sigma(n)\,n}.$$

Formálne teda permanent dostaneme vynechaním znamienkových koeficientov $\operatorname{sgn}\sigma = (-1)^{|\sigma|}$ v definícii determinantu. Dokážte postupne nasledujúce tvrdenia:

(a) Ak maticu chápeme ako riadok jej stĺpcov, tak permanent je n-lineárne symetrické zobrazenie $K^{n\times n} \to K$ (pozri cvičenie 10.3).

(b) Pre ľubovoľnú maticu $\boldsymbol{A} \in K^{n\times n}$ platí $\operatorname{per} \boldsymbol{A}^T = \operatorname{per} \boldsymbol{A}$.

(c) Ak $\operatorname{char} K = 2$, tak pre každú maticu $\boldsymbol{A} \in K^{n\times n}$ platí $\operatorname{per} \boldsymbol{A} = \det \boldsymbol{A}$.

10.19. (a) Odvoďte všeobecný vzorec na výpočet permanentu matíc rozmeru 2×2.

(b) Odvoďte vzorec analogický Sarrusovmu pravidlu na výpočet permanentu matíc rozmeru 3×3. [1]

(c) Vypočítajte permanenty reálnych matíc $\boldsymbol{A} = \begin{pmatrix} 1 & 3 \\ 2 & -6 \end{pmatrix}$, $\boldsymbol{B} = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 7 & -1 \\ 1 & 1 & 1 \end{pmatrix}$.

(c) Odvoďte z výsledkov úlohy (a), že permanent regulárnej štvorcovej matice sa môže rovnať nule, kým permanent singulárnej štvorcovej matice nemusí byť 0.

10.20. Nech $X = \{x_1, \ldots, x_n\}$ je n-prvková množina a (X, H) je orientovaný graf s množinou vrcholov X (pozri cvičenie 2.7). Hovoríme, že *permutácia* $\sigma \in \mathcal{S}_n$ *žije na grafe* (X, H), ak pre každé $i \leq n$ platí $(x_i, x_{\sigma(i)}) \in H$.

(a) Nech $\boldsymbol{H} \in \mathbb{R}^{n \times n}$ je incidenčná matica grafu (X, H). Potom počet všetkých permutácií $\sigma \in \mathcal{S}_n$, ktoré žijú na grafe (X, H), je práve per $\boldsymbol{H}$. Dokážte.

(b) Pre každý z grafov z obrázku 2.1 vypočítajte permanent jeho incidenčnej matice a určte počet permutácií, ktoré na ňom žijú (pokúste sa riešiť obe úlohy pre daný graf v optimálnom poradí).

---

[1] Stojí za poznámku, že – na rozdiel od determinantu – nepoznáme nijaký jednoduchý, rýchly algoritmus na výpočet permanentu štvorcových matíc všeobecného rádu n nad poľami charakteristiky $\neq 2$. Dokonca máme dobré dôvody domnievať sa, že taký algoritmus neexistuje.

Register